FREUD RÓBERT

LINEÁRIS ALGEBRA

Javított és bővített kilencedik kiadás, 2024

Lektorok:

Dr. Hermann Péter
egyetemi docens, kandidátus

Dr. Kiss Emil
egyetemi tanár, az MTA doktora

ISBN 963 463 080 4

Az első kiadás megírását részben az „Alapítvány a Magyar Felsőoktatásért és Kutatásért” támogatta.

TARTALOM

BEVEZETÉS

A könyv az előző kiadás javított és bővített változata.

Kiknek ajánljuk?

A könyv egy bevezető egy vagy két féléves lineáris algebra tárgy anyagát öleli fel, és betekintést nyújt további témákba is. Elsősorban a matematikus, informatikus és matematika tanárszakos hallgatók szempontjait tartja szem előtt, de jól használható más természettudományi, műszaki és társadalomtudományi területeken is. Emellett alkalmas a lineáris algebra önálló tanulmányozására, így mindenki haszonnal forgathatja, aki érdeklődik a téma iránt.

Előismeretek

A középiskolás anyagon túlmenően nincs szükség előismeretre. A felhasznált algebrai fogalmakat (komplex számok, polinom, test, gyűrű stb.) és ezek leglényegesebb tulajdonságait a könyv végén az „Algebrai alapfogalmak" c. fejezetben foglaljuk össze. Ez a „függelék" amellett, hogy megkönnyíti a könyv többi részének a megértését, egy önmagában is érdekes és hasznos területre nyújt betekintést.

Módszer

A „hogyan" mellett a „miért" megválaszolására is nagy hangsúlyt fektetünk, tehát a fogalmak, tételek és módszerek részletes tárgyalása magába foglalja az anyag mélyebb összefüggéseinek a megvilágítását is. A fogalmakat és állításokat a formális megfogalmazáson túlmenően is alaposan „körbejárjuk", „emberközelbe" hozzuk; ezeket mindig példákkal illusztráljuk, megpróbáljuk a „szemléletes" tartalmukat megjeleníteni, a „lényegi" vonásaikat megragadni, bemutatjuk a korábbi anyaghoz és a matematika más területeihez való kapcsolódást, felhívjuk a figyelmet az esetleges buktatókra, és elemezzük, mi indokolja az adott fogalom bevezetését. Nagy súlyt helyezünk arra, hogy lehetőleg a konkrétból kiindulva haladjunk az általános felé.

A bizonyítások leírásakor — különösen a bevezetőbb jellegű témaköröknél — elemi és kevésbé absztrakt segédeszközöket használunk, és a túlzottan tömör indoklások helyett inkább részletes magyarázatokat adunk, hogy a megértést a „kezdő" Olvasók számára is maximálisan megkönnyítsük. Gyakran külön is emlékeztetünk a korábban kikötött vagy a korábbiakból következő feltételekre.

Valódi és szórakoztató alkalmazásokat kínálunk, amelyek gyakran már meglepően egyszerű lineáris algebrai eszközökkel is látványosan kezelhetők. A teljes 9. fejezetet kombinatorikai jellegű problémáknak szenteljük. Itt a lineáris algebra természetes (és sokszor az egyetlen hatékony) eszköz számos gráfelméleti, geometriai, számelméleti kérdés megválaszolására. Megoldjuk

Hilbert harmadik problémáját, ellátogatunk Páratlanvárosba és Párosvárosba, és elővesszük Erdős Pál egyik kedvenc témáját, a Sidon-sorozatokat. A 10. fejezet rövid bevezető egy másik fontos alkalmazásba, a kódelméletbe.

Feladatok

A fejezeteket alkotó minden egyes pont után feladatok következnek. A feladatok részben az aktuális fogalmak, tételek és módszerek megértését ellenőrzik és ezek elmélyítését segítik elő, részben újabb példákat, összefüggéseket és alkalmazásokat mutatnak be, részben pedig az adott témakörhöz kapcsolódó egyéb problémákat vizsgálnak. Gyakran szerepelnek feladatnak „álcázott" tételek is, amelyek az anyag részletesen nem tárgyalt további érdekes vonatkozásaira, távolabbi összefüggéseire hívják fel a figyelmet.

Ennek megfelelően a feladatok mennyisége és nehézsége igen tág határok között mozog, az éppen sorra kerülő anyag témájától, terjedelmétől és mélységétől függően. A(z általunk) nehezebbnek ítélt feladatokat csillaggal, a kiemelkedően nehéz feladatokat pedig két csillaggal jelezzük. (Természetesen egy feladat nehézsége mindig relatív; a megoldó képességeitől, érdeklődésétől és általános előismeretétől eltekintve jelentősen függhet — többek között — a korábban megoldott feladatoktól is.)

A legtöbb feladat eredményét és/vagy a megoldáshoz vezető útmutatást az „Eredmények és útmutatások" c. fejezetben közöljük. Néhány (elsősorban nehezebb) feladathoz részletes megoldást is adunk a „Megoldások" c. fejezetben, ezeket a feladatokat a kitűzésnél **M** betűvel jelöltük meg.

Az egyes fejezetek kapcsolata

Szoros egységet alkot és egymásra épül az 1., a 2. és a 3. fejezet, amelyekben a „legklasszikusabb" lineáris algebra anyagot jelentő determinánsokat, mátrixokat és lineáris egyenletrendszereket tárgyaljuk.

Hasonló szoros kapcsolatban áll egymással a 4., az 5. és a 6. fejezet, amelyekben a vektorterekre, valamint a lineáris leképezésekre és transzformációkra vonatkozó általános alapismeretek szerepelnek. A 4. és 5. fejezet legnagyobb része az első három fejezet nélkül is megérthető.

A 7–10. fejezetek általában erősen támaszkodnak az első hat fejezetre. Közülük a bilineáris függvényeket és az euklideszi tereket bemutató 7. és 8. tartozik szorosan össze. A 9. fejezetben főleg kombinatorikus jellegű alkalmazásokat gyűjtöttünk csokorba, a 10. fejezet pedig algebrai kódokkal foglalkozik. Ez a két fejezet egymástól és — a 9. fejezet néhány részét leszámítva — a 7. és a 8. fejezettől is független.

A könyv végén szereplő „A" jelű fejezetben — mint már említettük — röviden összefoglaljuk a könyvben felhasznált algebrai alapismereteket.

Technikai tudnivalók

Az egyes fejezetek ún. pontokra tagolódnak. A definíciókat, a tételeket, feladatokat és képleteket $k.m.n$ típusú módon számoztuk, ahol k a fejezetet, m ezen belül a pontot és n a ponton belüli sorszámot jelenti. A definíciók és a tételek „közös listán" futnak, tehát pl. az 5.1.4 Definíció után az 5.1.5 Tétel következik. Az illusztrációs példák (sima, egy számmal történő) számozása pontonként újrakezdődik. A definíciók, illetve a tételek megfogalmazásának a végén ♣ áll, a bizonyítások befejezését pedig ■ jelzi.

A jelölések, fogalmak, tételek visszakeresését megkönnyít(het)i a „Tárgymutató, jelölések" c. fejezet, amelyet igyekeztünk nagyon részletesen összeállítani.

A leggyakrabban előforduló fogalmakkal kapcsolatban itt is felsoroljuk, hogy a vektorokat vastag latin kisbetűvel (pl. $\mathbf{a}$), a skalárokat általában görög kisbetűvel (pl. α), a mátrixokat dőlt latin nagybetűvel (pl. A), a lineáris leképezéseket írott latin nagybetűvel (pl. $\mathcal{A}$), a bilineáris függvényeket pedig vastag latin nagybetűvel (pl. $\mathbf{A}$) jelöljük. Felhívjuk még a figyelmet arra, hogy a nulla nagyon sok mindent jelenthet (egész számot, gyűrű nullelemét, testbeli skalárt, vektort, vektorteret, alteret, mátrixot, lineáris leképezést, bilineáris függvényt stb.), és ezek közül többet ugyanúgy is jelölünk, azonban a szövegösszefüggésből mindig kiderül, hogy melyik jelentésről van szó.

A polinomokat f vagy $f(x)$, a fokszámukat „deg", a komplex számok valós és képzetes részét „Re", illetve „Im" jelöli, pl. $\deg(x^3+x)=3$, $\operatorname{Re}(4-i)=4$, $\operatorname{Im}(4-i)=-1$. Megkülönböztetjük a (valós) számok alsó és felső egész részét, és ezeket $\lfloor\ \rfloor$, illetve $\lceil\ \rceil$ jelöli, így pl. $\lfloor\pi\rfloor=3$, $\lceil\pi\rceil=4$. Az oszthatóságra, a legnagyobb közös osztóra és a legkisebb közös többszörösre (az egész számok és a polinomok esetén is) a szokásos jelöléseket használjuk, tehát pl. $x-1 \mid x^2-1$, $(9,15)=3$, $[9,15]=45$. A $[\ ]$ szögletes zárójel a legtöbbször egyszerűen zárójelet, néha legkisebb közös többszöröst, a 9.6 pontban pedig zárt intervallumot jelöl, továbbá $[\mathcal{A}]$, illetve $[\mathbf{A}]$ az $\mathcal{A}$ lineáris leképezés, illetve az $\mathbf{A}$ bilineáris függvény mátrixát jelenti.

Tanácsok

Matematikáról lévén szó, nem kell külön hangsúlyoznunk, hogy az egyes fogalmak, tételek alapos megértése nélkül azok megtanulása fabatkát sem ér. Ezért azt javasoljuk az Olvasónak, hogy ne ugorja át a legapróbb homályosnak tűnő részletet sem, a felhasznált hivatkozásokat keresse vissza és ellenőrizze, és pontosan gondolja végig a „könnyen igazolható" jelzéssel közölt állításokat is.

A formális, pontról pontra történő megértésen túlmenően egy fogalomnak vagy tételnek akkor lesz igazán „mondanivalója”, ha azt jól el tudjuk helyezni a matematikai környezetében, világosan látjuk a kapcsolatait és alkalmazásait. Ehhez érdemes minél több illusztrációs példát végiggondolni, valamint az adott fogalomhoz, tételhez kapcsolódó feladatokat megoldani.

Néhány további jótanács az Olvasóhoz. A tanulás során ne ragaszkodjon betűről betűre a könyvbeli szöveghez, fogalmazza meg másképp, saját szavaival az adott fogalmat vagy állítást (de gondosan ellenőrizze, hogy tényleg „ugyanazt” mondja-e). Vizsgálja meg, hogy egy tétel bizonyításakor az egyes feltételeket hol használjuk ki, hogyan szól és igaz-e a tétel megfordítása stb.

A feladatok megoldását (a legkönnyebbektől eltekintve) ne csak fejben gondolja át, hanem írja is le részletesen; eközben gyakran egyszerűsödik a gondolatmenet, világosabbá válik a lényeg, és a(z esetleges) hibák vagy hiányok is kevésbé sikkadnak el.

Mindig próbálja meg kideríteni a feladat „mondanivalóját”. Az is nagyon hasznos, ha általánosít vagy önállóan vet fel újabb problémákat (még akkor is, ha ezeket nem tudja megoldani).

Lehetőleg csak akkor nézze meg a feladatokhoz adott útmutatást vagy megoldást, ha semmiképpen sem boldogul a feladattal. Térjen inkább visszsza többször is ugyanarra a problémára, esetleg oldja meg előbb valamelyik speciális esetet.

Eltérések az előző kiadáshoz képest

A könyv szerkezete alapvetően nem változott. A hibajavítások, átfogalmazások, néhány bizonyítás egyszerűsítése és egy-egy feladat cseréje, törlése vagy átcsoportosítása mellett

- a 6. fejezet kibővítettük a Cayley–Hamilton-tétel és a Jordan normálalak bizonyításával;
- a 9. fejezetben több újabb alkalmazás szerepel feladatok formájában;
- a 10. fejezet tárgyalásmódjában áttértünk a szokásos terminológiára: a kód (nem a kódoló függvényt, hanem) a kódszavak halmazát jelenti;
- az A fejezet elejére három új pontot iktattunk be kombinatorikai, számelméleti és a komplex számokra vonatkozó alapismeretekről.

Hibák és hiányosságok

A könyvben minden igyekezetem ellenére bizonyára akadnak hibák és hiányosságok. Minden észrevételt (legyen az akár a legapróbb sajtóhiba, akár a könyv egészére vonatkozó alapvető koncepcionális megjegyzés) bárkitől köszönettel fogadok.

Köszönetnyilvánítás

Több érdekes feladatot és sok értékes megjegyzést kaptam kollégáimtól, az ELTE Matematikai Intézet (belső és külső) munkatársaitól. Köszönettel tartozom hallgatóimnak is, részben azért, mert tőlük is számos visszajelzés érkezett, részben pedig azért, mert sok évtizedes oktatói pályafutásom során elsősorban a nekik tartott előadások és gyakorlatok során szereztem meg azokat a tapasztalatokat, amelyekre a könyv írásakor támaszkodni tudtam.

Név szerint szeretnék köszönetet mondani Babai Lászlónak, akitől nagyon sokat tanultam, és mindezt a könyvben is jelentősen hasznosítottam.

Külön köszönetet mondok néhai feleségemnek, Gyarmati Editnek, hiszen a könyv felépítése, szemléletmódja és stílusa egyaránt magán viseli az ő sok évtizedes oktatói munkájának, kísérletező kedvének és számos alapvető tartalmi és formai újításának a jegyeit. Emellett „nemhivatalos lektorként" messze a legszigorúbb kritikusomnak bizonyult, és rengeteg szakmai, didaktikai és stiláris javaslattal segítette a könyv megszületését.

Végül, szeretném megköszönni azt a nehéz és áldozatos munkát, amelyet az első kiadás két lektora, Hermann Péter és Kiss Emil végzett, akik rendkívüli alapossággal nézték át a kéziratot, aprólékosan ellenőrizték a feladatokat és azok eredményét, illetve megoldását, és a hibák kiszűrésén túl igen sok általános, konkrét és stiláris észrevételt tettek, amelyeket igyekeztem maximálisan figyelembe venni. Kiss Emil emellett igen nagy segítséget nyújtott azoknak a technikai problémáknak a megoldásában is, amelyek a számítógépes „szedési" munkám során merültek fel.

Budapest, 2024. augusztus 17.

Freud Róbert, freudro8@gmail.com
ELTE TTK Matematikai Intézet

1. DETERMINÁNSOK

A determinánsfogalom kialakulása történetileg a lineáris egyenletrendszerek megoldásához kapcsolódik, de a determinánsok azóta a matematika szinte minden területén alapvető fontosságúvá váltak. Ez a bonyolultnak és mesterkéltnek látszó fogalom (amely tulajdonképpen csak egy célszerű jelölésrendszer) nagyon szerencsésnek bizonyult a legkülönbözőbb problémák kényelmes, elegáns és természetes kezeléséhez. Erre számos példát tartalmaznak majd a későbbi fejezetek is.

1.1. Permutációk inverziószáma

A permutációk inverziószámára csak a determináns definíciójához és ennek kapcsán néhány tulajdonságának a bizonyításához lesz szükségünk. Emiatt megelégszünk a permutáció legegyszerűbb, „hétköznapi" definíciójával: n különböző elemnek valamilyen sorrendje. Jól ismert, hogy adott n elem esetén $n! = n \cdot (n-1) \cdot \ldots \cdot 2 \cdot 1$ ilyen sorrend lehetséges.

A továbbiakban feltesszük, hogy a kérdéses elemek számok, és ezen belül is általában az $1, 2, \ldots, n$ számok permutációiról lesz szó. Megállapításaink ugyanúgy érvényben maradnak, ha az elemek között egy „természetes sorrendet" rögzítünk, és a permutációknak az „ehhez a természetes sorrendhez viszonyított eltéréseit" vizsgáljuk.

Tekintsük tehát az $1, 2, \ldots, n$ számoknak egy sorrendjét. Az első helyen álló számot jelöljük $\sigma(1)$-gyel, a második helyen állót $\sigma(2)$-vel stb. Ha pl. $n = 5$, akkor a 31452 permutáció esetén $\sigma(1) = 3, \sigma(2) = 1, \sigma(3) = 4, \sigma(4) = 5$ és $\sigma(5) = 2$. Ez tulajdonképpen azt is jelenti, hogy a permutációt felfoghatjuk mint egy *függvény*t: ez a σ függvény az $\{1, 2, \ldots, n\}$ halmaznak önmagára történő kölcsönösen egyértelmű (bijektív) leképezése (az i-edik helyhez az ott álló $\sigma(i)$ számot rendeljük).

Megjegyezzük, hogy a permutációt legtöbbször ilyen bijekcióként célszerű tekinteni. A mi szempontjainknak azonban tökéletesen megfelel, ha a permutációra, mint az $1, 2, \ldots, n$ számok egy sorrendjére gondolunk.

Most rátérünk az inverzió definíciójára. Az inverzió(=„fordítottság") azt jelenti, hogy egy permutációban két elem egymáshoz képest a természetestől eltérő, „fordított módon" helyezkedik el:

1.1.1 Definíció

Az $1, 2, \ldots, n$ elemek egy permutációjában két elem *inverzió*ban áll, ha közülük a nagyobbik megelőzi a kisebbiket. Egy permutáció *inverziószám*án az inverzióban álló elempárok számát értjük. ♣

A σ permutáció inverziószámát $I(\sigma)$-val jelöljük. A fenti 31452 példában a 3 és az 1, a 3 és a 2, a 4 és a 2, valamint az 5 és a 2 állnak inverzióban, az inverziószám tehát 4.

A σ jelöléssel az inverzió úgy fogalmazható meg, hogy valamely $i < j$-re $\sigma(i) > \sigma(j)$ (azaz az előrébb, az i-edik helyen álló $\sigma(i)$ elem nagyobb a hátrébb, a j-edik helyen következő $\sigma(j)$ elemnél).

A továbbiakban csak az játszik majd szerepet, hogy egy adott permutációban az inverziószám páros-e vagy páratlan:

1.1.2 Definíció

Egy permutáció aszerint *páros*, illetve *páratlan*, hogy az inverziószáma páros, illetve páratlan. ♣

A fenti 31452 permutáció tehát páros. A legegyszerűbb páros permutáció az $12 \ldots n$ természetes sorrend, amely a $\sigma(x) = x$ identikus függvénynek felel meg; ennek 0 az inverziószáma.

1.1.3 Tétel

I. Ha egy permutációban két szomszédos elemet felcserélünk, akkor az inverziószám 1-gyel változik (nő vagy csökken).

II. Ha egy permutációban két tetszőleges elemet felcserélünk, akkor az inverziószám páratlannal változik. ♣

Bizonyítás: I. A két felcserélt elem viszonya megváltozott, azaz ha eredetileg inverzióban álltak, akkor a csere után már nem állnak inverzióban, és fordítva. Mivel szomszédosak voltak, ezért a többi elemhez képest az elhelyezkedésük nem változott, és természetesen a többi elem egymáshoz viszonyított helyzete sem módosult.

II. Ha a két elem, b és c között k darab másik áll, akkor először a hátrébb álló c-t sorra megcseréljük a mindig éppen előtte állóval, amíg közvetlenül b mögé nem kerül, ez szomszédos elemek közötti k cserét jelent. Ezután megcseréljük (a most egymás mellett levő) b-t és c-t. Végül újabb k cserével b-t rendre megcseréljük a mögötte álló elemekkel, amíg végül a b elem a c eredeti helyére nem kerül. Ez összesen $2k + 1$, szomszédos elemek közötti csere volt, amelyek mindegyikénél 1-gyel változott (nőtt vagy csökkent) az inverziószám.

Összességében az inverziószám tehát (egy $2k+1$-nél nem nagyobb) páratlan számmal változott. ■

Az előző tétel segítségével könnyen nyerhetünk információt a páros, illetve páratlan permutációk számára:

1.1.4 Tétel
Ha $n > 1$, akkor n elemnek ugyanannyi páros és páratlan permutációja van. ♣

Bizonyítás: Tekintsük az $1, 2, \ldots, n$ számok összes páratlan permutációját, és mindegyikben cseréljük fel az első és a második helyen álló elemet. Ekkor csupa páros permutációhoz jutunk, amelyek mind különbözők. Ebből azt kaptuk, hogy legalább annyi páros permutáció van, mint páratlan. Ha ugyanezt az eljárást a páros permutációkból kiindulva hajtjuk végre, akkor az adódik, hogy legalább annyi páratlan permutáció van, mint páros. Így a páros és páratlan permutációk száma valóban megegyezik ($= n!/2$). ■

Feladatok

Valamennyi feladatban az $1, 2, \ldots, n$ számok σ permutációiról lesz szó.

1.1.1
(a) Bizonyítsuk be, hogy $0 \leq I(\sigma) \leq \binom{n}{2}$.
(b) Legyen $0 \leq k \leq \binom{n}{2}$ tetszőleges egész. Bizonyítsuk be, hogy van olyan σ, amelyre $I(\sigma) = k$.

1.1.2 Mennyi az alábbi permutációk inverziószáma ($n = 101$)?
(a) $1, 3, 5, \ldots, 99, 101, 100, 98, \ldots, 4, 2$;
(b) $51, 52, 50, 53, 49, \ldots, 101, 1$;
(c) $62, 63, 64, \ldots, 101, 61, 60, 59, \ldots, 1$;
(d) $100, 101, 98, 99, 96, 97, \ldots, 2, 3, 1$.

1.1.3 Vegyünk egy tetszőleges permutációt, majd írjuk fel az elemeit pontosan fordított sorrendben, ezzel egy másik permutációt kaptunk. (Pl. a 25413-ból kiindulva a 31452 permutációt nyerjük.) Mi a szükséges és elégséges feltétele annak, hogy a két permutáció azonos paritású (azaz vagy mindkettő páros, vagy mindkettő páratlan) legyen?

1.1.4 Egy permutációban az első helyen álló elemet az utolsó, n-edik helyre visszük (a többi elem pedig egy hellyel előbbre csúszik). Mi volt az elmozgatott elem, ha az új permutációban ugyanannyi inverzió van, mint az eredetiben?

1.1.5

(a) Mi a lehető legnagyobb inverziószám-változás, amelyet két elem cseréjével megvalósíthatunk? Milyen esetben lép ez fel?

M*(b) P és C az alábbi játékot játsszák. P választ egy tetszőleges permutációt. Ezután C ebben a permutációban felcserél két tetszőleges elemet, majd megnézik, hogy a cserénél mennyit változott az inverziószám. P-nek az a célja, hogy a lehető legkisebb inverziószám-változás következzen be, C-nek pedig az, hogy a lehető legnagyobb. Mekkora lesz az inverziószám-változás, ha mindketten optimálisan játszanak?

1.1.6 P és C játékszenvedélyüket újabb játék(ok)ban élik ki. P választ egy tetszőleges permutációt. C feladata ezután a természetes sorrend visszaállítása bizonyos megengedett lépések egymás utáni alkalmazásával. P-nek az a célja, hogy C a természetes sorrendet a lehető legtöbb lépésben érje el, C-nek pedig az, hogy a lehető legkevesebben. Mekkora lesz a lépésszám, ha mindketten optimálisan játszanak és egy lépés

(a) két szomszédos nagyságú elem cseréjét jelenti (pl. a 6-ét és a 7-ét, akárhol is állnak);

*(b) két tetszőleges elem cseréjét jelenti;

*(c) az 1-esnek valamelyik másik elemmel történő cseréjét jelenti?

1.1.7 Mely n-ekre létezik az $1, 2, \ldots, n$ számoknak olyan permutációja, amelyben minden elem pontosan (a) 1; (b) 2; **M****(c) k másik elemmel áll inverzióban?

*1.1.8 Jelöljük $f(n, k)$-val az $1, 2, \ldots, n$ elemek azon permutációinak a számát, amelyekben pontosan k inverzió van.

(a) Bizonyítsuk be, hogy $f(n,k) = \sum_{i=k-n+1}^{k} f(n-1,i)$.

(b) Bizonyítsuk be, hogy $f(n,k) = f(n-1,k)+f(n,k-1)-f(n-1,k-n)$.

(c) Adjuk meg egyszerűbb alakban a $\sum_k f(n,k)$ összeget.

(d) Adjuk meg egyszerűbb alakban a $\sum_k k \cdot f(n,k)$ összeget.

(e) Bizonyítsuk be, hogy $n > 2$-re $\max_k f(n,k) \geq 2(n-2)!$

(f) Mely k-ra lesz $f(n,k)$ maximális (rögzített n mellett)?

1.2. A determináns definíciója

Legyen n rögzített pozitív egész. A determinánst első közelítésben úgy tekinthetjük, mint egy számot, amelyet n^2 darab számból bizonyos bonyolult szabályok szerint számítunk ki.

A determináns definícióját számok helyett általánosabban egy tetszőleges T kommutatív *test* elemeire fogjuk kimondani. A kommutatív test pontos definíciója megtalálható az A.5 pontban, röviden összefoglalva ez azt jelenti, hogy a „négy alapművelet" (a nullával való osztás kivételével) elvégezhető, és a szokásos műveleti azonosságok érvényesek. Legfontosabb példák: $\mathbf{R}$, $\mathbf{C}$, illetve $\mathbf{Q}$, a valós, a komplex, illetve a racionális számok teste, valamint F_p, a modulo p maradékosztályok teste, ahol p prímszám. Azt is megjegyezzük, hogy a determináns definíciójához és az ebben a fejezetben tárgyalt tulajdonságaihoz osztásra nincs is szükség, és így pl. egész számokból vagy polinomokból képezett determinánsról is beszélhetünk.

Nem befolyásolja a továbbiak megértését és az Olvasó helyes képet fog kapni a megfelelő fogalmakról akkor is, ha a továbbiakban a „T kommutatív test elemei" helyett egész egyszerűen (pl. valós vagy komplex) számokra gondol.

A determináns definíciójához lényeges lesz, hogy n^2 darab T-beli elemet egy $n \times n$-es *négyzet* alakú táblázatba rendezzünk. Az ilyen és az ennél általánosabb, *téglalap* alakú táblázatokat mátrixoknak nevezzük:

1.2.1 Definíció

Legyen T egy kommutatív test és k, n adott pozitív egészek. Ekkor a T test feletti $k \times n$-es *mátrix*on egy olyan téglalap alakú táblázatot értünk, amelynek k sora és n oszlopa van, és amelynek elemei T-ből valók. ♣

Jelölések: Magát a mátrixot úgy jelöljük, hogy a táblázatot zárójelek közé foglaljuk. A továbbiakban sima gömbölyű ( ) zárójelet fogunk használni, de szokásos a szögletes [ ] zárójel használata is.

Példa: $\begin{pmatrix} 0 & 7 & 5 \\ 1 & 8 & 4 \end{pmatrix}$ egy 2×3-as (valós elemű) mátrix.

Egy általános A mátrix i-edik sorának j-edik elemét α_{ij}-vel fogjuk jelölni. Az első index tehát azt jelzi, hogy a szóban forgó elem a táblázat hányadik sorában áll, a második index pedig azt, hogy hányadik oszlopban. Az előző

példában $\alpha_{23} = 4$. Ennek megfelelően egy $k \times n$-es mátrix általános alakja

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix}.$$

A mátrixok részletes tárgyalása a következő fejezetben kezdődik.

Ennek a fejezetnek a további részében csak $n \times n$-es *négyzetes* mátrixokról lesz szó. Ezek általános alakja

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}.$$

Most rátérünk a determináns definíciójára. Az A mátrix determinánsán (ezt $\det A$-val jelöljük majd) egy olyan T-beli elemet értünk, amelyet a következőképpen határozunk meg. Először is n-tényezős szorzatokat képezünk minden lehetséges módon úgy, hogy a mátrix minden sorából és minden oszlopából pontosan egy tényezőt veszünk (összesen $n!$ ilyen szorzat képezhető). A következő lépésben minden egyes szorzatot „$+$” vagy „$-$” előjellel látunk el: ez azt jelenti, hogy vagy magát a szorzatot tekintjük, vagy pedig a negatívját (ellentettjét). Az előjelezési szabályt a következő bekezdésben részletezzük. Végül ezeket az előjeles szorzatokat összeadjuk (azaz az összeg minden tagja vagy egy ilyen szorzat, vagy pedig a szorzat negatívja). Az így kapott ($n!$-tagú) összeget (amely tehát egy T-beli elem) nevezzük az A mátrix determinánsának vagy más szóval az α_{ij} elemekből képezett (n-edrendű vagy $n \times n$-es vagy n méretű) determinánsnak.

Egy szorzat „előjelezése” a következőképpen történik. A szorzat tényezőit írjuk fel olyan sorrendben, hogy az első helyen az 1. sorból vett elem álljon, a második helyen a 2. sorból vett elem stb. Ha itt rendre megnézzük, hogy a szorzat tényezői hányadik oszlopból valók, akkor ezek az oszlopindexek is valamilyen sorrendben az $1, 2, \dots, n$ számokat futják be (hiszen minden oszlopból pontosan egy elem szerepel), tehát ezek az oszlopindexek az $1, 2, \dots, n$ számok egy permutációját adják. A szorzatot aszerint látjuk el pozitív, illetve negatív előjellel (tehát aszerint szerepel maga a szorzat, illetve az ellentettje majd az összegben), hogy ez a permutáció páros, illetve páratlan.

Példa: $A = \begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{pmatrix}$ esetén az egyik szorzat a $2 \cdot 6 \cdot 7$. Itt a tényezők már sorok szerint vannak rendezve, és ezeket a tényezőket rendre a 2., a 3., majd az

1. oszlopból vettük. Az oszlopindexek permutációja tehát 231, amelyben két inverzió van. Így ez páros permutáció, a szorzat előjele tehát pozitív (vagyis maga ez a szorzat, nem pedig az ellentettje fog szerepelni a determinánst megadó összegben).

FIGYELEM! A szorzat előjelezésének semmi köze sincs maguknak a szorzótényezőknek az értékéhez, ez kizárólag az n tényezőnek a mátrixon belüli elhelyezkedésétől függ. Az előjel meghatározásánál csakis az oszlopindexek imént említett permutációjának paritása számít, ez a permutáció pedig mindig az $1, 2, \ldots, n$ természetes számokra vonatkozik, függetlenül attól, hogy a mátrix elemei (valós, komplex stb.) számok vagy sem (pl. maradékosztályok).

A determinánst úgy jelöljük, hogy a táblázatot (a zárójelek nélkül) két függőleges vonal közé tesszük.

A fentieket az alábbi definícióban foglaljuk össze:

1.2.2 Definíció

Az $A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix}$ mátrix *determinánsa* (vagy más szóval az α_{ij}, $i, j = 1, 2, \ldots, n$ elemekből képezett determináns)

$$\det A = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{vmatrix} = \sum_{\sigma} (-1)^{I(\sigma)} \alpha_{1\sigma(1)} \alpha_{2\sigma(2)} \ldots \alpha_{n\sigma(n)} \,. \quad \clubsuit$$

A jobb oldalon álló $\sum$ összegzést az $1, 2, \ldots, n$ számok minden lehetséges σ permutációjára kell elvégezni. Az összegben az $n!$ tagnak pontosan a felét láttuk el negatív előjelezéssel (azaz ennyiszer szerepel a szorzat helyett az ellentettje), hiszen ugyanannyi páratlan és páros permutáció van (az $n = 1$ triviális esettől eltekintve).

Példa:

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{cases} (-1)^0\, 1 \cdot 5 \cdot 9 + (-1)^1\, 1 \cdot 6 \cdot 8 + (-1)^1\, 2 \cdot 4 \cdot 9 + (-1)^2\, 2 \cdot 6 \cdot 7 \\ +(-1)^2\, 3 \cdot 4 \cdot 8 + (-1)^3\, 3 \cdot 5 \cdot 7 = 0 \,. \end{cases}$$

A definíció alapján meglehetősen nehézkes egy determináns kiszámítása. Később látni fogjuk, hogy egy determinánst szinte sohasem a definíció alapján

számítunk ki, hanem azoknak a módszereknek a segítségével, amelyeket majd a következő pontokban tárgyalunk.

Néhány további megjegyzés a determináns definíciójával kapcsolatban. Ha jobban belegondolunk, akkor a(z n-edrendű) determináns tulajdonképpen egy függvény, amely az $n \times n$-es mátrixokhoz rendel T-beli elemeket. Egy adott mátrix determinánsa ekkor egy konkrét függvényérték. A „determináns" szót mindkét értelemben fogjuk használni (tehát mind a függvényt, mind pedig annak egy értékét így nevezzük), de ez (reméljük) nem okoz félreértést.

Ha ki akarjuk hangsúlyozni, hogy egy adott A mátrix determinánsáról van szó, akkor erre a $\det A$ jelölést használjuk. Ha egy determináns valamelyik soráról, oszlopáról vagy eleméről beszélünk, ezen a megfelelő mátrix adott sorát, oszlopát, illetve elemét értjük. Például egy olyan kijelentés, hogy „a determinánsban két sort felcserélünk", annak a rövidített megfogalmazása, hogy a mátrixban felcserélünk két sort és az így keletkező mátrix determinánsát vizsgáljuk.

Még egyszer hangsúlyozzuk azonban, hogy a mátrix és a determináns alapvetően különböző matematikai fogalmak. A mátrix egy táblázat, tehát T-beli elemek bizonyos rendszere, míg a determináns egyetlen T-beli elemet jelent. Ezért nagyon ügyeljünk a határolójelek helyes használatára; mátrixnál ez gömbölyű (vagy szögletes) zárójel, determinánsnál pedig két függőleges egyenes vonal.

A determináns fenti definíciójában lényeges volt, hogy egy n-tényezős szorzatot először a sorindexek szerint rendezzünk, és csak utána nézzük az oszlopindexek permutációjának paritását (páros vagy páratlan voltát). Ha más sorrendben írjuk fel a tényezőket, akkor az oszlopindexek permutációja is más lesz, és a paritás is megváltozhat, ily módon nem nyerünk információt az előjelezéssel kapcsolatban. Az alábbi tétel akkor is lehetővé teszi az előjel meghatározását, ha a tényezőket tetszőleges sorrendben írtuk fel. Ez a kiszámítási mód egyben megszünteti a sorok és oszlopok szerepének eddigi aszimmetriáját.

1.2.3 Tétel

Tekintsünk egy, a determináns definíciójában szereplő n-tényezős szorzatot, ahol tehát minden sorból és minden oszlopból egy elem szerepel. Ez a szorzat (a tényezőket tetszőleges sorrendben felírva) $\alpha_{\rho(1)\pi(1)} \dots \alpha_{\rho(n)\pi(n)}$ alakú, ahol ρ a sorindexeknek, π az oszlopindexeknek megfelelő permutáció. Ekkor az előjelet $(-1)^{I(\rho)+I(\pi)}$ határozza meg. ♣

Bizonyítás: Ha ρ a természetes sorrendnek megfelelő permutáció, akkor ez éppen a determináns definíciójában szereplő előjelezés, hiszen $I(\rho) = 0$. Könnyen

látható, hogy a tényezőknek ebből a sorrendjéből kiindulva cserék egymásutánjával bármelyik másik sorrendhez eljuthatunk. Így elég azt megmutatnunk, hogy ha a szorzatban két tényezőt felcserélünk, akkor az $I(\rho) + I(\pi)$ összeg paritása nem változik. Ez valóban igaz: egy ilyen csere ugyanis mind a ρ, mind a π permutációban két elem cseréjét jelenti, ezért mindkét permutációban az inverziószám páratlannal változik, tehát az inverziószámok összegének paritása változatlan marad. ■

Az 1.2.3 Tétel egyik következménye, hogy a determináns definíciójában a sorok és oszlopok szerepe felcserélhető; az előjelezést úgy is végezhetjük, hogy a szorzatok tényezőit az oszlopok sorrendjében írjuk fel, és az ekkor kialakuló sorindexek permutációjának a paritását nézzük. Ez az 1.2.3 Tétel jelölései szerint annak az esetnek felel meg, amikor π éppen a természetes sorrend.

Feladatok

1.2.1 Mi az alábbi polinomokban x^3 együtthatója?

(a) $\begin{vmatrix} 3x & 5 & 7 & 1 \\ 2x^2 & 5x & 6 & 2 \\ 1 & x & 0 & 3 \\ 2 & 1 & 4 & 7 \end{vmatrix}$ (b) $\begin{vmatrix} 3x^2 & 5 & 7 & 1 \\ 2x^2 & 5x & 6 & 2 \\ 1 & x & 0 & 3 \\ 2 & 1 & 4 & 7 \end{vmatrix}$

1.2.2 Melyek igazak az alábbi állítások közül?

(a) Ha egy mátrix minden eleme racionális szám, akkor a mátrix determinánsa is racionális szám.

(b) Ha egy mátrix minden eleme irracionális szám, akkor a mátrix determinánsa is irracionális szám.

(c) Ha egy mátrixnak pontosan egy eleme irracionális szám, a többi pedig racionális, akkor a mátrix determinánsa irracionális szám.

(d) Ha egy $n \times n$-es mátrixnak legalább $n^2 - n + 1$ eleme 0, akkor a mátrix determinánsa 0.

(e) Ha egy mátrix determinánsa 0, akkor a mátrixban előfordul 0 elem.

(f) Ha egy mátrix elemei racionális számok és a determinánsa $1/27$, akkor a mátrixban van olyan elem, amelynek a nevezője 3-hatvány.

(g) Ha egy mátrix elemei racionális számok és a determinánsa $1/27$, akkor a mátrixban van olyan elem, amelynek a nevezője 3-mal osztható.

1.2.3 Számítsuk ki az n-edrendű determinánst, ha tudjuk, hogy

(a) $\alpha_{1j} = 0$ minden j-re (azaz az első sor minden eleme 0);

(b) $\alpha_{ij} = 0$ minden $i < j$-re (azaz a főátló felett minden elem 0);

(c) $\alpha_{ij} = 0$, ha $i + j > n + 1$ (azaz a mátrix bal alsó és jobb felső sarkát összekötő átló alatt minden elem 0).

1.2.4 Számítsuk ki az alábbi n-edrendű determinánsokat ($n > 1$).

(a) $\alpha_{ij} = \begin{cases} 1, & \text{ha } j \equiv i + 1 \pmod{n}; \\ 0, & \text{egyébként} \end{cases}$
(azaz közvetlenül a főátló felett, valamint a bal alsó sarokban 1-ek állnak, minden más elem 0).

(b) $\alpha_{ij} = 1$ (azaz minden elem 1).

(c) $\alpha_{ij} = \begin{cases} 1, & \text{ha } |j - i| = 1; \\ 0, & \text{egyébként} \end{cases}$
(azaz közvetlenül a főátló felett és alatt 1-ek állnak, a többi elem 0).

1.2.5 Egy $n \times n$-es mátrixban van egy k sorból és m oszlopból álló téglalap alakú rész, amelyben minden elem 0. Bizonyítsuk be, hogy ha $k + m > n$, akkor a mátrix determinánsa 0.

1.2.6 Egy $n \times n$-es mátrixban két elemet felcserélünk, a többin nem változtatunk. Tekintsük az eredeti és az új mátrix determinánsának a definíció szerinti felírását. Hány azonos szorzat szerepel a tagok között, ha a szorzatok előjelezését nem vesszük figyelembe? Változike a helyzet, ha a szorzatok előjelezését is figyelembe vesszük?

1.2.7 Egy 1000×1000-es valós elemű mátrixban tetszőleges számú elem helyére általunk választott elemeket írhatunk. Legkevesebb hány elem módosításával tudjuk elérni, hogy a keletkező determináns 0 legyen?

1.2.8 Tekintsük az $\alpha_{11}x_1 + \alpha_{12}x_2 = \beta_1$, $\alpha_{21}x_1 + \alpha_{22}x_2 = \beta_2$ lineáris egyenletrendszert, és tegyük fel, hogy $\begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix} \neq 0$. Bizonyítsuk be, hogy az egyenletrendszer egyetlen megoldása

$$x_1 = \frac{\begin{vmatrix} \beta_1 & \alpha_{12} \\ \beta_2 & \alpha_{22} \end{vmatrix}}{\begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix}}, \qquad x_2 = \frac{\begin{vmatrix} \alpha_{11} & \beta_1 \\ \alpha_{21} & \beta_2 \end{vmatrix}}{\begin{vmatrix} \alpha_{11} & \alpha_{12} \\ \alpha_{21} & \alpha_{22} \end{vmatrix}}.$$

1.2.9 Tekintsük azt a paralelogrammát, amelynek egyik csúcspontja az origó, két másik csúcspontja pedig (β_1, β_2), illetve (δ_1, δ_2). Bizonyítsuk be, hogy a paralelogramma területe $\begin{vmatrix} \beta_1 & \beta_2 \\ \delta_1 & \delta_2 \end{vmatrix}$ abszolút értéke.

*1.2.10 Tekintsük az összes olyan $n \times n$-es A mátrixot, amelyek minden sorában legfeljebb két darab nem nulla elem áll. Jelöljük $k(A)$-val, hány nem nulla tag lép fel abban az (előjeles n-tényezős szorzatokból képezett) összegben, amely $\det A$ definíció szerinti felírását adja. Mi $k(A)$ lehető legnagyobb értéke?

1.2.11 Bizonyítsuk be, hogy

$$\begin{vmatrix} 1849 & 1444 & 1896 & 1222 \\ 1490 & 1703 & 1790 & 1526 \\ 1342 & 1566 & 1541 & 1514 \\ 1242 & 1552 & 1382 & 1825 \end{vmatrix} \neq 0\,.$$

1.3. Elemi tulajdonságok

A determináns definíciójából azonnal adódnak az alábbi egyszerű állítások:

1.3.1 Tétel

I. Ha a főátló (azaz a bal felső sarkot a jobb alsó sarokkal összekötő „ÉNy-DK" irányú egyenes) alatt vagy fölött minden elem 0, akkor a determináns a főátlóbeli elemek szorzata.

II. Ha valamelyik sor vagy oszlop minden eleme 0, akkor a determináns is 0.

III. Ha valamelyik sor vagy oszlop minden elemét λ-val megszorozzuk, akkor a determináns is λ-val szorzódik. ♣

Bizonyítás: I. és II. lényegében szerepelt az 1.2.3 feladatban. III. esetében a determináns definíció szerinti felírásában minden szorzat λ-val szorzódik, hiszen minden szorzatban pontosan egy tényező van az adott sorból, illetve oszlopból. Mivel az előjelezés nem módosult, így a λ-t minden tagból kiemelve kapjuk, hogy a determinánst adó előjeles összeg is λ-szorosára változott. ■

Megjegyezzük, hogy a II. állítás a III-nak a $\lambda = 0$ speciális esete.

A következő tulajdonság hasonlóan igazolható (a bizonyítást az 1.3.4 feladatban tűztük ki):

1.3.2 Tétel

Ha valamelyik sor vagy oszlop minden eleme egy kéttagú összeg, akkor a determináns két determináns összegére bomlik, ahol az egyikben az adott sorban, illetve oszlopban rendre az összegek egyik tagja szerepel, a másikban pedig a másik tag, a többi elem pedig mind a két determinánsban ugyanaz, mint az eredetiben volt. Azaz (pl. az első sor elemeire nézve)

$$\begin{vmatrix} \alpha'_{11}+\alpha''_{11} & \alpha'_{12}+\alpha''_{12} & \dots & \alpha'_{1n}+\alpha''_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} \alpha'_{11} & \alpha'_{12} & \dots & \alpha'_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix} + \begin{vmatrix} \alpha''_{11} & \alpha''_{12} & \dots & \alpha''_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix} . \quad \clubsuit$$

Mielőtt továbbmennénk, egy általános észrevételt teszünk. Az eddigiekben úgy tapasztaltuk, hogy ha egy tulajdonság sorokra érvényes volt, akkor ugyanúgy fennállt oszlopokra is (és viszont). Megmutatjuk, hogy ez mindig szükségképpen így van. Az 1.2.3 Tétel alapján ugyanis a determinánsban a sorok és az oszlopok szerepe teljesen szimmetrikus, vagyis ha a determináns definíciójában a „sor" és „oszlop" szavakat következetesen kicseréljük, akkor ugyanahhoz a fogalomhoz jutunk. (Vigyázat, magából az 1.2.2 Definícióból ez nem látszott, viszont az 1.2.3 Tételből már következett.) Tegyük fel most, hogy a sorokkal kapcsolatban igazoltunk valamilyen általános tulajdonságot. Ha itt a bizonyításban következetesen a „sor" szó helyett az „oszlop" szót írjuk és viszont, akkor ugyanennek a tulajdonságnak az oszlopokra vonatkozó változatára kellett hogy nyerjünk egy kifogástalan levezetést.

Ennek alapján bármely, a sorokra fennálló tulajdonság oszlopokra is igaz. Megjegyezzük, hogy mindez majd az 1.3.6 Tételből is közvetlenül adódik. A további tulajdonságokat ezért csak sorokra fogjuk kimondani (de természetesen oszlopokra ugyanúgy érvényesek).

1.3.3 Tétel

Ha két sor egyenlő (azaz a megfelelő elemek megegyeznek), akkor a determináns 0. $\clubsuit$

Bizonyítás: Megmutatjuk, hogy a determináns definíció szerinti felírásában a szorzatok párba állíthatók úgy, hogy bármely két összetartozó szorzat ugyanaz,

azonban az előjelezésük ellentétes. Mivel minden pár összege 0, ezért a determináns is 0.

A bizonyítást az egyszerűség kedvéért arra az esetre mondjuk el, amikor az első két sor egyenlő: $\alpha_{1j} = \alpha_{2j}$ minden j-re.

A bizonyítás gondolatát először egy konkrét példán illusztráljuk. Legyen $n = 5$, és tekintsük a determináns definíciójában az

$$S = \alpha_{13}\alpha_{25}\alpha_{34}\alpha_{41}\alpha_{52}$$

szorzatot. Mivel a feltétel szerint $\alpha_{13} = \alpha_{23}$ és $\alpha_{25} = \alpha_{15}$, ezért a determinánsban szintén szereplő

$$S' = \alpha_{15}\alpha_{23}\alpha_{34}\alpha_{41}\alpha_{52}$$

szorzat egyenlő S-sel.

Vizsgáljuk most meg az S, illetve S' szorzatok előjelezését. Ehhez az oszlopindexekből képezett 35412, illetve 53412 permutáció inverziószámát kell tekintenünk. Az utóbbi permutációt az előzőből úgy nyertük, hogy az első két elemet felcseréltük. Ennek alapján az inverziószám páratlannal változott (jelen esetben 1-gyel, mert a felcserélt elemek szomszédosak voltak). Ez azt jelenti, hogy a két permutáció ellentétes paritású, és így az S és S' szorzatok előjelezése is ellentétes (jelen esetben a determinánst adó összegben $-S$ és $+S'$ fog szerepelni).

Pontosan ugyanígy kell végiggondolni az általános esetet is. A determináns definíciójában szereplő szorzatok általános alakja

$$S = \alpha_{1\sigma(1)}\alpha_{2\sigma(2)}\alpha_{3\sigma(3)}\dots\alpha_{n\sigma(n)}.$$

Ugyanez a szorzat még egyszer előfordul mint

$$S' = \alpha_{1\sigma(2)}\alpha_{2\sigma(1)}\alpha_{3\sigma(3)}\dots\alpha_{n\sigma(n)},$$

hiszen $\alpha_{1\sigma(1)} = \alpha_{2\sigma(1)}$ és $\alpha_{2\sigma(2)} = \alpha_{1\sigma(2)}$. Könnyen látható, hogy ezzel a szorzatokat valóban párba állítottuk.

Végül igazoljuk, hogy S és S' ellentétes előjelű lesz. S előjelét a $\sigma(1)\sigma(2)\sigma(3)\dots\sigma(n)$ permutáció paritása, S'-ét pedig a $\sigma(2)\sigma(1)\sigma(3)\dots\sigma(n)$ permutáció paritása adja. Mivel az utóbbi permutáció az előbbiből (az első) két elem cseréjével keletkezett, így a paritás valóban az ellenkezőjére változott. ∎

Az 1.3.3 Tételt az 1.3.1 Tétel III. részével kombinálva azonnal adódik az alábbi következmény:

1.3.3A Tétel
Ha valamelyik sor egy másik sor λ-szorosa, akkor a determináns 0. ♣

Az alábbi tulajdonság lesz az, amelyet a determinánsok számolásánál talán a legtöbbször fogunk alkalmazni.

1.3.4 Tétel
Ha egy sorhoz hozzáadjuk egy másik sor λ-szorosát, akkor a determináns nem változik. ♣

Bizonyítás: Az egyszerűbb leírás kedvéért tekintsük azt az esetet, amikor az első sorhoz adjuk hozzá a második sor λ-szorosát. Ekkor az 1.3.2 Tétel alapján

$$\begin{vmatrix} \alpha_{11}+\lambda\alpha_{21} & \alpha_{12}+\lambda\alpha_{22} & \dots & \alpha_{1n}+\lambda\alpha_{2n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix} =$$

$$= \begin{vmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix} + \begin{vmatrix} \lambda\alpha_{21} & \lambda\alpha_{22} & \dots & \lambda\alpha_{2n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix},$$

és a jobb oldalon álló második determináns az 1.3.3A Tétel szerint 0. ■

1.3.5 Tétel
Ha két sort felcserélünk, akkor a determináns a negatívjára változik. ♣

Bizonyítás: A bizonyítást most is az első két sor esetére végezzük. Az 1.3.4 Tételt fogjuk többször egymás után alkalmazni. Először a második sort kivonjuk az első sorból, majd az (új) első sort hozzáadjuk a második sorhoz, végül a(z új) második sort kivonjuk az (új) első sorból. Eközben a determináns nem változik, az első két sor j-edik eleme pedig a következőképpen módosul:

$$\begin{pmatrix} \alpha_{1j} \\ \alpha_{2j} \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{1j}-\alpha_{2j} \\ \alpha_{2j} \end{pmatrix} \mapsto \begin{pmatrix} \alpha_{1j}-\alpha_{2j} \\ \alpha_{1j} \end{pmatrix} \mapsto \begin{pmatrix} -\alpha_{2j} \\ \alpha_{1j} \end{pmatrix}.$$

Végül az első sorból (-1)-et kiemelve, a kapott determináns egyrészt az eredeti determináns (-1)-szerese (1.3.1/III Tétel), másrészt ez a determináns az eredetiből éppen az első két sor felcserélésével keletkezett. ■

1.3.6 Tétel

Ha az elemeket a főátlóra tükrözzük, akkor a determináns nem változik.

♣

Bizonyítás: Megmutatjuk, hogy a két determináns definíció szerinti felírásában ugyanazok a szorzatok szerepelnek és az előjelezésük is azonos.

Az eredeti determináns elemeit jelöljük α_{ij}-vel, az újét pedig β_{ij}-vel. A feltétel szerint $\beta_{ij} = \alpha_{ji}$ minden i, j-re.

Az eredeti determinánsban szereplő szorzat általános alakját most az 1.2.3 Tételben szereplő módon, $\alpha_{\rho(1)\pi(1)} \dots \alpha_{\rho(n)\pi(n)}$ formában írjuk fel, ahol ρ a sorindexek, π az oszlopindexek permutációja. Ugyanez a szorzat a főátlóra történő tükrözés után is szerepelni fog, éspedig $\beta_{\pi(1)\rho(1)} \dots \beta_{\pi(n)\rho(n)}$ alakban. A két szorzat előjelezése is megegyezik, hiszen az előjelet az 1.2.3 Tétel szerint az eredeti determinánsban $(-1)^{I(\rho)+I(\pi)}$, a tükrözés utániban pedig $(-1)^{I(\pi)+I(\rho)}$ határozza meg. ■

Megismételjük, hogy az 1.3.6 Tételből (is) következik, hogy bármely, a sorokra érvényes általános determinánstulajdonság szükségképpen igaz az oszlopokra is.

Az 1.3.1–1.3.6 Tételek alapján egy determinánst általában a következő módszerrel tudunk kiszámítani. Arra törekszünk, hogy végül a főátló alatt csupa 0 legyen, ekkor a determináns a főátlóbeli elemek szorzata. Ha az eljárás közben bármikor az adódik, hogy valamelyik sorban vagy oszlopban csupa 0 áll, akkor a determináns 0. Az eljárás során csak olyan lépéseket alkalmazunk, amikor a determináns nem változik, illetve csak előjelet vált (ez utóbbiakat természetesen gondosan nyomon kell követni).

Ha $\alpha_{11} \neq 0$, akkor minden sorból az első sor alkalmas többszörösét levonva, elérhetjük, hogy az első oszlop többi eleme 0 legyen. Ha a bal felső sarokban eredetileg 0 állt, akkor az első sort előbb felcseréljük egy olyan sorral, amelynek első eleme nem volt 0, és ezután végezzük a fenti kivonogatásokat. (Ha nincs ilyen sor, akkor az első oszlop minden eleme 0, tehát a determináns 0.)

Ha az első oszlopban az első elem kivételével már minden elem 0, akkor megtehetjük, hogy az első sor második, ..., n-edik elemét minden gondolkodás nélkül 0-ra változtatjuk. Ez abból következik, hogy ha az első oszlop megfelelő többeseit a többi oszlopból levonjuk, akkor az első sorban ezeknek az elemeknek a helyére 0 kerül, és közben semelyik másik elem sem módosul, valamint a determináns sem változik. Erre a lépésre azonban tulajdonképpen nem lesz szükségünk.

A későbbiekben az első oszlop már mindenképpen változatlan marad.

Most továbblépünk (az új) α_{22}-re. Ha ez nem nulla, akkor a harmadik, ..., n-edik sorból a második sor megfelelő többszörösét levonva, a főátló alatt a második oszlopba is csupa 0 kerül. Ha $\alpha_{22} = 0$, akkor ezen úgy segíthetünk, hogy a második sort valamelyik alkalmas *későbbi* sorral felcseréljük. (Ha a második oszlop minden további eleme is 0, akkor a determináns könnyen láthatóan maga is 0.) Ezt az eljárást folytatva, vagy kiderül, hogy a determináns 0, vagy pedig elérhetjük, hogy a főátló alatt csupa 0 álljon.

Példa: Az előző pontban már szerepelt $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$ determinánst a következőképpen számíthatjuk ki. A második, illetve harmadik sorból levonjuk az első sor 4-, illetve 7-szeresét: $\begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{vmatrix}$. Itt a harmadik sor a második sor kétszerese, tehát a determináns 0. (Ugyanez adódik a fenti eljárásból is: a harmadik sorból a második sor kétszeresét levonva, a harmadik sorba csupa 0 kerül.)

A fenti eljárást, pontosabban annak finomítását fogjuk lineáris egyenletrendszerek megoldásánál is alkalmazni; ezt hívják Gauss-féle kiküszöbölésnek (lásd a 3.1 pontot).

Megjegyezzük, hogy a determináns kiszámításánál a sorok helyett természetesen az oszlopokkal is hasonlóan manipulálhatunk, sőt akár felváltva, hol oszlopokkal, hol pedig sorokkal dolgozhatunk. Számos determináns kiszámításánál nem feltétlenül a fenti általános módszer a célravezető, hanem mindenféle egyedi trükköket lehet (vagy kell) alkalmazni.

Néhány jótanács. Érdemes a determináns elemeiből minél többet részletesen felírni, és ezeknek a változását az egyes lépéseknél gondosan regisztrálni. Gyakran a részletes és pontos felírás már félmegoldás, mert szinte sugallja, hogy a következő lépésben mit érdemes csinálni. Azt is fontos jelezni, hogy mi az a lépés, amit éppen végeztünk, mert különben később (pl. egy esetleges hibakeresésnél) gyakran már magunk sem tudjuk rekonstruálni, hogy mire is gondoltunk akkor.

Nagyon veszélyes, ha több lépést megpróbálunk összevonni. Ha pl. a második sorból kivontuk az első sort, akkor a következő lépésben már egy „másik" determinánst alakítunk tovább, amelynek új a második sora. Ezért legfeljebb olyan típusú összevonásokat szabad csinálni, amikor az egyes lépések nem befolyásolják egymást, pl. az első sort kivonjuk az összes többi sorból.

Pontosan át kell gondolni a „minden sorból kivonjuk a fölötte álló sort" típusú manővereket. Nem mindegy ugyanis, hogy ezt alulról, vagy felülről

kezdjük. Ha felülről kezdjük, akkor a harmadik sorból már egy *módosított* második sort (ti. az eredeti második sornak és az eredeti első sornak a különbségét) kell levonni. Ha alulról haladunk felfelé, akkor mindig az eredeti sorok kerülnek levonásra. Azt se felejtsük el, hogy az első sor mindenképpen változatlan marad.

Feladatok

1.3.1 Mi történik egy determinánssal, ha a függőleges középvonalára tükrözzük?

1.3.2 Hány olyan komplex szám van, amellyel egy $n \times n$-es komplex elemű mátrix minden elemét megszorozva a mátrix determinánsa az ellentettjére változik?

1.3.3 Számítsuk ki az alábbi determinánsokat:

$$\text{(a)} \begin{vmatrix} 123456 & 123426 \\ 123457 & 123427 \end{vmatrix}; \qquad \text{(b)} \begin{vmatrix} 1111 & 111 & 11 \\ 11111 & 1111 & 111 \\ 12345 & 1234 & 123 \end{vmatrix}.$$

1.3.4 Bizonyítsuk be az 1.3.2 Tételt.

1.3.5 Bizonyítsuk be az 1.3.5 Tételt közvetlenül, az 1.3.4 Tétel felhasználása nélkül.

1.3.6 Mutassuk meg, hogy pl. valós számokra az 1.3.5 Tételből azonnal következik az 1.3.3 Tétel. Alkalmazható-e ez a gondolatmenet bármely test esetén?

1.3.7 Legyen $\alpha \neq 0$ rögzített komplex szám. Egy (komplex elemű) $n \times n$-es mátrixban (minden k-ra és j-re) a k-adik sor j-edik elemét a) α^{j-k}-val; b) α^{j+k}-val megszorozzuk. Mi a kapcsolat a régi és az új mátrix determinánsa között?

1.3.8 Számítsuk ki az alábbi $n \times n$-es determinánsokat.

(a) $\alpha_{ij} = \begin{cases} i, & \text{ha } i = j; \\ 1, & \text{ha } i \neq j. \end{cases}$ (b) $\alpha_{ij} = \min(i, j)$.

(c) $\alpha_{ij} = ij$. (d) $\alpha_{ij} = i + j$. (e) $\alpha_{ij} = i^2 + j^2$.

1.3.9 Egy determináns minden sora számtani sorozat. Számítsuk ki a determinánst.

1.3.10 $3\,|\,5301$, $3\,|\,4227$, $3\,|\,8340$, $3\,|\,2346$ és történetesen $3\,|\begin{vmatrix} 5 & 3 & 0 & 1 \\ 4 & 2 & 2 & 7 \\ 8 & 3 & 4 & 0 \\ 2 & 3 & 4 & 6 \end{vmatrix}$. Vajon a véletlen játékával állunk-e szemben? Mi a helyzet 3 helyett 23-mal?

1.3.11 Legyenek $\gamma_1, \ldots, \gamma_n$ és $\delta_1, \ldots, \delta_n$ tetszőleges komplex számok, és tekintsük azt a mátrixot, amelyben az i-edik sor j-edik eleme $1+\gamma_i\delta_j$. Számítsuk ki a mátrix determinánsát.

1.3.12 Egy determináns főátlójának minden eleme γ, a többi helyen pedig δ áll. Számítsuk ki a determinánst.

1.3.13 Egy páratlan rendű négyzetes mátrixban $\alpha_{ij}+\alpha_{ji}=0$ teljesül minden i, j-re (ferdén szimmetrikus vagy antiszimmetrikus mátrix). Mennyi a determinánsa?

1.3.14 Egy komplex elemű D determináns bármely sorához van a determinánsnak (legalább egy és az adott sortól nem feltétlenül különböző) sora, amely ennek a sornak a konjugáltja (azaz a megfelelő elemek egymás konjugáltjai). Bizonyítsuk be, hogy D^2 valós szám.

1.3.15 Számítsuk ki az alábbi determinánst és általánosítsuk a feladatot:

$$\begin{vmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{vmatrix}.$$

1.3.16 Számítsuk ki az alábbi $n \times n$-es determinánsokat; b)-ben $\alpha_{ij} = i$, ha $j \equiv 1 \pmod{i}$, a többi helyen pedig 1 áll.

(a) $\begin{vmatrix} 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 0 & 0 & \ldots & 0 & 1 \\ 0 & 1 & 0 & \ldots & 0 & 1 \\ 0 & 0 & 1 & \ldots & 0 & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & 1 \end{vmatrix}$ (b) $\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & \ldots \\ 2 & 1 & 2 & 1 & 2 & \ldots \\ 3 & 1 & 1 & 3 & 1 & \ldots \\ 4 & 1 & 1 & 1 & 4 & \ldots \\ \vdots & \vdots & \vdots & \vdots & \vdots & \\ n & 1 & 1 & 1 & 1 & \ldots \end{vmatrix}$

1.3.17 Egy $n \times n$-es mátrix főátlójában csupa 1-es áll, közvetlenül a főátló alatt mind az $n-1$ elem -1, közvetlenül a főátló fölött rendre $1^2, 2^2, \ldots, (n-1)^2$ helyezkedik el, a többi elem pedig 0. Számítsuk ki a mátrix determinánsát.

1.3.18 Legyenek $\phi_1, \ldots, \phi_n$ tetszőleges szögek és az $n \times n$-es A mátrix elemei $\alpha_{ij} = \cos(\phi_i + \phi_j)$. Számítsuk ki $\det A$-t.

1.3.19 Egy $n \times n$-es mátrix elemei egész számok, és egyetlen sorban sincs két olyan szám, amely azonos maradékot adna n-nel osztva. Bizonyítsuk be, hogy ha n páratlan szám, akkor a mátrix determinánsa osztható n-nel. Mit állíthatunk páros n esetén?

1.3.20 Egy $\varphi(n) \times \varphi(n)$-es mátrix elemei n-hez relatív prím egész számok, és egyetlen sorban sincs két olyan szám, amely azonos maradékot adna n-nel osztva ($\varphi(n)$ az Euler-féle φ-függvény). Bizonyítsuk be, hogy ha $n > 2$, akkor a mátrix determinánsa osztható n-nel.

*1.3.21 Legyen $n \geq 7$ és tekintsük azt az $n \times n$-es mátrixot, amelyben $\alpha_{ij} = ij$ legkisebb *pozitív* maradéka modulo n (tehát ha ij osztható n-nel, akkor $a_{ij} = n$, nem pedig 0). Bizonyítsuk be, hogy a mátrix determinánsa 0.

1.4. Kifejtés

Ebben a pontban a determináns egy másik, rekurziós típusú kiszámítási módjával ismerkedünk meg, amikor egy n-edrendű determinánst n darab $n-1$-edrendű determinánsra vezetünk vissza. Ez elsősorban elméleti szempontból jelentős, de egyes determinánsok gyakorlati kiszámításánál is jól alkalmazható.

Ehhez először az előjeles aldeterminánsfogalmát definiáljuk. Ebben a pontban végig feltesszük, hogy $n > 1$.

1.4.1 Definíció

Tekintsünk egy n-edrendű determinánst. Hagyjuk el az i-edik sort és a j-edik oszlopot, így egy $(n-1) \times (n-1)$-es determináns keletkezik. Az α_{ij} elemhez tartozó A_{ij} *előjeles aldeterminánsa*on ennek a determinánsnak a $(-1)^{i+j}$-szeresét értjük. ♣

Példa: $\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$ esetén $A_{23} = (-1)^5 \begin{vmatrix} 1 & 2 \\ 7 & 8 \end{vmatrix} = 6.$

FIGYELEM! Az aldeterminánsa előjelezésének semmi köze sincs a determináns definíciójában az egyes szorzatok előjelezéséhez, itt semmiféle permutáció vagy inverziószám nem szerepel. Az aldeterminánsa előjelét kizárólag az határozza meg, hogy melyik sort és oszlopot hagytuk el: ha ezek indexe („sorszáma”)

azonos paritású (tehát ha páratlanadik sort és oszlopot vagy párosadik sort és oszlopot hagytunk el), akkor az előjel „+”, ellentétes paritás esetén pedig „−”. Az előjelezést így az ún. „sakktáblaszabály” adja:

$$\begin{array}{cccc} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & - & \dots \\ - & + & - & + & \dots \\ \vdots & \vdots & \vdots & \vdots & \ddots \end{array}$$

Speciálisan, a főátló elemeihez tartozó aldeterminánsok mindig pozitív előjelet kapnak.

Az „előjeles aldeterminánsˮ kifejezésben az „előjeles” jelzőt mindig ki fogjuk tenni, hogy ezt a fogalmat élesen megkülönböztessük a mátrixok rangjánál szereplő aldeterminánsfogalomtól (lásd a 3.4 pontot).

Az előjeles aldeterminánsok jelentőségét az ún. kifejtési tétel adja:

1.4.2 Tétel (Kifejtési tétel)

Ha egy sor minden elemét megszorozzuk a hozzá tartozó előjeles aldeterminánssal, az így kapott szorzatoknak az összege a determinánssal egyenlő:

$$\det A = \alpha_{i1}A_{i1} + \alpha_{i2}A_{i2} + \ldots + \alpha_{in}A_{in} = \sum_{j=1}^{n} \alpha_{ij}A_{ij}\,. \ \clubsuit$$

Ezt hívjuk a determináns i-edik sor szerinti kifejtésének. Természetesen hasonló állítás érvényes sorok helyett oszlopokra is.

Példa: a $D = \begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix}$ determinánst a második oszlopa szerint kifejtve

$$D = 2 \cdot (-1)^3 \begin{vmatrix} 4 & 6 \\ 7 & 9 \end{vmatrix} + 5 \cdot (-1)^4 \begin{vmatrix} 1 & 3 \\ 7 & 9 \end{vmatrix} + 8 \cdot (-1)^5 \begin{vmatrix} 1 & 3 \\ 4 & 6 \end{vmatrix} = 0$$

adódik (amely természetesen egyezik a korábban más módokon kiszámolt eredménnyel).

Bizonyítás: Tekintsük a $\det A = D$ determináns definíció szerinti felírását. Az n-tényezős szorzatokat csoportosítsuk aszerint, hogy az i-edik sorból melyik elem szerepel bennük. Ezt a közös elemet kiemelve, a determináns

$D = \alpha_{i1}\beta_1 + \alpha_{i2}\beta_2 + \ldots + \alpha_{in}\beta_n$ alakban írható. Megmutatjuk, hogy bármely j-re $\beta_j = A_{ij}$.

Fel fogjuk használni az 1.2.3 Tételt, amely akkor is lehetővé teszi a determinánsban szereplő szorzatok előjelezését, ha a szorzat tényezőit nem (feltétlenül) a sorindexek szerint rendeztük.

Tekintsük most a D determinánsban (rögzített j-re) az α_{ij}-t tartalmazó szorzatoknak egy olyan felírását, amikor az α_{ij} tényező áll elől. Egy ilyen szorzat általános alakja:

$$\alpha_{ij}\alpha_{\rho(2)\pi(2)} \ldots \alpha_{\rho(n)\pi(n)} \,. \tag{1.4.1}$$

Itt ρ a sorindexeknek, π az oszlopindexeknek megfelelő permutáció (tehát $\rho(1) = i, \pi(1) = j$). Ennek a szorzatnak az előjele (a D determinánst definíció szerint előállító összegben) az 1.2.3 Tétel szerint $(-1)^{I(\rho)+I(\pi)}$ (ahol $I(\rho)$, illetve $I(\pi)$ az $i, \rho(2), \ldots, \rho(n)$, illetve $j, \pi(2), \ldots, \pi(n)$ permutáció inverziószámát jelöli).

Az α_{ij} kiemelése után így β_j-re az alábbi összeg adódik:

$$\beta_j = \sum (-1)^{I(\rho)+I(\pi)} \, \alpha_{\rho(2)\pi(2)} \ldots \alpha_{\rho(n)\pi(n)} \,. \tag{1.4.2}$$

Itt az összegben minden olyan $n-1$-tényezős szorzatot kell venni, ahol a tényezők az i-edik sor és j-edik oszlop elhagyásával keletkezett D' determináns definíciójában szerepelnek.

Hasonlítsuk most össze az (1.4.2) jobb oldalán álló összeget (amely β_j-vel egyenlő) a D' determinánst definíció szerint előállító összeggel. Mindkét összegben ugyanazokról az $n-1$-tényezős szorzatokról van szó. Vizsgáljuk meg, hogy egy ilyen szorzatot milyen előjellel kellene venni a D' determináns kiszámításához. Ismét az 1.2.3 Tétel szerint ehhez meg kell nézni, hány inverzió fordul elő a sorindexek, valamint az oszlopindexek permutációjában együttvéve.

Ezeket az inverziókat nem befolyásolja, ha a sorok és oszlopok számozásánál megtartjuk az eredeti, D-beli sor-, illetve oszlopszámokat (vagyis a sorokra $1, 2, \ldots, i-1, i+1, \ldots, n$-et, az oszlopokra pedig $1, 2, \ldots, j-1, j+1, \ldots, n$-et). Ennek megfelelően a sorindexeknél a $\rho' = \rho(2)\rho(3)\ldots\rho(n)$ permutáció inverziószámát, $I(\rho')$-t, az oszlopindexeknél pedig a $\pi' = \pi(2)\pi(3)\ldots\pi(n)$ permutáció inverziószámát, $I(\pi')$-t kell tekinteni. (Tehát ρ' az $1, 2, \ldots, i-1$, $i+1, \ldots, n$ számoknak a sorindexek szerinti permutációja, π' pedig az $1, 2, \ldots$, $j-1, j+1, \ldots, n$ számoknak az oszlopindexek szerinti permutációja.)

Az (1.4.1)-ben szereplő eredeti ρ permutációt úgy nyerjük, ha $\rho' = \rho(2)\rho(3)\ldots\rho(n)$ elé $\rho(1) = i$-t írunk. Ezért $I(\rho)$ annyival nagyobb $I(\rho')$-nél,

ahány elemmel $\rho(1) = i$ inverzióban áll. Ezek az elemek nyilván éppen az i-nél kisebb számok, tehát $I(\rho) = I(\rho') + (i-1)$. Ugyanígy $I(\pi) = I(\pi') + (j-1)$.

Az előzőkből $I(\rho) + I(\pi) = i + j - 2 + I(\rho') + I(\pi')$ adódik. Ezt (1.4.2)-be behelyettesítve kapjuk, hogy

$$\beta_j = (-1)^{i+j-2} \sum (-1)^{I(\rho')+I(\pi')} \alpha_{\rho(2)\pi(2)} \dots \alpha_{\rho(n)\pi(n)} = (-1)^{i+j} D' = A_{ij}. \blacksquare$$

Az 1.4.2 Tétel egy másik bizonyítási lehetőségét az 1.4.4 feladatban jelezzük.

A determináns kifejtésével egy n-edrendű determináns kiszámítását visszavezettük n darab $(n-1)$-edrendű determináns kiszámítására. Általában olyan sor vagy oszlop szerint érdemes kifejteni, amelyben sok 0 fordul elő, hiszen a 0 elemekhez tartozó előjeles aldeterminánsokat nem kell kiszámítani.

A kifejtési tétel lehetővé teszi bizonyos típusú általános n-edrendű determinánsok rekurzió útján történő kiszámítását. Ez akkor működik, ha az n-edrendű D_n determinánst kifejtve ugyanolyan típusú alacsonyabb rendű determinánsok (pl. D_{n-1} és D_{n-2}) segítségével tudjuk felírni (ehhez esetleg egyes előjeles aldeterminánsokat is a kifejtési tétel segítségével kell tovább bontani). A kapott rekurzió alapján a D_n-re megsejtett (vagy szisztematikusan megtalált) formula teljes indukcióval igazolható.

A kifejtési tétel alkalmazásánál is célszerű az elemek részletes felírása, a lépések gondos regisztrálása és a változások pontos nyomonkövetése. Ne feledkezzünk el az aldeterminánsról megfelelő előjelezéséről. Ha a kifejtési tételt többször is alkalmazzuk, akkor ügyeljünk arra, hogy közben megváltozik a determinánsok mérete, valamint az egyes elemeknek a sorokban, illetve oszlopokban elfoglalt helyzete. Ennélfogva egy adott elemhez tartozó aldeterminánsminden újabb kifejtési lépésnél teljesen átalakul, beleértve az előjel módosulását is.

Egy determináns kiszámításának nem csak egyféle módja van. Gyakran érdemes a kifejtési tételt az elemi tulajdonságokkal ügyesen kombinálni. Az egyes megoldási módok bonyolultsága, idő- és számolásigénye között számottevő különbség lehet. Sajnos, egy konkrét determinánsnál általában nehéz előre megjósolni, hogy melyik út a leggyorsabb, illetve hogy egy kínálkozó módszer az adott esetben egyáltalán eredményes lesz-e.

A kifejtési tétel segítségével igazolható az ún. ferde kifejtés is:

1.4.3. Tétel (Ferde kifejtés)
Ha egy sor elemeit rendre egy másik sorhoz tartozó előjeles aldeterminánsokkal szorozzuk meg, az így kapott szorzatoknak az összege mindig 0:

$$k \neq r \Rightarrow \alpha_{r1}A_{k1} + \alpha_{r2}A_{k2} + \ldots + \alpha_{rn}A_{kn} = \sum_{j=1}^{n} \alpha_{rj}A_{kj} = 0. \ \clubsuit$$

FIGYELEM! A „kifejtés" szó itt megtévesztő, mert az összeg értékének semmi köze sincs az eredeti determinánshoz; ez az összeg mindig 0, függetlenül attól, hogy maga a determináns 0 vagy sem.

Bizonyítás: Egy *másik* determinánst fogunk készíteni, és arra alkalmazzuk majd a kifejtési tételt. Tekintsük azt az A' mátrixot, amelynek a k-adik sora ugyanaz, mint az eredeti determináns r-edik sora, a többi eleme pedig azonos az eredeti determináns megfelelő elemével. Azaz

$$\alpha'_{ij} = \begin{cases} \alpha_{ij}, & \text{ha } i \neq k; \\ \alpha_{rj}, & \text{ha } i = k. \end{cases}$$

A'-ben a k-adik és az r-edik sor egyenlő (mindkettő az eredeti determináns r-edik sora), ezért $\det A' = 0$. Ha most ezt a determinánst a k-adik sora szerint kifejtjük, akkor — felhasználva, hogy A-ban és A'-ben a k-adik sorhoz tartozó A_{kj} és A'_{kj} előjeles aldeterminánsok minden j-re megegyeznek — éppen a tételbeli összeget kapjuk:

$$\det A' = \alpha'_{k1}A'_{k1} + \alpha'_{k2}A_{k2} + \ldots + \alpha'_{kn}A'_{kn} = \alpha_{r1}A_{k1} + \alpha_{r2}A_{k2} + \ldots + \alpha_{rn}A_{kn}. \blacksquare$$

Feladatok

1.4.1 Egy $n \times n$-es D determináns minden elemét megszorozzuk a hozzá tartozó előjeles aldeterminánssal. Mi lesz az így kapott n^2 darab szorzat összege?

1.4.2 Egy determinánsban az első két sorhoz tartozó előjeles aldeterminánsok rendre megegyeznek, azaz minden j-re $A_{1j} = A_{2j}$. Számítsuk ki a determinánst.

1.4.3 Bizonyítsuk be, hogy α_{11}-et és α_{12}-t megcserélve a determináns akkor és csak akkor nem változik, ha $\alpha_{11} = \alpha_{12}$ vagy $A_{11} = A_{12}$.

1.4.4 Adjunk egy másik bizonyítást a kifejtési tételre az alábbi gondolatmenet alapján:

(i) A tételt először arra a nagyon speciális esetre igazoljuk, amikor az első sor szerint fejtünk ki, és az első sor utolsó $n-1$ eleme 0 (azaz legfeljebb a bal felső sarokban áll nem nulla elem).

(ii) Sor- és oszlopcserékkel vezessük vissza (i)-re azt a (még mindig meglehetősen) speciális esetet, amikor valamelyik sorban $(n-1)$ darab 0 áll (azaz legfeljebb egy elem különbözik 0-tól) és e szerint a sor szerint fejtünk ki.

(iii) Egy általános determinánst bontsunk az 1.3.2 Tétel felhasználásával (ii) típusú determinánsok összegére.

1.4.5 Egy $n \times n$-es márix bal felső sarkában 1-es áll, az első sor többi eleme β, az első oszlop többi eleme γ, a főátló többi eleme δ, az összes többi elem pedig 0. Számítsuk ki a mátrix determinánsát.

1.4.6 Egy $2k \times 2k$-as determináns főátlójának minden eleme γ, a bal alsó sarkot a jobb felső sarokkal összekötő átló minden eleme δ, a többi elem pedig 0. Számítsuk ki a determinánst.

1.4.7 Egy $n \times n$-es determinánsban a főátló minden eleme $\gamma+\delta$, közvetlenül a főátló alatt $n-1$ darab 1-es áll, közvetlenül a főátló felett mind az $n-1$ elem $\gamma\delta$, a többi elem pedig 0. Számítsuk ki a determinánst.

1.4.8 Tekintsünk egy olyan $n \times n$-es komplex elemű mátrixot, amelynek a determinánsa nem nulla. Hány olyan γ komplex szám van, amelyet a mátrix minden eleméhez hozzáadva az így kapott új mátrix determinánsa 0 lesz?

1.4.9 Egy $n \times n$-es determinánsban a bal felső sarokban $\cos\phi$ áll, a főátló többi eleme $2\cos\phi$, közvetlenül a főátló alatt és fölött mind a $2n-2$ elem 1-es, a többi elem pedig 0. Bizonyítsuk be, hogy a determináns $\cos(n\phi)$-vel egyenlő.

1.4.10 Legyenek $\beta_1, \ldots, \beta_n$ tetszőleges számok. Számítsuk ki $\det A$-t, ha az $n \times n$-es A mátrix elemei

$$\alpha_{ij} = \begin{cases} 1-\beta_i^2, & \text{ha } i=j; \\ -\beta_i\beta_j, & \text{ha } i \neq j. \end{cases}$$

1.4.11

(a) Tegyük fel, hogy egy determináns bármely sorában és bármely oszlopában az elemek összege 0. Bizonyítsuk be, hogy valamennyi előjeles aldeterminánsegyenlő.

(b) Tegyük fel, hogy valamennyi előjeles aldeterminánsegyenlő és ez a közös érték nem a 0. Bizonyítsuk be, hogy a determináns bármely sorában és bármely oszlopában az elemek összege 0.

*1.4.12 Egy determináns főátlójának minden eleme γ, a főátló felett csupa δ áll, a főátló alatt pedig csupa β. Számítsuk ki a determinánst.

M*1.4.13 (vö. az 1.2.7 feladattal)

(a) M és C a következő játékot játsszák. M megad egy $n \times n$-es valós elemű mátrixot, C pedig ebben rendre egy-egy elemet tetszőleges másik valós számra kicserélhet. Egy olyan mátrixhoz kell így eljutnia, amelynek a determinánsa nem nulla. M-nek az a célja, hogy C ezt a lehető legtöbb lépésben érje el, C-nek pedig az, hogy a lehető legkevesebben. Mekkora lesz a lépésszám, ha mindketten optimálisan játszanak?

(b) Oldjuk meg a feladatnak azt a módosítását, ha a változtatható elemek helyét is M jelöli ki a következő módon: a mátrix megadása után C vállalja, hogy hány lépésben végez, és ekkor M ennyi helyet kijelöl, és C az ott levő elemeket tetszőleges valós számokra cserélheti.

(c) Oldjuk meg az a) és b) feladatokat arra az esetre, ha a cél az, hogy a determináns nulla legyen.

M*1.4.14 Létezik-e minden n-re olyan $n \times n$-es valós elemű mátrix, amelynek a determinánsa nulla, de bármelyik (egyetlen) elemét akárhogyan megváltoztatva a kapott mátrixok determinánsa sohasem nulla?

*1.4.15 Az 1.4.2 kifejtési tétel általánosítása a *Laplace-kifejtés*. Legyen A egy $n \times n$-es mátrix és $1 \leq k \leq n-1$. Egy $k \times k$-as aldeterminánson tetszőleges k sorból és k oszlopból képezett determinánst értünk. Ennek előjeles komplementer aldeterminánsa a kimaradt sorokból és oszlopokból képezett $(n-k)\times(n-k)$-as aldeterminánsz $(-1)^S$-szerese, ahol S a $k \times k$-as aldeterminánsz sor- és oszlopindexeinek az összege. Rögzítsünk le k sort és szorozzuk össze az ehhez a k sorhoz tartozó mindegyik $k \times k$-as aldeterminánst a neki megfelelő előjeles komplementer aldeterminánssal. Igazoljuk, hogy ezeknek a szorzatoknak az összege az A mátrix determinánsa. (A $k = 1$ speciális esetben kapjuk a kifejtési tételt.)

1.5. Vandermonde-determináns

Gyakran előfordulnak az alábbi speciális típusú determinánsok:

1.5.1 Definíció

Legyen $\gamma_1, \gamma_2, \ldots, \gamma_n$ tetszőleges. A $\gamma_1, \gamma_2, \ldots, \gamma_n$ elemek által generált *Vandermonde-determináns*

$$V(\gamma_1, \gamma_2, \ldots, \gamma_n) = \begin{vmatrix} 1 & \gamma_1 & \gamma_1^2 & \ldots & \gamma_1^{n-1} \\ 1 & \gamma_2 & \gamma_2^2 & \ldots & \gamma_2^{n-1} \\ 1 & \gamma_3 & \gamma_3^2 & \ldots & \gamma_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma_n & \gamma_n^2 & \ldots & \gamma_n^{n-1} \end{vmatrix} . \clubsuit$$

A Vandermonde-determináns i-edik sorában tehát rendre γ_i-nek $0, 1, \ldots, n-1$-edik hatványa áll. Ha két generáló elem azonos, akkor két egyforma sor van, és így a determináns 0. Az alábbi szorzatalakból kiderül, hogy ennek a megfordítása is igaz.

1.5.2 Tétel

$$V(\gamma_1, \gamma_2, \ldots, \gamma_n) = \begin{vmatrix} 1 & \gamma_1 & \gamma_1^2 & \ldots & \gamma_1^{n-1} \\ 1 & \gamma_2 & \gamma_2^2 & \ldots & \gamma_2^{n-1} \\ 1 & \gamma_3 & \gamma_3^2 & \ldots & \gamma_3^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma_n & \gamma_n^2 & \ldots & \gamma_n^{n-1} \end{vmatrix} = \prod_{1 \le j < i \le n} (\gamma_i - \gamma_j) . \clubsuit$$

Bizonyítás: Vonjuk ki jobbról bal felé haladva minden oszlopból az őt megelőző oszlop γ_1-szeresét:

$$\begin{vmatrix} 1 & 0 & 0 & \ldots & 0 \\ 1 & \gamma_2 - \gamma_1 & \gamma_2^2 - \gamma_1\gamma_2 & \ldots & \gamma_2^{n-1} - \gamma_1\gamma_2^{n-2} \\ 1 & \gamma_3 - \gamma_1 & \gamma_3^2 - \gamma_1\gamma_3 & \ldots & \gamma_3^{n-1} - \gamma_1\gamma_3^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \gamma_n - \gamma_1 & \gamma_n^2 - \gamma_1\gamma_n & \ldots & \gamma_n^{n-1} - \gamma_1\gamma_n^{n-2} \end{vmatrix} .$$

Most vonjuk le minden sorból az első sort, ezzel az első oszlop utolsó $n-1$ eleme is 0 lesz, a többi elem pedig nem változott. A második, harmadik

stb. sorból rendre $\gamma_2-\gamma_1$-et, $\gamma_3-\gamma_1$-et stb. kiemelhetünk. Ezzel a

$$(\gamma_2-\gamma_1)\dots(\gamma_n-\gamma_1)\begin{vmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & \gamma_2 & \dots & \gamma_2^{n-2} \\ 0 & 1 & \gamma_3 & \dots & \gamma_3^{n-2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 1 & \gamma_n & \dots & \gamma_n^{n-2} \end{vmatrix} =$$

$$= (\gamma_2-\gamma_1)\dots(\gamma_n-\gamma_1)V(\gamma_2,\dots,\gamma_n)$$

alakra jutottunk. Így a feladatot egy eggyel kisebb rendű Vandermonde-determinánsra vezettük vissza. A fenti eljárást megismételve (vagy teljes indukcióval) adódik a tétel. ■

Feladatok

1.5.1 Fejezzük ki $V=V(\gamma_1,\dots,\gamma_n)$ segítségével az alábbi szorzatokat:
(a) $\prod_{1\le i<j\le n}(\gamma_i-\gamma_j)$; (b) $\prod_{1\le j\ne i\le n}(\gamma_i-\gamma_j)$.

1.5.2 Legyenek $\gamma_2,\dots,\gamma_n$ rögzített komplex számok. Hány megoldása van a $V(x,\gamma_2,\dots,\gamma_n)=0$ egyenletnek? Előfordulhat-e, hogy valamely δ komplex számra a $V(x,\gamma_2,\dots,\gamma_n)=\delta$ egyenletnek ennél (a) több; (b) kevesebb megoldása van?

1.5.3 Egy determináns minden sora mértani sorozat (0 elemet nem engedünk meg). Számítsuk ki a determinánst.

1.5.4 Számítsuk ki azt az $n\times n$-es determinánst, ahol az i-edik sor j-edik eleme i^j.

1.5.5
(a) Legyenek $f_0,\dots,f_{n-1}$ valós együtthatós polinomok, ahol $\deg f_k=k$, továbbá $\gamma_1,\dots,\gamma_n$ tetszőleges valós számok. Számítsuk ki azt az $n\times n$-es determinánst, amelyben az i-edik sor j-edik eleme $f_{i-1}(\gamma_j)$.
(b) Mennyi a determináns értéke, ha a polinomok fokszámára vonatkozó kikötést a $\deg f_k\le n-2$ feltételre cseréljük ki?

M 1.5.6 Legyenek $\alpha_1,\dots,\alpha_n,\beta_1,\dots,\beta_n$ valós számok, ahol $\alpha_i\beta_j\ne 1$. Számítsuk ki azt az $n\times n$-es determinánst, amelyben az i-edik sor j-edik eleme $(1-\alpha_i^n\beta_j^n)/(1-\alpha_i\beta_j)$.

1.5.7 Legyenek $\alpha_1, \ldots, \alpha_n, \beta_1, \ldots, \beta_n$ valós számok. Számítsuk ki azt az $n \times n$-es determinánst, amelyben az i-edik sor j-edik eleme $(\alpha_i + \beta_j)^{n-1}$.

1.5.8 Legyenek $\phi_1, \ldots, \phi_n$ olyan valós számok, amelyek koszinuszai páronként különbözők. Legyen $D_1 = V(\cos\phi_1, \ldots, \cos\phi_n)$, D_2 pedig az a determináns, ahol az i-edik sor j-edik eleme $\cos[(j-1)\phi_i]$. Bizonyítsuk be, hogy a D_2/D_1 hányados nem függ a ϕ_i számok választásától.

1.5.9 Legyenek $\gamma_1, \ldots, \gamma_n$ különböző valós számok.

(a) Hogyan változik a Vandermonde-determináns, ha γ_i-t és γ_j-t felcseréljük?

(b) Melyek azok a σ permutációk, amelyekre

$$V(\gamma_1, \gamma_2, \ldots, \gamma_n) = V(\gamma_{\sigma(1)}, \gamma_{\sigma(2)}, \ldots, \gamma_{\sigma(n)})?$$

1.5.10 Egy $n \times n$-es D determináns i-edik sorának j-edik eleme 2^{ij}. A 2-nek hányadik hatványával osztható D?

1.5.11 Legyenek $a_1, \ldots, a_n$ tetszőleges egész számok. Bizonyítsuk be, hogy $V(a_1, \ldots, a_n)$ osztható

(a) az $1, 2, \ldots, n-1$ számok legkisebb közös többszörösével;

*(b) $V(1, 2, \ldots, n)$-nel.

*1.5.12 Legyen $p > 2$ prím, és $V_p = V(1, 2, \ldots, p)$. Milyen maradékot ad p-vel osztva V_p^2?

*1.5.13 Számítsuk ki azt a determinánst, amely $V(\gamma_1, \ldots, \gamma_n)$-től annyiban tér el, hogy az utolsó oszlopban rendre (γ_i^{n-1} helyett) γ_i^n áll.

2. MÁTRIXOK

A mátrixok szorosan kapcsolódnak a determinánsok, illetve a lineáris egyenletrendszerek elméletéhez, de ezektől függetlenül is számos alkalmazásuk van. Különösen érdekes és fontos a mátrixszorzás és annak néhány „szokatlan" tulajdonsága. Ezeknek a „furcsaságoknak" az (egyik) „igazi" magyarázatát majd a lineáris leképezésekkel való kapcsolat adja, amit az 5. fejezetben tárgyalunk.

2.1. Mátrixműveletek

A mátrixokkal már az 1.2 pontban találkoztunk, de a teljesség kedvéért megismételjük a definíciót és a jelölésre vonatkozó tudnivalókat:

2.1.1 Definíció

Legyen T egy kommutatív test és k, n adott pozitív egészek. Ekkor a T test feletti $k \times n$-es *mátrix*on egy olyan téglalap alakú táblázatot értünk, amelynek k sora és n oszlopa van és amelynek elemei T-ből valók. ♣

A mátrixot úgy jelöljük, hogy a táblázatot gömbölyű zárójelek közé foglaljuk. (Ismét felhívjuk a figyelmet arra, hogy a két függőleges határolóvonal a determinánst jelenti.) Egy általános A mátrix i-edik sorának j-edik elemét α_{ij}-vel fogjuk jelölni. Ennek megfelelően egy $k \times n$-es (vagy $k \times n$ méretű) mátrix általános alakja

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix} .$$

A T feletti $k \times n$-es mátrixok halmazát $T^{k \times n}$-nel jelöljük.

Itt is megjegyezzük, hogy általános T test helyett első közelítésben legtöbbször nyugodtan gondolhatunk pl. a valós, a racionális vagy a komplex számokra. Emellett azonban — különösen az alkalmazások szempontjából — nagyon fontosak a véges testek is. Ezek legegyszerűbb fajtája F_p, a modulo p maradékosztályok teste, ahol p prímszám.

Most két mátrix összeadását, illetve egy mátrixnak egy T-beli elemmel való szorzását definiáljuk. Ezeknek a műveleteknek az értelmezése a „természetes módon", elemenként történik a T-beli összeadás és szorzás segítségével:

2.1.2 Definíció

Legyen $A, B \in T^{k\times n}$, $\lambda \in T$. Ekkor $A+B$-t, illetve λA-t úgy kapjuk meg, hogy a megfelelő helyeken álló elemeket összeadjuk, illetve minden elemet λ-val megszorzunk:

$$A+B=\begin{pmatrix}\alpha_{11} & \alpha_{12} & \dots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n}\\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn}\end{pmatrix}+\begin{pmatrix}\beta_{11} & \beta_{12} & \dots & \beta_{1n}\\ \beta_{21} & \beta_{22} & \dots & \beta_{2n}\\ \vdots & & & \\ \beta_{k1} & \beta_{k2} & \dots & \beta_{kn}\end{pmatrix}=$$

$$=\begin{pmatrix}\alpha_{11}+\beta_{11} & \alpha_{12}+\beta_{12} & \dots & \alpha_{1n}+\beta_{1n}\\ \alpha_{21}+\beta_{21} & \alpha_{22}+\beta_{22} & \dots & \alpha_{2n}+\beta_{2n}\\ \vdots & & & \\ \alpha_{k1}+\beta_{k1} & \alpha_{k2}+\beta_{k2} & \dots & \alpha_{kn}+\beta_{kn}\end{pmatrix}$$

és

$$\lambda A=\lambda\begin{pmatrix}\alpha_{11} & \alpha_{12} & \dots & \alpha_{1n}\\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n}\\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn}\end{pmatrix}=\begin{pmatrix}\lambda\alpha_{11} & \lambda\alpha_{12} & \dots & \lambda\alpha_{1n}\\ \lambda\alpha_{21} & \lambda\alpha_{22} & \dots & \lambda\alpha_{2n}\\ \vdots & & & \\ \lambda\alpha_{k1} & \lambda\alpha_{k2} & \dots & \lambda\alpha_{kn}\end{pmatrix}. \clubsuit$$

A T test elemeit szokás *skalár*oknak nevezni, és így egy mátrixnak egy T-beli elemmel vett szorzatát a mátrix *skalárszoros*ának hívjuk.

Az imént definiált műveletekre a megszokott tulajdonságok érvényesek:

2.1.3 Tétel

A $k\times n$-es mátrixok körében az összeadás asszociatív, kommutatív, létezik nullelem és minden elemnek létezik ellentettje. Ez részletesen kifejtve a következőket jelenti:

(i) minden $A, B, C \in T^{k\times n}$-re $(A+B)+C=A+(B+C)$, $A+B=B+A$;
(ii) létezik olyan 0-val jelölt mátrix, amelyre minden A-val $A+0=0+A=A$;
(iii) minden A-hoz van olyan $-A$-val jelölt mátrix, amelyre $A+(-A)=$ $=(-A)+A=0$.

A T elemeivel való szorzásra nézve az alábbi azonosságok érvényesek ($A, B \in T^{k\times n}$, $\lambda, \mu \in T$):

$(\lambda+\mu)A=\lambda A+\mu A$, $\lambda(A+B)=\lambda A+\lambda B$, $(\lambda\mu)A=\lambda(\mu A)$, $1A=A$, ahol 1 a T test egységeleme (azaz amellyel minden $\lambda \in T$-re $1\lambda=\lambda 1=\lambda$). $\clubsuit$

Az összeadás tulajdonságait úgy foglalhatjuk össze, hogy a $k\times n$-es mátrixok az összeadásra nézve egy kommutatív csoportot alkotnak (lásd az A.8

pontot). A két műveletre együttesen $T^{k\times n}$ vektortér T felett (lásd a 4.1 pontot).

Bizonyítás: Valamennyi tulajdonság azonnal adódik a műveletek definíciójából és a T-beli megfelelő tulajdonságból. Például a 0 mátrix (nullmátrix) az lesz, amelynek minden eleme (a T-beli) nulla stb. ■

Mind a T-beli nullát, mind pedig a nullmátrixot egyformán 0-val fogjuk jelölni, ez (remélhetőleg) nem okoz majd zavart.

Most rátérünk két mátrix szorzásának a definíciójára. Ez meglehetősen bonyolult és (legalábbis egyelőre) meglehetősen mesterkéltnek tűnik. Először megadjuk a formális definíciót, majd ehhez némi magyarázatot fűzünk.

2.1.4 Definíció

Legyen $A \in T^{k\times n}$, $B \in T^{n\times r}$. Ekkor $C = AB \in T^{k\times r}$ és az i-edik sor j-edik eleme

$$\gamma_{ij} = \alpha_{i1}\beta_{1j} + \alpha_{i2}\beta_{2j} + \ldots + \alpha_{in}\beta_{nj} = \sum_{s=1}^{n} \alpha_{is}\beta_{sj} \,.\ \clubsuit$$

Az A és B mátrix tehát akkor és csak akkor szorozható össze (ebben a sorrendben), ha A-nak ugyanannyi *oszlopa* van, mint ahány *sora* B-nek. Ekkor az AB mátrixnak annyi sora lesz, mint A-nak és annyi oszlopa, mint B-nek. A szorzatmátrixban az i-edik sor j-edik elemét úgy kapjuk meg, hogy A i-edik sorát és B j-edik oszlopát (mint két n komponensű vektort) skalárisan összeszorozzuk, azaz a megfelelő komponensek szorzatösszegét vesszük.

Példa: legyen $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 0 \end{pmatrix}$, $B = \begin{pmatrix} 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 \end{pmatrix}$. Ekkor az AB szorzat létezik, mert A oszlopainak a száma megegyezik B sorainak a számával. Ugyanakkor a BA szorzat nem létezik.

Az AB szorzatnak 3 sora és 4 oszlopa lesz. A második sor harmadik elemét A második sorának és B harmadik oszlopának a skalárszorzata adja: $3 \cdot 8 + 4 \cdot 12 = 72$.

Amíg a mátrixok szorzásában nem teszünk szert megfelelő gyakorlatra, addig érdemes a szorzást az alábbi séma szerint elvégezni. Helyezzük el az A

és B mátrixokat egymáshoz képest rézsút a következőképpen:

$$\begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix} \begin{pmatrix} \beta_{11} & \dots & \beta_{1r} \\ \beta_{21} & \dots & \beta_{2r} \\ \beta_{31} & \dots & \beta_{3r} \\ \vdots & \vdots & \vdots \\ \beta_{n1} & \dots & \beta_{nr} \end{pmatrix}$$
$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix}$$

Ekkor a két mátrix között (az A-tól jobbra, a B alatt) úgy kaphatjuk meg $C = AB$-t, hogy γ_{ij} éppen az őt létrehozó sor-oszlop párnak, A i-edik sorának és B j-edik oszlopának a metszéspontjába kerül:

$$\begin{pmatrix} & & & \\ & & & \\ & & & \\ & & & \end{pmatrix} \begin{pmatrix} \beta_{11} & \dots & \beta_{1r} \\ \beta_{21} & \dots & \beta_{2r} \\ \beta_{31} & \dots & \beta_{3r} \\ \vdots & \vdots & \vdots \\ \beta_{n1} & \dots & \beta_{nr} \end{pmatrix}$$
$$\begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix} \begin{pmatrix} \gamma_{11} & \dots & \gamma_{1r} \\ \gamma_{21} & \dots & \gamma_{2r} \\ \vdots & \vdots & \vdots \\ \gamma_{k1} & \dots & \gamma_{kr} \end{pmatrix}$$

A fenti példánkban:

$$\begin{pmatrix} & & & \\ & & & \\ & & & \end{pmatrix} \begin{pmatrix} 6 & 7 & 8 & 9 \\ 10 & 11 & 12 & 13 \end{pmatrix}$$
$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 0 \end{pmatrix} \begin{pmatrix} 26 & 29 & 32 & 35 \\ 58 & 65 & 72 & 79 \\ 30 & 35 & 40 & 45 \end{pmatrix}$$

Most rátérünk a mátrixszorzás tulajdonságainak a vizsgálatára. Kezdjük a kommutativitással. Legyen $A \in T^{k\times n}$, $B \in T^{n\times r}$, ekkor AB értelmes. Ha $k \neq r$, akkor a BA szorzat nem is létezik! Ha $k = r \neq n$, akkor AB és BA nem azonos alakúak, hiszen az egyik $k \times k$-as, a másik $n \times n$-es. Marad az az

eset, amikor $k = n = r$, azaz $A, B \in T^{n\times n}$. Azonban általában ilyenkor sem áll fenn $AB = BA$, pl.

$$\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}\begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix} = \begin{pmatrix} 19 & 22 \\ 43 & 50 \end{pmatrix} \neq \begin{pmatrix} 23 & 34 \\ 31 & 46 \end{pmatrix} = \begin{pmatrix} 5 & 6 \\ 7 & 8 \end{pmatrix}\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}.$$

A fenti példából az is érezhető, hogy az a ritka eset, ha két mátrix felcserélhető. Mindez azt jelenti, hogy a mátrixok szorzása „nagyon nem kommutatív".

A szorzással (és részben más műveletekkel) kapcsolatos további „szokásos" *azonosságok* viszont igazak:

2.1.5 Tétel

Ha $\lambda \in T$, és A, B, C tetszőleges olyan mátrixok, amelyekre az alábbi egyenlőségek valamelyik oldala értelmezve van, akkor a másik oldal is értelmes, és az egyenlőség teljesül.

I. $A(BC) = (AB)C$ (asszociativitás);
II. $A(B + C) = AB + AC$,
$(A + B)C = AC + BC$ (disztributivitás*ok*);
III. $\lambda(AB) = (\lambda A)B = A(\lambda B)$. ♣

Mivel a szorzás nem kommutatív, ezért a két disztributivitást külön kell bebizonyítani. Ugyanez az oka annak, hogy III-ban csak a T-beli elemet „emelhetjük át" a mátrixokon, A és B sorrendjén nem változtathatunk.

Bizonyítás: Belátjuk az asszociativitást, a többi azonosság hasonló számolással igazolható (lásd a 2.1.13 feladatot).

A szorzás definíciója alapján I. jobb, illetve bal oldala pontosan akkor értelmes, ha A oszlopainak a száma megegyezik B sorainak a számával és B oszlopainak a száma megegyezik C sorainak a számával. Legyen tehát $A \in T^{k\times n}, B \in T^{n\times r}, C \in T^{r\times t}$, ekkor $M = A(BC)$ és $N = (AB)C$ is $k \times t$-es. Kiszámítjuk M, illetve N i-edik sorának j-edik elemét, μ_{ij}-t, illetve ν_{ij}-t. Legyen $D = BC$. Ekkor

$$\begin{aligned}\mu_{ij} &= \alpha_{i1}\delta_{1j} + \ldots + \alpha_{in}\delta_{nj} = \\ &= \alpha_{i1}(\beta_{11}\gamma_{1j} + \ldots + \beta_{1r}\gamma_{rj}) + \ldots + \alpha_{in}(\beta_{n1}\gamma_{1j} + \ldots + \beta_{nr}\gamma_{rj}),\end{aligned}$$

vagyis

$$\mu_{ij} = \sum_{1\leq u\leq n,\, 1\leq v\leq r} \alpha_{iu}(\beta_{uv}\gamma_{vj}).$$

Hasonlóan kapjuk, hogy

$$\nu_{ij} = \sum_{1\le u\le n,\, 1\le v\le r} (\alpha_{iu}\beta_{uv})\gamma_{vj}\,.$$

Mivel T-ben a szorzás asszociatív, így valóban $\mu_{ij} = \nu_{ij}$. ■

Végül bevezetjük a mátrix transzponáltjának a fogalmát:

2.1.6 Definíció
Legyen $A \in T^{k\times n}$. Ekkor A *transzponált*ján azt a $B \in T^{n\times k}$ mátrixot értjük, amelyre $\beta_{ij} = \alpha_{ji}$. Az A mátrix transzponáltját A^T-vel jelöljük. ♣

A jelölésben a T betű a transzponált szó kezdőbetűjéből származik (és semmi köze sincs a T testhez, amelyből a mátrix elemeit vettük).

Példa: az $\begin{pmatrix} 1 & 2 \\ 3 & 4 \\ 5 & 6 \end{pmatrix}$ mátrix transzponáltja az $\begin{pmatrix} 1 & 3 & 5 \\ 2 & 4 & 6 \end{pmatrix}$ mátrix lesz.

A transzponálás geometriailag a (nem mindig igazán annak nevezhető) „főátlóra”, azaz a bal felső sarokból 45 fokos szögben jobbra lefelé haladó (ÉNy-DK irányú) egyenesre történő tükrözést jelenti. Másképpen fogalmazva, a transzponálás a sorok és oszlopok szerepét felcseréli.

Komplex elemű mátrixok esetén egy másik rokon fogalom, az adjungált (is) fontos szerephez jut:

2.1.7 Definíció
Legyen $A \in \mathbf{C}^{k\times n}$. Ekkor A *adjungált*ján azt a $B \in \mathbf{C}^{n\times k}$ mátrixot értjük, amelyre $\beta_{ij} = \overline{\alpha_{ji}}$ (ahol $\overline{z}$ a z komplex szám konjugáltját jelenti). Az A mátrix adjungáltját A^*-gal jelöljük. ♣

Egy mátrix adjungáltja tehát a transzponáltjának a konjugáltja. Valós elemű A esetén nyilván $A^* = A^T$.

A transzponálás, illetve adjungálás és a mátrixműveletek kapcsolatáról lásd a 2.1.20 feladatot.

Feladatok

2.1.1 Tekintsük az összes olyan különböző $k \times n$-es valós elemű mátrixot, amelyben minden elem 1, 2 vagy 3. Számítsuk ki ezeknek a mátrixoknak az összegét.

2.1.2 Mely α, β komplex számpárok rendelkeznek az alábbi tulajdonsággal: Minden $k \times n$-es komplex elemű mátrix felírható $\alpha A + \beta B$ alakban, ahol A és B valós elemű mátrixok.

2.1.3 Legyen E egy olyan négyzetes mátrix, amelynek a főátlójában 1-esek állnak, többi eleme pedig 0. Mi lesz az EA, illetve az AE szorzat, ha a szorzás elvégezhető (A egy tetszőleges mátrix)?

2.1.4 Számítsuk ki az alábbi mátrixokat:

$$\text{(a)} \begin{pmatrix} 2 & -4 \\ 1 & -2 \end{pmatrix}^{1111}; \quad \text{(b)} \begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}^{1111}; \quad \text{(c)} \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}^{1111}.$$

2.1.5 Számítsuk ki az alábbi mátrixokat:

$$\text{(a)} \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^{n}; \text{ (b)} \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}^{n}; \text{ (c)} \begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}^{n}.$$

2.1.6 Végezzük el az alábbi szorzásokat:

$$\text{(a)} \begin{pmatrix} a & 1-a \\ a & 1-a \end{pmatrix} \begin{pmatrix} b & 1-b \\ b & 1-b \end{pmatrix}; \qquad \text{(b)} \begin{pmatrix} a & -a \\ a & -a \end{pmatrix} \begin{pmatrix} b & -b \\ b & -b \end{pmatrix}.$$

2.1.7 Legyen A egy olyan mátrix, amelyben minden sorban és minden oszlopban az elemek összege 0, B pedig egy olyan mátrix, amelynek minden eleme egyenlő. Mi lesz az AB, illetve BA szorzat, ha a szorzás elvégezhető?

2.1.8 Az alábbiakban tegyük fel, hogy a szóban forgó AB, illetve BA szorzatok értelmesek. Melyek igazak az alábbi állítások közül?

(a) Ha A-nak van egy csupa 0 sora, akkor ez AB-re is teljesül.
(b) Ha A-nak van egy csupa 0 sora, akkor ez BA-ra is teljesül.
(c) Ha A-ban minden sor számtani sorozat, akkor ez AB-re is teljesül.
(d) Ha A-ban minden sor számtani sorozat, akkor ez BA-ra is teljesül.
(e) Ha A elemeinek az összege 0, akkor ez AB-re is teljesül.
(f) Ha A elemeinek az összege 0, akkor ez BA-ra is teljesül.

2.1.9 Vizsgáljuk meg az alábbi állítást és a hozzátartozó indoklást.
Ha az A és B azonos méretű négyzetes mátrixokra $A^{100} = B^{100} = 0$, akkor $(A+B)^{200} = 0$. Ugyanis

$$(A+B)^{200} = A^{200} + \binom{200}{1} A^{199}B + \ldots + \binom{200}{k} A^k B^{n-k} + \ldots,$$

és itt minden tag 0, hiszen $k \geq 100$ esetén $A^k = 0$, $k < 100$ esetén pedig $n - k > 100$, tehát $B^{n-k} = 0$.

2.1.10 Mi történik egy $n \times n$-es A mátrixszal, ha balról, illetve jobbról az alábbi $n \times n$-es mátrixokkal megszorozzuk:

$$B = \begin{pmatrix} 5 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}; \qquad C = \begin{pmatrix} 1 & 6 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \end{pmatrix}?$$

2.1.11 Legyen P egy olyan $n \times n$-es mátrix, amelynek minden sorában és minden oszlopában pontosan egy 1-es áll, a többi elem pedig 0. Mi történik egy $n \times n$-es A mátrixszal, ha balról, illetve jobbról P-vel megszorozzuk?

2.1.12 Legyenek A és B tetszőleges $n \times n$-es mátrixok. Mennyi az $AB - BA$ mátrix főátlójában levő elemek összege?

2.1.13 Bizonyítsuk be a 2.1.5 Tétel II. és III. állításait.

2.1.14 Tegyük fel, hogy $A^{100} = A^{72} = A$. Hány különböző (pozitív egész kitevős) hatványa van az A mátrixnak?

2.1.15 Egy $n \times n$-es A mátrix főátlójában és a főátló alatt minden elem 0. Bizonyítsuk be, hogy $A^n = 0$.

*2.1.16 Legyen p prímszám és A egy olyan $p \times p$-es mátrix a modulo p test felett, amelynek a főátlójában 1-esek állnak, a főátló alatt pedig minden elem 0. Számítsuk ki A^p-t.

*2.1.17 Legyen $A = \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix}$ és $E = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Bizonyítsuk be, hogy akkor és csak akkor létezik olyan k pozitív egész, amelyre $E + A + A^2 + \ldots + A^k = 0$, ha $\alpha/2\pi$ racionális szám, de nem egész.

M*2.1.18 Melyek azok az $A \in T^{n\times n}$ mátrixok, amelyek minden $B \in T^{n\times n}$ mátrixszal felcserélhetők, azaz minden B-re $AB = BA$?

2.1.19 Adva van k termék, az ezek előállításához szükséges n-féle alkatrész és az alkatrészeket alkotó r-féle anyag. Jelöljük α_{ij}-vel azt, hogy az i-edik termékhez a j-edik alkatrészből hány darabot kell felhasználni, β_{uv}-vel pedig azt, hogy az u-adik alkatrész a v-edik anyagból mennyit tartalmaz. Mi az α_{ij}-kből álló $k \times n$-es A mátrix és a β_{uv}-kből álló $n \times r$-es B mátrix $C = AB$ szorzatának a jelentése?

2.1.20 Bizonyítsuk be az alábbi azonosságokat (azaz lássuk be, hogy ha $\lambda \in T$ és A, B tetszőleges olyan mátrixok, amelyekre az alábbi egyenlőségek valamelyik oldala értelmezve van, akkor a másik oldal is értelmes és az egyenlőség teljesül):

$$(A+B)^T = A^T + B^T, \qquad (\lambda A)^T = \lambda A^T, \qquad (AB)^T = B^T A^T .$$

Fogalmazzuk meg és igazoljuk az adjungáltra vonatkozó hasonló azonosságokat is.

2.1.21 Legyen A valós elemű mátrix és tegyük fel, hogy az AA^T (valóban négyzetes mátrix valódi) főátlójában az elemek összege 0. Határozzuk meg A-t. Hogyan általánosíthatjuk a feladatot komplex elemű mátrixokra?

2.2. Az $n \times n$-es mátrixok gyűrűje

Alkalmazzuk most az előző pont eredményeit a négyzetes mátrixokra:

2.2.1 Tétel
Egy T test feletti összes $n \times n$-es mátrix a (mátrix)összeadásra és (mátrix)szorzásra nézve gyűrűt alkot. Ez a $T^{n\times n}$ gyűrű egységelemes, de ($n > 1$ esetén) nem kommutatív. ♣

A gyűrű pontos definícióját lásd az A.6 pontban (de ez közvetve tulajdonképpen a jelen tétel bizonyításában is szerepel).

Bizonyítás: Az összeadás és a szorzás a 2.1.2, illetve 2.1.4 Definíció alapján bármely két ilyen mátrixra értelmes. A 2.1.3 és 2.1.5 Tétel biztosítja, hogy az összeadás kommutatív és asszociatív, létezik nullelem, minden mátrixnak létezik ellentettje, a szorzás asszociatív és érvényesek a disztributivitások. $T^{n\times n}$ tehát valóban gyűrű. A szorzás egységeleme a 2.1.3 feladatban definiált E mátrix: a főátlóban 1-ek állnak, a többi elem 0. Végül a szorzás kommutativitásának a hiányát a 2.1.5 Tétel előtti ellenpéldával (pontosabban annak minden $n >$ 2-re történő általánosításával vagy pedig a 2.1.6a, illetve 2.1.10 feladat segítségével) igazolhatjuk. ■

FIGYELEM! Az, hogy a szorzás nem kommutatív, természetesen nem azt jelenti, hogy *semelyik* két mátrix nem cserélhető fel, például az E egységmátrix vagy a nullmátrix bármely mátrixszal felcserélhető, bármely mátrix felcserélhető a saját hatványaival stb.

A $T^{n\times n}$ gyűrűben a szorzás tulajdonságait nézve megállapíthatjuk, hogy általában nem lehet osztani, és a nemkommutativitáson kívül további „érdekesség" az, hogy két nem nulla mátrix szorzata is lehet a nullmátrix.

Ezek alaposabb vizsgálatához az alábbiakban (a négyzetes) mátrixokra előbb definiáljuk az inverz és a nullosztó fogalmát, majd részletesen tárgyaljuk az idevágó eredményeket. Megjegyezzük, hogy a tetszőleges gyűrűben az inverz és a nullosztó általános tulajdonságai szerepelnek az A.6 pontban, de most a mátrixok vonatkozásában ezeket is külön felsoroljuk.

Kezdjük az inverzzel. Mátrixon a továbbiakban mindig négyzetes mátrixot, $T^{n\times n}$ egy elemét értjük, E pedig az egységmátrixot, a $T^{n\times n}$ gyűrű egységelemét jelöli. A tetszőleges gyűrűre vonatkozó inverzfogalomnak megfelelően egy A mátrix *kétoldali inverzén* (vagy röviden *inverzén*) egy olyan K mátrixot értünk, amelyre $AK = KA = E$. Ha egy B mátrixra $BA = E$ teljesül, akkor B az A mátrix *bal oldali inverze* (vagy röviden *balinverze*), ha pedig $AJ = E$, akkor J az A mátrix *jobb oldali inverze* (vagy röviden *jobbinverze*).

Bármely gyűrűben teljesül (lásd az A.4, illetve A.6 pontot), hogy ha egy elemnek létezik bal- és jobbinverze is, akkor ezek szükségképpen egyenlők, és ekkor az elemnek nem lehet több bal-, illetve jobbinverze. Egy elem (kétoldali) inverze tehát egyértelműen meghatározott.

Az A mátrix (kétoldali) inverzét A^{-1}-gyel jelöljük.

A determinánsok segítségével jól le tudjuk írni, hogy mely mátrixoknak létezik inverze:

2.2.2 Tétel

I. Ha $\det A \neq 0$, akkor A-nak létezik (kétoldali) inverze.

II. Ha A-nak létezik balinverze (vagy jobbinverze), akkor $\det A \neq 0$. ♣

A két állítást összekapcsolva nyerjük, hogy $n \times n$-es mátrixokra az egyik oldali inverz létezése maga után vonja a másik oldali inverz létezését is, és a bal oldali, jobb oldali és kétoldali inverz bármelyikének a létezése ekvivalens a $\det A \neq 0$ feltétellel.

Megjegyezzük még, hogy I. bizonyítása során képletet is nyerünk A inverzére, és ezt a képletet később többször fel fogjuk használni.

Bizonyítás: I. bizonyításának a kulcsa a következő azonosság, amelyben az előjeles aldeterminánsokból képezett mátrix transzponáltja játszik fontos szerepet:

2.2.3 Lemma

Legyen $\hat{A}$ az a mátrix, amelyben az i-edik sor j-edik eleme A_{ji}, (*nem* A_{ij},) ahol A_{kl} az A mátrix α_{kl} eleméhez tartozó előjeles aldeterminánst jelöli. Ekkor

$$A\hat{A} = \hat{A}A = (\det A) \cdot E = \begin{pmatrix} \det A & 0 & \dots & 0 \\ 0 & \det A & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \det A \end{pmatrix} . \clubsuit$$

A lemma bizonyítása: Az $A\hat{A}$ mátrix i-edik sorának j-edik elemét úgy kapjuk meg, hogy az A mátrix i-edik sorát az $\hat{A}$ mátrix j-edik oszlopával szorozzuk össze: $\alpha_{i1}A_{j1} + \ldots + \alpha_{in}A_{jn}$, ami a kifejtés, illetve a ferde kifejtés (1.4.2 és 1.4.3 Tételek) szerint $\det A$, ha $i = j$, illetve 0, ha $i \neq j$. Az $A\hat{A}$ szorzat tehát valóban az egységmátrix $\det A$-szorosa. A másik állítást hasonlóan kapjuk az oszlopokra vonatkozó kifejtés, illetve ferde kifejtés segítségével. ■

A lemma alapján azonnal adódik, hogy $A^{-1} = \frac{1}{\det A} \cdot \hat{A}$.

II. igazolásához az alábbi tételt használjuk fel, amelyet itt bizonyítás nélkül közlünk:

2.2.4 Tétel (Determinánsok szorzástétele)

$$\det(AB) = \det A \cdot \det B\,. \clubsuit$$

Ez azt jelenti, hogy ha két (azonos méretű) determinánst a mátrixszorzás szabályai szerint „összeszorzunk", akkor a kapott determináns valóban a két determináns szorzata lesz. Mivel a determináns a főátlóra való tükrözésnél nem változik, ezért a fenti tétel sor-oszlop szorzás helyett sor-sor, oszlop-oszlop és oszlop-sor szorzás esetén is érvényben marad.

Rátérve a II. állítás bizonyítására, ha A-nak létezik balinverze, azaz $BA = E$, akkor a 2.2.4 Tétel szerint $\det B \cdot \det A = \det E = 1$, és így $\det A$ valóban nem lehet 0. ■

A 2.2.2 Tételre a 3.5 pontban a lineáris egyenletrendszerek segítségével újabb bizonyítást adunk majd. Megjegyezzük még, hogy a 2.2.4 Tételt (az egyik lehetséges módon) a 9.8 pont alapján láthatjuk be, erre a 9.8.4 feladatban utalunk. Egy másik utat a 2.2.15 feladatban vázolunk.

A továbbiakban $T^{n\times n}$ nullosztóit vizsgáljuk. A tetszőleges gyűrűre vonatkozó nullosztófogalomnak megfelelően egy A mátrix akkor *bal oldali nullosztó*, ha $A \neq 0$ és létezik olyan $U \neq 0$ mátrix, amelyre $AU = 0$. A jobb oldali nullosztó analóg módon definiálható.

Bármely gyűrűben teljesül (lásd az A.6.3 Tételt), hogy ha egy elemnek létezik balinverze, akkor ez az elem (nem nulla és) nem lehet bal oldali nullosztó. Hasonló állítás érvényes jobbinverzre és jobb oldali nullosztóra is.

A determinánsok segítségével az is jól jellemezhető, hogy mely mátrixok nullosztók:

2.2.5 Tétel

Egy (négyzetes) $A \neq 0$ mátrix akkor és csak akkor bal oldali (jobb oldali) nullosztó, ha $\det A = 0$. ♣

Bizonyítás: A „csak akkor" rész következik a 2.2.2 Tételből és az inverz és nullosztó előbb említett kapcsolatából. — Az „akkor" részt most csak arra a speciális esetre bizonyítjuk, ha az A mátrixban az A_{ij} előjeles aldeterminánsok között van nullától különböző, azaz (a 2.2.3 Lemmában definiált) $\hat{A}$ nem a nullmátrix. A 2.2.3 Lemma szerint ekkor $A\hat{A} = \hat{A}A = (\det A) \cdot E = 0 \cdot E = 0$, tehát az $\hat{A} \neq 0$ mátrix „igazolja" A nullosztó voltát. ■

A 2.2.5 tételre a 3.5 pontban két másfajta (és hiánytalan) bizonyítást adunk majd.

Szubjektív (és egyáltalán nem matematikai) összefoglalásként megállapíthatjuk, hogy az $n \times n$-es mátrixok gyűrűje a szorzás szempontjából „nem túl szép", a kommutativitás hiányán túlmenően „rengeteg" a nullosztó, amelyeknek így inverzük sem lehet, vagyis a mátrixok gyűrűje „messzemenően" nem test.

Feladatok Az alábbi feladatokban végig $T^{n\times n}$-beli mátrixokról van szó.

2.2.1 Melyek igazak az alábbi állítások közül?

(a) Ha $AB = BA$, akkor $(A + B)^2 = A^2 + 2AB + B^2$.
(b) Ha $(A + B)^2 = A^2 + 2AB + B^2$, akkor $AB = BA$.
*(c) Ha $(A + B)^3 = A^3 + 3A^2B + 3AB^2 + B^3$, akkor $AB = BA$.

2.2.2 Melyek igazak az alábbi állítások közül?

(a) Ha A-nak és B-nek létezik inverze, akkor AB-nek is létezik inverze.
(b) Ha AB-nek létezik inverze, akkor A-nak és B-nek is létezik inverze.
(c) Ha $A + B$-nek és $A - B$-nek létezik inverze, akkor $A^2 - B^2$-nek is létezik inverze.
(d) Ha A-nak és B-nek létezik inverze, akkor $A+B$-nek is létezik inverze.

(e) Ha $A+B$-nek létezik inverze, akkor A és B közül legalább az egyiknek létezik inverze.
(f) Ha A-nak létezik inverze, akkor $A + A^2$-nek is létezik inverze.
(g) Ha $A + A^2$-nek létezik inverze, akkor A-nak is létezik inverze.

2.2.3 Melyek igazak az alábbi állítások közül?

(a) Ha A jobb oldali nullosztó és $AB \neq 0$, akkor AB is jobb oldali nullosztó.
(b) Ha AB jobb oldali nullosztó, akkor A és B is jobb oldali nullosztó.
(c) Ha AB jobb oldali nullosztó, akkor A és B közül legalább az egyik jobb oldali nullosztó.
(d) Ha $A+B$ jobb oldali nullosztó, akkor A és B közül legalább az egyik jobb oldali nullosztó.

2.2.4 Az alábbi mátrixok közül melyeknek van inverze és melyek nullosztók? Az invertálhatóknak írjuk fel az inverzét, a nullosztókhoz pedig keressünk „nullosztópárt", azaz olyan nem nulla mátrixot, amellyel megszorozva a nullmátrixot kapjuk.

(a) $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & 2 \\ 3 & 6 \end{pmatrix}$; (c) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 7 & 9 \end{pmatrix}$; (d) $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 4 & 5 \\ 5 & 7 & 8 \end{pmatrix}$.

2.2.5 Hogyan jellemezhetők azok az egész elemű négyzetes mátrixok, amelyeknek az inverze is egész elemű?

2.2.6 Felsőháromszög-mátrixnak egy olyan négyzetes mátrixot nevezünk, amelyben a főátló alatt minden elem 0. Hogyan látszik egyszerűen, hogy egy felsőháromszög-mátrixnak van-e inverze? Igaz-e, hogy egy felsőháromszög-mátrix inverze is ilyen alakú?

2.2.7 Melyek igazak az alábbi állítások közül (A, B adott, X, Y pedig ismeretlen $n \times n$-es mátrixokat jelölnek)?

(a) Ha $\det A \neq 0$, akkor az $AX = B$ mátrixegyenlet megoldható.
(b) Ha $\det A = 0$, akkor $AX = B$ nem oldható meg.
(c) Ha $\det A = 0, \det B \neq 0$, akkor $AX = B$ nem oldható meg.
(d) Ha $\det A = 0, \det B = 0$, akkor $AX = B$ megoldható.
(e) $AX = B$-nek nem lehet egynél több megoldása.
(f) $AX = B$-nek akkor és csak akkor van pontosan egy megoldása, ha $\det A \neq 0$.
(g) Ha $AX = B$ megoldható, akkor $YA = B$ is megoldható.
(h) Ha $AX = B$ és $YA = B$ is egyértelműen megoldható, akkor ezek a megoldások megegyeznek.

2.2.8 Adjunk új megoldást az 1.5.5, 1.5.6 és 1.5.7 feladatokra a determinánsok szorzástételének felhasználásával.

2.2.9 Legyen $n > 1$ páratlan szám, A egy valós elemű $n \times n$-es mátrix, $\det A \neq 0$ és jelölje α_{ij}, illetve A_{ij} a megfelelő elemeket, illetve előjeles aldeterminánsokat. Bizonyítsuk be, hogy $A^2 = E$ akkor és csak akkor teljesül, ha minden i, j-re $\alpha_{ij} = A_{ji}$ vagy minden i, j-re $\alpha_{ij} = -A_{ji}$.

2.2.10 Tegyük fel, hogy $\det A \neq 0$ és készítsük el azt a B mátrixot, amelynek elemei az A megfelelő előjeles aldeterminánsai, azaz $\beta_{ij} = A_{ij}$. Ismételjük meg ugyanezt az eljárást most a B mátrixra. Bizonyítsuk be, hogy így az A mátrix számszorosát (pontosabban, egy T-beli elemmel való szorzatát, azaz *skalár*szorosát) kapjuk. (Az állítás $\det A = 0$ esetén is igaz, lásd a 3.4.17 feladatot.)

2.2.11 Legyen n páros szám, A és B valós elemű $n \times n$-es mátrixok, $\det A \neq 0$, és tegyük fel, hogy $\hat{A} = \hat{B}$. Bizonyítsuk be, hogy $A = B$. Mit állíthatunk (tetszőleges $n > 1$ és) komplex elemű mátrixok esetén?

2.2.12 Bizonyítsuk be, hogy az alábbi típusú 2×2-es valós mátrixok gyűrűt alkotnak a szokásos mátrixműveletekre. Vizsgáljuk meg a kommutativitást, határozzuk meg a bal, jobb, illetve kétoldali egységelemeket, valamint a nullosztókat. Ha van kétoldali egységelem, akkor nézzük meg, mely elemeknek lesz bal, jobb, illetve kétoldali inverze. Mikor kapunk testet? „Ismerősek-e" ezek a testek?

(a) $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$; (b) $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$; (c) $\begin{pmatrix} a & b \\ b & a \end{pmatrix}$;

(d) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$; (e) $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$.

M*2.2.13 Legyen A olyan valós elemű, invertálható mátrix, hogy mind A-ban, mind pedig A^{-1}-ben csupa nemnegatív szám szerepel. Bizonyítsuk be, hogy A minden sorában és minden oszlopában pontosan egy darab nem nulla szám fordul elő.

*2.2.14 Mely n-ekre létezik olyan racionális elemű $n \times n$-es mátrix, amelynek a köbe $2E$, azaz az egységmátrix kétszerese?

*2.2.15 Igazoljuk a determinánsok szorzástételét (2.2.4 Tétel) az alábbi lépésekben. Jelölje az $A, B, AB \in T^{n \times n}$ mátrixok determinánsát rendre D_A, D_B és D_{AB}.

(a) Lássuk be, hogy a $2n \times 2n$-es $\begin{pmatrix} A & 0 \\ -E & B \end{pmatrix}$ mátrix D determinánsa $D_A D_B$ (itt 0 a nullmátrix, E az egységmátrix).

(b) Az első n oszlop megfelelő többszöröseit a második n oszlophoz hozzáadva érjük el, hogy a keletkező mátrix jobb alsó negyede a nullmátrix legyen, így a $\begin{pmatrix} A & AB \\ -E & 0 \end{pmatrix}$ mátrixot kapjuk, amelynek determinánsa $D' = D$.

(c) Mutassuk meg, hogy $D' = D_{AB}$.

(d) Az (a)–(c) részekből következik $D_{AB} = D_A D_B$.

3. LINEÁRIS EGYENLETRENDSZEREK

Az általános lineáris egyenletrendszerek megoldására az egyik legtermészetesebben adódó, egyszerű és gyakorlati szempontból is jól alkalmazható eljárás a Gauss-féle kiküszöbölés, amelynek számos fontos elméleti következménye is van. Speciális egyenletrendszerekre vonatkozik a Cramer-szabály, amely a determinánsok segítségével ad képletet a megoldásra. A jelen fejezetben vezetjük be a lineáris függetlenséget és a mátrix rangját is, amelyek a későbbiekben is alapvető szerepet játszanak. Mindezek egyik alkalmazásaként visszatérünk a négyzetes mátrixok körében az invertálhatóság és a nullosztók kérdésére.

3.1. Gauss-kiküszöbölés

Egy k egyenletből álló n ismeretlenes *lineáris egyenletrendszer* általános alakja

$$\begin{aligned}
\alpha_{11}x_1 + \alpha_{12}x_2 + \ldots + \alpha_{1n}x_n &= \beta_1 \\
\alpha_{21}x_1 + \alpha_{22}x_2 + \ldots + \alpha_{2n}x_n &= \beta_2 \\
&\vdots \\
\alpha_{k1}x_1 + \alpha_{k2}x_2 + \ldots + \alpha_{kn}x_n &= \beta_k
\end{aligned}$$

ahol az α_{ij} együtthatók és a β_i konstansok egy T kommutatív test elemei. Az egyenletek száma (k) és az ismeretlenek száma (n) egymástól függetlenül is tetszőleges lehet (tehát pl. semmiképpen sem szorítkozunk csak a $k = n$ esetre).

Az egyenletrendszer egy *megoldás*án T-beli elemek egy olyan $\gamma_1, \ldots, \gamma_n$ sorozatát értjük, amelyeket a megfelelő x_i-k helyére beírva, valamennyi egyenletben egyenlőség teljesül.

Van olyan egyenletrendszer, amelynek nincs megoldása, van, amelyik egyértelműen oldható meg (azaz pontosan egy megoldása van) és van olyan, amelyet (egynél) több megoldás is kielégít. (Ez utóbbi esetben elég óvatosan fogalmaztunk, annak ellenére, hogy például valós számokra vonatkozó egyenletrendszereknél megszoktuk, hogy egynél több megoldás esetén a megoldásszám végtelen. Látni fogjuk, hogy végtelen test esetén ez valóban mindig így van. Azonban véges, mondjuk t elemű test esetén az összes szóba jövő $x_1, \ldots, x_n$-re is csak t^n lehetőségünk van, tehát eleve nem lehet végtelen sok megoldás.)

Az alábbi kérdésekre keressük a választ: (a) mi a feltétele annak, hogy egy egyenletrendszer megoldható legyen; (b) (megoldhatóság esetén) hány

megoldás van; (c) hogyan lehet az összes megoldást áttekinteni; (d) milyen módszerrel juthatunk el (egy vagy az összes) megoldáshoz.

Ebben a pontban a fenti kérdésekre a *Gauss-féle kiküszöbölés* (röviden *Gauss-kiküszöbölés* vagy latinosan *Gauss-elimináció*) segítségével adjuk meg a választ.

Az eljárás során az alábbi lépéseket fogjuk végezni, amelyek valamennyien az eredetivel ekvivalens egyenletrendszerekhez vezetnek (azaz olyanokhoz, amelyeknek pontosan ugyanazok a megoldásai, mint az eredetinek):

E1. Valamelyik egyenletet egy nullától különböző T-beli elemmel (a továbiakban: *skalár*ral) végigszorozzuk.
E2. Valamelyik egyenlethez egy másik egyenlet skalárszorosát hozzáadjuk.
E3. Két egyenletet felcserélünk.
E4. Az olyan egyenleteket, ahol valamennyi együttható és minden jobb oldali konstans is 0, elhagyjuk.

Ezeket a lépéseket *elemi ekvivalens átalakítások*nak nevezzük.

Az elemi ekvivalens átalakítások segítségével az egyenletrendszerből az alább részletezett módon egymás után ki fogjuk *küszöbölni* az ismeretleneket.

Tegyük fel, hogy $\alpha_{11} \neq 0$. Az első egyenletet osszuk végig α_{11}-gyel (azaz alkalmazzuk E1-et az α_{11} reciprokával), majd minden $i > 1$-re az i-edik egyenletből vonjuk ki az első egyenlet α_{i1}-szeresét. Ezzel a többi egyenletből *kiküszöböl*tük x_1-et.

Tegyük fel, hogy az így kapott egyenletrendszerben az új $\alpha_{22} \neq 0$. Ekkor az előző eljárást megismételhetjük: a második egyenletet végigosztjuk α_{22}-vel, majd minden $i > 2$-re az i-edik egyenletből kivonjuk a második egyenlet α_{i2}-szeresét stb.

Ha valamikor megakadtunk, pl. az előbb $\alpha_{22} = 0$ volt, de mondjuk $\alpha_{52} \neq 0$, akkor a második és az ötödik egyenletet felcseréljük, és így haladunk tovább.

Ha ez sem megy, azaz minden $i \geq 2$ esetén $\alpha_{i2} = 0$, akkor a harmadik ismeretlenre térünk át, vagyis α_{23}-at vizsgáljuk stb.

Nemsokára néhány konkrét példán keresztül illusztráljuk, hogyan fest mindez a gyakorlatban és hogyan juthatunk el így az egyenletrendszer megoldásához. Előtte azonban érdemes némi technikai egyszerűsítést bevezetni.

Vegyük észre, hogy a fenti lépések nyomon követéséhez elég csak az együtthatók és a jobb oldali konstansok változását figyelni, az x_i, + és = „jeleket" fölösleges mindig újra leírni. Ezért az egyenletrendszert egyszerűbben jellemezhetjük mátrixok segítségével: az α_{ij} együtthatókból képezett $k \times n$-es A mátrixot az egyenletrendszer *együtthatómátrix*ának nevezzük, a jobb oldali konstansokkal kibővített $k \times (n+1)$-es mátrixot pedig az egyenletrendszer

*kibővített mátrix*ának nevezzük és $A|\mathbf{b}$-vel jelöljük, azaz

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix}, \qquad A|\mathbf{b} = \left(\begin{array}{cccc|c} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} & \beta_1 \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} & \beta_2 \\ \vdots & & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} & \beta_k \end{array}\right).$$

A kibővített mátrixban az együtthatók alkotta rész és a jobb oldali konstansok közé iktatott függőleges vonallal jelezzük, hogy a kétféle típusú elemek eltérő szerepet játszanak az egyenletrendszerben. (Az $A|\mathbf{b}$ felírásnál $\mathbf{b}$ a jobb oldalon álló β_i konstansokból képezett „vektort" jelöli, erről bővebben ennek a pontnak a végén lesz szó.)

Azonnal adódik, hogy az egyenletekkel végzett E1–E4 elemi ekvivalens átalakításoknak a kibővített mátrixnál a sorokkal végzett hasonló változtatások felelnek meg:

M1. Valamelyik sort egy nullától különböző skalárral végigszorozzuk.
M2. Valamelyik sorhoz egy másik sor skalárszorosát hozzáadjuk.
M3. Két sort felcserélünk.
M4. A csupa 0-ból álló sorokat elhagyjuk.

A kibővített mátrixon végzett fenti lépéseket *elemi sorekvivalens átalakítások*nak nevezzük.

(Az ekvivalens lépések „visszacsinálhatósága" érdekében formailag teljesebb, ha E4-nél, illetve M4-nél az ilyen egyenletek, illetve sorok hozzávételét is megengedjük, de ennek gyakorlati alkalmazására nyilván sosincs szükség.)

Most három, valós számokra vonatkozó egyenletrendszeren mutatjuk be a kiküszöbölési eljárást.

P1 példa:

$$\begin{aligned} x_1 + 2x_2 &= 3 \\ 4x_1 + 5x_2 &= 6 \\ 7x_1 + 8x_2 &= 9 \end{aligned}$$

Ennek kibővített mátrixa $\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{array}\right)$. A jelzett kiküszöbölési eljárásnak megfelelően vonjuk ki a második sorból az első sor 4-szeresét, a harmadik sorból pedig az első sor 7-szeresét. Így az $\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{array}\right)$ mátrixhoz jutunk. Osszuk el a második sort -3-mal, majd adjuk hozzá ennek 6-szorosát

a harmadik sorhoz. Az így kapott mátrix $\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{array}\right)$. Itt a csupa nulla sor elhagyható, tehát marad az $\left(\begin{array}{cc|c} 1 & 2 & 3 \\ 0 & 1 & 2 \end{array}\right)$ mátrix. Itt a második sorból azonnal leolvasható, hogy $x_2 = 2$ (hiszen x_2 „ki van fejezve"). Ezt visszahelyettesíthetjük az első sornak megfelelő egyenletbe: $x_1 + 2x_2 = x_1 + 2 \cdot 2 = 3$, tehát $x_1 = -1$. Azonban ez a lépés is „automatizálható". Ha a legutolsó mátrixnál az első sor második elemét kiejtjük, akkor x_1 is „ki lesz fejezve". Vonjuk ki ezért az első sorból a második sor 2-szeresét, ekkor az $\left(\begin{array}{cc|c} 1 & 0 & -1 \\ 0 & 1 & 2 \end{array}\right)$ mátrixot kapjuk, ahonnan valóban $x_1 = -1$ is közvetlenül leolvasható.

Az egyenletrendszernek tehát egyetlen megoldása van: $x_1 = -1, x_2 = 2$.

P2 példa:

$$\begin{aligned} x_1 + x_2 + 2x_3 &= 3 \\ 4x_1 + 4x_2 + 5x_3 &= 6 \\ 7x_1 + 7x_2 + 8x_3 &= 10 \end{aligned}$$

A kiküszöbölés során a kibővített mátrix a következőképpen változik:

$$\left(\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 4 & 4 & 5 & 6 \\ 7 & 7 & 8 & 10 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 0 & 0 & -3 & -6 \\ 0 & 0 & -6 & -11 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 1 \end{array}\right).$$

Mivel az utolsó mátrix harmadik sora a lehetetlen $0x_1 + 0x_2 + 0x_3 = 1$ egyenletnek felel meg, ezért ennek az egyenletrendszernek nincs megoldása.

P3 példa:

$$\begin{aligned} x_1 + 2x_2 + 3x_3 &= 4 \\ 5x_1 + 6x_2 + 7x_3 &= 8 \\ 9x_1 + 10x_2 + 11x_3 &= 12 \\ 13x_1 + 14x_2 + 15x_3 &= 16 \end{aligned}$$

Most a következőképpen alakul a kiküszöbölés:

$$\left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \\ 13 & 14 & 15 & 16 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & -4 & -8 & -12 \\ 0 & -8 & -16 & -24 \\ 0 & -12 & -24 & -36 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{array}\right) \sim$$

$$\sim \left(\begin{array}{ccc|c} 1 & 2 & 3 & 4 \\ 0 & 1 & 2 & 3 \end{array}\right) \sim \left(\begin{array}{ccc|c} 1 & 0 & -1 & -2 \\ 0 & 1 & 2 & 3 \end{array}\right).$$

Itt x_3-ra semmilyen megkötés sem adódott, annak értéke tetszőlegesen megválasztható. Ha x_3 értékét már rögzítettük, akkor ennek segítségével a másik két ismeretlen már egyértelműen kifejezhető: $x_1 = -2 + x_3, x_2 = 3 - 2x_3$. Az egyenletrendszer összes megoldása tehát $x_1 = -2 + \nu, x_2 = 3 - 2\nu, x_3 = \nu$, ahol ν tetszőleges (valós szám).

A fenti példákból világosan látszik az általános eljárás. A „felülről lefelé" történő lépegetésnél végül egy olyan mátrixhoz jutunk, amelyben az első sort kivéve minden sor nullákkal kezdődik, az első valahány sorban az első nem nulla elem mindig 1-es (az ún. *vezéregyes*), ezek csupa különböző oszlopban, lépcsőzetesen lefelé és jobbra helyezkednek el, a vezéregyesek alatt pedig minden elem 0. Lehetnek ezen kívül olyan sorok is, amelyekben az együtthatómátrixnak megfelelő rész csupa nulla. Ezt *lépcsős alak*nak hívjuk. Lépcsős alakok például

$$\text{P4: } \left(\begin{array}{ccc|c} 1 & 2 & 3 & 6 \\ 0 & 1 & 7 & 3 \\ 0 & 0 & 1 & 5 \\ 0 & 0 & 0 & 0 \end{array}\right), \quad \text{P5: } \left(\begin{array}{cc|c} 1 & 2 & 2 \\ 0 & 1 & 3 \\ 0 & 0 & 2 \end{array}\right), \quad \text{P6: } \left(\begin{array}{ccccc|c} 1 & 2 & 3 & 5 & 6 & 7 \\ 0 & 0 & 1 & 2 & 3 & 4 \\ 0 & 0 & 0 & 1 & 2 & 3 \end{array}\right).$$

A P5 példánál a harmadik sor ellentmondást jelent, ezért a P5-höz tartozó egyenletrendszernek nincs megoldása. A P4 példa esetén a mátrix (csupa nulla) negyedik sora el is hagyható.

A lépcsős alakból most a vezéregyesek fölötti elemeket is kinullázhatjuk, ha alulról felfelé haladva az egyes sorokból a vezéregyes sorának megfelelő többszörösét levonjuk. A P4 és P6 példáknál ekkor az alábbi mátrixok adódnak:

$$\text{P4-nél: } \left(\begin{array}{ccc|c} 1 & 0 & 0 & 55 \\ 0 & 1 & 0 & -32 \\ 0 & 0 & 1 & 5 \end{array}\right), \qquad \text{P6-nál: } \left(\begin{array}{ccccc|c} 1 & 2 & 0 & 0 & -1 & -2 \\ 0 & 0 & 1 & 0 & -1 & -2 \\ 0 & 0 & 0 & 1 & 2 & 3 \end{array}\right).$$

Az ilyen alakot *redukált lépcsős alak*nak (a továbbiakban RLA) hívjuk. Ebben tehát az első sor kivételével minden sor nullákkal kezdődik, az első valahány sorban az első nem nulla elem egy-egy *vezéregyes*, ezek csupa különböző oszlopban, lépcsőzetesen lefelé és jobbra helyezkednek el, a vezéregyesek alatt és fölött pedig minden elem 0. Az esetleges további sorokban az együtthatómátrixnak megfelelő rész csupa nullából áll.

Az RLA-ból kényelmesen leolvashatjuk az egyenletrendszer összes megoldását. A P4-nek megfelelő egyenletrendszernél $x_1 = 55, x_2 = -32, x_3 = 5$, a P6 esetén pedig $x_1 = -2 + \nu - 2\mu, x_2 = \mu, x_3 = -2 + \nu, x_4 = 3 - 2\nu, x_5 = \nu$,

ahol ν és μ tetszőleges valós számok. Általában is megtudhatjuk, hogy az egyenletrendszer megoldható-e, ha igen, akkor mennyi a megoldásszám, és hogyan kapjuk meg az összes megoldást.

Az egyenletrendszer akkor és csak akkor *megoldható*, ha az RLA-ban nem fordul elő olyan sor, amelyben az együtthatóknak megfelelő rész csupa 0, a jobb oldali rész pedig nem 0 (a továbbiakban ezt *tilos sor*nak hívjuk). (A tilos sor léte már a lépcsős alaknál is kiderül, amelyet ekkor persze fölösleges tovább redukálni.)

A megoldás akkor és csak akkor *egyértelmű*, ha (nincs tilos sor és) minden oszlopban áll vezéregyes, azaz a vezéregyesek száma megegyezik az ismeretlenek számával. FONTOS! Ennek semmi köze sincs az olyan csupa nulla sorok létéhez vagy nemlétéhez, amelyeknek a jobb oldali része is nulla (nevezzük ezeket *fölösleges sor*oknak). Egy fölösleges sor csak azt jelenti, hogy az annak megfelelő egyenlet következik a többiből, tehát nem tartalmaz új információt, új megkötést, és így az ilyen sorok elhagyhatók. (Ilyen volt a P1 példánál a harmadik egyenlet, a P3 példánál pedig a harmadik és a negyedik egyenlet is.) Bármely egyenletrendszerhez hozzávehetünk fölösleges egyenleteket, például valamelyik egyenletet újra leírjuk, vagy két egyenlet összegét is beiktatjuk, és így fölösleges sor fog adódni; az egyenletrendszer megoldásai természetesen nem változtak meg, akár egyértelmű volt a megoldás, akár több megoldás volt, akár pedig nem volt megoldás.

Ha az egyenletrendszer megoldása egyértelmű, akkor az RLA azonnal megadja a megoldást. Ha a megoldás nem egyértelmű, akkor a vezéregyest nem tartalmazó oszlopoknak megfelelő ismeretlenek tetszőlegesen választhatók (azaz *szabad paraméterek*), a többi ismeretlen pedig ezekkel egyértelműen kifejezhető. (A P3 példában x_3 volt szabad paraméter, a P6-nak megfelelő egyenletrendszerben pedig x_2 és x_5.) A megoldásszám így végtelen test esetén végtelen, t elemű test esetén pedig t^s, ahol s a szabad paraméterek száma.

Mindezt röviden az alábbi tételben foglalhatjuk össze:

3.1.1 Tétel

I. Egy lineáris egyenletrendszer kibővített mátrixa elemi sorekvivalens átalakításokkal redukált lépcsős alakra hozható.

II. Az egyenletrendszer akkor és csak akkor oldható meg, ha a (redukált) lépcsős alakban nincs tilos sor.

III. Az egyenletrendszernek akkor és csak akkor egyértelmű a megoldása, ha (nincs tilos sor és) a vezéregyesek száma megegyezik az ismeretlenek számával.

IV. Ha több megoldás van, akkor a vezéregyest nem tartalmazó oszlopoknak megfelelő ismeretlenek szabad paraméterek (tetszőlegesen megválaszthatók), a többi ismeretlen pedig ezekkel egyértelműen kifejezhető. A megoldásszám ekkor végtelen test esetén végtelen, t elemű test esetén pedig t^s, ahol s a szabad paraméterek száma, és a(z összes) megoldás közvetlenül leolvasható a redukált lépcsős alakból. ♣

Megjegyezzük, hogy több megoldás esetén általában nemcsak egyféle paraméterezés lehetséges. A P3 példánál x_1 vagy x_2 is lehet szabad paraméter, ekkor a megoldásokat $x_1 = \mu, x_2 = -1 - 2\mu, x_3 = \mu + 2$, illetve $x_1 = -1/2 - \tau/2, x_2 = \tau, x_3 = 3/2 - \tau/2$ alakban kapjuk meg. Ezekhez is eljuthatunk a Gauss-eliminációval, de ehhez előbb az ismeretlenek sorrendjét alkalmasan meg kell változtatnunk (x_1-et, illetve x_2-t kell harmadikként írnunk). Az egyenletrendszer megoldásainak áttekintésére természetesen már egyféle paraméterezés is elegendő, ezért — a keveredések elkerülése érdekében — a legjobb, ha az ismeretleneket nem csereberéljük és az eredeti formában végezzük a kiküszöbölést. FIGYELEM! Az nem igaz, hogy s szabad paraméter esetén *bármelyik* s darab ismeretlen választható szabad paraméternek. Például az $x_1 + 2x_2 + 3x_3 = 1$, $x_1 + 2x_2 + 4x_3 = 1$ egyenletrendszernél x_3 értéke egyértelműen meghatározott, $x_3 = 0$, és csak a másik két ismeretlen vehető szabad paraméternek (a megoldások ekkor $x_1 = \nu, x_2 = 1/2 - \nu/2, x_3 = 0$, illetve $x_1 = 1 - 2\mu, x_2 = \mu, x_3 = 0$ alakban írhatók fel).

Néhány jótanács. A Gauss-kiküszöbölésnél is érdemes — a determinánsoknál látottakhoz hasonlóan — az egyes lépéseket gondosan regisztrálni és minél részletesebben kiírni.

Ne felejtsük el, hogy az eljárás során végig csak *sor*okkal dolgozunk. Alapszabály, hogy az oszlopokkal ne próbáljunk hasonlóképpen manipulálni, ekkor ugyanis nem az egyenleteket, hanem az ismeretleneket variálnánk. Például két oszlop cseréje a megfelelő két ismeretlen cseréjét jelenti, és így végig nyomon kell(enne) követni az ismeretlenek sorrendjének a megváltozásait is. A bonyolultabb átalakítások pedig már szinte áttekinthetetlen módon hoznak be új ismeretleneket a régiek helyett.

A (redukált) lépcsős alakra hozás nagyon hasznos eljárás az egyenletrendszer megoldására, de nem öncél. Ha más, egyszerűbb módon meg tudjuk oldani az egyenletrendszert, akkor nincsen rá szükség. Ne felejtsük azonban el, hogy egyetlen megoldás megtalálása általában még nem jelenti a teljes megoldást, tehát emellett valamilyen módon meg kell keresni a többi megoldást is, vagy pedig ki kell mutatni, hogy az egyenletrendszernek csak egy megoldása van.

FIGYELEM! Ne próbáljunk az egyenletrendszer megoldhatóságára vagy megoldásszámára pusztán az egyenletek és ismeretlenek számának a viszonyá-

ból következtetni. NAGYON ROSSZ „vezérelv", hogy „ha ugyanannyi ismeretlen van, mint egyenlet, akkor egyértelmű a megoldás, ha az ismeretlenek száma a nagyobb, akkor több megoldás van, ha pedig az egyenleteké a nagyobb, akkor nincs megoldás". Ez több szempontból is hibás okoskodás. Egyrészt — ahogy már korábban említettük — bármely egyenletrendszerhez hozzávehetünk új megkötést nem hordozó „fölösleges egyenleteket", ezzel az egyenletek száma megváltozik, ugyanakkor az ismeretlenek száma és a megoldások száma is változatlan marad. Másrészt akármilyen sok ismeretlen ellenére már két egyenlettel is tudunk megoldhatatatlanságot produkálni, ha például ugyanazokat az együtthatókat vesszük, de más jobb oldalt. (Tulajdonképpen már egy egyenlet is elég, ha minden együttható 0, de a jobb oldal nem az. Akik ezt „degenerált" példának találják, ne felejtsék el, hogy ez nem más, mint a tilos sor, amely minden megoldhatatlan egyenletrendszernél jelentkezik, csak esetleg rejtettebb formában, amit csak a kiküszöbölés hoz napvilágra.) A P1 és P3 példában több egyenlet volt, mint ismeretlen, mégis az egyiknek egyértelmű megoldása volt, a másiknak pedig végtelen sok! A P2 példában az egyenletek és az ismeretlenek száma megegyezett, mégsem volt megoldható stb. Az ismeretlenek és egyenletek számának viszonya szinte egyáltalán nincs hatással arra, hogy a megoldások száma 0, 1 vagy több; az egyetlen kivétel, hogy ha több ismeretlen van, mint egyenlet, akkor nem lehet egyértelmű megoldás (vigyázat, az nyugodtan lehet, hogy nincs megoldás!):

3.1.2 Tétel

Ha egy k egyenletből álló n ismeretlenes lineáris egyenletrendszernek egyetlen megoldása van, akkor $n \leq k$. ♣

Bizonyítás: Egyértelmű megoldás esetén az RLA-ban a vezéregyesek száma n, másrészt a vezéregyesek különböző sorokban helyezkednek el, tehát számuk legfeljebb k. Innen valóban $n \leq k$. ■

Ennek az észrevételnek egy egyszerű, de fontos következményét a későbbiekben sokszor fel fogjuk használni. Ehhez előbb bevezetjük a homogén lineáris egyenletrendszer fogalmát:

3.1.3 Definíció

Egy lineáris egyenletrendszert *homogén*nek nevezünk, ha a jobb oldali konstansok mindegyike nulla. ♣

Egy homogén egyenletrendszer biztosan megoldható, hiszen $x_1 = \ldots = x_n = 0$ mindig megoldás. Ezt *triviális megoldás*nak nevezzük. Így itt az

az érdekes kérdés, hogy mikor létezik nem triviális megoldás. Erre elégséges feltételt ad az alábbi

3.1.4 Tétel

Ha egy homogén lineáris egyenletrendszerben az ismeretlenek száma nagyobb, mint az egyenletek száma, akkor az egyenletrendszernek biztosan létezik nem triviális megoldása. ♣

Bizonyítás: Indirekt, tegyük fel, hogy a triviálison kívül nincs más megoldás. Ekkor az egyenletrendszernek egyetlen megoldása van, tehát a 3.1.2 Tétel szerint az ismeretlenek száma nem lehet nagyobb az egyenletek számánál, ami ellentmond a feltételnek. ■

A továbbiak előkészületeként az egyenletrendszerek két másik felírási módjával ismerkedünk meg. Ehhez szükségünk lesz az (oszlop)vektorok fogalmára.

3.1.5 Definíció

Az egy oszlopból álló mátrixokat *oszlopvektor*oknak nevezzük. Egy ilyen mátrix (egyetlen oszlopának) elemeit a vektor *komponensei*nek vagy *koordinátái*nak hívjuk. A T test elemeiből képzett q komponensű vektorok összességét ($T^{q\times 1}$ helyett röviden) T^q-val jelöljük. ♣

Ez a fogalom a sík-, illetve térvektorok (valós) számpárokként, illetve számhármasokként történő felírási módjának az általánosítása. Később még sokkal általánosabb értelemben fogjuk használni a „vektor” szót (lásd a 4.1 pontot).

T^q-ban — az általános mátrixműveleteknek megfelelően — beszélhetünk két vektor összegéről, illetve egy vektor skalárszorosáról (azaz T-beli elemmel vett szorzatáról), ezeket úgy kapjuk, hogy a megfelelő komponenseket összeadjuk, illetve a komponenseket a skalárral végigszorozzuk.

A vektorokat félkövér latin kisbetűkkel fogjuk jelölni.

Most rátérünk az egyenletrendszer egyik átírási módjára. Legyen

$$A = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & & & \\ \alpha_{k1} & \alpha_{k2} & \dots & \alpha_{kn} \end{pmatrix} \in T^{k\times n},$$

$$\mathbf{x} = \begin{pmatrix} x_1 \\ x_2 \\ \\ \vdots \\ \\ x_n \end{pmatrix} \in T^n, \qquad \mathbf{b} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \vdots \\ \beta_k \end{pmatrix} \in T^k,$$

azaz A az együtthatómátrix, $\mathbf{x}$ az ismeretlenekből képezett vektor és a (már említett) $\mathbf{b}$ a jobb oldali konstansokból álló vektor. Ekkor a mátrixszorzás definíciójának megfelelően az egyenletrendszer felírható $A\mathbf{x} = \mathbf{b}$ alakban.

A másik átírási módhoz legyen

$$\mathbf{a}_j = \begin{pmatrix} \alpha_{1j} \\ \alpha_{2j} \\ \vdots \\ \alpha_{kj} \end{pmatrix} \in T^k\,, \quad j = 1, 2, \ldots, n,$$

tehát az $\mathbf{a}_j$-k az A együtthatómátrix oszlopvektorai. Ekkor az egyenletrendszer a következőképpen írható fel: $x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \ldots + x_n\mathbf{a}_n = \mathbf{b}$.

Feladatok

3.1.1 Mutassuk meg, hogy az (56. oldalon szereplő) E1–E4 elemi ekvivalens átalakítások valóban az eredetivel ekvivalens egyenletrendszerhez vezetnek.

3.1.2 Legyen T a valós test. Az alábbi változtatások közül melyek vezetnek az eredetivel ekvivalens egyenletrendszerhez?

(a) Az első egyenlet helyére az összes egyenlet összegét írjuk.

(b) Az első egyenlet helyére az összes többi egyenlet összegét írjuk.

(c) Az első két egyenlet helyére az összes egyenlet összegét írjuk.

(d) Az első két egyenlet helyére ezek összegét és különbségét írjuk.

(e) Minden egyenletben minden együtthatóhoz és a jobb oldali konstansokhoz is 1-et hozzáadunk.

Mennyiben módosul(hat)nak a válaszok, ha $\mathbf{R}$ helyett más T test feletti egyenletrendszereket vizsgálunk?

3.1.3 Oldjuk meg a valós számok körében az alábbi egyenletrendszereket.

(a) $\begin{aligned} -x+3y+3z &= 2 \\ 3x+y+z &= 4 \\ 2x-2y+3z &= 10 \end{aligned}$ (b) $\begin{aligned} 2x+3y+z &= 11 \\ x-y-2z &= -7 \\ 3x+2y-z &= 2 \end{aligned}$ (c) $\begin{aligned} 2x+3y+z &= 11 \\ x-y-2z &= -7 \\ 3x+2y-z &= 4 \end{aligned}$

3.1.4 Hány megoldása van a modulo 5 maradékosztályok teste felett az alábbi egyenletrendszernek?

$$\begin{aligned} x_1+x_2+x_3 &= 1 \\ x_3+x_4+x_5 &= 4 \\ x_1+x_3+x_4 &= 2 \\ x_2+x_3+x_5 &= 3 \end{aligned}$$

3.1.5 Oldjuk meg a komplex számok körében a következő egyenletrendszereket.

(a) $\begin{aligned} x_1+ix_2-x_3 &= -i \\ ix_1-x_2-ix_3 &= 1 \\ -x_1-ix_2+x_3 &= i \\ -ix_1+x_2+ix_3 &= -1 \\ x_1+ix_2+x_3 &= i \end{aligned}$ (b) $\begin{aligned} x_1+x_2+x_3+x_4+x_5 &= 0 \\ x_1+ix_2+x_3+x_4+x_5 &= -1+i \\ x_1+x_2+ix_3+x_4+x_5 &= -1-i \\ x_1+x_2+x_3+ix_4+x_5 &= 1-i \\ x_1+x_2+x_3+x_4+ix_5 &= 1+i \end{aligned}$

3.1.6 Oldjuk meg a valós számok körében:

$$x_1+x_2=1, \qquad x_2+x_3=1, \qquad \ldots, \qquad x_n+x_1=1\,.$$

*3.1.7 Milyen n és m esetén lesz az alábbi ($n \times n$-es) valós egyenletrendszernek egyértelmű megoldása?

$$\begin{aligned} x_1+x_2+\ldots+x_m &= 1 \\ x_2+x_3+\ldots+x_{m+1} &= 1 \\ &\vdots \\ x_n+x_1+\ldots+x_{m-1} &= 1 \end{aligned}$$

3.1.8 Legyen $n > 1$, és oldjuk meg az alábbi n ismeretlenes és n egyenletből álló valós egyenletrendszert:

$$\begin{aligned}
x_1 + \ x_2 + \ x_3 + \ \ldots \ + \ x_n &= \ n \\
x_1 + 2x_2 + 2x_3 + \ \ldots \ + 2x_n &= n - 1 \\
x_1 + 2x_2 + 3x_3 + \ \ldots \ + 3x_n &= n - 2 \\
\vdots \quad \vdots \quad \vdots \quad \ddots \quad \vdots \quad \vdots \\
x_1 + 2x_2 + 3x_3 + \ \ldots \ + nx_n &= \ 1
\end{aligned}$$

vagyis az A együtthatómátrixban $\alpha_{ij} = \min(i, j)$.

3.1.9 Legyen $k, n > 2$ és p egy kn-nél nagyobb prímszám. A $k \times n$-es A mátrixot úgy képezzük, hogy sorban leírjuk 1-től kn-ig a számokat, tehát $\alpha_{ij} = (i-1)n + j$. Tekintsük az $A\mathbf{x} = \mathbf{b}$ egyenletrendszert a modulo p test felett.

(a) Megoldhatóság esetén hány megoldás van?
(b) Hány $\mathbf{b}$-re lesz az egyenletrendszer megoldható?

3.1.10 Adjunk példát olyan 3 ismeretlenes és 5 egyenletből álló egyenletrendszerre, melynek (a) nincs megoldása; (b) egyértelmű megoldása van; (c) végtelen sok megoldása van; (d) pontosan 7 megoldása van. Mi a helyzet 5 ismeretlen és 3 egyenlet esetén?

3.1.11 Milyen kapcsolat van a vezéregyesek, a szabad paraméterek és az ismeretlenek száma között?

3.1.12 Legyen T egy t elemszámú véges test, $n > k$ és tekintsünk T felett egy k egyenletből álló n ismeretlenes egyenletrendszert. Bizonyítsuk be, hogy megoldhatóság esetén a megoldásszám legalább t^{n-k}.

3.1.13 Tegyük fel, hogy egy (tetszőleges T test feletti) egyenletrendszernek egynél több megoldása van, és tekintsük a megoldásokban előforduló összes lehetséges x_1 értékek H halmazát. Bizonyítsuk be, hogy H vagy egyelemű, vagy pedig $H = T$.

3.1.14 Hogyan ábrázolhatjuk geometriailag a valós együtthatós kétismeretlenes (és akárhány egyenletből álló) egyenletrendszereket? Hogyan látszik a megoldhatóság és a megoldásszám? Mi a helyzet három ismeretlen esetén?

3.1.15 Legyen az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer egy megoldása $\mathbf{x}'$. Mutassuk meg, hogy az összes megoldást az $\mathbf{x}' + \mathbf{x}^*$ képlettel kapjuk, ahol $\mathbf{x}^*$ végigfut az $A\mathbf{x} = \mathbf{0}$ homogén egyenletrendszer összes megoldásán.

3.1.16 Legyen $A, A_i \in T^{k\times n}$, $\mathbf{x} \in T^n$, $\mathbf{b}, \mathbf{b}_i \in T^k$, és tekintsük az $A\mathbf{x} = \mathbf{b}$, $A_1\mathbf{x} = \mathbf{b}$ stb. egyenletrendszereket. Melyek igazak az alábbi állítások közül?

(a) Ha $A\mathbf{x} = \mathbf{b}_1$ és $A\mathbf{x} = \mathbf{b}_2$ megoldható, akkor $A\mathbf{x} = \mathbf{b}_1 + \mathbf{b}_2$ is megoldható.

(b) Ha $A_1\mathbf{x} = \mathbf{b}$ és $A_2\mathbf{x} = \mathbf{b}$ megoldható, akkor $(A_1 + A_2)\mathbf{x} = \mathbf{b}$ is megoldható.

(c) Ha $A\mathbf{x} = \mathbf{b}$-nek egyértelmű a megoldása, akkor $A\mathbf{x} = \mathbf{b}_1$-nek semmilyen $\mathbf{b}_1$-re sem lehet egynél több megoldása.

(d) Ha $A\mathbf{x} = \mathbf{b}$-nek egyértelmű a megoldása, akkor $A\mathbf{x} = \mathbf{b}_1$ is biztosan megoldható bármely $\mathbf{b}_1$-re.

(e) Ha $k < n$, akkor tetszőleges A-hoz van olyan $\mathbf{b}$, amelyre $A\mathbf{x} = \mathbf{b}$ nem oldható meg.

(f) Ha $k > n$, akkor tetszőleges A-hoz van olyan $\mathbf{b}$, amelyre $A\mathbf{x} = \mathbf{b}$ nem oldható meg.

M 3.1.17 Ábel és Béla (egymástól függetlenül) gondol 5–5 egész számot. Ábel a Béla által gondolt számok közül megkérdezheti bármely 2 összegének a paritását, Béla pedig Ábel számai közül bármely 3 összegének a paritását tudakolhatja meg. Ki tudja-e találni valamelyikük a másik által gondolt számok mindegyikének a paritását, és ha igen, akkor minimálisan hány kérdéssel tudja ezt megtenni?

3.1.18 Tekintsünk egy egész együtthatós lineáris egyenletrendszert (a jobb oldalon álló konstansok is egész számok). Melyek igazak az alábbi állítások közül?

(a) Ha van megoldás az egész számok körében, akkor van megoldás a komplex számok körében is.

(b) Ha van megoldás a komplex számok körében, akkor van megoldás a racionális számok körében is.

(c) Ha van megoldás a racionális számok körében, akkor van megoldás az egész számok körében is.

3.1.19 Ha egy egyenletrendszerben az együtthatók (beleértve a jobb oldalon álló konstansokat is) egész számok, akkor ezeket a modulo 11 maradékosztályok elemeinek is képzelhetjük, és ekkor a modulo 11 test feletti egyenletrendszerhez jutunk. Tekintsünk egy ilyen homogén egyenletrendszert. Melyek igazak az alábbi állítások közül?

(a) Ha van nem triviális megoldás a modulo 11 test felett, akkor nem triviális racionális megoldás is van.

(b) Ha van nem triviális racionális megoldás, akkor a modulo 11 test felett is van nem triviális megoldás.

3.2. Cramer-szabály

Ebben a pontban olyan speciális egyenletrendszerekről lesz szó, amelyekben megegyezik az ismeretlenek és az egyenletek száma. Az együtthatómátrix ekkor négyzetes, és így létezik determinánsa. Először megmutatjuk, hogy ha ez a determináns nem nulla, akkor az egyenletrendszernek bármilyen jobb oldal mellett pontosan egy megoldása van, és erre a megoldásra determinánsok segítségével képletet is adunk:

3.2.1 Tétel (Cramer-szabály)
Ha $A \in T^{n\times n}$ és $D = \det A \neq 0$, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek pontosan egy megoldása van. A megoldásban $x_j = D_j/D$, ahol a D_j determinánst úgy kapjuk, hogy D-ben a j-edik oszlop helyére a jobb oldali konstansokat (azaz a $\mathbf{b}$ vektor komponenseit) írjuk. ♣

Például

$$x_2 = \frac{\begin{vmatrix} \alpha_{11} & \beta_1 & \dots & \alpha_{1n} \\ \alpha_{21} & \beta_2 & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \beta_n & \dots & \alpha_{nn} \end{vmatrix}}{\begin{vmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{vmatrix}}$$

Bizonyítás: Mivel a feltétel szerint létezik A^{-1}, ezért az $A\mathbf{x} = \mathbf{b}$ egyenletrendszert balról A^{-1}-gyel beszorozva *ekvivalens* egyenletrendszert nyerünk. (Az ekvivalenciát az biztosítja, hogy a kapott egyenletrendszert balról A-val beszorozva ismét az eredeti egyenletrendszerhez jutunk vissza — közben természetesen többször kihasználtuk a mátrixszorzás tulajdonságait.) Így az $\mathbf{x} = A^{-1}\mathbf{b}$ egyenletrendszer keletkezett, ami „már meg is van oldva". Ezzel igazoltuk, hogy az eredeti egyenletrendszernek pontosan (ez az) egy megoldása van.

Hátra van még, hogy az $\mathbf{x} = A^{-1}\mathbf{b}$ megoldást a kívánt alakra hozzuk. A mátrixszorzás szabályai szerint x_j éppen az A^{-1} mátrix j-edik sorának és a $\mathbf{b}$ vektornak a szorzata. Felhasználva a mátrix inverzére a 2.2.2 Tétel bizonyításában adott képletet, így $x_j = (1/D)(A_{1j}\beta_1 + \ldots + A_{nj}\beta_n)$, ahol A_{lm} a D determináns megfelelő előjeles aldeterminánsait jelöli. Mivel a D_j determináns csak a j-edik oszlopában tér el D-től, ezért a j-edik oszlophoz tartozó megfelelő előjeles aldeterminánsok D-ben és D_j-ben azonosak. Ennélfogva

D_j-t a j-edik oszlopa szerint kifejtve $D_j = \beta_1 A_{1j} + \ldots + \beta_n A_{nj}$ adódik, tehát x_j valóban átírható $x_j = D_j/D$ alakba. ■

A Cramer-szabálynak elsősorban elméleti jelentősége van. Az egyenletrendszerek gyakorlati megoldásánál csak ritkán használjuk, hiszen egyrészt eleve csak igen speciális esetekben alkalmazható, másrészt még ekkor is általában jóval több számolást igényel, mint a Gauss-kiküszöbölés (gondoljuk meg, hogy a teljes eredményt adó Gauss-kiküszöbölés ebben az esetben alig tart tovább, mint egyetlen n-edrendű determinánsnak a kiszámítása, a Cramer-szabályhoz pedig $n+1$ darab ilyen determinánst kell kiszámítani).

Természetesen érdemes a Cramer-szabályra támaszkodni, ha a D és D_j determinánsok egyszerűen meghatározhatók. Hasznát vehetjük akkor is, ha „észreveszünk" egy megoldást és kimutatjuk, hogy $D \neq 0$; ekkor ugyanis a fenti tételből tudjuk, hogy a (ki)talált megoldáson kívül több megoldás nem is lehet.

A Cramer-szabály történeti (és középiskolai tanítási) szempontból is érdekes. Ha az $\alpha_{11}x_1 + \alpha_{12}x_2 = \beta_1$, $\alpha_{21}x_1 + \alpha_{22}x_2 = \beta_2$ általános 2 ismeretlenes és 2 egyenletből álló (mondjuk valós) egyenletrendszert (akármilyen módszerrel) megoldjuk, akkor könnyen adódik, hogy (pontosan) akkor van egyértelmű megoldás, ha $\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21} \neq 0$, és ekkor

$$x_1 = \frac{\beta_1\alpha_{22} - \beta_2\alpha_{12}}{\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}}\,, \qquad x_2 = \frac{-\beta_1\alpha_{21} + \beta_2\alpha_{11}}{\alpha_{11}\alpha_{22} - \alpha_{12}\alpha_{21}}\,.$$

Vegyük észre, hogy ez éppen a Cramer-szabály az $n = 2$ esetben. Némi fáradsággal még $n = 3$-ra is kihozhatjuk „kisipari módszerekkel" a megfelelő eredményt. Éppen az ilyen típusú észrevételek indították el a determinánsfogalom kialakulását és alkalmazását a lineáris egyenletrendszerek megoldására.

A Cramer-szabálynál nagyon fontos feltétel, hogy az együtthatómátrix determinánsa ne legyen nulla. Az x_j-re felírt képlet $D = 0$ esetén persze eleve értelmetlen, azonban ennél több is igaz; ha $D = 0$, akkor az egyenletrendszernek semmiképpen sem lehet egyértelmű megoldása:

3.2.2 Tétel

Ha $A \in T^{n\times n}$ és $D = \det A = 0$, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer vagy nem oldható meg, vagy pedig egynél több megoldása van. ♣

Bizonyítás: Végezzünk Gauss-kiküszöbölést az $A\mathbf{x} = \mathbf{b}$ egyenletrendszerrel, de most a(z esetleg keletkező) csupa nulla sorokat ne hagyjuk el. Ekkor az elemi ekvivalens átalakítások során kapott együtthatómátrixok determinánsa — a determinánsokra vonatkozó elemi tulajdonságok szerint — továbbra is

nulla marad. Így az RLA bal oldalának a determinánsa is nulla. Ha az egyenletrendszernek egyértelmű lenne a megoldása, akkor minden oszlopba kerülne vezéregyes, de ekkor az RLA bal oldala az egységmátrix lenne, amelynek a determinánsa nem nulla. Ez az ellentmondás biztosítja, hogy az egyenletrendszernek nem lehet egyértelmű megoldása. ■

Megjegyezzük, hogy a 3.2.2 Tétel bizonyításának mintájára az is igazolható, hogy ha az együtthatómátrix determinánsa nem nulla, akkor az egyenletrendszernek egyetlen megoldása van. (Ekkor már általában nem igaz, hogy a Gauss-kiküszöbölés során kapott együtthatómátrixok determinánsa nem változik, az azonban igaz, hogy sohasem válik nullává.) Ezzel a Cramer-szabály egy részére új bizonyítás adódott („csak" a képletet nem kaptuk meg ily módon).

A fentiek alapján (az ugyanannyi ismeretlent és egyenletet tartalmazó) homogén lineáris egyenletrendszerekre az alábbi eredményt nyerjük:

3.2.3 Tétel

Legyen $A \in T^{n\times n}$. Az $A\mathbf{x} = \mathbf{0}$ homogén lineáris egyenletrendszernek akkor és csak akkor van nem triviális megoldása, ha $\det A = 0$. ♣

Bizonyítás: Ha $\det A = 0$, akkor a 3.2.2 Tétel szerint nem lehet egyértelmű megoldás, tehát a triviális megoldáson kívül kell még lennie megoldásnak. Ha $\det A \neq 0$, akkor a 3.2.2 Tétel utáni megjegyzés (vagy a 3.2.1 Tétel) alapján egyértelmű a megoldás, tehát csak a triviális megoldás létezik. ■

Megjegyezzük, hogy mindezek alapján új (és teljes) bizonyítást nyerhetünk a négyzetes mátrixok invertálhatóságáról és a nullosztókról szóló 2.2.2 és 2.2.5 tételekre is, ezeket a 3.5 pontban tárgyaljuk majd.

A Cramer-szabály egyik alkalmazásaként most egy interpolációs polinomokról szóló tételt igazolunk:

3.2.4 Tétel

Legyenek $\gamma_1, \ldots, \gamma_n$ a T test különböző elemei, $\beta_1, \ldots, \beta_n$ pedig tetszőleges T-beli elemek. Ekkor pontosan egy olyan legfeljebb $n-1$-edfokú $f \in T[x]$ polinom létezik (megengedve a foknélküli nulla polinomot is), amelyre $f(\gamma_i) = \beta_i$, $i = 1, 2, \ldots, n$. ♣

Bizonyítás: Legyen $f = \delta_0 + \delta_1 x + \ldots + \delta_{n-1}x^{n-1}$, ekkor a feltétel pontosan a

$$\begin{array}{ccccc} \delta_0 + \gamma_1\delta_1 + & \ldots & + \gamma_1^{n-1}\delta_{n-1} & = & \beta_1 \\ \delta_0 + \gamma_2\delta_1 + & \ldots & + \gamma_2^{n-1}\delta_{n-1} & = & \beta_2 \\ \vdots \quad \vdots & \ddots & \vdots & & \vdots \\ \delta_0 + \gamma_n\delta_1 + & \ldots & + \gamma_n^{n-1}\delta_{n-1} & = & \beta_n \end{array}$$

egyenletrendszert jelenti, ahol a δ_i-k az ismeretlenek. Az egyenletrendszer determinánsa a $V(\gamma_1, \ldots, \gamma_n)$ Vandermonde-determináns, amely a γ_i-k különbözősége miatt nem nulla. Így a Cramer-szabály alapján az egyenletrendszernek pontosan egy megoldása van. ■

A Cramer-szabály képletét alkalmazva megkaphatjuk magukat a δ_i együtthatókat, tehát az f polinomot is, azonban — mint említettük — nem biztos, hogy ez a leggyorsabb eljárás f előállítására. Ha szerencsénk van, akkor itt is „kitalálhatjuk" a polinomot, és ezután az egyértelműség miatt már biztosak lehetünk abban, hogy ez az egyetlen megfelelő polinom.

Az f-et (az adott γ_i „helyekhez" és β_i helyettesítési értékekhez tartozó) *interpolációs polinom*nak nevezzük. Az „interpolációs" jelző arra utal, hogy (nagyon pongyolán fogalmazva) az f polinom valósítja meg azt a „lehető legegyszerűbb" függvényt, amely a γ_i helyeken előírt β_i helyettesítési értékek segítségével határozza meg („iktatja közbe") a többi helyen felvett értéket. Az f polinom két másik előállítási módjára, valamint egyértelműségének további lehetséges bizonyításaira nézve lásd a 3.2.9–3.2.11 feladatokat.

Feladatok

3.2.1 Oldjuk meg a komplex számok körében az alábbi egyenletrendszert.

$$\begin{array}{rcl} x_1 + x_2 + x_3 + x_4 & = & 2 + 2i \\ x_1 + 2x_2 + 3x_3 + 4x_4 & = & 4 + 4i \\ x_1 + 3x_2 + 6x_3 + 10x_4 & = & 7 + 6i \\ x_1 + 4x_2 + 10x_3 + 20x_4 & = & 11 + 8i \end{array}$$

3.2.2 Oldjuk meg a valós számok körében:

$$x_1 + 2x_2 = 3, \qquad x_2 + 3x_3 = 4, \qquad \ldots, \qquad x_n + (n+1)x_1 = n + 2\,.$$

3.2.3 Oldjuk meg az alábbi valós egyenletrendszereket, ahol (b)-ben $\alpha_i \neq \alpha_j$, ha $i \neq j$.

$$\text{(a)}\quad \begin{aligned} x_1 + \quad & x_2 + \ldots + \quad x_n = n \\ x_1 + \quad & 2x_2 + \ldots + \quad nx_n = n^2 \\ & \vdots \\ x_1 + 2^{n-1}x_2 + \ldots + n^{n-1}x_n &= n^n \end{aligned}$$

$$\text{(b)}\quad \begin{aligned} x_1 + \quad & x_2 + \ldots + \quad x_n = 1 \\ \alpha_1 x_1 + \quad & \alpha_2 x_2 + \ldots + \quad \alpha_n x_n = \beta \\ & \vdots \\ \alpha_1^{n-1}x_1 + \alpha_2^{n-1}x_2 + \ldots + \alpha_n^{n-1}x_n &= \beta^{n-1} \end{aligned}$$

3.2.4 Használjuk a 3.2.1 Tétel jelöléseit. Melyek igazak az alábbi állítások közül?

(a) Ha $D = 0$, de van olyan j, amelyre $D_j \neq 0$, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer nem oldható meg.

(b) Ha $D = 0$ és minden j-re $D_j = 0$, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek egynél több megoldása van.

3.2.5 Legyenek $A_1, A_2 \in T^{n\times n}$ invertálható mátrixok, és tekintsük az $A_1\mathbf{x} = \mathbf{b}$ és $A_2\mathbf{x} = \mathbf{b}$ egyenletrendszereket (azonos jobb oldallal). Bizonyítsuk be, hogy

(a) pontosan akkor lesz bármilyen $\mathbf{b}$ esetén a két egyenletrendszernek közös megoldása, ha $A_1 = A_2$;

(b) pontosan akkor *nem* lesz semmilyen $\mathbf{b} \neq \mathbf{0}$ esetén sem a két egyenletrendszernek közös megoldása, ha $A_1 - A_2$ is invertálható.

3.2.6

(a) Legyen $m_{ij}, \quad i, j = 1, 2, \ldots, n$ olyan n^2 darab egész szám, hogy az m_{ij}-kből képezett determináns nem osztható 7-tel. Tegyük fel, hogy $v_1, \ldots, v_n$ olyan egész számok, hogy $v_1 m_{j1} + \ldots + v_n m_{jn}$ bármely j-re osztható 7-tel. Bizonyítsuk be, hogy ekkor minden v_i osztható 7-tel.

*(b) Hogyan általánosítható a feladat 7 helyett tetszőleges egész számra?

A további feladatok az interpolációs polinomhoz kapcsolódnak. A 3.2.4 Tétel jelöléseit fogjuk használni.

3.2.7 Határozzuk meg azt a legfeljebb harmadfokú f komplex együtthatós polinomot, amelyre

(a) $f(-1) = 12,\ f(4) = 7,\ f(6) = 5,\ f(9) = 2$;

(b) $f(1) = f(-1) = 3,\ f(2) = f(-2) = 9$;

(c) $f(1) = i,\ f(i) = -1,\ f(-1) = -i,\ f(-i) = 1$;

(d) $f(-1) = f(i) = f(-i) = 1,\ f(1) = 9$.

3.2.8 Hány olyan *pontosan* a) $n-1$-edfokú; b) n-edfokú f polinom van, amely a 3.2.4 Tétel (többi) feltételeit kielégíti?

3.2.9 Adjunk új bizonyítást a 3.2.4 Tételben szereplő f *egyértelműség*ére, arra támaszkodva, hogy egy polinomnak legfeljebb annyi gyöke lehet, mint amennyi a fokszáma.

3.2.10 *Newton-féle interpolációs polinom.* Adjunk új bizonyítást a 3.2.4 Tételre (azaz f *létezés*ére és *egyértelműség*ére) úgy, hogy f-et a következő alakban keressük:

$$f = \nu_0 + \nu_1(x-\gamma_1) + \nu_2(x-\gamma_1)(x-\gamma_2) + \ldots + \nu_{n-1}(x-\gamma_1)\cdot\ldots\cdot(x-\gamma_{n-1}).$$

3.2.11 *Lagrange-féle interpolációs polinom.* Legyen $n > 1$.

(a) Keressünk olyan legfeljebb $n-1$-edfokú L_i polinomot, amelyre $L_i(\gamma_j) = 0$, ha $j \neq i$ és $L_i(\gamma_i) = 1$. [Ez azt jelenti, hogy az interpolációs problémát (először) abban a nagyon speciális esetben oldjuk meg, amikor az előírt helyettesítési értékek egyike 1, az összes többi pedig 0. Az L_i-ket (a γ_i helyekhez tartozó) *Lagrange-féle alappolinom*oknak nevezzük.]

(b) Mutassuk meg, hogy az $f = \sum_{i=1}^{n} \beta_i L_i$ polinom megfelel a 3.2.4 Tétel feltételeinek.

M*3.2.12 Legyen $n > 1$.

(a) Melyik (jólismert) polinom az (n darab) L_i Lagrange-féle alappolinom összege?

(b) Legyenek $\gamma_1, \ldots, \gamma_n$ különböző valós számok és ν tetszőleges valós. Adjuk meg egyszerűbb alakban az alábbi két valós számot:

$$\text{(b1)} \quad \sum_{i=1}^{n} \prod_{j \neq i} \frac{\nu - \gamma_j}{\gamma_i - \gamma_j}\,, \qquad \text{(b2)} \quad \sum_{i=1}^{n} \prod_{j \neq i} \frac{1}{\gamma_i - \gamma_j}\,.$$

3.2.13 Melyek igazak az alábbi állítások közül?

(a) Ha egy (komplex együtthatós) polinom minden egész helyen egész értéket vesz fel, akkor a polinom egész együtthatós.

(b) Ha egy (komplex együtthatós) polinom minden racionális helyen racionális értéket vesz fel, akkor a polinom racionális együtthatós.

*3.2.14 Legyen T véges test. Mutassuk meg, hogy minden $\Phi : T \to T$ függvény polinomfüggvény, azaz van olyan $f \in T[x]$ polinom, hogy minden $\tau \in T$-re $f(\tau) = \Phi(\tau)$.

*3.2.15 Ali Baba a kincset a 40 rablóra akarja hagyni, de fél, hogy azok összevesznek, és ezért olyan módszert szeretne, hogy csak akkor juthassanak hozzá, ha már legalább 25 rabló előre megegyezett, hogyan osztozkodnak. A kincshez vezető útvonalat egy számítógép rejti, ehhez csak úgy lehet hozzáférni, ha valaki bepötyögi a megfelelő jelszót, ami egy (meglehetősen nagy) természetes szám. Ali Baba az Interpol tanácsára egyenként mindegyik rablónak a fülébe súg valamit. Ha bármelyik 25 rabló összefog, akkor meg tudja fejteni a kulcsszámot, de 24-en hiába próbálkoznak, együttesen sem lesz semmilyen információjuk a számról. Mit tanácsolt Ali Babának az Interpol(áció)?

3.3. Lineáris függetlenség T^k-ban

Az előző pontban a lineáris egyenletrendszerek $A\mathbf{x} = \mathbf{b}$ alakját használtuk. A most következő vizsgálatok a 3.1 pont végén említett másik átírási módhoz kapcsolódnak.

Felelevenítve az ott mondottakat, legyen

$$\mathbf{a}_j = \begin{pmatrix} \alpha_{1j} \\ \alpha_{2j} \\ \vdots \\ \alpha_{kj} \end{pmatrix} \in T^k, \quad j = 1, 2, \ldots, n,$$

tehát az $\mathbf{a}_j$-k az A együtthatómátrix oszlopvektorai. Ekkor az egyenletrendszer a következőképpen írható fel: $x_1\mathbf{a}_1 + x_2\mathbf{a}_2 + \ldots + x_n\mathbf{a}_n = \mathbf{b}$.

3.3.1 Definíció

Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_m \in T^k$ és $\lambda_1, \ldots \lambda_m \in T$, azaz vegyünk m darab T^k-beli *vektor*t és ugyanennyi T-beli *skalár*t. Ekkor a $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m \in T^k$ vektort az $\mathbf{u}_i$ vektorok (λ_i skalárokkal képzett) *lineáris kombináció*jának nevezzük. ♣

Ennek alapján a lineáris egyenletrendszer megoldhatósága éppen azt jelenti, hogy $\mathbf{b}$ előáll az $\mathbf{a}_j$ oszlopvektorok lineáris kombinációjaként, és az ilyen előállítás(ok)ban szereplő skalárok szolgáltatják az egyenletrendszer megoldását (megoldásait).

Különösen fontos lesz a homogén egyenletrendszer, azaz a $\mathbf{b} = \mathbf{0}$ eset. A homogén egyenletrendszer triviális megoldásának éppen az felel meg, ha az $\mathbf{a}_j$-k mindegyikét a $\lambda_j = 0$ skalárral szorozzuk meg, és az így elkészített $0\mathbf{a}_1 + \ldots + 0\mathbf{a}_n$ ún. *triviális* lineáris kombináció eredménye természetesen valóban a nullvektor. nem triviális megoldás pedig egy olyan *nem triviális* lineáris kombinációt jelent, amely a nullvektort állítja elő, azonban a kombinációban szereplő skalárok nem mindegyike nulla.

Alapvetően fontos két definíció következik:

3.3.2 Definíció

Az $\mathbf{u}_1, \ldots, \mathbf{u}_m \in T^k$ vektorok *lineárisan összefüggő*k, ha léteznek olyan $\lambda_1, \ldots, \lambda_m \in T$ skalárok, amelyek nem mind 0-k, és $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$. ♣

3.3.3 Definíció

Az $\mathbf{u}_1, \ldots, \mathbf{u}_m \in T^k$ vektorok *lineárisan független*ek, ha $\lambda_1\mathbf{u}_1 + \ldots + +\lambda_m\mathbf{u}_m = \mathbf{0}$ **CSAK** úgy valósulhat meg, ha mindegyik $\lambda_i = 0$. Azaz

$$\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0} \Rightarrow \lambda_i = 0,\ i = 1, \ldots, m.\ \clubsuit$$

Egy $\mathbf{u}_1, \ldots, \mathbf{u}_m \in T^k$ vektorrendszerre tehát a lineáris függetlenség és a lineáris összefüggés közül pontosan az egyik teljesül. A „lineáris” jelzőt a rövidség kedvéért gyakran elhagyjuk.

A „vektorrendszer” kifejezésben a „rendszer” szó arra utal, hogy (a halmazzal ellentétben) ugyanaz a vektor többször is előfordulhat az $\mathbf{u}_i$-k között. Ez a körülmény lényegesen befolyásol(hat)ja a függetlenség kérdését: ha az $\mathbf{u}_i$-k között szerepelnek azonos vektorok, pl. $\mathbf{u}_1 = \mathbf{u}_2$, akkor $1\mathbf{u}_1 + (-1)\mathbf{u}_2 + +0\mathbf{u}_3 + \ldots + 0\mathbf{u}_m = \mathbf{0}$, tehát az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorrendszer mindenképpen összefüggő.

Példák:

P1. Az $\mathbf{u}_1 = \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix}$, $\mathbf{u}_2 = \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix}$, $\mathbf{u}_3 = \begin{pmatrix} 1 \\ 1 \\ 1 \end{pmatrix} \in \mathbf{R}^3$ vektorok lineárisan összefüggők, mert $1\mathbf{u}_1 + 1\mathbf{u}_2 + (-3)\mathbf{u}_3 = \mathbf{0}$.

P2. Az előző $\mathbf{u}_1, \mathbf{u}_2$, valamint az $\mathbf{u}_4 = \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix}$ vektorokból álló rendszer lineárisan független. Ennek igazolásához írjuk ki részletesen a $\lambda_1\mathbf{u}_1 + \lambda_2\mathbf{u}_2 + +\lambda_4\mathbf{u}_4 = \mathbf{0}$ egyenlőséget:

$$\lambda_1 \begin{pmatrix} 1 \\ 2 \\ 1 \end{pmatrix} + \lambda_2 \begin{pmatrix} 2 \\ 1 \\ 2 \end{pmatrix} + \lambda_4 \begin{pmatrix} 2 \\ 1 \\ 1 \end{pmatrix} = \begin{pmatrix} \lambda_1 + 2\lambda_2 + 2\lambda_4 \\ 2\lambda_1 + \lambda_2 + \lambda_4 \\ \lambda_1 + 2\lambda_2 + \lambda_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 0 \end{pmatrix},$$

ami pontosan

$$\begin{aligned} \lambda_1 + 2\lambda_2 + 2\lambda_4 &= 0 \\ 2\lambda_1 + \lambda_2 + \lambda_4 &= 0 \\ \lambda_1 + 2\lambda_2 + \lambda_4 &= 0 \end{aligned}$$

teljesülését jelenti. A Gauss-kiküszöböléssel könnyen adódik, hogy ennek a homogén egyenletrendszernek csak triviális megoldása van, azaz **CSAK** $\lambda_1 = \lambda_2 = \lambda_4 = 0$ lehetséges, így az $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_4$ vektorok valóban függetlenek.

Természetesen a P1 példában, az $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ vektorok lineáris összefüggésének az igazolásához sincs szükség arra, hogy valahonnan megsejtsük a megfelelő skalárokat. Ekkor a

$$\begin{aligned} \lambda_1 + 2\lambda_2 + \lambda_3 &= 0 \\ 2\lambda_1 + \lambda_2 + \lambda_3 &= 0 \\ \lambda_1 + 2\lambda_2 + \lambda_3 &= 0 \end{aligned}$$

homogén egyenletrendszert kell vizsgálni, és Gauss-kiküszöböléssel kapjuk az általános megoldást: $\lambda_1 = \lambda_2 = -\mu/3, \lambda_3 = \mu$, ahol μ tetszőleges valós szám. Mivel van nem triviális megoldás, ezért a vektorok összefüggők, és bármely $\mu \neq 0$ szolgáltat egy alkalmas nem triviális kombinációt. (A P1 példában az indoklásként rögtön az elején felírt kombinációhoz — amelyet talán tényleg „ki lehetett találni" — a $\mu = -3$ paraméterérték tartozik).

Az imént elmondottak teljesen általános érvényűek: az $\mathbf{u}_1, \ldots, \mathbf{u}_n \in T^k$ vektorok lineáris összefüggőségének, illetve függetlenségének az eldöntéséhez tekintsük az $U\mathbf{x} = \mathbf{0}$ homogén lineáris egyenletrendszert, ahol az $U \in T^{k\times n}$ mátrix oszlopvektorai az $\mathbf{u}_j$-k. Ha ennek az egyenletrendszernek csak triviális megoldása van, akkor az $\mathbf{u}_j$ vektorok függetlenek, ha pedig létezik nem triviális

megoldás is, akkor összefüggők. Azt, hogy létezik-e az egyenletrendszernek nem triviális megoldása vagy sem, Gauss-eliminációval határozhatjuk meg. nem triviális megoldás létezése esetén a megoldások egyúttal meg is adják a skalárokat a nullvektort előállító lineáris kombinációkhoz.

A lineáris függetlenség kérdésénél adódó homogén egyenletrendszereknél általában a Gauss-kiküszöbölés alkalmazása a legcélszerűbb. Abban a (nagyon) speciális esetben, amikor a vektorok száma megegyezik k-val (tehát a komponensek számával), egy négyzetes U mátrixot kapunk, és így alkalmazhatjuk a 3.2.3 Tételt is: a vektorok ebben az esetben akkor és csak akkor összefüggők, ha $\det U = 0$ (azonban ez összefüggőség esetén nem ad információt a nem triviális lineáris kombinációkban szereplő skalárokról).

Ha a vektorok száma k-nál nagyobb, akkor egy olyan homogén egyenletrendszerhez jutunk, amelyben több az ismeretlen, mint az egyenlet. A 3.1.4 Tétel szerint ennek mindig van nem triviális megoldása, a vektorok tehát *biztosan* összefüggők. Ezt az egyszerű tényt nagyon sokszor fel fogjuk használni, ezért külön tételként is megfogalmazzuk:

3.3.4 Tétel

Akárhogyan választunk T^k-ban k-nál több vektort, ezek szükségképpen lineárisan összefüggők. ♣

A lineáris függetlenség, illetve összefüggőség definíciójából azonnal adódnak az alábbi egyszerű észrevételek. Egyetlen vektor egyedül akkor és csak akkor független, ha nem a nullvektor. Két vektor akkor és csak akkor lineárisan független, ha egyik sem skalárszorosa a másiknak. Több vektor esetén ez már *nem igaz*, lásd pl. a P1 példában szereplő $\mathbf{u}_1, \mathbf{u}_2$ és $\mathbf{u}_3$ vektorokat, amelyek közül egyik sem skalárszorosa a másiknak, mégis összefüggők.

Az alábbi tételben a definíciók néhány további egyszerű következményét foglaljuk össze (melegen ajánljuk, hogy az Olvasó próbálja ezeket előbb önállóan bebizonyítani, és csak utána nézze meg az általunk közölt bizonyításokat):

3.3.5 Tétel

I. Ha egy (legalább kételemű) lineárisan független rendszerből egy tetszőleges elemet elhagyunk, akkor a maradék vektorok is lineárisan független rendszert alkotnak.

II. Ha egy lineárisan összefüggő rendszerhez egy tetszőleges vektort hozzáveszünk, akkor az így kapott vektorrendszer is lineárisan összefüggő.

III. Egy legalább kételemű vektorrendszer akkor és csak akkor lineárisan összefüggő, ha van benne (*legalább* egy) olyan vektor, amely előáll a többi vektor lineáris kombinációjaként.

IV. Ha $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független, de az $\mathbf{u}_{m+1}$ vektor hozzávételével kapott rendszer lineárisan összefüggő, akkor $\mathbf{u}_{m+1}$ előáll az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineáris kombinációjaként.

V. Tegyük fel, hogy valamely $\mathbf{v}$ vektor előáll az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineáris kombinációjaként. Ez az előállítás akkor és csak akkor egyértelmű, ha $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független. ♣

Bizonyítás: Lássuk be először II-t. Tegyük fel, hogy az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineárisan összefüggők, azaz léteznek olyan $\lambda_1, \ldots, \lambda_m \in T$ skalárok, amelyek nem mind 0-k, és $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$. Ekkor a vektorrendszerhez tetszőleges $\mathbf{u}_{m+1}$ vektort hozzávéve, a $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m + 0\mathbf{u}_{m+1}$ lineáris kombináció nem triviálisan állítja elő a nullvektort, tehát a kibővített vektorrendszer is összefüggő.

I-et indirekt igazoljuk. Ha a maradék vektorok összefüggők lennének, akkor az elhagyott vektort visszavéve II. alapján az eredeti rendszer is összefüggő lett volna.

III-nál tegyük fel először, hogy pl. $\mathbf{u}_m$ előáll a többi $\mathbf{u}_i$ lineáris kombinációjaként, azaz $\mathbf{u}_m = \delta_1\mathbf{u}_1 + \ldots + \delta_{m-1}\mathbf{u}_{m-1}$. Ezt nullára rendezve $\mathbf{0} = \delta_1\mathbf{u}_1 + \ldots + \delta_{m-1}\mathbf{u}_{m-1} + (-1)\mathbf{u}_m$ adódik, ami a nullvektor egy nem triviális előállítása, hiszen a -1 skalár biztosan nem nulla. Ebből következik, hogy a vektorok összefüggők. A megfordításhoz legyenek az $\mathbf{u}_i$ vektorok összefüggők, vegyük a nullvektor egy nem triviális $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$ előállítását, ahol mondjuk $\lambda_1 \neq 0$. Ekkor az $\mathbf{u}_1$ vektor $\mathbf{u}_1 = (-\lambda_2/\lambda_1)\mathbf{u}_2 + \ldots + (-\lambda_m/\lambda_1)\mathbf{u}_m$ formában előáll a többi vektor lineáris kombinációjaként.

III. második részében azt is igazoltuk, hogy bármelyik olyan vektor kifejezhető a többi lineáris kombinációjaként, amely a nullvektort adó (egyik) nem triviális lineáris kombinációban nem nulla skalárral van megszorozva. Így IV-hez elég azt belátnunk, hogy az $\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{u}_{m+1}$ vektorok egy nem triviális lineáris kombinációjában $\mathbf{u}_{m+1}$ együtthatója nem nulla. Ez valóban igaz, mert különben $\mathbf{0} = \lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m + 0\mathbf{u}_{m+1} = \lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m$ miatt a nullvektor az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok egy nem triviális lineáris kombinációjaként is előállna, ami ellentmond azok függetlenségének.

Végül V-höz csak azt kell végiggondolnunk, hogy $\rho_1\mathbf{u}_1 + \ldots + \rho_m\mathbf{u}_m = \pi_1\mathbf{u}_1 + \ldots + \pi_m\mathbf{u}_m$ pontosan akkor teljesül, ha $(\rho_1 - \pi_1)\mathbf{u}_1 + \ldots + (\rho_m - \pi_m)\mathbf{u}_m = \mathbf{0}$. ■

A III. és IV. állítással kapcsolatban külön is megjegyezzük, hogy lineáris összefüggőség esetén általában *több* olyan vektor is van, amely kifejezhető a többiek lineáris kombinációjaként. Ugyanígy, ha független vektorokhoz egy új vektort hozzávéve összefüggő rendszert kapunk, akkor általában nemcsak az új vektor írható fel a régiek lineáris kombinációjaként, hanem „szinte mindig" a régi vektorok között is van(nak) olyan(ok), amely(ek) előáll(nak) a többiek (azaz a többi régi és az új vektor) alkalmas lineáris kombinációjaként (lásd a 3.3.4 és 3.3.5 feladatokat).

A lineáris függetlenség szokatlan fogalom, alaposan meg kell emészteni. Ne felejtsük például el, hogy a lineáris függetlenséget sohasem lehet úgy megfogni, hogy az adott vektoroknak a csupa nulla skalárral vett lineáris kombinációját tekintjük. Ez ugyanis mindig a nullvektort eredményezi, tekintet nélkül arra, hogy a vektorok függetlenek vagy összefüggők voltak.

A lineáris függetlenséggel kapcsolatos kezdeti nehézségeken legkönnyebben úgy juthatunk túl, ha egyrészt mindent nagyon aprólékosan végiggondolunk, a legszigorúbban tartva magunkat a definíciókhoz, másrészt a bennünk kialakuló képet — ha lehet — minél többször összevetjük a sík- és térvektorok körében (azaz $\mathbf{R}^2$-ben és $\mathbf{R}^3$-ban) fennálló helyzettel, ahol tényleg „látjuk", mi mit jelent és a geometriai szemléletre (is) támaszkodhatunk.

A lineáris függetlenség fogalmát a 4.4 pontban majd tetszőleges vektortérre is általánosítjuk. Többszörösen kiderül azonban, hogy a fogalom minden lényeges eleme megtalálható már a most definiált T^k-beli speciális esetben is; egyrészt azt itt elmondottak szinte szó szerint átvihetők az általános esetre, másrészt pedig belátjuk majd, hogy minden (ún. véges dimenziós) vektortér „tulajdonképpen" megegyezik valamelyik T^k-val (lásd a 4.7 és 5.2 pontokat). Ennek ellenére (vagy éppen ezért) a lineáris függetlenség alapvető szerephez jut a matematika valamennyi ágában.

Feladatok

(Lásd a 4.4.1–4.4.8 feladatokat is.)

3.3.1 Döntsük el az alábbi $\mathbf{R}^4$-beli vektorokról, hogy lineárisan összefüggők vagy függetlenek. Ha összefüggők, fejezzük ki az egyiket a többi lineáris kombinációjaként.

(i) $\begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}-2\\5\\0\\1\end{pmatrix}, \begin{pmatrix}-1\\4\\1\\2\end{pmatrix}$ (ii) $\begin{pmatrix}1\\2\\3\\4\end{pmatrix}, \begin{pmatrix}-2\\5\\1\\1\end{pmatrix}, \begin{pmatrix}-1\\4\\1\\2\end{pmatrix}$

3.3.2 Döntsük el az alábbi $\mathbf{R}^4$-beli vektorokról, hogy lineárisan összefüggők vagy függetlenek.

(i) $\begin{pmatrix}1\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}$ (ii) $\begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\0\\1\end{pmatrix}$

(iii) $\begin{pmatrix}1\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\0\\1\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}$

Legyen T a modulo 3 test. Mennyiben változik a helyzet, ha a fenti vektorokat T^4-belieknek tekintjük?

3.3.3 Melyek igazak az alábbi állítások közül?

(a) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_5$ lineárisan független, de $\mathbf{u}_1, \ldots, \mathbf{u}_7$ lineárisan összefüggő, akkor $\mathbf{u}_6$ és $\mathbf{u}_7$ közül legalább az egyik felírható az $\mathbf{u}_1, \ldots, \mathbf{u}_5$ vektorok lineáris kombinációjaként.

(b) Ha van olyan $\mathbf{u} \neq \mathbf{0}$ vektor, amely felírható $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ lineáris kombinációjaként és $\mathbf{u}_4, \mathbf{u}_5, \mathbf{u}_6$ lineáris kombinációjaként is, akkor az $\mathbf{u}_1, \ldots, \mathbf{u}_6$ vektorok lineárisan összefüggők.

(c) Ha az $\mathbf{u}_1, \ldots, \mathbf{u}_6$ vektorok egyike sem a nullvektor és lineárisan összefüggők, akkor van olyan $\mathbf{u} \neq \mathbf{0}$ vektor, amely felírható $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3$ lineáris kombinációjaként és $\mathbf{u}_4, \mathbf{u}_5, \mathbf{u}_6$ lineáris kombinációjaként is.

3.3.4 Melyek igazak az alábbi állítások közül?

(a) Ha egy $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$ nem triviális lineáris kombinációban $\lambda_3 \neq 0$, akkor $\mathbf{u}_3$ előáll a többi $\mathbf{u}_i$ vektor lineáris kombinációjaként.

(b) Ha egy $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$ nem triviális lineáris kombinációban $\lambda_3 = 0$, akkor $\mathbf{u}_3$ *nem* áll elő a többi $\mathbf{u}_i$ vektor lineáris kombinációjaként.

(c) Ha az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok között pontosan d olyan van, amely kifejezhető a többi $m-1$ vektor lineáris kombinációjaként, akkor az $\mathbf{u}_i$ vektorok közül kiválasztható $m-d$ elemű független rendszer.

(d) Ha az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok között pontosan d olyan van, amely kifejezhető a többi $m-1$ vektor lineáris kombinációjaként, akkor az $\mathbf{u}_i$ vektorok közül nem választható ki $m-d$-nél több elemű független rendszer.

3.3.5 Tegyük fel, hogy $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független, $\mathbf{u}_1, \ldots, \mathbf{u}_m, \mathbf{v}$ lineárisan összefüggő, továbbá egyik $\mathbf{u}_i$ sem írható fel a $\mathbf{v}$ és a többi $\mathbf{u}_j$ lineáris kombinációjaként. Határozzuk meg $\mathbf{v}$-t.

3.3.6 Az $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4$ vektorok lineárisan függetlenek, $\mathbf{u}_5 \neq \mathbf{0}$ és $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_5$ lineárisan összefüggő. Mit állíthatunk lineáris függetlenség, illetve összefüggőség szempontjából az $\mathbf{u}_3, \mathbf{u}_4, \mathbf{u}_5$ vektorokról? (Lehetséges válaszok: szükségképpen függetlenek — szükségképpen összefüggők — lehetnek függetlenek is és összefüggők is.)

3.3.7

(a) Megadható-e öt vektor úgy, hogy közülük az első három vektor lineárisan összefüggő, de bármelyik másik vektorhármas lineárisan független legyen?

(b) Megadható-e öt vektor úgy, hogy közülük az első három vektor lineárisan független, de bármelyik másik vektorhármas lineárisan összefüggő legyen, és a vektorok egyike sem a nullvektor?

3.3.8 Legyenek $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4 \in \mathbf{R}^8$ lineárisan függetlenek. Döntsük el, hogy az alábbi vektorrendszerek lineárisan függetlenek vagy összefüggők:

(a) $\mathbf{u}_1 - \mathbf{u}_2,\ \mathbf{u}_2 - \mathbf{u}_3,\ \mathbf{u}_3 - \mathbf{u}_4$;

(b) $\mathbf{u}_1 - \mathbf{u}_2,\ \mathbf{u}_2 - \mathbf{u}_3,\ \mathbf{u}_3 - \mathbf{u}_1$;

(c) $\mathbf{u}_1 + \mathbf{u}_2,\ \mathbf{u}_2 + \mathbf{u}_3,\ \mathbf{u}_3 + \mathbf{u}_4,\ \mathbf{u}_4 + \mathbf{u}_1$;

(d) $\mathbf{u}_1 + \mathbf{u}_2,\ \mathbf{u}_2 + \mathbf{u}_3,\ \mathbf{u}_3 + \mathbf{u}_4,\ \mathbf{u}_4 + \mathbf{u}_2$;

(e) $\mathbf{u}_1 + \pi\mathbf{u}_2 + \sqrt{2}\mathbf{u}_3 + (\sin 1^\circ)\mathbf{u}_4,\ 100\mathbf{u}_1 + 77\mathbf{u}_2 + (3/11)\mathbf{u}_3 + \mathbf{u}_4,$
$\mathbf{u}_1 + 5^6\mathbf{u}_2 + \pi^2\mathbf{u}_3 - (1/8)\mathbf{u}_4,\ (\lg 3)\mathbf{u}_1 + 1999\mathbf{u}_2 + \mathbf{u}_3 + \mathbf{u}_4,\ \mathbf{u}_1 + \mathbf{u}_2 + \mathbf{u}_3$.

Oldjuk meg a feladatot arra az esetre is, ha az $\mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \mathbf{u}_4$ vektorok lineárisan összefüggők voltak.

3.3.9 Tekintsünk m darab vektort, és készítsük el ezeknek q darab lineáris kombinációját. Mit állíthatunk az így kapott vektorokról lineáris függetlenség, ill. összefüggőség szempontjából, ha az eredeti vektorok lineárisan (a) függetlenek; (b) összefüggők voltak, és α) $q = m + 1$; β) $q = m$; γ) $q = m - 1$? (Ez összesen hat kérdés. Lehetséges válaszok: szükségképpen függetlenek — szükségképpen összefüggők — lehetnek függetlenek is és összefüggők is.)

3.3.10 Legyenek $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$ lineárisan független vektorok és $\lambda \neq 0$ egy T-beli skalár. Mutassuk meg, hogy ekkor a $\lambda\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_m$, illetve $\mathbf{u}_1 + \lambda\mathbf{u}_2, \mathbf{u}_2, \ldots, \mathbf{u}_m$ vektorrendszerek is lineárisan függetlenek.

3.3.11 Bizonyítsuk be, hogy egy mátrix oszlopvektorainak a lineáris függetlensége, illetve összefüggősége nem változik meg, ha a mátrixszal elemi (a) oszlopekvivalens; (b) sorekvivalens átalakításokat végzünk [ami (b)-nél az 58. oldalon felsorolt M1–M4 lépéseket, (a)-nál pedig ezek oszlopokra vonatkozó változatait jelenti].

*3.3.12 Vegyünk 11 tetszőleges pozitív egészt, amelyek egyike sem osztható 30-nál nagyobb prímszámmal. Bizonyítsuk be, hogy a számok közül kiválasztható néhány (esetleg csak egy, esetleg az összes), amelyek szorzata négyzetszám.

3.4. A mátrix rangja

A mátrixokra háromféle rangfogalmat definiálunk, kettőt a lineáris függetlenség és egyet a determinánsok segítségével, majd megmutatjuk, hogy ezek bármely mátrix esetén megegyeznek. Az is kiderül, hogy ez a közös érték éppen az RLA-beli vezéregyesek száma. Ennek alapján a rang kiszámítása is a legegyszerűbben általában a Gauss-kiküszöbölés segítségével történhet. Végül az egyenletrendszerek megoldhatóságának, illetve egyértelmű megoldhatóságának a feltételét fogjuk a rang segítségével megfogalmazni.

Tekintsünk egy $A \in T^{k\times n}$ mátrixot. Ennek n darab oszlopvektora van, amelyek T^k-beli vektorok. Hasonlóképpen értelmezhetjük a *sorvektor*okat is, ez k darab T^n-beli vektort jelent. (A sorvektorok tulajdonképpen $1 \times n$-es és nem $n \times 1$-es mátrixok, azonban általában nem lényeges, hogy a két fogalom, azaz $T^{1\times n}$ és $T^{n\times 1}$ között különbséget tegyünk, és így mindkettőt T^n-nel fogjuk jelölni.) Az A mátrix sorvektorai éppen az A^T transzponált mátrix oszlopvektorai.

A mátrix oszloprangját az oszlopai közül kiválasztható lineárisan független vektorok maximális számaként értelmezzük:

3.4.1/O Definíció

Egy A mátrix *oszloprang*ja r, ha A oszlopvektorai között található r lineárisan független, de r-nél több nem. ♣

Az, hogy r-nél több független oszlop nem választható ki, azt jelenti, hogy akárhogyan veszünk r-nél több oszlopot, ezek szükségképpen lineárisan összefüggők (vagy már eleve is csak r oszlop volt összesen).

Ha az oszloprang r, akkor általában többféleképpen is kiválasztható r darab lineárisan független oszlop, sőt még az is előfordulhat, hogy bármelyik r darab oszlop lineárisan független (lásd a 3.4.13 feladatot).

Áttérve a sorokra, a sorrang analóg módon a sorvektorok közül a függetlenek maximális számát jelenti:

3.4.1/S Definíció

Egy A mátrix *sorrang*ja r, ha A sorvektorai között található r lineárisan független, de r-nél több nem. ♣

Könnyen adódik (lásd a 3.4.1 feladatot), hogy mindkét definícióban az „r-nél több" szavak helyett elég „$r+1$"-et írni.

Ahogy már jeleztük, be fogjuk látni, hogy a két látszólag teljesen eltérő fogalom mindig egybeesik.

Példák: Az $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$ mátrix oszloprangja 2, mert pl. az első két oszlop lineárisan független, azonban bármely három oszlopvektor már lineárisan összefügg. A sorrang — összhangban az előrebocsátott megjegyzéssel — szintén 2. A nullmátrix oszloprangja 0, hiszen bármely egyetlen oszlopa már önmagában is összefüggő. Az $n \times n$-es E egységmátrix (oszlop- és sor)rangja n, ugyanis az oszlopai lineárisan függetlenek. Egy $k \times n$-es mátrix oszloprangja nyilván egyrészt legfeljebb n, másrészt legfeljebb k, hiszen az oszlopok T^k-ból valók és ott bármely $k+1$ vektor már biztosan összefügg [tehát a(z oszlop)rang kisebb vagy egyenlő, mint a sorok és oszlopok számának a minimuma].

A determinánsranghoz szükségünk lesz az általános aldeterminánsfogalomra. *Aldeterminánson* ezután egy tetszőleges négyzetes részmátrixnak a determinánsát értjük: kiválasztjuk a mátrix valahány (mondjuk h) sorát, majd ettől függetlenül ugyanennyi oszlopát, és az ezek metszéspontjaiban álló (h^2 darab elemből képzett) h-adrendű (azaz $h \times h$-as) determinánst vesszük. A(z n-edrendű) determináns kifejtésénél szerepet játszó A_{ij} előjeles aldeterminánsa „előjel nélküli része" ennek $h = n-1$ speciális esete volt.

A mátrix determinánsrangja a legnagyobb méretű nem nulla aldeterminánsa rendje:

3.4.1/D Definíció

Egy A mátrix *determinánsrang*ja r, ha van olyan $r \times r$-es aldeterminánsa, ami nem nulla, de bármely r-nél nagyobb rendű aldeterminánsa (ha egyáltalán van ilyen) már nulla. ♣

Az „r-nél nagyobb" szavak helyére most is „$r+1$"-et írhatunk (lásd a 3.4.1 feladatot).

Az oszloprangnál említettekhez hasonlóan az $r \times r$-es aldeterminánsok között több olyan is lehet, amelyik nem nulla (lásd a 3.4.14 feladatot).

A fenti első példában szereplő mátrixnál pl. a bal felső 2×2-es aldeterminánsnem nulla, ugyanakkor bármely 3×3-as aldeterminánsnulla, így a determinánsrang (is) 2. Az is világos, hogy a determinánsrang (is) mindig legfeljebb akkora, mint a sorok vagy az oszlopok száma, hiszen ennél nagyobb aldeterminánsmár nem is készíthető. Könnyen adódik, hogy egy mátrixnak és a transzponáltjának megegyezik a determinánsrangja, ugyanis A^T aldeterminánsait A megfelelő aldeterminánsainak transzponáltjaként kapjuk, és a transzponálás nem változtatja meg a determináns értékét.

3.4.2 Tétel

Egy mátrix oszloprangja, sorrangja és determinánsrangja megegyezik. ♣

Ezt a közös értéket nevezzük a mátrix *rang*jának (minden külön jelző nélkül). Az A mátrix rangját $r(A)$-val jelöljük.

Bizonyítás: Jelölje (ideiglenesen) az A mátrix oszlop-, sor-, illetve determinánsrangját $o(A)$, $s(A)$, illetve $d(A)$.

I. Tegyük fel, hogy $o(A)$ és $d(A)$ egyenlőségét már beláttuk. Innen $s(A) = d(A)$ már könnyen következik a transzponált felhasználásával: $s(A) = o(A^T) = d(A^T) = d(A)$.

II. Az oszlop- és determinánsrang egyenlőségéhez először megmutatjuk, hogy az elemi sorekvivalens átalakítások során egyik sem változik, és ezután már elég azt igazolnunk, hogy a Gauss-kiküszöböléssel kapott RLA-ban mindkettőt éppen a vezéregyesek száma adja.

III. Az oszlopranghoz (bizonyos) oszlopok lineáris függetlenségét kell vizsgálni. Ez olyan homogén lineáris egyenletrendszert jelent, amelynek az együtthatómátrixa az eredeti mátrixnak a kérdéses oszlopokból álló részmátrixa. Az, hogy ennek a homogén lineáris egyenletrendszernek létezik-e nem triviális megoldása, vagy sem, valóban nem változik az elemi sorekvivalens átalakításokkal (hiszen ekvivalens egyenletrendszerekhez jutunk), tehát a(z eredeti) mátrix oszloprangja is változatlan marad.

IV. A determinánsrang változatlanságát arra az elemi sorekvivalens átalakításra mutatjuk meg, amikor az egyik sorhoz valamelyik másik sor skalárszorosát hozzáadjuk, a többi (ennél egyszerűbb) eset igazolását az Olvasóra bízzuk.

Elég belátnunk, hogy a determinánsrang nem nő. Ugyanis az átalakítást ugyanezen skalárszoros kivonásával „visszacsinálhatjuk”, és ha a determináns-

rang a két lépés egyikében sem nőtt, akkor mindkét lépésben csak egyenlőség állhat fenn, hiszen végül az eredeti mátrixhoz jutottunk vissza.

Tegyük fel például, hogy A harmadik sorához az első sor λ-szorosát adtuk hozzá, és jelöljük az így kapott mátrixot B-vel. A $d(B) \le d(A)$ egyenlőtlenséghez azt kell megmutatnunk, hogy ha A-ban minden (mondjuk) $h \times h$-as aldeterminánsa nulla, akkor ugyanez B-ben is teljesül. Vegyünk B-ben egy tetszőleges h-adrendű D aldeterminánst. Ha D-ben nem szerepel a B mátrix harmadik sora, akkor D egyben A-nak is aldeterminánsa, tehát a feltétel szerint nulla. Ha D-ben B első és harmadik sora is szerepel, akkor az utóbbiból az előbbi λ-szorosát levonva D nem változott, ugyanakkor ismét egy A-beli aldeterminánshoz jutottunk, tehát D most is nulla. Végül nézzük azt az esetet, amikor D-ben B harmadik sora szerepel, de az első sor nem. Álljon D mondjuk B első h oszlopából és $2., 3., \dots, h+1$-edik sorából. Ekkor

$$D = \begin{vmatrix} \alpha_{21} & \alpha_{22} & \dots & \alpha_{2h} \\ \alpha_{31}+\lambda\alpha_{11} & \alpha_{32}+\lambda\alpha_{12} & \dots & \alpha_{3h}+\lambda\alpha_{1h} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{h+1,1} & \alpha_{h+1,2} & \dots & \alpha_{h+1,h} \end{vmatrix} =$$

$$= \begin{vmatrix} \alpha_{21} & \alpha_{22} & \dots & \alpha_{2h} \\ \alpha_{31} & \alpha_{32} & \dots & \alpha_{3h} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{h+1,1} & \alpha_{h+1,2} & \dots & \alpha_{h+1,h} \end{vmatrix} + \lambda \begin{vmatrix} \alpha_{21} & \alpha_{22} & \dots & \alpha_{2h} \\ \alpha_{11} & \alpha_{12} & \dots & \alpha_{1h} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{h+1,1} & \alpha_{h+1,2} & \dots & \alpha_{h+1,h} \end{vmatrix} =$$

$$= D_1 + \lambda D_2 \,.$$

Itt D_1 az A mátrix egy h-adrendű aldeterminánsa, tehát 0, D_2 pedig (esetleges) sorcserékkel alakítható át egy ilyen aldeterminánssá, és ezért szintén 0. Ennélfogva $D = 0$ is teljesül.

V. Tekintsük most egy („jobb oldal nélküli") mátrix RLA-ját és jelöljük a vezéregyesek számát r-rel. Megmutatjuk, hogy az oszloprang és a determinánsrang egyaránt r. Mivel az azonosan nulla sorok törölhetők, így feltehetjük, hogy az RLA-ban a sorok száma összesen r. Így egyik rang sem lehet r-nél nagyobb. Ugyanakkor a vezéregyeseket tartalmazó oszlopok az $r \times r$-es egységmátrixot alkotják, tehát lineárisan függetlenek, továbbá az ebből képzett aldeterminánsnak nem nulla (hanem 1), azaz mindkét rang valóban r. ■

Külön is kiemeljük a bizonyításnak azt a „melléktermékét", hogy a rang a Gauss-kiküszöbölés során nem változik, és éppen az RLA-beli vezéregyesek számát jelenti. Mivel a most bizonyított tétel szerint a rang szempontjából a sorok és oszlopok szerepe felcserélhető, ezért a fentieket azzal (az

egyébként közvetlenül is igazolható ténnyel) egészíthetjük ki, hogy a rangot az elemi oszlopekvivalens átalakítások sem befolyásolják. Ez azt jelenti, hogy a rang meghatározásánál — hasonlóan a determinánsok kiszámításához — szabad a Gauss-kiküszöbölést az oszlopok szerint (vagy akár vegyesen is) végezni. (Azonban ismételten felhívjuk a figyelmet arra, hogy egyenletrendszerek megoldásánál ettől messzemenően óvakodjunk.)

Most rátérünk a rang és az egyenletrendszerek kapcsolatára.

3.4.3 Tétel

Az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer akkor és csak akkor oldható meg, ha $r(A) = r(A|\mathbf{b})$, azaz az együtthatómátrix rangja megegyezik a kibővített mátrix rangjával. Megoldhatóság esetén a megoldás akkor és csak akkor egyértelmű, ha a (közös) rang megegyezik az ismeretlenek számával. ♣

Bizonyítás: Írjuk fel az egyenletrendszert $x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n = \mathbf{b}$ alakban, ahol az $\mathbf{a}_j \in T^k$ vektorok az $A \in T^{k\times n}$ együtthatómátrix oszlopvektorai.

I. Tegyük fel először, hogy $r(A) = r(A|\mathbf{b}) = r$, és vegyünk r független oszlopot A-ból, legyenek ezek mondjuk $\mathbf{a}_1, \ldots, \mathbf{a}_r$. Az $\mathbf{a}_1, \ldots, \mathbf{a}_r, \mathbf{b}$ vektorrendszer $r(A|\mathbf{b}) = r$ miatt lineárisan összefüggő. A 3.3.5/IV Tétel szerint ekkor $\mathbf{b}$ kifejezhető az $\mathbf{a}_1, \ldots, \mathbf{a}_r$ vektorok lineáris kombinációjaként. Ehhez a többi oszlopvektort 0 együtthatóval hozzávéve kapjuk, hogy $\mathbf{b}$ felírható az A mátrix (összes) oszlopainak lineáris kombinációjaként, ami éppen az egyenletrendszer megoldhatóságát jelenti.

II. A megfordításhoz most induljunk ki abból, hogy az egyenletrendszer megoldható, tehát $\mathbf{b}$ előáll az $\mathbf{a}_j$ oszlopvektorok lineáris kombinációjaként:

$$\mathbf{b} = \alpha_1\mathbf{a}_1 + \ldots + \alpha_n\mathbf{a}_n\,. \tag{3.4.1}$$

Jelöljük $r(A)$-t röviden r-rel, és lássuk be, hogy az $A|\mathbf{b}$ kibővített mátrix rangja is r. A kibővítés miatt nyilván $r(A|\mathbf{b}) \geq r$, tehát elég azt megmutatnunk, hogy $A|\mathbf{b}$ bármely $r+1$ oszlopa lineárisan összefügg. Ha a kiválasztott $r+1$ oszlop között nem szerepel $\mathbf{b}$, akkor ez $r(A) = r$-ből következik. Vegyük tehát $\mathbf{b}$-t és A-nak r oszlopát, mondjuk $\mathbf{a}_1, \ldots, \mathbf{a}_r$-et. Ha $\mathbf{a}_1, \ldots, \mathbf{a}_r$ összefüggő, akkor a 3.3.5/II Tétel szerint $\mathbf{a}_1, \ldots, \mathbf{a}_r, \mathbf{b}$ is az lesz. Marad tehát az az eset, amikor $\mathbf{a}_1, \ldots, \mathbf{a}_r$ lineárisan független. Vegyünk egy tetszőleges $r+1$-edik $\mathbf{a}_j$ oszlopot ($j > r$), ekkor $r(A) = r$ miatt $\mathbf{a}_1, \ldots, \mathbf{a}_r, \mathbf{a}_j$ lineárisan összefüggő, és ismét használva a 3.3.5/IV Tételt kapjuk, hogy $\mathbf{a}_j$ előáll $\mathbf{a}_1, \ldots, \mathbf{a}_r$ lineáris kombinációjaként. Az $\mathbf{a}_j$ vektoroknak ezeket az előállításait (3.4.1)-be beírva az adódik, hogy $\mathbf{b}$-t ki tudjuk fejezni csak az $\mathbf{a}_1, \ldots, \mathbf{a}_r$ oszlopok lineáris

kombinációjaként is. Ekkor viszont $\mathbf{a}_1, \ldots, \mathbf{a}_r, \mathbf{b}$ szükségképpen összefüggők, amivel ennek az esetnek a bizonyítását is befejeztük.

III. Megoldhatóság esetén a megoldás pontosan akkor egyértelmű, ha $\mathbf{b}$ egyértelműen állítható elő az A mátrix oszlopvektorainak lineáris kombinációjaként. A 3.3.5/V Tétel szerint ez azzal ekvivalens, hogy az $\mathbf{a}_j$ oszlopvektorok lineárisan függetlenek, azaz az A mátrix rangja megegyezik az oszlopok, vagyis az ismeretlenek számával. (Másik lehetőségként hivatkozhattunk volna a 3.1.1/III Tételre is.) ■

Feladatok

3.4.1 Mutassuk meg, hogy ha egy mátrixban bármely $r+1$ oszlop összefüggő, akkor bármely ennél több oszlop is lineárisan összefüggő. Hasonlóan, ha bármely $r+1$-edrendű aldeterminánsa nulla, akkor bármely ennél nagyobb méretű aldeterminánsa is nulla.

3.4.2 Hány $h \times h$-as aldeterminánsa van egy $k \times n$-es mátrixnak?

3.4.3 Számítsuk ki az alábbi mátrixok rangját.

(i) $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 5 & 6 \\ 3 & 5 & 9 \\ 0 & 1 & 0 \end{pmatrix}$ (ii) $\begin{pmatrix} 1 & 3 & 9 \\ 2 & 4 & 8 \\ 9 & 3 & 1 \\ 8 & 4 & 2 \end{pmatrix}$ (iii) $\begin{pmatrix} 1 & -2 & 3 \\ -3 & 6 & -9 \\ 2 & -4 & 6 \\ -4 & 8 & -12 \end{pmatrix}$

3.4.4 Legyenek $\gamma_1, \ldots, \gamma_k$ és $\delta_1, \ldots, \delta_n$ tetszőleges komplex számok, és tekintsük azt a két $k \times n$-es mátrixot, amelyben az i-edik sor j-edik eleme

(a) $\gamma_i \delta_j$; (b) $\gamma_i + \delta_j$.

Számítsuk ki a mátrixok rangját.

3.4.5 Mennyi egy olyan mátrix rangja, amelynek minden sorában különböző (és nem nulla) hányadosú mértani sorozat áll?

3.4.6

(a) Bizonyítsuk be, hogy egy mátrix egy elemét megváltoztatva a rang legfeljebb 1-gyel változik.

(b) Igaz-e, hogy bármely mátrixban van olyan elem, amelyet alkalmasan módosítva a mátrix rangja megváltozik?

(c) Tekintsünk egy 10×20-as mátrixot, amelynek a rangja 5. Igaz-e, hogy mindenképpen van olyan elem, amelyet alkalmasan módosítva a mátrix rangja csökken?

(d) Tekintsünk egy 10×20-as mátrixot, amelynek a rangja 5. Igaz-e, hogy mindenképpen van olyan elem, amelyet alkalmasan módosítva a mátrix rangja nő?

3.4.7 Bizonyítsuk be, hogy egy ($k \times n$-es) mátrix rangja akkor és csak akkor 1, ha felírható egy nem nulla oszlopvektornak és egy nem nulla sorvektornak (azaz egy $k \times 1$-es és egy $1 \times n$-es nem nulla mátrixnak) a szorzataként. (Az ilyen szorzatokat *diád*oknak vagy *diadikus szorzat*oknak nevezzük.)

3.4.8 Legyen az A mátrix minden eleme 0 vagy 1. Ekkor A elemeit valós számoknak, racionális számoknak, illetve az F_2 modulo 2 test elemeinek tekintve három különböző ($\mathbf{R}^{k\times n}$-, $\mathbf{Q}^{k\times n}$-, illetve $F_2^{k\times n}$-beli) mátrixot kapunk. Milyen kapcsolatban áll egymással ennek a három mátrixnak a rangja?

3.4.9 Legyen A egy 7×6-os valós mátrix, B pedig az a 4×6-os mátrix, amely A első 4 sorából áll. Melyek igazak az alábbi állítások közül?

(a) Ha B első három oszlopa lineárisan független, akkor A első három oszlopa is lineárisan független.

(b) Ha B első három oszlopa lineárisan összefüggő, akkor A első három oszlopa is lineárisan összefüggő.

3.4.10 Igazoljuk, hogy ha egy mátrixban a sorok is lineárisan függetlenek és az oszlopok is lineárisan függetlenek, akkor négyzetes mátrixról van szó.

3.4.11 Legyen A egy 6×5-ös valós mátrix. Melyek igazak az alábbi állítások közül?

(a) Ha az első 3 sor lineárisan összefüggő, akkor a bal felső 3×3-as aldeterminánsa 0.

(b) Ha a bal felső 3×3-as aldeterminánsa 0, akkor az első 3 sor lineárisan összefüggő.

(c) Ha az első 3 oszlop lineárisan összefüggő és az utolsó 3 oszlop is lineárisan összefüggő, akkor a mátrix rangja legfeljebb 3.

(d) Ha az első 2 oszlop lineárisan összefüggő és az utolsó 2 oszlop is lineárisan összefüggő, akkor a mátrix rangja legfeljebb 3.

3.4.12 Mutassuk meg, hogy két (azonos test feletti, azonos alakú) mátrixnak akkor és csak akkor ugyanannyi a rangja, ha az egyik mátrixból elemi sor- és oszlopekvivalens átalakítások egymásutánjával megkaphatjuk a másik mátrixot.

3.4.13

(a) Adjunk példát olyan 5×7-es mátrixra, amelynek a rangja 4, és pontosan 8-féleképpen lehet az oszlopai közül 4 független kiválasztani.

(b) Bizonyítsuk be, hogy ha egy mátrix rangja r, és csak egyféleképpen lehet az oszlopai közül r független kiválasztani, akkor a többi oszlop csupa nullából áll.

M*(c) Legyen k, n tetszőleges és $1 \leq r \leq \min(n, k)$. Adjunk példát olyan $k \times n$-es mátrixra, amelynek a rangja r, és bármelyik r darab oszlop lineárisan független.

3.4.14

(a) Adjunk példát olyan 5×8-as mátrixra, amelynek a rangja 3, és pontosan 60 darab 3-adrendű nem nulla aldeterminánsa van.

(b) Bizonyítsuk be, hogy ha egy mátrix rangja r, és csak egyetlen r-edrendű nem nulla aldeterminánsa van, akkor ezen r^2 elemen kívül a mátrix minden eleme nulla.

M*(c) Legyen k, n tetszőleges és $1 \leq r \leq \min(n, k)$. Adjunk példát olyan $k \times n$-es mátrixra, amelynek a rangja r, és egyetlen r-edrendű aldeterminánsa sem nulla.

3.4.15 Melyek igazak az alábbi állítások közül?

(a) Ha az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer megoldható, akkor az $A|\mathbf{b}$ kibővített mátrix oszlopai lineárisan összefüggők.

(b) Ha az $A|\mathbf{b}$ kibővített mátrix oszlopai lineárisan összefüggők, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer megoldható.

(c) Ha az A mátrix oszlopai lineárisan függetlenek, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer megoldható.

(d) Ha az A mátrix sorai lineárisan függetlenek, akkor az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer megoldható.

(e) Ha az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek pontosan egy megoldása van, akkor az A mátrix oszlopai lineárisan függetlenek.

(f) Ha az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek pontosan egy megoldása van, akkor az A mátrix sorai lineárisan függetlenek.

3.4.16 Az A mátrixnak 10 sora van, ezek lineárisan függetlenek. Az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek pontosan 13 megoldása van. Hány oszlopa van A-nak?

*3.4.17

(a) Legyen az $A \in T^{n\times n}$ mátrix determinánsa nulla. Készítsük el azt a B mátrixot, amelynek elemei az A megfelelő előjeles aldeterminánsai, azaz $\beta_{ij} = A_{ij}$. Bizonyítsuk be, hogy $r(B) \leq 1$.

(b) (Vö. a 2.2.10 feladattal.) Ismételjük meg az a)-beli eljárást az ott kapott B mátrixra. Bizonyítsuk be, hogy $n > 2$ esetén az eredmény mindig a nullmátrix lesz.

M*3.4.18 Előáll-e minden valós mátrix olyan mátrixok összegeként, amelyek

(a) minden sora számtani sorozat;

(b) minden sora vagy minden oszlopa számtani sorozat;

(c) minden sora mértani sorozat?

M 3.4.19

(a) R és C a következő játékot játsszák. R megad egy k egyenletből álló, n ismeretlenes, a valós számokon értelmezett lineáris egyenletrendszert (k és n rögzített természetes számok), C pedig az együtthatók és a jobb oldali konstansok közül rendre egy-egy általa választott elemet akárhogyan megváltoztathat. Egy olyan egyenletrendszerhez kell így eljutnia, amelynek van megoldása. R-nek az a célja, hogy C ezt a lehető legtöbb lépésben érje el, C-nek pedig az, hogy a lehető legkevesebben. Mekkora lesz a lépésszám, ha mindketten optimálisan játszanak?

*(b) Oldjuk meg a feladatot arra az esetre is, ha C-nek egy olyan egyenletrendszerhez kell így eljutnia, amelynek nincs megoldása.

3.5. Reguláris és szinguláris mátrixok

Ebben a pontban visszatérünk a négyzetes mátrixok invertálhatóságával kapcsolatos kérdésekre és jelentősen kiegészítjük a 2.2 pontban tanultakat az egyenletrendszerek és a mátrixrang segítségével.

3.5.1 Definíció

Egy négyzetes mátrixot *szinguláris*nak (vagy *elfajuló*nak) nevezünk, ha a determinánsa nulla, és *reguláris*nak (vagy *nem szinguláris*nak, *nem elfajuló*nak), ha a determinánsa nem nulla. ♣

Számos ekvivalens feltételt bizonyítottunk egy mátrix regularitására, illetve szingularitására, először ezeket foglaljuk össze.

3.5.2 Tétel

Egy tetszőleges $A \in T^{n\times n}$ mátrixra az alábbi feltételek ekvivalensek (A ekkor reguláris):

(D) $\det A \neq 0$;
(I) A-nak létezik (kétoldali) inverze;
(bI) A-nak létezik balinverze;
(jI) A-nak létezik jobbinverze;
(nbN) A nem nulla és nem bal oldali nullosztó;
(njN) A nem nulla és nem jobb oldali nullosztó;
(T) az $A\mathbf{x} = \mathbf{0}$ homogén egyenletrendszernek csak triviális megoldása van;
(VE) van olyan $\mathbf{b}(\in T^n)$, amelyre az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek pontosan egy megoldása van;
(ME) bármely $\mathbf{b}(\in T^n)$-re az $A\mathbf{x} = \mathbf{b}$ egyenletrendszernek pontosan egy megoldása van;
(R) $r(A) = n$;
(OF) A oszlopai lineárisan függetlenek;
(SF) A sorai lineárisan függetlenek. ♣

Bizonyítás: A (D) feltétel éppen a regularitás definíciója. A többi feltételnek az ezzel való ekvivalenciáját az alábbi tételek biztosítják:

(I), (bI), (jI): 2.2.2 Tétel.

(nbN), (njN): 2.2.5 Tétel.

(T): 3.2.3 Tétel.

(VE), (ME): 3.2.2 Tétel és az utána tett megjegyzés.

(R), (OF), (SF): 3.4.2 Tétel. ■

A komplementer feltételek természetesen a szingularitás ekvivalens alakjait adják (érdemes ezeket is megfogalmazni).

Az alábbiakban megmutatjuk, hogy egy mátrix inverze közvetlenül is kapcsolódik az egyenletrendszerekhez. Ezzel egyrészt új bizonyítást nyerünk a 2.2.2 Tételre, másrészt lehetővé válik, hogy egy mátrix inverzét a Gauss-eliminációval számoljuk ki, ami általában lényegesen gyorsabban célhoz vezet, mint a 2.2.2 Tétel bizonyításában kapott képlet alkalmazása.

Az $A \in T^{n\times n}$ mátrix jobbinverzének a meghatározása az $AX = E$ mátrixegyenlet megoldását jelenti. Jelölje az X mátrix oszlopait $\mathbf{x}_1, \ldots, \mathbf{x}_n$, az E mátrix oszlopait pedig $\mathbf{e}_1, \ldots, \mathbf{e}_n$. Ekkor $AX = E$ átírható $A\mathbf{x}_1 = \mathbf{e}_1$, $\ldots, A\mathbf{x}_n = \mathbf{e}_n$ alakba. Így A^{-1} meghatározása ennek az n egyenletrendszernek a megoldását jelenti. Itt mind az n együtthatómátrix A.

Ha $\det A \neq 0$, akkor a 3.2.2 Tétel utáni megjegyzés szerint mindegyik egyenletrendszer (egyértelműen) megoldható, tehát A-nak létezik jobbinverze. (Azért nem a 3.2.1 Tételre hivatkoztunk, mert annak a bizonyítása felhasználta a 2.2.2 Tételt.)

Ha $\det A = 0$, akkor megmutatjuk, hogy legalább az egyik $A\mathbf{x}_j = \mathbf{e}_j$ egyenletrendszer nem oldható meg, tehát nem létezik A-nak jobbinverze. A 3.2.2 Tétel bizonyításában láttuk, hogy $\det A = 0$ esetén a Gauss-kiküszöböléssel (sorelhagyás nélkül) kapott RLA bal oldalának a determinánsa is nulla. Ez csak úgy lehet, ha az RLA-ban (legalább) az utolsó sor nulla, és így biztos létezik olyan $\mathbf{b} \in T^n$, amelyre az $A\mathbf{x} = \mathbf{b}$ egyenletrendszer nem oldható meg. Tegyük most fel indirekt, hogy mindegyik $A\mathbf{x}_j = \mathbf{e}_j$ megoldható lenne. Ekkor a megoldásoknak a $\mathbf{b}$ megfelelő komponenseivel vett lineáris kombinációja az $A\mathbf{x} = \mathbf{b}$ egy megoldását adná, ami ellentmondás.

A balinverzre vonatkozó eredmény azonnal adódik, ha az $YA = E$ mátrixegyenlet transzponálásával kapott, vele ekvivalens $A^T Y^T = E$ egyenletre alkalmazzuk az imént igazoltakat. Ezzel befejeztük a 2.2.2 Tétel egy új bizonyítását.

Nézzük most a fentiek alapján egy mátrix inverzének a számolását a gyakorlatban. Az $A\mathbf{x}_1 = \mathbf{e}_1, \ldots, A\mathbf{x}_n = \mathbf{e}_n$ egyenletrendszereket egyszerre is tudjuk kezelni, mivel közös az együtthatómátrixuk. Írjuk le az A-t (csak egy példányban), majd mellé a vonal után sorban az $\mathbf{e}_1, \ldots, \mathbf{e}_n$ vektorokat, azaz az A mellé tulajdonképpen az E egységmátrix kerül: $A|\mathbf{e}_1 \ldots \mathbf{e}_n = A|E$. Alkalmazzuk a Gauss-kiküszöbölést. Ha $\det A \neq 0$, akkor az A-ból kialakuló RLA az egységmátrix lesz, és ekkor a jobb oldalakból kapott rész éppen A^{-1}-et adja. Ha $\det A = 0$, akkor az A-ból képződő RLA utolsó sora csupa nulla lesz (és ez az n egyenletrendszer közül legalább az egyiknél tilos sort ad), ekkor nem létezik inverz. Azt, hogy $\det A$ nulla vagy nem nulla, NEM kellett külön előre kiszámítani, a Gauss-kiküszöbölés során automatikusan kiderült. Az eljárást az alábbi tételben foglaljuk össze:

3.5.3 Tétel

Az $A \in T^{n\times n}$ mátrix mellé írjuk le az $n \times n$-es E egységmátrixot, azaz tekintsük $A|E$-t. Az A-nak akkor és csak akkor létezik inverze, ha $A|E$-ből a Gauss-kiküszöböléssel $E|B$ alakú mátrixhoz jutunk, és ekkor $B = A^{-1}$. ♣

A fentiekhez hasonlóan a nullosztók vizsgálatát is közvetlenül összekapcsolhatjuk az egyenletrendszerekkel. Az A pontosan akkor bal oldali nullosztó, ha $A \neq 0$ és az $AX = 0$ mátrixegyenletnek van $X \neq 0$ megoldása. Jelöljük most is az X mátrix oszlopait $\mathbf{x}_1, \ldots, \mathbf{x}_n$-nel. Ekkor $AX = 0$ átírható $A\mathbf{x}_1 = \mathbf{0}, \ldots, A\mathbf{x}_n = \mathbf{0}$ alakba. Itt most az $A\mathbf{x} = \mathbf{0}$ homogén egyenletrendszer n

(teljesen azonos) példányáról van szó és így az $A \neq 0$ mátrix pontosan akkor bal oldali nullosztó, ha $A\mathbf{x} = \mathbf{0}$-nak van nem triviális megoldása. A 3.2.3 Tétel szerint ez pontosan akkor teljesül, ha $\det A = 0$. A másik oldali nullosztó esetét ugyanide vezethetjük vissza az inverznél látott transzponálási trükkel. Ezzel a 2.2.5 Tételre új bizonyítást adtunk.

Természetesen most sem kell magát a determinánst kiszámolni. Az, hogy $A\mathbf{x} = \mathbf{0}$-nak van-e nem triviális megoldása, (sima) Gauss-kiküszöböléssel eldönthető. A (triviális és esetleges nem triviális) megoldásokat egymástól függetlenül az X mátrix oszlopaiba beírva, megkapjuk az $AX = 0$ mátrixegyenlet összes megoldását (azaz $X = 0$-t mindenképpen, valamint ha A bal oldali nullosztó, akkor A összes jobb oldali nullosztó „párját").

A 2.2.5 Tételre még egy bizonyítást leolvashatunk a mátrix rangja segítségével. Az előbbiekből ismét felhasználjuk, hogy $A \neq 0$ akkor és csak akkor bal oldali nullosztó, ha $A\mathbf{x} = \mathbf{0}$-nak van nem triviális megoldása. Ez azzal ekvivalens, hogy A oszlopai lineárisan összefüggők, azaz (oszloprangot nézve) $r(A) < n$. Ugyanezt determinánsrangként tekintve kapjuk a $\det A = 0$ feltételt.

Feladatok

3.5.1 Számítsuk ki az alábbi (valós) mátrixok inverzét.

$$\text{(a)} \quad \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 1 \end{pmatrix} \qquad \text{(b)} \quad \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 6 & 10 \\ 1 & 4 & 10 & 20 \end{pmatrix}$$

3.5.2 Határozzuk meg az alábbi $n \times n$-es (valós) mátrixok inverzét:

$$A = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 1 & 1 & \dots & 1 \\ 1 & 1 & 2 & 1 & \dots & 1 \\ 1 & 1 & 1 & 2 & \dots & 1 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & 1 & 1 & \dots & 2 \end{pmatrix} \qquad B = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n \\ 0 & 1 & 2 & 3 & \dots & n-1 \\ 0 & 0 & 1 & 2 & \dots & n-2 \\ 0 & 0 & 0 & 1 & \dots & n-3 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

$$C = \begin{pmatrix} 1 & 1 & 1 & 1 & \dots & 1 \\ 1 & 2 & 2 & 2 & \dots & 2 \\ 1 & 2 & 3 & 3 & \dots & 3 \\ 1 & 2 & 3 & 4 & \dots & 4 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2 & 3 & 4 & \dots & n \end{pmatrix}$$

azaz $\alpha_{ij} = 2$, ha $i = j \geq 2$, és 1 egyébként; $\beta_{ij} = j - i + 1$, ha $i \leq j$, és 0 egyébként; $\gamma_{ij} = \min(i, j)$.

3.5.3 Keressük meg az alábbi valós A mátrixok összes jobb és bal oldali nullosztó párját, azaz az összes olyan 4×4-es X és Y (nem nulla) mátrixot, amelyre $AX = 0$, illetve $YA = 0$.

$$\text{(a)} \begin{pmatrix} 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \end{pmatrix} \qquad \text{(b)} \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 2 & 3 & 4 \\ 1 & 3 & 5 & 7 \\ 2 & 3 & 4 & 5 \end{pmatrix}$$

3.5.4 Egy $n \times n$-es $A \neq 0$ mátrix minden sorában az elemek összege nulla. Bizonyítsuk be, hogy A nullosztó, és adjunk meg olyan $B \neq 0$ mátrixot, amelyre $AB = 0$.

3.5.5 Döntsük el, hogy az alábbi $n \times n$-es valós mátrix milyen n-re invertálható, illetve milyen n-re nullosztó. Írjuk is fel az inverzét, illetve adjuk meg hozzá az összes „nullosztópárt”, azaz olyan nem nulla mátrixot, amellyel megszorozva a nullmátrixot kapjuk.

$$\begin{pmatrix} 1 & 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & 1 & \dots & 0 \\ 0 & 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 0 & 0 & 0 & \dots & 1 \end{pmatrix}$$

(A mátrixban $\alpha_{11} = \ldots = \alpha_{nn} = \alpha_{12} = \ldots = \alpha_{n-1,n} = \alpha_{n1} = 1$, minden más elem pedig nulla.)

3.5.6

(a) Legyen $A \in T^{n \times n}$ és jelölje $\mathbf{e}_j$ az $n \times n$-es egységmátrix j-edik oszlopát. Bizonyítsuk be, hogy ha az n darab $A\mathbf{x} = \mathbf{e}_j$ egyenletrendszer közül pontosan m oldható meg, akkor $r(A) \geq m$.

(b) Lássuk be, hogy (a)-ban általában nem igaz az egyenlőség: mutassunk példát olyan A-ra, amelynek a rangja $n - 1$, ugyanakkor az $A\mathbf{x} = \mathbf{e}_j$ egyenletrendszerek közül egyetlenegy sem oldható meg.

3.5.7 Legyen $A \in T^{n \times n}$, $\det A = 0$, és tegyük fel hogy az $A\mathbf{x} = \mathbf{0}$ és $A^T\mathbf{x} = \mathbf{0}$ egyenletrendszereknek ugyanazok a megoldásai. Következik-e ebből, hogy A szimmetrikus mátrix, azaz $A^T = A$?

3.5.8 Legyen $A \in T^{n\times n}$, $A \neq 0$ és $\det A = 0$.

(a) Mutassuk meg, hogy az A-hoz tartozó bal és jobb oldali nullosztópárok általában nem esnek egybe, azaz $AB = 0 \not\Rightarrow BA = 0$. ($B$ is $n \times n$-es mátrix.)

*(b) Igazoljuk, hogy mindig van olyan $B \neq 0$, amelyre $AB = BA = 0$.

M*(c) Adjuk meg az összes olyan A-t, amelyre $AB = 0 \iff BA = 0$.

4. VEKTORTEREK

A lineáris algebra a lineáris egyenletrendszerek elméletéből fejlődött ki. Láttuk, hogy az egyenletrendszerek kezelésében fontos szerepet játszottak a T^k-beli vektorok, pontosabban ezek bizonyos tulajdonságai. Ebben a fejezetben egy olyan algebrai struktúrát vezetünk be, a vektorteret, amely mindezeket általánosítja és absztrakt megközelítésben tárgyalja. A kapott eredményeket az egyenletrendszereken messze túlmenően rendkívül széles körben lehet alkalmazni a matematika különböző területein. Ezekből a 9. és 10. fejezetben adunk majd ízelítőt.

4.1. Vektortér

Legyen T egy tetszőleges kommutatív test (lásd az A.5.1 Definíciót). Legfontosabb példák: $\mathbf{R}$, $\mathbf{C}$, illetve $\mathbf{Q}$, azaz a valós, a komplex, illetve a racionális számok teste, valamint F_p, a modulo p maradékosztályok teste, ahol p prímszám.

A vektortér fogalmához a közönséges (sík- vagy tér)vektorok, illetve a T^k-beli vektorok összeadásának és skalárral való szorzásának a tulajdonságait általánosítjuk.

4.1.1 Definíció

Egy V nem üres halmazt *vektortér*nek nevezünk a T test felett, ha az alábbi kikötések (az ún. *vektortéraxiómák*) teljesülnek.

(Ö) A V halmazon értelmezve van egy *összeadás* nevű művelet: bármely $\mathbf{u}, \mathbf{v} \in V$ elempárhoz egyértelműen hozzárendelünk egy V-beli elemet, amelyet $\mathbf{u}+\mathbf{v}$-vel jelölünk.

(Ö1) Az összeadás *asszociatív*, azaz bármely $\mathbf{u}, \mathbf{v}, \mathbf{w} \in V$ elemekre

$$(\mathbf{u}+\mathbf{v})+\mathbf{w} = \mathbf{u}+(\mathbf{v}+\mathbf{w})\,.$$

(Ö2) Az összeadás *kommutatív*, azaz bármely $\mathbf{u}, \mathbf{v} \in V$ elemekre

$$\mathbf{u}+\mathbf{v} = \mathbf{v}+\mathbf{u}\,.$$

(Ö3) Létezik *nullelem*, azaz van olyan $\mathbf{0} \in V$, amellyel bármely $\mathbf{v} \in V$ elemre

$$\mathbf{0}+\mathbf{v} = \mathbf{v}+\mathbf{0} = \mathbf{v}\,.$$

(Ö4) Minden elemnek létezik *ellentett*je, azaz bármely $\mathbf{v} \in V$ elemhez létezik olyan $-\mathbf{v} \in V$, amelyre

$$\mathbf{v} + (-\mathbf{v}) = (-\mathbf{v}) + \mathbf{v} = \mathbf{0}\,.$$

(S) A T test és a V halmaz között értelmezve van egy *skalárral való szorzás*nak nevezett művelet az alábbi módon: bármely $\lambda \in T$ és $\mathbf{u} \in V$ elempárhoz egyértelműen hozzárendelünk egy V-beli elemet, amelyet $\lambda\mathbf{u}$-val jelölünk.

(S1) Bármely λ, $\mu \in T$ és $\mathbf{v} \in V$ esetén

$$(\lambda + \mu)\mathbf{v} = \lambda\mathbf{v} + \mu\mathbf{v}\,.$$

(S2) Bármely $\lambda \in T$ és $\mathbf{u}$, $\mathbf{v} \in V$ esetén

$$\lambda(\mathbf{u} + \mathbf{v}) = \lambda\mathbf{u} + \lambda\mathbf{v}\,.$$

(S3) Bármely λ, $\mu \in T$ és $\mathbf{v} \in V$ esetén

$$(\lambda\mu)\mathbf{v} = \lambda(\mu\mathbf{v})\,.$$

(S4) Bármely $\mathbf{v} \in V$-re

$$1\mathbf{v} = \mathbf{v}\,,$$

ahol 1 a T test egységeleme (azaz amellyel minden $\lambda \in T$-re $1\lambda = \lambda 1 = \lambda$). ♣

A V halmaz elemeit *vektor*oknak, a T test elemeit pedig *skalár*oknak nevezzük. A vektorokat általában félkövér latin kisbetűkkel, a skalárokat pedig legtöbbször görög kisbetűkkel fogjuk jelölni.

A fentiek szerint egy vektortér megadásához meg kell mondanunk a vektorok V halmazát, a T testet és értelmeznünk kell a két műveletet, az összeadást és a skalárral való szorzást. Ezután ellenőriznünk kell, hogy az (Ö1)–(Ö4) és az (S1)–(S4) axiómák teljesülnek-e.

Megjegyzések a vektortéraxiómákhoz

Az összeadás egy szokásos művelet, vagyis egy $V \times V \to V$ függvény. A skalárral való szorzás azonban az eddig megszokottaktól eltérően egy „öszvér” művelet; egy $T \times V \to V$ függvény.

Az összeadás tulajdonságait úgy foglalhatjuk össze, hogy V erre az összeadásra nézve egy kommutatív csoportot alkot.

Az (S1) axióma formailag a disztributivitásra emlékeztet, azonban a két $+$ különböző műveleteket jelöl: a bal oldali a T-beli, a jobb oldali pedig a V-beli összeadást. Hasonló problémát takar az (S3) axióma is.

A skalárral való szorzással kapcsolatban $\mathbf{v}\lambda$-ról nem beszélünk, csak $\lambda\mathbf{v}$-ről, a másikra nincs semmi szükség. Ha valakit ez (nagyon) zavar, akkor vagy úgy tekinti, hogy $\mathbf{v}\lambda$ a $\lambda\mathbf{v}$ egy alternatív jelölése, vagy pedig egy újabb műveletként vezeti be, és akkor az axiómák közé $\lambda\mathbf{v} = \mathbf{v}\lambda$-t is be kell venni.

A V-ről nem lett volna szükséges *külön* kikötni, hogy nem az üres halmaz, mert ezt a tulajdonságot az (Ö3) axióma biztosítja. Hasonló esetekben azonban a jövőben is inkább kitesszük a nem üres jelzőt, ezzel is hangsúlyozva, hogy általában egy algebrai struktúrán eleve nem üres halmazt értünk.

A vektortéraxiómák fenti rendszere a hagyományos megadást követi. Az axiómák közül (Ö2) elhagyható, mert levezethető a többi axiómából (lásd a 4.1.13 feladatot). Ettől eltekintve azonban a többi axióma független egymástól (lásd a 4.1.14 feladatot).

FONTOS! A vektortér keretében a vektorok között szorzást általában *nem* értelmezünk. Később azonban szerepelni fognak olyan *speciális* vektorterek, amelyeken valamilyen szorzást is bevezetünk: ilyenek lesznek egyfelől az *algebrák* (lásd az 5.6 pontot), másfelől az ún. *skalárszorzat*tal ellátott *euklideszi terek* (lásd a 8. fejezetet).

Példák vektortérre

P1. Az origóból kiinduló sík-, illetve térvektorok a valós test felett a szokásos vektorösszeadásra és a valós számmal való szorzásra nézve.

P2. T^k a T test felett, ha a műveleteket a szokásos módon komponensenként végezzük. (Az előző példa tulajdonképpen a $T = \mathbf{R}$ és $k = 2$, illetve $k = 3$ speciális esetnek felel meg.)

P3. $T^{k\times n}$, azaz a $k \times n$-es mátrixok a T test felett a mátrixok szokásos összeadására és skalárral való szorzására nézve. (Az előző példa az $n = 1$ speciális eset.)

P4. $T[x]$, azaz a T feletti polinomok a T felett a szokásos műveletekre nézve.

P5. Az összes valós számon értelmezett valós értékű függvények a valós test felett a szokásos műveletekre $[f+g : \alpha \mapsto f(\alpha)+g(\alpha)$ és $\lambda f : \alpha \mapsto \lambda f(\alpha)]$.

P6. A valós számsorozatok a valós test felett a szokásos műveletekre.

P7. A komplex számok a valós test felett a komplex számok körében értelmezett műveletekre.

További példák: lásd a 4.1.1–4.1.4 feladatokat.

A vektortéraxiómák következményei

A műveletek általános tulajdonságaiból (lásd az A.4 pontot) azonnal következik, hogy a nullvektor ($\mathbf{0}$) és minden vektornak az ellentettje *egyértelmű*, továbbá elvégezhető a *kivonás*, azaz bármely $\mathbf{u}, \mathbf{v} \in V$ vektorokhoz egyértelműen létezik olyan $\mathbf{w} \in V$ vektor, amelyre $\mathbf{v}+\mathbf{w} = \mathbf{u}$, ezt $\mathbf{w} = \mathbf{u}-\mathbf{v}$-vel jelöljük; a követelménynek eleget tevő (egyetlen) vektor: $\mathbf{w} = \mathbf{u} + (-\mathbf{v})$.

Az összeadás asszociativitása és kommutativitása miatt a többtagú összegek esetén a zárójelek elhagyhatók és a tagok sorrendje tetszőlegesen átírható.

A formálisan a disztributivitásra, illetve asszociativitásra emlékeztető (S1)–(S3) axiómák alapján a skalárral való szorzásnál is a megszokott szabályok alkalmazhatók (pl. „több tag szorzása több taggal").

További egyszerű, de fontos következményeket tartalmaz a

4.1.2 Tétel

(i) Bármely $\lambda \in T$-re $\lambda\mathbf{0} = \mathbf{0}$.
(ii) Bármely $\mathbf{v} \in V$-re $0\mathbf{v} = \mathbf{0}$, ahol a 0 a T test nulleleme.
(iii) Bármely $\mathbf{v} \in V$-re $(-1)\mathbf{v} = -\mathbf{v}$, ahol -1 a T test egységelemének az ellentettje (a testben).
(iv) Ha $\lambda\mathbf{v} = \mathbf{0}$, akkor $\lambda = 0$ vagy $\mathbf{v} = \mathbf{0}$. ♣

Bizonyítás: Az első állítást igazoljuk, a többi hasonló technikával történik (lásd a 4.1.10 feladatot). Legyen $\mathbf{v} \in V$ tetszőleges. Ekkor (Ö3) alapján $\mathbf{v} + \mathbf{0} = \mathbf{v}$. Szorozzuk meg ezt λ-val: $\lambda(\mathbf{v} + \mathbf{0}) = \lambda\mathbf{v}$. Itt a bal oldalt (S2) alapján átalakítjuk:

$$\lambda\mathbf{v} + \lambda\mathbf{0} = \lambda\mathbf{v}\,.$$

Adjuk most hozzá mindkét oldalhoz $\lambda\mathbf{v}$ ellentettjét, ekkor a jobb oldal $\mathbf{0}$ lesz, a bal oldal pedig

$$-\lambda\mathbf{v} + (\lambda\mathbf{v} + \lambda\mathbf{0}) = (-\lambda\mathbf{v} + \lambda\mathbf{v}) + \lambda\mathbf{0} = \mathbf{0} + \lambda\mathbf{0} = \lambda\mathbf{0}\,,$$

amivel (i)-et bebizonyítottuk. ■

Feladatok

4.1.1 Döntsük el, hogy a valós együtthatós polinomok alábbi részhalmazai vektorteret alkotnak-e a valós test felett, ha a műveleteket a szokásos módon definiáljuk. Egy általános polinomot f-fel, az f fokszámát $\deg f$-fel, az i-edfokú tag együtthatóját α_i-vel, a főegyütthatót α_n-nel jelöljük (tehát $\alpha_n \neq 0$, ha f nem a nullpolinom). A jelölésben nem teszünk különbséget polinom és polinomfüggvény között.

(a) $\{f \mid \deg f = 100 \text{ vagy } f = 0\}$;
(b) $\{f \mid \deg f \leq 100 \text{ vagy } f = 0\}$;
(c) $\{f \mid \deg f \geq 100 \text{ vagy } f = 0\}$;
(d) $\{f \mid x^3 + 1 \text{ osztója az } f\text{-nek}\}$;
(e) $\{f \mid x^3 + 1\text{-gyel osztva az } f \text{ konstans maradékot ad}\}$;
(f) $\{f \mid f(5) = 0\}$;
(g) $\{f \mid f(5) = 1\}$;
(h) $\{f \mid f(3) = 2f(4)\}$;
(i) $\{f \mid f \text{ együtthatóinak az összege } 0\}$;
(j) $\{f \mid \alpha_0 + \alpha_1 = 0\}$;
(k) $\{f \mid \alpha_0 + \alpha_n = 0\}$;
(l) $\{f \mid f\text{-nek van valós gyöke}\}$;
(m) $\{f \mid f \text{ minden együtthatója racionális}\}$.

4.1.2 Döntsük el, hogy a valós számsorozatok alábbi részhalmazai vektorteret alkotnak-e a valós test felett, ha a műveleteket a szokásos módon definiáljuk. Egy általános sorozatot $S = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ formában jelölünk.

(a) $\{S \mid \alpha_0 = 2\alpha_3 + \alpha_5\}$;
(b) $\{S \mid \alpha_0 = 2\alpha_3\alpha_5\}$;
(c) $\{S \mid \alpha_{n+1} = \alpha_n + \alpha_{n-1},\ n = 1, 2, \ldots\}$;
(d) a korlátos sorozatok;
(e) a konvergens sorozatok;
(f) $\{S \mid \lim_{n\to\infty} \alpha_n = 999\}$;
(g) a monoton növő sorozatok;
(h) a monoton sorozatok;
(i) $\{S \mid \alpha_i = 0$ végtelen sok i-re$\}$;
(j) $\{S \mid \alpha_i = 0$ legfeljebb véges sok i kivételével$\}$;
(k) $\{S \mid \alpha_i = 0$ legfeljebb 100 darab i kivételével$\}$;
(l) $\{S \mid \alpha_i = 0$ legfeljebb az első 100 darab i kivételével$\}$;
(m) a (végtelen) számtani sorozatok;
(n) a (végtelen) mértani sorozatok, megengedve a csupa 0 sorozatot is;
(o) a periodikus sorozatok.

4.1.3 Döntsük el, hogy az összes valós számon értelmezett valós értékű függvények alábbi részhalmazai vektorteret alkotnak-e a valós test felett, ha a műveleteket a szokásos módon definiáljuk. Egy általános függvényt f-fel jelölünk.

(a) A folytonos függvények;
(b) a legfeljebb véges sok pontban szakadó függvények;
(c) a legfeljebb öt pontban szakadó függvények;
(d) $\{f \mid f\text{-nek van valós gyöke}\}$;
(e) $\{f \mid f\text{-nek legfeljebb véges sok valós gyöke van}\}$;
(f) a páros függvények;
(g) a polinomfüggvények;
(h) a periodikus függvények;
(i) a felülről korlátos függvények;
(j) $\{f \mid f(5) \geq 0\}$;
(k) $\{f \mid f(5) = f(8)\}$;
(l) $\{f \mid \exists a \neq b\, f(a) = f(b)\}$;
(m) $\{f \mid f(\pi)$ egész szám$\}$.

4.1.4 Hogyan általánosíthatók a P5, P6 és P7 példákban szereplő vektorterek?

4.1.5 Legyen V a pozitív valós számok halmaza, $T = \mathbf{R}$, és definiáljuk az $\oplus$ összeadást és a $\odot$ skalárral való szorzást a következőképpen:

$$u \oplus v = uv, \quad \lambda \odot v = v^{\lambda},$$

ahol az egyenlőségek jobb oldalán a valós számok szokásos szorzása, illetve hatványozása szerepel ($u, v \in V, \lambda \in T$). Vektorteret kapunk-e így?

4.1.6 Legyen V a komplex számok halmaza, $T = \mathbf{Q}$, és definiáljuk az $\oplus$ összeadást és a $\odot$ skalárral való szorzást a következőképpen:

$$u \oplus v = u + v + 1, \quad \lambda \odot v = \lambda v + \lambda - 1,$$

ahol az egyenlőségek jobb oldalán a komplex számok szokásos összeadása, illetve szorzása szerepel ($u, v \in V, \lambda \in T$). Vektorteret kapunk-e így?

4.1.7 Legyen V az egész számok halmaza a szokásos összeadással és $T = \mathbf{Q}$. A $\odot$ skalárral való szorzást a következőképpen értelmezzük:

$$\lambda \odot v = \lfloor \lambda v \rfloor,$$

ahol az egyenlőség jobb oldalán a racionális számok szokásos szorzása szerepel és $\lfloor\ \rfloor$ a szám (alsó) egész részét jelöli ($v \in V$, $\lambda \in T$). Vektorteret kapunk-e így?

*4.1.8

(a) Legyen V az egész számok halmaza a szokásos összeadással és $T = \mathbf{Q}$. Lehet-e a $\odot$ skalárral való szorzást úgy értelmezni, hogy vektorteret kapjunk?

(b) Legyen V az egész számok halmaza a szokásos összeadással. Van-e olyan T test, amely fölött lehet a $\odot$ skalárral való szorzást úgy értelmezni, hogy vektorteret kapjunk?

(c) Legyen V az egész számok halmaza és $T = \mathbf{Q}$. Lehet-e az $\oplus$ összeadást és a $\odot$ skalárral való szorzást úgy értelmezni, hogy vektorteret kapjunk?

(d) Legyen V az egész számok halmaza és $T = \mathbf{C}$. Lehet-e az $\oplus$ összeadást és a $\odot$ skalárral való szorzást úgy értelmezni, hogy vektorteret kapjunk?

(e) Legyen V a valós számsorozatok halmaza a szokásos összeadással és $T = \mathbf{C}$. Lehet-e a $\odot$ skalárral való szorzást úgy értelmezni, hogy vektorteret kapjunk?

**(f) Legyen V a valós számok halmaza a szokásos összeadással és $T = \mathbf{C}$. Lehet-e a $\odot$ skalárral való szorzást úgy értelmezni, hogy vektorteret kapjunk?

4.1.9 Legyen V a komplex számsorozatok halmaza a szokásos összeadással és $T = \mathbf{C}$. Vizsgáljuk meg, hogy az alább értelmezett $\odot$ skalárral való szorzások mellett mely vektortéraxiómák teljesülnek és melyek nem. Egy általános sorozatot $S = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ formában jelölünk, az egyenlőségek jobb oldalán a komplex számok szokásos szorzása szerepel, $\mathrm{Re}(\lambda)$ a λ valós részét jelenti ($S \in V$, $\lambda \in T$).

(a) $\lambda \odot S = S$;

(b) $\lambda \odot S = (\lambda\alpha_0, \alpha_1, \alpha_2, \ldots)$;

(c) $\lambda \odot S = (\lambda\alpha_0, 0, 0, \ldots)$;

(d) $\lambda \odot S = (\mathrm{Re}(\lambda)\alpha_0, \mathrm{Re}(\lambda)\alpha_1, \mathrm{Re}(\lambda)\alpha_2, \ldots)$.

4.1.10 Bizonyítsuk be a 4.1.2 Tétel utolsó három állítását.

4.1.11 Melyek igazak az alábbi állítások közül? (V vektortér a T test felett, $\mathbf{u}$, $\mathbf{v} \in V$, λ, $\mu \in T$.)

(a) Ha $\mathbf{v} \neq \mathbf{0}$ és $\lambda\mathbf{v} = \mu\mathbf{v}$, akkor $\lambda = \mu$.
(b) Ha $\lambda \neq 0$ és $\lambda\mathbf{u} = \lambda\mathbf{v}$, akkor $\mathbf{u} = \mathbf{v}$.
(c) Ha $\mathbf{u} \neq \mathbf{0}$, $\mathbf{v} \neq \mathbf{0}$, $\lambda \neq 0$, $\mu \neq 0$ és $\lambda\mathbf{u} = \mu\mathbf{v}$, akkor $\mathbf{u} = \mathbf{v}$ és $\lambda = \mu$.

4.1.12 Bizonyítsuk be, hogy az (S4) vektortéraxióma helyettesíthető az alábbi két feltétel akármelyikével (vagyis ha az (S4)-et ezek akármelyikével kicseréljük, akkor a többi axiómával együtt pontosan ugyanahhoz a vektortérfogalomhoz jutunk).

(a) $\forall \mathbf{v} \in V \ \exists \lambda \in T \quad \lambda\mathbf{v} = \mathbf{v}$.
*(b) Ha $\lambda\mathbf{v} = \mathbf{0}$, akkor $\lambda = 0$ vagy $\mathbf{v} = \mathbf{0}$.

4.1.13 Bizonyítsuk be, hogy az összeadás kommutativitása következik a többi vektortéraxiómából.

*4.1.14 Bizonyítsuk be, hogy az összeadás kommutativitásától eltekintve a többi vektortéraxióma független egymástól, azaz egyik sem vezethető le az összes többiből. (Ezt úgy igazolhatjuk, ha példát mutatunk arra, amikor az az egy axióma nem teljesül, az összes többi viszont igen.)

4.2. Altér

4.2.1 Definíció

Egy T test feletti V vektortér egy nem üres $W \subseteq V$ részhalmazát *altér*nek nevezzük V-ben, ha W maga is vektortér *ugyanazon* T felett *ugyanazokra* a V-beli vektortérműveletekre (pontosabban ezeknek a műveleteknek a W-re történő megszorításaira) nézve. ♣

Azt, hogy W altér V-ben, szokás $W \leq V$ módon jelölni.

Vegyük észre, hogy az altér nem egyszerűen olyan részhalmaz, amely egyben vektortér is, hanem ennél jóval több: W *részstruktúrája* a V vektortérnek; a W szempontjából a T test és a műveletek eleve adottak. Ily módon pl. a 4.1.5 feladatban szereplő vektortér *nem* altere a valós számok önmaga feletti szokásos vektorterének.

Egy $W \subseteq V$ részhalmaz tehát akkor lesz altér, ha kielégíti az összes vektortéraxiómát. Lehet, hogy már magával (Ö)-vel és/vagy (S)-sel, vagyis a műveletek értelmezésével baj van, mert W nem *zárt* a V-beli műveletekre

vagy ezek valamelyikére, más szóval (legalább) az egyik V-beli művelet *kivezet* W-ből. Az alábbi tétel mutatja, hogy a műveleti zártság viszont már biztosítja az altérséget, azaz, ha a műveletek nem vezetnek ki, akkor a többi axiómával sem lehet baj.

4.2.2 Tétel

Egy T test feletti V vektortérben egy W nem üres részhalmaz akkor és csak akkor altér, ha

(i) $\mathbf{u}, \mathbf{v} \in W \Rightarrow \mathbf{u} + \mathbf{v} \in W$;
(ii) $\mathbf{v} \in W, \lambda \in T \Rightarrow \lambda\mathbf{v} \in W$. ♣

Bizonyítás: Ha W altér, akkor (i) és (ii) nyilván teljesülnek, hiszen — mint láttuk — ezek csak azt fejezik ki, hogy a V vektortér műveleteinek a megszorításai a W halmazon is műveletek.

A megfordításhoz be kell látnunk, hogy (i) és (ii) fennállása esetén a vektortéraxiómák mind teljesülnek. Az „azonosság típusú" axiómák, tehát (Ö1), (Ö2), (S1)–(S4) mindentől függetlenül V valamennyi elemére, így W elemeire is igazak. Azt kell tehát csak belátni, hogy W-ben van nullelem, és minden elemnek van ellentettje. Legyen $\mathbf{v} \in W$ tetszőleges (ilyen $\mathbf{v}$ elem létezik, hiszen $W \neq \emptyset$), ekkor (ii) miatt $\mathbf{0} = 0\mathbf{v} \in W$, és ez nyilván megfelel nullelemnek W-ben is. Ezután tetszőleges $\mathbf{v} \in W$-re $-\mathbf{v} = (-1)\mathbf{v} \in W$ eleget tesz az ellentett követelményének. ■

Megjegyezzük, hogy a 4.2.1 Definícióban a $W \neq \emptyset$ feltételt nem kellett volna *külön* előírni, hiszen egy vektortér eleve nem lehet az üres halmaz, azonban a 4.2.2 Tételnél nem hagyható el ez a kikötés, ugyanis az (i) és (ii) feltételeket az üres halmaz is teljesíti.

A tétel alapján így annak eldöntéséhez, hogy egy vektortér adott részhalmaza altér-e, nem kell valamennyi axiómát végignézni, hanem elég csupán a műveleti zártságot ellenőrizni. Egy másik jól használható kritériumot ad a 4.2.5 feladat a) része.

A tétel bizonyításából azt is kaptuk, hogy a W altér nulleleme megegyezik a V vektortér nullelemével, és hasonló a helyzet az ellentettel. Ez magából a nullelem fogalmából, sőt egyértelműségéből sem következik (lásd a 4.2.14 és 4.2.15 feladatokat).

Példák altérre

P1. Bármely vektortérben az egész tér, illetve a csak a $\mathbf{0}$ vektorból álló részhalmaz mindig altér. Ezeket *triviális alterek*nek nevezzük. (A csak a $\mathbf{0}$-ból

álló alteret $\{\mathbf{0}\}$ helyett röviden $\mathbf{0}$-val fogjuk jelölni, tehát ezt az alteret és magát a $\mathbf{0}$ vektort jelölésben nem fogjuk megkülönböztetni egymástól.)

P2. Jellemezzük az origóból kiinduló vektorokat a végpontjukkal. Ekkor a(z origóból induló) síkvektorok szokásos vektorterében pontosan az origón átmenő egyenesek a nem triviális alterek, a térvektorok esetében pedig az origón átmenő egyenesek és síkok.

P3. Bármely vektortérben egy tetszőleges, de rögzített vektor összes skalárszorosai mindig alteret alkotnak.

P4. Legyen $A \in T^{k\times n}$ egy tetszőleges, de rögzített $k \times n$-es mátrix. Ekkor $\operatorname{Ker} A = \{\mathbf{x} \in T^n \mid A\mathbf{x} = \mathbf{0}\}$ altér T^n-ben és $\operatorname{Im} A = \{A\mathbf{x} \mid \mathbf{x} \in T^n\} = \{\mathbf{y} \in T^k \mid \exists \mathbf{x} \in T^n \ A\mathbf{x} = \mathbf{y}\}$ altér T^k-ban. Ezt a két alteret az A mátrix *magterének*, illetve *képterének* hívjuk.

Feladatok

4.2.1 Mi köze van az altér fogalmához a 4.1.1–4.1.3 feladatoknak?

4.2.2 Legyen V a T test feletti 100×100-as mátrixok szokásos $T^{100\times100}$ vektortere. Az alábbi részhalmazok közül melyek alterek V-ben?

(a) $\{A \in V \mid AB = BA\}$, ahol $B \in T^{100\times100}$ egy rögzített mátrix;
(b) $\{A \in V \mid AB = 0\}$, ahol $B \in T^{100\times100}$ egy rögzített mátrix;
(c) $\{A \in V \mid A^2 = 0\}$;
(d) a nilpotens mátrixok (van olyan hatványuk, amelyik a 0 mátrix);
(e) a szinguláris mátrixok (beleértve a 0 mátrixot is);
(f) a 3 rangú mátrixok és a 0 mátrix;
(g) a legfeljebb 3 rangú mátrixok;
(h) a diagonális mátrixok (a főátlón kívül minden elem 0);
(i) a felsőháromszög-mátrixok (a főátló alatt minden elem 0);
(j) a szimmetrikus mátrixok (minden i, j-re $\alpha_{ij} = \alpha_{ji}$).

4.2.3 Milyen módszerrel lehet általában egy adott mátrix magterét és képterét meghatározni? Mi lesz $\operatorname{Ker} A$ és $\operatorname{Im} A$ az $A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 5 \\ 3 & 4 & 5 & 6 \end{pmatrix}$ mátrix esetén?

4.2.4 Adjunk példát olyan vektortérre és abban olyan részhalmazra, amely

(a) az összeadásra zárt, de a skalárral való szorzásra nem;
(b) a skalárral való szorzásra zárt, de az összeadásra nem;
(c) sem az összeadásra, sem a skalárral való szorzásra nem zárt.

Bármilyen test felett tudunk mindhárom esetre példát mutatni?

4.2.5 Legyen V vektortér a T test felett és W a V egy nem üres részhalmaza. Az alábbi feltételek közül melyekből következik, hogy W altér V-ben?

(a) $\mathbf{u}, \mathbf{v} \in W, \lambda, \mu \in T \Rightarrow \lambda\mathbf{u} + \mu\mathbf{v} \in W$;

(b) $\mathbf{u}, \mathbf{v} \in W, \lambda \in T \Rightarrow \lambda\mathbf{u} + \mathbf{v} \in W$;

(c) $\mathbf{u}, \mathbf{v} \in W, \lambda \in T \Rightarrow \lambda\mathbf{u} \in W$ és $\mathbf{u} - \mathbf{v} \in W$;

(d) $\mathbf{u}, \mathbf{v} \in W, \lambda \in T \Rightarrow \lambda\mathbf{u} \in W$ valamint $\mathbf{u}+\mathbf{v} \in W$ és $\mathbf{u}-\mathbf{v} \in W$ közül legalább az egyik teljesül;

(e) $\mathbf{u} + \mathbf{v} \in W \Rightarrow \mathbf{u} \in W$ és $\mathbf{v} \in W$;

(f) $\mathbf{u} + \mathbf{v} \in W \Rightarrow \mathbf{u} \in W$ és $\mathbf{v} \in W$ közül legalább az egyik teljesül.

4.2.6 Legyen V vektortér a T test felett és W a V egy nem triviális altere. Melyek igazak az alábbi állítások közül ($\mathbf{u}, \mathbf{v} \in V$, $\lambda \in T$)?

(a) $\mathbf{u} + \mathbf{v} \in W \Rightarrow \mathbf{u}, \mathbf{v} \in W$;

(b) $\lambda \neq 0$, $\lambda\mathbf{v} \in W \Rightarrow \mathbf{v} \in W$;

(c) $\mathbf{u} \in W$, $\mathbf{v} \notin W \Rightarrow \mathbf{u} + \mathbf{v} \notin W$;

(d) $\mathbf{u} \notin W$, $\mathbf{v} \notin W \Rightarrow \mathbf{u} + \mathbf{v} \notin W$;

(e) $\mathbf{u} \notin W$, $\mathbf{v} \notin W \Rightarrow \mathbf{u} + \mathbf{v} \in W$.

4.2.7 Legyen V vektortér $\mathbf{R}$ felett, W egy nem triviális altér V-ben és $\mathbf{u}, \mathbf{v} \in V$. Az alábbi feltételekből mi következik az $\mathbf{u}$, $\mathbf{v}$ vektorok és W viszonyára (tartalmazási szempontból)? Ha több eset is lehetséges, akkor ezek mindegyikére adjunk példát.

(a) $\mathbf{u} + \mathbf{v} \in W$; (b) $\mathbf{u} + \mathbf{v} \notin W$;

(c) $2\mathbf{u} + 3\mathbf{v} \in W$, $\mathbf{u} + 7\mathbf{v} \in W$; (d) $2\mathbf{u} + 3\mathbf{v} \in W$, $\mathbf{u} + 7\mathbf{v} \notin W$;

(e) $2\mathbf{u} + 3\mathbf{v} \notin W$, $\mathbf{u} + 7\mathbf{v} \notin W$.

Mennyiben változik a helyzet más test esetén?

4.2.8 Legyen W altér a valós test feletti V vektortérben, $\mathbf{u}$, $\mathbf{v}$, $\mathbf{w} \in V$, és tegyük fel, hogy

$$\mathbf{u} + \mathbf{v} \in W, \quad \mathbf{v} + 2\mathbf{w} \notin W, \quad \mathbf{w} + 3\mathbf{u} \in W.$$

Mit állíthatunk az $5\mathbf{u} + 3\mathbf{v} + \mathbf{w}$, illetve $6\mathbf{u} + 3\mathbf{v} + \mathbf{w}$ vektorok és W kapcsolatáról? (Az illető vektor biztosan eleme-e az altérnek, biztosan nem eleme az altérnek, vagy mindkét eset előfordulhat?)

4.2.9 Jellemezzük azokat a vektortereket, amelyeknek csak triviális alterei vannak.

4.2.10 Bizonyítsuk be, hogy ha egy végtelen test feletti vektortérnek van nem triviális altere, akkor végtelen sok altere van.

4.2.11 Hány altere van az F_2 test feletti F_2^2 vektortérnek? Hát az F_p test feletti F_p^2-nek? (A további általánosítást lásd a 4.6.14 feladatnál.)

4.2.12

(a) Bizonyítsuk be, hogy egy vektortérben akárhány altér metszete is altér.

(b) Adjunk szükséges és elégséges feltételt arra, hogy két altér egyesítése is altér legyen.

(c) Lehet-e két altér halmazelméleti különbsége vagy szimmetrikus differenciája altér?

*(d) Lehet-e három egymást páronként nem tartalmazó altér egyesítése altér?

M**(e) Legyen T végtelen test. Bizonyítsuk be, hogy egy T feletti vektortér nem állhat elő véges sok valódi alterének az egyesítéseként.

M**(f) Legyen T véges test. Bizonyítsuk be, hogy egy T feletti vektortér nem állhat elő $|T|+1$-nél kevesebb valódi alterének az egyesítéseként.

M**(g) Legyen T véges test. Bizonyítsuk be, hogy ha egy T feletti vektortérnek nem csak triviális alterei vannak, akkor előáll $|T|+1$ darab valódi alterének az egyesítéseként.

4.2.13 Legyen W altér a V vektortérben és $U \subseteq W$. Bizonyítsuk be, hogy U akkor és csak akkor altér V-ben, ha altér W-ben (vagyis az altérség nem függ attól, hogy „mekkora” az eredeti vektortér).

4.2.14 Legyen $V = \{c \in \mathbf{R} \mid c \geq 3\}$, $T = \mathbf{Q}$, és definiáljuk az $\oplus$ összeadást és a $\odot$ skalárral való szorzást a következőképpen:

$$u \oplus v = \max(u\,,\, v), \quad \lambda \odot v = v \quad (u,\, v \in V,\, \lambda \in T).$$

Legyen $W = \{c \in \mathbf{R} \mid c \geq 5\}$, ekkor W zárt a $\oplus$ és $\odot$ műveletekre. Továbbá V nulleleme a 3, W-é pedig az 5. Hogyan fér ez össze azzal, hogy egy altér nulleleme szükségképpen megegyezik a vektortér nullelemével (lásd a 4.2.2 Tétel bizonyítását)?

4.2.15 Az alábbiakban négy bizonyítást adunk arra, hogy egy altér nulleleme szükségképpen megegyezik a vektortér nullelemével, ezek közül azonban csak az egyik helyes. Melyik a helyes, és mi a hiba a többiben? (A V vektortér nullelemét $\mathbf{0}_V$, a W altérét pedig $\mathbf{0}_W$ jelöli.)

(a) Mivel $\mathbf{0}_V + \mathbf{v} = \mathbf{v}$ minden $\mathbf{v} \in V$ vektorra, tehát W elemeire is teljesül, ezért $\mathbf{0}_V$ definíció szerint W-nek is nulleleme. A W-beli nullelem egyértelműsége alapján így $\mathbf{0}_W = \mathbf{0}_V$.

(b) Ha $\mathbf{0}_W \neq \mathbf{0}_V$ lenne, akkor V-ben két nullelem lenne, ami ellentmond a V-beli nullelem egyértelműségének.

(c) Legyen $\mathbf{v} \in W$ tetszőleges. Ekkor $\mathbf{0}_V + \mathbf{v} = \mathbf{v}$ és $\mathbf{0}_W + \mathbf{v} = \mathbf{v}$ egyaránt fennáll, tehát $\mathbf{0}_V + \mathbf{v} = \mathbf{0}_W + \mathbf{v}$. Itt mindkét oldalhoz a $\mathbf{v}$ vektor W-beli ellentettjét hozzáadva a kívánt $\mathbf{0}_V = \mathbf{0}_W$ egyenlőséget kapjuk.

(d) Legyen $\mathbf{v} \in W$ tetszőleges. Ekkor $\mathbf{0}_V + \mathbf{v} = \mathbf{v}$ és $\mathbf{0}_W + \mathbf{v} = \mathbf{v}$ egyaránt fennáll, tehát $\mathbf{0}_V + \mathbf{v} = \mathbf{0}_W + \mathbf{v}$. Itt mindkét oldalhoz a $\mathbf{v}$ vektor V-beli ellentettjét hozzáadva a kívánt $\mathbf{0}_V = \mathbf{0}_W$ egyenlőséget kapjuk.

4.2.16 Legyen W altér a T test feletti V vektortérben és $\mathbf{u} \in V$ tetszőleges rögzített vektor. Az $\mathbf{u} + W = \{\mathbf{u} + \mathbf{w} \mid \mathbf{w} \in W\}$ halmazt a W altér *eltolt*jának vagy *lineáris sokaság*nak nevezzük.

(a) Adjuk meg a síkvektorok, illetve a térvektorok szokásos vektorterében az összes lineáris sokaságot.

(b) Bizonyítsuk be, hogy ugyanazon W altér szerint képzett két lineáris sokaság vagy diszjunkt, vagy egybeesik.

*(c) Bizonyítsuk be, hogy ha különböző alterek szerint képezünk két lineáris sokaságot, és ezek nem diszjunktak, akkor a metszetük is lineáris sokaság.

*(d) Bizonyítsuk be, hogy a nem üres $L \subseteq V$ akkor és csak akkor lineáris sokaság, ha

$$\mathbf{a}, \mathbf{b}, \mathbf{c} \in L,\ \lambda \in T \Rightarrow \mathbf{a} + \lambda(\mathbf{b} - \mathbf{c}) \in L\,.$$

*4.2.17 Legyen W altér a T test feletti V vektortérben, és tekintsük a W szerint képezett lineáris sokaságok, vagyis W összes (különböző) eltoltjainak az F halmazát. Definiáljuk F-en az $\oplus$ összeadást és a $\odot$ skalárral való szorzást a következőképpen:

$$(\mathbf{u} + W) \oplus (\mathbf{v} + W) = (\mathbf{u} + \mathbf{v}) + W, \quad \lambda \odot (\mathbf{u} + W) = \lambda\mathbf{u} + W.$$

Bizonyítsuk be, hogy ezekre a műveletekre F vektorteret alkot a T test felett. Ezt a teret a V vektortér W altere szerint vett *faktortér*nek nevezzük, és V/W-vel jelöljük.

4.3. Generálás

4.3.1 Definíció

Legyen V vektortér a T test felett, $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$, $\lambda_1, \ldots \lambda_n \in T$. A $\lambda_1\mathbf{a}_1 + \ldots + \lambda_n\mathbf{a}_n$ vektort az $\mathbf{a}_i$ vektorok (λ_i skalárokkal képzett) *lineáris kombináció*jának nevezzük. ♣

Ismeretes, hogy a (közönséges háromdimenziós) térben három (vagy több) rögzített, nem egy síkba eső vektor lineáris kombinációjaként a tér minden vektora előállítható. Ezt a tényt szokás úgy is kifejezni, hogy az adott vektorok *kifeszítik* vagy *generálják* a teret. Tetszőleges vektortérre a megfelelő általánosítást az alábbi definíció szolgáltatja.

4.3.2 Definíció

Az $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$ vektorokat a V vektortér *generátorrendszer*ének nevezzük, ha V minden eleme előáll az $\mathbf{a}_i$ vektorok lineáris kombinációjaként.

♣

A „rendszer" szó arra utal, hogy (a halmazzal ellentétben) ugyanaz a vektor többször is előfordulhat az $\mathbf{a}_i$-k között. A generátorrendszer fogalmánál azonban ennek nemigen van jelentősége, ugyanis a lineáris kombinációk halmazát nyilván nem befolyásolja, ha (a többi vektor változatlanul hagyása mellett) valamelyik vektort egy vagy több példányban szerepeltetjük. (A lineáris függetlenség kérdésénél más a helyzet, lásd a 3.3, illetve 4.4 pontban.)

A vektortér elemei általában többféleképpen is felírhatók egy adott generátorrendszer elemeinek lineáris kombinációjaként. Később látni fogjuk, hogy különösen fontos szerepet játszanak az olyan generátorrendszerek, amelyek segítségével a vektortér minden eleme *egyértelműen* állítható elő, ezek az ún. *bázis*ok (lásd a 4.5 pontot).

Egy vektortérnek általában nagyon sok generátorrendszere lehet, gyakran előfordul azonban az is, hogy egyáltalán nincs (véges) generátorrendszere (lásd a 4.3.2 feladatot). A végtelen generátorrendszer bevezetésének a lehetőségét ennek a pontnak a végén fogjuk jelezni. Néhány, külön jelzett helytől eltekintve azonban generátorrendszeren mindig véges sok (de legalább egy) elemből álló generátorrendszert fogunk érteni.

Az $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$ vektorok összes lineáris kombinációinak a halmaza abban az esetben is fontos szerepet játszik, ha az $\mathbf{a}_i$ vektorok nem alkotnak generátorrendszert. Ez indokolja a következő definíciót.

4.3.3 Definíció

Az $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$ vektorok által *generált altér*en az $\mathbf{a}_i$ vektorok összes lineáris kombinációinak a halmazát értjük, és ezt $\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$-nel jelöljük. Azaz:

$$\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle = \{ \lambda_1 \mathbf{a}_1 + \ldots + \lambda_n \mathbf{a}_n \mid \lambda_1, \ldots, \lambda_n \in T \} \,. \ \clubsuit$$

A definíció alapján pl. az egy vektor által generált altér az adott vektor összes skalárszorosaiból áll. A (közönséges háromdimenziós) térben két nem egy egyenesbe eső vektor által generált altér az általuk „kifeszített" sík. Az is nyilvánvaló, hogy az $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$ vektorok pontosan akkor alkotnak generátorrendszert V-ben, ha $\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle = V$.

A „generált altér" elnevezés jogosságát az alábbi tétel támasztja alá:

4.3.4 Tétel

$U = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$ az $\mathbf{a}_i$ vektorokat tartalmazó *legszűkebb* altér, azaz

(i) U altér;

(ii) $\mathbf{a}_i \in U, \quad i = 1, \ldots, n$;

(iii) ha W altér és $\mathbf{a}_i \in W, \quad i = 1, \ldots, n$, akkor $U \subseteq W$. $\clubsuit$

Bizonyítás: (i) Egyszerű számolással adódik, hogy a lineáris kombinációk halmaza altér. (ii) A $\lambda_i = 1$, $\lambda_j = 0$, ha $j \neq i$ skalárokkal képezett lineáris kombináció éppen $\mathbf{a}_i$, tehát ez az altér tartalmazza az $\mathbf{a}_i$ vektorokat. Végül (iii): Ha egy W altér tartalmazza az $\mathbf{a}_i$ vektorokat, akkor ezek skalárszorosait, majd az ezekből képezett összegeket is tartalmaznia kell. Vagyis minden lineáris kombináció szükségképpen eleme W-nek. ■

Megjegyezzük, hogy szokás a generált altér fogalmát éppen az (i)–(iii) tulajdonságokkal *definiálni*. A kétféle definíció ekvivalenciáját a 4.3.4 Tétel biztosítja. A generált altér egy harmadik jellemzését lásd a 4.3.9 feladatban.

Külön kiemeljük, hogy egy altér generátorrendszere mindig magának az altérnek az elemeiből kell, hogy álljon, „külső" elemek nem jöhetnek szóba (ez nyilvánvalóan adódik pl. a 4.3.4 Tétel (ii) állításából).

Most a két altér által generált altér fogalmát vezetjük be.

4.3.5 Definíció

Legyenek W és Z alterek a V vektortérben. A W és Z által generált altérnek a $\{\mathbf{w} + \mathbf{z} \mid \mathbf{w} \in W, \mathbf{z} \in Z\}$ alteret nevezzük, és ezt $\langle W, Z \rangle$-vel vagy $W + Z$-vel jelöljük. $\clubsuit$

A 4.3.4 Tételhez hasonlóan adódik, hogy $\langle W, Z\rangle$ éppen a két alteret tartalmazó legszűkebb altér (lásd a 4.3.11 feladatot).

Fontos az az eset, amikor $\langle W, Z\rangle$ elemei *egyértelműen* írhatók fel $\mathbf{w}+\mathbf{z}$ alakban ($\mathbf{w}\in W$, $\mathbf{z}\in Z$). Erre vonatkozik a következő tétel.

4.3.6 Tétel

Legyenek W és Z alterek V-ben. A $\langle W, Z\rangle$ altér elemeinek $\mathbf{w}+\mathbf{z}$ alakban történő előállítása (ahol $\mathbf{w}\in W$, $\mathbf{z}\in Z$) akkor és csak akkor egyértelmű, ha $W\cap Z=\mathbf{0}$. ♣

Bizonyítás: Tegyük fel először, hogy $W\cap Z=\mathbf{0}$ és valamely $\mathbf{x}\in\langle W, Z\rangle$-re

$$\mathbf{x}=\mathbf{w}_1+\mathbf{z}_1=\mathbf{w}_2+\mathbf{z}_2,\ \text{ ahol }\ \mathbf{w}_i\in W,\ \mathbf{z}_i\in Z\,.$$

Az egyenlőséget átrendezve $\mathbf{w}_1-\mathbf{w}_2=\mathbf{z}_2-\mathbf{z}_1$ adódik. Itt a bal oldalon W-beli, a jobb oldalon pedig Z-beli vektor áll, tehát a feltétel miatt ez csak a $\mathbf{0}$ lehet. Vagyis $\mathbf{w}_1=\mathbf{w}_2$, $\mathbf{z}_1=\mathbf{z}_2$, amivel az egyértelműséget igazoltuk.

Megfordítva, tegyük fel, hogy minden vektor egyértelműen áll elő a kívánt alakban, és legyen $\mathbf{u}\in W\cap Z$. Ekkor $\mathbf{u}=\mathbf{u}+\mathbf{0}=\mathbf{0}+\mathbf{u}$ két különböző előállítást jelent, ha $\mathbf{u}\neq\mathbf{0}$. Vagyis csak $\mathbf{u}=\mathbf{0}$ lehetséges, azaz valóban $W\cap Z=\mathbf{0}$. ■

A $W\cap Z=\mathbf{0}$ esetben a W és Z altereket *diszjunkt*aknak nevezzük (ennél „diszjunktabbak” nem lehetnek, hiszen a $\mathbf{0}$ vektor bármely altérnek eleme).

4.3.7 Definíció

Ha $W\cap Z=\mathbf{0}$, akkor a $\langle W, Z\rangle$ alteret a W és Z *direkt összeg*ének hívjuk, és $W\oplus Z$-vel jelöljük. ♣

Direkt összegről tehát csak diszjunkt alterek esetén beszélhetünk.

Végtelen sok vektor generátuma

A problémát ekkor az jelenti, hogy végtelen sok vektor összegét (általában) nem tudjuk értelmezni. Tekinthetjük azonban az adott vektorok összes *véges* részhalmazának összes lineáris kombinációit:

4.3.8 Definíció

Legyen H a T test feletti V vektortér tetszőleges nem üres részhalmaza. Ekkor a H által generált $\langle H\rangle$ altéren a H halmaz elemeivel minden lehetséges

módon képezett összes (véges, de tetszőlegesen hosszú) lineáris kombinációt értjük. ♣

Most is megmutatható, hogy $\langle H\rangle$ az a legszűkebb altér, amely H-t tartalmazza. Az is könnyen adódik, hogy ha W és Z alterek, akkor $\langle W, Z\rangle = \langle W \cup Z\rangle$.

Ebben az általánosabb értelemben egy $H \subseteq V$ részhalmaz akkor *generátorrendszere* V-nek, ha $\langle H\rangle = V$. Más megfogalmazásban ez azt jelenti, hogy bármely $\mathbf{v} \in V$ vektorhoz található véges sok olyan H-beli vektor, hogy $\mathbf{v}$ felírható ezek alkalmas lineáris kombinációjaként. Más és más $\mathbf{v}$-hez általában más és más H-beli vektorok tartoznak, sőt többnyire még ezek darabszáma sem lesz korlátos.

Ily módon már bármely V vektortérnek létezik generátorrendszere, hiszen pl. nyilvánvalóan $V = \langle V\rangle$.

A végesben megszokott szemléletünk most csalóka lehet: a valós együtthatós polinomok szokásos vektorterében az 1, x, x^2, ... polinomok — a várakozásunknak megfelelően — generátorrendszert alkotnak, azonban a valós számsorozatok szokásos vektorterében *nem* alkotnak generátorrendszert azok a sorozatok, amelyeknek egyetlen tagja 1, a többi pedig 0, ugyanis ilyenek *véges* lineáris kombinációjaként nem áll elő például a csupa 1-ből álló sorozat.

Feladatok

4.3.1 Az alábbi vektorrendszerek közül melyek alkotnak a szokásos $\mathbf{C}^4$ vektortérben generátorrendszert?

(a) $\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}, \begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\1\\1\\1\end{pmatrix}$;

(b) $\begin{pmatrix}1\\-1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\-1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\0\\1\\-1\end{pmatrix}$;

(c) $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\2\\4\\8\end{pmatrix}, \begin{pmatrix}1\\3\\9\\27\end{pmatrix}, \begin{pmatrix}1\\4\\16\\64\end{pmatrix}$.

4.3.2 A 4.1 pontban, valamint a 4.1.1–4.1.3 feladatokban szereplő példák közül mely vektortereknek van véges generátorrendszere?

4.3.3 Melyek igazak az alábbi állítások közül?

(a) Ha egy generátorrendszerhez egy tetszőleges vektort hozzáveszünk, akkor ismét generátorrendszert kapunk.

(b) Ha egy legalább kételemű generátorrendszerből egy tetszőleges vektort elhagyunk, akkor ismét generátorrendszert kapunk.

(c) Minden legalább kételemű generátorrendszerben van olyan vektor, amelyet elhagyva a maradék vektorok továbbra is generátorrendszert alkotnak.

(d) Ha egy generátorrendszerben előfordul két azonos vektor, akkor ezek egyik példányát elhagyva a maradék vektorok továbbra is generátorrendszert alkotnak.

(e) Egy legalább kételemű generátorrendszerben akkor és csak akkor van olyan vektor, amelyet elhagyva a maradék vektorok továbbra is generátorrendszert alkotnak, ha a generátorrendszer valamelyik eleme felírható a többi elem lineáris kombinációjaként.

4.3.4 Legyen V a valós együtthatós polinomok szokásos vektortere. Melyek igazak az alábbi tartalmazások közül?

(a) $x^3 + 7x^2 + 5x \in \langle x^3 + 2x, 3x^3 + 4x, 5x^2 + 6x \rangle$;

(b) $x^3 + 7x^2 + 5 \in \langle x^3 + 2x, 3x^3 + 4x, 5x^2 + 6x \rangle$;

(c) $x - 1 \in \langle x^3 - x, x^3 - x^2, x^3 - 1, 2x^2 - 3x + 1 \rangle$;

(d) $x + 1 \in \langle x^3 - x, x^3 - x^2, x^3 - 1, 2x^2 - 3x + 1 \rangle$;

(e) $x + 1 \in \langle x^3 - x, x^3 - x^2, x^3 - 1, 2x^2 + 3x + 1 \rangle$.

4.3.5 Tegyük fel, hogy egy V vektortér $\mathbf{a}$, $\mathbf{b}$ és $\mathbf{c}$ elemeire $\mathbf{a} + \mathbf{b} + \mathbf{c} = \mathbf{0}$. Bizonyítsuk be, hogy $\langle \mathbf{a}, \mathbf{b} \rangle = \langle \mathbf{a}, \mathbf{c} \rangle$.

4.3.6 Tegyük fel, hogy egy V vektortér $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ és $\mathbf{d}$ elemeire $\mathbf{a}+\mathbf{b}+\mathbf{c}+\mathbf{d} = \mathbf{0}$. Melyek igazak az alábbi állítások közül?

(a) $\langle \mathbf{a}, \mathbf{b} \rangle = \langle \mathbf{a}, \mathbf{c} \rangle$; (b) $\langle \mathbf{a}, \mathbf{b} \rangle = \langle \mathbf{c}, \mathbf{d} \rangle$; (c) $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle = \langle \mathbf{a}, \mathbf{c}, \mathbf{d} \rangle$;

(d) $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle = \langle \mathbf{a}, \mathbf{d} \rangle$; (e) $\langle \mathbf{a}, \mathbf{b}, \mathbf{c} \rangle \supseteq \langle \mathbf{a}, \mathbf{d} \rangle$.

4.3.7 Tegyük fel, hogy egy V vektortér $\mathbf{a}, \mathbf{b}$ és $\mathbf{c}$ elemeire $\mathbf{a} \notin \langle \mathbf{b}, \mathbf{c} \rangle$, $\mathbf{b} \notin \langle \mathbf{a}, \mathbf{c} \rangle$ és $\mathbf{c} \in \langle \mathbf{a}, \mathbf{b} \rangle$. Határozzuk meg a $\mathbf{c}$ vektort.

4.3.8 Bizonyítsuk be, hogy adott $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$ vektorok esetén csak egy olyan U létezik, amely kielégíti a 4.3.4 Tétel (i)–(iii) követelményeit.

4.3.9 Bizonyítsuk be, hogy az $\mathbf{a}_1, \ldots, \mathbf{a}_n \in V$ vektorok által generált altér megegyezik az $\mathbf{a}_i$-ket tartalmazó összes altér metszetével.

4.3.10 Legyen V az összes valós számon értelmezett valós értékű függvények szokásos vektortere. Egy általános függvényt f-fel jelölünk. Jellemezzük a W és Z alterek által generált $\langle W, Z\rangle$ alteret, ahol

(a) $W = \{\text{páros függvények}\}, \quad Z = \{\text{páratlan függvények}\}$;

(b) $W = \{f \mid f(5) = 0\}, \quad Z = \{f \mid f(6) = 0\}$;

(c) $W = \{f \mid f(x) = 0, \text{ ha } x \neq 5\}, \quad Z = \{f \mid f(x) = 0, \text{ ha } x \neq 6\}$;

(d) $W = \{f \mid \forall\, x \in \mathbf{Q} \;\; f(x) = 0\}, \quad Z = \{f \mid \forall\, x \notin \mathbf{Q} \;\; f(x) = 0\}$;

(e) $W = \{f \mid \forall\, x,\, y \in \mathbf{Q} \;\; f(x) = f(y)\}$,
$Z \;\; = \{f \mid \forall\, x,\, y \notin \mathbf{Q} \;\; f(x) = f(y)\}$.
Mely esetekben lesz $\langle W, Z\rangle = W \oplus Z$?

4.3.11 Legyenek W és Z alterek V-ben. Bizonyítsuk be, hogy $\langle W, Z\rangle$ éppen a két alteret tartalmazó legszűkebb altér. (Fogalmazzuk meg pontosan, hogy mit jelent a „legszűkebbség”.)

4.3.12 Legyenek W_1, W_2 és W_3 alterek V-ben. Milyen kapcsolatban áll egymással

(a) $\langle W_1, W_2\rangle \cap W_3$ és $\langle W_1 \cap W_3, W_2 \cap W_3\rangle$;

(b) $\langle W_1 \cap W_2\,,\, W_3\rangle$ és $\langle W_1, W_3\rangle \cap \langle W_2, W_3\rangle$;

(c) $W_1 \subseteq W_3$ esetén $\langle W_1, W_2\rangle \cap W_3$ és $\langle W_1\,,\, W_2 \cap W_3\rangle$?

4.3.13 Legyen V a valós számsorozatok szokásos vektortere. Egy általános sorozatot $S = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ formában jelölünk. Döntsük el, hogy V direkt összege-e W-nek és Z-nek, ahol

(a) $W = \{S \mid \alpha_5 = 0\}, \quad Z = \{S \mid \alpha_6 = 0\}$;

(b) $W = \{S \mid \alpha_5 = 0\}, \quad Z = \{S \mid \alpha_i = 0, \text{ ha } i \neq 5\}$;

(c) $W = \{S \mid \alpha_5 = 0\}, \quad Z = \{S \mid \alpha_1 = \ldots = \alpha_5,\, \alpha_6 = \alpha_7 = \ldots = 0\}$;

(d) $W = \{S \mid \alpha_5 = 0\}, \quad Z = \{S \mid \alpha_5 \neq 0\}$;

(e) $W = \{S \mid \alpha_i = 0, \text{ ha } i \text{ páros}\}, \quad Z = \{S \mid \alpha_i = 0, \text{ ha } i \text{ páratlan}\}$;

(f) $W = \{S \mid \alpha_i = 0, \text{ ha } i \neq 5\}, \quad Z = \{S \mid \alpha_i = 0, \text{ ha } i \neq 6\}$.

*4.3.14 Általánosítsuk a 4.3.5 Definíciót és a 4.3.6 Tételt kettőnél több (de véges sok) altérre, majd ennek alapján a direkt összeg fogalmát is (4.3.7 Definíció) terjesszük ki kettőnél több altér esetére.

*4.3.15 Adjuk meg a 4.1.1–4.1.3 feladatokban szereplő részhalmazok által generált altereket, kivéve a 4.1.2 feladat (n) és a 4.1.3 feladat (h) részét.

*4.3.16 Tekintsük az összes valós számon értelmezett valós értékű függvényeket a *racionális* test feletti vektortérként a szokásos műveletekre. Legyen ebben H az egész értékű függvények halmaza. Döntsük el, hogy az alábbi függvények elemei-e a H által generált $\langle H \rangle$ altérnek.

(a) $f(x) = \begin{cases} 5/7, & \text{ha } x \in \mathbf{Q}; \\ 3/8, & \text{ha } x \notin \mathbf{Q}. \end{cases}$

(b) $g(x) = \begin{cases} 1/x, & \text{ha } x = 1, 2, 3, \ldots; \\ 0, & \text{egyébként.} \end{cases}$

**(c) Oldjuk meg a feladatot abban az esetben is, ha a racionális test helyett a valós testet vesszük.

4.3.17 Tekintsük a valós számsorozatok szokásos V vektorterét a valós test felett. Generátorrendszert alkotnak-e V-ben az alábbi részhalmazok?

(a) Azok a sorozatok, amelyeknek minden eleme 0 vagy 1;

**(b) azok a sorozatok, amelyeknek minden eleme racionális;

(c) azok a sorozatok, amelyeknek minden eleme irracionális.

4.4. Lineáris függetlenség

A lineáris függetlenség és összefüggés fogalmával speciális esetben a mátrixok és egyenletrendszerek kapcsán a 3. fejezetben már foglalkoztunk. Az ott megismert definíciók szó szerint átvihetők tetszőleges vektortérre, és az alaptulajdonságok is érvényben maradnak. Most mindezeket röviden összefoglaljuk.

Legyen V vektortér a T test felett, $\mathbf{u}_1, \ldots, \mathbf{u}_n \in V$, $\lambda_1, \ldots \lambda_n \in T$, és tekintsük a $\lambda_1\mathbf{u}_1 + \ldots + \lambda_n\mathbf{u}_n$ lineáris kombinációt. Ha minden $\lambda_i = 0$, akkor ez az ún. *triviális* lineáris kombináció nyilván a $\mathbf{0}$ vektort eredményezi. Előfordulhat azonban, hogy a $\mathbf{0}$ vektort más együtthatókkal, *nem triviális* lineáris kombinációként is megkaphatjuk. Ebben az esetben az $\mathbf{u}_i$ vektorokat *lineárisan összefüggő*nek, ellenkező esetben pedig *lineárisan független*nek nevezzük. Azaz

4.4.1 Definíció

Az $\mathbf{u}_1, \ldots, \mathbf{u}_m \in V$ vektorok *lineárisan összefüggő*k, ha léteznek olyan $\lambda_1, \ldots, \lambda_m \in T$ skalárok, amelyek nem mind 0-k, és $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$. ♣

4.4.2 Definíció

Az $\mathbf{u}_1, \ldots, \mathbf{u}_m \in V$ vektorok *lineárisan független*ek, ha $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$ **CSAK** úgy valósulhat meg, ha mindegyik $\lambda_i = 0$. Azaz

$$\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0} \Rightarrow \lambda_i = 0,\ i = 1, \ldots, m. \ \clubsuit$$

Egy $\mathbf{u}_1, \ldots, \mathbf{u}_m \in V$ vektorrendszerre tehát a lineáris függetlenség és a lineáris összefüggés közül pontosan az egyik teljesül. A „lineáris" jelzőt a rövidség kedvéért gyakran elhagyjuk.

Ismét megemlítjük, hogy a „vektorrendszer" kifejezésben a „rendszer" szó arra utal, hogy (a halmazzal ellentétben) ugyanaz a vektor többször is előfordulhat az $\mathbf{u}_i$-k között. Ez a körülmény lényegesen befolyásol(hat)ja a függetlenség kérdését: ha az $\mathbf{u}_i$-k között szerepelnek azonos vektorok, akkor a vektorrendszer biztosan összefüggő.

Azonnal adódnak az alábbi egyszerű észrevételek. Egyetlen vektor egyedül akkor és csak akkor független, ha nem a nullvektor. Két vektor akkor és csak akkor lineárisan független, ha egyik sem skalárszorosa a másiknak. Több vektor esetén ez már *nem igaz*: például a síkban tetszőleges három vektor összefüggő.

FONTOS! A lineáris függetlenség fogalma számos „csapdát" rejt, ezért — főleg az elején — célszerű ezzel kapcsolatban mindent nagyon alaposan végiggondolni, nehogy egy hibás „szemlélet" alapján téves elképzelések alakuljanak ki.

A 3.3.5 Tétel tetszőleges vektortérben ugyanúgy érvényes:

4.4.3 Tétel

I. Ha egy (legalább kételemű) lineárisan független rendszerből egy tetszőleges elemet elhagyunk, akkor a maradék vektorok is lineárisan független rendszert alkotnak.

II. Ha egy lineárisan összefüggő rendszerhez egy tetszőleges vektort hozzáveszünk, akkor az így kapott vektorrendszer is lineárisan összefüggő.

III. Egy legalább kételemű vektorrendszer akkor és csak akkor lineárisan összefüggő, ha van benne (*legalább* egy) olyan vektor, amely előáll a többi vektor lineáris kombinációjaként.

IV. Ha $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független, de az $\mathbf{u}_{m+1}$ vektor hozzávételével kapott rendszer lineárisan összefüggő, akkor $\mathbf{u}_{m+1}$ előáll az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineáris kombinációjaként.

V. Tegyük fel, hogy valamely $\mathbf{v}$ vektor előáll az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineáris kombinációjaként. Ez az előállítás akkor és csak akkor egyértelmű, ha $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független. ♣

Bizonyítás: Lásd a 3.3.5 Tételnél. ■

4.4.4 Definíció

Egy $\mathbf{v}$ vektor *lineárisan függ* az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektoroktól, ha $\mathbf{v}$ előáll az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineáris kombinációjaként. ♣

Ha $\mathbf{v}$ lineárisan függ az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektoroktól, akkor a $\mathbf{v}, \mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineárisan összefüggők, de megfordítva ez *nem igaz*! A 4.4.3 Tétel III. állítása szerint az összefüggőség azzal ekvivalens, hogy a vektorok között *van* olyan, amelyik lineárisan függ a többitől. (Egy összefüggő rendszerben egyébként általában több ilyen vektor van, és természetesen az is előfordul*hat*, hogy az összes vektor ilyen. Lásd a 4.4.4–4.4.6 feladatokat.)

A generált altér fogalmának felhasználásával azonnal adódik, hogy $\mathbf{v}$ pontosan akkor függ $\mathbf{u}_1, \ldots, \mathbf{u}_m$-től lineárisan, ha $\mathbf{v} \in \langle \mathbf{u}_1, \ldots, \mathbf{u}_m \rangle$.

Végül megemlítjük, hogy *végtelen sok* vektor lineáris függetlenségén azt értjük, hogy közülük *bármely* véges sok lineárisan független. (A problémát — a generált altérnél látottakhoz hasonlóan — most is az okozza, hogy végtelen sok vektor lineáris kombinációjának nincs értelme.)

Feladatok (Lásd a 3.3 pont feladatait is.)

4.4.1 Melyek igazak az alábbi állítások közül?

(a) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ lineárisan független és $\mathbf{v}_1, \ldots, \mathbf{v}_{100}$ is lineárisan független, akkor $\mathbf{u}_1, \ldots, \mathbf{u}_{100}, \mathbf{v}_1, \ldots, \mathbf{v}_{100}$ is lineárisan független.

(b) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_{100}, \mathbf{v}_1, \ldots, \mathbf{v}_{100}$ lineárisan független, akkor $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ és $\mathbf{v}_1, \ldots, \mathbf{v}_{100}$ is lineárisan független.

(c) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ lineárisan független és $\mathbf{v}_1, \ldots, \mathbf{v}_{100}$ is lineárisan független, akkor $\mathbf{u}_1 + \mathbf{v}_1, \ldots, \mathbf{u}_{100} + \mathbf{v}_{100}$ is lineárisan független.

(d) Ha $\mathbf{u}_1 + \mathbf{v}_1, \ldots, \mathbf{u}_{100} + \mathbf{v}_{100}$ lineárisan független, akkor $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ és $\mathbf{v}_1, \ldots, \mathbf{v}_{100}$ is lineárisan független.

(e) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ között szerepel olyan vektor, amelyik valamelyik másik $\mathbf{u}_i$-nek skalárszorosa, akkor $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ lineárisan összefüggő.

(f) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ közül bármelyik 99 vektor lineárisan független, akkor $\mathbf{u}_1, \ldots, \mathbf{u}_{100}$ is lineárisan független.

(g) Ha $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{100}$ lineárisan független, akkor $\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_3, \ldots, \mathbf{u}_{100}$ is lineárisan független.

(h) Ha $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{100}$ lineárisan összefüggő, akkor $\mathbf{u}_1 + \mathbf{u}_2, \mathbf{u}_3, \ldots, \mathbf{u}_{100}$ is lineárisan összefüggő.

(i) Ha $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{100}$ lineárisan független, akkor $\mathbf{u}_1, \mathbf{u}_1 + \mathbf{u}_2, \ldots, \mathbf{u}_1 + \mathbf{u}_2 + \ldots + \mathbf{u}_{100}$ is lineárisan független.

(j) Ha $\mathbf{u}_1, \mathbf{u}_2, \ldots, \mathbf{u}_{100}$ lineárisan összefüggő, akkor $\mathbf{u}_1, \mathbf{u}_1 + \mathbf{u}_2, \ldots, \mathbf{u}_1 + \mathbf{u}_2 + \ldots + \mathbf{u}_{100}$ is lineárisan összefüggő.

4.4.2 Tegyük fel, hogy $\mathbf{a}$, $\mathbf{b}$ és $\mathbf{c}$ egyike sem a nullvektor. Mit állíthatunk $\mathbf{a}$ és $\mathbf{c}$ viszonyáról lineáris függetlenség, illetve összefüggőség szempontjából, ha tudjuk, hogy

(a) $\mathbf{a}$, $\mathbf{b}$ lineárisan összefüggő, $\mathbf{b}$, $\mathbf{c}$ lineárisan összefüggő;
(b) $\mathbf{a}$, $\mathbf{b}$ lineárisan független, $\mathbf{b}$, $\mathbf{c}$ lineárisan összefüggő;
(c) $\mathbf{a}$, $\mathbf{b}$ lineárisan független, $\mathbf{b}$, $\mathbf{c}$ lineárisan független?

4.4.3 Tegyük fel, hogy egy végtelen test feletti vektortérben az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektoroknak csak véges sok lineáris kombinációja állítja elő a nullvektort. Következik-e ebből, hogy $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független?

4.4.4 Tegyük fel, hogy az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok között *pontosan* egy olyan van, amely lineárisan függ a többi $m-1$ vektortól. Bizonyítsuk be, hogy ekkor ez szükségképpen a nullvektor.

4.4.5 Legyen $m \geq 2$ és $0 \leq s \leq m$. Adjunk meg m különböző vektort úgy valamely alkalmas vektortérben, hogy közöttük *pontosan* s darab olyan legyen, amely(ek mindegyike) lineárisan függ a többi $m-1$ vektortól.

4.4.6 Tegyük fel, hogy az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineárisan összefüggők. Melyek igazak az alábbi állítások közül?

(a) Ha az $\mathbf{u}_i$-k közül bármelyik $m-1$ lineárisan független, akkor mindegyik $\mathbf{u}_i$ lineárisan függ a többi $m-1$-től.
(b) Ha mindegyik $\mathbf{u}_i$ lineárisan függ a többi $m-1$-től, akkor az $\mathbf{u}_i$-k közül bármelyik $m-1$ lineárisan független.
(c) Ha egy $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$ nem triviális lineáris kombinációban $\lambda_t \neq 0$, akkor $\mathbf{u}_t$ lineárisan függ a többi $m-1$ vektortól.
(d) Ha egy $\lambda_1\mathbf{u}_1 + \ldots + \lambda_m\mathbf{u}_m = \mathbf{0}$ nem triviális lineáris kombinációban $\lambda_t = 0$, akkor $\mathbf{u}_t$ *nem* függ lineárisan a többi $m-1$ vektortól.

4.4.7 Tegyük fel, hogy $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, $\mathbf{d}$ lineárisan független, $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$, $\mathbf{e}$ lineárisan összefüggő, $\mathbf{c}$, $\mathbf{d}$, $\mathbf{e}$ lineárisan összefüggő és $\mathbf{e} \neq \mathbf{0}$. Mit állíthatunk az $\mathbf{a}$, $\mathbf{b}$, $\mathbf{d}$, $\mathbf{e}$ vektorokról lineáris függetlenség, illetve összefüggőség szempontjából?

4.4.8 Tegyük fel, hogy $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ lineárisan független, de $\mathbf{a}$, $\mathbf{b}$, $\mathbf{d}$ is, $\mathbf{a}$, $\mathbf{c}$, $\mathbf{d}$ is és $\mathbf{b}$, $\mathbf{c}$, $\mathbf{d}$ is lineárisan összefüggő. Határozzuk meg a $\mathbf{d}$ vektort.

4.4.9 Tekintsük a komplex együtthatós polinomok szokásos vektorterét a komplex test felett. Vizsgáljuk meg az alábbi vektorrendszereket lineáris függetlenség, illetve összefüggőség szempontjából.

(a) $(x+1)(x+2)$, $(x+2)(x+3)$, $(x+3)(x+1)$;

(b) $(x+1)(x+2)$, $(x+2)(x+3)$, $(x+3)(x+4)$, $(x+4)(x+1)$;

(c) x^3+ix^2-x-i, $-ix^3-x^2+x+i$, $-x^3-ix^2+ix+1$, ix^3+x^2-ix-1;

(d) 1000 darab olyan polinom, amelyek mind különböző fokúak;

(e) 1000 darab olyan polinom, amelyek mind azonos fokúak;

(f) 1000 darab olyan valós együtthatós polinom, amelyek irreducibilisek a valós test felett;

(g) 1000 darab olyan racionális együtthatós polinom, amelyek irreducibilisek a racionális test felett.

4.4.10 Legyen V a valós test feletti vektortér, $m \geq 2$, $1 \leq k < m$, és tegyük fel, hogy az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineárisan függetlenek. Mi a szükséges és elégséges feltétele annak, hogy

(a) $\mathbf{u}_1+\mathbf{u}_2$, $\mathbf{u}_2+\mathbf{u}_3$, $\ldots$, $\mathbf{u}_m+\mathbf{u}_1$, illetve

(b) $\mathbf{u}_1+\mathbf{u}_2+\ldots+\mathbf{u}_k$, $\mathbf{u}_2+\mathbf{u}_3+\ldots+\mathbf{u}_{k+1}$, $\ldots$, $\mathbf{u}_m+\mathbf{u}_1+\ldots+\mathbf{u}_{k-1}$

lineárisan független legyen?

M 4.4.11 Jelöljük V_T-vel a T^k vektorteret a T test felett a szokásos műveletekre. Legyenek $\mathbf{u}_1, \ldots, \mathbf{u}_m$ olyan k hosszúságú sorozatok, amelyek minden eleme 0 vagy 1. Ezeket $T=\mathbf{Q}$, $T=\mathbf{R}$ és $T=F_p$-re is tekinthetjük V_T elemeinek. Így mást és mást jelent(het) ezeknek a 0–1 vektoroknak a különböző testek „feletti" lineáris függetlensége. Melyek igazak az alábbi állítások közül?
Ha $\mathbf{u}_1, \ldots, \mathbf{u}_m$ lineárisan független

(a) $T=\mathbf{R}$ felett, akkor független $T=\mathbf{Q}$ felett is;
(b) $T=\mathbf{Q}$ felett, akkor független $T=\mathbf{R}$ felett is;
(c) $T=\mathbf{Q}$ felett, akkor független $T=F_2$ felett is;
(d) $T=F_2$ felett, akkor független $T=\mathbf{Q}$ felett is;
(e) $T=\mathbf{Q}$ felett, akkor független véges sok p kivételével minden $T=F_p$ felett is.

4.4.12 Tekintsük a valós számokat a *racionális* test feletti vektortérként a szokásos műveletekre. Bizonyítsuk be, hogy

(a) különböző prímszámok rögzített alapú logaritmusai mindig lineárisan függetlenek;

(b) egy valós szám összes pozitív egész kitevős hatványai akkor és csak akkor lineárisan függetlenek, ha a szám *transzcendens*. (A transzcendens szám definícióját lásd az A.10 pontban az A.10.6 Definíció után.)

4.4.13 Bizonyítsuk be, hogy az $\langle \mathbf{u} \rangle \oplus \langle \mathbf{v} \rangle$ direkt összeg akkor és csak akkor létezik, ha $\mathbf{u}$ és $\mathbf{v}$ lineárisan független, vagy $\mathbf{u}$ és $\mathbf{v}$ közül legalább az egyik $\mathbf{0}$.

4.5. Bázis

4.5.1 Definíció
*Bázis*on lineárisan független generátorrendszert értünk. ♣

A generátorrendszer definíciójából és a 4.4.3 Tétel V. állításából azonnal következik a

4.5.2 Tétel
Egy $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorrendszer akkor és csak akkor bázis, ha a vektortér minden eleme *egyértelműen* előáll az $\mathbf{u}_1, \ldots, \mathbf{u}_m$ vektorok lineáris kombinációjaként. ♣

Példák: T^n-ben, illetve $T^{k\times n}$-ben bázist alkotnak azok a vektorok, illetve mátrixok, amelyeknek egyetlen eleme 1, a többi 0. Természetesen egy vektortérnek általában nagyon sok bázisa van. A közönséges háromdimenziós térben bármely három, nem egy síkba eső vektor bázist alkot.

A $\mathbf{0}$ térnek nincs bázisa, ugyanis egyetlen eleme, a $\mathbf{0}$, már önmagában lineárisan összefüggő. A valós számsorozatok szokásos vektorterének nincs (véges sok elemből) bázisa, hiszen már véges generátorrendszere sincs. Bázison a továbbiakban mindig *véges* sok vektorból álló rendszert fogunk érteni. A végtelen elemű bázis bevezetésének a lehetőségére ennek a pontnak a végén röviden utalunk.

Alapvető fontosságú a

4.5.3 Tétel
Egy vektortérben bármely két bázis azonos elemszámú. ♣

Ennél erősebb tételt fogunk igazolni:

4.5.4 Tétel
Legyen $\mathbf{f}_1, \ldots, \mathbf{f}_n$ lineárisan független rendszer és $\mathbf{g}_1, \ldots, \mathbf{g}_k$ generátorrendszer egy V vektortérben. Ekkor $n \leq k$. ♣

A 4.5.4 Tételből valóban azonnal következik a 4.5.3 Tétel: az első bázist független rendszernek, a másodikat generátorrendszernek tekintve kapjuk, hogy az elsőnek legfeljebb annyi eleme van, mint a másodiknak, majd ugyanezt fordított szereposztásban is elvégezzük.

A 4.5.4 Tételre két bizonyítást adunk.

Első bizonyítás: Indirekt, tegyük fel, hogy $n > k$. Az ellentmondást úgy fogjuk kihozni, hogy megmutatjuk, hogy a

$$\lambda_1\mathbf{f}_1 + \lambda_2\mathbf{f}_2 + \ldots + \lambda_n\mathbf{f}_n = \mathbf{0} \tag{4.5.1}$$

egyenlőség nem csak $\lambda_1 = \ldots = \lambda_n = 0$ esetén teljesül. Mivel a $\mathbf{g}_j$-k generátorrendszert alkotnak, ezért valamennyi $\mathbf{f}_i$ előáll a $\mathbf{g}_j$-k lineáris kombinációjaként:

$$\begin{aligned}
\mathbf{f}_1 =& \alpha_{11}\mathbf{g}_1 + \alpha_{21}\mathbf{g}_2 + \ldots + \alpha_{k1}\mathbf{g}_k \\
\mathbf{f}_2 =& \alpha_{12}\mathbf{g}_1 + \alpha_{22}\mathbf{g}_2 + \ldots + \alpha_{k2}\mathbf{g}_k \\
&\vdots \\
\mathbf{f}_n =& \alpha_{1n}\mathbf{g}_1 + \alpha_{2n}\mathbf{g}_2 + \ldots + \alpha_{kn}\mathbf{g}_k
\end{aligned}$$

Írjuk be ezeket az előállításokat (4.5.1)-be az $\mathbf{f}_i$-k helyére, és rendezzük át a bal oldalt a $\mathbf{g}_j$-k szerint:

$$\begin{aligned}
(\lambda_1\alpha_{11} + \lambda_2\alpha_{12} + \ldots + \lambda_n\alpha_{1n})\mathbf{g}_1 + (\lambda_1\alpha_{21} + \lambda_2\alpha_{22} + \ldots + \lambda_n\alpha_{2n})\mathbf{g}_2 + \\
+ \ldots + (\lambda_1\alpha_{k1} + \lambda_2\alpha_{k2} + \ldots + \lambda_n\alpha_{kn})\mathbf{g}_k = \mathbf{0}\,.
\end{aligned}$$

Ezzel a $\mathbf{0}$-t felírtuk a $\mathbf{g}_j$-k lineáris kombinációjaként. Ha itt minden $\mathbf{g}_j$ együtthatója 0, akkor az egyenlőség biztosan teljesül (lehet, hogy máskor is, hiszen a $\mathbf{g}_j$-k nem feltétlenül függetlenek). Az, hogy minden $\mathbf{g}_j$ együtthatója 0 legyen, az

$$\begin{aligned}
\alpha_{11}\lambda_1 + \alpha_{12}\lambda_2 + \ldots + \alpha_{1n}\lambda_n &= 0 \\
\alpha_{21}\lambda_1 + \alpha_{22}\lambda_2 + \ldots + \alpha_{2n}\lambda_n &= 0 \\
&\vdots \\
\alpha_{k1}\lambda_1 + \alpha_{k2}\lambda_2 + \ldots + \alpha_{kn}\lambda_n &= 0
\end{aligned}$$

feltételt jelenti. Ez egy olyan homogén lineáris egyenletrendszer a λ-kra, amelyben n ismeretlen van és csak k egyenlet, tehát az $n > k$ indirekt feltevésünk szerint biztosan létezik nem triviális megoldás. Vagyis (4.5.1) nem csak triviálisan teljesül, ami ellentmond az $\mathbf{f}_j$-k függetlenségének. ■

Második bizonyítás:

4.5.5 Lemma (Kicserélési tétel)

Legyen $\mathbf{f}_1, \ldots, \mathbf{f}_n$ lineárisan független rendszer és $\mathbf{g}_1, \ldots, \mathbf{g}_k$ generátorrendszer egy V vektortérben. Ekkor *bármely* $\mathbf{f}_i$-hez található olyan $\mathbf{g}_j$, hogy

$$\mathbf{f}_1, \ldots, \mathbf{f}_{i-1}, \mathbf{g}_j, \mathbf{f}_{i+1}, \ldots, \mathbf{f}_n$$

is lineárisan független rendszer. (Azaz bármelyik $\mathbf{f}_i$ „kicserélhető" alkalmas $\mathbf{g}_j$-vel.) ♣

A kicserélési tétel bizonyítása: Tegyük fel indirekt, hogy pl. $\mathbf{f}_1$-re ez nem igaz, tehát az $\mathbf{f}_2, \ldots, \mathbf{f}_n$ vektorokhoz akármelyik $\mathbf{g}_j$-t hozzávéve mindig összefüggő rendszert kapunk. Mivel $\mathbf{f}_2, \ldots, \mathbf{f}_n$ független (4.4.3/I Tétel), így mindegyik $\mathbf{g}_j$ előáll ezek lineáris kombinációjaként (4.4.3/IV Tétel). Ekkor nyilván a $\mathbf{g}_j$-k minden lineáris kombinációja is felírható az $\mathbf{f}_2, \ldots, \mathbf{f}_n$ vektorokkal. A $\mathbf{g}_j$-k azonban generátorrendszert alkotnak, tehát lineáris kombinációik kiadják az egész vektorteret. Így V minden eleme, speciálisan $\mathbf{f}_1$ is előáll $\mathbf{f}_2, \ldots, \mathbf{f}_n$ lineáris kombinációjaként. Ez viszont ellentmond $\mathbf{f}_1, \ldots, \mathbf{f}_n$ lineáris függetlenségének. ■

Most levezetjük a kicserélési tételből a 4.5.4 Tételt. Cseréljük ki először $\mathbf{f}_1$-et valamelyik $\mathbf{g}_j$-re, majd az így kapott *új* független rendszerből cseréljük ki $\mathbf{f}_2$-t alkalmas $\mathbf{g}$-re stb., egészen addig, amíg az $\mathbf{f}_i$-k el nem fogynak. Az így nyert független rendszerben már csak $\mathbf{g}$-k szerepelnek, és a függetlenség miatt nem lehet közöttük két egyenlő. Vagyis valóban legalább annyi $\mathbf{g}$-nek kellett lennie, mint $\mathbf{f}$-nek. ■

A következő két tétel azt mutatja, hogy nagyon sokféleképpen juthatunk bázishoz, nevezetesen, lényegében bármely generátorrendszerből kiválaszthatunk bázist, illetve bármely független rendszert kiegészíthetünk bázissá.

4.5.6 Tétel

Egy $V \neq \mathbf{0}$ vektortér bármely (véges) generátorrendszere tartalmaz bázist. ♣

Bizonyítás: Ha a generátorrendszer lineárisan független, akkor ő maga bázis. Ha összefüggő, akkor van benne olyan elem, amely előáll a többiek lineáris kombinációjaként, pl. $\mathbf{g}_k = \mu_1\mathbf{g}_1 + \ldots + \mu_{k-1}\mathbf{g}_{k-1}$. Ezt a $\mathbf{g}_k$ elemet elhagyva

a maradék továbbra is generátorrendszert alkot, ugyanis bármely $\mathbf{v} \in V$-re

$$\begin{aligned}\mathbf{v} &= \alpha_1\mathbf{g}_1 + \ldots + \alpha_{k-1}\mathbf{g}_{k-1} + \alpha_k\mathbf{g}_k = \\ &= \alpha_1\mathbf{g}_1 + \ldots + \alpha_{k-1}\mathbf{g}_{k-1} + \alpha_k(\mu_1\mathbf{g}_1 + \ldots + \mu_{k-1}\mathbf{g}_{k-1}) = \\ &= (\alpha_1 + \alpha_k\mu_1)\mathbf{g}_1 + \ldots + (\alpha_{k-1} + \alpha_k\mu_{k-1})\mathbf{g}_{k-1}.\end{aligned}$$

Ha az így kapott $\mathbf{g}_1, \ldots, \mathbf{g}_{k-1}$ generátorrendszer már független, akkor készen vagyunk. Ha összefüggő, akkor megismételjük az előzőket. Az eljárás előbb-utóbb befejeződik (a „legrosszabb" esetben akkor, amikor a generátorrendszer már csak egyetlen vektorból áll, ami $V \neq \mathbf{0}$ miatt nem lehet a nullvektor és így biztosan független). ■

4.5.7 Tétel

Ha egy V vektortérnek van (véges) generátorrendszere, akkor bármely lineárisan független rendszer kiegészíthető bázissá. ♣

Bizonyítás: Ha a független rendszer generátorrendszer is, akkor ő maga bázis. Ha nem, akkor van olyan $\mathbf{v}$ vektor, amely nem áll elő a független rendszer elemeinek lineáris kombinációjaként. Ekkor a független rendszerhez $\mathbf{v}$-t hozzávéve továbbra is független rendszert kapunk (4.4.3/IV Tétel). Ha még ez sem bázis, akkor az eljárást tovább folytatjuk. Mivel a vektortérnek van véges (mondjuk s elemű) generátorrendszere, tehát a 4.5.4 Tétel szerint ennél több független vektor nem lehet V-ben. Az eljárás így előbb-utóbb véget kell hogy érjen. ■

A 4.5.6 és 4.5.7 Tételek bizonyításai egyúttal módszert is adnak arra, hogyan lehet adott generátorrendszerből bázist kiválasztani, illetve adott független rendszert bázissá kiegészíteni.

A generátorrendszerhez és a lineáris függetlenséghez hasonlóan a bázis fogalmát is kiterjeszthetjük végtelen sok vektor esetére: bázison ekkor is lineárisan független generátorrendszert értünk. A 4.5.2 Tétel megfelelője úgy szól, hogy egy H vektorhalmaz akkor és csak akkor bázis, ha a vektortér minden eleme lényegében egyértelműen állítható elő véges sok H-beli vektor lineáris kombinációjaként; a „lényegében" jelző arra utal, hogy két előállítás csak 0 együtthatójú tagokban különbözhet egymástól. Transzfinit eszközökkel igazolható, hogy minden $V \neq \mathbf{0}$ vektortérnek van bázisa, ezt általában *Hamel-bázis*nak nevezik. A 4.5.3 Tétel megfelelője is érvényes: egy vektortér bármely két (Hamel-)bázisa azonos *számosságú*.

Feladatok

4.5.1 Tekintsük a legfeljebb 20-adfokú valós együtthatós polinomok szokásos vektorterét a valós test felett. Adjunk meg egy-egy bázist az alábbi alterekben. Egy általános polinomot $f = \alpha_0 + \alpha_1 x + \ldots + {} + \alpha_{20} x^{20}$-nal jelölünk. A jelölésben nem teszünk különbséget polinom és polinomfüggvény között.

(a) $\{f \mid \deg f \leq 10 \text{ vagy } f = 0\}$;
(b) $\{f \mid x^3 + 1 \text{ osztója az } f\text{-nek}\}$;
(c) $\{f \mid x^3 + 1\text{-gyel osztva az } f \text{ konstans maradékot ad}\}$;
(d) $\{f \mid f(5) = 0\}$;
(e) $\{f \mid f \text{ együtthatóinak az összege } 0\}$;
(f) $\{f \mid f(3) = 2f(4)\}$;
(g) $\{f \mid \alpha_0 = \alpha_1 = \alpha_{13}\}$.

4.5.2 Tekintsük a 2×3-as racionális elemű mátrixok szokásos $\mathbf{Q}^{2\times 3}$ vektorterét a racionális test felett. Döntsük el, hogy az alábbiak közül melyek alkotnak bázist. A lineárisan független rendszereket egészítsük ki bázissá, a generátorrendszerekből válasszunk ki bázist.

(a) Azok a mátrixok, amelyeknek egyik eleme 0, a többi pedig 5;
(b) azok a mátrixok, amelyeknek két eleme 0, a többi pedig 5;
(c) azok a mátrixok, amelyekben valamelyik sor vagy oszlop minden eleme 5, a többi elem pedig 0;
(d) azok a mátrixok, amelyekben valamelyik oszlop elemei (tetszőleges sorrendben) az 5 és a 6 , a többi elem pedig 0;
(e) az $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \end{pmatrix}$ mátrix és ennek tükörképei a mátrix(ot alkotó téglalap) függőleges, illetve vízszintes középvonalára, valamint középpontjára;
(f) az $\begin{pmatrix} 1 & 2 & 3 \\ 4 & 6 & 8 \end{pmatrix}$ mátrix és ennek tükörképei a mátrix(ot alkotó téglalap) függőleges, illetve vízszintes középvonalára, valamint középpontjára.

4.5.3 *Maximális* független rendszeren olyan független vektorrendszert értünk, amely már nem bővíthető, azaz a vektortér bármely elemét hozzávéve biztosan összefüggő rendszert kapunk. *Maximális elemszámú* független rendszer olyan független rendszert jelent, amelynél nagyobb elemszámú független rendszer nem található a vektortérben. Bizonyítsuk be, hogy az imént definiált két fogalom bármely vektortérben egybeesik.

4.5.4 Az előző feladat mintájára definiáljuk a *minimális*, illetve a *minimális elemszámú* generátorrendszer fogalmát, és igazoljuk ezek egybeesését egymással és az előző feladatban értelmezett fogalmakkal.

4.5.5 Bizonyítsuk be, hogy ha egy vektortérben nincs 19 elemű generátorrendszer, akkor van benne 20 elemű független rendszer.

4.5.6 Tegyük fel, hogy $\langle \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3 \rangle = \langle \mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3, \mathbf{b}_4 \rangle$. Mit állíthatunk az $\mathbf{a}_1$, $\mathbf{a}_2$, $\mathbf{b}_1$, $\mathbf{b}_2$ vektorrendszerről lineáris függetlenség, illetve összefüggőség szempontjából?

4.5.7 Legyen W egy nem triviális altér a V vektortérben. Melyek igazak az alábbi állítások közül?

(a) V tetszőleges bázisának W-be eső elemei bázist alkotnak W-ben.

(b) W tetszőleges bázisa kiegészíthető V bázisává, feltéve hogy V-nek egyáltalán van bázisa.

(c) Ha V-nek van k elemű bázisa, akkor W-nek van k elemű generátorrendszere.

(d) Ha V-nek van k elemű bázisa, akkor W-nek van k elemű lineárisan független rendszere.

(e) Ha W-nek van k elemű bázisa, akkor V-nek van k elemű generátorrendszere.

(f) Ha W-nek van k elemű bázisa, akkor V-nek van k elemű lineárisan független rendszere.

4.5.8 Legyen $n \geq 2$ és $\mathbf{u}_1, \ldots, \mathbf{u}_n$ bázis a valós test feletti V vektortérben. Az alábbi vektorrendszerek közül melyek alkotnak lineárisan független rendszert, generátorrendszert, illetve bázist?

(a) $\mathbf{u}_1 - \mathbf{u}_2$, $\mathbf{u}_2 - \mathbf{u}_3$, $\ldots$, $\mathbf{u}_n - \mathbf{u}_1$;

(b) $\mathbf{u}_1 - \mathbf{u}_2$, $\mathbf{u}_2 - \mathbf{u}_3$, $\ldots$, $\mathbf{u}_{n-1} - \mathbf{u}_n$;

(c) $\mathbf{u}_1 + \mathbf{u}_2$, $\mathbf{u}_2 + \mathbf{u}_3$, $\ldots$, $\mathbf{u}_n + \mathbf{u}_1$;

(d) $\mathbf{u}_1 + \mathbf{u}_2$, $\mathbf{u}_2 + \mathbf{u}_3$, $\ldots$, $\mathbf{u}_{n-1} + \mathbf{u}_n$, $\mathbf{u}_n$;

(e) $\mathbf{u}_1 - \mathbf{u}_2$, $\mathbf{u}_2 - \mathbf{u}_3$, $\ldots$, $\mathbf{u}_n - \mathbf{u}_1$, $\mathbf{u}_1 + \mathbf{u}_2 + \ldots + \mathbf{u}_n$.

4.5.9 Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$ bázis a V vektortérben és $\mathbf{v} = \alpha_1\mathbf{u}_1 + \ldots + \alpha_n\mathbf{u}_n$. Bizonyítsuk be, hogy $\mathbf{u}_1 + \mathbf{v}, \ldots, \mathbf{u}_n + \mathbf{v}$ akkor és csak akkor bázis, ha $\alpha_1 + \ldots + \alpha_n \neq -1$.

4.5.10 Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$ bázis a V vektortérben és

$$\mathbf{v}_i = \beta_{1i}\mathbf{u}_1 + \ldots + \beta_{ni}\mathbf{u}_n, \quad i = 1, 2, \ldots, n\,.$$

Bizonyítsuk be, hogy $\mathbf{v}_1, \ldots, \mathbf{v}_n$ akkor és csak akkor alkot bázist V-ben, ha a β_{ij}-kből képzett $n \times n$-es determináns nem nulla.

4.5.11 Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$, illetve $\mathbf{v}_1, \ldots, \mathbf{v}_n$ két tetszőleges bázis a V vektortérben. Bizonyítsuk be, hogy *bármely* $\mathbf{u}_i$-hez található olyan $\mathbf{v}_j$, hogy az $\mathbf{u}_i$-t és $\mathbf{v}_j$-t egymással kicserélve ismét két bázist kapunk.

4.5.12

(a) Van-e a modulo 3 maradékosztályok F_3 teste felett olyan vektortér, amelynek 243 eleme van?

(b) Van-e a modulo 3 maradékosztályok F_3 teste felett olyan vektortér, amelynek 300 eleme van?

**(c) Bizonyítsuk be, hogy egy véges test elemszáma csak prímhatvány lehet.

(d) Bizonyítsuk be, hogy egy véges vektortér elemszáma csak prímhatvány lehet.

4.5.13 Tegyük fel, hogy egy vektortérnek (van bázisa, de) csak véges sok bázisa van. Bizonyítsuk be, hogy ekkor a vektortér csak véges sok elemből áll.

*4.5.14

(a) Hány bázisa van az F_p test feletti F_p^2 vektortérnek? És F_p^n-nek?

(b) Az F_p test feletti $n \times n$-es mátrixok közül hánynak létezik inverze?

(c) Bizonyítsuk be, hogy bármely p prímszámra és bármely n pozitív egészre

$$n! \,|\, (p^n - 1)(p^n - p) \ldots (p^n - p^{n-1})\,.$$

4.6. Dimenzió

4.6.1 Definíció

Egy V vektortér *dimenzió*ján egy bázisának elemszámát értjük. Ha a vektortérnek nincs véges generátorrendszere, akkor a dimenziója végtelen. Végül a $\mathbf{0}$ tér dimenziója 0. ♣

A V vektortér dimenzióját $\dim V$-vel jelöljük.

A 4.6.1 Definícióban felhasználtuk, hogy valamennyi bázisnak ugyanaz az elemszáma (4.5.3 Tétel), és így a dimenzió nem függ a bázis választásától. A végtelen dimenzió fogalmát a Hamel-bázisokra az előző pont végén elmondottak segítségével tovább finomíthatjuk.

Példák: a „közönséges háromdimenziós tér" dimenziója valóban 3, T^n-é n, $T^{k\times n}$-é kn. A T feletti polinomok szokásos vektortere végtelen dimenziós, ebben a legfeljebb r-edfokú polinomok $r+1$-dimenziós alteret alkotnak.

A (0-nál nagyobb, de véges) dimenzió a bázis elemszáma helyett több más ekvivalens módon is megadható. Ezek közül a két legfontosabb: a lineárisan független elemek maximális száma, illetve a generátorrendszerek elemszámának a minimuma.

4.6.2 Tétel

Legyen $V \neq \mathbf{0}$ vektortér és n pozitív egész. Ekkor az alábbi feltételek ekvivalensek:

(i) $\dim V = n$;

(ii) V-ben található n független vektor, de bármely $n+1$ vektor összefügg;

(iii) V-ben található n elemű generátorrendszer, de $n-1$ elemű nem. ♣

Könnyen adódik, hogy (ii)-ben „$n+1$" helyett „több, mint n", (iii)-ban „$n-1$" helyett „kevesebb, mint n" is írható.

Bizonyítás: (i) ⇒ (ii): A feltétel szerint V-ben van n elemű bázis. Ez definíció szerint n független vektorból áll, és ennél több független vektor a 4.5.4 Tétel alapján nem fordulhat elő. — (ii) ⇒ (i): Az n független vektorról megmutatjuk, hogy bázis. A feltétel szerint ezekhez bármely vektort hozzávéve már összefüggő rendszert kapunk. A 4.4.3/IV Tétel alapján ekkor a hozzávett vektor előáll az eredeti n vektor lineáris kombinációjaként. Mivel ez bármely vektorra igaz, ezért az eredeti n vektor generátorrendszert, azaz a függetlenség miatt bázist alkot. — (i) és (iii) ekvivalenciája hasonló módon igazolható. ■

Gyakran jól használható az alábbi egyszerű észrevétel.

4.6.3 Tétel

Legyen n pozitív egész és $\dim V = n$. Ekkor V-ben bármely n elemű független rendszer bázist alkot. Ugyanez áll bármely n elemű generátorrendszerre is. ♣

Bizonyítás: Ha az n elemű független rendszer nem lenne bázis, akkor a 4.5.7 Tétel szerint kibővíthető bázissá. Ennek az új bázisnak azonban n-nél több eleme lenne, a dimenzió tehát nem lehetne n. A generátorrendszerre vonatkozó állítás hasonlóan igazolható. ■

A 4.6.3 Tétel alapján egy n-dimenziós térben n vektor pontosan akkor bázis, ha lineárisan független. Ez megkönnyíti, hogy adott vektorokról eldöntsük, bázist alkotnak-e, hisz a bázis definíciójában szereplő két feltétel közül elég az egyiket ellenőrizni. (Ha pedig a vektorok száma nem egyezik meg a tér dimenziójával, akkor biztosan nem alkotnak bázist.) Ezt az észrevételt az előző pont feladatainál is felhasznál(hat)tuk (volna).

A következő tétel a vektortér és egy benne levő altér dimenziójának a kapcsolatát írja le. Az eredmény a várakozásnak megfelelően összhangban van a szemléletes elképzelésünkkel.

4.6.4 Tétel

I. Legyen W altér V-ben. Ekkor $\dim W \leq \dim V$.

II. Ha V *véges dimenziós*, W altér V-ben és $\dim W = \dim V$, akkor $W = V$.

♣

Bizonyítás: I. Ha $W = \mathbf{0}$ vagy $\dim V = \infty$, akkor az állítás nyilvánvaló. A többi esetben V-nek van bázisa. Egy V-beli bázis elemszámánál több független elem W-ben sem lehet, hiszen azok a vektorok V-ben is függetlenek lennének, és ez ellentmondana a 4.5.4 Tételnek. Így a 4.6.2 Tétel szerint valóban $\dim W \leq \dim V$.

II. Az állítás $V = \mathbf{0}$ esetén nyilvánvaló. Egyébként legyen $\dim V = \dim W = n(\neq 0)$, és tekintsük W egy (n elemű) bázisát. Ez V-ben is független rendszer, tehát a 4.6.3 Tétel szerint V-nek is bázisa. Azaz W-nek ez a generátorrendszere V-ben is generátorrendszer, és így V nem lehet bővebb W-nél. ■

A 4.6.4 Tétel II. állítása végtelen dimenzió esetén nem igaz: pl. a polinomok szokásos vektorterében valódi alteret alkotnak az x-szel osztható polinomok, ugyanakkor a két dimenzió megegyezik.

4.6.5 Definíció

Az $\mathbf{a}_1, \ldots, \mathbf{a}_n$ vektorrendszer *rangja* r, ha az $\mathbf{a}_i$ vektorok között található r lineárisan független, de $r+1$ már nem. ♣

A vektorrendszer rangja tehát a vektorok közül a lineárisan függetlenek maximális száma. Általában több ilyen maximális elemszámú független rendszer is kiválasztható az adott vektorokból.

Ez a rangdefiníció a mátrixnál látottak általánosítása: egy mátrix oszloprangja éppen az oszlopvektoraiból álló vektorrendszer rangja.

A következő tétel a generált altér dimenziójára vonatkozik.

4.6.6 Tétel

Az $\mathbf{a}_1, \ldots, \mathbf{a}_n$ vektorok által generált $\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$ altér dimenziója az $\mathbf{a}_1, \ldots, \mathbf{a}_n$ vektorrendszer rangja. ♣

Bizonyítás: Legyen pl. $\mathbf{a}_1, \ldots, \mathbf{a}_r$ egy maximális elemszámú független rendszer. Belátjuk, hogy ez bázist alkot $W = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle$-ben. A függetlenség teljesül, tehát csak azt kell igazolnunk, hogy W minden eleme felírható $\mathbf{a}_1, \ldots, \mathbf{a}_r$ lineáris kombinációjaként. Ezt nyilván elég W generátorelemeire megmutatni. Mivel bármely i-re az $\mathbf{a}_1, \ldots, \mathbf{a}_r$ vektorokhoz $\mathbf{a}_i$-t hozzávéve ez az $r+1$ vektor már biztosan összefüggő, így a hozzávett vektor valóban előáll $\mathbf{a}_1, \ldots, \mathbf{a}_r$ lineáris kombinációjaként. ■

A fentiek felhasználásával újabb bizonyítást nyerhetünk a lineáris egyenletrendszer megoldhatóságának a mátrixranggal megadott feltételére (lásd a 3.4.3 Tételt):

4.6.7 Tétel

Egy lineáris egyenletrendszer akkor és csak akkor oldható meg, ha az együtthatómátrix rangja megegyezik a kibővített mátrix rangjával. ♣

Bizonyítás: Írjuk fel az egyenletrendszert

$$x_1\mathbf{a}_1 + \ldots + x_n\mathbf{a}_n = \mathbf{b}$$

alakban, ahol $\mathbf{a}_i$ az együtthatómátrix i-edik oszlopa. Az egyenletrendszer akkor és csak akkor oldható meg, ha

$$\mathbf{b} \in \langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle.$$

Ez tovább ekvivalens az

$$\langle \mathbf{a}_1, \ldots, \mathbf{a}_n \rangle = \langle \mathbf{a}_1, \ldots, \mathbf{a}_n, \mathbf{b} \rangle$$

feltétellel, hiszen két altér pontosan akkor egyenlő, ha kölcsönösen tartalmazzák egymás generátorait. Itt a bal oldali altér része a jobb oldalinak, és mindketten véges dimenziósak, ezért a 4.6.4/II Tétel szerint pontosan akkor egyenlők, ha a dimenziójuk megegyezik, azaz

$$\dim \langle \mathbf{a}_1, \dots, \mathbf{a}_n \rangle = \dim \langle \mathbf{a}_1, \dots, \mathbf{a}_n, \mathbf{b} \rangle.$$

A 4.6.6 Tétel szerint ez azt jelenti, hogy a két vektorrendszer rangja ugyananynyi. Mivel ez a két rang éppen az együtthatómátrix, illetve a kibővített mátrix (oszlop)rangja, ezzel a tételünket bebizonyítottuk. ■

Feladatok

4.6.1 Mennyi az alábbi vektorterek dimenziója? (A műveletek a „szokásosak".)

(a) A komplex számok $\mathbf{R}$ felett;
(b) a komplex számok $\mathbf{Q}$ felett;
(c) a szimmetrikus $n \times n$-es mátrixok;
(d) az F_p test feletti polinomok;
(e) az F_p test feletti polinom*függvény*ek;
(f) az $\mathbf{R}$ feletti homogén 6-odfokú 4-változós polinomok (azaz amelyekben minden tag „összfoka" pontosan 6) és a 0;
(g) az $\mathbf{R}$ feletti legfeljebb 6-odfokú 4-változós polinomok (azaz amelyekben minden tag „összfoka" legfeljebb 6) és a 0;
(h) azok a $[0, 1]$ intervallumban értelmezett szakaszonként lineáris, folytonos „töröttvonalak", amelyek legfeljebb a 19 nevezőjű racionális számoknál „törnek meg";
(i) egy k egyenletet és n ismeretlent tartalmazó homogén lineáris egyenletrendszer megoldásai, ahol az együtthatómátrix rangja r;
(j) egy mátrix magtere (lásd a 4.2 pont P4 példáját);
(k) egy mátrix képtere.

4.6.2 Bázist alkotnak-e a legfeljebb 12-edfokú valós együtthatós polinomok szokásos vektorterében az alábbi vektorrendszerek?

(a) $(x-1)(x-2)\dots(x-12)$, $(x-2)(x-3)\dots(x-13)$, $\dots$, $(x-13)(x-14)\dots(x-24)$;
(b) $(x-1)^{12}$, $(x-2)^{12}$, $\dots$, $(x-13)^{12}$;
(c) $(x-1)^{12}$, $(x-1)^{11}(x-2)$, $\dots$, $(x-2)^{12}$;
(d) $(x^2-1)^6$, $(x^2-2)^6$, $\dots$, $(x^2-8)^6$, $(x-1)^{12}$, $\dots$, $(x-5)^{12}$.

4.6.3 Legyenek $0 \leq k \leq n$ tetszőleges egészek. Bizonyítsuk be, hogy minden n-dimenziós vektortérben van k-dimenziós altér.

4.6.4 Legyen V a T test feletti $n \times n$-es mátrixok szokásos $T^{n\times n}$ vektortere és $B \in T^{n\times n}$ egy rögzített mátrix. Tekintsük V-ben azokat az A mátrixokat, amelyekre $BA = 0$, ezek egy W alteret alkotnak. Bizonyítsuk be, hogy $\dim W$ osztható n-nel.

4.6.5 Legyenek W_1 és W_2 alterek V-ben, $\dim V = 40$, $\dim W_1 = 23$ és $\dim W_2 = 18$. Bizonyítsuk be, hogy $W_1 \cap W_2 \neq \mathbf{0}$.

4.6.6 Legyenek W_1 és W_2 alterek V-ben. Bizonyítsuk be, hogy

(a) $\dim\langle W_1, W_2\rangle \leq \dim W_1 + \dim W_2$;

(b) $\dim(W_1 \oplus W_2) = \dim W_1 + \dim W_2$;

(c) $\dim\langle W_1, W_2\rangle = \dim W_1 + \dim W_2 - \dim(W_1 \cap W_2)$.

M*4.6.7

(a) Legyen V egy 100-dimenziós vektortér a valós test felett. Hány olyan vektor létezik V-ben, amelyek közül *bármely* 100 bázist alkot?

(b) Oldjuk meg ugyanezt a feladatot az F_2, az F_{97}, illetve az F_{101} test feletti vektortérre is.

4.6.8 A *Fibonacci-számok* sorozatát a

$$\varphi_0 = 0, \quad \varphi_1 = 1, \quad \varphi_{i+1} = \varphi_i + \varphi_{i-1}, \quad i = 1, 2, \ldots$$

rekurzióval definiáljuk. Adjunk explicit képletet φ_n-re. (Útmutatás: Tekintsük az összes olyan α_0, α_1, … valós számsorozatot, amely kielégíti az $\alpha_{i+1} = \alpha_i + \alpha_{i-1}$, $\quad i = 1, 2, \ldots$ feltételt. (i) Számítsuk ki az így adódó vektortér dimenzióját. (ii) Ezután keressünk olyan bázist, amelynek elemei „szép” sorozatok, és írjuk fel a Fibonacci-sorozatot ennek a bázisnak a segítségével.)

4.6.9 Adjuk meg paraméteresen az összes 3×3-as *bűvös négyzet*et (ahol az elemek valós számok, és minden sorösszeg, oszlopösszeg és átlóösszeg egyenlő).

4.6.10 Hány dimenziós alteret generálnak a 4.3.1 feladat (a), (b), illetve (c) részében szereplő vektorrendszerek?

4.6.11 Egy V vektortér $\mathbf{a}_1, \ldots, \mathbf{a}_k$ elemeiről tudjuk, hogy az $\mathbf{a}_i + \mathbf{a}_j$, $1 \leq i < j \leq k$, vektorok bázist alkotnak V-ben. Bizonyítsuk be, hogy $\dim V = 1$ vagy 3.

4.6.12 Bizonyítsuk be, hogy egy vektorrendszer rangja nem változik meg, ha
(a) valamelyik vektort egy $\lambda \neq 0$ skalárral megszorzunk;
(b) az egyik vektorhoz egy másik vektor λ-szorosát hozzáadjuk.

4.6.13 Legyen A, $B \in T^{k\times n}$ és jelöljük $r(A)$-val az A mátrix rangját. Bizonyítsuk be, hogy $r(A+B) \leq r(A)+r(B)$.

*4.6.14 Hány r-dimenziós altér van az F_p test feletti F_p^n vektortérben?

**4.6.15 Hány olyan $k \times n$-es mátrix van, amelynek az elemei az F_p testből valók és a rangja r?

4.6.16
(a) Bizonyítsuk be, hogy ha egy mátrix minden eleme 0 vagy 1, akkor az F_2 test feletti rangja legfeljebb annyi, mint a valós test feletti rangja.
(b) Adjunk meg olyan 0–1 mátrixot, amelynek az F_2 test feletti rangja 1000-rel kevesebb, mint a valós test feletti rangja.

M(c) Melyik az a legkisebb n, amelyre van olyan $n\times n$-es 0–1 mátrix, amely rendelkezik a b)-beli tulajdonsággal?

4.7. Koordináták

4.7.1 Definíció

Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ egy rögzített bázis a V vektortérben. Ekkor minden $\mathbf{v} \in V$ vektor egyértelműen írható fel $\mathbf{v} = \alpha_1\mathbf{b}_1 + \ldots + \alpha_n\mathbf{b}_n$ alakban. Az α_i skalárokat a $\mathbf{v}$ vektornak a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis szerinti *koordinátái*nak nevezzük. ♣

Ha a közönséges háromdimenziós térben a szokásos merőleges egységvektorok alkotta bázist vesszük, akkor a koordináták éppen a szokásos koordináták lesznek. Ha T^n-ben azokat a bázisvektorokat tekintjük, amelyek egy komponense 1, a többi 0, akkor egy vektor koordinátái az őt alkotó komponensek lesznek. Más bázisban természetesen általában mások lesznek egy vektor koordinátái.

Ha a bázist rögzítjük, akkor a vektor helyett kényelmesen dolgozhatunk a koordinátáival. Két vektor összegének a koordinátáit éppen a megfelelő koordináták összegeként kapjuk, és hasonló érvényes a skalárszorosra is. Így a koordinátázással egy T feletti n-dimenziós V vektorteret tulajdonképpen T^n-re vezettünk vissza. Más szóval V és T^n algebrai szempontból „ugyanaz”, csak az elemeket és a műveleteket „másképp jelöjük”. Az egymással „ilyen”

kapcsolatban álló vektortereket *izomorf*nak (=azonos alakúnak) nevezzük. Mindezt az 5.2 pontban fogjuk pontosítani.

Feladatok

4.7.1 Hogyan változnak egy vektor koordinátái, ha a bázisban

(a) két elemet megcserélünk;

(b) az egyik báziselemet $\lambda(\neq 0)$-val megszorozzuk;

(c) az egyik báziselemhez egy másik λ-szorosát hozzáadjuk.

4.7.2 Adjuk meg az összes olyan vektort, amelynek a koordinátái bármely bázisban ugyanazok.

4.7.3 Tekintsük $\mathbf{C}^3$-ban az $\begin{pmatrix}1\\2\\5\end{pmatrix}, \begin{pmatrix}3\\7\\8\end{pmatrix}, \begin{pmatrix}2\\5\\2\end{pmatrix}$ bázist. Adjuk meg ebben a bázisban az $\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\end{pmatrix}$ és $\begin{pmatrix}0\\0\\1\end{pmatrix}$ vektorok koordinátáit.

4.7.4 Legyen $\mathbf{v} \neq \mathbf{0}$ adott vektor egy n-dimenziós vektortérben, és tekintsük az összes olyan $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázist, amely szerint $\mathbf{v}$ első két koordinátája 1. Mik $\mathbf{b}_1$ lehetséges értékei?

4.7.5

(a) A szultán gondolt $\mathbf{R}^{1001}$-ben egy bázist, amit Seherezádénak 1001 éjszaka alatt ki kell találnia, különben kivégzik. Éjszakánként egyetlen — általa választott — vektorról megkérdezheti, hogy mik a koordinátái. Életben marad-e Seherezádé?

(b) Mi a helyzet akkor, ha mindig csak az első koordinátára kérdezhet rá, és a kegyelem feltétele az első bázisvektor kitalálása?

5. LINEÁRIS LEKÉPEZÉSEK

Lineáris leképezéseknek (vagy vektortérhomomorfizmusoknak) a vektorterek művelettartó leképezéseit nevezzük. Fontos speciális eset az izomorfizmus, amikor a leképezés kölcsönösen egyértelmű, ekkor a két vektortér „tulajdonképpen ugyanaz". A vektorterek „szép" szerkezetét mutatja, hogy a vektorteret már a dimenziója egyértelműen meghatározza, azaz (rögzített test felett) bármely két egyező dimenziójú vektortér izomorf.

Látni fogjuk, hogy a lineáris leképezések — a közöttük bevezetett műveleteket is beleértve — szoros kapcsolatban állnak a mátrixokkal. A leképezések mátrixokkal történő jellemzése mind elméleti, mind pedig gyakorlati szempontból rendkívül jelentős.

5.1. Lineáris leképezés

5.1.1 Definíció

Legyenek V_1 és V_2 *ugyanazon* T kommutatív test feletti vektorterek. A V_1-*ről* V_2-*be* ható $\mathcal{A}$ függvényt *(homogén) lineáris leképezés*nek nevezzük, ha *művelettartó*, azaz

(i) minden $\mathbf{u}$, $\mathbf{v} \in V_1$-re $\mathcal{A}(\mathbf{u}+\mathbf{v}) = \mathcal{A}\mathbf{u} + \mathcal{A}\mathbf{v}$;
(ii) minden $\mathbf{u} \in V_1$, $\lambda \in T$-re $\mathcal{A}(\lambda\mathbf{u}) = \lambda(\mathcal{A}\mathbf{u})$. ♣

A lineáris leképezés tehát a V_1 vektortér *minden* eleméhez *egyértelműen* hozzárendel egy V_2-beli vektort. Az nyugodtan előfordulhat, hogy *több* V_1-beli elemhez is ugyanazt a V_2-beli vektort rendeljük hozzá, azaz egy V_2-beli vektornak lehet több *ősképe* is V_1-ben. Másfelől, az sem biztos, hogy minden V_2-beli vektor fellép a képek között, azaz lehet, hogy valamely V_2-beli vektornak egyáltalán nincs ősképe V_1-ben.

Az (i)-ben szereplő $+$ jelek nem ugyanazt a műveletet jelölik: a bal oldalon a V_1-beli, a jobb oldalon pedig a V_2-beli összeadásról van szó. Hasonló a helyzet (ii)-ben a skalárral való szorzással.

A lineáris leképezéseket írott nagybetűvel fogjuk jelölni. Az elnevezésben a „homogén" jelzőt általában elhagyjuk. Maga a fogalom az algebrai struktúrák *homomorfizmus*ának speciális esete.

A lineáris leképezés az összegtartásból és a skalárszorostartásból következően a nullelemet, az ellentettet és a lineáris kombinációt is „tartja":

5.1.2 Tétel

I. $\mathcal{A}\mathbf{0}_1 = \mathbf{0}_2$, ahol $\mathbf{0}_i$ a V_i vektortér nulleleme.
II. $\mathcal{A}(-\mathbf{u}) = -(\mathcal{A}\mathbf{u})$.
III. $\mathcal{A}(\lambda_1\mathbf{u}_1 + \ldots + \lambda_k\mathbf{u}_k) = \lambda_1\mathcal{A}\mathbf{u}_1 + \ldots + \lambda_k\mathcal{A}\mathbf{u}_k$. ♣

Bizonyítás: Az összegtartásból $\mathcal{A}\mathbf{u} = \mathcal{A}(\mathbf{u} + \mathbf{0}_1) = \mathcal{A}\mathbf{u} + \mathcal{A}\mathbf{0}_1$. Itt mindkét oldalhoz az $\mathcal{A}\mathbf{u}$ vektor (V_2-beli) ellentettjét hozzáadva, megkapjuk I-et. Ezután az $\mathcal{A}$ leképezést az $\mathbf{u}+(-\mathbf{u}) = \mathbf{0}$ összegre alkalmazva, a művelettartás és I. igazolja II-t. (Okoskodhattunk volna a $-\mathbf{u} = (-1)\mathbf{u}$ összefüggés alapján is.) Végül III. azonnal adódik (i) és (ii) ismételt alkalmazásával. ■

Minden lineáris leképezés két fontos halmazt indukál; a képelemek összességét (V_2-ben), ez a *képtér*, valamint a $\mathbf{0}$-ra képződő (V_1-beli) elemek halmazát, ez a *magtér*:

5.1.3 Definíció

Legyen $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be. Az $\mathcal{A}$ leképezés *képtere* a képelemek halmaza, ezt $\operatorname{Im}\mathcal{A}$-val jelöljük. Tehát

$$\operatorname{Im}\mathcal{A} = \{\mathbf{y} \in V_2 \mid \exists \mathbf{x} \in V_1 \;\; \mathcal{A}\mathbf{x} = \mathbf{y}\} = \{\mathcal{A}\mathbf{x} \mid \mathbf{x} \in V_1\}\,. \;\clubsuit$$

5.1.4 Definíció

Legyen $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be. Az $\mathcal{A}$ leképezés *magtere* a V_2 nullvektorára képződő elemek halmaza, ezt $\operatorname{Ker}\mathcal{A}$-val jelöljük. Tehát

$$\operatorname{Ker}\mathcal{A} = \{\mathbf{x} \in V_1 \mid \mathcal{A}\mathbf{x} = \mathbf{0}\}\,. \;\clubsuit$$

$\operatorname{Im}\mathcal{A}$ így V_2-nek, $\operatorname{Ker}\mathcal{A}$ pedig V_1-nek részhalmaza. Mint az elnevezés jelzi, ennél több is igaz:

5.1.5 Tétel

$\operatorname{Im}\mathcal{A}$ altér V_2-ben, $\operatorname{Ker}\mathcal{A}$ altér V_1-ben. ♣

Bizonyítás: A magtér nem üres, mert $\mathcal{A}\mathbf{0} = \mathbf{0}$, továbbá zárt a műveletekre, hiszen ha $\mathcal{A}\mathbf{u} = \mathcal{A}\mathbf{v} = \mathbf{0}$, akkor

$$\mathcal{A}(\mathbf{u}+\mathbf{v}) = \mathcal{A}\mathbf{u} + \mathcal{A}\mathbf{v} = \mathbf{0}+\mathbf{0} = \mathbf{0} \quad \text{és} \quad \mathcal{A}(\lambda\mathbf{u}) = \lambda(\mathcal{A}\mathbf{u}) = \lambda\mathbf{0} = \mathbf{0}\,.$$

A képtérre vonatkozó állítás hasonlóan igazolható. ■

Példák lineáris leképezésre

P1. Legyen $V_1 = V_2$ a síkvektorok szokásos vektortere ($T = \mathbf{R}$). Ekkor lineáris leképezés pl.

(a) az origó körül tetszőleges szöggel történő elforgatás;

(b) az origóból történő középpontos nagyítás;

(c) az origón átmenő bármely egyenesre való tükrözés;

(d) az origón átmenő bármely egyenesre történő adott irányú vetítés.

Az eltolás *nem* (homogén) lineáris leképezés, mert például a nullvektor képe nem a nullvektor.

Az (a), (b) és (c) példánál $\operatorname{Ker}\mathcal{A} = \mathbf{0}$, $\operatorname{Im}\mathcal{A} = V_2$, a (d) esetben a képtér az az egyenes, amelyre vetítünk, a magtér pedig a vetítés irányába eső, az origón átmenő egyenes.

P2. Tetszőleges V_1 és V_2 esetén feleltessük meg V_1 minden elemének a V_2 nullelemét. Ezt a lineáris leképezést a *nulla leképezés*nek nevezzük és $\mathcal{O}$-val jelöljük. Magtere a teljes V_1, képtere a V_2-beli $\mathbf{0}$.

P3. Ha $V = V_1 = V_2$, akkor feleltessük meg minden elemnek önmagát. Ezt a lineáris leképezést az *identikus leképezés*nek nevezzük és $\mathcal{E}$-vel jelöljük. Magtere a $\mathbf{0}$, képtere a teljes V.

P4. Legyen $A \in T^{k\times n}$, $V_1 = T^n$, $V_2 = T^k$, és legyen a lineáris leképezés az A mátrixszal történő szorzás, azaz $\mathcal{A}\mathbf{x} = A\mathbf{x}$. A kép- és magtér éppen az A mátrix kép-, illetve magtere lesz (lásd a 4.2 pont P4 példáját).

P5. Legyen V_1 egy n-dimenziós vektortér és $V_2 = T^n$. Rögzítsük le V_1-nek egy bázisát, és tetszőleges V_1-beli vektort írjunk fel a báziselemek lineáris kombinációjaként. Minden vektornak feleltessük meg az ebben a felírásban szereplő koordinátákból képezett T^n-beli vektort (ezt az eredeti vektornak az adott bázis szerinti *mátrix*ának vagy *koordinátavektor*ának nevezzük). Az így kapott lineáris leképezés magtere $\mathbf{0}$, képtere a teljes T^n.

P6. A matematika legkülönbözőbb területei igen bőségesen szolgáltatnak fontos példákat lineáris leképezésekre. Az analízis témaköréből választott alábbi — meglehetősen pongyola módon megfogalmazott — megfeleltetéseknél az Olvasóra bízzuk a vektorterek pontos megadását, a leképezések linearitásának a belátását, valamint a mag- és a képtér meghatározását.

Rendeljük hozzá (alkalmas valós) függvényekhez a helyettesítési értéküket, a deriváltjukat, az integráljukat, az értelmezési tartomány egy adott

részhalmazára történő megszorításukat, egy adott függvénnyel vett szorzatukat, sorozatokhoz a határértéküket, az elemek (végtelen) összegét, alkalmas részsorozatot stb.

További példák: lásd az 5.1.1–5.1.4 feladatokat.

5.1.6 Definíció

Azokat a lineáris leképezéseket, amelyeknél $V = V_1 = V_2$, a V vektortér *lineáris transzformáció*inak nevezzük. ♣

Lineáris transzformáció esetén is előfordulhat, hogy a képtér nem a teljes V, továbbá több vektornak is lehet ugyanaz a képe.

A P1 és P3 példák tehát lineáris transzformációk.

Feladatok

5.1.1 Legyen $V = V_1 = V_2$ a valós test feletti legfeljebb 100-adfokú polinomok (és a 0) szokásos vektortere. Döntsük el, hogy az alábbi megfeleltetések lineáris transzformációk-e V-n, és ha igen, adjuk meg kép- és magterüket, valamint ezek dimenzióját. Egy általános polinomot f-fel vagy szükség esetén $f(x)$-szel, az i-edfokú tag együtthatóját α_i-vel, a főegyütthatót α_n-nel jelöljük (tehát $\alpha_n \neq 0$, ha f nem a nullpolinom).

(a) $f \mapsto f'$; (b) $f(x) \mapsto xf(x)$;

(c) $f(x) \mapsto f(x) - xf'(x)$; (d) $f(x) \mapsto f(x+1) - f(x)$;

(e) $f \mapsto \alpha_0 x$; (f) $f \mapsto \alpha_n x^2$;

(g) $f \mapsto (\alpha_0 + \alpha_1 + \ldots + \alpha_n)(x + x^2)$; (h) $f \mapsto (\deg f)x^3$;

(i) $f \mapsto f$ maradéka $x^7 + 4x + 1$-gyel osztva;

j) $f \mapsto \alpha_n + \alpha_{n-1}x + \ldots + \alpha_0 x^n$.

5.1.2 Legyen $T = \mathbf{R}$ és $V = V_1 = V_2 = \mathbf{C}$ a szokásos műveletekkel. Döntsük el, hogy az alábbi megfeleltetések lineáris transzformációk-e V-n, és ha igen, adjuk meg kép- és magterüket, valamint ezek dimenzióját. Minden z komplex számnak feleltessük meg

(a) a valós részét;
(b) a valós és a képzetes része közül a nagyobbikat (ha egyenlők, akkor bármelyiket);
(c) az abszolút értékét;
(d) a szögét;

(e) a konjugáltját;
(f) egy rögzített komplex számmal való szorzatát;
(g) önmagával való szorzatát;
(h) a valós rész π-szerese $(1+i)$-szeresének és a képzetes rész $\sqrt{2}$-szerese $(1111i-5/3)$-szorosának a különbségét.

5.1.3 Legyen T a modulo 2 maradékosztálytest, $V_1 = T^{3\times 3}$, $V_2 = T^3$ a szokásos műveletekkel. Döntsük el, hogy az alábbi megfeleltetések lineáris leképezések-e V_1-ről V_2-be, és ha igen, adjuk meg kép- és magterüket, valamint ezek dimenzióját. Minden mátrixnak feleltessük meg

(a) a középső oszlopát;
(b) azt a vektort, amelynek minden koordinátája a mátrix determinánsa;
(c) azt a vektort, amelynek minden koordinátája a mátrix nyoma (a főátló elemeinek az összege);
(d) azt a vektort, amelynek minden koordinátája a mátrix rangjának modulo 2 vett maradéka;
(e) a csupa 1 koordinátájú (oszlop)vektorral való szorzatát;
(f) a csupa 1 koordinátájú vektort, ha a mátrix reguláris volt, és a nullvektort, ha a mátrix szinguláris volt.

5.1.4 Legyen $V = V_1 = V_2$ a racionális számsorozatok szokásos vektortere. Egy általános sorozatot $S = (\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots)$ formában jelölünk. Adjuk meg az alábbi lineáris transzformációk kép- és magterét, valamint ezek dimenzióját.

(a) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (0, \alpha_0, \alpha_1, \ldots, \alpha_{n-1}, \ldots)$, azaz a sorozatot eggyel „jobbratoltuk”;

(b) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (\alpha_1, \alpha_2, \alpha_3, \ldots, \alpha_{n+1}, \ldots)$, azaz a sorozatot eggyel „balratoltuk”;

(c) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (\alpha_0, \alpha_0, \alpha_1, \alpha_1, \ldots, \alpha_n, \alpha_n, \ldots)$, azaz a sorozatot „megdupláztuk”;

(d) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (\alpha_0, \alpha_{10}, \alpha_{20}, \ldots, \alpha_{10n}, \ldots)$, azaz a sorozatot „megtizedeltük”;

(e) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (\alpha_0 - \alpha_1, \alpha_1 - \alpha_2, \ldots, \alpha_n - \alpha_{n+1}, \ldots)$, azaz a különbségsorozatot képeztük;

(f) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (\alpha_0 + \alpha_1, \alpha_0 - \alpha_1, \alpha_2 + \alpha_3, \alpha_2 - \alpha_3, \ldots)$;

(g) $(\alpha_0, \alpha_1, \ldots, \alpha_n, \ldots) \mapsto (\alpha_0 + \alpha_1, \alpha_2 + \alpha_3, \alpha_0 + \alpha_2, \alpha_1 + \alpha_3, \alpha_4 + \alpha_5, \alpha_6 + \alpha_7, \alpha_4 + \alpha_6, \alpha_5 + \alpha_7, \ldots)$.

5.1.5 Legyen W a V vektortér egy nem triviális altere. Lineáris transzformációt definiálnak-e V-n az alábbi megfeleltetések?

(a) $\mathcal{A}\mathbf{x} = \begin{cases} \mathbf{x}, & \text{ha } \mathbf{x} \in W; \\ \mathbf{0}, & \text{ha } \mathbf{x} \notin W. \end{cases}$

(b) $\mathcal{B}\mathbf{x} = \begin{cases} \mathbf{x}, & \text{ha } \mathbf{x} \notin W; \\ \mathbf{0}, & \text{ha } \mathbf{x} \in W. \end{cases}$

5.1.6 Adjunk példát olyan leképezésre valamely V_1 és V_2 (azonos T test feletti) vektorterek között, amely

(a) skalárszorostartó, de nem összegtartó;
(b) összegtartó, de nem skalárszorostartó;
(c) sem az összeget, sem a skalárszorost nem tartja.

5.1.7 Adjuk meg az összes olyan V vektorteret, amely rendelkezik az alábbi tulajdonsággal. Ha V' tetszőleges vektortér ugyanazon test felett, és V-nek a V'-be történő valamely leképezése skalárszorostartó, akkor ez a leképezés szükségképpen lineáris.

*5.1.8 Bizonyítsuk be, hogy

(a) a modulo p maradékosztályok teste, illetve
(b) a racionális számok teste

feletti vektorterek esetében egy összegtartó leképezés szükségképpen lineáris.

Mi a helyzet a valós test felett?

5.1.9 Legyen $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be, $\mathbf{c}_i \in V_1$. Melyek igazak az alábbi állítások közül?

(a) Ha $\mathbf{c}_1, \ldots, \mathbf{c}_k$ lineárisan független, akkor $\mathcal{A}\mathbf{c}_1, \ldots, \mathcal{A}\mathbf{c}_k$ is lineárisan független.

(b) Ha $\mathcal{A}\mathbf{c}_1, \ldots, \mathcal{A}\mathbf{c}_k$ lineárisan független, akkor $\mathbf{c}_1, \ldots, \mathbf{c}_k$ is lineárisan független.

(c) Ha $\mathbf{c}_1, \ldots, \mathbf{c}_k$ generátorrendszer V_1-ben, akkor $\mathcal{A}\mathbf{c}_1, \ldots, \mathcal{A}\mathbf{c}_k$ generátorrendszer V_2-ben.

(d) Ha $\mathbf{c}_1, \ldots, \mathbf{c}_k$ generátorrendszer V_1-ben, akkor $\mathcal{A}\mathbf{c}_1, \ldots, \mathcal{A}\mathbf{c}_k$ generátorrendszer $\operatorname{Im}\mathcal{A}$-ban.

(e) Ha $\mathcal{A}\mathbf{c}_1, \ldots, \mathcal{A}\mathbf{c}_k$ generátorrendszer $\operatorname{Im}\mathcal{A}$-ban, akkor $\mathbf{c}_1, \ldots, \mathbf{c}_k$ generátorrendszer V_1-ben.

5.1.10 Legyen $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be és $\mathbf{c}_1, \ldots, \mathbf{c}_k$ generátorrendszer V_1-ben. Lássuk be, hogy az $\mathcal{A}\mathbf{c}_1, \ldots, \mathcal{A}\mathbf{c}_k$ vektorrendszer rangja $\dim \operatorname{Im}\mathcal{A}$.

5.1.11 Legyen $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be. Bizonyítsuk be, hogy

$$\mathcal{A}\mathbf{u} = \mathcal{A}\mathbf{v} \iff \mathbf{u} - \mathbf{v} \in \operatorname{Ker}\mathcal{A}\,.$$

5.1.12 Bizonyítsuk be, hogy $\operatorname{Im}\mathcal{A}$ bármely két elemének ugyanannyi ősképe van. Mennyi lehet ez a szám, ha a modulo 101 maradékosztályok teste feletti vektorterekről van szó?

5.1.13 Tegyük fel, hogy $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be és $\mathbf{u}_1, \ldots, \mathbf{u}_k$ olyan lineárisan független vektorok V_1-ben, amelyekre $\mathcal{A}\mathbf{u}_1 = \ldots = \mathcal{A}\mathbf{u}_k$. Bizonyítsuk be, hogy $\dim \operatorname{Ker}\mathcal{A} \geq k - 1$.

5.1.14 Tegyük fel, hogy $\mathbf{0} \neq V_1$ véges dimenziós, és legyen $\mathcal{A}$ tetszőleges nem nulla lineáris leképezés V_1-ről V_2-be. Bizonyítsuk be, hogy V_1-nek van olyan $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázisa, amelyre az $\mathcal{A}\mathbf{b}_i$ vektorok mind $\mathbf{0}$-tól különbözők.

5.1.15 Legyen $\mathbf{0} \neq V$ véges dimenziós vektortér és $\mathcal{A} : V \to Z$ lineáris leképezés. Bizonyítsuk be, hogy V-nek akkor és csak akkor van olyan bázisa, amelyre mindegyik báziselem képe ugyanaz, ha $\dim \operatorname{Im}\mathcal{A} \leq 1$.

5.1.16 Legyen $\mathcal{A}$ lineáris leképezés V_1-ről V_2-be. Egy tetszőleges $H \subseteq V_1$ részhalmaz képének az $\mathcal{A}H = \{\mathcal{A}\mathbf{x} \mid \mathbf{x} \in H\} \subseteq V_2$ halmazt nevezzük. Legyen U és Z két altér V_1-ben. Milyen kapcsolatban áll egymással

(a) $\mathcal{A}U \cap \mathcal{A}Z$ és $\mathcal{A}(U \cap Z)$;

(b) $\mathcal{A}\langle U, Z\rangle$ és $\langle \mathcal{A}U, \mathcal{A}Z\rangle$?

5.2. Izomorfizmus

5.2.1 Definíció

Ha egy $V_1 \to V_2$ lineáris leképezés egyúttal kölcsönösen egyértelmű (egy-egyértelmű, bijektív) megfeleltetést létesít V_1 és V_2 között, akkor *izomorfizmus*nak nevezzük. A V vektortér akkor *izomorf* a Z vektortérrel, ha létezik $V \to Z$ izomorfizmus. ♣

Azt, hogy V izomorf Z-vel, $V \cong Z$ módon jelöljük.

Az izomorfizmus tehát olyan lineáris leképezés, amelynél V_2 minden elemének *pontosan egy* ősképe van. Más szóval: különböző V_1-beli elemek képe szükségképpen különböző, és minden V_2-beli elem fellép képként.

Az izomorf vektorterek algebrai szempontból megkülönböztethetetlenek egymástól: teljesen ugyanolyanok, csak az elemek és a műveletek másképp vannak jelölve.

Az előző pont példái közül a P1a–c, P3 és P5 leképezések izomorfizmusok. Az alábbi egyszerű észrevétel mutatja, hogy az izomorfizmus már a magteréről és a képteréről felismerhető.

5.2.2 Tétel
Az $\mathcal{A} : V_1 \to V_2$ lineáris leképezés akkor és csak akkor izomorfizmus, ha $\operatorname{Ker}\mathcal{A} = \mathbf{0}$ és $\operatorname{Im}\mathcal{A} = V_2$. ♣

Bizonyítás: Az $\operatorname{Im}\mathcal{A} = V_2$ feltétel nyilván ekvivalens azzal, hogy V_2 minden eleme fellép képként. Így elég belátni, hogy a magtérre vonatkozó feltétel éppen azt jelenti, hogy különböző vektorok képe is különböző. Tegyük fel először, hogy különböző elemek képe különböző. Mivel a $\mathbf{0}$ képe $\mathbf{0}$, más vektor nem képződhet a $\mathbf{0}$-ba, vagyis a magtér valóban csak a $\mathbf{0}$-ból áll. Megfordítva, tegyük fel, hogy $\operatorname{Ker}\mathcal{A} = \mathbf{0}$ és legyen $\mathcal{A}\mathbf{u} = \mathcal{A}\mathbf{v}$. Az 5.1.11 feladat alapján ekkor $\mathbf{u} - \mathbf{v} \in \operatorname{Ker}\mathcal{A} = \mathbf{0}$, tehát valóban $\mathbf{u} = \mathbf{v}$. ■

Az, hogy egy V_1 vektortér izomorf-e egy V_2 vektortérrel vagy sem, egy relációt jelent az adott test feletti vektorterek körében. Ezt a relációt *izomorfiá*nak szokás nevezni.

5.2.3 Tétel
A vektorterek körében az izomorfia ekvivalenciareláció. ♣

Bizonyítás:
Reflexivitás: az identikus leképezés nyilván izomorfizmus.
Szimmetria: Ha $\mathcal{A} : U \to V$ izomorfizmus, akkor megmutatjuk, hogy az $\mathcal{A}$ leképezés inverze, $\mathcal{A}^{-1} : V \to U$ is izomorfizmus. Az egy-egyértelműség világos, így csak a művelettartást kell igazolni. Nézzük pl. az összegtartást. Legyen $\mathbf{v}_1$, $\mathbf{v}_2 \in V$. Ekkor $\mathcal{A}^{-1}\mathbf{v}_i$ az az (egyértelműen meghatározott) $\mathbf{u}_i \in U$, amelyre $\mathcal{A}\mathbf{u}_i = \mathbf{v}_i$. Mivel $\mathcal{A}$ összegtartó, ezért

$$\mathcal{A}(\mathbf{u}_1 + \mathbf{u}_2) = \mathcal{A}\mathbf{u}_1 + \mathcal{A}\mathbf{u}_2 = \mathbf{v}_1 + \mathbf{v}_2,$$

vagyis valóban

$$\mathcal{A}^{-1}(\mathbf{v}_1 + \mathbf{v}_2) = \mathbf{u}_1 + \mathbf{u}_2 = \mathcal{A}^{-1}\mathbf{v}_1 + \mathcal{A}^{-1}\mathbf{v}_2.$$

A skalárszorostartás ugyanígy igazolható.
Tranzitivitás: az előzőhöz hasonlóan belátható, hogy két izomorfizmus egymásutánja (kompozíciója) is izomorfizmus. ■

A fentiek alapján tehát jogosan mondhatjuk, hogy két vektortér „egymással" izomorf.

A 4.7 pontban már előrevetítettük, hogy minden véges (és $\neq 0$) dimenziós vektortér valamelyik T^n-nel izomorf:

5.2.4 Tétel

Ha $n \neq 0$ és V a T test felett egy n-dimenziós vektortér, akkor $V \cong T^n$. ♣

Bizonyítás: Az izomorfiát az 5.1 pont P5 példájában megadott leképezés igazolja. ■

A fentiek következménye, hogy adott T test felett „csak egyetlen" n-dimenziós vektortér létezik:

5.2.5 Tétel

Egy T test feletti két véges dimenziós vektortér akkor és csak akkor izomorf, ha a dimenziójuk megegyezik. Azaz véges dimenziós U és V esetén

$$U \cong V \iff \dim U = \dim V\,. \ \clubsuit$$

Bizonyítás: Feltehetjük, hogy egyik vektortér sem a $\mathbf{0}$, mert akkor az állítás nyilvánvaló. Ha mindkét dimenzió n, akkor az előző tétel szerint mindkét vektortér izomorf T^n-nel, tehát — mivel az izomorfia ekvivalenciareláció — egymással is izomorfak. Megfordítva, legyen $U \cong V$, azaz van egy $\mathcal{A} : U \to V$ izomorfizmus. Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$ bázis U-ban. Megmutatjuk, hogy ekkor $\mathcal{A}\mathbf{u}_1, \ldots, \mathcal{A}\mathbf{u}_n$ bázis lesz V-ben, ami igazolni fogja a dimenziók egyenlőségét. Legyen $\mathbf{v} \in V$ tetszőleges. Be kell látnunk, hogy $\mathbf{v}$ egyértelműen felírható

$$\mathbf{v} = \lambda_1(\mathcal{A}\mathbf{u}_1) + \ldots + \lambda_n(\mathcal{A}\mathbf{u}_n)$$

alakban. Az $\mathcal{A}$ leképezés linearitása miatt ez átírható a

$$\mathbf{v} = \mathcal{A}(\lambda_1\mathbf{u}_1 + \ldots + \lambda_n\mathbf{u}_n)$$

feltétellé. Az egy-egyértelműség miatt $\mathbf{v}$-nek pontosan egy $\mathbf{u} \in U$ ősképe van, amelyre $\mathcal{A}\mathbf{u} = \mathbf{v}$. Ennek alapján az előző feltétel tovább alakítható

$$\mathbf{u} = \lambda_1\mathbf{u}_1 + \ldots + \lambda_n\mathbf{u}_n$$

formában. Mivel $\mathbf{u}_1, \ldots, \mathbf{u}_n$ bázis U-ban, ezért ilyen tulajdonságú $\lambda_1, \ldots, \lambda_n$ együtthatórendszer valóban pontosan egy létezik. ■

Az 5.2.5 Tétel végtelen dimenzióra is átvihető, ha dimenzión a szokásos módon a (Hamel-)bázis *számosság*át értjük (lásd a 4.5 pont végét).

Feladatok

5.2.1 Keressük meg az izomorfizmusokat az 5.1.1–5.1.4 feladatokban.

5.2.2 Milyen ismert vektorterekkel izomorfak a 4.1.5, illetve 4.1.6 feladatokban megadott vektorterek?

5.2.3 Legyen $\mathcal{A} : U \to V$ lineáris leképezés. Az alábbi feltételek közül melyekből következik, hogy $\mathcal{A}$ izomorfizmus?

(a) Minden U-beli lineárisan független rendszer képe lineárisan független V-ben.

(b) Minden U-beli generátorrendszer képe generátorrendszer V-ben.

(c) Minden U-beli bázis képe bázis V-ben.

(d) Van olyan U-beli bázis, amelynek a képe bázis V-ben.

(e) Van olyan U-beli lineáris független rendszer, amelynek a képe lineárisan független V-ben, és van olyan U-beli generátorrendszer is, amelynek a képe generátorrendszer V-ben.

5.2.4 Bizonyítsuk be, hogy adott test felett bármely két véges dimenziós vektortér közül valamelyik izomorf a másik egy alkalmas alterével.

5.2.5 Egy n-dimenziós vektortérben hány páronként nemizomorf altér van?

5.2.6 Az alábbi $\mathbf{R}$ feletti vektorterek között keressük meg az izomorfakat (a műveletek a szokásosak, a polinomoknál a 0 polinomot mindig beleértjük):

(a) Azok a legfeljebb 20-adfokú valós együtthatós polinomok, amelyekben minden tag kitevője prímszám.

(b) Azok a legfeljebb 15-ödfokú valós együtthatós polinomok, amelyek (valós függvényként tekintve őket) páros függvények.

(c) Azok a legfeljebb 9-edfokú valós együtthatós polinomok, amelyeknek a π gyöke.

(d) Azok a legfeljebb 9-edfokú valós együtthatós polinomok, amelyeknek az i (komplex képzetes egység) gyöke.

(e) Azok a legfeljebb 100-adfokú valós együtthatós polinomok, amelyek $x^{29} + 1$-gyel és $2x^{29} + 1$-gyel is oszthatók.

(f) $\mathbf{C}^4$ (a *valós* test felett!)

(g) Azok a 3×4-es valós mátrixok, amelyeknek az első és utolsó sora megegyezik.

(h) Azok a 7×7-es valós mátrixok, amelyekben a főátlóbeli elemek mind egyenlők.
(i) Azok a 7×7-es valós mátrixok, amelyekben a főátlón kívüli elemek mind egyenlők.
(j) Azok a végtelen valós számsorozatok, amelyekben bármely kilenc szomszédos elem összege 0.
(k) Azok a minden valós számon értelmezett valós értékű függvények, amelyeknek az $x = 1, 2, \ldots, 8$ helyek kivételével minden helyettesítési értéke 0.

5.3. Leképezés jellemzése a báziselemek képével

Az, hogy egy leképezés lineáris, az első pillanatban nem tűnik nagyon erős megkötésnek. A látszat azonban csal. Ez rögtön kiderül, ha valamely vektortéren elemenként próbálunk értelmezni egy lineáris leképezést. Hacsak nem valami „szép szabály" szerint dolgozunk, szinte biztos, hogy a leképezésünk nem „sikeredik" lineárissá (lásd pl. az 5.1.5 feladatot). A művelettartás követelménye láthatatlan szálakkal hálózza be a leképezés szerkezetét, amelybe könnyen belegabalyodhatunk. Ugyanez a probléma jelentkezik akkor is, ha egy valóban lineáris leképezést valahogy kezelni akarunk. Reménytelenül el lehet veszni a(z általában) végtelen sok elem és a művelettartásból adódó áttekinthetetlennek tűnő szabályrengeteg útvesztőjében.

Ezeken a gondokon teljes mértékben segít az alábbi fontos tétel. Ez lényegében azt fejezi ki, hogy a lineáris leképezések egy (rögzített) bázis elemeinek a képeivel jellemezhetők: egyrészt a báziselemek képei tetszőlegesen, minden megkötöttség nélkül megválaszthatók, másrészt viszont ezek már egyértelműen meghatározzák a többi elem képét, azaz a teljes lineáris leképezést.

5.3.1 Tétel

Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis a V_1 vektortérben, és legyenek $\mathbf{c}_1, \ldots, \mathbf{c}_n$ *tetszőleges* elemek a(z ugyanazon test feletti) V_2 vektortérben. Ekkor *pontosan egy* olyan $\mathcal{A} : V_1 \to V_2$ lineáris leképezés létezik, amelyre

$$\mathcal{A}\mathbf{b}_i = \mathbf{c}_i, \quad i = 1, 2, \ldots, n\,,$$

azaz, amely a $\mathbf{b}_i$ báziselemeket rendre éppen a kijelölt $\mathbf{c}_i$ elemekbe viszi. ♣

Bizonyítás: Vegyünk V_1-ből egy tetszőleges $\mathbf{u}$ vektort, ez egyértelműen felírható $\mathbf{u} = \beta_1\mathbf{b}_1 + \ldots + \beta_n\mathbf{b}_n$ alakban. *Ha létezik* a mondott tulajdonságú $\mathcal{A}$

lineáris leképezés, akkor a feltételek és a művelettartás miatt szükségképpen

$$\mathcal{A}\mathbf{u} = \mathcal{A}(\beta_1\mathbf{b}_1 + \ldots + \beta_n\mathbf{b}_n) = \beta_1(\mathcal{A}\mathbf{b}_1) + \ldots + \beta_n(\mathcal{A}\mathbf{b}_n) = \beta_1\mathbf{c}_1 + \ldots + \beta_n\mathbf{c}_n$$

teljesül. Ez azt mutatja, hogy $\mathcal{A}\mathbf{u}$ egyértelműen meg van határozva, tehát legfeljebb egy ilyen $\mathcal{A}$ létezhet. Sőt, az is kiderült, hogy *csak* az

$$\mathcal{A}\mathbf{u} = \beta_1\mathbf{c}_1 + \ldots + \beta_n\mathbf{c}_n$$

képlettel definiált leképezés jöhet szóba. Erről kell tehát megmutatni, hogy valóban lineáris leképezés. Először is vegyük észre, hogy a β_i együtthatók a $\mathbf{b}_i$-k bázis volta miatt léteznek és egyértelműek, tehát $\mathcal{A}\mathbf{u}$ tényleg egyértelműen definiálva van. Az összegtartás igazolásához legyen $\mathbf{v} = \gamma_1\mathbf{b}_1 + \ldots + \gamma_n\mathbf{b}_n$, ekkor $\mathbf{u} + \mathbf{v} = (\beta_1 + \gamma_1)\mathbf{b}_1 + \ldots + (\beta_n + \gamma_n)\mathbf{b}_n$. Az $\mathcal{A}$ leképezés definíciója alapján

$$\mathcal{A}(\mathbf{u} + \mathbf{v}) = (\beta_1 + \gamma_1)\mathbf{c}_1 + \ldots + (\beta_n + \gamma_n)\mathbf{c}_n = \mathcal{A}\mathbf{u} + \mathcal{A}\mathbf{v}\,.$$

A skalárszorostartás ugyanígy igazolható. ■

Ennek a tételnek az alapján a lineáris leképezéseket általában úgy fogjuk megadni, hogy a báziselemek képeit választjuk meg. Ezen múlik majd a lineáris leképezések mátrixok segítségével történő jellemzése is (lásd az 5.7 pontot).

Feladatok

5.3.1 Legyen W a V véges dimenziós vektortér egy nem triviális altere. Bizonyítsuk be, hogy V-nek létezik olyan lineáris transzformációja, amelynek W a magtere, illetve a képtere (vö. az 5.1.5 feladattal).

5.3.2 Melyek azok a $V_1 \to V_2$ lineáris leképezések, amelyeket már a magterük, illetve a képterük teljesen meghatároz (azaz semelyik másik $V_1 \to V_2$ lineáris leképezésnek nem lehet ugyanez a mag-, illetve képtere)?

5.3.3

(a) Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$ generátorrendszer V_1-ben, és legyenek $\mathbf{c}_1, \ldots, \mathbf{c}_n$ *tetszőleges* elemek a(z ugyanazon test feletti) V_2-ben. Hány olyan $\mathcal{A} : V_1 \to V_2$ lineáris leképezés létezik, amelyre $\mathcal{A}\mathbf{u}_i = \mathbf{c}_i$, $i = 1, 2, \ldots, n$?

(b) Vizsgáljuk meg ugyanezt a kérdést, ha az $\mathbf{u}_i$-kről csak annyit tudunk, hogy lineárisan függetlenek.

5.3.4 Hány olyan $\mathcal{A}$ lineáris transzformáció van az $\mathbf{R}^2$ vektortéren, amelyre

(a) $\mathcal{A}\begin{pmatrix}1\\3\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$ és $\mathcal{A}\begin{pmatrix}2\\6\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$;

(b) $\mathcal{A}\begin{pmatrix}1\\3\end{pmatrix}=\begin{pmatrix}0\\0\end{pmatrix}$ és $\mathcal{A}\begin{pmatrix}2\\3\end{pmatrix}=\begin{pmatrix}1\\0\end{pmatrix}$;

(c) $\mathcal{A}\begin{pmatrix}1\\3\end{pmatrix}=\begin{pmatrix}6\\5\end{pmatrix}$ és $\mathcal{A}\begin{pmatrix}2\\6\end{pmatrix}=\begin{pmatrix}12\\10\end{pmatrix}$?

5.3.5 Legyenek k és n pozitív egészek és T a modulo p maradékosztályok teste. Hány $\mathcal{A}: T^n \to T^k$ lineáris leképezés létezik?

5.3.6 Legyenek V_1 és V_2 tetszőleges véges dimenziós vektorterek egy T test felett. Bizonyítsuk be, hogy létezik olyan $\mathcal{A}: V_1 \to V_2$ lineáris leképezés, amelyre $\operatorname{Ker}\mathcal{A}=\mathbf{0}$ és $\operatorname{Im}\mathcal{A}=V_2$ közül legalább az egyik teljesül.

5.4. Dimenziótétel

5.4.1 Tétel

Tegyük fel, hogy V_1 véges dimenziós és V_2 tetszőleges vektortér a T test felett, továbbá legyen $\mathcal{A}$ tetszőleges lineáris leképezés V_1-ről V_2-be. Ekkor

$$\dim\operatorname{Ker}\mathcal{A}+\dim\operatorname{Im}\mathcal{A}=\dim V_1\,.\ \clubsuit$$

A V_2 dimenziója értelemszerűen nem játszik szerepet, hiszen V_2 tartalmazhat tetszőleges nagy részt $\mathcal{A}$ képterén kívül.

A bizonyításból az is kiderül, hogy ha $\dim V_1=\infty$, akkor a mag és a kép közül legalább az egyiknek a dimenziója végtelen, tehát a tétel erre az esetre is igaz. Sőt, abban az erősebb formában is érvényben marad, ha a végtelen dimenziók között a Hamel-bázisok *számosság*a alapján különbséget teszünk (lásd a 4.6.1 Definíció utáni megjegyzést).

Bizonyítás: Az állítás nyilvánvaló, ha $\mathcal{A}=\mathcal{O}$. Egyébként legyen $\mathcal{A}\mathbf{c}_1,\ldots,\mathcal{A}\mathbf{c}_r$ bázis $\operatorname{Im}\mathcal{A}$-ban és $\mathbf{b}_1,\ldots,\mathbf{b}_s$ bázis $\operatorname{Ker}\mathcal{A}$-ban. ($\operatorname{Ker}\mathcal{A}=\mathbf{0}$ esetén $s=0$, és a további gondolatmenet erre is érvényes. A részletek átgondolását az Olvasóra bízzuk.) A tételhez elég belátnunk, hogy $\mathbf{b}_1,\ldots,\mathbf{b}_s,\mathbf{c}_1,\ldots,\mathbf{c}_r$ bázis V_1-ben, azaz minden $\mathbf{u}\in V_1$ egyértelműen felírható ezek lineáris kombinációjaként.

A képtér bázisát használva

$$\mathcal{A}\mathbf{u} = \sum_{i=1}^{r} \lambda_i (\mathcal{A}_i \mathbf{c}_i) = \mathcal{A}\left(\sum_{i=1}^{r} \lambda_i \mathbf{c}_i\right)$$

egyértelmű λ_i együtthatókkal. Az 5.1.11 feladat alapján ezzel ekvivalens, hogy

$$\mathbf{u} - \sum_{i=1}^{r} \lambda_i \mathbf{c}_i \in \operatorname{Ker} \mathcal{A}, \quad \text{vagyis} \quad \mathbf{u} - \sum_{i=1}^{r} \lambda_i \mathbf{c}_i = \sum_{j=1}^{s} \mu_j \mathbf{b}_j$$

egyértelmű μ_j együtthatókkal. Tehát $\mathbf{u}$ valóban egyértelműen írható fel a szóban forgó vektorok lineáris kombiációjaként:

$$\mathbf{u} = \sum_{i=1}^{r} \lambda_i \mathbf{c}_i + \sum_{j=1}^{s} \mu_j \mathbf{b}_j. \quad \blacksquare$$

A most bizonyított dimenzió-összefüggésnek egyik fontos következménye az

5.4.2 Tétel

Legyen V véges dimenziós vektortér és $\mathcal{A}$ lineáris transzformáció V-n. Ekkor

$$\operatorname{Im} \mathcal{A} = V \iff \operatorname{Ker} \mathcal{A} = \mathbf{0}\,. \quad \clubsuit$$

Bizonyítás: Ha $\operatorname{Im} \mathcal{A} = V$, akkor $\dim \operatorname{Im} \mathcal{A} = \dim V$, tehát $\dim \operatorname{Ker} \mathcal{A} = 0$, vagyis $\operatorname{Ker} \mathcal{A} = \mathbf{0}$. A megfordítás is hasonlóan igazolható (az utolsó lépésben fel kell használni a 4.6.4/II Tételt). $\blacksquare$

Az 5.4.2 Tétel azt mutatja, hogy véges dimenziós tér lineáris transzformációja esetén az izomorfizmusra az 5.2.2 Tételben adott két feltétel bármelyikéből következik a másik. Végtelen dimenzióra ez nem igaz, lásd pl. az 5.1.4 feladatot.

Feladatok

Az alábbi feladatokban szereplő vektorterekről feltesszük, hogy *véges dimenziós*ak.

5.4.1 Mely vektortereknek létezik olyan lineáris transzformációja, amelynél a kép- és magtér egybeesik?

5.4.2 Legyenek $\mathcal{A} : V_1 \to V_2$ és $\mathcal{B} : V_2 \to V_1$ lineáris leképezések. Az alábbi feltételek közül melyekből következik, hogy V_1 és V_2 izomorf?

(a) $\operatorname{Im}\mathcal{A} = V_2$ és $\operatorname{Im}\mathcal{B} = V_1$;

(b) $\operatorname{Ker}\mathcal{A} = \mathbf{0}$ és $\operatorname{Ker}\mathcal{B} = \mathbf{0}$;

(c) $\operatorname{Im}\mathcal{A} = V_2$ és $\operatorname{Ker}\mathcal{B} = \mathbf{0}$.

5.4.3 Legyen $\mathcal{A}$ lineáris transzformáció V-n és $\mathcal{A}\mathbf{u}_1, \ldots, \mathcal{A}\mathbf{u}_k$ generátorrendszer V-ben. Következik-e ebből, hogy az $\mathbf{u}_1, \ldots, \mathbf{u}_k$ vektorok is generátorrendszert alkotnak V-ben?

5.4.4 Oldjuk meg az 5.2.3 feladatot abban az esetben, ha a két vektortér megegyezik.

5.4.5 Egy $\mathcal{A} : V_1 \to V_2$ lineáris leképezésről a következőket tudjuk:

(i) Bármely 4 elem képe lineárisan összefüggő.

(ii) Bármely 6 lineárisan független V_1-beli elem között van olyan, amelynek a képe nem a nulla.

Bizonyítsuk be, hogy $\dim V_1 \leq 8$.

5.4.6 Tegyük fel, hogy az $\mathcal{A}, \mathcal{B} : V_1 \to V_2$ lineáris leképezésekre $\operatorname{Ker}\mathcal{A} \subseteq \subseteq \operatorname{Ker}\mathcal{B}$ és $\operatorname{Im}\mathcal{A} \subseteq \operatorname{Im}\mathcal{B}$. Bizonyítsuk be, hogy ekkor $\operatorname{Ker}\mathcal{A} = \operatorname{Ker}\mathcal{B}$ és $\operatorname{Im}\mathcal{A} = \operatorname{Im}\mathcal{B}$.

5.4.7 Tegyük fel, hogy az $\mathcal{A}, \mathcal{B} : V_1 \to V_2$ lineáris leképezésekre

$$V_1 = \operatorname{Ker}\mathcal{A} \oplus \operatorname{Ker}\mathcal{B} \quad \text{és} \quad V_2 = \operatorname{Im}\mathcal{A} \oplus \operatorname{Im}\mathcal{B}\,.$$

Bizonyítsuk be, hogy ekkor $V_1 \cong V_2$.

5.5. Lineáris leképezések összege és skalárszorosa

5.5.1 Definíció

Az $\mathcal{A}, \mathcal{B} : V_1 \to V_2$ lineáris leképezések *összeg*én azt az $\mathcal{A} + \mathcal{B}$-vel jelölt leképezést értjük, amely minden $\mathbf{u} \in V_1$ vektorhoz az $\mathcal{A}\mathbf{u} + \mathcal{B}\mathbf{u} \in V_2$ vektort rendeli hozzá. Azaz

$$(\mathcal{A} + \mathcal{B})\mathbf{u} = \mathcal{A}\mathbf{u} + \mathcal{B}\mathbf{u}\,. \ \clubsuit$$

Két leképezés összegét tehát csak akkor értelmezzük, ha mindkét leképezés *ugyanarról* a V_1 vektortérről *ugyanabba* a V_2 vektortérbe hat. Ekkor az összegük is V_1-ről V_2-be képez.

A definícióbeli képletben a két + jel nem ugyanazt jelenti: a bal oldalon leképezések összeadásáról van szó, amelyet éppen most értelmezünk, a jobb oldalon pedig V_2-beli vektorok összeadása szerepel. (A képlet tehát már ezért sem tekinthető valamiféle disztributivitásnak.)

5.5.2 Definíció

Az $\mathcal{A} : V_1 \to V_2$ lineáris leképezésnek a $\lambda \in T$ *skalárral való szorzat*án azt a $\lambda\mathcal{A}$-val jelölt leképezést értjük, amely minden $\mathbf{u} \in V_1$ vektorhoz a $\lambda(\mathcal{A}\mathbf{u}) \in V_2$ vektort rendeli hozzá. Azaz

$$(\lambda\mathcal{A})\mathbf{u} = \lambda(\mathcal{A}\mathbf{u})\,. \ \clubsuit$$

A skalárszorosra is az összegnél látottakkal analóg megjegyzések érvényesek.

5.5.3 Tétel

Legyen V_1 és V_2 két tetszőleges vektortér ugyanazon T test felett. Ekkor az összes $V_1 \to V_2$ lineáris leképezésből álló halmaz vektorteret alkot a T test felett az imént definiált műveletekre nézve. Ezt a vektorteret $\mathrm{Hom}\,(V_1\,,\,V_2)$-vel jelöljük. $\clubsuit$

Bizonyítás: Először is azt kell megmutatni, hogy két lineáris leképezés összege, illetve egy lineáris leképezés skalárszorosa is lineáris. Belátjuk, hogy $\mathcal{A}+\mathcal{B}$ összegtartó, a többi hasonlóan igazolható.

$$(\mathcal{A}+\mathcal{B})(\mathbf{u}+\mathbf{v}) = \mathcal{A}(\mathbf{u}+\mathbf{v})+\mathcal{B}(\mathbf{u}+\mathbf{v}) = \mathcal{A}\mathbf{u}+\mathcal{A}\mathbf{v}+\mathcal{B}\mathbf{u}+\mathcal{B}\mathbf{v} = (\mathcal{A}+\mathcal{B})\mathbf{u}+(\mathcal{A}+\mathcal{B})\mathbf{v}.$$

Közben a leképezések összegének definícióját és $\mathcal{A}$, illetve $\mathcal{B}$ összegtartását használtuk ki (valamint a V_2-ben a többtagú összegek tetszőleges átrendezhetőségét).

$\mathrm{Hom}\,(V_1\,,\,V_2)$ nulleleme a $\mathcal{O}$ nulla leképezés, amely V_1 minden elemének a V_2-beli $\mathbf{0}$-t felelteti meg. Könnyen adódik, hogy a $\mathcal{O}$ is lineáris leképezés, és valóban nullelem.

Egy $\mathcal{A}$ lineáris leképezés ellentettje az a $-\mathcal{A}$-val jelölt leképezés lesz, amelyet a $(-\mathcal{A})\mathbf{u} = -(\mathcal{A}\mathbf{u})$ összefüggéssel definiálunk minden $\mathbf{u} \in V_1$-re. Annak ellenőrzését, hogy ez lineáris és valóban eleget tesz az ellentett követelményének, az Olvasóra bízzuk.

Az összes többi vektortéraxióma valamilyen azonosság. Ezek közül $(\lambda+\mu)\mathcal{A} = \lambda\mathcal{A}+\mu\mathcal{A}$ teljesülését részletesen igazoljuk, a többi bizonyítása teljesen hasonlóan történik. Egyfelől

$$[(\lambda+\mu)\mathcal{A}]\mathbf{u} = (\lambda+\mu)(\mathcal{A}\mathbf{u}),$$

másfelől

$$(\lambda\mathcal{A}+\mu\mathcal{A})\mathbf{u}=(\lambda\mathcal{A})\mathbf{u}+(\mu\mathcal{A})\mathbf{u}=\lambda(\mathcal{A}\mathbf{u})+\mu(\mathcal{A}\mathbf{u}).$$

(Közben csak a leképezések közötti műveletek definícióit használtuk.) A jobb oldalakon álló vektorok pedig éppen azért egyeznek meg, mert a szóban forgó axióma a V_2 vektortérben teljesül. ■

Feladatok

5.5.1 Bizonyítsuk be, hogy bármely $\mathcal{A}$, $\mathcal{B}\in\operatorname{Hom}(V_1\,,\,V_2)$ esetén

(a) $\operatorname{Ker}(\mathcal{A}+\mathcal{B})\supseteq\operatorname{Ker}\mathcal{A}\cap\operatorname{Ker}\mathcal{B}$;

(b) $\operatorname{Im}(\mathcal{A}+\mathcal{B})\subseteq\langle\operatorname{Im}\mathcal{A}\,,\,\operatorname{Im}\mathcal{B}\rangle$;

(c) $\operatorname{Ker}(\lambda\mathcal{A})=\operatorname{Ker}\mathcal{A}$, ha $\lambda\neq 0$;

(d) $\operatorname{Im}(\lambda\mathcal{A})=\operatorname{Im}\mathcal{A}$, ha $\lambda\neq 0$.

Az (a) és (b) résznél adjunk példákat, amikor egyenlőség teljesül, illetve nem teljesül.

5.5.2 Legyen $V_1=V_2$ a síkvektorok szokásos vektortere. Mi lesz az $\mathcal{A}+\mathcal{B}$ transzformáció, ha

(a) $\mathcal{A}$ az x-tengelyre, $\mathcal{B}$ az y-tengelyre történő tükrözés;

(b) $\mathcal{A}$ az x-tengelyre, $\mathcal{B}$ az y-tengelyre történő merőleges vetítés;

(c) $\mathcal{A}$ az origó körüli $+60$ fokos, $\mathcal{B}$ az origó körüli -60 fokos elforgatás;

(d) $\mathcal{A}$ az origó körüli Φ, $\mathcal{B}$ az origó körüli $-\Phi$ szöggel történő elforgatás;

(e) $\mathcal{A}$ a helybenhagyás, $\mathcal{B}$ az origó körüli $+90$ fokos elforgatás?

5.5.3 Döntsük el, hogy alteret alkotnak-e $\operatorname{Hom}(V_1\,,\,V_2)$-ben azok a leképezések, amelyeknél

(a) a magtér V_1-nek egy rögzített U_1 altere;

(b) a képtér legfeljebb egydimenziós;

(c) minden elem képe egy előre megadott V_2-beli vektor valamilyen skalárszorosa;

(d) V_1-nek egy előre megadott U_1 alteréből minden elem képe V_2-nek egy előre megadott U_2 alterébe esik;

(e) egy előre megadott V_1-beli elem képe egy előre megadott V_2-beli vektor lesz.

5.5.4 Legyen $V_1 = V_2 = V$, ekkor $\operatorname{Hom}(V_1, V_2)$-t $\operatorname{Hom} V$-vel jelöljük. Döntsük el, hogy alteret alkotnak-e $\operatorname{Hom} V$-ben azok a transzformációk, amelyek

(a) izomorfizmusok;
(b) nem izomorfizmusok;
(c) egy előre megadott vektort önmagába visznek át (azaz helyben hagyják);
(d) magtere tartalmazza a képteret.

5.5.5 Legyenek $\mathcal{A}, \mathcal{B} \in \operatorname{Hom}(V_1, V_2)$. Melyek igazak az alábbi állítások közül?

(a) $\operatorname{Im}\mathcal{A} \cap \operatorname{Im}\mathcal{B} = \mathbf{0} \Rightarrow \operatorname{Ker}(\mathcal{A}+\mathcal{B}) = \operatorname{Ker}\mathcal{A} \cap \operatorname{Ker}\mathcal{B}$.

(b) $\operatorname{Ker}(\mathcal{A}+\mathcal{B}) = \operatorname{Ker}\mathcal{A} \cap \operatorname{Ker}\mathcal{B} \Rightarrow \operatorname{Im}\mathcal{A} \cap \operatorname{Im}\mathcal{B} = \mathbf{0}$.

5.5.6 Legyen a V_1 vektortér egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, a V_2 vektortér egy bázisa pedig $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Definiáljuk a $\mathcal{C}_{ij} \in \operatorname{Hom}(V_1, V_2)$ leképezést a következőképpen:

$$\mathcal{C}_{ij}\mathbf{a}_r = \begin{cases} \mathbf{b}_i, & \text{ha } r = j; \\ \mathbf{0}, & \text{ha } r \neq j. \end{cases} \qquad 1 \leq j \leq n, \quad 1 \leq i \leq k.$$

Bizonyítsuk be, hogy a $\mathcal{C}_{ij}$ leképezések bázist alkotnak $\operatorname{Hom}(V_1, V_2)$-ben.

5.5.7 Bizonyítsuk be, hogy véges dimenziós vektorterek esetén

$$\dim \operatorname{Hom}(V_1, V_2) = \dim V_1 \cdot \dim V_2 .$$

5.5.8 Legyenek $\mathcal{A}_1, \ldots, \mathcal{A}_r \in \operatorname{Hom}(V_1, V_2)$. Melyek igazak az alábbi állítások közül?

(a) Ha $\mathcal{A}_1, \ldots, \mathcal{A}_r$ lineárisan összefüggő $\operatorname{Hom}(V_1, V_2)$-ben, akkor minden $\mathbf{x} \in V_1$-re $\mathcal{A}_1\mathbf{x}, \ldots, \mathcal{A}_r\mathbf{x}$ lineárisan összefüggő V_2-ben.

(b) Ha van olyan nem nulla $\mathbf{x} \in V_1$ vektor, amelyre $\mathcal{A}_1\mathbf{x}, \ldots, \mathcal{A}_r\mathbf{x}$ lineárisan összefüggő V_2-ben, akkor $\mathcal{A}_1, \ldots, \mathcal{A}_r$ lineárisan összefüggő $\operatorname{Hom}(V_1, V_2)$-ben.

(c) Ha minden $\mathbf{x} \in V_1$-re $\mathcal{A}_1\mathbf{x}, \ldots, \mathcal{A}_r\mathbf{x}$ lineárisan összefüggő V_2-ben, akkor $\mathcal{A}_1, \ldots, \mathcal{A}_r$ lineárisan összefüggő $\operatorname{Hom}(V_1, V_2)$-ben.

M 5.5.9 Legyen $V_1 = \mathbf{C}^4$, $V_2 = \mathbf{C}^2$ és $\mathcal{A}_{ij} \in \mathrm{Hom}\,(V_1\,,\,V_2)$ a következő:

$$\mathcal{A}_{ij}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\end{pmatrix} = \begin{pmatrix}\alpha_i\\ \alpha_j\end{pmatrix} \quad 1 \le i, j \le 4\,.$$

(a) Bizonyítsuk be, hogy bármely három (különböző) $\mathcal{A}_{ij}$ lineárisan független $\mathrm{Hom}\,(V_1\,,\,V_2)$-ben.

(b) Adjunk meg négy olyan (különböző) $\mathcal{A}_{ij}$-t, amely lineárisan összefüggő $\mathrm{Hom}\,(V_1\,,\,V_2)$-ben.

*(c) Maximálisan hány olyan (különböző) $\mathcal{A}_{ij}$ van, amely lineárisan független $\mathrm{Hom}\,(V_1\,,\,V_2)$-ben?

5.6. Lineáris leképezések szorzása

A lineáris leképezések szorzása (egymás után alkalmazása, kompozíciója) különösen a $(V \to V)$ transzformációk esetén játszik fontos szerepet, amelyek erre a szorzásra, valamint az összeadásra és a skalárral való szorzásra nézve egy *algebrá*nak nevezett speciális struktúrát alkotnak. A leképezések szorzása nagyon hasonló tulajdonságokat mutat, mint amilyeneket a mátrixszorzásnál tapasztaltunk. Ennek igazi oka a következő pontban derül majd ki.

5.6.1 Definíció

Legyenek V_1, V_2 és V_3 ugyanazon T test feletti vektorterek, $\mathcal{A} \in \mathrm{Hom}\,(V_2\,,\,V_3)$, $\mathcal{B} \in \mathrm{Hom}\,(V_1\,,\,V_2)$. Ekkor az $\mathcal{A}$ és $\mathcal{B}$ lineáris leképezések *szorzat*án azt az $\mathcal{AB}$-vel jelölt $V_1 \to V_3$ leképezést értjük, amely minden $\mathbf{u} \in V_1$ vektorhoz az $\mathcal{A}(\mathcal{B}\mathbf{u}) \in V_3$ vektort rendeli hozzá. Azaz

$$(\mathcal{AB})\mathbf{u} = \mathcal{A}(\mathcal{B}\mathbf{u})\,. \ \clubsuit$$

Az $\mathcal{AB}$ szorzatot tehát úgy kapjuk, hogy előbb a *második* tényezőként szereplő $\mathcal{B}$ leképezést alkalmazzuk, majd ezután az $\mathcal{A}$-t. Ezt a mesterkéltnek tűnő sorrendiséget azonban az $(\mathcal{AB})\mathbf{u} = \mathcal{A}(\mathcal{B}\mathbf{u})$ képlet azonnal megmagyarázza. A „természetes" sorrend akkor adódna, ha a leképezést (mint operátort) a vektor *mögé* írnánk, ekkor a definíció nyilván $\mathbf{u}(\mathcal{CD}) = (\mathbf{u}\mathcal{C})\mathcal{D}$ alakot öltene. Az analízis hagyományos függvényjelölését követve megmaradunk az $\mathcal{A}\mathbf{u}$ formánál (és ennek megfelelően egy-két esetben látszólag mesterkélt módon járunk el új fogalmak definiálásánál).

Hangsúlyozzuk, hogy két lineáris leképezés szorzatát *csak akkor* értelmeztük, ha eleget tettek az 5.6.1 Definíció feltételeinek, vagyis az a vektortér, amelybe a második tényező képez, ugyanaz, mint amelyiken az első tényező hat.

5.6.2 Tétel
Két lineáris leképezés szorzata is lineáris, azaz ha $\mathcal{A} \in \mathrm{Hom}\,(V_2\,,\,V_3)$ és $\mathcal{B} \in \mathrm{Hom}\,(V_1\,,\,V_2)$, akkor $\mathcal{AB} \in \mathrm{Hom}\,(V_1\,,\,V_3)$. ♣

Bizonyítás: A szorzás definíciója és $\mathcal{B}$, illetve $\mathcal{A}$ linearitása miatt

$$(\mathcal{AB})(\lambda\mathbf{u}) = \mathcal{A}(\mathcal{B}(\lambda\mathbf{u})) = \mathcal{A}(\lambda(\mathcal{B}\mathbf{u})) = \lambda(\mathcal{A}(\mathcal{B}\mathbf{u})) = \lambda((\mathcal{AB})\mathbf{u}).$$

Az összegtartás hasonlóan igazolható. ■

A szorzás tulajdonságainak vizsgálatát kezdjük a *kommutativitás* kérdésével. Ha $\mathcal{A} \in \mathrm{Hom}\,(V_2\,,\,V_3)$, $\mathcal{B} \in \mathrm{Hom}\,(V_1\,,\,V_2)$ és $V_3 \neq V_1$, akkor a $\mathcal{BA}$ szorzat *nincs is értelmezve*. Ha $V_3 = V_1$, de $V_1 \neq V_2$, akkor $\mathcal{AB} \in \mathrm{Hom}\,(V_1\,,\,V_1)$, ugyanakkor $\mathcal{BA} \in \mathrm{Hom}\,(V_2\,,\,V_2)$, tehát semmiképpen sem lehetnek egyenlők. Marad az az eset, amikor $V_1 = V_2 = V_3 = V$, azonban $\mathcal{AB}$ és $\mathcal{BA}$ általában ekkor is különbözők (lásd pl. az 5.6.1–5.6.4 feladatokat). Vagyis a lineáris leképezések szorzása (messzemenően) *nem kommutatív*.

A szorzással (és részben más műveletekkel) kapcsolatos további „szokásos” *azonosságok* viszont igazak:

5.6.3 Tétel
Ha $\lambda \in T$, és $\mathcal{A}$, $\mathcal{B}$, $\mathcal{C}$ tetszőleges olyan lineáris leképezések, amelyekre az alábbi egyenlőségek valamelyik oldala értelmezve van, akkor a másik oldal is értelmes, és az egyenlőség teljesül.

I. $\mathcal{A}(\mathcal{BC}) = (\mathcal{AB})\mathcal{C}$ (asszociativitás);
II. $\mathcal{A}(\mathcal{B}+\mathcal{C}) = \mathcal{AB} + \mathcal{AC}$,
$(\mathcal{A}+\mathcal{B})\mathcal{C} = \mathcal{AC} + \mathcal{BC}$ (disztributivitás*ok*);
III. $\lambda(\mathcal{AB}) = (\lambda\mathcal{A})\mathcal{B} = \mathcal{A}(\lambda\mathcal{B})$. ♣

Mivel a szorzás nem kommutatív, ezért a két disztributivitást külön kell bebizonyítani. Ugyanez az oka annak, hogy III-ban csak a skalárt „emelhetjük át” a leképezéseken, $\mathcal{A}$ és $\mathcal{B}$ sorrendjén nem változtathatunk.

Bizonyítás: I-ben bármelyik oldal pontosan akkor értelmes, ha $\mathcal{A} \in \mathrm{Hom}\,(V_3\,,\,V_4)$, $\mathcal{B} \in \mathrm{Hom}\,(V_2\,,\,V_3)$, $\mathcal{C} \in \mathrm{Hom}\,(V_1\,,\,V_2)$, és ekkor minden

$\mathbf{x} \in V_1$-re

$$(\mathcal{A}(\mathcal{BC}))\mathbf{x} = \mathcal{A}((\mathcal{BC})\mathbf{x}) = \mathcal{A}(\mathcal{B}(\mathcal{C}\mathbf{x}))\,,$$

illetve

$$((\mathcal{AB})\mathcal{C})\mathbf{x} = (\mathcal{AB})(\mathcal{C}\mathbf{x}) = \mathcal{A}(\mathcal{B}(\mathcal{C}\mathbf{x}))\,,$$

tehát I-ben az egyenlőség két oldalán valóban ugyanaz a leképezés áll. [Itt tulajdonképpen arról van szó, hogy függvények kompozíciója (egymás után alkalmazása) mindig asszociatív, hiszen akármelyik zárójelezést felbontva a függvényeket végül is a megfelelő sorrendben egymás után kell alkalmazni.]

II. és III. igazolása hasonló módon történik, csak ott a szorzás definícióján kívül a leképezések linearitását is fel kell használni (lásd az 5.6.6 feladatot). ■

A továbbiakban egy adott V vektortér lineáris transzformációival foglalkozunk. Az összes ilyen transzformációk halmazát (Hom $(V\,,\,V)$ helyett röviden) Hom V-vel jelöljük.

5.6.4 Tétel

Hom V a leképezések közötti összeadásra és skalárral való szorzásra nézve vektortér, az összeadásra és a szorzásra nézve gyűrű, továbbá teljesül a

$$\lambda(\mathcal{AB}) = (\lambda\mathcal{A})\mathcal{B} = \mathcal{A}(\lambda\mathcal{B}), \quad \mathcal{A},\, \mathcal{B} \in \operatorname{Hom} V,\, \lambda \in T$$

azonosság. ♣

Bizonyítás: A vektortérre vonatkozó állítás az 5.5.3 Tétel speciális esete. Az, hogy a szorzás valóban művelet Hom V-ben, az 5.6.2 Tételből következik. A gyűrűben a szorzásra vonatkozó azonosságok, valamint a szorzást és a skalárral való szorzást összekapcsoló azonosság az 5.6.3 Tételből adódik. ■

Az alábbiakban általánosan összefoglaljuk az 5.6.4 Tételben kimondott tulajdonságokat.

5.6.5 Definíció

Egy A nem üres halmaz *algebra* (vagy *hiperkomplex rendszer*) a T kommutatív test felett, ha

(i) értelmezve van A-n egy összeadás, egy szorzás és egy T elemeivel való szorzás;

(ii) A az összeadásra és a szorzásra nézve gyűrű;

(iii) A az összeadásra és a T elemeivel való szorzásra nézve vektortér;

(iv) érvényes a szorzást és a T elemeivel való szorzást összekapcsoló

$$\lambda(ab) = (\lambda a)b = a(\lambda b),\ \lambda \in T,\ a,\ b \in A$$

azonosság. ♣

Példák algebrára

P1. $\operatorname{Hom} V$ a megadott műveletekre (T felett).

P2. Adott méretű négyzetes mátrixok ($T^{n\times n}$) a szokásos műveletekre (T felett).

P3. Polinomok ($T[x]$) a szokásos műveletekre (T felett).

P4. A komplex számok a valós test felett a szokásos műveletekre. Általánosabban: ha T_1 *részteste* T_2-nek (tehát T_1 nemcsak részhalmaza T_2-nek, hanem a T_1-beli műveletek éppen a T_2-beli műveletek megszorításai), akkor T_2 algebra T_1 felett.

P5. A komplex számok általánosítása a *kvaterniók*. Ezek $\alpha_0+\alpha_1 i+\alpha_2 j+\alpha_3 k$ alakú kifejezések, ahol $\alpha_i \in \mathbf{R}$. Az összeadást és a valós számmal való szorzást „komponensenként" értelmezzük. A szorzást úgy *definiáljuk*, hogy „minden tagot minden taggal meg kell szorozni", az együttható valósok „átemelendők" i-n, j-n és k-n, és végül az „alapvektorokat" a következő szabály szerint kell összeszorozni:

$$i^2 = j^2 = k^2 = -1,\ ij = k,\ ji = -k,\ jk = i,\ kj = -i,\ ik = -j,\ ki = j\,.$$

Megmutatható, hogy így a valós test felett egy 4-dimenziós algebrát kapunk, amely *nem kommutatív test*.

A kvaterniók alapján szokták az algebrákra néha a hiperkomplex (komplexen túli) rendszer elnevezést is használni.

A kvaterniók Frobenius alábbi nevezetes tétele szerint a számfogalom lezárásának tekinthetők:

> Legyen A egy olyan véges dimenziós algebra $\mathbf{R}$ felett, amely egyúttal (nem feltétlenül kommutatív) test. Ekkor A mint algebra vagy a valós számokkal, vagy a komplex számokkal, vagy pedig a kvaterniókkal izomorf.

További példák: lásd az 5.6.19 feladatot.

A szorzás tulajdonságai $\operatorname{Hom} V$-ben

Korábban már jeleztük, hogy $\operatorname{Hom} V$-ben a szorzás *nem kommutatív*. Könnyen látható, hogy az $\mathcal{E}$ identikus leképezés kétoldali *egységelem*.

A következőkben az invertálhatóságra és a nullosztókra fogalmazunk meg tételeket.

5.6.6 Tétel

Egy $\mathcal{A} \in \operatorname{Hom} V$ lineáris transzformációnak akkor és csak akkor létezik (kétoldali) inverze, ha $\mathcal{A}$ izomorfizmus. ♣

Bizonyítás: Ha $\mathcal{A}$ izomorfizmus, akkor az 5.2.3 Tétel bizonyításánál láttuk, hogy az $\mathcal{A}$ bijekció inverze, $\mathcal{A}^{-1}$ is lineáris leképezés, tehát eleme $\operatorname{Hom} V$-nek. Megfordítva, legyen $\mathcal{B}$ az $\mathcal{A}$ transzformáció inverze: $\mathcal{AB} = \mathcal{BA} = \mathcal{E}$. Ekkor egyrészt minden $\mathbf{u} \in V$-re $\mathbf{u} = \mathcal{A}(\mathcal{B}\mathbf{u})$, tehát $\mathbf{u} \in \operatorname{Im}\mathcal{A}$, vagyis $\operatorname{Im}\mathcal{A} = V$. Másrészt, ha $\mathcal{A}\mathbf{u} = \mathcal{A}\mathbf{v}$, akkor $\mathbf{u} = \mathcal{B}(\mathcal{A}\mathbf{u}) = \mathcal{B}(\mathcal{A}\mathbf{v}) = \mathbf{v}$, vagyis különböző vektorok $\mathcal{A}$ szerinti képe is különböző. Így $\mathcal{A}$ valóban izomorfizmus. ■

Eredményünket az 5.2.2 Tétellel egybevetve adódik, hogy $\mathcal{A} \in \operatorname{Hom} V$-nek akkor és csak akkor létezik inverze, ha $\operatorname{Ker}\mathcal{A} = \mathbf{0}$ és $\operatorname{Im}\mathcal{A} = V$. Az 5.4.2 Tételből azt is tudjuk, hogy *véges dimenziós* V esetén ezen két feltétel bármelyike maga után vonja a másikat.

Az 5.6.6 Tétel bizonyításából az is leolvasható, hogy ha $\mathcal{A}$-nak létezik jobbinverze, akkor szükségképpen $\operatorname{Im}\mathcal{A} = V$, illetve ha $\mathcal{A}$-nak létezik balinverze, akkor szükségképpen $\operatorname{Ker}\mathcal{A} = \mathbf{0}$. Mindezt a fentiekkel egybevetve kapjuk, hogy *véges dimenzió* esetén az egyik oldali inverz létezése maga után vonja a másik oldali inverz létezését. Végtelen dimenzió esetén ez nem igaz, annyi azonban megmutatható, hogy $\operatorname{Im}\mathcal{A} = V$, illetve $\operatorname{Ker}\mathcal{A} = \mathbf{0}$ a megfelelő oldali inverz létezésének nemcsak szükséges, hanem egyben elégséges feltétele is.

A nullosztókról szóló tételt csak a véges dimenziós esetre mondjuk ki. Az egyik oldali nullosztókra, illetve a végtelen dimenzióra vonatkozóan hasonló jellegű a helyzet, mint amit az invertálhatóságnál tapasztaltunk. (Mindezekkel kapcsolatban lásd az 5.6.10–5.6.16 feladatokat.)

5.6.7 Tétel

Legyen V véges dimenziós vektortér. Ha $\mathcal{A} \in \operatorname{Hom} V$ bal vagy jobb oldali nullosztó, akkor $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$. Megfordítva, ha $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$ és $\mathcal{A} \neq \mathcal{O}$, akkor $\mathcal{A}$ mind bal, mind pedig jobb oldali nullosztó. ♣

Bizonyítás: Többször fel fogjuk használni az alábbi egyszerű észrevételt: $\mathcal{AB} = \mathcal{O}$ akkor és csak akkor igaz, ha $\operatorname{Ker}\mathcal{A} \supseteq \operatorname{Im}\mathcal{B}$. Valóban, $\mathcal{A}(\mathcal{B}\mathbf{u}) = \mathbf{0}$ pontosan akkor teljesül minden $\mathbf{u} \in V$-re, ha $\operatorname{Im}\mathcal{B}$ valamennyi $\mathcal{B}\mathbf{u}$ eleme $\operatorname{Ker}\mathcal{A}$-ba esik.

Legyen először $\mathcal{A}$ bal oldali nullosztó, azaz valamilyen $\mathcal{C} \neq \mathcal{O}$ lineáris transzformációra $\mathcal{AC} = \mathcal{O}$. Ekkor az előzőek szerint $\operatorname{Ker}\mathcal{A} \supseteq \operatorname{Im}\mathcal{C} \neq \mathbf{0}$, vagyis valóban $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$. Ha $\mathcal{A}$ jobb oldali nullosztó, akkor ugyanígy $\operatorname{Im}\mathcal{A} \neq V$ adódik, de ez a dimenzió végessége miatt ekvivalens a $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$ feltétellel.

Megfordítva, tegyük fel, hogy $\mathcal{A} \neq \mathcal{O}$ és $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$. Először megmutatjuk, hogy $\mathcal{A}$ bal oldali nullosztó, azaz valamilyen $\mathcal{C} \neq \mathcal{O}$ lineáris transzformációra $\mathcal{AC} = \mathcal{O}$. A $\mathcal{C}$ transzformációt V egy alkalmas bázisán fogjuk megadni. Legyen $\operatorname{Ker}\mathcal{A}$ egy bázisa $\mathbf{b}_1, \ldots, \mathbf{b}_s$, ezt egészítsük ki a $\mathbf{b}_{s+1}, \ldots, \mathbf{b}_n$ vektorokkal V egy bázisává. Legyen most $\mathcal{C}$ az a lineáris transzformáció, amelyre

$$\mathcal{C}\mathbf{b}_i = \begin{cases} \mathbf{b}_i, & \text{ha } 1 \leq i \leq s; \\ \mathbf{0}, & \text{ha } i > s. \end{cases}$$

Ekkor nyilván $\mathcal{C} \neq \mathcal{O}$ és $\mathcal{AC} = \mathcal{O}$.

Hasonlóan okoskodhatunk, amikor azt akarjuk igazolni, hogy $\mathcal{A}$ jobb oldali nullosztó. Ekkor az $\operatorname{Im}\mathcal{A} \neq V$ feltételből indulunk ki, $\operatorname{Im}\mathcal{A}$ egy bázisát egészítjük ki V bázisává, és így konstruálunk olyan $\mathcal{B} \neq \mathcal{O}$ transzformációt, amelyre $\mathcal{BA} = \mathcal{O}$. A részletek végiggondolását az Olvasóra bízzuk. ■

Feladatok

5.6.1 Legyen $V_1 = V_2$ a síkvektorok szokásos vektortere. Döntsük el, hogy $\mathcal{AB} = \mathcal{BA}$ teljesül-e, ha

(a) $\mathcal{A}$ az x-tengelyre, $\mathcal{B}$ az $y = x$ egyenesre történő tükrözés;

(b) $\mathcal{A}$ az x-tengelyre, $\mathcal{B}$ az $y = x$ egyenesre történő merőleges vetítés;

(c) $\mathcal{A}$ az origó körüli $+60$ fokos, $\mathcal{B}$ az origó körüli -90 fokos elforgatás;

(d) $\mathcal{A}$ az origóból történő ötszörös nagyítás, $\mathcal{B}$ az origó körüli $+90$ fokos elforgatás.

5.6.2 Legyen $V = \mathbf{C}^3$ és definiáljuk az $\mathcal{A}$, $\mathcal{B} \in \operatorname{Hom} V$ transzformációkat a következőképpen:

$$\mathcal{A}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_2 \\ \alpha_1 \\ \alpha_3 \end{pmatrix}, \qquad \mathcal{B}\begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \alpha_3 \end{pmatrix} = \begin{pmatrix} \alpha_1 \\ \alpha_3 \\ \alpha_2 \end{pmatrix}.$$

Adjuk meg az $\mathcal{AB}$, $\mathcal{BA}$, $\mathcal{A}^{101}$, $(\mathcal{AB})^{101}$ transzformációkat.

5.6.3 Legyen V véges dimenziós vektortér. Adjuk meg az összes olyan $\mathcal{A} \in \operatorname{Hom} V$-t, amely V minden lineáris transzformációjával felcserélhető (azaz minden $\mathcal{B} \in \operatorname{Hom} V$-re $\mathcal{AB} = \mathcal{BA}$).

5.6.4 Melyek azok a véges dimenziós V vektorterek, amelyekre a $\operatorname{Hom} V$-beli szorzás kommutatív?

5.6.5 Legyen $\mathcal{A} \in \operatorname{Hom}(V_2\,,\,V_3)$, $\mathcal{B} \in \operatorname{Hom}(V_1\,,\,V_2)$. Milyen kapcsolatban áll egymással $\operatorname{Ker}\mathcal{AB}$ és $\operatorname{Ker}\mathcal{B}$, illetve $\operatorname{Im}\mathcal{AB}$ és $\operatorname{Im}\mathcal{A}$?

5.6.6 Bizonyítsuk be az 5.6.3 Tétel II. és III. állítását.

5.6.7 Legyen $\mathcal{A} \in \operatorname{Hom}(V_2\,,\,V_3)$, $\mathcal{B} \in \operatorname{Hom}(V_1\,,\,V_2)$. Bizonyítsuk be, hogy

$$\dim \operatorname{Im}\mathcal{B} = \dim \operatorname{Im}\mathcal{AB} + \dim(\operatorname{Ker}\mathcal{A} \cap \operatorname{Im}\mathcal{B})\,.$$

5.6.8 Legyen V véges dimenziós vektortér, $\mathcal{A} \in \operatorname{Hom} V$. Bizonyítsuk be, hogy

$$\operatorname{Ker}\mathcal{A}^2 = \operatorname{Ker}\mathcal{A} \iff \operatorname{Im}\mathcal{A}^2 = \operatorname{Im}\mathcal{A} \iff \operatorname{Ker}\mathcal{A} \cap \operatorname{Im}\mathcal{A} = \mathbf{0}\,.$$

*5.6.9 Legyen A egy 5×5-ös valós mátrix, és tegyük fel, hogy $A^{1000} = 0$. Bizonyítsuk be, hogy ekkor $A^5 = 0$.

5.6.10 Legyen V a valós együtthatós polinomok szokásos vektortere, és definiáljuk az $\mathcal{A}$, $\mathcal{B} \in \operatorname{Hom} V$ transzformációkat a következőképpen (egy általános polinomot $f(x)$-szel, az i-edfokú tag együtthatóját α_i-vel jelöljük):

$$\mathcal{A}[f(x)] = xf(x) \qquad \mathcal{B}[f(x)] = [f(x) - \alpha_0]/x\,.$$

Állapítsuk meg $\mathcal{A}$-ról, illetve $\mathcal{B}$-ről, hogy hány bal-, illetve jobbinverze van, valamint hogy bal, illetve jobb oldali nullosztó-e.

5.6.11 Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis a V vektortérben. Az alábbi lineáris transzformációk közül melyeknek van bal-, illetve jobbinverzük, és melyek bal, illetve jobb oldali nullosztók. Invertálhatóság esetén adjuk meg az inverzet, a nullosztókhoz pedig adjunk meg egy-egy hozzájuk tartozó bal, illetve jobb oldali nullosztópárt.

(a) $\mathcal{A} : \mathbf{b}_1 \mapsto \mathbf{b}_1 - \mathbf{b}_2,\ \mathbf{b}_2 \mapsto \mathbf{b}_2 - \mathbf{b}_3,\ \ldots,\ \mathbf{b}_n \mapsto \mathbf{b}_n - \mathbf{b}_1$;

(b) $\mathcal{B} : \mathbf{b}_1 \mapsto \mathbf{b}_1,\ \mathbf{b}_2 \mapsto \mathbf{b}_1 + \mathbf{b}_2,\ \ldots,\ \mathbf{b}_n \mapsto \mathbf{b}_1 + \mathbf{b}_n$;

(c) $\mathcal{C} : \mathbf{b}_1 \mapsto \mathbf{b}_1 + \mathbf{b}_2 + \ldots + \mathbf{b}_n,\ \ldots,\ \mathbf{b}_n \mapsto \mathbf{b}_1 + \mathbf{b}_2 + \ldots + \mathbf{b}_n$.

5.6.12 Melyek azok a V véges dimenziós vektorterek, amelyekre minden nem nulla $\mathcal{A} \in \operatorname{Hom} V$ transzformációnak létezik inverze?

5.6.13 Melyek azok a V véges dimenziós vektorterek, amelyekre $\operatorname{Hom} V$ nullosztómentes?

5.6.14 Melyek azok a V véges dimenziós vektorterek, amelyekre létezik olyan $\mathcal{A}$, $\mathcal{B} \in \operatorname{Hom} V$, hogy

(a) $\mathcal{AB} = \mathcal{O}$, de $\mathcal{BA} \neq \mathcal{O}$; (b) $\mathcal{AB} = \mathcal{O}$, de $\mathcal{BA} = \mathcal{E}$?

5.6.15 Legyen V véges dimenziós vektortér és $\mathcal{A} \in \operatorname{Hom} V$ nullosztó. Mutassuk meg, hogy létezik olyan nem nulla $\mathcal{B} \in \operatorname{Hom} V$, amely egyszerre teljesíti az $\mathcal{AB} = \mathcal{O}$ és $\mathcal{BA} = \mathcal{O}$ feltételeket.

5.6.16 Legyen V véges dimenziós vektortér, $\mathcal{A}$, $\mathcal{B} \in \operatorname{Hom} V$. Melyek igazak az alábbi állítások közül?

(a) Ha $\mathcal{A}$-nak és $\mathcal{B}$-nek létezik inverze, akkor $\mathcal{AB}$-nek is létezik inverze.

(b) Ha $\mathcal{AB}$-nek létezik inverze, akkor $\mathcal{A}$-nak és $\mathcal{B}$-nek is létezik inverze.

(c) Ha $\mathcal{A}$ és $\mathcal{B}$ bal oldali nullosztó és $\mathcal{AB} \neq \mathcal{O}$, akkor $\mathcal{AB}$ is bal oldali nullosztó.

(d) Ha $\mathcal{AB}$ bal oldali nullosztó, akkor $\mathcal{A}$ és $\mathcal{B}$ is bal oldali nullosztó.

(e) Ha $\mathcal{A}+\mathcal{B}$-nek létezik inverze, akkor $\mathcal{A}$ és $\mathcal{B}$ közül legalább az egyiknek létezik inverze.

(f) Ha $\mathcal{A}+\mathcal{B}$ bal oldali nullosztó, akkor $\mathcal{A}$ és $\mathcal{B}$ közül legalább az egyik bal oldali nullosztó.

5.6.17 Legyen V véges dimenziós vektortér, $\mathcal{A} \in \operatorname{Hom} V$. Tekintsük $\operatorname{Hom} V$ alábbi két részhalmazát:

$$B = \{\mathcal{C} \in \operatorname{Hom} V \mid \mathcal{CA} = \mathcal{O}\}; \qquad J = \{\mathcal{D} \in \operatorname{Hom} V \mid \mathcal{AD} = \mathcal{O}\}$$

(azaz „az $\mathcal{A}$-hoz tartozó bal, illetve jobb oldali nullosztók halmazát"). Bizonyítsuk be, hogy B és J alterek $\operatorname{Hom} V$-ben, és számítsuk ki a dimenziójukat.

5.6.18 Legyen V véges dimenziós vektortér. Egy $\mathcal{P} \in \operatorname{Hom} V$ lineáris transzformációt *projekció*nak nevezünk, ha $\mathcal{P}^2 = \mathcal{P}$.

(a) Létezik-e $\mathcal{O}$-n és $\mathcal{E}$-n kívül más projekció is?

(b) Vajon miért nevezik az ilyen transzformációkat projekciónak?

(c) Mely projekcióknak létezik (bal és/vagy jobb oldali) inverze?

(d) Bizonyítsuk be, hogy $\mathcal{P}$ akkor és csak akkor projekció, ha $\mathcal{E} - \mathcal{P}$ projekció.

(e) Legyen $T = \mathbf{R}$. Bizonyítsuk be, hogy $\mathcal{P}$ akkor és csak akkor projekció, ha $2\mathcal{P} - \mathcal{E}$ önmagának az inverze. Mutassuk meg, hogy van olyan test, amely felett ez az állítás nem igaz.

(f) Bizonyítsuk be, hogy ha $\mathcal{P}$ projekció és $\lambda \neq 0, -1$, akkor $\mathcal{P} + \lambda\mathcal{E}$-nek létezik inverze.

*(g) Bizonyítsuk be, hogy $\mathcal{P}$ akkor és csak akkor projekció, ha V felbontható $V = U_1 \oplus U_2$ alakban, ahol $\mathcal{P}$ az U_1 altér elemeit helyben hagyja, U_2 elemeit pedig $\mathbf{0}$-ba viszi.

*5.6.19 Legyen V véges dimenziós vektortér. Bizonyítsuk be, hogy minden $\mathcal{A} \in \operatorname{Hom} V$-hez található olyan $\mathcal{B} \in \operatorname{Hom} V$, amellyel $\mathcal{ABA} = \mathcal{A}$.

5.6.20 Az alábbi struktúrák közül melyek alkotnak algebrát?

(a) Tetszőleges vektortér, ha a szorzást úgy értelmezzük, hogy bármely két vektor szorzata a nullvektor.
(b) A (közönséges 3-dimenziós) tér vektorai a szokásos összeadásra, skalárral való szorzásra, valamint a vektoriális szorzatra nézve.
(c) A valós számsorozatok a szokásos (komponensenkénti) műveletekre.
(d) T^n, ha a szorzást is komponensenként értelmezzük.
(e) Az összes valós számon értelmezett valós értékű függvények a szokásos műveletekre.
(f) Az előző példa, ha a szorzást a függvényösszetétellel (kompozícióval, egymás után alkalmazással) értelmezzük.
(g) Az $\alpha+\beta\sqrt{2}$, α, $\beta \in \mathbf{Q}$ alakú számok a racionális test felett a szokásos műveletekre.
(h) Bármely gyűrű a modulo 2 test felett, ha a skalárral való szorzást $0\mathbf{a} = \mathbf{0}$, $1\mathbf{a} = \mathbf{a}$ módon definiáljuk.
(i) A $\begin{pmatrix} z & w \\ -\overline{w} & \overline{z} \end{pmatrix}$ alakú 2×2-es *komplex* elemű mátrixok a *valós* test felett a szokásos műveletekre.
(j) Az előző mátrixok, de a komplex test felett.

5.6.21 Végezzük el az alábbi kvaternió-műveleteket:

a) $(1+i)(1+j) - (1+j)(1+k)$;
b) $(i+j+k)^{100}$;
c) $(1+i-j-k)(1-i+j-k)(1-i-j+k)$.

5.6.22 A $v = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$ kvaternió *konjugált*ján a $\overline{v} = \alpha_0 - \alpha_1 i - \alpha_2 j - \alpha_3 k$ kvaterniót értjük. Számítsuk ki a $v\overline{v}$ szorzatot. Hogyan lehet ennek segítségével egy kvaternió (multiplikatív) inverzét meghatározni?

5.6.23 Hány megoldása van a kvaterniók körében az $x^2+1 = 0$ egyenletnek? Hogyan fér ez össze azzal a tétellel, hogy „egy polinomnak legfeljebb annyi gyöke lehet, mint amennyi a foka”?

M*5.6.24 Legyen $n > 1$ és v tetszőleges olyan kvaternió, amely nem egy valós szám. Hány n-edik gyöke van v-nek a kvaterniók körében?

5.6.25 Bizonyítsuk be, hogy egy legalább kételemű, véges dimenziós algebra akkor és csak akkor (nem feltétlenül kommutatív) test, ha nullosztómentes.

5.7. Lineáris leképezés mátrixa

A lineáris leképezéseket mátrixokkal fogjuk jellemezni. Ezt az teszi lehetővé, hogy a leképezés megadható V_1 báziselemeinek a képével, a képek pedig felírhatók V_2 báziselemeinek a segítségével. Kiderül, hogy a mátrixreprezentáció a műveleteket is tartja, ami megmagyarázza, hogy miért hasonlítanak annyira a leképezések és a mátrixok tulajdonságai. Ez a kapcsolat mindkét irányban hasznosnak bizonyul, mert így leképezésekre vonatkozó állításokat mátrixok segítségével igazolhatunk, és viszont. Gyakorlati alkalmazásoknál a leképezések helyett szinte mindig a mátrixukkal dolgozunk.

5.7.1 Definíció

Legyen a V_1 vektortér egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, a V_2 vektortér egy bázisa pedig $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Egy $\mathcal{A} \in \mathrm{Hom}\,(V_1\,,\,V_2)$ leképezésnek az $\mathbf{a}_1, \ldots, \mathbf{a}_n$ és $\mathbf{b}_1, \ldots, \mathbf{b}_k$ bázispár szerinti *mátrix*án azt a $k \times n$-es mátrixot értjük, amelynek j-edik oszlopában az $\mathcal{A}\mathbf{a}_j$ vektornak a $\mathbf{b}_1, \ldots, \mathbf{b}_k$ bázis szerinti koordinátái állnak. Ezt a mátrixot $[\mathcal{A}]_{a,b}$-vel jelöljük.

Részletesebben kiírva, legyen

$$\begin{aligned}
\mathcal{A}\mathbf{a}_1 &= \alpha_{11}\mathbf{b}_1 + \alpha_{21}\mathbf{b}_2 + \ldots + \alpha_{k1}\mathbf{b}_k \\
\mathcal{A}\mathbf{a}_2 &= \alpha_{12}\mathbf{b}_1 + \alpha_{22}\mathbf{b}_2 + \ldots + \alpha_{k2}\mathbf{b}_k \\
&\vdots \\
\mathcal{A}\mathbf{a}_n &= \alpha_{1n}\mathbf{b}_1 + \alpha_{2n}\mathbf{b}_2 + \ldots + \alpha_{kn}\mathbf{b}_k\,.
\end{aligned}$$

Ekkor

$$[\mathcal{A}]_{a,b} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{k1} & \alpha_{k2} & \ldots & \alpha_{kn} \end{pmatrix}. \quad \clubsuit$$

Az $[\mathcal{A}]_{a,b}$ mátrix oszlopai tehát tulajdonképpen rendre az $\mathbf{a}_j$ báziselemek képei, mégpedig a $\mathbf{b}_i$ báziselemek segítségével felírva.

A mátrix természetesen erősen függ attól, hogy milyen bázisokat választottunk a két vektortérben, más bázispár esetén általában a mátrix is egészen más lesz.

Szükségünk lesz egy vektor mátrixára is (ez a fogalom már az 5.1 pont P5 példájában is szerepelt):

5.7.2 Definíció

Legyen $\mathbf{c}_1, \ldots, \mathbf{c}_r$ bázis a V vektortérben. Tudjuk, hogy ekkor minden $\mathbf{v} \in V$ egyértelműen felírható $\mathbf{v} = \gamma_1\mathbf{c}_1 + \ldots + \gamma_r\mathbf{c}_r$ alakban. A $\mathbf{v}$ vektornak a $\mathbf{c}_1, \ldots, \mathbf{c}_r$ bázis szerinti (koordináta)*mátrix*án (vagy *koordinátavektor*án) a

$$[\mathbf{v}]_c = \begin{pmatrix} \gamma_1 \\ \gamma_2 \\ \vdots \\ \gamma_r \end{pmatrix}$$

(oszlop)mátrixot értjük. ♣

A vektor mátrixa is bázisfüggő.

Ha a korábbiakból egyértelmű, hogy mely bázis(pár)ról van szó, akkor a vektor, illetve leképezés mátrixának jelölésénél a bázis(pár)ra vonatkozó indexet elhagyhatjuk.

Először megmutatjuk, hogy rögzített bázispár esetén a képvektor mátrixa a leképezés mátrixának és az eredeti vektor mátrixának a szorzata.

5.7.3 Tétel

Legyen a V_1 vektortér egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, a V_2 vektortér egy bázisa pedig $\mathbf{b}_1, \ldots, \mathbf{b}_k$, továbbá $\mathcal{A} \in \mathrm{Hom}\,(V_1\,,\, V_2)$ és $\mathbf{v} \in V_1$. Ekkor

$$[\mathcal{A}\mathbf{v}]_b = [\mathcal{A}]_{a,b} \cdot [\mathbf{v}]_a$$

ahol a jobb oldalon a két mátrix szorzata áll. ♣

Bizonyítás: Legyen

$$[\mathbf{v}]_a = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{pmatrix} \quad \text{és} \quad [\mathcal{A}]_{a,b} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & & \vdots \\ \alpha_{k1} & \alpha_{k2} & \ldots & \alpha_{kn} \end{pmatrix}.$$

Ekkor

$$\begin{aligned}\mathcal{A}\mathbf{v} &= \mathcal{A}(\lambda_1\mathbf{a}_1 + \ldots + \lambda_n\mathbf{a}_n) = \lambda_1(\mathcal{A}\mathbf{a}_1) + \ldots + \lambda_n(\mathcal{A}\mathbf{a}_n) = \\ &= \lambda_1(\alpha_{11}\mathbf{b}_1 + \ldots + \alpha_{k1}\mathbf{b}_k) + \ldots + \lambda_n(\alpha_{1n}\mathbf{b}_1 + \ldots + \alpha_{kn}\mathbf{b}_k) = \\ &= (\alpha_{11}\lambda_1 + \ldots + \alpha_{1n}\lambda_n)\mathbf{b}_1 + \ldots + (\alpha_{k1}\lambda_1 + \ldots + \alpha_{kn}\lambda_n)\mathbf{b}_k\,,\end{aligned}$$

vagyis $\mathbf{b}_i$ együtthatója valóban $[\mathcal{A}]$ i-edik sorának és $[\mathbf{v}]$ (egyetlen) oszlopának a szorzata, amint állítottuk. ■

Most azt igazoljuk, hogy ha rögzített bázispár esetén minden leképezésnek megfeleltetjük a mátrixát, ez egy izomorfizmust létesít a lineáris leképezések és a (megfelelő méretű) mátrixok vektortere között.

5.7.4 Tétel
Ha $\dim V_1 = n$, $\dim V_2 = k$, akkor $\mathrm{Hom}\,(V_1\,,\,V_2) \cong T^{k\times n}$. ♣

Bizonyítás: Legyen a V_1 vektortér egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, a V_2 vektortér egy bázisa pedig $\mathbf{b}_1, \ldots, \mathbf{b}_k$, és feleltessük meg minden $\mathcal{A} \in \mathrm{Hom}\,(V_1\,,\,V_2)$ leképezésnek a(z adott bázispár szerinti) mátrixát:

$$\mathcal{A} \mapsto [\mathcal{A}]_{a,b}\,.$$

Megmutatjuk, hogy így egy $\mathrm{Hom}\,(V_1\,,\,V_2) \to T^{k\times n}$ vektortérizomorfizmust definiáltunk.

1. Ily módon minden $\mathcal{A} \in \mathrm{Hom}\,(V_1\,,\,V_2)$-hez egyértelműen hozzárendeltünk egy $k \times n$-es mátrixot, hiszen bármely $\mathcal{A}$ lineáris leképezés esetén adott (bázis)elemek képei egyértelműen meghatározottak, és ezek a képek egyértelműen felírhatók egy adott V_2-beli bázis segítségével.

2. Bármely mátrixnak pontosan egy ősképe van. Ugyanis a mátrix éppen az $\mathbf{a}_j$ báziselemek képét adja meg egyértelműen, és az 5.3.1 Tétel szerint pontosan egy olyan $\mathcal{A}$ lineáris leképezés létezik, amely az adott báziselemekhez éppen az előírt vektorokat rendeli.

3. Az összegtartás igazolása: $(\mathcal{A}+\mathcal{B})\mathbf{a}_j = \mathcal{A}\mathbf{a}_j + \mathcal{B}\mathbf{a}_j$ és a rögzített $\mathbf{b}_i$ bázis miatt az $[\mathcal{A}+\mathcal{B}]$ mátrix j-edik oszlopa éppen az $[\mathcal{A}]$ és $[\mathcal{B}]$ mátrixok j-edik oszlopainak az összege lesz, tehát valóban $[\mathcal{A}+\mathcal{B}] = [\mathcal{A}] + [\mathcal{B}]$. A skalárszorostartás hasonlóan bizonyítható. ■

Hangsúlyozzuk, hogy a fenti izomorfizmus csak *rögzített* bázispár esetén érvényes, tehát amikor valamennyi leképezés mátrixát ugyanabban a bázispárban írjuk fel.

Az előző tétel egyszerű következménye:

5.7.5 Tétel
Véges dimenziós vektorterek esetén

$$\dim \mathrm{Hom}\,(V_1\,,\,V_2) = \dim V_1 \cdot \dim V_2\,. \ \clubsuit$$

Bizonyítás: Legyen $\dim V_1 = n$, $\dim V_2 = k$. Ekkor $\mathrm{Hom}\,(V_1\,,\,V_2) \cong T^{k\times n}$, és a $T^{k\times n}$ vektortér dimenziója kn (ezt már a 4.5–4.6 pontokban beláttuk). ■

Megjegyezzük, hogy a tétel állítását és egy másik bizonyítását az 5.5.6–5.5.7 feladatok is tartalmazzák. Az ott megadott leképezésekből álló bázis az 5.7.4 tétel izomorfizmusánál éppen a mátrixok szokásos bázisába megy át.

Most rátérünk a szorzással kapcsolatos művelettartásra.

5.7.6 Tétel
Legyen V_1 egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, V_2 egy bázisa $\mathbf{b}_1, \ldots, \mathbf{b}_k$, V_3 egy bázisa pedig $\mathbf{c}_1, \ldots, \mathbf{c}_r$. Legyen továbbá $\mathcal{A} \in \mathrm{Hom}\,(V_2\,,\,V_3)$, $\mathcal{B} \in \mathrm{Hom}\,(V_1\,,\,V_2)$. Ekkor

$$[\mathcal{A}\mathcal{B}]_{a,c} = [\mathcal{A}]_{b,c} \cdot [\mathcal{B}]_{a,b}\,. \ \clubsuit$$

Bizonyítás: Legyen

$$[\mathcal{A}]_{b,c} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1k} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2k} \\ \vdots & \vdots & & \vdots \\ \alpha_{r1} & \alpha_{r2} & \ldots & \alpha_{rk} \end{pmatrix} \quad \text{és} \quad [\mathcal{B}]_{a,b} = \begin{pmatrix} \beta_{11} & \ldots & \beta_{1n} \\ \beta_{21} & \ldots & \beta_{2n} \\ \beta_{31} & \ldots & \beta_{3n} \\ \vdots & \vdots & \vdots \\ \beta_{k1} & \ldots & \beta_{kn} \end{pmatrix}.$$

Azt kell igazolnunk, hogy $(\mathcal{A}\mathcal{B})\mathbf{a}_j$ i-edik koordinátája megegyezik az $[\mathcal{A}]$ mátrix i-edik sorának és a $[\mathcal{B}]$ mátrix j-edik oszlopának a szorzatával.

$$\begin{aligned}(\mathcal{A}\mathcal{B})\mathbf{a}_j = \mathcal{A}(\mathcal{B}\mathbf{a}_j) = \mathcal{A}(\beta_{1j}\mathbf{b}_1 + \ldots + \beta_{kj}\mathbf{b}_k) = \beta_{1j}(\mathcal{A}\mathbf{b}_1) + \ldots + \beta_{kj}(\mathcal{A}\mathbf{b}_k) = \\ = \beta_{1j}(\alpha_{11}\mathbf{c}_1 + \ldots + \alpha_{r1}\mathbf{c}_r) + \ldots + \beta_{kj}(\alpha_{1k}\mathbf{c}_1 + \ldots + \alpha_{rk}\mathbf{c}_r) = \\ = (\beta_{1j}\alpha_{11} + \ldots + \beta_{kj}\alpha_{1k})\mathbf{c}_1 + \ldots + (\beta_{1j}\alpha_{r1} + \ldots + \beta_{kj}\alpha_{rk})\mathbf{c}_r\,.\end{aligned}$$

Itt $\mathbf{c}_i$ együtthatója $\beta_{1j}\alpha_{i1} + \ldots + \beta_{kj}\alpha_{ik}$, ami valóban az $[\mathcal{A}]$ mátrix i-edik sorának és a $[\mathcal{B}]$ mátrix j-edik oszlopának a szorzata. ■

A következőkben $\mathcal{A} \in \operatorname{Hom} V$ lineáris transzformációk mátrixát vizsgáljuk. Ebben az esetben kikötjük, hogy a bázispár mindkét bázisa *azonos* legyen. Erre egyrészt a szorzás művelettartása miatt van szükség (lásd a következő tételt), másrészt pedig ekkor mutatja a mátrix „természetes" módon, „hogyan transzformálta, miképp változtatta a vektorteret" az $\mathcal{A}$ lineáris transzformáció (azaz a bázisvektorok *önmagukhoz mérve* hogyan változtak).

5.7.7 Tétel

Legyen $\mathbf{a}_1, \ldots, \mathbf{a}_n$ rögzített bázis a V vektortérben. Ekkor az $\mathcal{A} \mapsto [\mathcal{A}]_a$ megfeleltetés izomorfizmus a $\operatorname{Hom} V$ és $T^{n\times n}$ *algebrák* között. ♣

Bizonyítás: Az 5.7.4 Tételben láttuk, hogy a fenti megfeleltetés bijektív, összeg- és skalárszorostartó, az 5.7.6 Tétel pedig biztosítja a szorzásra vonatkozó művelettartást is. ■

Az 5.7.7 Tétel alapján új bizonyítást adhatunk pl. az 5.6.7 Tételre (lásd az 5.7.10 feladatot), és véges dimenziós esetben a transzformációk szorzásának tetszőleges tulajdonságát visszavezethetjük a négyzetes mátrixok szorzásának megfelelő tulajdonságára. Okoskodhatunk természetesen fordítva is, pl. ily módon kaphatunk egy „természetes" magyarázatot a mátrixszorzás asszociativitására, vagy akár magának a mátrixszorzásnak a definíciójára is, amely annak idején ugyancsak mesterkéltnek tűn(hetet)t.

Feladatok

5.7.1 Legyen V a legfeljebb 6-odfokú valós együtthatós polinomok szokásos vektortere és $\mathcal{A} \in \operatorname{Hom} V$ az a lineáris transzformáció, amely minden polinomnak megfelelteti a deriváltját.

(a) Írjuk fel $\mathcal{A}$ mátrixát a szokásos bázisban.

(b) Van-e olyan bázis V-ben, amelyben $[\mathcal{A}]$ minden eleme 0 vagy 1?

*(c) Van-e olyan bázis V-ben, amelyben $[\mathcal{A}]$ minden eleme nullától különböző?

(d) Van-e olyan bázis V-ben, amelyben $[\mathcal{A}]$ utolsó két oszlopa csupa 0?

(e) Van-e olyan bázis V-ben, amelyben $[\mathcal{A}]$ utolsó két sora csupa 0?

5.7.2 Írjuk fel a sík nevezetes lineáris transzformációinak mátrixát többféle bázisban.

5.7.3 Legyen V_1 a legfeljebb 5-ödfokú, V_2 pedig a legfeljebb 2-odfokú komplex együtthatós polinomok szokásos vektortere. Egy általános polinomot f-fel jelölünk, polinom és polinomfüggvény között nem teszünk

különbséget. Írjuk fel az alábbi lineáris leképezések mátrixát alkalmas bázispárban.

(a) $f \mapsto f(0) + f(1)x + f(2)x^2$;

(b) f-nek feleltessük meg az $x^3 + 1$ polinommal vett osztási maradékát;

(c) f-nek feleltessük meg azt a legfeljebb 2-odfokú polinomot, amely a 0, 1 és 2 helyen ugyanazt az értéket veszi fel, mint f.

5.7.4 Legyen a V_1 vektortér egy bázisa $\mathbf{a}_1, \ldots, \mathbf{a}_n$, a V_2 vektortér egy bázisa pedig $\mathbf{b}_1, \ldots, \mathbf{b}_k$. Hogyan változik egy $\mathcal{A} \in \operatorname{Hom}(V_1, V_2)$ leképezés mátrixa, ha a megfelelő bázisban

(a) $\mathbf{a}_1$-et és $\mathbf{a}_2$-t felcseréljük; (b) $\mathbf{b}_1$-et és $\mathbf{b}_2$-t felcseréljük;

(c) $\mathbf{a}_3$ helyett $\lambda\mathbf{a}_3$-at veszünk; (d) $\mathbf{b}_3$ helyett $\lambda\mathbf{b}_3$-at veszünk;

(e) $\mathbf{a}_3$ helyett $\mathbf{a}_3 + \mu\mathbf{a}_2$-t veszünk; (f) $\mathbf{b}_3$ helyett $\mathbf{b}_3 + \mu\mathbf{b}_2$-t veszünk?

5.7.5 Legyen V kétdimenziós vektortér $\mathbf{R}$ felett. Döntsük el, van-e olyan $\mathcal{A} \in \operatorname{Hom} V$, amelynek két különböző bázisban felírt mátrixa

(a) $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$ és $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$;

(b) $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ és $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$;

(c) $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$ és $\begin{pmatrix} 2 & 0 \\ 0 & 0 \end{pmatrix}$;

(d) $\begin{pmatrix} \frac{1}{2} & \frac{\sqrt{3}}{2} \\ -\frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix}$ és $\begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix}$;

(e) $\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$ és $\begin{pmatrix} 2 & 6 \\ 1 & 3 \end{pmatrix}$;

(f) $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$ és $\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$.

5.7.6 Legyen $V_1 \neq V_2$ és $\mathcal{A} \in \operatorname{Hom}(V_1, V_2)$ tetszőleges leképezés. Bizonyítsuk be, hogy van olyan bázispár, hogy $[\mathcal{A}]$ „fődiagonálisában” minden elem 1 vagy 0, a mátrix többi eleme pedig 0.

5.7.7 Legyen $V_1 \neq V_2$. Bizonyítsuk be, hogy $\mathcal{A} \in \operatorname{Hom}(V_1, V_2)$ akkor és csak akkor izomorfizmus, ha alkalmas bázispárban $\mathcal{A}$ mátrixa az egységmátrix.

5.7.8 Legyen $\dim V = 2$ és $\mathcal{A} \in \operatorname{Hom} V$. Bizonyítsuk be, hogy ha $\mathcal{A} \neq \mathcal{O}$, de $\mathcal{A}^2 = \mathcal{O}$, akkor V alkalmas bázisában $[\mathcal{A}] = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$.

5.7.9 Melyek azok az $\mathcal{A} \in \operatorname{Hom} V$ lineáris transzformációk, amelyeknek bármely bázisban ugyanaz a mátrixa?

5.7.10 Az 5.7.7 Tétel felhasználásával adjunk új bizonyítást az 5.6.7 Tételre.

5.7.11 Bizonyítsuk be, hogy egy $\mathcal{A}$ lineáris leképezés mátrixát bármely bázispárban felírva, a kapott mátrix rangja megegyezik $\operatorname{Im}\mathcal{A}$ dimenziójával. (Ezt az egyértelműen meghatározott számot az $\mathcal{A}$ leképezés *rang*jának nevezzük.)

5.7.12 Legyen $A \in T^{k\times n}$, $B \in T^{n\times s}$. Igazoljuk a mátrixrangokra az alábbi becsléseket:
(a) $r(AB) \le \min(r(A), r(B)$; (b) $AB = 0 \Rightarrow r(A) + r(B) \le n$.

5.7.13 Igaz-e, hogy ha egy 2×2-es A valós mátrixra $A^{100} = A^{-1}$, akkor A az egységmátrix?

5.7.14 Nevezzük egy adott transzformáció valamely mátrixát bázismeghatározónak, ha egyértelműen megállapítható, hogy a mátrixot mely bázis szerint írtuk fel.
(a) Bizonyítsuk be, hogy ha T nem a modulo 2 test, akkor egyáltalán nem létezik bázismeghatározó mátrix.
(b) A modulo 2 test felett van olyan transzformáció, amelynek minden mátrixa bázismeghatározó.

5.8. Áttérés új bázisra

Tegyük fel, hogy ismerjük egy lineáris leképezésnek egy adott bázispár szerinti mátrixát. Az alábbi tétel megmutatja, hogyan kaphatjuk meg ekkor a leképezésnek valamely másik bázispár szerinti mátrixát.

5.8.1 Tétel

Legyen a V_1 vektortér egy-egy bázisa (a „régi") $\mathbf{a}_1, \dots, \mathbf{a}_n$, illetve (az „új") $\mathbf{a}'_1, \dots, \mathbf{a}'_n$, és hasonlóképpen a V_2 vektortér egy-egy bázisa $\mathbf{b}_1, \dots, \mathbf{b}_k$, illetve $\mathbf{b}'_1, \dots, \mathbf{b}'_k$. Legyen $\mathcal{S} \in \operatorname{Hom} V_1$ az a(z egyértelműen meghatározott) lineáris transzformáció, amelyre $\mathcal{S}(\mathbf{a}_j) = \mathbf{a}'_j$, $j = 1, \dots, n$, és hasonlóan $\mathcal{T} \in \operatorname{Hom} V_2$, amelyre $\mathcal{T}(\mathbf{b}_i) = \mathbf{b}'_i$, $i = 1, \dots, k$. Legyen továbbá $\mathcal{A} \in \operatorname{Hom}(V_1, V_2)$. Ekkor

$$[\mathcal{A}]_{a',b'} = [\mathcal{T}]_b^{-1} \cdot [\mathcal{A}]_{a,b} \cdot [\mathcal{S}]_a \,. \ \clubsuit$$

A $\mathcal{T}$, illetve $\mathcal{S}$ transzformációkat az új bázisra történő áttérés *kísérő* transzformációinak nevezzük. Az $\mathcal{A}$ leképezés új mátrixát a fenti tétel szerint úgy kapjuk meg, hogy $\mathcal{A}$ régi mátrixát megszorozzuk jobbról a V_1-beli $\mathcal{S}$

kísérő transzformáció mátrixával, balról pedig a V_2-beli $\mathcal{T}$ kísérő transzformáció mátrixának az *inverz*ével.

Megjegyezzük, hogy a kísérő transzformációk mátrixa azonos, akár a régi, akár az új bázis szerint írjuk fel (lásd az 5.8.3 feladatot).

Ha $V_1 = V_2$, azaz $\mathcal{A}$ lineáris transzformáció, akkor csak egy új és egy régi bázis van, és az áttérést értelemszerűen az 5.8.1 Tétel alábbi speciális esete írja le:

5.8.1A Tétel

Legyen a V vektortér egy-egy bázisa (a „régi") $\mathbf{a}_1, \ldots, \mathbf{a}_n$, illetve (az „új") $\mathbf{a}'_1, \ldots, \mathbf{a}'_n$ és $\mathcal{S} \in \operatorname{Hom} V$ az a(z egyértelműen meghatározott) lineáris transzformáció, amelyre $\mathcal{S}(\mathbf{a}_j) = \mathbf{a}'_j$, $j = 1, \ldots, n$. Legyen továbbá $\mathcal{A} \in \operatorname{Hom} V$. Ekkor

$$[\mathcal{A}]_{a'} = [\mathcal{S}]_a^{-1} \cdot [\mathcal{A}]_a \cdot [\mathcal{S}]_a \,. \ \clubsuit$$

Most rátérünk az 5.8.1 Tétel bizonyítására.

Bizonyítás: Az (új) $A' = [\mathcal{A}]_{a',b'}$ mátrix elemeit jelöljük α'_{ij}-vel. Ekkor az A' mátrix j-edik oszlopa definíció szerint az alábbi egyenlőségből adódik:

$$\mathcal{A}(\mathbf{a}'_j) = \alpha'_{1j}\mathbf{b}'_1 + \ldots + \alpha'_{kj}\mathbf{b}'_k \,.$$

Az $(\mathcal{AS})(\mathbf{a}_j) = \mathcal{A}(\mathcal{S}\mathbf{a}_j)$, $\mathcal{S}\mathbf{a}_j = \mathbf{a}'_j$ és $\mathbf{b}'_i = \mathcal{T}\mathbf{b}_i$ összefüggések, valamint $\mathcal{T}$ linearitása alapján ez a következőképpen írható át:

$$\begin{aligned}(\mathcal{AS})(\mathbf{a}_j) = \mathcal{A}(\mathcal{S}\mathbf{a}_j) = \mathcal{A}(\mathbf{a}'_j) = \alpha'_{1j}\mathbf{b}'_1 + \ldots + \alpha'_{kj}\mathbf{b}'_k = \\ = \alpha'_{1j}(\mathcal{T}\mathbf{b}_1) + \ldots + \alpha'_{kj}(\mathcal{T}\mathbf{b}_k) = \mathcal{T}(\alpha'_{1j}\mathbf{b}_1 + \ldots + \alpha'_{kj}\mathbf{b}_k) \,.\end{aligned}$$

Azaz $(\mathcal{AS})(\mathbf{a}_j) = \mathcal{T}(\alpha'_{1j}\mathbf{b}_1 + \ldots + \alpha'_{kj}\mathbf{b}_k)$. Ezt balról $\mathcal{T}^{-1}$-gyel megszorozva

$$(\mathcal{T}^{-1}\mathcal{AS})(\mathbf{a}_j) = \alpha'_{1j}\mathbf{b}_1 + \ldots + \alpha'_{kj}\mathbf{b}_k$$

adódik. Ez definíció szerint azt jelenti, hogy a $\mathcal{T}^{-1}\mathcal{AS}$ leképezésnek a régi (azaz a „vesszőtlen") bázispárban felírt mátrixa megegyezik $A' = [\mathcal{A}]_{a',b'}$-vel. Vagyis $[\mathcal{A}]_{a',b'} = [\mathcal{T}^{-1}\mathcal{AS}]_{a,b}$, ami az 5.7.6 Tétel alapján átírható a kívánt $[\mathcal{T}]_b^{-1} \cdot [\mathcal{A}]_{a,b} \cdot [\mathcal{S}]_a$ alakba. ■

Egy másik bizonyítási lehetőségre nézve lásd az 5.8.6 feladatot.

Feladatok

5.8.1 Legyen V a legfeljebb 2-odfokú valós együtthatós polinomok szokásos vektortere és $\mathcal{A} \in \operatorname{Hom} V$ az a lineáris transzformáció, amely minden polinomnak megfelelteti a deriváltját. Írjuk fel $\mathcal{A}$ mátrixát az alábbi bázisokban:

(a) $1 + x, x + x^2, x^2 + 1$;

(b) $x^2 + 1, -2x^2 + 2x, x^2 - 1$;

(c) $x^2 + x + 1, 2x + 1, -x^2 - x + 1$.

5.8.2 Adjunk az 5.8.1 Tétel segítségével új megoldást az 5.7.4, 5.7.5 és 5.7.9 feladatokra.

5.8.3 Mutassuk meg, hogy az új bázisra történő áttérésnél a kísérő transzformációk mátrixa ugyanaz, akár a régi, akár az új bázis szerint írjuk fel ezeket.

5.8.4 Lássuk be, hogy egy lineáris transzformáció bármely bázis szerinti mátrixának ugyanaz a determinánsa.

5.8.5 Legyen V vektortér $\mathbf{R}$ felett, $2 \leq \dim V < \infty$. Igaz-e, hogy minden $\mathcal{A} \in \operatorname{Hom} V$ lineáris transzformációnak van olyan mátrixa, amely

(a) szimmetrikus;
(b) diagonális;
(c) nem csupa különböző elemből áll;
(d) felsőháromszög (azaz a főátló alatt minden elem nulla)?

5.8.6 Adjunk egy másik bizonyítást az 5.8.1 Tételre az alábbi gondolatmenet alapján:

(A) Igazoljuk először azokat a speciális eseteket, amikor a kísérő transzformáció a következő típusú „elemi átalakítások” valamelyike: (i) egy báziselemet egy (nem nulla) skalárszorosára változtatunk; (ii) egy báziselemhez hozzáadjuk egy másik báziselem skalárszorosát; (iii) két báziselemet felcserélünk (lásd az 5.7.4 feladatot).

(B) Mutassuk meg, hogy ha a tétel igaz az $\mathcal{S}_1$ és $\mathcal{S}_2$ kísérő transzformációkra és bármely $\mathcal{A}$-ra, akkor abban az esetben is igaz marad, ha a kísérő transzformáció az $\mathcal{S}_1$ és $\mathcal{S}_2$ transzformációk $\mathcal{S}_1\mathcal{S}_2$ szorzata. Bizonyítsuk be az analóg állítást a $\mathcal{T}$-kre is.

(C) A Gauss-kiküszöbölés mintájára lássuk be, hogy bármely kísérő transzformáció előállítható az (A)-ban jelzett elemi átalakítások egymásutánjával.

5.8.7 Legyenek $V_1 \neq V_2$, valamint V véges dimenziós vektorterek a T *végtelen test* felett.

(a) Mely $\mathcal{A} \in \operatorname{Hom}(V_1, V_2)$ leképezéseknek létezik olyan mátrixa, amelynek egyik eleme sem nulla?

*(b) Mely $\mathcal{A} \in \operatorname{Hom} V$ transzformációknak létezik olyan mátrixa, amelynek egyik eleme sem nulla?

Megjegyzés: Az (a) részben a $V_1 \neq V_2$ kikötés elhagyható, ha *kivételesen* megengedjük, hogy a mátrixhoz a $V_1 = V_2$ esetben is használhatunk két különböző bázist.

*5.8.8 Legyen V vektortér a T *végtelen test* felett, $2 \leq \dim V < \infty$, és $\mathcal{A} \in \operatorname{Hom} V$ tetszőleges lineáris transzformáció. Mutassuk meg, hogy végtelen sok olyan bázis van V-ben, amelyek egymásnak nem skalárszorosai, és $[\mathcal{A}]$-t ezek akármelyike szerint felírva mindig ugyanazt a mátrixot kapjuk.

6. SAJÁTÉRTÉK, MINIMÁLPOLINOM

Ebben a fejezetben véges dimenziós vektorterek lineáris transzformációival foglalkozunk. A sajátértékek központi szerepet játszanak ezek leírásánál és a legkülönfélébb alkalmazásokban. A sajátértékek meghatározásának fő eszköze a karakterisztikus polinom, de a minimálpolinommal is szoros kapcsolatban állnak. A sajátértékek, a karakterisztikus polinom és a minimálpolinom segítségével olyan bázis létezését is garantálhatjuk, amelyben a transzformáció mátrixa a „lehető legszebb".

6.1. Sajátérték, sajátvektor

Ebben a fejezetben V mindig véges dimenziós, nem nulla vektortér a T kommutatív test felett és $\mathcal{A} \in \operatorname{Hom} V$ tetszőleges lineáris transzformáció. A dimenzió végességét általában igen erősen ki fogjuk használni. Az Olvasónak javasoljuk, hogy gondolja majd végig, melyek azok a megállapítások, amelyek végtelen dimenzióra is átmenthetők.

Ha $\mathcal{A}$ egy nem nulla vektort a skalárszorosába képez le (azaz a vektor a transzformáció hatására a „saját egyenesében" marad), akkor ezt a vektort (az $\mathcal{A}$-hoz tartozó) sajátvektornak, a megfelelő skalárt (azaz „a nagyítás/kicsinyítés mértékét") sajátértéknek nevezzük. Pontosabban:

6.1.1 Definíció

Egy $\lambda \in T$ skalárt az $\mathcal{A}$ lineáris transzformáció *sajátérték*ének nevezünk, ha létezik olyan $\mathbf{v} \in V$ *nem nulla* vektor, amelyre $\mathcal{A}\mathbf{v} = \lambda\mathbf{v}$. ♣

6.1.2 Definíció

Egy $\mathbf{v} \in V$ *nem nulla* vektort az $\mathcal{A}$ lineáris transzformáció *sajátvektor*ának nevezünk, ha létezik olyan $\lambda \in T$ skalár, amelyre $\mathcal{A}\mathbf{v} = \lambda\mathbf{v}$. ♣

A sajátérték definíciójában a nullvektort mindenképpen ki kellett zárnunk, hiszen $\mathcal{A}\mathbf{0} = \lambda\mathbf{0}$ minden λ-ra fennáll, vagyis a kikötés nélkül a test minden eleme sajátérték lenne.

A sajátvektoroknál is célszerű kihagyni a nullvektort, például azért, mert a „hozzá tartozó" λ nem egyértelmű (sőt bármi lehet).

FIGYELEM! A saját*érték*ek köréből azonban **nem** zárjuk ki a 0 *skalár*t. A definícióból azonnal adódik, hogy a 0 pontosan akkor sajátértéke $\mathcal{A}$-nak, ha $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$, a megfelelő sajátvektorok pedig a magtér nem nulla elemei.

Példák: $\mathcal{E}$-nek egyetlen sajátértéke az 1, és minden nem nulla vektor sajátvektor. A síkon egy origó körüli forgatásnak nincs sajátértéke (és így sajátvektora sem), ha a forgatás szöge nem egész számú többszöröse π-nek. Egy origón átmenő egyenesre való tükrözés sajátértékei az 1 és a -1, egy vetítésé az 1 és a 0 (a sajátvektorok meghatározását az Olvasóra bízzuk).

Ha $\mathbf{v} \neq \mathbf{0}$ és $\mathcal{A}\mathbf{v} = \lambda\mathbf{v}$, akkor λ-t a $\mathbf{v}$-hez tartozó sajátértéknek, $\mathbf{v}$-t pedig a λ-hoz tartozó (egyik) sajátvektornak nevezzük.

6.1.3 Tétel

I. Minden sajátvektorhoz csak egy sajátérték tartozik.

II. Egy adott λ sajátértékhez tartozó összes sajátvektor és a $\mathbf{0}$ alteret alkotnak. Ezt az alteret a λ-hoz tartozó *sajátaltér*nek nevezzük. ♣

Megjegyzés: Egy sajátaltér — a sajátérték definíciója alapján — nem állhat egyedül a $\mathbf{0}$ vektorból.

Bizonyítás: I. Ha valamely $\mathbf{v} \neq \mathbf{0}$ vektorra λ-val és μ-vel is teljesül $\mathcal{A}\mathbf{v} = \lambda\mathbf{v} = \mu\mathbf{v}$, akkor ebből $\mathbf{v} \neq \mathbf{0}$ miatt $\lambda = \mu$ következik.

II. Az adott halmazba pontosan azok a $\mathbf{v}$ vektorok tartoznak, amelyekre $\mathcal{A}\mathbf{v} = \lambda\mathbf{v}$. Azt kell igazolnunk, hogy ez a (nyilvánvalóan) nem üres halmaz zárt az összeadásra és a skalárral való szorzásra. Legyen $\mathcal{A}\mathbf{v} = \lambda\mathbf{v}$ és $\mathcal{A}\mathbf{z} = \lambda\mathbf{z}$, ekkor

$$\mathcal{A}(\mathbf{v} + \mathbf{z}) = \mathcal{A}\mathbf{v} + \mathcal{A}\mathbf{z} = \lambda\mathbf{v} + \lambda\mathbf{z} = \lambda(\mathbf{v} + \mathbf{z}),$$

és hasonlóan adódik $\mathcal{A}(\alpha\mathbf{v}) = \lambda(\alpha\mathbf{v})$ is. ■

Megjegyzés: Mivel $\mathcal{A}\mathbf{v} = \lambda\mathbf{v} \iff (\mathcal{A} - \lambda\mathcal{E})\mathbf{v} = \mathbf{0}$, ezért a λ-hoz tartozó sajátaltér éppen $\mathrm{Ker}(\mathcal{A} - \lambda\mathcal{E})$. Ezzel egyben újabb bizonyítást is nyertünk arra, hogy a sajáteltér valóban altér.

Sajátvektorokból álló bázis esetén igen „szép” a lineáris transzformáció mátrixa: a főátlón kívül minden elem 0 (azaz a mátrix diagonális).

6.1.4 Tétel

Egy transzformáció mátrixa akkor és csak akkor diagonális, ha a mátrixot sajátvektorokból álló bázis (sajátbázis) szerint írtuk fel. Ekkor a főátlóban álló elemek éppen a megfelelő bázisvektorokhoz tartozó sajátértékek. ♣

Bizonyítás:

$$[\mathcal{A}]_a = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

pontosan akkor teljesül, ha $\mathcal{A}\mathbf{a}_1 = \lambda_1\mathbf{a}_1, \dots, \mathcal{A}\mathbf{a}_n = \lambda_n\mathbf{a}_n$. ■

A lineáris transzformációk és mátrixok kapcsolatának megfelelően a sajátérték és sajátvektor fogalmát négyzetes mátrixokra is értelmezhetjük:

6.1.5 Definíció

Legyen $A \in T^{n\times n}$. Ha egy $\lambda \in T$ skalárra és egy $\mathbf{x} \in T^n$ *nem nulla* vektorra $A\mathbf{x} = \lambda\mathbf{x}$ teljesül, akkor a λ az A mátrix *sajátérték*e, az $\mathbf{x}$ pedig az A *sajátvektor*a. ♣

Megjegyzés: Szokás megkülönböztetni egy mátrix bal, illetve jobb oldali sajátvektorait. A 6.1.5 Definíció jelenti a jobb oldali sajátvektort, míg bal oldali sajátvektoron olyan nem nulla $\mathbf{x}^T$ *sor*vektort értünk, amelyre alkalmas λ-val (*) $\mathbf{x}^T A = \lambda\mathbf{x}^T$ teljesül (a kitevőben a T a transzponáltat jelöli). A (*) egyenlőséget transzponálva a vele ekvivalens $A^T\mathbf{x} = \lambda\mathbf{x}$ adódik, azaz az A bal oldali sajátvektorai éppen az A transzponáltjának jobb oldali sajátvektorai. A következő pontban látni fogjuk, hogy A és A^T sajátértékei ugyanazok (6.2.11 feladat), tehát a sajátértékeknél nem szükséges a bal, illetve jobb oldali jelző. A továbbiakban mátrix sajátvektorán mindig jobb oldali sajátvektort fogunk érteni.

6.1.6 Definíció

Az A és B azonos alakú négyzetes mátrixok *hasonló*k, ha ugyanannak a lineáris transzformációnak két különböző bázis szerinti mátrixai. Jelölés: $A \sim B$. ♣

Így pl. az 5.7.5 feladat azt kérdezi, hogy az adott mátrixpárok hasonlók-e.

Az 5.8.1A Tétel alapján két mátrix hasonlóságát a lineáris transzformációkra történő hivatkozás nélkül is megfogalmazhatjuk: A és B akkor és csak akkor hasonló, ha alkalmas S invertálható mátrixra $B = S^{-1}AS$. Ebből, de közvetlenül a 6.1.6 Definícióból is adódik, hogy a mátrixok hasonlósága ekvivalenciareláció.

A 6.1.1, 6.1.2 és 6.1.5 Definíciók alapján világos, hogy egy lineáris transzformációnak és (bármelyik) mátrixának ugyanazok a sajátértékei: Ha V bázisa

$\mathbf{c}_1, \ldots, \mathbf{c}_n$, akkor $\mathcal{A}\mathbf{v} = \lambda\mathbf{v} \iff [\mathcal{A}]_c[\mathbf{v}]_c = \lambda[\mathbf{v}]_c$. Ez az ekvivalencia a transzformáció és a mátrix sajátvektorainak kapcsolatát is megadja.

Ebből következik, hogy két hasonló mátrixnak ugyanazok a sajátértékei, a megfelelő sajátvektorok viszonya pedig a következő. Legyen $B = S^{-1}AS$, azaz $SB = AS$, ekkor $\mathbf{x} \neq \mathbf{0}$ pontosan akkor sajátvektora B-nek, ha $S\mathbf{x}$ sajátvektora A-nak. Valóban, a $B\mathbf{x} = \lambda\mathbf{x}$ egyenlőséget (balról) S-sel megszorozva $SB\mathbf{x} = S(\lambda\mathbf{x})$, azaz $AS\mathbf{x} = \lambda S\mathbf{x}$ adódik, ez S invertálhatósága miatt ekvivalens az eredetivel és $\mathbf{x} \neq 0 \iff S\mathbf{x} \neq \mathbf{0}$.

Feladatok

6.1.1 Legyen V a legfeljebb 6-odfokú valós együtthatós polinomok (és a 0) szokásos vektortere. Egy általános polinomot f-fel jelölünk. Határozzuk meg az alábbi lineáris transzformációk sajátértékeit és sajátvektorait. Hány dimenziósak a megfelelő sajátalterek? Mely transzformációknak létezik diagonális mátrixa?

(a) $f \mapsto f'$; (b) $f \mapsto xf'$;

(c) $f \mapsto f(6)x^6$; (d) $f \mapsto f$ maradéka $x^2 + 2x + 3$-mal osztva.

6.1.2 Legyen $\mathcal{A}, \mathcal{B} \in \operatorname{Hom} V$ és α közös sajátértéke $\mathcal{A}$-nak és $\mathcal{B}$-nek. Következik-e ebből, hogy $\mu\mathcal{A}$-nak, $\mathcal{A} + \mathcal{B}$-nek, $\mathcal{A}^2$-nek, $\mathcal{A}\mathcal{B}$-nek, illetve $\mathcal{A}^{-1}$-nek is van sajátértéke, és ha igen, akkor hogyan függ ez a sajátérték α-tól?

6.1.3 Legyen $\mathcal{A}, \mathcal{B} \in \operatorname{Hom} V$ és $\mathbf{v}$ közös sajátvektora $\mathcal{A}$-nak és $\mathcal{B}$-nek. Következik-e ebből, hogy $\mathbf{v}$ sajátvektora $\mu\mathcal{A}$-nak, $\mathcal{A} + \mathcal{B}$-nek, $\mathcal{A}^2$-nek, $\mathcal{A}\mathcal{B}$-nek, illetve $\mathcal{A}^{-1}$-nek is, és ha igen, akkor milyen sajátérték tartozik hozzá?

6.1.4 Melyek igazak az alábbi állítások közül?

(a) Ha $\mathbf{v}$ sajátvektora $\mathcal{A}^2$-nek, akkor $\mathbf{v}$ sajátvektora $\mathcal{A}$-nak.

(b) Ha a 0 sajátértéke $\mathcal{A}^2$-nek, akkor a 0 sajátértéke $\mathcal{A}$-nak.

(c) Ha $\mu^2 = \lambda$, és a λ sajátértéke $\mathcal{A}^2$-nek, akkor a μ és a $-\mu$ közül legalább az egyik sajátértéke $\mathcal{A}$-nak.

6.1.5 Melyek igazak az alábbi állítások közül?

(a) Ha $\mathcal{A} + \mathcal{B} = \mathcal{E}$, akkor $\mathcal{A}$-nak és $\mathcal{B}$-nek ugyanazok a sajátvektorai.

(b) Ha $\mathcal{A}\mathcal{B} = \mathcal{O}$, akkor $\mathcal{A}$-nak és $\mathcal{B}$-nek ugyanazok a sajátvektorai.

(c) $\mathcal{A}^2 = \mathcal{O}$ akkor és csak akkor teljesül, ha az $\mathcal{A}$-nak a 0 az egyetlen sajátértéke.

(d) $\mathcal{A} \neq \mathcal{O}$ akkor és csak akkor nullosztó, ha a 0 sajátértéke $\mathcal{A}$-nak.

(e) $\mathcal{A}$ minden sajátvektora $\operatorname{Ker}\mathcal{A}$ és $\operatorname{Im}\mathcal{A}$ közül legalább az egyiknek eleme.

(f) $\mathcal{A}^2 = \mathcal{A} \neq \mathcal{O}$ akkor és csak akkor teljesül, ha $\operatorname{Im}\mathcal{A}$ az $\mathcal{A}$-nak sajátaltere.

6.1.6 Adjunk meg a (közönséges háromdimenziós) térben egy-egy olyan lineáris transzformációt, amelynek 1, 2, illetve 3 (különböző) sajátértéke van.

6.1.7 Legyenek $\mathbf{u}$ és $\mathbf{v}$ az $\mathcal{A}$ transzformáció sajátvektorai. Mi a szükséges és elégséges feltétele annak, hogy $\mathbf{u}+\mathbf{v}$ is sajátvektora legyen $\mathcal{A}$-nak?

6.1.8 Melyek azok a lineáris transzformációk, amelyeknek minden nem nulla vektor sajátvektora?

6.1.9 Legyenek $\mathbf{v}_1, \ldots, \mathbf{v}_k$ az $\mathcal{A}$ lineáris transzformáció olyan sajátvektorai, amelyek közül bármelyik kettőhöz különböző sajátérték tartozik. Bizonyítsuk be, hogy $\mathbf{v}_1, \ldots, \mathbf{v}_k$ lineárisan független.

6.1.10 Bizonyítsuk be, hogy ha $\dim V = n$, akkor bármely $\mathcal{A} \in \operatorname{Hom} V$-nek legfeljebb n (különböző) sajátértéke lehet.

6.1.11 Egy transzformáció mátrixa valamely bázisban $\begin{pmatrix} 1 & 1 & 1 \\ 1 & 1 & 1 \\ 1 & 1 & 1 \end{pmatrix}$. Bizonyítsuk be, hogy van olyan bázis is, amelyben ugyanennek a transzformációnak a mátrixa $\begin{pmatrix} 3 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

6.1.12 Lássuk be:

(a) $\mathcal{AB}$ és $\mathcal{BA}$ sajátértékei ugyanazok.

(b) Ha $\mathcal{B}$ invertálható, akkor $\mathcal{A}$ és $\mathcal{B}^{-1}\mathcal{AB}$ sajátértékei ugyanazok.

6.2. Karakterisztikus polinom

6.2.1 Tétel

Legyen $\mathbf{a}_1, \ldots, \mathbf{a}_n$ bázis V-ben, $\mathcal{A} \in \operatorname{Hom} V$. Egy $\lambda \in T$ skalár akkor és csak akkor sajátértéke $\mathcal{A}$-nak, ha az $[\mathcal{A} - \lambda\mathcal{E}]_a$ mátrix determinánsa $\det([\mathcal{A} - \lambda\mathcal{E}]_a) = 0$. ♣

Bizonyítás: λ akkor és csak akkor sajátérték, ha van olyan $\mathbf{x} \neq \mathbf{0}$ vektor, amelyre $\mathcal{A}\mathbf{x} = \lambda\mathbf{x}$, azaz $(\mathcal{A} - \lambda\mathcal{E})\mathbf{x} = \mathbf{0}$. Az 5.7.3 Tétel alapján ez átírható $[\mathcal{A} - \lambda\mathcal{E}][\mathbf{x}] = [\mathbf{0}]$ alakba, azaz λ pontosan akkor sajátérték, ha ennek a homogén lineáris egyenletrendszernek van nem triviális megoldása. Ez pedig azzal ekvivalens, hogy az együtthatómátrix determinánsa $\det([\mathcal{A} - \lambda\mathcal{E}]_a) = 0$. ■

A tétel alapján lehetőségünk nyílik arra (legalábbis elvileg, de sokszor a gyakorlatban is), hogy a sajátértékeket kiszámítsuk: λ-t változónak tekintve, az $[\mathcal{A} - \lambda\mathcal{E}]_a$ mátrix determinánsa λ-nak egy n-edfokú polinomja, és ennek a gyökei a sajátértékek. A bizonyításból egyúttal a megfelelő sajátvektorok meghatározására is leolvasható egy eljárás: a szóban forgó homogén lineáris egyenletrendszerek (nem triviális) megoldásait kell megkeresnünk (például Gauss-kiküszöböléssel).

Azonnal adódik, hogy a tétel állításában szereplő determinánsnak mint polinomnak a gyökei nem függnek attól, hogy melyik bázisban írtuk fel a transzformáció mátrixát, hiszen ezek a gyökök éppen a sajátértékek. Ennél jóval több is igaz: maga ez a determináns-polinom sem függ a bázis megválasztásától (a mátrixra ez természetesen már nem érvényes). Ennek bizonyítását nem részletezzük (azt kell megvizsgálni, hogyan változik meg a transzformáció mátrixa, ha másik bázisra térünk át, és ezután fel kell használni, hogy mátrixok szorzatának a determinánsa a tényezők determinánsainak a szorzata — lásd az 5.8.1A Tételt és az 5.8.4 feladatot).

A szóban forgó polinomot a transzformáció karakterisztikus polinomjának nevezzük:

6.2.2 Definíció

Legyen az $\mathcal{A} \in \operatorname{Hom} V$ transzformáció mátrixa (valamilyen bázisban)

$$[\mathcal{A}] = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}.$$

Az $\mathcal{A}$ *karakterisztikus polinom*ján a

$$k_{\mathcal{A}}(x) = \det[\mathcal{A} - x\mathcal{E}] = \begin{vmatrix} \alpha_{11} - x & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} - x & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} - x \end{vmatrix}$$

polinomot értjük. ♣

Az előrebocsátott megjegyzés szerint ez a polinom csak az $\mathcal{A}$ transzformációtól függ, és független a mátrix (azaz a bázis) megválasztásától. Főegyütthatója $(-1)^n$, az $n-1$-edfokú tag együtthatója az $[\mathcal{A}]$ főátlójában levő elemek összegének ($[\mathcal{A}]$ ún. *nyom*ának) a $(-1)^{n-1}$-szerese, a konstans tag pedig $[\mathcal{A}]$ determinánsa. Így $[\mathcal{A}]$ nyoma és determinánsa sem függ attól, hogy a mátrixot melyik bázisban írtuk fel.

A 6.2.2 Definíció alapján a 6.2.1 Tétel azt mondja ki, hogy a transzformáció sajátértékei pontosan a karakterisztikus polinom gyökei.

Értelmezhetjük négyzetes mátrixok karakterisztikus polinomját is a 6.2.2 Definíció mintájára, és ennek alapján mátrixokra is igaz, bogy a karakterisztikus polinom gyökei éppen a mátrix sajátértékei. A transzformációk és mátrixok kapcsolata alapján világos, hogy hasonló mátrixoknak ugyanaz a karakterisztikus polinomja.

Feladatok

6.2.1 Írjuk fel a 6.1.1 feladatban szereplő transzformációk karakterisztikus polinomját.

6.2.2 Legyen V a síkvektorok szokásos vektortere. Írjuk fel az alábbi transzformációk karakterisztikus polinomját.

(a) Tükrözés origón átmenő egyenesre;
(b) adott irányú vetítés origón átmenő egyenesre;
(c) 90 fokos elforgatás az origó körül;
(d) 60 fokos elforgatás az origó körül;
(e) helybenhagyás;
(f) középpontos tükrözés az origóra;
(g) 5-szörös arányú középpontos nagyítás az origóból.

6.2.3 Legyen $\mathcal{A}$ karakterisztikus polinomja $f(x)$. Hogyan kapjuk meg $\mu\mathcal{A}$ karakterisztikus polinomját?

6.2.4 Adjunk új bizonyítást a 6.1.10 és 6.1.9 feladatokra (ebben a sorrendben).

6.2.5 Bizonyítsuk be, hogy a komplex test feletti (véges dimenziós) vektortérben minden lineáris transzformációnak van sajátvektora.

6.2.6

(a) Van-e a (közönséges) síkon olyan lineáris transzformáció, amelynek nincs sajátvektora?

(b) Van-e a (közönséges) téren olyan lineáris transzformáció, amelynek nincs sajátvektora?

6.2.7 Legyen $T = \mathbf{R}$ és $\mathbf{b}_1, \ldots, \mathbf{b}_4$ bázis a V vektortérben. Határozzuk meg az alábbi lineáris transzformációk karakterisztikus polinomját, sajátértékeit és sajátvektorait. Mely transzformációknak létezik diagonális mátrixa?

(a) $\mathbf{b}_1 \mapsto \mathbf{b}_2, \quad \mathbf{b}_2 \mapsto \mathbf{b}_3, \quad \mathbf{b}_3 \mapsto \mathbf{b}_4, \quad \mathbf{b}_4 \mapsto \mathbf{b}_1$;

(b) $\mathbf{b}_1 \mapsto \mathbf{b}_2, \quad \mathbf{b}_2 \mapsto \mathbf{b}_1, \quad \mathbf{b}_3 \mapsto \mathbf{b}_4, \quad \mathbf{b}_4 \mapsto \mathbf{b}_4$;

(c) $\mathbf{b}_1 \mapsto \mathbf{b}_1 + \mathbf{b}_2, \quad \mathbf{b}_2 \mapsto \mathbf{b}_2 + \mathbf{b}_3, \quad \mathbf{b}_3 \mapsto \mathbf{b}_3 + \mathbf{b}_4, \quad \mathbf{b}_4 \mapsto \mathbf{b}_4 + \mathbf{b}_1$.

Oldjuk meg a feladatot a komplex test felett is.

6.2.8 Egy lineáris transzformációnak hány (különböző) diagonális mátrixa létezik (feltéve, hogy egyáltalán létezik diagonális mátrixa)?

6.2.9 Legyen $\dim V = n$ és tegyük fel, hogy az $\mathcal{A} \in \operatorname{Hom} V$ transzformációnak n különböző sajátértéke van. Bizonyítsuk be, hogy a sajátértékek összege, illetve szorzata az $[\mathcal{A}]$ (tetszőleges bázisban felírt) mátrix nyoma, illetve determinánsa.

6.2.10 Oldjuk meg újra az 5.7.5 feladatot.

6.2.11 Lássuk be, hogy egy mátrixnak és a transzponáltjának ugyanaz a karakterisztikus polinomja, és így a sajátértékeik is megegyeznek.

6.3. Minimálpolinom

Legyen $V \neq \mathbf{0}$ egy véges dimenziós vektortér a T test felett, $\dim V = n$, $\mathcal{A} \in \operatorname{Hom} V$, $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k \in T[x]$.

Értelmezni fogjuk az f polinomnak az $\mathcal{A}$ „helyen” felvett „helyettesítési értékét”, $f(\mathcal{A})$-t, ami maga is egy $V \to V$ lineáris transzformáció lesz.

Először definiáljuk az $\mathcal{A}$ nulladik hatványát a kézenfekvő $\mathcal{A}^0 = \mathcal{E}$ egyenlőséggel (ahol $\mathcal{E}$ az identikus transzformáció). Ezután már természetes módon adódik az $f(\mathcal{A}) = \alpha_0\mathcal{E} + \alpha_1\mathcal{A} + \ldots + \alpha_k\mathcal{A}^k$ definíció. Nyilván $f(\mathcal{A}) \in \operatorname{Hom} V$.

Könnyen ellenőrizhető, hogy két polinom összegének, illetve szorzatának a helyettesítési értéke a helyettesítési értékek összege, illetve szorzata, azaz

$$(f+g)(\mathcal{A}) = f(\mathcal{A}) + g(\mathcal{A}) \qquad \text{és} \qquad (fg)(\mathcal{A}) = f(\mathcal{A})g(\mathcal{A})\,.$$

A *gyök*öt is a „szokásos” módon értelmezzük: az $\mathcal{A}$ transzformáció gyöke az f polinomnak, ha $f(\mathcal{A}) = \mathcal{O}$.

6.3.1 Definíció

Az f polinom az $\mathcal{A}$ transzformáció *minimálpolinom*ja, ha f a(z egyik) legkisebb fokú olyan (nem nulla) polinom, amelynek az $\mathcal{A}$ gyöke. Az $\mathcal{A}$ minimálpolinomját $m_{\mathcal{A}}$-val jelöljük. ♣

Példák: A nulla transzformáció (egyik) minimálpolinomja x, a síkban egy tengelyes tükrözésé x^2-1, a 90 fokos elforgatásé x^2+1, egy egyenesre történő vetítésé x^2-x.

6.3.2 Tétel

Minden $\mathcal{A}$-nak létezik minimálpolinomja, és ez konstans szorzó erejéig egyértelmű. ♣

Ennek alapján nem okoz problémát, hogy az $m_{\mathcal{A}}$ jelölés az $\mathcal{A}$ *akármelyik* minimálpolinomját jelentheti, hiszen ezek a polinomok egymástól csak egy konstans szorzóban különböznek. Ennek megfelelően a továbbiakban mindig (határozott névelővel) „a" minimálpolinomról fogunk beszélni (de ezen akármelyik „példányt" érthetjük). Ha valaki (nagyon) egyértelműsíteni akar, akkor választhatja mondjuk azt az alakot, amelynek a főegyütthatója 1.

Bizonyítás: Először az egyértelműséget igazoljuk. Tegyük fel, hogy $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$ és $g = \beta_0 + \beta_1 x + \ldots + \beta_k x^k$ is minimálpolinomja $\mathcal{A}$-nak, α_k, $\beta_k \neq 0$. Ekkor a $h = \alpha_k g - \beta_k f$ polinomra

$$h(\mathcal{A}) = \alpha_k g(\mathcal{A}) - \beta_k f(\mathcal{A}) = \alpha_k \mathcal{O} - \beta_k \mathcal{O} = \mathcal{O}\,,$$

ugyanakkor h foka kisebb k-nál. A minimálpolinom definíciója miatt így csak $h = 0$ lehetséges, azaz valóban $f = \gamma g$, ahol $\gamma = \alpha_k/\beta_k$.

Most a minimálpolinom létezését bizonyítjuk. Ehhez elég megmutatnunk, hogy egyáltalán létezik olyan nem nulla polinom, amelynek az $\mathcal{A}$ gyöke, ugyanis az ilyen tulajdonságú polinomok között kell lennie minimális fokúnak, és az megfelel minimálpolinomnak.

Tekintsük $\operatorname{Hom} V$-ben az

$$\mathcal{E}, \mathcal{A}, \mathcal{A}^2, \ldots, \mathcal{A}^{n^2} \quad (n = \dim V)$$

transzformációkat. Mivel $\dim \operatorname{Hom} V = n^2$, ezért ezek lineárisan összefüggők. Így létezik olyan $\gamma_0, \gamma_1, \ldots, \gamma_{n^2} \in T$, ahol nem minden γ_i nulla és

$$\gamma_0 \mathcal{E} + \gamma_1 \mathcal{A} + \ldots + \gamma_{n^2} \mathcal{A}^{n^2} = \mathcal{O}\,.$$

Ez azt jelenti, hogy $\mathcal{A}$ gyöke a

$$\gamma_0 + \gamma_1 x + \ldots + \gamma_{n^2} x^{n^2}$$

nem nulla polinomnak. ■

A bizonyításból az is kiderült, hogy a minimálpolinom foka $\deg m_{\mathcal{A}} \leq n^2$. Ennél több is igaz: $\deg m_{\mathcal{A}} \leq n$. Ez következik majd a 6.3.5, valamint a 6.5.6 Tételből is.

A minimálpolinom segítségével könnyen áttekinthetjük azokat a polinomokat, amelyeknek az $\mathcal{A}$ gyöke; ezek éppen a minimálpolinom többszörösei (polinomszorosai):

6.3.3 Tétel

$$g(\mathcal{A}) = \mathcal{O} \iff m_{\mathcal{A}} \,|\, g\,. \ \clubsuit$$

Bizonyítás: Ha $m_{\mathcal{A}} \,|\, g$, azaz $g = t m_{\mathcal{A}}$, akkor

$$g(\mathcal{A}) = t(\mathcal{A}) m_{\mathcal{A}}(\mathcal{A}) = t(\mathcal{A}) \cdot \mathcal{O} = \mathcal{O}\,,$$

tehát $\mathcal{A}$ valóban gyöke g-nek.

Megfordítva, tegyük fel, hogy $g(\mathcal{A}) = \mathcal{O}$. Osszuk el g-t maradékosan $m_{\mathcal{A}}$-val: $g = t m_{\mathcal{A}} + r$, ahol $\deg r < \deg m_{\mathcal{A}}$ vagy $r = 0$. Ekkor

$$r(\mathcal{A}) = g(\mathcal{A}) - t(\mathcal{A}) m_{\mathcal{A}}(\mathcal{A}) = \mathcal{O} - t(\mathcal{A})\mathcal{O} = \mathcal{O}\,.$$

A minimálpolinom definíciója miatt $\deg r < \deg m_{\mathcal{A}}$ nem lehet, ezért $r = 0$, azaz valóban $m_{\mathcal{A}} \,|\, g$. ■

A 6.3.3 Tétel a minimálpolinom megkereséséhez is segítséget nyújthat: ha már találtunk egy olyan (nem nulla) polinomot, amelynek a transzformáció gyöke, akkor a minimálpolinom csak ennek osztói közül kerülhet ki.

A karakterisztikus polinomhoz hasonlóan a minimálpolinom is szoros kapcsolatban áll a sajátértékekkel:

6.3.4 Tétel

A minimálpolinom (T-beli) gyökei éppen a sajátértékek. ♣

Bizonyítás: Először azt igazoljuk, hogy minden sajátérték gyöke a minimálpolinomnak. Legyen $m_{\mathcal{A}} = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$, és tegyük fel, hogy $\lambda \in T$

sajátértéke $\mathcal{A}$-nak, azaz alkalmas $\mathbf{u} \neq \mathbf{0}$ vektorral $\mathcal{A}\mathbf{u} = \lambda\mathbf{u}$ teljesül. Ekkor

$$\mathcal{A}^2\mathbf{u} = \mathcal{A}(\mathcal{A}\mathbf{u}) = \mathcal{A}(\lambda\mathbf{u}) = \lambda(\mathcal{A}\mathbf{u}) = \lambda(\lambda\mathbf{u}) = \lambda^2\mathbf{u}\,,$$

és ugyanígy igazolható (teljes indukcióval), hogy bármely j pozitív egészre $\mathcal{A}^j\mathbf{u} = \lambda^j\mathbf{u}$.

Az $m_{\mathcal{A}}(\mathcal{A}) = \mathcal{O}$ transzformációt az $\mathbf{u}$ vektorra alkalmazva a $\mathbf{0}$ vektort kapjuk. Így

$$\begin{aligned}\mathbf{0} = m_{\mathcal{A}}(\mathcal{A})\mathbf{u} &= (\alpha_0\mathcal{E} + \alpha_1\mathcal{A} + \ldots + \alpha_k\mathcal{A}^k)\mathbf{u} = \\ &= \alpha_0(\mathcal{E}\mathbf{u}) + \alpha_1(\mathcal{A}\mathbf{u}) + \ldots + \alpha_k(\mathcal{A}^k\mathbf{u}) = \alpha_0\mathbf{u} + \alpha_1(\lambda\mathbf{u}) + \ldots + \alpha_k(\lambda^k\mathbf{u}) = \\ &= (\alpha_0 + \alpha_1\lambda + \ldots + \alpha_k\lambda^k)\mathbf{u} = m_{\mathcal{A}}(\lambda)\mathbf{u}\,,\end{aligned}$$

azaz $m_{\mathcal{A}}(\lambda)\mathbf{u} = \mathbf{0}$. Mivel $\mathbf{u} \neq \mathbf{0}$, ezért innen $m_{\mathcal{A}}(\lambda) = 0$ következik, vagyis λ valóban gyöke a minimálpolinomnak.

Megfordítva, azt kell még megmutatnunk, hogy a minimálpolinom minden gyöke egyben sajátérték is. Legyen $\lambda \in T$ gyöke $m_{\mathcal{A}}$-nak, ekkor a minimálpolinom $m_{\mathcal{A}} = (x - \lambda)g$ alakban írható. Az $\mathcal{A}$ transzformációt behelyettesítve

$$\mathcal{O} = m_{\mathcal{A}}(\mathcal{A}) = (\mathcal{A} - \lambda\mathcal{E})g(\mathcal{A})$$

adódik. Ez azt jelenti, hogy $\operatorname{Ker}(\mathcal{A} - \lambda\mathcal{E}) \supseteq \operatorname{Im} g(\mathcal{A})$. Mivel $\deg g < \deg m_{\mathcal{A}}$, ezért $g(\mathcal{A}) \neq \mathcal{O}$, tehát $\operatorname{Im} g(\mathcal{A}) \neq \mathbf{0}$. Így $\operatorname{Ker}(\mathcal{A} - \lambda\mathcal{E}) \neq \mathbf{0}$ is teljesül. Mivel $\operatorname{Ker}(\mathcal{A} - \lambda\mathcal{E})$ bármely nem nulla eleme a λ-hoz tartozó sajátvektor, tehát λ valóban sajátérték. ■

Az alábbi tétel a karakterisztikus polinom és a minimálpolinom szoros kapcsolatát mutatja:

6.3.5 Tétel (Cayley–Hamilton-tétel)
A minimálpolinom osztója a karakterisztikus polinomnak. ♣

A 6.3.3 Tétel alapján a Cayley–Hamilton-tétel úgy is fogalmazható, hogy minden transzformáció gyöke a karakterisztikus polinomjának.

A 6.2.1, 6.3.4 és 6.3.5 Tételek a sajátértékekek, a karakterisztikus polinom és a minimálpolinom közötti összefüggésekről szólnak, azonban ezek egyike sem következik a másik kettőből, lásd a 6.3.19 feladatot.

Bizonyítás: A 6.3.3 Tétel szerint azt kell igazolnunk, hogy az $\mathcal{A}$ transzformáció gyöke a $k_{\mathcal{A}}(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_n x^n$ karakterisztikus polinomnak.

Alkalmazzuk a 2.2.3 Lemmát az $\mathcal{A} - x\mathcal{E}$ transzformáció (egyik) $A - xE$ mátrixára:

$$(A - xE)B(x) = \big(\det(A - xE)\big)E = k_{\mathcal{A}}(x)E, \tag{6.3.1}$$

ahol $B(x)$ az $A-xE$ mátrix előjeles aldeterminánsaiból képezett mátrix transzponáltja. Mivel az aldeterminánsok az x-nek $(n-1)$-edfokú polinomjai, ezért a $B(x)$ mátrix az x egy olyan $n-1$-edfokú

$$B(x) = B_0 + B_1x + \ldots + B_{n-1}x^{n-1}$$

polinomja, ahol a B_i együtthatók $n \times n$-es mátrixok (ebben a felfogásban a mátrixegyütthatókat a változó hatványai elé írtuk). A (6.3.1) egyenlőség ennek megfelelően az

$$(A - Ex)(B_0 + B_1x + \ldots + B_{n-1}x^{n-1}) = \gamma_0E + \gamma_1Ex + \ldots + \gamma_nEx^n \tag{6.3.2}$$

alakot ölti. Végezzük el (6.3.2) bal oldalán a szorzást és hasonlítsuk össze rendre a két oldalon az x-hatványok együtthatóit:

$$\begin{aligned} AB_0 &= \gamma_0E; \\ AB_1 - B_0 &= \gamma_1E; \\ &\vdots \\ AB_{n-1} - B_{n-2} &= \gamma_{n-1}E; \\ -B_{n-1} &= \gamma_nE. \end{aligned} \tag{6.3.3}$$

Szorozzuk meg balról a (6.3.3) egyenletrendszer második egyenletét A-val, a harmadikat A^2-tel stb., az utolsót A^n-nel, majd adjuk össze az így kapott egyenleteket. Ekkor a bal oldalon a 0 mátrix, a jobb oldalon pedig $\gamma_0E+\gamma_1A+ +\ldots+\gamma_nA^n = k_{\mathcal{A}}(A)$ adódik. Ez azt jelenti, hogy az A mátrix és így az $\mathcal{A}$ transzformáció is valóban gyöke a karakterisztikus polinomnak. ■

Értelmezhetjük négyzetes mátrixok minimálpolinomját is a 6.3.1 Definíció mintájára, és ennek alapján a 6.3.2–6.3.5 Tételek mátrixokra is érvényesek maradnak. A transzformációk és mátrixok kapcsolata alapján világos, hogy hasonló mátrixoknak ugyanaz a minimálpolinomja, de ez a transzformációkra történő hivatkozás nélkül is belátható (6.3.20 feladat).

Feladatok

6.3.1 Írjuk fel a 6.1.1, 6.2.2 és 6.2.7 feladatokban szereplő transzformációk minimálpolinomját.

6.3.2 Jellemezzük azokat a transzformációkat, amelyek minimálpolinomja elsőfokú.

6.3.3 Hogyan olvasható le a minimálpolinomról, hogy a transzformációnak létezik-e inverze?

6.3.4 Bizonyítsuk be, hogy (invertálható $\mathcal{A}$ esetén) $\mathcal{A}^{-1}$ felírható $\mathcal{A}$ polinomjaként, azaz van olyan ($\mathcal{A}$-tól függő) $f \in T[x]$, amelyre $\mathcal{A}^{-1} = f(\mathcal{A})$.

6.3.5 Invertálható transzformáció esetén hogyan kapjuk meg $\mathcal{A}$ minimálpolinomjából $\mathcal{A}^{-1}$ minimálpolinomját?

6.3.6 Melyek igazak az alábbi állítások közül?

(a) A minimálpolinom mindig irreducibilis (T felett).

(b) Ha egy transzformáció gyöke egy (T felett) irreducibilis polinomnak, akkor ez a polinom a transzformáció minimálpolinomja.

(c) Ha $T = \mathbf{C}$, és a karakterisztikus polinomnak nincs többszörös gyöke, akkor a minimálpolinom megegyezik a karakterisztikus polinommal.

(d) Ha $T = \mathbf{C}$, és a minimálpolinom megegyezik a karakterisztikus polinommal, akkor a karakterisztikus polinomnak nincs többszörös gyöke.

(e) Ha a transzformációnak létezik diagonális mátrixa, akkor a minimálpolinomnak nincs többszörös gyöke.

(f) Ha egy f polinomnak az $\mathcal{A}$ gyöke, akkor f-nek az $\mathcal{A}$ minden sajátértéke is gyöke.

(g) Ha $T = \mathbf{C}$, és egy f polinomnak az $\mathcal{A}$ minden sajátértéke gyöke, akkor f-nek az $\mathcal{A}$ is gyöke.

6.3.7 Adjunk új bizonyítást a 6.2.5 feladatra.

6.3.8 Adjunk új bizonyítást az 5.6.9 feladatra.

6.3.9 Van-e az egységmátrixon kívül olyan 2×2-es
(a) valós elemű; (b) racionális elemű
mátrix, amelynek az ötödik hatványa az egységmátrix?

6.3.10 Mi a kapcsolata $\mathcal{AB}$ és $\mathcal{BA}$ minimálpolinomjának?

6.3.11 Bizonyítsuk be, hogy $\mathcal{A}$ és $\mathcal{B}^{-1}\mathcal{AB}$ minimálpolinomja ugyanaz.

6.3.12 Legyen $\dim V = n$, $\mathcal{A} \in \operatorname{Hom} V$ és $k \geq n$ tetszőleges egész. Bizonyítsuk be, hogy létezik olyan (pontosan) k-adfokú polinom, amelynek az $\mathcal{A}$ gyöke és amelyben a $k-1, k-2, \ldots, n$-edfokú tagok együtthatója mind 0.

6.3.13 Tekintsük $\operatorname{Hom} V$-ben az $\mathcal{A}^i, \quad i = 0, 1, 2, \ldots$ $(\mathcal{A}^0 = \mathcal{E})$ transzformációk által generált alteret. Hány dimenziós ez az altér?

*6.3.14 Legyen $\deg m_{\mathcal{A}} = k$. Mik $\deg m_{\mathcal{A}^2}$ lehetséges értékei?

M**6.3.15 A komplex test feletti vektorterek esetében $\mathcal{A}$ és $\mathcal{A}^2$ minimálpolinomja akkor és csak akkor egyezik meg, ha $m_{\mathcal{A}}$-nak (i) minden gyöke 0 vagy páratlan rendű egységgyök, (ii) a 0 legfeljebb egyszeres gyök, és (iii) bármely gyöknek a négyzete is gyök és multiplicitásuk is azonos.

6.3.16 Legyen h tetszőleges polinom. Bizonyítsuk be, hogy a $h(\mathcal{A})$ transzformációnak akkor és csak akkor létezik inverze, ha $(h\,,\, m_{\mathcal{A}}) = 1$.

6.3.17 Legyen $D \in T^{n\times n}$ rögzített mátrix és $\mathcal{A} \in \operatorname{Hom}(T^{n\times n})$ a következő: tetszőleges $B \in T^{n\times n}$ mátrixra $\mathcal{A}(B) = DB$.
Milyen kapcsolat áll fenn $\mathcal{A}$ és D sajátértékei, illetve minimálpolinomja között? Érvényes-e ugyanez a karakterisztikus polinomra is?

*6.3.18 Bizonyítsuk be, hogy minden legalább elsőfokú polinom minimálpolinomja egy alkalmas lineáris transzformációnak.

6.3.19 Mutassuk meg, hogy a 6.2.1, 6.3.4 és 6.3.5 Tételek egyike sem következik a másik kettőből.

6.3.20 A lineáris transzformációkra történő hivatkozás nélkül igazoljuk, hogy hasonló mátrixoknak ugyanaz a minimálpolinomja.

6.3.21 Egy valós elemű A négyzetes mátrixot tekinthetünk komplex elemű mátrixnak is. Bizonyítsuk be, hogy A-nak az $\mathbf{R}$ feletti minimálpolinomja egyben $\mathbf{C}$ feletti minimálpolinom is.

6.3.22 (a) Lássuk be, hogy egy racionális elemű négyzetes mátrix karakterisztikus polinomjában és minimálpolinomjában pontosan ugyanazok az irreducibilis tényzők szerepelnek (csak nem feltétlenül ugyanakkora multiplicitással).
(b) Adjunk új megoldást a 2.2.14 feladatra.

6.4. Invariáns altér

6.4.1 Definíció
Egy U altér az $\mathcal{A}$-nak *invariáns altere* (vagy *$\mathcal{A}$-invariáns altér, $\mathcal{A}$ szerint invariáns altér*), ha $\mathbf{u} \in U \Rightarrow \mathcal{A}\mathbf{u} \in U$. ♣

Amikor egyértelmű, hogy melyik $\mathcal{A}$ transzformációt nézzük, akkor nem fontos az elnevezésben külön utalni az $\mathcal{A}$-ra, és használhatjuk a sima „invariáns altér" kifejezést. Ne felejtsük azonban el, hogy mindig egy adott transzformáció szerinti invariáns altérről van szó, önmagában annak semmi értelme sincs, hogy egy altér „csak úgy" invariáns.

Példák invariáns altérre:
$\operatorname{Im}\mathcal{A}$ és minden azt tartalmazó altér, $\operatorname{Ker}\mathcal{A}$ és annak minden altere, egy sajátvektor által generált altér, egy sajátaltér és annak minden altere, (nem feltétlenül azonos sajátértékhez tartozó) sajátvektorok által generált altér. (A legutolsó példának az első kivételével a többi — a nulla altértől eltekintve — mind speciális esete.)

Számos invariáns alteret kaphatunk az alábbi általános konstrukció segítségével. Vegyünk egy tetszőleges $\mathbf{u}$ vektort, ennek az $\mathcal{A}$ szerinti képét, $\mathcal{A}\mathbf{u}$-t, majd $\mathcal{A}\mathbf{u}$-nak a képét, $\mathcal{A}^2\mathbf{u}$-t stb. Az így kapott $\mathcal{A}^i\mathbf{u}, \quad i = 0, 1, 2, \ldots$ $(\mathcal{A}^0 = \mathcal{E})$ vektorok által generált altér (az $\mathcal{A}$ szerint) invariáns altér lesz.

6.4.2 Definíció
Az $\mathbf{u}$ vektor és az $\mathcal{A}$ transzformáció által generált $\langle \mathbf{u}, \mathcal{A} \rangle$ altéren az $\mathcal{A}^i\mathbf{u}$, $i = 0, 1, 2, \ldots$ vektorok által generált alteret értjük:

$$\langle \mathbf{u}, \mathcal{A} \rangle = \langle \mathbf{u}, \mathcal{A}\mathbf{u}, \mathcal{A}^2\mathbf{u}, \ldots \rangle \,. \ \clubsuit$$

Az $\langle \mathbf{u}, \mathcal{A} \rangle$ altér az $\mathcal{A}$-nak az $\mathbf{u}$ vektort tartalmazó legszűkebb invariáns altere (lásd a 6.4.12 feladatot). Ennek megfelelően használható az „$\mathbf{u}$ által generált $\mathcal{A}$-invariáns altér" elnevezés és az $\langle \mathbf{u} \rangle_{\mathcal{A}}$ jelölés is. Ez utóbbi jelölésnél viszont nagyon kell vigyázni arra, nehogy a transzformációra utaló indexet lefelejtsük, hiszen anélkül az egészen más jelentésű („sima") generált altér fogalmához jutunk (ami egyébként felfogható az $\mathcal{A} = \mathcal{E}$ speciális esetnek is). A továbbiakban végig a 6.4.2 Definícióban eredetileg megadott elnevezést és az $\langle \mathbf{u}, \mathcal{A} \rangle$ jelölést fogjuk használni.

Könnyen adódik, hogy $\langle \mathbf{u}, \mathcal{A} \rangle$ definíciójában a végtelen elemű $\mathcal{A}^i\mathbf{u}$ generátorrendszer végessel is helyettesíthető, hiszen ezek között a vektorok között

legfeljebb $n = \dim V$ darab lehet lineárisan független. Az is megmutatható, hogy elég az *első* n kitevőt, azaz $0 \leq i \leq n-1$-et venni (lásd még a 6.5.4 Tételt és bizonyítását).

Feladatok

6.4.1 Bizonyítsuk be, hogy ha U_1 és U_2 invariáns alterei $\mathcal{A}$-nak, akkor $U_1 \cap U_2$ és $\langle U_1, U_2 \rangle$ is invariáns alterek.

6.4.2 Melyek igazak az alábbi állítások közül?

(a) Ha U invariáns altere $\mathcal{A}$-nak, akkor invariáns altere $\mathcal{A}^3$-nek is.

(b) Ha U invariáns altere $\mathcal{A}^3$-nek, akkor invariáns altere $\mathcal{A}$-nak is.

(c) U invariáns altere $\mathcal{A}$-nak, $U \cap \operatorname{Im}\mathcal{A} = \mathbf{0} \Rightarrow U \subseteq \operatorname{Ker}\mathcal{A}$.

(d) U invariáns altere $\mathcal{A}$-nak, $U \cap \operatorname{Ker}\mathcal{A} = \mathbf{0} \Rightarrow U \subseteq \operatorname{Im}\mathcal{A}$.

6.4.3 Tekintsük egy transzformáció mátrixát a $\mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_n$ bázisban és legyen $k < n$. Hogyan állapítható meg a mátrixról, hogy az első k bázisvektor által generált $\langle \mathbf{b}_1, \mathbf{b}_2, \ldots, \mathbf{b}_k \rangle$ altér invariáns-e?

6.4.4 Legyen $\dim V = n$ és U egy k-dimenziós altér. Tekintsük azokat az $\mathcal{A} \in \operatorname{Hom} V$ transzformációkat, amelyeknek az U invariáns altere.

(a) Lássuk be, hogy ezek alteret, sőt részalgebrát alkotnak $\operatorname{Hom} V$-ben.

(b) Hány dimenziós ez az altér?

6.4.5

(a) Melyek azok a transzformációk, amelyekre minden altér invariáns?

(b) Melyek azok a transzformációk, amelyekre minden 13-dimenziós altér invariáns?

6.4.6 Legyen $\mathcal{AB} = \mathcal{BA}$. Bizonyítsuk be, hogy $\operatorname{Im}\mathcal{A}$, $\operatorname{Ker}\mathcal{A}$, valamint $\mathcal{A}$ minden sajátaltere invariáns altere $\mathcal{B}$-nek.

6.4.7

(a) Bizonyítsuk be, hogy tetszőleges $\lambda \neq 0$-ra és μ-re $\mathcal{A}, \lambda\mathcal{A}, \mathcal{A} + \mu\mathcal{E}$ és $\lambda\mathcal{A} + \mu\mathcal{E}$ invariáns alterei egybeesnek.

(b) Tegyük fel, hogy $\mathcal{A}$ és $\mathcal{B}$ invariáns alterei egybeesnek. Következik-e ebből, hogy $\mathcal{B} = \lambda\mathcal{A} + \mu\mathcal{E}$ (alkalmas $\lambda \neq 0$-ra és μ-re)?

6.4.8 Hány invariáns altere van a legfeljebb n-edfokú valós együtthatós polinomok szokásos vektorterében a deriválásnak mint lineáris transzformációnak?

6.4.9
(a) Bizonyítsuk be, hogy tetszőleges f polinomra $\operatorname{Ker} f(\mathcal{A})$ invariáns altere $\mathcal{A}$-nak.
(b) Igazoljuk, hogy $\operatorname{Ker} f(\mathcal{A}) = \operatorname{Ker} g(\mathcal{A}) \iff (f\,,\, m_{\mathcal{A}}) = (g\,,\, m_{\mathcal{A}})$.
(c) Mutassuk meg, hogy bármely transzformációnak legalább annyi invariáns altere van, mint ahány páronként nem-egységszeres osztója van a minimálpolinomjának.
(d) Melyek azok a transzformációk, amelyeknek csak triviális invariáns alterei vannak (azaz csak a nulla és az egész tér)?

M 6.4.10 Lássuk be az előző feladat állításait, ha a magtér helyett mindenhol képtér szerepel.

6.4.11 Legyen $m_{\mathcal{A}} = fg$. Következik-e ebből
(a) $\operatorname{Im} f(\mathcal{A}) \subseteq \operatorname{Ker} g(\mathcal{A})$; (b) $\operatorname{Im} f(\mathcal{A}) = \operatorname{Ker} g(\mathcal{A})$?

6.4.12 Igazoljuk, hogy $\langle \mathbf{u}, \mathcal{A}\rangle$ valóban az $\mathbf{u}$ vektort tartalmazó legszűkebb $\mathcal{A}$-invariáns altér, azaz (i) $\mathcal{A}$-invariáns altér, (ii) tartalmazza $\mathbf{u}$-t, és (iii) része bármely olyan $\mathcal{A}$-invariáns altérnek, amelyben az $\mathbf{u}$ benne van.

6.4.13 Mely $\mathbf{u}$ vektorokra lesz $\langle \mathbf{u}, \mathcal{A}\rangle$ dimenziója 0, illetve 1?

6.4.14 Mutassunk példát olyan $\mathcal{A}$ transzformációra és ennek olyan invariáns alterére, amely nem $\langle \mathbf{u}, \mathcal{A}\rangle$ alakú.

6.4.15 Melyek igazak az alábbi állítások közül?
(a) Ha $\lambda \neq 0$, akkor $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \lambda\mathbf{u}, \mathcal{A}\rangle$.
(b) $\langle \mathbf{u}+\mathbf{v}, \mathcal{A}\rangle = \big\langle \langle \mathbf{u}, \mathcal{A}\rangle\,,\, \langle \mathbf{v}, \mathcal{A}\rangle\big\rangle$.
(c) $\langle \mathbf{u}, \mathcal{A}^2\rangle \subseteq \langle \mathbf{u}, \mathcal{A}\rangle$.
(d) Ha van olyan $\mathcal{A}$, amelyre $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \mathbf{v}, \mathcal{A}\rangle$, akkor $\mathbf{u} = \lambda\mathbf{v}$.
(e) Ha minden $\mathcal{A}$-ra $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \mathbf{v}, \mathcal{A}\rangle$, akkor $\mathbf{u} = \lambda\mathbf{v}$.
(f) Ha van olyan $\mathbf{u} \neq \mathbf{0}$, amelyre $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \mathbf{u}, \mathcal{B}\rangle$, akkor $\mathcal{A} = \lambda\mathcal{B}$.
(g) Ha minden $\mathbf{u}$-ra $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \mathbf{u}, \mathcal{B}\rangle$, akkor $\mathcal{A} = \lambda\mathcal{B}$.

6.5. Rend

Legyen $V \neq \mathbf{0}$ egy véges dimenziós vektortér a T kommutatív test felett, $\dim V = n$, $\mathcal{A} \in \operatorname{Hom} V$. A minimálpolinom definíciója szerint bármely $\mathbf{u} \in V$ vektorra $m_{\mathcal{A}}(\mathcal{A})\mathbf{u} = \mathbf{0}$. Ha egy rögzített $\mathbf{u}$ vektort tekintünk, akkor ehhez

általában már a minimálpolinomnál alacsonyabb fokú $f \in T[x]$ polinomok is találhatók, amelyekre $f(\mathcal{A})\mathbf{u} = \mathbf{0}$.

6.5.1 Definíció

Az $\mathbf{u}$ vektornak az $\mathcal{A}$ szerinti *rend*je az a legalacsonyabb fokú h (nem nulla) *polinom*, amelyre $h(\mathcal{A})\mathbf{u} = \mathbf{0}$. ♣

Az $\mathbf{u}$ vektor $\mathcal{A}$ szerinti rendjét $o_{\mathcal{A}}(\mathbf{u})$-val jelöljük. (Az o a latin *ordo*=rend szó kezdőbetűjéből származik). Ha egyértelmű, hogy melyik transzformációról van szó, akkor a transzformációt jelző index el is hagyható: $o(\mathbf{u})$.

Példák: A nullvektor az egyetlen, amelynek a rendje az 1 (vagy bármely nem nulla konstans) polinom, a magtér nem nulla elemeinek a rendje x. A rend akkor és csak akkor elsőfokú, ha a vektor sajátvektor.

A rend számos hasonló tulajdonsággal rendelkezik, mint a minimálpolinom. Ezeket az alábbi tételben foglaljuk össze.

6.5.2 Tétel

Bármely vektornak létezik rendje. Ez konstans szorzó erejéig egyértelműen meghatározott. A rend foka legfeljebb $n(= \dim V)$. $g(\mathcal{A})\mathbf{u} = \mathbf{0} \iff \iff o_{\mathcal{A}}(\mathbf{u}) \mid g$. ♣

A bizonyítás a 6.3.2 és 6.3.3 tételekéhez analóg módon történhet, lásd a 6.5.2 feladatot.

A 6.5.2 Tétel utolsó részéből azonnal adódik, hogy a rend mindig osztója a minimálpolinomnak. A következő állítás arra vonatkozik, hogy alkalmas vektorok rendjéből hogyan kaphatjuk meg a minimálpolinomot.

6.5.3 Tétel

Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_s$ tetszőleges generátorrendszer V-ben. Ekkor $m_{\mathcal{A}}$ az $o_{\mathcal{A}}(\mathbf{u}_i)$ polinomok legkisebb közös többszöröse. ♣

Bizonyítás: Legyen $h_i = o_{\mathcal{A}}(\mathbf{u}_i)$ és a H polinom ezek legkisebb közös többszöröse, $H = [h_1, \ldots, h_s]$. Mivel $h_i \mid m_{\mathcal{A}}$, ezért $H \mid m_{\mathcal{A}}$ is teljesül. A fordított irányú oszthatósághoz azt kell belátnunk, hogy $H(\mathcal{A}) = \mathcal{O}$. Mivel $h_i \mid H$, ezért $H(\mathcal{A})\mathbf{u}_i = \mathbf{0}$. Továbbá a feltétel szerint bármely $\mathbf{v} \in V$ vektor előáll az $\mathbf{u}_i$ vektorok $\mathbf{v} = \sum_{i=1}^{s} \lambda_i \mathbf{u}_i$ lineáris kombinációjaként. Így $H(\mathcal{A})\mathbf{v} = = \sum_{i=1}^{s} \lambda_i H(\mathcal{A})\mathbf{u}_i = \mathbf{0}$, tehát valóban $H(\mathcal{A}) = \mathcal{O}$. ■

A következő tétel megmutatja, hogy a rendből alkalmas invariáns alterek dimenziója is leolvasható:

6.5.4 Tétel
Az $\mathbf{u}$ vektor és az $\mathcal{A}$ transzformáció által generált $\langle \mathbf{u}, \mathcal{A} \rangle$ altér dimenziója megegyezik az $\mathbf{u}$ rendjének a fokával:

$$\dim\langle \mathbf{u}, \mathcal{A} \rangle = \deg o_{\mathcal{A}}(\mathbf{u})\,. \ \clubsuit$$

Bizonyítás: A nullvektorra az állítás igaz. Legyen $\mathbf{u} \neq \mathbf{0}$ és $o_{\mathcal{A}}(\mathbf{u}) = h = x^k + \alpha_{k-1}x^{k-1} + \ldots + \alpha_0$. Azt kell belátnunk, hogy az $\langle \mathbf{u}, \mathcal{A} \rangle$ altér k-dimenziós. Ehhez megmutatjuk, hogy az $\mathbf{u}, \mathcal{A}\mathbf{u}, \ldots, \mathcal{A}^{k-1}\mathbf{u}$ vektorok bázist alkotnak az $\langle \mathbf{u}, \mathcal{A} \rangle$ altérben.

A lineáris függetlenség igazolásához indirekt okoskodunk; tegyük fel, hogy létezne valamilyen nem triviális $\beta_0\mathbf{u} + \beta_1\mathcal{A}\mathbf{u} + \ldots + \beta_{k-1}\mathcal{A}^{k-1}\mathbf{u} = \mathbf{0}$ lineáris kombináció. Ekkor az $f = \beta_0 + \beta_1 x + \ldots + \beta_{k-1}x^{k-1}$ polinomra $f(\mathcal{A})\mathbf{u} = \mathbf{0}$. Ez azonban ellentmond annak, hogy az $\mathbf{u}$ vektor rendje k-adfokú.

Most belátjuk, hogy a kérdéses vektorok generálják az $\langle \mathbf{u}, \mathcal{A} \rangle$ alteret. Ehhez azt kell igazolnunk, hogy minden $\mathcal{A}^i\mathbf{u}$ vektor előáll az $\mathbf{u}, \mathcal{A}\mathbf{u}, \ldots, \mathcal{A}^{k-1}\mathbf{u}$ vektorok lineáris kombinációjaként. Az $i < k$ kitevőkre ez nyilvánvaló, $i = k$-ra pedig $h(\mathcal{A})\mathbf{u} = \mathbf{0}$ átrendezéséből adódik:

$$\mathcal{A}^k\mathbf{u} = -\alpha_0\mathbf{u} - \alpha_1(\mathcal{A}\mathbf{u}) - \ldots - \alpha_{k-1}(\mathcal{A}^{k-1}\mathbf{u})\,. \tag{6.5.1}$$

Nézzük most az $i = k+1$ kitevőt. A (6.5.1) egyenlőségre az $\mathcal{A}$ transzformációt alkalmazva azt kapjuk, hogy $\mathcal{A}^{k+1}\mathbf{u}$ kifejezhető az $\mathcal{A}\mathbf{u}, \ldots, \mathcal{A}^k\mathbf{u}$ vektorok lineáris kombinációjaként. Ha itt $\mathcal{A}^k\mathbf{u}$ helyére a (6.5.1)-beli előállítást beírjuk, akkor az $\mathcal{A}^{k+1}\mathbf{u}$ vektort a kívánt módon előállítottuk az $\mathbf{u}, \mathcal{A}\mathbf{u}, \ldots, \mathcal{A}^{k-1}\mathbf{u}$ vektorok lineáris kombinációjaként. Ugyanígy haladhatunk tovább magasabb kitevőkre is (pl. teljes indukcióval).

Az $i \geq k$ kitevőkre vonatkozóan úgy is okoskodhatunk, hogy x^i helyett annak a renddel való osztási maradékéba helyettesítjük be az $\mathcal{A}$ transzformációt. ■

Az előző tétel segítségével bizonyos dimenziójú invariáns alterek létezését is garantálni tudjuk:

6.5.5 Tétel

Ha a minimálpolinomnak van (T feletti) r-edfokú irreducibilis tényezője, akkor $\mathcal{A}$-nak van r-dimenziós invariáns altere. ♣

Megjegyzések: 1. Az $r = 1$ speciális esetben a 6.3.4 Tétel egyik felét kapjuk, a bizonyítás is az ottanihoz hasonlóan történik.

2. Később látni fogjuk (6.5.8 Tétel), hogy a 6.5.5 Tételben az irreducibilitás feltétele elhagyható.

Bizonyítás: Legyen $m_{\mathcal{A}} = hg$, ahol h irreducibilis és $\deg h = r$. Azt fogjuk megmutatni, hogy van olyan $\mathbf{u} \neq \mathbf{0}$ vektor, amelyre $o_{\mathcal{A}}(\mathbf{u}) = h$. Ekkor a 6.5.4 Tétel szerint az $\langle \mathbf{u}, \mathcal{A} \rangle$ invariáns altér dimenziója éppen $\deg h = r$ lesz.

Mivel $\deg g < \deg m_{\mathcal{A}}$, ezért $g(\mathcal{A}) \neq \mathcal{O}$, azaz $\operatorname{Im} g(\mathcal{A}) \neq \mathbf{0}$. Az $\mathcal{A}$ transzformációt $m_{\mathcal{A}}$-ba behelyettesítve $\mathcal{O} = m_{\mathcal{A}}(\mathcal{A}) = h(\mathcal{A})g(\mathcal{A})$ adódik. Ennélfogva $\operatorname{Ker} h(\mathcal{A}) \supseteq \operatorname{Im} g(\mathcal{A})$. Legyen $\mathbf{u}$ tetszőleges nem nulla vektor $\operatorname{Im} g(\mathcal{A})$-ban. Ekkor $h(\mathcal{A})\mathbf{u} = \mathbf{0}$, tehát $o_{\mathcal{A}}(u) \mid h$. Mivel h irreducibilis és $\mathbf{u} \neq \mathbf{0}$, így csak $o_{\mathcal{A}}(\mathbf{u}) = h$ lehetséges. ■

Most bebizonyítjuk, hogy maga a minimálpolinom is szerepel a rendek között.

6.5.6 Tétel

Minden transzformációnál létezik olyan vektor, amelynek a rendje a minimálpolinom. ♣

Bizonyítás: A 6.5.3 Tétel szerint a minimálpolinom egy (tetszőleges) generátorrendszer elemei rendjeinek a legkisebb közös többszöröse. Így elég az alábbi lemmát igazolnunk:

6.5.7 Lemma

Ha a $h_1, \ldots, h_s$ polinomok az $\mathbf{u}_1, \ldots, \mathbf{u}_s$ elemek rendjei, akkor a h_i polinomok legkisebb közös többszöröse is valamely $\mathbf{u}$ vektor rendje. ♣

A lemma bizonyítása több lépésben történik. A h_i polinomok $[h_1, h_2, \ldots, h_s]$ legkisebb közös többszörösét H-val fogjuk jelölni.

(i) Két relatív prím polinom esetén:

$$(h_1, h_2) = 1 \Longrightarrow o(\mathbf{u}_1 + \mathbf{u}_2) = h_1 h_2 = H\,.$$

Legyen $\mathbf{u} = \mathbf{u}_1 + \mathbf{u}_2$, és jelöljük $o(\mathbf{u})$-t K-val. Megmutatjuk, hogy $H = K$. Először a $K \mid H$ oszthatóságot igazoljuk. Ez azzal egyenértékű, hogy

$H(\mathcal{A})\mathbf{u} = \mathbf{0}$. Valóban, $o(\mathbf{u}_i) \mid H$ miatt

$$H(\mathcal{A})\mathbf{u} = H(\mathcal{A})(\mathbf{u}_1 + \mathbf{u}_2) = H(\mathcal{A})\mathbf{u}_1 + H(\mathcal{A})\mathbf{u}_2 = \mathbf{0} + \mathbf{0} = \mathbf{0}\,.$$

A másik irányú, $H \mid K$ oszthatósághoz $h_i \mid K$-t kell igazolni ($i = 1, 2$). Mivel

$$(Kh_1)(\mathcal{A})\mathbf{u}_2 = (Kh_1)(\mathcal{A})\mathbf{u} - (Kh_1)(\mathcal{A})\mathbf{u}_1 = \mathbf{0} - \mathbf{0} = \mathbf{0}\,,$$

ezért $o(\mathbf{u}_2) = h_2 \mid Kh_1$, amiből $(h_1, h_2) = 1$ miatt $h_2 \mid K$ következik. Ugyanígy adódik $h_1 \mid K$ is.

(ii) Páronként relatív prím polinomok esetén:

$$(h_i, h_j) = 1, \quad 1 \le i < j \le s \Longrightarrow o(\mathbf{u}_1 + \ldots + \mathbf{u}_s) = h_1 \ldots h_s = H\,.$$

Ez (i)-ből teljes indukcióval adódik.

(iii) Egy rend minden osztója is rend: ha $f = gh$ és $f = o(\mathbf{v})$, akkor $g = o[h(\mathcal{A})\mathbf{v}]$.
Ennek igazolását a 6.5.5 feladatban tűztük ki.

(iv) Ha két tetszőleges h_1 és h_2 polinom rend, akkor a legkisebb közös többszörösük is rend.

Írjuk fel h_1 és h_2 „kanonikus alakját", azaz bontsuk fel mindkét polinomot irreducibilis tényezők hatványainak a szorzatára:

$$h_1 = \alpha_1 p_1^{k_{11}} \ldots p_r^{k_{r1}}\,,$$
$$h_2 = \alpha_2 p_1^{k_{12}} \ldots p_r^{k_{r2}}\,,$$

ahol α_i konstans, a p_j polinomok páronként nem konstansszoros irreducibilis polinomok és a k_{ji} kitevők nemnegatív egészek. Ekkor a $H = [h_1, h_2]$ legkisebb közös többszörös kanonikus alakja

$$H = p_1^{k_{13}} \ldots p_r^{k_{r3}}\,,$$

ahol $k_{j3} = \max(k_{j1}, k_{j2})$. Mivel $p_j^{k_{j3}}$ bármely j-re osztója h_1-nek vagy h_2-nek, ezért (iii) alapján $p_j^{k_{j3}}$ is rend. Továbbá a $p_j^{k_{j3}}$ tényezők páronként relatív prímek, így (ii) szerint a szorzatuk, azaz H is rend.

(v) A tetszőleges számú polinomra vonatkozó állítás (iv)-ből teljes indukcióval következik. ■

A 6.5.6 Tételnek számos fontos következménye van. A 6.3 pontban említettük, hogy a minimálpolinom foka legfeljebb a tér dimenziója. Ez most azonnal adódik abból, hogy a rend foka nem lehet nagyobb a dimenziónál (lásd a 6.5.2 Tételt). Egy másik következmény a 6.5.5 Tétel általánosítása:

6.5.8 Tétel
Ha a minimálpolinomnak van r-edfokú osztója, akkor $\mathcal{A}$-nak van r-dimenziós invariáns altere. ♣

Bizonyítás: A 6.5.6 Tétel szerint a minimálpolinom is rend. A 6.5.7 Lemma bizonyításában szereplő (iii) állítás(=6.5.5 feladat) alapján ekkor a minimálpolinom minden osztója is rend. Végül a 6.5.4 Tétel biztosítja, hogy minden rend foka egyben valamely invariáns altér dimenziója is. ■

Feladatok

6.5.1 Hogyan kapjuk meg $\mathbf{u}$ rendjéből (a) $\lambda\mathbf{u}$; (b) $\mathcal{A}\mathbf{u}$; (c) $f(\mathcal{A})\mathbf{u}$ rendjét, ahol f tetszőleges polinom?

6.5.2 Bizonyítsuk be a 6.5.2 Tétel állításait.

6.5.3 Tekintsük $\mathcal{A}$ megszorítását az $U = \langle \mathbf{u}, \mathcal{A}\rangle$ (invariáns) altérre. Mi lesz a megszorított ($\operatorname{Hom} U$-beli) transzformáció minimálpolinomja?

6.5.4 Bizonyítsuk be, hogy $o_{\mathcal{A}}(\mathbf{u})$-nak akkor és csak akkor van gyöke (T-ben), ha $\mathcal{A}$-nak van az $\langle \mathbf{u}, \mathcal{A}\rangle$ altérbe eső sajátvektora.

6.5.5 Igazoljuk a 6.5.7 Lemma bizonyításában szereplő (iii) állítást: ha az f polinom egy $\mathbf{v}$ vektor rendje, akkor f minden osztója is egy alkalmas vektor rendje.

6.5.6 Melyek igazak az alábbi állítások közül?

(a) Ha $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \mathbf{v}, \mathcal{A}\rangle$, akkor $\mathbf{u}$ és $\mathbf{v}$ rendje megegyezik.

(b) Ha $\mathbf{u}$ és $\mathbf{v}$ rendje megegyezik, akkor $\langle \mathbf{u}, \mathcal{A}\rangle = \langle \mathbf{v}, \mathcal{A}\rangle$.

(c) Ha $o(\mathbf{u})$ és $o(\mathbf{v})$ relatív prímek, és egyik sem konstans, akkor $\mathbf{u}$ és $\mathbf{v}$ lineárisan független.

(d) Ha $\mathbf{u}$ és $\mathbf{v}$ lineárisan független, akkor $o(\mathbf{u})$ és $o(\mathbf{v})$ relatív prímek.

(e) Ha $\mathbf{u}_1, \ldots, \mathbf{u}_s$ lineárisan független, akkor $o(\mathbf{u}_1 + \ldots + \mathbf{u}_s) = [o(\mathbf{u}_1), \ldots, o(\mathbf{u}_s)]$.

6.5.7 Bizonyítsuk be, hogy bármely vektor rendjének a foka legfeljebb eggyel több, mint a képtér dimenziója. Mi következik ebből a minimálpolinom fokszámára?

*6.5.8 Legyen $\dim V = n$, és tegyük fel, hogy $\mathcal{A}$-nak n különböző sajátértéke van. Bizonyítsuk be, hogy ekkor $\mathcal{A}$ invariáns altereinek a száma pontosan 2^n.

6.5.9 Adjunk új bizonyítást arra, hogy bármely transzformációnak legalább annyi invariáns altere van, mint ahány páronként nem-egységszeres osztója van a minimálpolinomjának.

6.5.10 Mutassuk meg, hogy

$$\frac{\big[o(\mathbf{u}), o(\mathbf{v})\big]}{\big(o(\mathbf{u}), o(\mathbf{v})\big)} \,\Big|\, o(\mathbf{u}+\mathbf{v}) \,\Big|\, \big[o(\mathbf{u}), o(\mathbf{v})\big] .$$

Hogyan kapcsolódik ez a 6.5.7 Lemma bizonyításában szereplő (i) állításhoz?

6.5.11 Milyen kapcsolatban áll $o_{\lambda\mathcal{A}}(\mathbf{u})$, illetve $o_{\mathcal{A}^2}(\mathbf{u})$ fokszáma $o_{\mathcal{A}}(\mathbf{u})$ fokával?

6.5.12 Legyen $\mathcal{A}, \mathcal{B} \in \operatorname{Hom} V$ és tegyük fel, hogy minden $\mathbf{v} \in V$ vektorra $o_{\mathcal{A}}(\mathbf{v}) = o_{\mathcal{B}}(\mathbf{v})$.

(a) Bizonyítsuk be, hogy $\mathcal{A}$ és $\mathcal{B}$ sajátértékei és sajátvektorai megegyeznek, és minimálpolinomjuk is azonos.

(b) Ha $\mathcal{A}$-nak létezik sajátvektorokból álló bázisa, akkor $\mathcal{A} = \mathcal{B}$.

(c) Mutassunk példát $\mathbf{R}$, illetve $\mathbf{C}$ felett, amikor $\mathcal{A} \neq \mathcal{B}$.

6.6. Transzformációk szép mátrixa

Egy transzformáció mátrixa annál „szebb”, minél közelebb áll a diagonális alakhoz, azaz a(z esetleges) nem nulla elemek minél inkább a főátló körül koncentrálódnak, pl. az ilyen mátrixokat (viszonylag) kényelmesen lehet hatványozni.

Láttuk (6.1.4 Tétel), hogy egy transzformációnak akkor és csak akkor van diagonális mátrixa, ha létezik sajátvektorokból álló bázisa. Ezt úgy is interpretálhatjuk, hogy a tér ekkor egydimenziós invariáns altereinek a direkt összege.

Az alábbiakban először megnézzük, milyen mátrixot eredményez, ha a bázist két invariáns altérből vesszük (azaz a tér két invariáns alterének direkt összege), majd megvizsgáljuk, hogyan kaphatunk ilyen invariáns altereket. Végül megemlítjük, hogy speciálisan a komplex test felett milyen lesz egy tetszőleges transzformáció „lehető legszebb mátrixa” (az ún. Jordan-féle normálalak).

6.6.1 Tétel

Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ a V vektortér egy olyan bázisa, hogy $U_1 = \langle \mathbf{b}_1, \ldots, \mathbf{b}_k \rangle$ és $U_2 = \langle \mathbf{b}_{k+1}, \ldots, \mathbf{b}_n \rangle$ az $\mathcal{A}$ transzformáció invariáns alterei. Ekkor az $[\mathcal{A}]_b$ mátrixban a bal felső $k \times k$-as és a jobb alsó $(n-k) \times (n-k)$-as négyzet kivételével minden elem nulla. Azaz a mátrix $\begin{pmatrix} A_1 & 0 \\ 0 & A_2 \end{pmatrix}$ alakú, ahol A_1 egy $k \times k$-as, A_2 egy $(n-k) \times (n-k)$-as mátrix, a bal alsó $(n-k) \times k$-as és a jobb felső $k \times (n-k)$-as rész pedig nullmátrix. ♣

A 6.6.1 Tétel azonnal következik abból, hogy U_1 és U_2 invariáns alterek. Megjegyezzük, hogy az A_i mátrix $(i = 1, 2)$ éppen az $\mathcal{A}$ transzformáció U_i-re történő megszorításának a mátrixa (a megfelelő bázisban). A fenti felbontást a jövőben röviden úgy fogjuk mondani, hogy az A mátrixot az A_1 és A_2 *blokk*okra bontottuk fel, illetve az A mátrix az A_1 és A_2 mátrixok *direkt összeg*e.

6.6.2 Tétel

Tegyük fel, hogy $m_{\mathcal{A}} = g_1 g_2$, ahol $(g_1\,,\, g_2) = 1$. Ekkor $V = U_1 \oplus U_2$, ahol az U_i-k az $\mathcal{A}$-nak invariáns alterei, és az $\mathcal{A}$ transzformáció U_i-re történő megszorításának a minimálpolinomja éppen g_i. ♣

Bizonyítás: Megmutatjuk, hogy az $U_i = \operatorname{Ker} g_i(\mathcal{A})$ választás megfelel.

(a) Ezek az U_i-k a 6.4.9a feladat szerint valóban invariáns alterek.

(b) $V = U_1 \oplus U_2$ igazolásához azt kell belátnunk, hogy

$$\text{(b1)}\ \ U_1 \cap U_2 = \mathbf{0} \quad \text{és} \quad \text{(b2)}\ \ \langle U_1, U_2 \rangle = V\,.$$

(b1) Tegyük fel, hogy $\mathbf{u} \in U_1 \cap U_2$, azaz $g_i(\mathcal{A})\mathbf{u} = \mathbf{0}$, $i = 1, 2$. Ez azt jelenti, hogy $o_{\mathcal{A}}(\mathbf{u}) \,|\, g_i$, tehát $o_{\mathcal{A}}(\mathbf{u}) \,|\, (g_1, g_2) = 1$, azaz $\mathbf{u} = \mathbf{0}$.

(b2) Mivel $(g_1, g_2) = 1$, így alkalmas h_1 és h_2 polinomokkal $1 = g_1 h_1 + g_2 h_2$. Ezért $\mathcal{E} = g_1(\mathcal{A})h_1(\mathcal{A}) + g_2(\mathcal{A})h_2(\mathcal{A})$. Ezt tetszőleges $\mathbf{v}$ vektorra alkalmazva $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$ adódik, ahol $\mathbf{v}_i = g_i(\mathcal{A})h_i(\mathcal{A})\mathbf{v}$. Itt $\mathbf{v}_1 \in U_2$, hiszen

$$g_2(\mathcal{A})\mathbf{v}_1 = (g_2 g_1 h_1)(\mathcal{A})\mathbf{v} = (m_{\mathcal{A}} h_1)(\mathcal{A})\mathbf{v} = \mathbf{0}\,.$$

Ugyanígy adódik $\mathbf{v}_2 \in U_1$ is.

(c) Végül legyen az $\mathcal{A}$ transzformáció U_i-re történő megszorításának a minimálpolinomja r_i, be kell látnunk, hogy $r_i = g_i$. Mivel $U_1 = \operatorname{Ker} g_1(\mathcal{A})$, ezért minden $\mathbf{u} \in U_1$-re $g_1(\mathcal{A})\mathbf{u} = \mathbf{0}$, tehát $r_1 \,|\, g_1$.

A másik irányú, $g_1 \,|\, r_1$ oszthatóság igazolásához tekintsük egy tetszőleges $\mathbf{v} \in V$ vektorra a (b2) szerinti $\mathbf{v} = \mathbf{v}_1 + \mathbf{v}_2$ felbontást, ahol $\mathbf{v}_1 \in U_2$, $\mathbf{v}_2 \in U_1$. Láttuk, hogy $g_2(\mathcal{A})\mathbf{v}_1 = \mathbf{0}$, továbbá r_1 definíciója alapján $r_1(\mathcal{A})\mathbf{v}_2 = \mathbf{0}$. Így az $s = r_1 g_2$ polinomra $s(\mathcal{A})\mathbf{v} = s(\mathcal{A})\mathbf{v}_1 + s(\mathcal{A})\mathbf{v}_2 = \mathbf{0}$ minden $\mathbf{v} \in V$-re. Ez azt jelenti, hogy $m_{\mathcal{A}} = g_1 g_2 \,|\, s = r_1 g_2$, azaz $g_1 \,|\, r_1$.

Ezzel igazoltuk, hogy $r_1 = g_1$, és ugyanígy kapjuk az $r_2 = g_2$ egyenlőséget is. ■

A 6.6.2 Tételből teljes indukcióval kapjuk, hogy ha a minimálpolinomot (páronként nem-egységszeres) irreducibilis tényezők hatványainak a szorzatára bontjuk, $m_{\mathcal{A}} = p_1^{k_1} \dots p_t^{k_t}$, akkor a V vektortér olyan U_i invariáns alterek direkt összege, ahol az $\mathcal{A}$ transzformáció U_i-ra történő $\mathcal{A}_i$ megszorításának a minimálpolinomja éppen $p_i^{k_i}$. A 6.6.1 Tétel szerint így $\mathcal{A}$-nak az U_i alterek szerinti bázisban vett mátrixa olyan A_i blokkokra bomlik, ahol $A_i = [\mathcal{A}_i]$.

Mindezek alapján elég olyan transzformációk „szép” mátrixát keresni, amelyek minimálpolinomja egy irreducibilis polinom hatványa. Ez általában igen nehéz feladat. Speciálisan a komplex test felett egyszerűbb a helyzet, hiszen itt egy irreducibilis polinom csak elsőfokú lehet. Erre vonatkozik az alábbi tétel:

6.6.3 Tétel

Legyen $\mathcal{B} \in \operatorname{Hom} V$, $m_{\mathcal{B}} = (x - \lambda)^k$. Ekkor alkalmas bázisban $\mathcal{B}$ mátrixa olyan B_j blokkokból áll (lehet, hogy csak egyből), ahol

(i) a B_j-k méretének a maximuma $k \times k$, azaz mindegyik B_j legfeljebb $k \times k$-as, de van közöttük pontosan $k \times k$-as is,

és

(ii) mindegyik B_j-ben a főátló minden eleme λ, közvetlenül a főátló alatt minden elem 1, az összes többi elem pedig 0.

(Egy blokk 1×1-es is lehet, ilyenkor egyetlen λ-ból áll.)

Azaz

$$[\mathcal{B}] = \begin{pmatrix} B_1 & 0 & \dots & 0 \\ 0 & B_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & B_r \end{pmatrix}, \qquad B_j = \begin{pmatrix} \lambda & 0 & 0 & \dots & 0 \\ 1 & \lambda & 0 & \dots & 0 \\ 0 & 1 & \lambda & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & \lambda \end{pmatrix},$$

ahol a B_j mérete $q_j \times q_j$, $\sum_{j=1}^{r} q_j = \dim V$ és $\max_{1 \le j \le r} q_j = k$. ♣

Bizonyítás: Legyen $\mathcal{C} = \mathcal{B} - \lambda\mathcal{E}$, ekkor $\mathcal{C}$ minimálpolinomja x^k, és azt kell igazolni, hogy alkalmas bázisban $\mathcal{C}$ mátrixa olyan C_j blokkokból áll, amelyek méretének maximuma k, és minden C_j-ben közvetlenül a főátló alatt csupa 1-es áll, az összes többi elem pedig 0 (beleértve a főátlót is).

Ez azt jelenti, hogy egy q méretű blokkhoz tartozó bázis

$$\mathbf{u}_1, \quad \mathbf{u}_2 = \mathcal{C}\mathbf{u}_1, \quad \mathbf{u}_3 = \mathcal{C}\mathbf{u}_2 = \mathcal{C}^2\mathbf{u}_1, \quad \ldots, \quad \mathbf{u}_q = \mathcal{C}\mathbf{u}_{q-1} = \mathcal{C}^{q-1}\mathbf{u}_1 \tag{6.6.1a}$$

alakú, ahol

$$\mathcal{C}\mathbf{u}_q = \mathcal{C}^q\mathbf{u}_1 = \mathbf{0}. \tag{6.6.2a}$$

Más szóval, az adott blokkhoz tartozó q-dimenziós invariáns altér $\langle \mathbf{u}_1, \mathcal{C}\rangle$, ahol q az $\mathbf{u}_1$ vektor $\mathcal{C}$ szerinti rendjének a foka.

Mindezek alapján bevezetjük a következő definíciót:

6.6.4 Definíció

Legyen $\mathcal{C} \in \operatorname{Hom} V$, $m_{\mathcal{C}} = x^k$. Egy x^q rendű $\mathbf{u} \in V$ vektor *pályája* az

$$\mathbf{u}, \quad \mathcal{C}\mathbf{u}, \quad \mathcal{C}^2\mathbf{u}, \quad \ldots, \quad \mathcal{C}^{q-1}\mathbf{u} \tag{6.6.1b}$$

vektorok halmaza, ahol tehát q a legkisebb olyan pozitív egész, amelyre

$$\mathcal{C}^q\mathbf{u} = \mathbf{0}. \tag{6.6.2b}$$

A q szám a pálya *hossza*. ♣

A 6.5.4 Tételből adódik, hogy a pályában szereplő vektorok lineárisan függetlenek.

Az előzőek szerint a 6.6.3 Tétel az alábbi lemmával ekvivalens:

6.6.5 Lemma

Legyen $\mathcal{C} \in \operatorname{Hom} V$, $m_{\mathcal{C}} = x^k$. Ekkor V-nek létezik pályákból álló bázisa, amelyek hosszának maximuma k. ♣

A 6.6.5 lemmára (azaz a fenti módon átfogalmazott 6.6.3 Tételre) két bizonyítást adunk.

Első bizonyítás: A minimálpolinom foka szerinti teljes indukcióval bizonyítunk. Ha $k = 1$, akkor $\mathcal{C} = \mathcal{O}$, azaz minden $\mathbf{u}$ vektorra $\mathcal{C}\mathbf{u} = \mathbf{0}$. Ez azt jelenti, hogy minden nem nulla vektor pályája 1 hosszú, vagyis tetszőleges bázis megfelel a feltételeknek.

Tegyük fel, hogy az állítás igaz a k-nál kisebb pozitív egészekre és legyen $\mathcal{C} \in \operatorname{Hom} V$, $m_{\mathcal{C}} = x^k$. Tekintsük a $\mathcal{C}$ transzformáció $\mathcal{C}'$ megszorítását a $W = \operatorname{Im} \mathcal{C}$ invariáns altérre. A $\mathcal{C}'$ transzformáció minimálpolinomja x^{k-1}, ugyanis egyrészt a képtér bármely $\mathbf{w} = \mathcal{C}\mathbf{u}$ vektorára $\mathcal{C}^{k-1}\mathbf{w} = \mathcal{C}^k\mathbf{u} = \mathbf{0}$, másrészt ha minden képtérbeli $\mathbf{w}$-re $\mathcal{C}^j\mathbf{w} = \mathbf{0}$, akkor minden $\mathbf{u} \in V$-re $\mathcal{C}^{j+1}\mathbf{u} = \mathcal{C}^j(\mathcal{C}\mathbf{u}) = \mathbf{0}$, tehát $j \geq k-1$.

Az indukciós feltétel szerint W-nek létezik pályákból álló bázisa, amelyek hosszának maximuma $k-1$. Legyen az i-edik pálya induló eleme $\mathbf{w}_i = \mathcal{C}\mathbf{v}_i$ és a hossza q_i, $i = 1, 2, \ldots, r$, ahol $q_1 = k-1$. Tekintsük minden i-re V-ben a $\mathbf{v}_i$ vektor P_i pályáját, azaz a $\mathbf{w}_i$ vektor pályájának $\mathbf{v}_i$-vel való kibővítését, a P_i pálya hossza tehát q_i+1. Legyen a P_i pályákban szereplő vektorok által V-ben együttesen generált altér U, $H = U \cap \operatorname{Ker} \mathcal{C}$ és Z a H altér egy $\operatorname{Ker} \mathcal{C}$-beli H_1 direkt kiegészítőjének tetszőleges bázisa. Megmutatjuk, hogy

(i) a P_i pályák egyesítése bázist alkot U-ban;
(ii) a P_i pályák $\mathcal{C}^{q_i}\mathbf{v}_i$ utolsó elemei bázist alkotnak H-ban;
(iii) a P_i pályák és Z egyesítése bázist alkot V-ben.

Mivel Z elemei a magtérben vannak, ezért 1 hosszúságú pályákat jelentenek, és így V-nek a (iii)-beli bázisa pályákból áll, ami éppen a bizonyítandó állítás.

Rátérve (i) igazolására, azt kell megmutatnunk, hogy a P_i pályák egyesítésében szereplő vektorok lineárisan függetlenek, azaz

$$\sum_{i=1}^{r} \sum_{j=0}^{q_i} \lambda_{ij} \mathcal{C}^j \mathbf{v}_i = \mathbf{0} \tag{6.6.3}$$

esetén minden $\lambda_{ij} = 0$. A (6.6.3) bal oldalán szereplő lineáris kombinációt bontsuk két részre: álljon $\mathbf{s}_1$ azokból a tagokból, ahol $j = q_i$, az $\mathbf{s}_2$ pedig azokból, ahol $j < q_i$ (tehát $\mathbf{s}_1$ a pályák utolsó elemeinek a lineáris kombinációja, $\mathbf{s}_2$ pedig a többié, és $\mathbf{s}_1 + \mathbf{s}_2 = \mathbf{0}$). Alkalmazzuk (6.6.3)-ra a $\mathcal{C}$ transzformációt. Ekkor $\mathcal{C}\mathbf{s}_1 = \mathbf{0}$. Az indukciós feltevés szerint az $\mathbf{s}_1$-ben szereplő vektorok lineárisan függetlenek, tehát itt minden λ_{ij} együttható 0. Továbbá $\mathbf{0} = \mathcal{C}\mathbf{s}_2$ a $\mathbf{v}_i$-k helyett a $\mathcal{C}\mathbf{v}_i = \mathbf{w}_i$-kel képzett vektorok megfelelő lineáris kombinációja. Az ebben szereplő vektorok is lineárisan függetlenek az indukciós feltevés szerint, tehát minden itteni λ_{ij} is 0. Ezzel (i)-et beláttuk.

Továbbmenve (ii)-re, azt vizsgáljuk, U mely elemei vannak a magtérben. Tudjuk, hogy (i) alapján minden $\mathbf{v} \in U$ egyértelműen felírható a (6.6.3) bal oldalán szereplő $\mathbf{s}_1 + \mathbf{s}_2$ alakban. Így $\mathcal{C}\mathbf{u} = \mathbf{0}$ azt jelenti, hogy $\mathcal{C}\mathbf{s}_1 + \mathcal{C}\mathbf{s}_2 = \mathbf{0} + \mathcal{C}\mathbf{s}_2 = \mathbf{0}$. Ahogy (i)-ben is láttuk, a $\mathcal{C}\mathbf{s}_2$-beli vektorok függetlensége miatt ez azzal ekvivalens, hogy minden $\mathbf{s}_2$-beli $\lambda_{ij} = 0$, tehát $\mathbf{s}_2 = \mathbf{0}$, és így $\mathbf{u} = \mathbf{s}_1$. Mivel az $\mathbf{s}_1$-beli vektorok is lineárisan függetlenek, ezért bázist alkotnak az általuk generált H altérben.

Végül, (iii) bizonyításához vegyük észre, hogy (ii) alapján $U \cap H_1 = \mathbf{0}$, tehát a (iii)-ban megadott vektorok lineárisan függetlenek. Mivel számuk

$$\dim U + \dim H_1 = \dim \operatorname{Im} \mathcal{C} + r + \dim H_1 = \dim \operatorname{Im} \mathcal{C} + \dim \operatorname{Ker} \mathcal{C} = \dim V,$$

így bázist alkotnak V-ben. ■

Második bizonyítás: Ez a szellemes gondolatmenet Terence Tao-tól származik. Nyilván létezik V-nek pályákból álló generátorrendszere, például V egy tetszőleges bázisából induló pályák egyesítése az. Megmutatjuk, hogy ha egy ilyen generátorrendszer elemei lineárisan összefüggők, akkor alkalmas változtatással rövidebb összhosszúságú pályákból álló generátorrendszert is képezhetünk. Ezt véges sokszor ismételve lineárisan független generátorrendszerhez, azaz bázishoz kell jutnunk.

A könnyebb érthetőség kedvéért minden lépést egy konkrét példán keresztül is illusztrálunk.

Vegyük a generátorrendszer elemeinek egy olyan nem triviális lineáris kombinációját, ami $\mathbf{0}$, és csak a nem 0 együtthatójú tagokat tartsuk meg. A példánkban a pályák hossza legyen rendre 3, 4, 5 és 5, és mondjuk

$$6\mathbf{v}_1 + 7\mathcal{C}^2\mathbf{v}_1 + 8\mathcal{C}\mathbf{v}_2 + 9\mathcal{C}^2\mathbf{v}_2 + 10\mathcal{C}^3\mathbf{v}_3 + 11\mathcal{C}^2\mathbf{v}_4 = \mathbf{0}.$$

Alkalmazzuk a lineáris kombinációra $\mathcal{C}$ egy olyan hatványát, hogy minden pályából legfeljebb egy tag maradjon meg (a többiek már a $\mathbf{0}$-ba mennek át), a példánkban ez $\mathcal{C}^2$, és az eredmény

$$6\mathcal{C}^2\mathbf{v}_1 + 8\mathcal{C}^3\mathbf{v}_2 + 11\mathcal{C}^4\mathbf{v}_4 = \mathbf{0}.$$

Vegyük a legkisebb m egészt, ami $\mathcal{C}$ kitevőjeként itt előfordul, és írjuk át a lineáris kombinációt $\mathcal{C}^m\mathbf{v} = \mathbf{0}$ alakba. A példánkban $m = 2$ és

$$\mathcal{C}^2(6\mathbf{v}_1 + 8\mathcal{C}\mathbf{v}_2 + 11\mathcal{C}^2\mathbf{v}_4) = \mathbf{0},$$

tehát

$$\mathbf{v} = 6\mathbf{v}_1 + 8\mathcal{C}\mathbf{v}_2 + 11\mathcal{C}^2\mathbf{v}_4.$$

Mivel $\mathcal{C}$-nek a lehető legnagyobb hatványát emeltük ki, ezért a $\mathbf{v}$ vektorban legalább egy $\mathbf{v}_i$ „személyesen" szerepel (tehát **nem** a $\mathcal{C}$ valamelyik hatványa szerinti képe), a példánkban $i = 1$. Ez azt jelenti, hogy ez a $\mathbf{v}_i$ kifejezhető a $\mathbf{v}$ és a többi pályából vett elemek lineáris kombinációjaként, a példánkban

$$\mathbf{v}_1 = \frac{1}{6}\mathbf{v} - \frac{4}{3}\mathcal{C}\mathbf{v}_2 - \frac{11}{6}\mathcal{C}^2\mathbf{v}_4.$$

Ezért, ha ezen $\mathbf{v}_i$ pályáját kicseréljük $\mathbf{v}$ pályájára, akkor továbbra is generátorrendszert kapunk. A példánkban a $\mathbf{v}_1, \mathcal{C}\mathbf{v}_1, \mathcal{C}^2\mathbf{v}_1$ pályát cseréljük ki a $\mathbf{v}, \mathcal{C}\mathbf{v}$ pályára. Az új pálya hossza m, ami kisebb, mint az elhagyott P_i hossza, hiszen $\mathcal{C}^m\mathbf{v_i}$ a P_i pálya $m+1$-edik eleme volt. ■

A 6.6.1–6.6.3 Tételekből azonnal adódik, hogy a komplex test felett egy tetszőleges transzformáció „legszebb" mátrixa:

6.6.6 Tétel (Jordan-féle normálalak)
Legyen V a komplex test feletti véges dimenziós vektortér, $\mathcal{A} \in \operatorname{Hom} V$, $m_{\mathcal{A}} = (x-\lambda_1)^{k_1} \dots (x-\lambda_t)^{k_t}$. Ekkor alkalmas bázisban $\mathcal{A}$ mátrixa a 6.6.2 Tétel szerinti A_i blokkokból áll, $i = 1, 2, \dots, t$, egy-egy A_i blokk pedig a 6.6.3 Tételből adódó A_{ij} alblokkokból. Az A_{ij} alblokkok méretének (rögzített i melletti) maximuma k_i, és az A_{ij} alblokkok főátlójában minden elem λ_i, közvetlenül a főátló alatt minden elem 1, az összes többi elem pedig 0. ♣

A 6.6.6 Tételben leírt $[\mathcal{A}]$ mátrixot az $\mathcal{A}$ transzformációhoz tartozó *Jordan-féle normálalak*nak vagy röviden *Jordan-alak*nak hívjuk. Ha a transzformáció egy (tetszőleges bázis szerinti) mátrixát tekintjük, akkor ennek a mátrixnak a Jordan-alakján a transzformációhoz tartozó Jordan-alakot értjük.

A tételt azzal is kiegészíthetjük, hogy egy transzformáció (illetve mátrix) Jordan-alakja lényegében egyértelmű (eltekintve az egyes blokkok, illetve azokon belül az egyes alblokkok sorrendjétől).

A Jordan-alak szerint a komplex test felett bármely transzformációnak van „majdnem diagonális mátrixa": csak a főátlóban és közvetlenül a főátló alatt állhatnak nem nulla elemek, a főátlóban a sajátértékek szerepelnek, közvetlenül a főátló alatt pedig 1-ek (az alblokkokon belül), illetve 0-k (az alblokkok, illetve blokkok határánál).

Feladatok

6.6.1 Bizonyítsuk be, hogy $\mathcal{A}$-nak akkor és csak akkor létezik diagonális mátrixa, ha $m_{\mathcal{A}}$ csupa különböző gyöktényező szorzatára bomlik.

6.6.2 Legyen $\dim V = n$, és tegyük fel, hogy $\mathcal{A}$-nak n különböző sajátértéke van.

(a) Bizonyítsuk be, hogy ha $\mathcal{AB} = \mathcal{BA}$, akkor $\mathcal{B}$-nek létezik diagonális mátrixa.

(b) Bizonyítsuk be, hogy $\mathcal{AB} = \mathcal{BA}$ akkor és csak akkor teljesül, ha valamilyen f polinomra $\mathcal{B} = f(\mathcal{A})$.

6.6.3 Legyen $\mathcal{A} \in \operatorname{Hom} V$ és U invariáns altere $\mathcal{A}$-nak. Milyen kapcsolatban áll az $\mathcal{A}$ transzformáció U-ra történő megszorításának a minimálpolinomja az eredeti minimálpolinommal? Vizsgáljuk meg ugyanezt a kérdést a karakterisztikus polinomokra is.

6.6.4 Legyenek U_1 és U_2 invariáns alterei $\mathcal{A}$-nak. Tekintsük az $\mathcal{A}$ transzformációnak a megszorítását az U_1, U_2, $U_1 \cap U_2$, illetve $\langle U_1, U_2 \rangle$ (invariáns) alterekre, és legyenek a megfelelő minimálpolinomok rendre m_1, m_2, $m_\cap$, illetve $m_{\langle\,\rangle}$. Bizonyítsuk be, hogy

(a) $m_{\langle\,\rangle} = [m_1, m_2]$;

(b) $m_\cap \mid (m_1, m_2)$, de általában nem áll fenn egyenlőség.

6.6.5 Legyenek U_1 és U_2 invariáns alterei $\mathcal{A}$-nak. Tekintsük az $\mathcal{A}$ transzformációnak a megszorítását az U_1, U_2, $U_1 \cap U_2$, illetve $\langle U_1, U_2 \rangle$ (invariáns) alterekre, és legyenek a megfelelő karakterisztikus polinomok rendre k_1, k_2, $k_\cap$, illetve $k_{\langle\,\rangle}$. Bizonyítsuk be, hogy

(a) $[k_1, k_2] \mid k_{\langle\,\rangle}$, de általában nem áll fenn egyenlőség;

(b) $k_\cap \mid (k_1, k_2)$, de általában nem áll fenn egyenlőség;

(c) $k_1 \cdot k_2 = k_\cap \cdot k_{\langle\,\rangle}$.

*6.6.6 Bizonyítsuk be, hogy végtelen test esetén egy transzformációnak akkor és csak akkor van véges sok invariáns altere, ha a minimálpolinom foka megegyezik a tér dimenziójával. Az invariáns alterek száma ekkor a minimálpolinom páronként nem-egységszeres osztóinak a számával egyenlő.

6.6.7 Legyen $\mathcal{A} \in \operatorname{Hom} V$. Bizonyítsuk be, hogy az alábbi feltételek ekvivalensek.

(i) $\mathcal{A}$ minden invariáns altere (alkalmas $f \in T[x]$ polinommal) $\operatorname{Ker} f(\mathcal{A})$ alakú.

(ii) $\mathcal{A}$ minden invariáns altere (alkalmas $g \in T[x]$ polinommal) $\operatorname{Im} g(\mathcal{A})$ alakú.

(iii) $\mathcal{A}$ minden invariáns altere (alkalmas $\mathbf{u} \in V$ vektorral) $\langle \mathbf{u}, \mathcal{A} \rangle$ alakú.

(iv) A minimálpolinom foka megegyezik a tér dimenziójával.

(v) A minimálpolinom megegyezik a karakterisztikus polinommal.

6.6.8 A mátrixok hasonlóságának az analógiájára két lineáris transzformációt, $\mathcal{A}, \mathcal{B} \in \operatorname{Hom} V$-t *hasonló*nak nevezünk, ha „van közös mátrixuk”, azaz van olyan $\mathbf{a}_1, \ldots, \mathbf{a}_n$, illetve $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis, hogy $[\mathcal{B}]_b = [\mathcal{A}]_a$. Ezt $\mathcal{A} \sim \mathcal{B}$-vel jelöljük.

(a) Melyek azok a transzformációk, amelyek csak önmagukhoz hasonlók?

(b) Bizonyítsuk be, hogy $\mathcal{A}$ és $\mathcal{B}$ akkor és csak akkor hasonló, ha van olyan invertálható $\mathcal{C}$, amelyre $\mathcal{B} = \mathcal{C}^{-1}\mathcal{A}\mathcal{C}$.

(c) Igazoljuk, hogy a hasonlóság ekvivalenciareláció.

(d) Legyen $\mathcal{A} \sim \mathcal{B}$. Következik-e ebből $\mathcal{A}+\mathcal{D} \sim \mathcal{B}+\mathcal{D}$, illetve $\mathcal{A}\mathcal{D} \sim \mathcal{B}\mathcal{D}$?

(e) Bizonyítsuk be, hogy ha $\mathcal{A} \sim \mathcal{B}$, akkor tetszőleges f polinomra $f(\mathcal{A}) \sim f(\mathcal{B})$.

(f) Bizonyítsuk be, hogy hasonló transzformációk karakterisztikus polinomja és minimálpolinomja megegyezik. Igaz-e ennek az állításnak a megfordítása?

6.6.9 Adott V esetén melyek azok a transzformációk, amelyeket a minimálpolinomjuk egyértelműen meghatároz?

6.6.10 Írjuk fel az alábbi 3×3-as mátrixok Jordan-alakját:

$$\text{(a)}\ \begin{pmatrix} 1 & 0 & 1 \\ 0 & 2 & 0 \\ 1 & 0 & 1 \end{pmatrix};\ \text{(b)}\ \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix};\ \text{(c)}\ \begin{pmatrix} 1 & 1 & 1 \\ 0 & 2 & 0 \\ 1 & 1 & 1 \end{pmatrix};\ \text{(d)}\ \begin{pmatrix} 1 & 0 & 0 \\ 2 & 1 & 2 \\ 0 & 0 & 1 \end{pmatrix}.$$

6.6.11 Írjuk fel az alábbi $n \times n$-es $A = (\alpha_{ij})$ mátrixok Jordan-alakját.

(a) $\alpha_{ij} = \begin{cases} 1, & \text{ha } j = i+1; \\ 0, & \text{egyébként.} \end{cases}$
(Közvetlenül a főátló felett 1-ek állnak, minden más elem 0.)

(b) $\alpha_{ij} = \begin{cases} 1, & \text{ha } j \equiv i+1 \pmod{n}; \\ 0, & \text{egyébként.} \end{cases}$
(Közvetlenül a főátló felett, valamint a bal alsó sarokban 1-ek állnak, minden más elem 0.)

(c) $\alpha_{ij} = \begin{cases} 1, & \text{ha } j = i-2; \\ 0, & \text{egyébként.} \end{cases}$
(A főátló alatti második átlóban 1-ek állnak, minden más elem 0.)

(d) $\alpha_{ij} = \begin{cases} 1, & \text{ha } j < i; \\ 0, & \text{egyébként.} \end{cases}$
(A főátló alatt mindenütt 1-ek állnak, a többi elem pedig 0.)

(e) $\alpha_{ij} = 1$. (Minden elem 1.)

(f) $\alpha_{ij} = \begin{cases} 1, & \text{ha } i+j = n+1; \\ 0, & \text{egyébként.} \end{cases}$
(A bal alsó és jobb felső sarkot összekötő átlóban 1-ek állnak, a többi elem 0.)

6.6.12 Hogyan kapjuk meg egy Jordan-alakban megadott mátrix (tetszőleges nagy pozitív egész kitevős) hatványait?

6.6.13 Hogyan olvashatjuk le a Jordan-alakból a minimálpolinomot és a karakterisztikus polinomot?

6.6.14 Legyen V a komplex test feletti n-dimenziós vektortér, $\mathcal{A} \in \operatorname{Hom} V$ és $0 \leq k \leq n$. Mutassuk meg, hogy $\mathcal{A}$-nak létezik k-dimenziós invariáns altere.

6.6.15 Legyen V a komplex test feletti véges dimenziós vektortér. Melyek azok a transzformációk, amelyeket

(a) a minimálpolinomjuk;
(b) a karakterisztikus polinomjuk;
(c) a minimál- és a karakterisztikus polinomjuk együttesen

hasonlóság erejéig egyértelműen meghatároz?

*6.6.16 Bizonyítsuk be, hogy bármely komplex elemű négyzetes mátrix hasonló a transzponáltjához.

*6.6.17 Számítsuk ki az alábbi mátrixok 2000-ik hatványát:

(a) $A = \begin{pmatrix} 3 & 1 \\ 2 & 4 \end{pmatrix}$; (b) $B = \begin{pmatrix} 3 & 1 \\ -1 & 1 \end{pmatrix}$.

7. BILINEÁRIS FÜGGVÉNYEK

A valós bilineáris függvények és kvadratikus alakok vizsgálata a geometriából, a másodrendű görbék és felületek általánosításaként alakult ki. Jellemzésüknél központi szerephez jut az általánosított merőlegességfogalom, az ortogonalitás. A „legszebb" bilineáris függvény a skalárszorzat, amely az euklideszi tereket „hozza létre" (lásd a következő fejezetet). Röviden arra is rámutatunk, hogyan kell módosítani a bilineáris függvény definícióját a komplex test esetén, hogy a valósban megismert „jó tulajdonságokat" át lehessen menteni.

7.1. Valós bilineáris függvény

7.1.1 Definíció

Legyen V vektortér $\mathbf{R}$ felett. Az $\mathbf{A} : V \times V \to \mathbf{R}$ leképezést (valós) *bilineáris függvény*nek nevezzük, ha mindkét változójában lineáris, azaz az egyik változó bármely rögzített értéke esetén a másik változójában lineáris.

Ez részletesen kiírva a következőket jelenti ($\mathbf{u}$, $\mathbf{u}'$, $\mathbf{v}$, $\mathbf{v}' \in V$, $\lambda \in \mathbf{R}$):

(i) $\mathbf{A}$ minden $(\mathbf{u}, \mathbf{v})$ vektorpárhoz egyértelműen hozzárendel egy valós számot;
(ii) $\mathbf{A}(\mathbf{u} + \mathbf{u}', \mathbf{v}) = \mathbf{A}(\mathbf{u}, \mathbf{v}) + \mathbf{A}(\mathbf{u}', \mathbf{v})$;
(iii) $\mathbf{A}(\lambda\mathbf{u}, \mathbf{v}) = \lambda\mathbf{A}(\mathbf{u}, \mathbf{v})$;
(iv) $\mathbf{A}(\mathbf{u}, \mathbf{v} + \mathbf{v}') = \mathbf{A}(\mathbf{u}, \mathbf{v}) + \mathbf{A}(\mathbf{u}, \mathbf{v}')$;
(v) $\mathbf{A}(\mathbf{u}, \lambda\mathbf{v}) = \lambda\mathbf{A}(\mathbf{u}, \mathbf{v})$. ♣

A bilineáris függvényeket vastag latin nagybetűvel fogjuk jelölni. A definícióból és a lineáris leképezések tulajdonságaiból azonnal következnek az alábbi azonosságok:

(vi) $\mathbf{A}(\mathbf{u}, \mathbf{0}) = \mathbf{A}(\mathbf{0}, \mathbf{v}) = 0$; (vii) $\mathbf{A}(-\mathbf{u}, \mathbf{v}) = \mathbf{A}(\mathbf{u}, -\mathbf{v}) = -\mathbf{A}(\mathbf{u}, \mathbf{v})$;

$$\text{(viii)} \quad \mathbf{A}\left(\sum_{i=1}^{k} \lambda_i \mathbf{u}_i, \sum_{j=1}^{m} \mu_j \mathbf{v}_j\right) = \sum_{i=1}^{k} \sum_{j=1}^{m} \lambda_i \mu_j \mathbf{A}(\mathbf{u}_i, \mathbf{v}_j).$$

Példák bilineáris függvényre

P1. Legyen V az origóból kiinduló sík-, illetve térvektorok szokásos vektortere és $\mathbf{A}$ a (geometriából ismert) *skalárszorzat*: két vektorhoz a hosszaiknak és a közbezárt szög koszinuszának a szorzatát rendeljük. (Ha az

egyik vagy mindkét vektor nullvektor, akkor a skalárszorzat nulla, és ez összhangba hozható a fentiekkel, mert a közbezárt szöggel ugyan probléma van, azonban a nulla hosszat bármivel szorozva ismét nullát kapunk.) A skalárszorzat megadható a vektorok szokásos (derékszögű egységvektorok szerinti) koordinátáival is: a megfelelő koordináták szorzatösszegét kell képezni.

P2. A skalárszorzat második jellemzését tetszőleges $\mathbf{R}^k$-ra általánosíthatjuk: a két vektorhoz a megfelelő koordináták szorzatösszegét rendeljük, azaz ha $\mathbf{u} = \begin{pmatrix} u_1 \\ \vdots \\ u_k \end{pmatrix}$, $\mathbf{v} = \begin{pmatrix} v_1 \\ \vdots \\ v_k \end{pmatrix}$, akkor $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \sum_{i=1}^{k} u_i v_i$.

Ennek alapján a valós test feletti tetszőleges k-dimenziós vektortéren is értelmezhetünk skalárszorzatot: rögzítünk egy bázist, és utána ugyanígy a megfelelő koordináták szorzatösszegét vesszük.

Itt jegyezzük meg, hogy ebben és a következő fejezetben az eddigiektől eltérően a vektorok komponenseit, illetve koordinátáit nem görög betűkkel, hanem — az általános szokásnak megfelelően — latin kisbetűkkel fogjuk jelölni.

P3. Az előző példa jelöléseit megtartva bilineáris függvény $\mathbf{R}^k$-n például $u_1v_2 + 2u_2v_1$ vagy $u_1v_1 - 3u_2v_2$ stb.

P4. Minden vektorpárhoz a nulla valós számot rendelve kapjuk a(z azonosan nulla) $\mathbf{0}$ bilineáris függvényt.

P5. Végül nézzünk néhány végtelen dimenziós példát. Legyen V a valós együtthatós polinomok szokásos vektortere, és két polinomhoz rendeljük hozzá a szorzatuknak egy adott helyen vett helyettesítési értékét. Ugyanezt polinomok helyett (pl.) folytonos függvényekre is megtehetjük. Egy másik lehetséges hozzárendelés a szorzatfüggvény integrálja egy adott intervallumon.

A fejezet további részében csak *véges dimenziós* vektorterekkel foglalkozunk. Legyen $\dim V = n$, és rögzítsünk le egy $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázist.

Belátjuk, hogy a lineáris leképezésekhez hasonlóan a bilineáris függvények is jellemezhetők a báziselemek képével, és ez lehetővé teszi a mátrixos megadást.

7.1.2 Tétel

Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis a V vektortérben és α_{ij}, $i, j = 1, 2, \ldots, n$ tetszőleges valós számok. Ekkor *pontosan* egy olyan $\mathbf{A}$ bilineáris függvény létezik, amelyre

$$\mathbf{A}(\mathbf{b}_i, \mathbf{b}_j) = \alpha_{ij}, \quad i, j = 1, 2, \ldots, n. \ \clubsuit$$

Bizonyítás: Az 5.3.1 Tétel bizonyításának a gondolatmenetét követjük. Vegyünk V-ből tetszőleges $\mathbf{u}$ és $\mathbf{v}$ vektorokat, ezek egyértelműen felírhatók $\mathbf{u} = u_1\mathbf{b}_1 + \ldots + u_n\mathbf{b}_n$, illetve $\mathbf{v} = v_1\mathbf{b}_1 + \ldots + v_n\mathbf{b}_n$ alakban. *Ha létezik* a mondott tulajdonságú $\mathbf{A}$ bilineáris függvény, akkor a (viii) tulajdonság alapján szükségképpen

$$\mathbf{A}(\mathbf{u},\mathbf{v}) = \mathbf{A}(u_1\mathbf{b}_1 + \ldots + u_n\mathbf{b}_n, v_1\mathbf{b}_1 + \ldots + v_n\mathbf{b}_n) = \\ = \sum_{i,j=1}^{n} u_i v_j \mathbf{A}(\mathbf{b}_i,\mathbf{b}_j) = \sum_{i,j=1}^{n} u_i v_j \alpha_{ij}$$

teljesül. Ez azt mutatja, hogy $\mathbf{A}(\mathbf{u},\mathbf{v})$ egyértelműen meg van határozva, tehát legfeljebb egy ilyen $\mathbf{A}$ létezhet. Sőt, az is kiderült, hogy *csak* az $\mathbf{A}(\mathbf{u},\mathbf{v}) = \sum_{i,j=1}^{n} u_i v_j \alpha_{ij}$ képlettel definiált függvény jöhet szóba. Erről kell tehát megmutatni, hogy valóban bilineáris, ami a (ii)–(v) tulajdonságok ellenőrzését jelenti. Ennek végigszámolását az Olvasóra bízzuk. ■

7.1.3 Definíció

Az $\mathbf{A}$ bilineáris függvénynek a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis szerinti *mátrix*án azt az $n \times n$-es mátrixot értjük, amelyben az i-ik sor j-ik eleme $\alpha_{ij} = \mathbf{A}(\mathbf{b}_i,\mathbf{b}_j)$. Ezt a mátrixot $[\mathbf{A}]_b$-vel jelöljük. ♣

Ne felejtsük el, hogy a lineáris leképezésekhez hasonlóan a bilineáris függvény mátrixa is erősen bázisfüggő, más bázist választva általában a mátrix is egészen más lesz.

7.1.4 Tétel

Rögzített bázis mellett kölcsönösen egyértelmű megfeleltetés áll fenn a V-n értelmezett bilineáris függvények és az $n \times n$-es (valós) mátrixok között. Ha az $\mathbf{u}$, illetve $\mathbf{v}$ vektor koordinátái az adott bázisban $u_1, \ldots, u_n$, illetve $v_1, \ldots, v_n$, akkor

$$\mathbf{A}(\mathbf{u},\mathbf{v}) = \sum_{i,j=1}^{n} \alpha_{ij} u_i v_j \tag{7.1.1}$$

vagy mátrixos felírásban

$$\mathbf{A}(\mathbf{u},\mathbf{v}) = [\mathbf{u}]^T[\mathbf{A}][\mathbf{v}] = (u_1, u_2, \ldots, u_n) \begin{pmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix}. \tag{7.1.2}$$

♣

Bizonyítás: A kölcsönös egyértelműséget a 7.1.2 Tétel biztosítja. A (7.1.1) előállítást a 7.1.2 Tétel bizonyítása során igazoltuk. A (7.1.1) és (7.1.2) képletek ekvivalenciája a (7.1.2)-beli mátrixszorzások elvégzésével adódik. ■

A mátrixos jellemzés, illetve (7.1.1) és (7.1.2) az összes bilineáris függvény kényelmes áttekintését teszi lehetővé.

Feladatok

V végig a valós test feletti véges dimenziós vektorteret jelent.

7.1.1 Legyen V a legfeljebb 4-edfokú valós együtthatós polinomok (beleértve a 0 polinomot is) szokásos vektortere. Válasszuk ki az alábbi leképezések közül a bilineáris függvényeket, és írjuk fel a mátrixukat a szokásos bázisban. Legyen f, g képe

(a) fg; (b) $f(1) + g(1)$; (c) $f(1)g(2)$; (d) $f'(1)g(2)$;

(e) fg-ben x^2 együtthatója.

7.1.2 Írjuk fel a P2, P3 és P4 példákban szereplő bilineáris függvények mátrixát (alkalmas bázisban).

7.1.3 Mi lehet egy valós bilineáris függvény értékkészlete (azaz a felvett értékeinek az összessége)?

7.1.4 Hogyan módosul a 7.1.2 Tétel állítása, ha bázis helyett (a) generátorrendszeren; (b) lineárisan független rendszeren írjuk elő a bilineáris függvény értékét?

7.1.5 Definiáljunk a V-n értelmezett bilineáris függvények körében természetes módon összeadást és skalárszorost, és mutassuk meg, hogy így egy vektorteret kapunk. Hány dimenziós ez a vektortér?

7.1.6 Legyen V egy bázisa $\mathbf{b}_1, \ldots, \mathbf{b}_n$. Hogyan változik egy $\mathbf{A}$ bilineáris függvény mátrixa, ha

(a) $\mathbf{b}_1$-et és $\mathbf{b}_2$-t felcseréljük;

(b) $\mathbf{b}_3$ helyett $\lambda\mathbf{b}_3$-at veszünk ($\lambda \neq 0$);

(c) $\mathbf{b}_3$ helyett $\mathbf{b}_3 + \mu\mathbf{b}_2$-t veszünk?

7.1.7 Adjuk meg az összes olyan bilineáris függvényt, amelynek bármely bázisban ugyanaz a mátrixa.

7.1.8 Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ rögzített bázis V-ben, és tekintsük a P2 példában értelmezett (a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis szerinti) skalárszorzatot. Jelöljük $\mathbf{c}$ és $\mathbf{d}$ skalárszorzatát $\mathbf{c}\cdot\mathbf{d}$-vel.

(a) Legyen $\mathcal{A} \in \operatorname{Hom} V$ egy tetszőleges lineáris transzformáció. Lássuk be, hogy $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \mathbf{u} \cdot \mathcal{A}\mathbf{v}$ bilineáris függvényt határoz meg.

(b) Mutassuk meg, hogy az (a)-beli $\mathcal{A}$ lineáris transzformációnak és $\mathbf{A}$ bilineáris függvénynek a $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázisban felírt mátrixa ugyanaz: $[\mathcal{A}]_b = [\mathbf{A}]_b$.

(c) Bizonyítsuk be, hogy minden bilineáris függvény előáll az (a)-beli alakban alkalmas $\mathcal{A} \in \operatorname{Hom} V$-vel.

7.1.9 A $V \to \mathbf{R}$ lineáris leképezéseket, azaz $\operatorname{Hom}(V, \mathbf{R})$ elemeit *lineáris függvény*eknek nevezzük.

(a) Legyen Φ és Ψ két lineáris függvény. Mutassuk meg, hogy $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \Phi(\mathbf{u})\Psi(\mathbf{v})$ bilineáris függvényt definiál. Mennyi lesz $\mathbf{A}$ mátrixának a rangja?

M*(b) Lássuk be, hogy tetszőleges $\mathbf{A}$ bilineáris függvény előáll $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \sum_{m=1}^{r} \Phi_m(\mathbf{u})\Psi_m(\mathbf{v})$ alakban, ahol Φ_m, Ψ_m lineáris függvények $(m = 1, 2, \ldots, r)$. Mi az r lehető legkisebb értéke?

7.2. Ortogonalizálás

Legyen V továbbra is egy véges dimenziós vektortér a valós test fölött. Ebben a pontban azt vizsgáljuk, mikor létezik egy $\mathbf{A}$ bilineáris függvénynek „szép” mátrixa, nevezetesen mely $\mathbf{A}$-khoz található olyan bázis, amelyben $\mathbf{A}$ mátrixa diagonális (azaz a főátlón kívül minden elem nulla). Kiderül, hogy a transzformációknál tapasztaltakhoz képest itt jóval kedvezőbb a helyzet. Könnyen adódik az az egyszerű szükséges feltétel, hogy $\mathbf{A}$ szimmetrikus legyen. Meglepő, hogy ez egyben elégséges is a diagonalizálhatósághoz.

7.2.1 Definíció
Egy $\mathbf{A}$ bilineáris függvény *szimmetrikus*, ha minden $\mathbf{u}, \mathbf{v} \in V$-re $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \mathbf{A}(\mathbf{v}, \mathbf{u})$. ♣

Az előző pont példái közül szimmetrikus volt a skalárszorzat, a nulla függvény és a P3 példában másodiknak megadott függvény, de nem volt szimmetrikus az ottani első függvény.

7.2.2 Tétel
Egy $\mathbf{A}$ bilineáris függvény akkor és csak akkor szimmetrikus, ha (akármelyik bázisban felírt) mátrixa szimmetrikus (azaz megegyezik a transzponáltjával). ♣

Bizonyítás: Ha az $\mathbf{A}$ bilineáris függvény szimmetrikus, akkor a szimmetriát speciálisan a $\mathbf{b}_i$ báziselemekre kihasználva $\alpha_{ij} = \mathbf{A}(\mathbf{b}_i, \mathbf{b}_j) = \mathbf{A}(\mathbf{b}_j, \mathbf{b}_i) = \alpha_{ji}$ adódik, tehát a mátrix is szimmetrikus. Megfordítva, ha $\alpha_{ij} = \alpha_{ji}$, akkor pl. a 7.1.4 Tétel (1) képletéből leolvasható $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \mathbf{A}(\mathbf{v}, \mathbf{u})$, tehát ekkor az $\mathbf{A}$ bilineáris függvény is szimmetrikus. ■

Most rátérünk a diagonalizálhatóság kérdésére. Először tegyük fel, hogy $\mathbf{A}$-nak létezik diagonális mátrixa. Mivel egy diagonális mátrix eleve szimmetrikus, így (az előző tétel alapján) ekkor $\mathbf{A}$-nak mindenesetre szimmetrikusnak kell lennie. Mint a bevezetőben már említettük, a megfordítás is igaz:

7.2.3 Tétel
Legyen $\mathbf{A}$ szimmetrikus bilineáris függvény V-n. Ekkor létezik olyan bázis, amelyben $\mathbf{A}$ mátrixa diagonális. ♣

Mielőtt rátérnénk a bizonyításra, néhány magyarázó megjegyzést teszünk. A diagonális mátrix pontosan azt jelenti, hogy a szóban forgó $\mathbf{c}_1, \ldots, \mathbf{c}_n$ bázisban $\mathbf{A}(\mathbf{c}_i, \mathbf{c}_j) = 0$, ha $i \neq j$. Ha speciálisan a bilineáris függvény a sík- vagy térvektorok szokásos skalárszorzata, akkor $\mathbf{A}(\mathbf{u}, \mathbf{v}) = 0$ azt jelenti, hogy $\mathbf{u}$ és $\mathbf{v}$ egymásra merőlegesek, vagy — görög-latin eredetű szóval — ortogonálisak. Ennek általánosítása a következő

7.2.4 Definíció
Legyen A szimmetrikus bilineáris függvény. Az $\mathbf{u}, \mathbf{v} \in V$ vektorok $\mathbf{A}$-*ortogonális*ak, ha $\mathbf{A}(\mathbf{u}, \mathbf{v}) = 0$. ♣

Ennek alapján a 7.2.3 tételt úgy is megfogalmazhatjuk, hogy egy $\mathbf{A}$ szimmetrikus bilineáris függvényhez mindig található $\mathbf{A}$-ortogonális bázis.

A tételre három bizonyítást adunk. Ezek közül az első nem teljes, mert a szimmetrikus bilineáris függvényeknek csak egy bizonyos — bár mint később látni fogjuk, talán a legfontosabb — osztályára alkalmazható. Ugyanakkor a bizonyítás nagy előnye, hogy meg is konstruál egy $\mathbf{A}$-ortogonális bázist. A második és harmadik bizonyítás bármely szimmetrikus bilineáris függvényre működik, és ezek is alkalmasak $\mathbf{A}$-ortogonális bázis tényleges megadására. A második bizonyítás alapgondolata hasonló az elsőéhez, de az általános eset kezeléséhez néhány technikai jellegű módosításra van szükség. A harmadik bizonyítás a Gauss-elimináció segítségével diagonalizálja $\mathbf{A}$ mátrixát. Mindegyik bizonyítás után (ugyanazon a) konkrét példán illusztráljuk a módszert.

A 7.2.3 Tétel első bizonyítása (Gram–Schmidt ortogonalizáció): Feltesszük, hogy $\mathbf{A}(\mathbf{u},\mathbf{u}) \neq 0$, ha $\mathbf{u} \neq \mathbf{0}$. Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ tetszőleges bázis V-ben. Ebből gyártunk egy $\mathbf{c}_1, \ldots, \mathbf{c}_n$ $\mathbf{A}$-ortogonális bázist, amelynek elemeit rekurzíve konstruáljuk meg a következő séma szerint:

$$\begin{aligned}
&\mathbf{c}_1 = \mathbf{b}_1\,,\\
&\mathbf{c}_2 = \mathbf{b}_2 + \rho_{21}\mathbf{c}_1\,,\\
&\mathbf{c}_3 = \mathbf{b}_3 + \rho_{31}\mathbf{c}_1 + \rho_{32}\mathbf{c}_2\,,\\
&\vdots\\
&\mathbf{c}_n = \mathbf{b}_n + \rho_{n1}\mathbf{c}_1 + \rho_{n2}\mathbf{c}_2 + \ldots + \rho_{n,n-1}\mathbf{c}_{n-1}\,,
\end{aligned}$$

ahol a ρ_{qs} skalárokat később alkalmasan megválasztjuk.

Először azt mutatjuk meg, hogy a $\mathbf{c}_1, \ldots, \mathbf{c}_n$ vektorok a ρ_{qs} skalárok tetszőleges értéke esetén bázist alkotnak V-ben. Mivel $n = \dim V$, ezért elég azt igazolni, hogy $\mathbf{c}_1, \ldots, \mathbf{c}_n$ generátorrendszer, és ehhez elég azt belátni, hogy mindegyik $\mathbf{b}_j$ előáll a $\mathbf{c}_i$-k lineáris kombinációjaként. Ez viszont azonnal következik a $\mathbf{c}_j$-re felírt egyenletből, ha onnan $\mathbf{b}_j$-t ($\mathbf{c}_1, \ldots, \mathbf{c}_j$ segítségével) kifejezzük.

Most azt igazoljuk, hogy a ρ_{qs} együtthatók alkalmas megválasztásával a $\mathbf{c}_i$ vektorok $\mathbf{A}$-ortogonálisak lesznek. Ehhez a $\mathbf{c}_j$-ket úgy fogjuk egymás után meghatározni, hogy a $\mathbf{c}_j$ vektor $\mathbf{A}$-ortogonális legyen $\mathbf{c}_1, \ldots, \mathbf{c}_{j-1}$ mindegyikére.

Nézzük először $\mathbf{c}_2$-t. Erre az egyetlen feltétel $\mathbf{A}(\mathbf{c}_2, \mathbf{c}_1) = 0$ teljesülése. Írjuk be ide $\mathbf{c}_2$ előállítását:

$$0 = \mathbf{A}(\mathbf{c}_2, \mathbf{c}_1) = \mathbf{A}(\mathbf{b}_2 + \rho_{21}\mathbf{c}_1, \mathbf{c}_1) = \mathbf{A}(\mathbf{b}_2, \mathbf{c}_1) + \rho_{21}\mathbf{A}(\mathbf{c}_1, \mathbf{c}_1)\,.$$

Innen $\rho_{21} = -\mathbf{A}(\mathbf{b}_2, \mathbf{c}_1)/\mathbf{A}(\mathbf{c}_1, \mathbf{c}_1)$. (A feltevésünk szerint a nevező nem nulla.)

Hasonlóan okoskodhatunk általában is. Tegyük fel, hogy $\mathbf{c}_1, \ldots, \mathbf{c}_{m-1}$-ről az első $m-1$ egyenlet alapján már tudjuk, hogy $\mathbf{A}$-ortogonálisak. Legyen $j < m$ tetszőleges és nézzük, milyen követelményt jelent $\mathbf{c}_m$ és $\mathbf{c}_j$ $\mathbf{A}$-ortogonalitása az m-edik egyenletben:

$$\begin{aligned}
0 = \mathbf{A}(\mathbf{c}_m, \mathbf{c}_j) = \mathbf{A}(\mathbf{b}_m + \rho_{m1}\mathbf{c}_1 + \rho_{m2}\mathbf{c}_2 + \ldots + \rho_{mj}\mathbf{c}_j + \ldots + \rho_{m,m-1}\mathbf{c}_{m-1}, \mathbf{c}_j) =\\
= \mathbf{A}(\mathbf{b}_m, \mathbf{c}_j) + \rho_{m1}\mathbf{A}(\mathbf{c}_1, \mathbf{c}_j) + \ldots + \rho_{mj}\mathbf{A}(\mathbf{c}_j, \mathbf{c}_j) + \ldots + \rho_{m,m-1}\mathbf{A}(\mathbf{c}_{m-1}, \mathbf{c}_j).
\end{aligned}$$

Ha $i < m$ és $i \neq j$, akkor $\mathbf{c}_i$ és $\mathbf{c}_j$ $\mathbf{A}$-ortogonalitását már tudjuk, tehát $\mathbf{A}(\mathbf{c}_i, \mathbf{c}_j) = 0$, és az előző feltétel így a $0 = \mathbf{A}(\mathbf{b}_m, \mathbf{c}_j) + \rho_{mj}\mathbf{A}(\mathbf{c}_j, \mathbf{c}_j)$ alakra redukálható, ahonnan $\rho_{mj} = -\mathbf{A}(\mathbf{b}_m, \mathbf{c}_j)/\mathbf{A}(\mathbf{c}_j, \mathbf{c}_j)$. Ezzel igazoltuk, hogy az m-edik egyenletbeli ρ_{mj} együtthatók valóban megválaszthatók úgy, hogy $\mathbf{c}_m$ a $\mathbf{c}_1, \ldots, \mathbf{c}_{m-1}$ vektorok mindegyikére $\mathbf{A}$-ortogonális legyen. ■

Megjegyzések: Az $\mathbf{A}(\mathbf{u},\mathbf{u}) \neq 0$ feltételt csak az egymás után adódó $\mathbf{c}_1, \ldots, \mathbf{c}_{n-1}$ vektorokra kellett felhasználnunk. Így szerencsés esetben az eljárás olyankor is működhet, ha az $\mathbf{A}(\mathbf{u},\mathbf{u})$ értékek között ugyan előfordul (nem triviálisan) a nulla, de az ortogonalizáció során nem botlunk ilyen $\mathbf{u}$-kba (ilyen lesz az alább tárgyalt illusztrációs példa is).

Egy vektortérben egy adott $\mathbf{A}$-hoz nagyon sokféle $\mathbf{A}$-ortogonális bázis létezik. Ez már a fenti bizonyításból is kiderül, hiszen más és más $\mathbf{b}_i$ bázisból kiindulva általában különböző $\mathbf{c}_i$ bázisokhoz jutunk.

Még egyszer hangsúlyozzuk, hogy a bizonyítás egyúttal a gyakorlatban is jól használható eljárást adott $\mathbf{A}$-ortogonális bázis konstrukciójára. Ezt most egy konkrét példával illusztráljuk.

Példa: Legyen $V = \mathbf{R}^3$, az $\mathbf{u}$, illetve $\mathbf{v}$ vektor komponenseit jelölje u_1, u_2, u_3, illetve v_1, v_2, v_3. Keressünk $\mathbf{A}$-ortogonális bázist és diagonális mátrixot a következő szimmetrikus bilineáris függvényhez:

$$\mathbf{A}(\mathbf{u},\mathbf{v}) = 4u_1v_1 + 2u_1v_2 + 2u_2v_1 + 2u_1v_3 + 2u_3v_1 + 2u_2v_3 + 2u_3v_2\,. \quad (7.2.1)$$

Vegyük kiinduló bázisnak a szokásos $\mathbf{b}_1 = \begin{pmatrix}1\\0\\0\end{pmatrix}$, $\mathbf{b}_2 = \begin{pmatrix}0\\1\\0\end{pmatrix}$, $\mathbf{b}_3 = \begin{pmatrix}0\\0\\1\end{pmatrix}$ egységvektorokat. A konstrukció szerint $\mathbf{c}_1 = \mathbf{b}_1$. Ezután $\mathbf{c}_2 = \mathbf{b}_2 + \rho_{21}\mathbf{c}_1$. Az $\mathbf{A}(\mathbf{c}_2,\mathbf{c}_1) = 0$ feltételből megkapjuk ρ_{21}-et:

$$0 = \mathbf{A}(\mathbf{c}_2,\mathbf{c}_1) = \mathbf{A}\left[\begin{pmatrix}0\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}\right] + \rho_{21}\mathbf{A}\left[\begin{pmatrix}1\\0\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\end{pmatrix}\right] = 2 + 4\rho_{21}\,,$$

ahonnan $\rho_{21} = -1/2$. Így

$$\mathbf{c}_2 = \begin{pmatrix}0\\1\\0\end{pmatrix} - \frac{1}{2}\begin{pmatrix}1\\0\\0\end{pmatrix} = \begin{pmatrix}-1/2\\1\\0\end{pmatrix}\,.$$

(Ha nem akarunk törtekkel számolni, akkor nyugodtan beszorozhatjuk $\mathbf{c}_2$-t egy nem nulla skalárral, hiszen az $\mathbf{A}$-ortogonalitáson ez nem változtat.) Hasonlóan továbbhaladva, a

$$\mathbf{c}_3 = \mathbf{b}_3 + \rho_{31}\mathbf{c}_1 + \rho_{32}\mathbf{c}_2 = \begin{pmatrix}0\\0\\1\end{pmatrix} + \rho_{31}\begin{pmatrix}1\\0\\0\end{pmatrix} + \rho_{32}\begin{pmatrix}-1/2\\1\\0\end{pmatrix}$$

előállításban az $\mathbf{A}(\mathbf{c}_3, \mathbf{c}_1) = 0$ feltételből $\rho_{31} = -1/2$, az $\mathbf{A}(\mathbf{c}_3, \mathbf{c}_2) = 0$ feltételből pedig $\rho_{32} = 1$ adódik. Innen

$$\mathbf{c}_3 = \begin{pmatrix} -1 \\ 1 \\ 1 \end{pmatrix} .$$

Ezzel megkaptunk egy $\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3$ $\mathbf{A}$-ortogonális bázist. Az ennek megfelelő diagonális mátrix főátlójába az $\mathbf{A}(\mathbf{c}_i, \mathbf{c}_i)$ értékek kerülnek, így

$$[\mathbf{A}]_c = \begin{pmatrix} 4 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix} .$$

A 7.2.3 Tétel második bizonyítása: Először azt igazoljuk, hogy ha minden $\mathbf{u} \in V$-re $\mathbf{A}(\mathbf{u}, \mathbf{u}) = 0$, akkor $\mathbf{A}$ a(z azonosan) nulla bilineáris függvény, azaz minden $\mathbf{u}, \mathbf{v} \in V$-re $\mathbf{A}(\mathbf{u}, \mathbf{v}) = 0$. Ez rögtön adódik az

$$\begin{aligned} \mathbf{A}(\mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v}) &= \mathbf{A}(\mathbf{u}, \mathbf{u}) + \mathbf{A}(\mathbf{u}, \mathbf{v}) + \mathbf{A}(\mathbf{v}, \mathbf{u}) + \mathbf{A}(\mathbf{v}, \mathbf{v}) = \\ &= \mathbf{A}(\mathbf{u}, \mathbf{u}) + 2\mathbf{A}(\mathbf{u}, \mathbf{v}) + \mathbf{A}(\mathbf{v}, \mathbf{v}) \end{aligned}$$

összefüggésből.

Rátérve a tétel bizonyítására, ha $\mathbf{A}$ a nulla függvény, akkor bármely bázis $\mathbf{A}$-ortogonális ($\mathbf{A}$ mátrixa a nullmátrix). Egyébként válasszunk egy tetszőleges olyan $\mathbf{d}$ vektort, amelyre $\mathbf{A}(\mathbf{d}, \mathbf{d}) \neq 0$ (ilyen vektor az előzetes megjegyzés szerint biztosan létezik).

Tekintsük a $\mathbf{d}$-re $\mathbf{A}$-ortogonális összes vektor W halmazát, azaz

$$W = \{\mathbf{w} \in V \mid \mathbf{A}(\mathbf{d}, \mathbf{w}) = 0\} .$$

Megmutatjuk, hogy W altér, és V minden $\mathbf{v}$ eleme egyértelműen írható fel

$$\mathbf{v} = \lambda\mathbf{d} + \mathbf{w} \tag{7.2.2}$$

alakban, ahol $\mathbf{w} \in W$ (vagyis V a $\langle\mathbf{d}\rangle$ és W alterek direkt összege).

W nem az üres halmaz, mert a $\mathbf{0}$ mindenképpen eleme, továbbá egyszerű számolással ellenőrizhető, hogy az összeadásra és a skalárral való szorzásra zárt, tehát valóban altér. A (7.2.2)-beli felírás azzal ekvivalens, hogy $\mathbf{v} - \lambda\mathbf{d} \in W$, azaz $\mathbf{A}(\mathbf{d}, \mathbf{v} - \lambda\mathbf{d}) = 0$. Ez átírható az $\mathbf{A}(\mathbf{d}, \mathbf{v}) - \lambda\mathbf{A}(\mathbf{d}, \mathbf{d}) = 0$

alakba, ahonnan adódik, hogy a feltételeknek pontosan egy λ érték felel meg: $\lambda = \mathbf{A}(\mathbf{d},\mathbf{v})/\mathbf{A}(\mathbf{d},\mathbf{d})$.

Ezután válasszuk a keresett $\mathbf{A}$-ortogonális bázis első elemének $\mathbf{d}$-t, és ismételjük meg a fenti eljárást a(z eggyel) kisebb dimenziós W altérre stb. Így legfeljebb $\dim V - 1$ lépésben egy $\mathbf{A}$-ortogonális bázist kapunk. [Az eljárás akkor ér véget hamarabb, ha közben valamelyik (legalább kétdimenziós) altéren az $\mathbf{A}$ (megszorítása) már azonosan nulla.] ■

Az első és a második bizonyítást összevetve, az első az alterek egyre bővülő láncában épít fel $\mathbf{A}$-ortogonális rendszert, a második pedig tulajdonképpen fordított irányban haladva alterek egyre szűkülő láncán keresztül jut el egy ilyen rendszerhez.

A második bizonyítással kapcsolatban megjegyezzük, hogy W tulajdonságainak az igazolását a mátrixok segítségével, a $[\mathbf{d}]^T[\mathbf{A}][\mathbf{w}] = 0$ egyenletből is megkaphattuk volna, és ennek segítségével egyúttal W elemeit is ténylegesen elő tudjuk állítani. Ily módon ténylegesen meg is konstruálhatunk egy $\mathbf{A}$-ortogonális bázist. Nézzük meg ezt a gyakorlatban az első bizonyítás utáni (7.2.1) példán.

Az $\mathbf{A}$ mátrixa az eredeti $\mathbf{b}_i$ bázisban $\begin{pmatrix} 4 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix}$. Próbálkozzunk indulásként most is a $\mathbf{d} = \mathbf{b}_1$ vektorral. Ez megfelel, mert $\mathbf{A}(\mathbf{b}_1,\mathbf{b}_1) = 4 \neq 0$. Keressük meg a $\mathbf{d}$-re $\mathbf{A}$-ortogonális $\mathbf{w}$ vektorokat az $\mathbf{A}(\mathbf{d},\mathbf{w}) = [\mathbf{d}]^T[\mathbf{A}][\mathbf{w}] = 0$ egyenletből:

$$0 = \begin{pmatrix} 1 & 0 & 0 \end{pmatrix} \begin{pmatrix} 4 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix} \begin{pmatrix} w_1 \\ w_2 \\ w_3 \end{pmatrix} = 4w_1 + 2w_2 + 2w_3\,,$$

tehát W elemei a $\mathbf{w} = \begin{pmatrix} \alpha \\ \beta \\ -2\alpha - \beta \end{pmatrix}$ alakú vektorok. Ezek között kell most folytatni az ortogonalizálást [hiszen ezek valamennyien $\mathbf{A}$-ortogonálisak az elsőként választott $\begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix}$ vektorra]. Második vektornak megfelel pl. (az $\alpha = 1$, $\beta = 0$ értékekből adódó) $\mathbf{d}_2 = \begin{pmatrix} 1 \\ 0 \\ -2 \end{pmatrix}$, mert $\mathbf{A}(\mathbf{d}_2,\mathbf{d}_2) = -4 \neq 0$. A $\mathbf{d}_2$-re

W-n belül $\mathbf{A}$-ortogonális vektorokat a

$$0 = (\,1 \quad 0 \quad -2\,) \begin{pmatrix} 4 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix} \begin{pmatrix} \alpha \\ \beta \\ -2\alpha - \beta \end{pmatrix} = -4\alpha - 4\beta\,,$$

azaz $\beta = -\alpha$ feltételből kapjuk meg, ezek a vektorok tehát $\begin{pmatrix} \alpha \\ -\alpha \\ -\alpha \end{pmatrix}$ alakúak. (Ezen az egydimenziós altéren az $\mathbf{A}$ egyébként már a nulla függvény.) Így az $\mathbf{A}$-ortogonális bázis utolsó elemének pl. ($\alpha = 1$ választással) $\begin{pmatrix} 1 \\ -1 \\ -1 \end{pmatrix}$ vehető. A bilineáris függvény mátrixa ebben a bázisban $\begin{pmatrix} 4 & 0 & 0 \\ 0 & -4 & 0 \\ 0 & 0 & 0 \end{pmatrix}$.

A 7.2.3 Tétel harmadik bizonyítása: Írjuk fel $\mathbf{A}$ mátrixát egy tetszőleges $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázisban. A 7.1.6 feladatbeli változtatásokat fogjuk alkalmazni. Ezek tulajdonképpen a jól ismert elemi ekvivalens átalakítások, csak most mindig együtt kell végrehajtani ugyanazt az átalakítást a sorokra és a megfelelő oszlopokra is. Vegyük észre azt is, hogy egy-egy ilyen együttes lépés a mátrix szimmetriáját nem rontja el.

Foglaljuk össze, mik ezek a lépések és hogyan változik ekkor a mátrix.

(a) Két báziselemet felcserélve a mátrix megfelelő sorait és oszlopait kell felcserélni.

(b) A $\mathbf{b}_i$ báziselemet egy $\lambda \neq 0$ skalárral szorozva az i-edik sor és oszlop λ-val szorzódik, és speciálisan α_{ii} a λ^2-szeresére változik.

(c) Ha $\mathbf{b}_i$ helyére $\mathbf{b}_i + \mu\mathbf{b}_j$ kerül ($j \neq i$), akkor az i-edik sorhoz, illetve oszlophoz hozzáadjuk a j-edik sor, illetve oszlop μ-szörösét, és speciálisan az új i-edik sor i-edik eleme $\alpha'_{ii} = \alpha_{ii} + \mu\alpha_{ji} + \mu\alpha_{ij} + \mu^2\alpha_{jj}$ lesz.

Nézzük, hogyan működik a fenti lépésekkel végzett módosított Gauss-kiküszöbölés. Ha a bal felső sarokban álló elem nem nulla, akkor a többi sorból, illetve oszlopból az első sor, illetve oszlop megfelelő többszöröseit levonva az első sor és oszlop többi eleme nullává válik. Ha a bal felső sarokban nulla állt, de a főátló valamelyik másik eleme nem nulla, akkor egy sor- és oszlopcserével elérhetjük, hogy ez a nem nulla elem kerüljön a bal felső sarokba. Ha a főátló elemei nullák, de az első oszlop és sor (mondjuk) harmadik eleme ($\alpha_{13} = \alpha_{31}$) nem volt nulla, akkor adjuk hozzá az első sorhoz/oszlophoz a harmadik sort/oszlopot, ekkor a bal felső sarokba $\alpha'_{11} = \alpha_{11} + 2\alpha_{31} + \alpha_{33} = 2\alpha_{31} \neq 0$

került, és ezután indulhat a kivonogatás. Ha az első sor és oszlop minden eleme eleve nulla volt, akkor (egyelőre) ne csináljunk semmit.

Így elértük, hogy az első sorban és az első oszlopban az első elemtől (esetleg) eltekintve minden további elem nulla. Ezen a soron és oszlopon később már nem változtatunk. Most ugyanezt az eljárást megismételjük a többi sor és oszlop alkotta ugyancsak szimmetrikus, eggyel kisebb méretű mátrixra (ezek az átalakítások az első sort és oszlopot nem befolyásolják). Ugyanígy továbbhaladva, végül egy diagonális mátrixhoz jutunk. ■

Látjuk, hogy a harmadik bizonyítás is egy nagyon kényelmes eljárást ad a diagonális mátrix megkereséséhez. A módszer a megfelelő **A**-ortogonális bázist is előállítja, ha nyomon követjük, hogy az egyes mátrixlépések során hogyan változott a bázis. Ezt ismét az előző bizonyítások után már megvizsgált (7.2.1) példán illusztráljuk.

A kiinduló bázis $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$, a mátrix $\begin{pmatrix} 4 & 2 & 2 \\ 2 & 0 & 2 \\ 2 & 2 & 0 \end{pmatrix}$. A második sorból levonjuk az első sor felét, majd a második oszlopból levonjuk az (új!) első oszlop felét. Ezzel a bázisunk és a mátrixunk a következőképpen változott:

$$\text{Új bázis:} \quad \mathbf{b}_1,\ \mathbf{b}_2 - (1/2)\mathbf{b}_1,\ \mathbf{b}_3, \qquad \text{új mátrix:} \quad \begin{pmatrix} 4 & 0 & 2 \\ 0 & -1 & 1 \\ 2 & 1 & 0 \end{pmatrix}.$$

Most a harmadik sorból/oszlopból vonjuk le az első sor/oszlop felét:

$$\text{Új bázis:} \quad \mathbf{b}_1,\ \mathbf{b}_2 - (1/2)\mathbf{b}_1,\ \mathbf{b}_3 - (1/2)\mathbf{b}_1, \qquad \text{új mátrix:} \quad \begin{pmatrix} 4 & 0 & 0 \\ 0 & -1 & 1 \\ 0 & 1 & -1 \end{pmatrix}.$$

Végül a harmadik sorhoz/oszlophoz adjuk hozzá a második sort/oszlopot:

$$\text{Új bázis:} \quad \mathbf{b}_1,\ \mathbf{b}_2 - (1/2)\mathbf{b}_1,\ \mathbf{b}_3 + \mathbf{b}_2 - \mathbf{b}_1, \qquad \text{új mátrix:} \quad \begin{pmatrix} 4 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Az így nyert **A**-ortogonális bázis ugyanaz, mint amit az első bizonyítás módszerével gyártottunk.

A szimmetrikus bilineáris függvény mátrixát kicsit még tovább „szépíthetjük”: az **A**-ortogonális bázisvektorokat alkalmas skalárszorosukkal helyettesítve az is elérhető, hogy a diagonális mátrix főátlójában csak ± 1 és 0 szerepeljenek. Ezt a bázist használva a bilineáris függvény — a skalárszorzathoz

nagyon hasonló — igen egyszerű alakot ölt. Mindezt pontosan a következő tételben fogalmazzuk meg.

7.2.5 Tétel

Bármely $\mathbf{A}$ szimmetrikus bilineáris függvénynek létezik olyan mátrixa, amelyben a főátló elemei csak az 1, a -1 és a 0 közül kerülhetnek ki, a főátlón kívül pedig minden elem 0.

Az ilyen mátrixot adó bázisban a bilineáris függvény az $\mathbf{A}(\mathbf{u},\mathbf{v}) = \sum_{i=1}^{n} \gamma_i u_i v_i$ alakra egyszerűsödik, ahol $\gamma_i = \pm 1$ vagy 0 és $u_1,\dots,u_n$, illetve $v_1,\dots,v_n$ az $\mathbf{u}$, illetve $\mathbf{v}$ vektorok koordinátáit jelölik. ♣

A skalárszorzat ennek speciális esete, amikor mindegyik $\gamma_i = 1$.

Bizonyítás: Legyen $\mathbf{c}_1,\dots,\mathbf{c}_n$ egy $\mathbf{A}$-ortogonális bázis és $\mathbf{A}(\mathbf{c}_i,\mathbf{c}_i) = \mu_i$. A $\mathbf{c}_i$-ket alkalmas skalárral megszorozva a következőképpen „normáljuk”: ha $\mu_i = 0$, akkor legyen $\mathbf{e}_i = \mathbf{c}_i$, ha pedig $\mu_i \neq 0$, akkor legyen $\mathbf{e}_i = (1/\sqrt{|\mu_i|})\mathbf{c}_i$. [Ez tulajdonképpen az előző tétel harmadik bizonyításában jelzett, de ott fel nem használt (b) típusú átalakítás.] Ekkor az $\mathbf{e}_i$ vektorok is $\mathbf{A}$-ortogonálisak, és $\mathbf{A}(\mathbf{e}_i,\mathbf{e}_i) = \pm 1$, illetve 0, aszerint, hogy μ_i pozitív, negatív, illetve nulla volt. Így az $\mathbf{A}$-nak az $\mathbf{e}_i$ bázisban felírt mátrixa a kívánt tulajdonságú lesz.

A tétel második állítása azonnal adódik a 7.1.4 Tételből. ■

Amint korábban említettük, egy bilineáris függvényhez sokféle $\mathbf{A}$-ortogonális bázis található. A diagonális mátrix azonban bizonyos szempontból már nagyon behatárolt:

7.2.6 Tétel (Tehetetlenségi tétel)

Egy bilineáris függvény diagonális mátrixában (a főátlóban) a pozitív, a negatív és a nulla elemek száma egyértelműen meghatározott. ♣

Bizonyítás: Tekintsük az $\mathbf{A}$ két diagonális mátrixát. Jelölje a főátlóbeli pozitív, negatív és nulla elemek számát a két mátrixban rendre r,s,t, illetve r',s',t' (bármelyik darabszám nulla is lehet, továbbá $r+s+t = r'+s'+t' = \dim V$). Legyen ennek megfelelően az egyik $\mathbf{A}$-ortogonális bázis

$$\mathbf{m}_1,\dots,\mathbf{m}_r,\mathbf{n}_1,\dots,\mathbf{n}_s,\mathbf{o}_1,\dots,\mathbf{o}_t,$$

ahol

$$\mathbf{A}(\mathbf{m}_i,\mathbf{m}_i) > 0,\ \mathbf{A}(\mathbf{n}_j,\mathbf{n}_j) < 0,\ \mathbf{A}(\mathbf{o}_k,\mathbf{o}_k) = 0,$$

a másik bázist pedig hasonló módon alkossák az $\mathbf{m}'_i$, $\mathbf{n}'_j$, $\mathbf{o}'_k$ vektorok.

Először megmutatjuk, hogy a „vesszőtlen” $\mathbf{m}_i\,, \mathbf{o}_k$ és a „vesszős” $\mathbf{n}'_j$ összesen $r+t+s'$ darab vektor (együttesen) lineárisan független rendszert alkot. Tekintsük ehhez egy olyan lineáris kombinációjukat, ami $\mathbf{0}$-t ad, és rendezzük át ezt úgy, hogy a bal oldalra a „vesszőtlen”, a jobb oldalra pedig a „vesszős” vektorok kerüljenek:

$$\mu_1\mathbf{m}_1+\ldots+\mu_r\mathbf{m}_r+\omega_1\mathbf{o}_1+\ldots+\omega_t\mathbf{o}_t=\nu_1\mathbf{n}'_1+\ldots+\nu_{s'}\mathbf{n}'_{s'}\,. \tag{7.2.3}$$

Elég belátnunk, hogy a két oldal közös értéke $\mathbf{0}$. Ekkor ugyanis az $\mathbf{m}_i, \mathbf{o}_k$ vektorok lineáris függetlensége miatt a bal oldalon minden együttható 0, és az $\mathbf{n}'_j$ vektorok függetlenségét felhasználva ugyanez adódik a jobb oldalon is, tehát valóban valamennyi együttható 0.

Jelöljük (7.2.3)-ban a két oldal közös értékét $\mathbf{u}$-val. Mivel $\mathbf{u}$ az $\mathbf{m}_i$ és $\mathbf{o}_k$ vektorok lineáris kombinációja, ezért a bilineáris függvény 7.1.4 Tételbeli képlete szerint

$$\mathbf{A}(\mathbf{u},\mathbf{u})=\sum_{i=1}^{r}\mu_i^2\mathbf{A}(\mathbf{m}_i,\mathbf{m}_i)+\sum_{k=1}^{t}\omega_k^2\mathbf{A}(\mathbf{o}_k,\mathbf{o}_k)\geq 0\,. \tag{7.2.4}$$

Ugyanígy, lévén $\mathbf{u}$ az $\mathbf{n}'_j$ vektorok lineáris kombinációja is,

$$\mathbf{A}(\mathbf{u},\mathbf{u})=\sum_{j=1}^{s'}\nu_j^2\mathbf{A}(\mathbf{n}'_j,\mathbf{n}'_j)\leq 0\,. \tag{7.2.5}$$

A (7.2.4) és (7.2.5) egyenlőtlenségekből kapjuk, hogy $\mathbf{A}(\mathbf{u},\mathbf{u})=0$, és ekkor (7.2.5) alapján valóban csak $\mathbf{u}=\mathbf{0}$ lehetséges.

Ezzel beláttuk, hogy az $\mathbf{m}_i$, $\mathbf{o}_k$ és $\mathbf{n}'_j$ vektorok (együttesen is) lineárisan függetlenek.

Mivel egy lineárisan független rendszer elemszáma nem lehet nagyobb a dimenziónál, így $r+t+s'\leq\dim V=r+t+s$, ahonnan $s'\leq s$. Fordított szereposztással kapjuk, hogy $s\leq s'$, tehát $s=s'$.

Az $\mathbf{m}$-ek és $\mathbf{n}$-ek szerepét felcserélve ugyanígy adódik $r=r'$. Végül $t=\dim V-r-s=\dim V-r'-s'=t'$. ■

Feladatok

7.2.1 Egy bilineáris függvényt *antiszimmetrikus*nak nevezünk, ha minden $\mathbf{u},\mathbf{v}\in V$-re $\mathbf{A}(\mathbf{u},\mathbf{v})=-\mathbf{A}(\mathbf{v},\mathbf{u})$. Mutassuk meg, hogy $\mathbf{A}$ akkor és csak akkor antiszimmetrikus, ha minden $\mathbf{x}\in V$-re $\mathbf{A}(\mathbf{x},\mathbf{x})=0$.

7.2.2 Bizonyítsuk be, hogy minden bilineáris függvény egyértelműen előállítható egy szimmetrikus és egy antiszimmetrikus bilineáris függvény összegeként.

7.2.3 Tekintsük a V-n értelmezett bilineáris függvények B vektorterét, amelyről a 7.1.5 feladatban volt szó.

(a) Mutassuk meg, hogy B-ben a szimmetrikus, illetve antiszimmetrikus függvények egy S, illetve A alteret alkotnak.

(b) Hány dimenziós altér S, illetve A?

(c) Lássuk be, hogy a B vektortér az S és A alterek direkt összege.

7.2.4 Ha $\mathbf{A}$ bilineáris függvény V-n, akkor az $\mathbf{A}$ (pontosabban az $\mathbf{A}$ megszorítása) a V bármely alterén is bilineáris. Legyenek U és W alterek V-ben. Melyek igazak az alábbi állítások közül?

(a) Ha $\mathbf{A}$ szimmetrikus $\langle U, W\rangle$-n, akkor szimmetrikus U-n és W-n is.

(b) Ha $\mathbf{A}$ szimmetrikus U-n és W-n, akkor szimmetrikus $\langle U, W\rangle$-n is.

7.2.5 Legyen $\mathbf{S}$ a szokásos skalárszorzat $\mathbf{R}^4$-ben. Jelölje egy általános $\mathbf{u} \in \mathbf{R}^4$ vektor komponenseit u_1, u_2, u_3, u_4. Adjunk meg $\mathbf{S}$-ortogonális bázist $\mathbf{R}^4$ alábbi alterein:

(a) $U_1 = \{\mathbf{u} \mid u_1 = u_4\}$;

(b) $U_2 = \{\mathbf{u} \mid u_1, \ldots, u_4$ számtani sorozat $\}$;

(c) $U_3 = \{\mathbf{u} \mid \sum_{i=1}^{4} u_i = 0\}$.

7.2.6 Legyen V a legfeljebb 4-edfokú valós együtthatós polinomok (beleértve a 0 polinomot is) szokásos vektortere. Írjuk fel az alábbi szimmetrikus bilineáris függvények egy-egy diagonális mátrixát, és adjunk is meg egy-egy $\mathbf{A}$-ortogonális bázist. Legyen f, g képe

(a) $f(1)g(1)$; (b) fg-ben x^2 együtthatója;

(c) $f(1)g(1) + f(2)g(2) + f(3)g(3) + f(4)g(4) + f(5)g(5)$.

7.2.7 Legyen $\dim V = 3$, az $\mathbf{u}$, illetve $\mathbf{v}$ vektorok koordinátáit egy rögzített $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ bázisban jelölje u_1, u_2, u_3, illetve v_1, v_2, v_3. Adjuk meg az alábbi bilineáris függvények egy-egy diagonális mátrixát és $\mathbf{A}$-ortogonális bázisát.

(a) $\sum_{i,j=1}^{3} iju_iv_j$; (b) $\sum_{i,j=1}^{3}(i+j-1)u_iv_j$.

7.2.8 Bizonyítsuk be, hogy ha az $\mathbf{A}$ szimmetrikus bilineáris függvényhez találhatók olyan $\mathbf{u}, \mathbf{v} \in V$ vektorok, amelyekre $\mathbf{A}(\mathbf{u}, \mathbf{u}) > 0$ és $\mathbf{A}(\mathbf{v}, \mathbf{v}) < 0$, akkor van olyan $\mathbf{0} \neq \mathbf{w} \in V$ is, amelyre $\mathbf{A}(\mathbf{w}, \mathbf{w}) = 0$.

M 7.2.9 Legyen $\dim V = n$, $\mathbf{A}$ egy szimmetrikus bilineáris függvény V-n és $\mathbf{v} \in V$. Lássuk be, hogy a $\mathbf{v}$-re $\mathbf{A}$-ortogonális vektorok alteret alkotnak V-ben. Hány dimenziós lehet ez az altér?

M 7.2.10 Nevezzünk két, ugyanazon a V vektortéren értelmezett bilineáris függvényt, $\mathbf{A}$-t és $\mathbf{B}$-t ekvivalensnek, ha „van közös mátrixuk", azaz van olyan $\mathbf{a}_1, \ldots, \mathbf{a}_n$, illetve $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázis, hogy $[\mathbf{B}]_b = [\mathbf{A}]_a$. Hány páronként nemekvivalens szimmetrikus bilineáris függvény létezik V-n?

7.3. Kvadratikus alak

Az előző pontban már láttuk, hogy az $\mathbf{A}(\mathbf{u}, \mathbf{u})$ értékek fontos szerepet játszanak az $\mathbf{A}$ bilineáris függvény vizsgálatánál.

7.3.1 Definíció
Az $\tilde{\mathbf{A}}(\mathbf{x}) = \mathbf{A}(\mathbf{x}, \mathbf{x}) : V \to \mathbf{R}$ függvényt az $\mathbf{A}$ bilineáris függvényhez tartozó *kvadratikus alak*nak nevezzük. ♣

A kvadratikus alak tehát tulajdonképpen a bilineáris függvény egy megszorítása, amikor mindkét változó helyére azonos vektort írunk. Így minden kvadratikus alak valamilyen bilineáris függvényből származik.

Egy bilineáris függvény nyilván egyértelműen meghatároz egy kvadratikus alakot. Ennek a megfordítása nem igaz, ugyanaz a kvadratikus alak több bilineáris függvényből is létrejöhet. Érvényes azonban, hogy a *szimmetrikus* bilineáris függvények és a kvadratikus alakok között már kölcsönösen egyértelmű a kapcsolat (lásd a 7.3.1 feladatot). Ennek megfelelően a kvadratikus alakokat mindig szimmetrikus bilineáris függvényből származóknak fogjuk tekinteni.

A 7.1.4 Tétel képletei szerint a kvadratikus alak

$$\tilde{\mathbf{A}}(\mathbf{x}) = [\mathbf{x}]^T [\mathbf{A}][\mathbf{x}] = \sum_{i,j=1}^{n} \alpha_{ij} x_i x_j$$

formában írható fel, ahol $x_1, \ldots, x_n$ az $\mathbf{x}$ vektor koordinátái az adott bázisban. Ez a kifejezés az x_i-knek (homogén) másodfokú polinomja, ez indokolja a kvadratikus alak elnevezést.

Tekintsük most a bilineáris függvény egy olyan mátrixát, amely diagonális és a főátlóban csak ± 1, illetve 0 áll. Az ennek megfelelő $\mathbf{A}$-ortogonális bázisban a kvadratikus alak a 7.2.5 Tétel szerint *előjeles négyzetösszeg*gé válik,

azaz $\tilde{\mathbf{A}}(\mathbf{x}) = \sum_{i=1}^{n} \gamma_i x_i^2$ alakú lesz, ahol $\gamma_i = \pm 1$ vagy 0. Ennek fontos speciális esete, hogy a skalárszorzathoz tartozó kvadratikus alak a koordináták négyzetösszegével egyenlő.

Nézzük meg, hogyan kaphatjuk meg a gyakorlatban ezt az előjeles négyzetösszeget. Vegyük ismét a 7.2.3 Tétel különféle bizonyításainak illusztrálására választott

$$\mathbf{A}(\mathbf{u},\mathbf{v}) = 4u_1v_1 + 2u_1v_2 + 2u_2v_1 + 2u_1v_3 + 2u_3v_1 + 2u_2v_3 + 2u_3v_2 \quad (7.2.1)$$

szimmetrikus bilineáris függvényt. Az ehhez tartozó kvadratikus alak

$$\tilde{\mathbf{A}}(\mathbf{x}) = 4x_1^2 + 4x_1x_2 + 4x_1x_3 + 4x_2x_3\,.$$

Itt x_1, x_2, x_3 az $\mathbf{x}$ vektornak az eredeti $\mathbf{b}_i$ bázis szerinti koordinátái. Nézzünk olyan diagonális mátrixot, amelynek a főátlójában minden γ_i elem ± 1 vagy 0. Ha az ennek megfelelő bázisban felírt koordináták $\hat{x}_1, \hat{x}_2, \hat{x}_3$, akkor $\tilde{\mathbf{A}}(\mathbf{x}) = \gamma_1\hat{x}_1^2 + \gamma_2\hat{x}_2^2 + \gamma_3\hat{x}_3^2$. Ezért azt kell kiszámítani, hogy a diagonális bázis szerinti $\hat{x}_1, \hat{x}_2, \hat{x}_3$ koordináták hogyan kaphatók meg az eredeti x_1, x_2, x_3 koordinátákból. Erre vannak elég egyszerű általános módszerek, mi azonban megelégszünk a konkrét eset vizsgálatával.

A legkönnyebben a harmadik bizonyítást követve érhetünk célhoz. Emlékezzünk vissza, hogy ott a mátrixon szimmetrikusan elemi sor/oszlop-ekvivalens átalakításokat hajtottunk végre, és közben nyomon követtük a bázis változását is. Egy füst alatt a koordináták változását is regisztrálhatjuk, és így az eljárás végén azonnal megkapjuk a keresett $\hat{x}_1, \hat{x}_2, \hat{x}_3$ koordinátákat.

Nézzük a konkrét esetet. Az első lépésben a $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ bázisból a $\mathbf{b}_1$, $\mathbf{b}_2 - (1/2)\mathbf{b}_1$, $\mathbf{b}_3$ bázisra tértünk át. Könnyen láthatóan ekkor csak az x_1 koordinátát kell módosítani az x_2 segítségével, mégpedig „fordítva”, mint ahogy a $\mathbf{b}_2$ báziselemet a $\mathbf{b}_1$-gyel megváltoztattuk. Az új koordináták ekkor $x_1 + (1/2)x_2$, x_2 , x_3 , hiszen

$$x_1\mathbf{b}_1 + x_2\mathbf{b}_2 + x_3\mathbf{b}_3 = [x_1 + (1/2)x_2]\mathbf{b}_1 + x_2[\mathbf{b}_2 - (1/2)\mathbf{b}_1] + x_3\mathbf{b}_3\,.$$

Hasonlóan követve a további két átalakítást, ennek során a koordináták a következőképpen módosulnak: $x_1 + (1/2)x_2 + (1/2)x_3$, x_2 , x_3, majd $x_1+(1/2)x_2+(1/2)x_3$, x_2-x_3 , x_3. Végül a $\begin{pmatrix} 4 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ diagonális mátrixot „normáljuk”: az első sort és oszlopot felezve az $\begin{pmatrix} 1 & 0 & 0 \\ 0 & -1 & 0 \\ 0 & 0 & 0 \end{pmatrix}$ mátrixhoz jutunk, ekkor az (aktuális) első báziselem 1/2-del szorzódott, az első koordináta

ennek megfelelően megduplázódott, így $2x_1 + x_2 + x_3\,,\ x_2 - x_3\,,\ x_3$ adódik. Ezek már a keresett $\hat{x}_i$ koordináták, hiszen a mátrix diagonális és az átló elemei $1, -1, 0$. Mindezek alapján az

$$\tilde{\mathbf{A}}(\mathbf{x}) = \hat{x}_1^2 - \hat{x}_2^2 = (2x_1 + x_2 + x_3)^2 - (x_2 - x_3)^2$$

előjeles négyzetösszeg előállítást kapjuk.

Ha nem lépésenként követjük nyomon a koordináták változását, akkor eljárhatunk pl. úgy, hogy az $\mathbf{x} = \sum x_i \mathbf{b}_i = \sum \hat{x}_i \hat{\mathbf{b}}_i$ egyenlőségbe beírjuk az új $\hat{\mathbf{b}}_i$ bázisvektorok előállítását az eredeti $\mathbf{b}_i$-k segítségével, majd ezután a két oldalon a $\mathbf{b}_i$-k együtthatóit összehasonlítva egy lineáris egyenletrendszer adódik a keresett $\hat{x}_i$ koordinátákra, amit (pl. Gauss-kiküszöböléssel) megoldunk.

Egy kvadratikus alak ilyen előjeles négyzetösszegként történő előállítása többféleképpen is megvalósulhat, hiszen sokféle megfelelő $\mathbf{A}$-ortogonális bázist találhatunk. (Bármelyik előállításban azonban mindig ugyanannyi a pozitív, a negatív és a nulla előjelű tagok száma, ezt a tehetetlenségi tétel garantálja.)

Hangsúlyozzuk, hogy a tárgyalt előjeles négyzetösszegek nem lehetnek akármilyenek, hanem csakis olyanok, amelyeket egy alkalmas $\mathbf{A}$-ortogonális bázis szerinti koordinátákból írtunk fel; ez éppen a négyzetösszeg tagjainak a (pontosan megfogalmazható értelemben vett) lineáris függetlenségét jelenti.

Most a kvadratikus alakok különböző típusainak az áttekintésére térünk rá. Bármely kvadratikus alakra $\tilde{\mathbf{A}}(\mathbf{0}) = 0$. A többi vektoron felvett értékektől függően a nem azonosan nulla kvadratikus alakokat (és ennek alapján a szimmetrikus bilineáris függvényeket) a következőképpen osztályozzuk:

7.3.2 Definíció

Az $\mathbf{A} \neq \mathbf{0}$ szimmetrikus bilineáris függvényhez tartozó $\tilde{\mathbf{A}}$ kvadratikus alak

(PD) *pozitív definit*, ha minden $\mathbf{x} \neq \mathbf{0}$-ra $\tilde{\mathbf{A}}(\mathbf{x}) > 0$;
(ND) *negatív definit*, ha minden $\mathbf{x} \neq \mathbf{0}$-ra $\tilde{\mathbf{A}}(\mathbf{x}) < 0$;
(PSZ) *pozitív szemidefinit*, ha minden $\mathbf{x}$-re $\tilde{\mathbf{A}}(\mathbf{x}) \geq 0$, és van olyan $\mathbf{x} \neq \mathbf{0}$, hogy $\tilde{\mathbf{A}}(\mathbf{x}) = 0$;
(NSZ) *negatív szemidefinit*, ha minden $\mathbf{x}$-re $\tilde{\mathbf{A}}(\mathbf{x}) \leq 0$, és van olyan $\mathbf{x} \neq \mathbf{0}$, hogy $\tilde{\mathbf{A}}(\mathbf{x}) = 0$; és végül
(I) *indefinit*, ha $\tilde{\mathbf{A}}(\mathbf{x})$ felvesz pozitív és negatív értéket is. ♣

A kvadratikus alak jellege igen egyszerűen leolvasható a bilineáris függvény diagonális mátrixából:

7.3.3 Tétel

Tekintsük az $\mathbf{A}$ szimmetrikus bilineáris függvény egy diagonális mátrixát. Ekkor $\mathbf{A}$ (illetve $\tilde{\mathbf{A}}$) pontosan akkor

- azonosan nulla, ha a főátló minden eleme nulla;
- pozitív definit, ha a főátló minden eleme pozitív;
- negatív definit, ha a főátló minden eleme negatív;
- pozitív szemidefinit, ha a főátlóban van pozitív és nulla elem is, de negatív nincs;
- negatív szemidefinit, ha a főátlóban van negatív és nulla elem is, de pozitív nincs;
- indefinit, ha a főátlóban van pozitív és negatív elem is. ♣

Bizonyítás: Az állítások a kvadratikus alak előjeles négyzetösszegként való felírásából azonnal következnek. ■

Megjegyezzük, hogy indefinit esetben a diagonális mátrix főátlójában előfordul*hat* nulla is, de ez nem minden indefinit alaknál teljesül.

Gyakran szükségünk van arra, hogy a kvadratikus alak jellegét *akármelyik* mátrixából (diagonalizálás nélkül) eldönthessük. Erre igazán jó kritérium csak definit alakok esetén adható, ezt bizonyítás nélkül közöljük.

7.3.4 Tétel

Tekintsük az $\mathbf{A}$ szimmetrikus bilineáris függvény egy tetszőleges $A \in \mathbf{R}^{n\times n}$ mátrixát.

Az $\mathbf{A}$ akkor és csak akkor pozitív definit, ha minden $k \leq n$-re az A bal felső sarkában levő k-adrendű aldeterminánsa pozitív.

Az $\mathbf{A}$ akkor és csak akkor negatív definit, ha minden $k \leq n$-re az A bal felső sarkában levő k-adrendű aldeterminánsa aszerint pozitív, illetve negatív, hogy k páros, illetve páratlan. ♣

Mint a fejezet bevezetőjében már említettük, a kvadratikus alakok természetes módon merülnek fel a geometriában a másodrendű görbék és felületek leírásánál, de számos további alkalmazásuk is van a matematika különféle területein.

Végül megjegyezzük, hogy a pozitív definit $\mathbf{A}$-k kulcsfontosságú szerepet játszanak majd a következő fejezetben.

Feladatok

7.3.1

(a) Bizonyítsuk be, hogy az $\mathbf{A}$ és $\mathbf{B}$ (nem feltétlenül szimmetrikus) bilineáris függvényekhez akkor és csak akkor tartozik ugyanaz a kvadratikus alak, ha $\mathbf{A}-\mathbf{B}$ antiszimmetrikus (a definíciót lásd a 7.2.1 feladatban).

(b) Igazoljuk, hogy a szimmetrikus bilineáris függvények és a kvadratikus alakok között kölcsönösen egyértelmű kapcsolat áll fenn.

7.3.2 Állapítsuk meg a 7.2.5–7.2.7 feladatokban szereplő szimmetrikus bilineáris függvények (illetve a hozzájuk tartozó kvadratikus alakok) jellegét.

7.3.3 Mi a különböző jellegű kvadratikus alakok értékkészlete? Mennyiben változik a helyzet, ha csak a nem nulla vektorokon felvett értékeket vesszük figyelembe?

7.3.4 Legyen $\tilde{\mathbf{A}}$ az $\mathbf{A}$ szimmetrikus bilineáris függvényhez tartozó kvadratikus alak.

(a) Hogyan kaphatjuk meg $\tilde{\mathbf{A}}(\lambda\mathbf{x})$ értékét $\tilde{\mathbf{A}}(\mathbf{x})$-ből?

(b) Mi a szükséges és elégséges feltétele (adott $\mathbf{x}$ és $\mathbf{z}$ mellett) $\tilde{\mathbf{A}}(\mathbf{x}+\mathbf{z}) = \tilde{\mathbf{A}}(\mathbf{x}) + \tilde{\mathbf{A}}(\mathbf{z})$ teljesülésének?

7.3.5

(a) Milyen jellegű lesz a $\lambda\mathbf{A}$ (szimmetrikus) bilineáris függvény (λ-tól és $\mathbf{A}$ jellegétől függően)?

(b) Milyen jellegű lehet $\mathbf{A}+\mathbf{B}$, ha $\mathbf{A}$ és $\mathbf{B}$ egymástól függetlenül pozitív/negatív definit/szemidefinit, illetve indefinit?

7.3.6 Írjuk át az alábbi (3-dimenziós) kvadratikus alakokat előjeles négyzetösszeggé:

(a) x_1x_2; (b) $x_1x_2 + x_2x_3$;

(c) $x_1x_2 + x_2x_3 + x_3x_1$; (d) $x_1^2 - 3x_3^2 - 2x_1x_2 + 2x_1x_3 - 6x_2x_3$;

(e) $x_1^2 + x_2^2 + 3x_3^2 + 4x_1x_2 + 2x_1x_3 + 2x_2x_3$.

7.3.7 Írjuk át az alábbi (4-dimenziós) kvadratikus alakokat előjeles négyzetösszeggé:

(a) $\sum_{i,j=1}^{4} x_ix_j$; (b) $x_1x_2 + x_2x_3 + x_3x_4$;

(c) $x_1x_2 + x_2x_3 + x_3x_4 + x_4x_1$; (d) $\sum_{i<j} x_ix_j$.

7.3.8 Hol a hiba az alábbi okoskodásban?
Tekintsük az $x_1^2+x_2^2+(x_1+x_2)^2 = (x_1\sqrt{3})^2+(x_2\sqrt{3})^2-(x_1-x_2)^2$ kvadratikus alakot. Mindkét felírás előjeles négyzetösszeg, azonban az egyik felírásban három pozitív együttható szerepel, a másik felírásban viszont van negatív is. Ez (látszólag) ellentmond a tehetetlenségi tételnek.

7.3.9 Mutassuk meg, hogy egy szimmetrikus bilineáris függvény mátrixának a determinánsa általában megváltozik, ha más bázisra térünk át, azonban a determináns előjele (tehát, hogy a determináns pozitív, negatív vagy nulla) nem függ a bázis megválasztásától.

7.3.10 Melyek igazak az alábbi állítások közül?
(a) Ha $\mathbf{A}$ pozitív vagy negatív definit, akkor $\det[\mathbf{A}] \neq 0$.
(b) Ha $\det[\mathbf{A}] \neq 0$, akkor $\mathbf{A}$ pozitív vagy negatív definit.

7.3.11 Határozzuk meg a páronként nemekvivalens pozitív/negatív definit/szemidefinit, illetve indefinit szimmetrikus bilineáris függvények számát egy n-dimenziós V-n. (Az „ekvivalens” szó jelentését lásd a 7.2.10 feladatban.)

7.3.12 Mely $\mathbf{A}$ szimmetrikus bilineáris függvényekre teljesül az alábbi állítás: Ha az $\mathbf{a}_1, \ldots, \mathbf{a}_k$ nem nulla vektorok páronként $\mathbf{A}$-ortogonálisak, akkor szükségképpen lineárisan függetlenek.

M*7.3.13 Melyek azok az $\mathbf{A}$ szimmetrikus bilineáris függvények, amelyekre bármely $\mathbf{v} \neq \mathbf{0}$ vektor eleme egy alkalmas $\mathbf{A}$-ortogonális bázisnak?

M*7.3.14 Nevezzük az $\tilde{\mathbf{A}}$ kvadratikus alak *mag*jának a „gyökei” halmazát:

$$\operatorname{Ker}\tilde{\mathbf{A}} = \{\mathbf{v} \in V \mid \tilde{\mathbf{A}}(\mathbf{v}) = 0\}.$$

(a) Mely kvadratikus alakokra lesz a mag altér?
(b) Mely kvadratikus alakokra választható ki a magból V-nek egy bázisa?
(c) Mennyi a magban található lineárisan független rendszerek elemszámának a maximuma?
(d) Mennyi a magban található alterek dimenziójának a maximuma?

7.4. Komplex bilineáris függvény

Ebben a pontban V egy véges dimenziós vektorteret jelent a komplex test felett. A bilineáris függvényeket úgy szeretnénk értelmezni, hogy az ortogonalizációval és a kvadratikus alakokkal kapcsolatos eredmények a komplex esetre is átvihetők legyenek.

Ha változtatás nélkül fenntartanánk a 7.1.1 Definíciót, akkor $\mathbf{A}(i\mathbf{x}, i\mathbf{x}) = i^2\mathbf{A}(\mathbf{x},\mathbf{x}) = -\mathbf{A}(\mathbf{x},\mathbf{x})$ miatt például nem léteznének definit vagy szemidefinit kvadratikus alakok. Ezért és más hasonló okok miatt annyit módosítunk a bilineáris függvény definícióján, hogy az *első* változót λ-val megszorozva a függvényérték nem λ-val, hanem annak komplex konjugáltjával, $\overline{\lambda}$-tal szorzódik (a többi kikötés, tehát az összegre bontások és a második változóból a skalár kiemelése *változatlan* marad). Azaz:

7.4.1 Definíció

Az $\mathbf{A} : V \times V \to \mathbf{C}$ leképezést (komplex) *bilineáris függvény*nek nevezzük, ha (a 7.1.1 Definíció képletszámozása szerint)

(ii) $\mathbf{A}(\mathbf{u}+\mathbf{u}',\mathbf{v}) = \mathbf{A}(\mathbf{u},\mathbf{v}) + \mathbf{A}(\mathbf{u}',\mathbf{v})$;

!(iii)! $\mathbf{A}(\lambda\mathbf{u},\mathbf{v}) = \overline{\lambda}\mathbf{A}(\mathbf{u},\mathbf{v})$ ← **FIGYELEM!** Itt a jobb oldalon lambda *konjugáltja* szerepel;

(iv) $\mathbf{A}(\mathbf{u},\mathbf{v}+\mathbf{v}') = \mathbf{A}(\mathbf{u},\mathbf{v}) + \mathbf{A}(\mathbf{u},\mathbf{v}')$;

(v) $\mathbf{A}(\mathbf{u},\lambda\mathbf{v}) = \lambda\mathbf{A}(\mathbf{u},\mathbf{v})$. ♣

A valósban látottakhoz hasonlóan a komplex bilineáris függvények is jellemezhetők a báziselemek képével (7.1.2 Tétel, csak a bilineáris függvénynek most kicsit módosul a képlete, lásd alább), és ugyanúgy definiáljuk most is a bilineáris függvény mátrixát (7.1.3 Definíció). A 7.1.4 Tételben a (7.1.1) és (7.1.2) előállítások annyiban változnak, hogy az *első* vektor koordinátái helyére azok komplex konjugáltjait kell írni:

7.4.2 Tétel

Jelölje az $\mathbf{A}$ komplex bilineáris függvény mátrixának elemeit egy adott bázisban α_{ij}, az $\mathbf{u}$, illetve $\mathbf{v}$ vektorok koordinátáit pedig $u_1,\dots,u_n$, illetve $v_1,\dots,v_n$. Ekkor

$$\mathbf{A}(\mathbf{u},\mathbf{v}) = \sum_{i,j=1}^{n} \alpha_{ij}\overline{u_i}v_j = [\mathbf{u}]^*[\mathbf{A}][\mathbf{v}] =$$

$$= (\overline{u_1},\overline{u_2},\dots,\overline{u_n}) \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix} \begin{pmatrix} v_1 \\ v_2 \\ \vdots \\ v_n \end{pmatrix},$$

ahol a * a mátrix *adjungált*ját (azaz transzponáltjának a konjugáltját) jelenti. ♣

A bizonyítás teljesen hasonlóan történik, mint a valós esetben. (A jövőben is csak azokat a bizonyításokat részletezzük, ahol jelentős eltérés van a valós bilineáris függvényekhez képest.)

Tekintsük most a kvadratikus alak problémáját (még az ortogonalizáció előtt). A kvadratikus alak definíciója (és $\tilde{\mathbf{A}}$ jelölése) változatlan (7.3.1 Definíció). Először azt igazoljuk, hogy a valós esettől eltérően itt a kvadratikus alak egyértelműen meghatározza a(z őt származtató) bilineáris függvényt, vagyis komplex esetben kölcsönösen egyértelmű kapcsolat áll fenn a kvadratikus alakok és az *összes* bilineáris függvény között.

7.4.3 Tétel

Minden kvadratikus alak pontosan egy bilineáris függvényből származik. ♣

Bizonyítás: Ki fogjuk fejezni $\mathbf{A}(\mathbf{u},\mathbf{v})$-t az $\tilde{\mathbf{A}}(\mathbf{x}) = \mathbf{A}(\mathbf{x},\mathbf{x})$ értékek segítségével. Ehhez „fejtsük ki" az $\tilde{\mathbf{A}}(\mathbf{u}+\mathbf{v})$, illetve $\tilde{\mathbf{A}}(\mathbf{u}+i\mathbf{v})$ kifejezéseket:

$$\mathbf{A}(\mathbf{u}+\mathbf{v},\mathbf{u}+\mathbf{v}) = \mathbf{A}(\mathbf{u},\mathbf{u}) + \mathbf{A}(\mathbf{u},\mathbf{v}) + \mathbf{A}(\mathbf{v},\mathbf{u}) + \mathbf{A}(\mathbf{v},\mathbf{v})\,,$$
$$\mathbf{A}(\mathbf{u}+i\mathbf{v},\mathbf{u}+i\mathbf{v}) = \mathbf{A}(\mathbf{u},\mathbf{u}) + i\mathbf{A}(\mathbf{u},\mathbf{v}) - i\mathbf{A}(\mathbf{v},\mathbf{u}) + \mathbf{A}(\mathbf{v},\mathbf{v})\,.$$

A második egyenlőséghez az első i-szeresét hozzáadva $\mathbf{A}(\mathbf{v},\mathbf{u})$ kiesik és így $\mathbf{A}(\mathbf{u},\mathbf{v})$ (egyértelműen) kifejezhető a kvadratikus alak $\mathbf{u}, \mathbf{v}, \mathbf{u}+\mathbf{v}$ és $\mathbf{u}+i\mathbf{v}$ helyeken felvett értékeivel. ■

Egy komplex bilineáris függvény esetén általában a kvadratikus alak is komplex értékű. A definit, szemidefinit, illetve indefinit jelleg eleve csak akkor értelmezhető, ha a kvadratikus alak csak valós értékeket vesz fel. Az alábbiakban ennek teljesülésére adunk egy egyszerű szükséges és elégséges feltételt.

7.4.4 Tétel

Az $\tilde{\mathbf{A}}$ kvadratikus alak akkor és csak akkor vesz fel csupa valós értéket, ha minden $\mathbf{u},\mathbf{v}$ vektorra $\mathbf{A}(\mathbf{u},\mathbf{v}) = \overline{\mathbf{A}(\mathbf{v},\mathbf{u})}$.

Az ilyen tulajdonságú $\mathbf{A}$-kat *Hermite-féle* vagy *ermitikus* bilineáris függvényeknek nevezzük. [A francia Hermite név szóeleji h-ját (valamint szóvégi e-jét) nem ejtjük, és ezért ez a h betű az ermitikus jelzőből már ki is marad.] Szokásos még az *önadjungált* bilineáris függvény elnevezés is (magyarázatát lásd alább, az ermitikus függvény mátrixánál). ♣

Bizonyítás: Ha $\mathbf{A}(\mathbf{u},\mathbf{v}) = \overline{\mathbf{A}(\mathbf{v},\mathbf{u})}$, akkor ezt speciálisan $\mathbf{u} = \mathbf{v} = \mathbf{x}$-re alkalmazva $\mathbf{A}(\mathbf{x},\mathbf{x}) = \overline{\mathbf{A}(\mathbf{x},\mathbf{x})}$ adódik. Így $\tilde{\mathbf{A}}(\mathbf{x})$ megegyezik a konjugáltjával,

tehát valós szám. Ezzel beláttuk, hogy a kvadratikus alak csak valós értékeket vehet fel.

Megfordítva, tegyük fel, hogy a kvadratikus alak csak valós értékeket vesz fel. Az előző tétel bizonyításában szereplő két „egyenletből" ekkor azt kapjuk, hogy $\mathbf{A}(\mathbf{u},\mathbf{v})+\mathbf{A}(\mathbf{v},\mathbf{u})$ és $i[\mathbf{A}(\mathbf{u},\mathbf{v})-\mathbf{A}(\mathbf{v},\mathbf{u})]$ is valós. Innen rögtön adódik, hogy $\mathbf{A}(\mathbf{u},\mathbf{v})$ és $\mathbf{A}(\mathbf{v},\mathbf{u})$ csak egymás konjugáltjai lehetnek. ■

A továbbiakban csak ermitikus bilineáris függvényekkel foglalkozunk. Ezekre értelemszerű módosításokkal átvihetők a valósban megismert fogalmak és eredmények. Az alábbi felsorolásban ezeket röviden összefoglaljuk.

Egy bilineáris függvény akkor és csak akkor ermitikus, ha (akármelyik bázisban felírt) mátrixa *önadjungált*, azaz megegyezik az adjungáltjával. (A 7.2.2 Tétel megfelelője.) Az önadjungáltság következménye, hogy a mátrix főátlójának minden eleme valós szám.

Minden ermitikus bilineáris függvénynek létezik diagonális mátrixa. (A 7.2.3 Tétel megfelelője. A három bizonyítás bármelyike különösebb nehézség nélkül átvihető a komplex esetre.) Az önadjungáltság miatt a diagonális mátrix főátlójában (és így az egész mátrixban is) csupa valós szám áll.

Legyen A ermitikus bilineáris függvény. Az $\mathbf{u},\mathbf{v}\in V$ vektorok $\mathbf{A}$-*ortogonális*ak, ha $\mathbf{A}(\mathbf{u},\mathbf{v})=0$. (A 7.2.4 Definíció megfelelője.)

Bármely ermitikus bilineáris függvénynek létezik olyan mátrixa, amelyben a főátló elemei csak az 1, a -1 és a 0 közül kerülhetnek ki, a főátlón kívül pedig minden elem 0. Az ilyen mátrixot adó bázisban a bilineáris függvény az $\mathbf{A}(\mathbf{u},\mathbf{v})=\sum_{j=1}^{n}\gamma_j\overline{u_j}v_j$ alakra egyszerűsödik, ahol $\gamma_j=\pm1$ vagy 0 és $u_1,\dots,u_n$, illetve $v_1,\dots,v_n$ az $\mathbf{u}$, illetve $\mathbf{v}$ vektorok koordinátáit jelölik. A kvadratikus alak előjeles négyzetösszeg előállítása ennek megfelelően

$$\tilde{\mathbf{A}}(\mathbf{x})=\sum_{j=1}^{n}\gamma_j\overline{x_j}x_j=\sum_{j=1}^{n}\gamma_j|x_j|^2$$

alakú lesz. (A 7.2.5 Tétel megfelelője.)

Egy ermitikus bilineáris függvény diagonális mátrixában (a főátlóban) a pozitív, a negatív és a nulla elemek száma egyértelműen meghatározott. (A 7.2.6 Tehetetlenségi Tétel megfelelője. Mint már említettük, a diagonális mátrixban minden elem valós.)

Végül a kvadratikus alakok (pozitív/negatív definit/szemidefinit, illetve indefinit) jellegének a definíciója és az erre vonatkozó eredmények megegyeznek a valós esetben látottakkal. (A 7.3.2 Definíció és a 7.3.3–7.3.4 Tételek megfelelői; értelemszerűen mindenhová „szimmetrikus" helyett „ermitikus"-t és — az utolsó tételben — $\mathbf{R}$ helyett $\mathbf{C}$-t kell írni.)

Feladatok

A feladatokban a komplex test feletti véges dimenziós vektortéren értelmezett komplex bilineáris függvények szerepelnek.

7.4.1 Hogyan célszerű módosítani a skalárszorzat definícióját a komplex esetre?

7.4.2 Adjuk meg a komplex bilineáris függvények közül a szimmetrikusakat [azaz amelyeknél minden $\mathbf{u}, \mathbf{v}$-re $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \mathbf{A}(\mathbf{v}, \mathbf{u})$ teljesül].

7.4.3 Melyek igazak az alábbi állítások közül (az A négyzetes, komplex elemű mátrix)?

(a) Ha A önadjungált mátrix, akkor $\det A$ valós szám.
(b) Ha $\det A$ valós szám, akkor A önadjungált mátrix.

7.4.4 Oldjuk meg a 7.1.6 feladatot komplex bilineáris függvényre.

7.4.5 Gondoljuk végig a 7.2.3 ortogonalizációs tétel mindhárom bizonyítását a komplex esetre is.

7.4.6 Határozzuk meg az alábbi mátrixokkal megadott ermitikus bilineáris függvények egy-egy diagonális mátrixát, $\mathbf{A}$-ortogonális bázisát, a kvadratikus alak jellegét, és írjuk is fel a kvadratikus alakot előjeles négyzetösszegként:

$$\text{(a)} \begin{pmatrix} 1 & i \\ -i & 1 \end{pmatrix}; \qquad \text{(b)} \begin{pmatrix} 0 & i \\ -i & 0 \end{pmatrix}; \qquad \text{(c)} \begin{pmatrix} 1 & \rho & \rho^2 \\ \rho^2 & 1 & \rho \\ \rho & \rho^2 & 1 \end{pmatrix},$$

ahol $\rho = \cos 120^\circ + i \sin 120^\circ$.

7.4.7 Mi lehet egy ermitikus kvadratikus alak értékkészlete? Mutassunk példát arra, hogy tetszőleges bilineáris függvényt megengedve sokkal változatosabb képet kapunk: a kvadratikus alak értékkészlete lehet a komplex sík bármelyik, origón átmenő egyenese, ilyen egyenes által határolt félsík, origó végpontú félegyenes, az egész sík és origó csúcsú tetszőleges szögtartomány is.

7.4.8 Nevezzünk egy $\mathbf{F}$ bilineáris függvényt *ferdén ermitikus*nak, ha minden $\mathbf{u}, \mathbf{v}$-re $\mathbf{F}(\mathbf{u}, \mathbf{v}) = -\overline{\mathbf{F}(\mathbf{v}, \mathbf{u})}$.

(a) Hogyan ismerhető fel egy ferdén ermitikus függvény a(z akármilyen bázisban felírt) mátrixáról?

(b) Bizonyítsuk be, hogy a ferdén ermitikus függvények éppen az ermitikus függvények i-szeresei.

(c) Hogyan ismerhető fel egy ferdén ermitikus függvény a hozzá tartozó kvadratikus alakról?

(d) Lássuk be, hogy minden komplex bilineáris függvény egyértelműen írható fel egy ermitikus és egy ferdén ermitikus függvény összegeként.

7.4.9 Melyek igazak az alábbi állítások közül?

(a) Ha $\mathbf{A}$-nak létezik diagonális mátrixa, akkor $\mathbf{A}$ ermitikus.

(b) Bármely $\mathbf{A}$ esetén két vektor $\mathbf{A}$-ortogonalitása szimmetrikus fogalom, azaz $\mathbf{A}(\mathbf{u},\mathbf{v}) = 0 \iff \mathbf{A}(\mathbf{v},\mathbf{u}) = 0$.

(c) Ha $\mathbf{A}$ ermitikus, akkor $\mathbf{A}(\mathbf{u},\mathbf{v}) = 0 \iff \mathbf{A}(\mathbf{v},\mathbf{u}) = 0$.

(d) Ha $\mathbf{A}(\mathbf{u},\mathbf{v}) = 0 \iff \mathbf{A}(\mathbf{v},\mathbf{u}) = 0$, akkor $\mathbf{A}$ ermitikus.

*7.4.10 Bizonyítsuk be, hogy az $\mathbf{A}(\mathbf{u},\mathbf{v}) = 0 \iff \mathbf{A}(\mathbf{v},\mathbf{u}) = 0$ tulajdonsággal pontosan az ermitikus függvények skalárszorosai rendelkeznek.

8. EUKLIDESZI TEREK

Az euklideszi tér a (közönséges) síknak, illetve térnek a legközvetlenebb általánosítása: skalárszorzattal ellátott vektorteret jelent. A skalárszorzat segítségével nemcsak a merőlegesség, hanem a hosszúság, a távolság és — valós esetben — a szög is értelmezhető, és ezekre a geometriából megszokott tulajdonságok jelentős része érvényben marad. A szokásos merőleges egységvektoroknak az ortonormált bázis felel meg. Az euklideszi tér lineáris transzformációit vizsgálva fontos szerephez jut az adjungált transzformáció. Külön is foglalkozunk néhány olyan transzformációtípussal, amely speciális kapcsolatban áll az adjungáltjával. Azt is meghatározzuk, mely transzformációknál létezik sajátvektorokból álló ortonormált bázis (azaz mely transzformációknak van olyan diagonális mátrixa, amelyet merőleges egységvektorok szerint írtunk fel); itt eltérő választ kapunk a valós és a komplex esetben.

8.1. Valós euklideszi tér

Ebben a pontban kizárólag a valós test feletti véges dimenziós vektorterekkel foglalkozunk, bár az eredmények egy része átvihető végtelen dimenzióra is (lásd a 8.1.15–8.1.17 feladatokat).

A geometriából ismert skalárszorzatból indulunk ki, ami két sík-, illetve térvektorhoz a szokásos Descartes-féle koordinátáik szorzatösszegét rendeli. Ezt általánosítja az alábbi

8.1.1 Definíció

Legyen $\mathbf{e}_1, \ldots, \mathbf{e}_n$ *rögzített* bázis V-ben. Ekkor az adott bázis szerint vett *skalárszorzat*on (más szóhasználattal: *skaláris szorzat*on, *belső szorzat*on) azt az $\mathbf{S} : V \times V \to \mathbf{R}$ függvényt értjük, amely két vektorhoz a koordinátáik szorzatösszegét rendeli:

$$\mathbf{S}(\mathbf{x}, \mathbf{z}) = \mathbf{x} \cdot \mathbf{z} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \cdot \begin{pmatrix} z_1 \\ \vdots \\ z_n \end{pmatrix} = \sum_{j=1}^{n} x_j z_j \,. \ \clubsuit$$

Két vektor skalárszorzatát a közéjük írt ponttal fogjuk jelölni.

A fentiekben (a jelöléstől eltekintve) tulajdonképpen megismételtük a 7.1 pont P1 és P2 példáját.

Véletlenül se keverjük össze a „skalárszorzat" szót a hasonló hangzású „skalárszoros", illetve „skalárral való szorzás" kifejezésekkel: a skalárszorzat két vektorhoz egy skalárt (egy valós számot) rendel, az utóbbiak pedig egy vektort (mátrixot, leképezést stb.) szoroznak meg egy skalárral, aminek az eredménye ismét egy vektor (mátrix, leképezés stb.) lesz.

Rátérve a skalárszorzat tulajdonságaira, azonnal adódik, hogy a skalárszorzat szimmetrikus bilineáris függvény és (a kvadratikus alakja) pozitív definit. Ez részletesen kiírva a következőket jelenti:

$$\mathbf{x}\cdot\mathbf{z}=\mathbf{z}\cdot\mathbf{x};\quad (\mathbf{x}+\mathbf{x}')\cdot\mathbf{z}=\mathbf{x}\cdot\mathbf{z}+\mathbf{x}'\cdot\mathbf{z};\quad (\lambda\mathbf{x})\cdot\mathbf{z}=\lambda(\mathbf{x}\cdot\mathbf{z});\quad \mathbf{x}\neq\mathbf{0}\Rightarrow\mathbf{x}\cdot\mathbf{x}>0$$

(természetesen az összegre és skalárszorosra vonatkozó tulajdonságok a második változó szerint is érvényesek, de a szimmetria miatt ezeket nem tüntettük fel külön).

A 7.2.3 ortogonalizációs tételből (a 7.2.5 Tételben megfogalmazott formában) az előzők megfordítása is következik: egy pozitív definit szimmetrikus bilineáris függvényhez mindig található olyan bázis, hogy a szerinte vett skalárszorzat éppen az adott függvénnyel egyenlő. Végezzük el ugyanis az ortogonalizációt és a „normálást", ekkor bármely szimmetrikus bilineáris függvény mátrixa diagonális lesz, ahol a főátlóban minden elem ±1 vagy 0. A pozitív definitség miatt azonban a főátlóban nulla és negatív szám nem állhat, tehát a mátrix ekkor az egységmátrix. Így a bilineáris függvény $[\mathbf{x}]^T E[\mathbf{z}]=\sum_{j=1}^{n} x_j z_j$, ami valóban az $\mathbf{x}\cdot\mathbf{z}$ skalárszorzat.

Ez az ekvivalencia lehetővé teszi a skalárszorzat bázistól független definícióját, amely például a végtelen dimenzióra történő kiterjesztésnél hasznos, de véges dimenziós esetben is gyakran kényelmesebb, mint a koordinátás megadás.

A fentieket fontosságuk miatt külön tételként is kimondjuk:

8.1.2 Tétel

A skalárszorzatot pozitív definit szimmetrikus bilineáris függvényként is definiálhatjuk. ♣

Most az euklideszi tér definíciója következik:

8.1.3 Definíció

Euklideszi téren egy skalárszorzattal ellátott vektorteret értünk. ♣

Euklideszi teret tehát úgy kapunk, hogy kijelölünk a (valós, véges dimenziós) vektortéren egy skalárszorzatot (a „$\cdot$" jelölés ezentúl ezt a **rögzített** skalárszorzatot jelenti). A skalárszorzatot a 8.1.2 Tétel szerint kétféleképpen

is kijelölhetjük: vagy lerögzítünk egy bázist, vagy pedig megadunk egy pozitív definit szimmetrikus bilineáris függvényt.

Egy bázis a skalárszorzatot nyilván egyértelműen meghatározza (két vektorhoz a koordinátáik szorzatösszegét rendeli). A megfordítás nem igaz, több bázis is létrehozhatja ugyanazt a skalárszorzatot: ehhez (az előbbi gondolatmenet szerint) pontosan az kell, hogy az adott bázisban a (pozitív definit szimmetrikus bilineáris) függvény mátrixa az egységmátrix legyen. Az ilyen bázis „merőleges egységvektorokból" áll: bármely bázisvektor önmagával vett skalárszorzata (az egységmátrix főátlójának megfelelő eleme, tehát) 1, két különböző bázisvektor skalárszorzata pedig 0. Euklideszi térben az ilyen vektorrendszerekre külön elnevezést vezetünk be:

8.1.4 Definíció

Az $\mathbf{e}_1, \ldots, \mathbf{e}_n$ vektorokat *ortonormált rendszer*nek nevezzük, ha $\mathbf{e}_i \cdot \mathbf{e}_j = 0$, ha $i \neq j$ és 1, ha $i = j$.

Ha az $\mathbf{e}_i$ vektorok emellett bázist is alkotnak, akkor *ortonormált bázis*ról beszélünk. ♣

Ha az euklideszi tér skalárszorzatát bázis megadásával jelöltük ki, akkor ez a bázis mindenképpen ortonormált, de sok másik ortonormált bázis is létezik. Sőt, tetszőleges ortonormált rendszer kiegészíthető ortonormált bázissá: ez a 7.2.3 Tétel első bizonyításából (a Gram–Schmidt ortogonalizációból) adódik.

Tekintsük most egy euklideszi tér valamely alterét. Ekkor ez az altér maga is euklideszi tér lesz az eredeti skalárszorzatra (pontosabban annak megszorítására, leszűkítésére) nézve, még akkor is, ha a skalárszorzatot eredetileg kijelölő bázisnak akár egyetlen eleme sem esik ebbe az altérbe. Ez a 8.1.2 Tételből következik: az altérre történő leszűkítés ugyanis változatlanul pozitív definit szimmetrikus bilineáris függvény, és így a 8.1.2 Tétel szerint skalárszorzatot definiál.

A továbbiakban a merőleges kiegészítő altér fogalmát és tulajdonságait tárgyaljuk. Ehhez először a merőlegességet definiáljuk:

8.1.5 Definíció

Egy euklideszi térben az $\mathbf{a}$ és $\mathbf{b}$ vektorok *merőleges*ek (vagy *ortogonális*ak), ha skalárszorzatuk nulla: $\mathbf{a} \cdot \mathbf{b} = 0$.

Ezt a geometriából ismert módon $\mathbf{a} \perp \mathbf{b}$-vel jelöljük. ♣

Ne felejtsük el, hogy a merőlegesség erősen függ a választott skalárszorzattól. Ha tehát ugyanazon a V vektortéren egy másik skalárszorzatot veszünk

(és így persze egy másik euklideszi teret kapunk), akkor (általában) más vektorpárok lesznek egymásra merőlegesek.

8.1.6 Definíció

Egy V euklideszi térben egy H részhalmaz $H^\perp$ *merőleges kiegészítő*jén a H minden elemére merőleges vektorok halmazát értjük, azaz $H^\perp = \{\mathbf{x} \in V \mid (\mathbf{h} \in H \Rightarrow \mathbf{h}\cdot\mathbf{x} = 0)\}$. ♣

Egyszerű számolással ellenőrizhető, hogy $H^\perp$ minden esetben altér V-ben. Ha H maga is altér volt, akkor ennél lényegesen több is igaz:

8.1.7 Tétel

Ha U altér, akkor a V euklideszi tér minden vektora egyértelműen írható fel egy U-beli és egy $U^\perp$-beli vektor összegeként. ♣

Ez más megfogalmazásban azt jelenti (4.3.6 Tétel, 4.3.7 Definíció), hogy V az U és $U^\perp$ alterek direkt összege: $V = U \oplus U^\perp$. Ha V a közönséges tér (a szokásos skalárszorzattal) és U pl. egy (origón átmenő) sík, akkor azt a jól ismert geometriai tényt kapjuk, hogy minden $\mathbf{v}$ vektor egyértelműen előállítható egy U-ba eső vektor (ami a $\mathbf{v}$ vektor merőleges vetülete) és egy az U síkra merőleges vektor összegeként. Ennek mintájára tetszőleges euklideszi tér esetén is beszélünk egy $\mathbf{v}$ vektornak az U altérbe eső *merőleges vetület*éről: ez a 8.1.7 Tételben megadott előállításnál az összegnek az U-ba eső tagja.

Első bizonyítás: Vegyünk az U-ban egy $\mathbf{b}_1, \ldots, \mathbf{b}_k$ ortonormált bázist, és ezt a $\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$ vektorokkal egészítsük ki a V ortonormált bázisává. (Ezt, mint az előbb már jeleztük, pl. a Gram–Schmidt ortogonalizációval valósíthatjuk meg.) Ekkor tetszőleges $\mathbf{v} \in V$ vektor felírható $\mathbf{v} = \sum_{j=1}^{n} \lambda_j \mathbf{b}_j$ alakban. Itt az első k bázisvektor lineáris kombinációja egy U-beli, a maradék $n-k$ bázisvektor lineáris kombinációja pedig egy $U^\perp$-beli vektort jelent. Ezzel megadtuk a $\mathbf{v}$ vektornak egy kívánt előállítását.

Hátra van még az egyértelműség igazolása. A 4.3.6 Tétel szerint ehhez azt kell belátni, hogy $U \cap U^\perp = \mathbf{0}$. Tegyük fel, hogy $\mathbf{a} \in U \cap U^\perp$. Ekkor $\mathbf{a} \perp \mathbf{a}$ is teljesül, azaz $\mathbf{a}\cdot\mathbf{a} = 0$, de így csak $\mathbf{a} = \mathbf{0}$ lehet. ■

A bizonyításból az is kiderült, hogy $U^\perp$ egy bázisa $\mathbf{b}_{k+1}, \ldots, \mathbf{b}_n$.

A fenti bizonyítás tulajdonképpen a konkrét felbontás megkeresésére is alkalmas, bár az innen leolvasható eljárás meglehetősen bonyolult. Az alábbi bizonyításból egy lényegesen egyszerűbb és gyakorlati szempontból használhatóbb algoritmust nyerünk.

Második bizonyítás: Legyen most is $\mathbf{b}_1, \dots, \mathbf{b}_k$ ortonormált bázis U-ban, $\mathbf{v} \in V$ tetszőleges, és keressük a $\mathbf{v} = \mathbf{u} + \mathbf{u}^\perp$ előállítást, ahol $\mathbf{u} \in U, \mathbf{u}^\perp \in U^\perp$. Írjuk be ide az $\mathbf{u} = \sum_{j=1}^k \lambda_j \mathbf{b}_j$ alakot, majd a kapott egyenlőség mindkét oldalának vegyük rendre a $\mathbf{b}_m$ $(m = 1, 2, \dots, k)$ vektorokkal a skalárszorzatát:

$$\mathbf{v}\cdot\mathbf{b}_m = \sum_{j=1}^{k} \lambda_j(\mathbf{b}_j\cdot\mathbf{b}_m) + \mathbf{u}^\perp\cdot\mathbf{b}_m\,. \tag{8.1.1}$$

A jobb oldalon $\mathbf{b}_j\cdot\mathbf{b}_m = 0$, ha $j \neq m$, ugyanígy $\mathbf{u}^\perp\cdot\mathbf{b}_m = 0$ (hiszen $\mathbf{b}_m \in U$, $\mathbf{u}^\perp \in U^\perp$), és végül $\mathbf{b}_m\cdot\mathbf{b}_m = 1$, tehát (8.1.1) a $\mathbf{v}\cdot\mathbf{b}_m = \lambda_m$ alakot ölti. Ezzel megkaptuk a λ_m együtthatók és így $\mathbf{u}$ egyetlen lehetséges értékét: $\mathbf{u} = \sum_{j=1}^k (\mathbf{v}\cdot\mathbf{b}_j)\mathbf{b}_j$.

Azt kell már csak megmutatni, hogy ez valóban megfelel, vagyis $\mathbf{u}^\perp = \mathbf{v} - \sum_{j=1}^k (\mathbf{v}\cdot\mathbf{b}_j)\mathbf{b}_j \in U^\perp$. Könnyen adódik, hogy egy $\mathbf{a}$ vektor akkor és csak akkor merőleges U minden elemére, ha U egy (tetszőlegesen választott) bázisának elemeire merőleges, így elég belátni, hogy a fenti $\mathbf{u}^\perp$-nek mindegyik $\mathbf{b}_j$-vel vett skalárszorzata nulla. Ez pedig egyszerű számolással azonnal adódik. ■

Feladatok

8.1.1 Bizonyítsuk be, hogy $\mathbf{R}^4$-ben az $\begin{pmatrix}1\\0\\0\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\0\\0\\1\end{pmatrix}$ szokásos egységvektorok és az $\begin{pmatrix}1/2\\1/2\\1/2\\1/2\end{pmatrix}, \begin{pmatrix}1/2\\-1/2\\1/2\\-1/2\end{pmatrix}, \begin{pmatrix}1/2\\-1/2\\-1/2\\1/2\end{pmatrix}, \begin{pmatrix}1/2\\1/2\\-1/2\\-1/2\end{pmatrix}$ vektorok ugyanazt a skalárszorzatot definiálják.

8.1.2 Mutassuk meg, hogy egy euklideszi térben páronként merőleges nem nulla vektorok szükségképpen lineárisan függetlenek.

8.1.3 Bizonyítsuk be, hogy minden legalább kétdimenziós euklideszi térben végtelen sok ortonormált bázis létezik.

8.1.4 Legyen V a legfeljebb másodfokú valós együtthatós polinomok szokásos vektortere. Lássuk be, hogy az alábbi függvények skalárszorzatot definiálnak, és adjunk meg egy-egy ortonormált bázist (f és g tetszőleges V-beli polinomokat jelölnek, f', illetve f'' pedig az f első, illetve második deriváltját).

(a) $\int_{-1}^{+1} f(t)g(t)dt$; (b) $f(1)g(1) + f'(1)g'(1) + f''(1)g''(1)$;

(c) $\sum_{|j|<5} f(j)g(j)$; (d) $\sum_{j=1}^{9} f(j)g(j)$.

8.1.5 Bizonyítsuk be, hogy egy euklideszi térben $\mathbf{b}$ akkor és csak akkor merőleges az $\mathbf{a}_1, \ldots, \mathbf{a}_k$ vektorok mindegyikére, ha $\mathbf{b} \in \langle \mathbf{a}_1, \ldots, \mathbf{a}_k \rangle^\perp$.

8.1.6 Legyen U altér a V euklideszi térben. Igazoljuk, hogy $\dim U + \dim U^\perp = \dim V$.

8.1.7 Tekintsük az $\mathbf{R}^5$ euklideszi teret a szokásos skalárszorzattal. Jelölje egy általános $\mathbf{v} \in V$ vektor komponenseit $v_1, \ldots, v_5$. Adjuk meg az alábbi alterek merőleges kiegészítőjét.

(a) $W_1 = \{\mathbf{v} \mid v_1 = v_2 = 0\}$;

(b) $W_2 = \{\mathbf{v} \mid v_1 = v_2 = v_3 = v_4 = v_5\}$;

(c) $W_3 = \{\mathbf{v} \mid \sum_{j=1}^{5} v_j = 0,\ 2v_1 + v_2 = v_4 + 2v_5\}$.

8.1.8 Legyen U és W két altér a V euklideszi térben, $\dim U + \dim W \geq \geq \dim V$ és $\mathbf{u}\cdot\mathbf{w} = 0$ bármely $\mathbf{u} \in U, \mathbf{w} \in W$ esetén. Igazoljuk, hogy $W = U^\perp$.

8.1.9 Legyenek U_1 és U_2 egy euklideszi tér alterei. Bizonyítsuk be, hogy

(a) $U_1 \subseteq U_2 \iff U_1^\perp \supseteq U_2^\perp$;

(b) $\langle U_1, U_2 \rangle^\perp = U_1^\perp \cap U_2^\perp$;

(c) $(U_1 \cap U_2)^\perp = \langle U_1^\perp, U_2^\perp \rangle$.

8.1.10

(a) Adjunk meg az $\mathbf{R}^2$ szokásos euklideszi térben végtelen sok olyan vektort, amelyek közül bármely kettő lineárisan független, de semelyik kettő sem merőleges.

*(b) Legyen V egy n-dimenziós euklideszi tér ($n > 0$). Adjunk meg V-ben végtelen sok olyan vektort, amelyek közül bármely n lineárisan független, de semelyik kettő sem merőleges.

*8.1.11 Legyen V egy n-dimenziós euklideszi tér és $\mathbf{b}_1, \ldots, \mathbf{b}_n$ tetszőleges bázis. Bizonyítsuk be, hogy pontosan egy olyan $\mathbf{c}_1, \ldots, \mathbf{c}_n$ bázis létezik, amelyre $\mathbf{b}_i\cdot\mathbf{c}_j = 0$, ha $i \neq j$, és 1, ha $i = j$.

8.1.12 Legyen a V véges dimenziós valós vektortér az U és W alterek direkt összege. Értelmezzünk V-n skalárszorzatot úgy, hogy a kapott euklideszi térben $W = U^\perp$ legyen. Hány ilyen skalárszorzat létezik?

8.1.13 Legyen V egy n-dimenziós euklideszi tér. A $V \to \mathbf{R}$ lineáris leképezéseket, azaz $\mathrm{Hom}\,(V, \mathbf{R})$ elemeit *lineáris függvény*eknek nevezzük (ezt a fogalmat már a 7.1.9 feladatban is bevezettük).

(a) Legyen $\mathbf{c} \in V$ rögzített vektor. Mutassuk meg, hogy $\Phi_\mathbf{c}(\mathbf{x}) = \mathbf{c}\cdot\mathbf{x}$ lineáris függvény.

(b) Legyen Ψ tetszőleges lineáris függvény. Bizonyítsuk be, hogy ekkor létezik, mégpedig pontosan egy olyan $\mathbf{c} \in V$ vektor, amellyel $\Psi(\mathbf{x}) = \mathbf{c}\cdot\mathbf{x}$.

Megjegyzés: A feladat két része együttesen azt fejezi ki, hogy az összes lineáris függvényt a V elemeinek egy rögzített vektorral képezett skalárszorzataként kapjuk meg. A fenti $\mathbf{c} \to \Phi_{\mathbf{c}}$ megfeleltetés a V vektortér és a lineáris függvények alkotta $\mathrm{Hom}\,(V\,,\mathbf{R})$ ún. *duális tér* között kölcsönösen egyértelmű, sőt könnyen láthatóan művelettartó is, és így (vektortér)izomorfizmus.

8.1.14 Két euklideszi teret akkor nevezünk *izomorf*nak, ha létezik közöttük olyan kölcsönösen egyértelmű lineáris leképezés, amely (nemcsak az összeadásra és a skalárral való szorzásra, hanem) a skalárszorzatra nézve is művelettartó. Bizonyítsuk be, hogy két euklideszi tér akkor és csak akkor izomorf, ha megegyezik a dimenziójuk.

*8.1.15 Végtelen dimenziós euklideszi teret is értelmezhetünk, ha a skalárszorzatot (bázis felhasználása nélkül) pozitív definit szimmetrikus bilineáris függvényként definiáljuk.

Legyen V azoknak az $\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots)$ végtelen valós számsorozatoknak a halmaza, ahol az elemek négyzeteiből képzett végtelen sor konvergens: $V = \{\mathbf{a} = (\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots) \mid \sum_{j=1}^{\infty} \alpha_j^2 < \infty\}$.

(a) Mutassuk meg, hogy V a sorozatok szokásos összeadására és számmal való szorzására vektorteret alkot.

(b) Igazoljuk, hogy az $\mathbf{a}\cdot\mathbf{b} = (\alpha_1, \alpha_2, \ldots, \alpha_k, \ldots)\cdot(\beta_1, \beta_2, \ldots, \beta_k, \ldots) = \\ = \sum_{j=1}^{\infty} \alpha_j\beta_j$ hozzárendelés skalárszorzatot definiál V-n.

(c) Legyen U azoknak a sorozatoknak az altere V-ben, amelyek legfeljebb véges sok nem nulla elemet tartalmaznak. Mi lesz $U^\perp$?

*8.1.16 Legyen U altér egy V végtelen dimenziós euklideszi térben.

(a) Mutassuk meg, hogy $U^\perp = V \iff U = \mathbf{0}$.

(b) Igaz-e, hogy $U^\perp = \mathbf{0} \iff U = V$?

(c) Lássuk be, hogy $(U^\perp)^\perp \supseteq U$, de nem mindig érvényes egyenlőség.

(d) Bizonyítsuk be, hogy $((U^\perp)^\perp)^\perp = U^\perp$.

*8.1.17 Vizsgáljuk meg a 8.1.7 Tétel és a 8.1.9 feladat állításait végtelen dimenziós euklideszi térre.

8.2. Hossz, távolság, szög

A skalárszorzat segítségével most felépítjük az euklideszi tér geometriáját. A címbeli fogalmak tetszőleges euklideszi térre történő kiterjesztésénél a (közönséges) sík-, illetve térbeli kapcsolatokat vesszük alapul.

8.2.1 Definíció

Egy euklideszi térben az $\mathbf{x}$ vektor *hosszán* (vagy *normáján* vagy *abszolút értékén*) az önmagával vett skalárszorzatának a négyzetgyökét értjük. A skalárszorzat definíciója szerint ezt úgy kapjuk, hogy az $\mathbf{x}$ egy ortonormált bázisban vett koordinátáinak négyzetösszegéből négyzetgyököt vonunk. Az $\mathbf{x}$ vektor hosszát $\|\mathbf{x}\|$-szel jelöljük. Összefoglalva:

$$\|\mathbf{x}\| = \sqrt{\mathbf{x}\cdot\mathbf{x}} = \sqrt{\sum_{j=1}^{n} x_j^2}\,,$$

ahol $x_1, \ldots, x_n$ az $\mathbf{x}$ vektor koordinátái egy ortonormált bázisban. ♣

8.2.2 Tétel

A hossz az alábbi tulajdonságokkal rendelkezik:

(N1) $\|\mathbf{x}\| \geq 0$ és $\|\mathbf{x}\| = 0 \iff \mathbf{x} = \mathbf{0}$.

(N2) $\|\lambda\mathbf{x}\| = |\lambda| \cdot \|\mathbf{x}\|$.

(N3) $\|\mathbf{x} + \mathbf{z}\| \leq \|\mathbf{x}\| + \|\mathbf{z}\|$. ♣

Bizonyítás: (N1), illetve (N2) azonnal következik a skalárszorzat pozitív definitségéből, illetve bilinearitásából. Az (N3) *háromszögegyenlőtlenség* igazolására a 8.2.8 Tétel után kerül majd sor. ■

8.2.3 Definíció

Egy $\mathbf{R}$ feletti V vektorteret *normált (vektor)tér*nek nevezünk, ha értelmezve van rajta egy $\|\cdot\| : V \to \mathbf{R}$ *norma*, amely rendelkezik az (N1), (N2) és (N3) tulajdonságokkal. ♣

A 8.2.2 Tételt tehát úgy is fogalmazhatjuk, hogy minden euklideszi tér egyben normált tér is. Ennek a megfordítása nem igaz, lásd a 8.2.4–8.2.5 feladatokat.

A hossz segítségével azonnal értelmezhető a távolság:

8.2.4 Definíció

Egy normált térben két vektor *távolság*án a különbségvektoruk hosszát értjük. Az $\mathbf{x}$ és $\mathbf{z}$ vektorok távolságát $\tau(\mathbf{x},\mathbf{z})$-vel jelöljük. Így $\tau(\mathbf{x},\mathbf{z}) = \|\mathbf{x}-\mathbf{z}\|$. ♣

8.2.5 Tétel

A távolság az alábbi tulajdonságokkal rendelkezik:

(M1) $\tau(\mathbf{x},\mathbf{z}) \geq 0$ és $\tau(\mathbf{x},\mathbf{z}) = 0 \iff \mathbf{x} = \mathbf{z}$.

(M2) $\tau(\mathbf{x},\mathbf{z}) = \tau(\mathbf{z},\mathbf{x})$.

(M3) $\tau(\mathbf{x},\mathbf{z}) \leq \tau(\mathbf{x},\mathbf{w}) + \tau(\mathbf{w},\mathbf{z})$. ♣

Bizonyítás: Mindhárom (M) tulajdonság azonnal következik az azonos sorszámú (N) tulajdonságból [(N2)-t csak $\lambda = -1$-re kell felhasználni]. ■

8.2.6 Definíció

Egy H halmazt *metrikus tér*nek nevezünk, ha értelmezve van rajta egy $\tau : H \times H \to \mathbf{R}$ *távolság* (vagy *metrika*), amely rendelkezik az (M1), (M2) és (M3) tulajdonságokkal. ♣

A 8.2.5 Tételt tehát úgy is fogalmazhatjuk, hogy minden normált tér (és így speciálisan minden euklideszi tér) egyben metrikus tér is. Ennek a megfordítása nem igaz, lásd a 8.2.6–8.2.7 feladatokat.

Végül következik a szög definíciója. A síkon (vagy térben) két nem nulla vektor skalárszorzata a két vektor hosszának és a közbezárt szög koszinuszának a szorzata, azaz $\mathbf{x}\cdot\mathbf{z} = \|\mathbf{x}\| \cdot \|\mathbf{z}\| \cdot \cos\varphi$. Innen $\cos\varphi$ kifejezhető: $\cos\varphi = (\mathbf{x}\cdot\mathbf{z})/(\|\mathbf{x}\| \cdot \|\mathbf{z}\|)$ (a nevezőben $\|\mathbf{x}\|$ és $\|\mathbf{z}\|$ nem nulla, mert $\mathbf{x}$ és $\mathbf{z}$ nem nullvektor). Ennek alapján a közbezárt szög koszinusza megadható csak a skalárszorzat segítségével, és ez lehetővé teszi a szög definícióját tetszőleges euklideszi térben:

8.2.7 Definíció

Ha $\mathbf{x}$ és $\mathbf{z}$ egy euklideszi tér nullától különböző vektorai, akkor a *közbezárt szög*ükön azt a $0 \leq \varphi \leq \pi$ szöget értjük, amelyre

$$\cos\varphi = \frac{\mathbf{x}\cdot\mathbf{z}}{\|\mathbf{x}\| \cdot \|\mathbf{z}\|} = \frac{\mathbf{x}\cdot\mathbf{z}}{\sqrt{\mathbf{x}\cdot\mathbf{x}}\sqrt{\mathbf{z}\cdot\mathbf{z}}} \,. \quad ♣$$

A fenti definíció csak akkor értelmez valóban szöget, ha a $\cos\varphi$-re megadott kifejezés -1 és $+1$ közé esik. Ezt az alábbi tétel biztosítja:

8.2.8 Tétel (Cauchy–Bunyakovszkij–Schwarz-egyenlőtlenség) Egy euklideszi tér bármely $\mathbf{x}$ és $\mathbf{z}$ vektorára fennáll az

$$|\mathbf{x}\cdot\mathbf{z}| \leq \|\mathbf{x}\| \cdot \|\mathbf{z}\|$$

egyenlőtlenség. Egyenlőség akkor és csak akkor teljesül, ha $\mathbf{x}$ és $\mathbf{z}$ lineárisan összefüggők (azaz az egyik a másiknak skalárszorosa). ♣

Azonnal megállapíthatjuk, hogy ha $\mathbf{x}$ és $\mathbf{z}$ közül legalább az egyik a nullvektor, akkor mindkét oldal 0, tehát elég azzal az esettel foglalkozni, amikor $\mathbf{x}$ és $\mathbf{z}$ egyike sem $\mathbf{0}$.

Első bizonyítás: Tekintsük az $\mathbf{x}$ és $\mathbf{z}$ által generált alteret. Ez egy legfeljebb 2-dimenziós euklideszi tér, és így a közönséges síkkal vagy annak egy alterével izomorf (mint euklideszi tér is, lásd a 8.1.14 feladatot). A síkon viszont igaz az egyenlőtlenség (hiszen éppen abból indultunk ki), továbbá egyenlőség pontosan akkor érvényes, ha a vektorok párhuzamosak, azaz összefüggők. ■

Második bizonyítás: Írjuk fel mindkét oldalt egy ortonormált bázis szerinti koordináták segítségével, majd emeljünk négyzetre. Mivel mindkét oldalon nemnegatív szám áll, így a négyzetre emelés ekvivalens egyenlőtlenséget eredményez. Ez a következőképpen fest:

$$(x_1z_1 + \ldots + x_nz_n)^2 \leq (x_1^2 + \ldots + x_n^2)(z_1^2 + \ldots + z_n^2)\,.$$

A műveleteket elvégezve és átrendezve a

$$0 \leq \sum_{1\leq i<j\leq n} (x_iz_j - x_jz_i)^2$$

alakot kapjuk. A jobb oldali négyzetösszeg nyilván nemnegatív (amivel az egyenlőtlenséget már igazoltuk), és csak akkor nulla, ha minden tagja nulla. Ez utóbbi azt jelenti, hogy $\mathbf{x}$ és $\mathbf{z}$ koordinátái arányosak, tehát az egyik vektor valóban a másik skalárszorosa. ■

Megjegyezzük, hogy a második bizonyítás tulajdonképpen egy valós számokra vonatkozó elemi egyenlőtlenséget igazolt középiskolás úton. Ennek speciális eseteként megkaphatjuk a számtani és négyzetes közép közötti egyenlőtlenséget is (lásd a 8.2.8 feladatot).

Harmadik bizonyítás: Legyen λ tetszőleges skalár, és tekintsük a

$$\|\lambda\mathbf{x}+\mathbf{z}\|^2 = (\lambda\mathbf{x}+\mathbf{z})\cdot(\lambda\mathbf{x}+\mathbf{z}) = \lambda^2(\mathbf{x}\cdot\mathbf{x}) + 2\lambda(\mathbf{x}\cdot\mathbf{z}) + \mathbf{z}\cdot\mathbf{z}$$

skalárszorzatot. Ez ($\mathbf{x}\neq\mathbf{0}$ miatt) λ-nak másodfokú polinomja, továbbá minden λ valós számra nemnegatív értéket vesz fel. Ez csak úgy lehet, ha a diszkriminánsa nempozitív, azaz

$$(\mathbf{x}\cdot\mathbf{z})^2 - (\mathbf{x}\cdot\mathbf{x})(\mathbf{z}\cdot\mathbf{z}) \leq 0\,.$$

Ez éppen a bizonyítandó egyenlőtlenség négyzetre emelt alakja.

Egyenlőség pontosan akkor teljesül, ha a diszkrimináns nulla, ami (a negatív diszkriminánsú másik esettel szemben) éppen azt jelenti, hogy a szóban forgó másodfokú polinomnak van gyöke. Ekkor tehát alkalmas λ-ra $\|\lambda\mathbf{x}+\mathbf{z}\| = 0$, azaz $\lambda\mathbf{x}+\mathbf{z} = \mathbf{0}$, vagyis $\mathbf{z} = -\lambda\mathbf{x}$. ■

A Cauchy–Bunyakovszkij–Schwarz-egyenlőtlenség (a továbbiakban CBS) igen széles körben alkalmazható. Most a 8.2.2 Tételbeli (N3) háromszögegyenlőtlenség még hiányzó bizonyítását pótoljuk a segítségével.

A háromszögegyenlőtlenség bizonyítása [8.2.2 Tétel, (N3)]: $\|\mathbf{x}+\mathbf{z}\| \leq \|\mathbf{x}\|+\|\mathbf{z}\|$ teljesülését kell belátnunk. Ezzel (a nemnegativitás miatt) ekvivalens, ha a két oldal négyzetére látjuk be a megfelelő egyenlőtlenséget. A bal oldal négyzete $\|\mathbf{x}\|^2 + 2(\mathbf{x}\cdot\mathbf{z}) + \|\mathbf{z}\|^2$, a jobb oldal négyzete pedig $\|\mathbf{x}\|^2 + 2\cdot\|\mathbf{x}\|\cdot\|\mathbf{z}\| + \|\mathbf{z}\|^2$. Csak a középső tagban van eltérés, és ott a CBS biztosítja a kívánt irányú egyenlőtlenséget. ■

A fenti bizonyításból az is kiderült, hogy (a geometriai tapasztalatunkkal összhangban) a háromszögegyenlőtlenségben pontosan akkor áll egyenlőség, ha a két vektor egyirányú, azaz az egyik a másiknak *nemnegatív* skalárszorosa.

Feladatok

8.2.1 Mennyi egy ortonormált bázis két elemének a távolsága?

8.2.2 Mennyi az $\mathbf{x}$ és $\mathbf{z}$ vektorok szöge, ha $\|\mathbf{x}\| = \|\mathbf{z}\| = \|\mathbf{x}-\mathbf{z}\| \neq 0$?

8.2.3 Bizonyítsuk be tetszőleges euklideszi térben az alábbi állításokat. Mely közismert geometriai tételek általánosításáról van szó?

(a) $\mathbf{x}\perp\mathbf{z} \iff \|\mathbf{x}+\mathbf{z}\|^2 = \|\mathbf{x}\|^2 + \|\mathbf{z}\|^2$.

(b) $\|\mathbf{x}\| = \|\mathbf{z}\| \iff \mathbf{x}+\mathbf{z}\perp\mathbf{x}-\mathbf{z}$.

(c) $\|\mathbf{x}+\mathbf{z}\|^2 + \|\mathbf{x}-\mathbf{z}\|^2 = 2\|\mathbf{x}\|^2 + 2\|\mathbf{z}\|^2$.

8.2.4 Az alábbi $\mathbf{R}^n \to \mathbf{R}$ függvények közül melyekre lesz az $\mathbf{R}^n$ vektortér normált tér? (Az $\mathbf{x}$ vektor komponenseit x_j-vel jelöljük.)

(a) $\max_{j=1}^n x_j$; (b) $\max_{j=1}^n |x_j|$; (c) $|x_1|$; (d) $\sum_{j=1}^n |x_j|$;

**(e) $(\sum_{j=1}^n |x_j|^3)^{1/3}$.

8.2.5

(a) Mutassunk példát olyan normált térre, amely nem euklideszi tér, azaz a norma nem skalárszorzatból származik.

**(b) Bizonyítsuk be, hogy egy normált tér pontosan akkor tehető euklideszi térré (azaz pontosan akkor definiálható rajta egy, az $\|\mathbf{x}\|^2 = \mathbf{x}\cdot\mathbf{x}$ azonosságot kielégítő skalárszorzat), ha bármely $\mathbf{x}$ és $\mathbf{z}$ esetén $\|\mathbf{x}+\mathbf{z}\|^2 + \|\mathbf{x}-\mathbf{z}\|^2 = 2\|\mathbf{x}\|^2 + 2\|\mathbf{z}\|^2$ teljesül.

8.2.6 Az alábbiakban $\mathbf{R}^n$-en többféleképpen megpróbáljuk két vektor távolságát definiálni. Mely esetekben kapunk metrikus teret? (Az $\mathbf{x}$, illetve $\mathbf{z}$ vektor komponenseit x_j-vel, illetve z_j-vel jelöljük.)

(a) $|x_1 - z_1|$; (b) $\sum_{j=1}^n |x_j - z_j|$;

(c) Ahány komponensben $\mathbf{x}$ és $\mathbf{z}$ különbözik, azaz ahány j-re $x_j \neq z_j$.

8.2.7 Mutassunk példát olyan vektortérre, amely metrikus tér, de a metrika nem normából származik (azaz nem definiálható úgy egy norma, hogy a $\tau(\mathbf{x},\mathbf{z}) = \|\mathbf{x}-\mathbf{z}\|$ azonosság teljesüljön).

8.2.8 Hogyan következik a CBS-ből a számtani és négyzetes közép közötti egyenlőtlenség:

$$\sqrt{\frac{x_1^2 + \ldots + x_n^2}{n}} \geq \frac{x_1 + \ldots + x_n}{n}\,.$$

Mikor áll egyenlőség?

8.2.9 Melyek igazak az alábbi állítások közül (k tetszőleges pozitív egész, a $\mathbf{c}_i$ vektorok egy euklideszi tér elemei)?

(a) Ha a $\mathbf{c}_1, \ldots, \mathbf{c}_k$ vektorok páronként merőlegesek, akkor $\|\sum_{j=1}^k \mathbf{c}_j\|^2 = \sum_{j=1}^k \|\mathbf{c}_j\|^2$.

(b) Ha $\|\sum_{j=1}^k \mathbf{c}_j\|^2 = \sum_{j=1}^k \|\mathbf{c}_j\|^2$, akkor a $\mathbf{c}_1, \ldots, \mathbf{c}_k$ vektorok páronként merőlegesek.

8.2.10 Milyen szöget zárnak be az $\mathbf{R}^4$ szokásos euklideszi térben az alábbi vektorok?

(a) $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ és $\begin{pmatrix}1\\1\\1\\0\end{pmatrix}$; (b) $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}$ és $\begin{pmatrix}1\\-1\\-1\\-1\end{pmatrix}$; (c) $\begin{pmatrix}1\\\sqrt{2}\\1\\0\end{pmatrix}$ és $\begin{pmatrix}0\\1\\\sqrt{2}\\1\end{pmatrix}$.

8.2.11 Tekintsünk az $\mathbf{R}^4$ szokásos euklideszi térben egy egységnyi oldalú kockát.

(a) Határozzuk meg a csúcsok, az élek és a testátlók számát.
(b) Milyen hosszúak a testátlók?
(c) Milyen szöget zár be egy testátló egy éllel?
(d) Milyen szöget zár be két testátló?
(e) Mennyi a kocka köré, illetve a kockába írt (4-dimenziós) gömb sugara?

8.2.12 Definiáljuk és számítsuk ki az $\mathbf{R}^4$ szokásos euklideszi térben az $U = \{\mathbf{u} = \begin{pmatrix}u_1\\u_2\\u_3\\u_4\end{pmatrix} \mid u_1+u_2+u_3+u_4 = 0\}$ altér és az $\begin{pmatrix}1\\2\\3\\4\end{pmatrix}$ vektor távolságát.

8.2.13 Tegyük fel, hogy az $A\mathbf{x} = \mathbf{b}$ valós egyenletrendszer nem oldható meg. Ekkor olyan $\mathbf{z}$ közelítő megoldást szeretnénk találni, amelyre az $A\mathbf{z}$ vektor a lehető legközelebb van $\mathbf{b}$-hez. Hogyan keressünk ilyen $\mathbf{z}$-t, és milyen értelemben lesz ez legjobb közelítő megoldás? Illusztráljuk mindezt az alábbi egyenletrendszeren:

$$\begin{aligned} x_1 + \ x_2 + \ x_3 + \ x_4 &= 1\\ x_1 + 2x_2 + 3x_3 + 4x_4 &= 1\\ x_1 + 3x_2 + 5x_3 + 7x_4 &= 7 \end{aligned}$$

8.2.14 Legyen $\mathbf{e}_1, \dots, \mathbf{e}_n$ egy euklideszi tér ortonormált bázisa. Igazoljuk az alábbi azonosságokat:

(a) $\mathbf{x} = \sum_{j=1}^{n} (\mathbf{e}_j \cdot \mathbf{x})\mathbf{e}_j$;
(b) $\mathbf{x}\cdot\mathbf{z} = \sum_{j=1}^{n} (\mathbf{x}\cdot\mathbf{e}_j)(\mathbf{e}_j\cdot\mathbf{z})$;
(c) *Parseval-formula*: $\|\mathbf{x}\|^2 = \sum_{j=1}^{n} |\mathbf{x}\cdot\mathbf{e}_j|^2$.

8.2.15 (*Bessel-egyenlőtlenség.*) Mutassuk meg, hogy ha $\mathbf{c}_1, \dots, \mathbf{c}_k$ ortonormált rendszer, akkor bármely $\mathbf{x}$ vektorra $\|\mathbf{x}\|^2 \geq \sum_{j=1}^{k} |\mathbf{x}\cdot\mathbf{c}_j|^2$. Mikor áll egyenlőség?

8.2.16 Lássuk be, hogy a CBS (nemcsak a skalárszorzatokra, azaz a pozitív definit függvényekre, hanem) a pozitív szemidefinit függvényekre is igaz: ha $\mathbf{A}$ egy pozitív szemidefinit szimmetrikus bilineáris függvény, akkor bármely $\mathbf{x}$ és $\mathbf{z}$ vektorra $|\mathbf{A}(\mathbf{x},\mathbf{z})|^2 \le \mathbf{A}(\mathbf{x},\mathbf{x})\cdot\mathbf{A}(\mathbf{z},\mathbf{z})$.

M*8.2.17 Egy n-dimenziós euklideszi térben maximálisan hány (nem nulla) vektor adható meg úgy, hogy közülük bármely kettő (a) 60; (b) 120 fokos szöget zárjon be egymással?

*8.2.18 Mutassuk meg, hogy a CBS végtelen dimenziós euklideszi térben is igaz (a végtelen dimenziós euklideszi tér értelmezését lásd a 8.1.15 feladatban).

8.3. Komplex euklideszi tér

Most a komplex test feletti véges dimenziós vektorterekre adaptáljuk az előző két pontban tárgyalt fogalmakat és eredményeket.

8.3.1 Definíció

Legyen $\mathbf{e}_1,\dots,\mathbf{e}_n$ *rögzített* bázis V-ben. Ekkor az adott bázis szerint vett *skalárszorzat*on az alábbi $\mathbf{S}: V\times V\to\mathbf{C}$ függvényt értjük:

$$\mathbf{S}(\mathbf{x},\mathbf{z}) = \mathbf{x}\cdot\mathbf{z} = \begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix}\cdot\begin{pmatrix} z_1\\ \vdots\\ z_n\end{pmatrix} = \sum_{j=1}^{n}\overline{x_j}z_j\,. \ \clubsuit$$

A valós esethez képest tehát annyi a változás, hogy az *első* vektor koordinátáinak a *komplex konjugált*ját kell venni.

Az így definiált skalárszorzat pozitív definit *ermitikus* bilineáris függvény, ami részletesen kiírva a következőket jelenti:

$$\textbf{!!!}\ \mathbf{x}\cdot\mathbf{z} = \overline{\mathbf{z}\cdot\mathbf{x}}\ \textbf{!!!}\ ;\quad (\mathbf{x}+\mathbf{x}')\cdot\mathbf{z} = \mathbf{x}\cdot\mathbf{z}+\mathbf{x}'\cdot\mathbf{z};\quad \textbf{!!!}\ (\lambda\mathbf{x})\cdot\mathbf{z} = \overline{\lambda}(\mathbf{x}\cdot\mathbf{z})\ \textbf{!!!}\ ;$$
$$\mathbf{x}\cdot(\mathbf{z}+\mathbf{z}') = \mathbf{x}\cdot\mathbf{z}+\mathbf{x}\cdot\mathbf{z}';\quad \mathbf{x}\cdot(\lambda\mathbf{z}) = \lambda(\mathbf{x}\cdot\mathbf{z});\quad \mathbf{x}\neq\mathbf{0}\Rightarrow\mathbf{x}\cdot\mathbf{x}>0\,.$$

A valós esethez képest tehát két helyen van változás: a két tényező felcserélésekor a skalárszorzat a komplex konjugáltjába megy át, valamint az *első* tényezőt λ-val szorozva a skalárszorzat nem λ-val, hanem annak konjugáltjával, $\overline{\lambda}$-tal szorzódik. Megjegyezzük még, hogy az $\mathbf{x}\neq\mathbf{0}\Rightarrow\mathbf{x}\cdot\mathbf{x}>0$ feltétel azt is magában foglalja, hogy $\mathbf{x}\cdot\mathbf{x}$ minden $\mathbf{x}$-re *valós* szám (ez egyébként az $\mathbf{x}\cdot\mathbf{z}=\overline{\mathbf{z}\cdot\mathbf{x}}$ tulajdonságból adódik — vö. a 7.4.4 Tétellel).

Az ortogonalizációs tétel komplex változata szerint most is igaz a megfordítás: minden pozitív definit ermitikus bilineáris függvényhez található olyan bázis, hogy a szerinte vett skalárszorzat éppen az adott függvénnyel egyenlő. Így a 8.1.2 Tétel megfelelője érvényben marad:

8.3.2 Tétel
A (komplex) skalárszorzatot pozitív definit ermitikus bilineáris függvényként is definiálhatjuk. ♣

Ezután az euklideszi tér, az ortonormált rendszer, az ortonormált bázis, a merőlegesség, a merőleges kiegészítő értelmezése ugyanaz, mint a valós esetben volt (8.1.3–8.1.6 Definíciók). A 8.1.7 Tétel is változtatás nélkül érvényes.

A vektor hossza komplex euklideszi térben is az önmagával vett skalárszorzat négyzetgyöke (8.2.1 Definíció). Ez (a pozitív definitség miatt) most is (nemnegatív) *valós* szám. A vektor hosszát egy ortonormált bázis szerinti koordinátákkal úgy írhatjuk fel, hogy a koordináták *abszolút értékének* négyzetösszegéből vonunk négyzetgyököt:

$$\|\mathbf{x}\| = \sqrt{\mathbf{x}\cdot\mathbf{x}} = \sqrt{\sum_{j=1}^{n} \overline{x_j} x_j} = \sqrt{\sum_{j=1}^{n} |x_j|^2}\,.$$

A hosszra ugyanúgy teljesülnek a 8.2.2 Tétel (N1)–(N3) állításai, tehát egy komplex euklideszi tér egyben (komplex) normált tér is.

A (norma segítségével definiált) távolság fogalma és (M1)–(M3) tulajdonságai (8.2.4 Definíció, 8.2.5 Tétel) azonosak a valós esetben látottakkal, és így most is metrikus teret kapunk.

Szöget nem értelmezünk (csak merőlegességet), hiszen a 8.2.7 Definíció most $\cos\varphi$-re általában komplex értéket adna.

A Cauchy–Bunyakovszkij–Schwarz egyenlőtlenség (8.2.8 Tétel) azonban továbbra is érvényes, a második bizonyítás minimális változtatással, a harmadik bizonyítás pedig némi trükk alkalmazásával átvihető a komplex esetre is (lásd a 8.3.4 feladatot).

Feladatok

8.3.1 Mutassuk meg, hogy az alábbi feladatok állításai komplex euklideszi térben is érvényben maradnak: 8.1.2, 8.1.3, 8.1.5, 8.1.6, 8.1.8, 8.1.9, 8.1.11, 8.1.14, 8.2.14, 8.2.15.

8.3.2 Legyen V egy komplex euklideszi tér. Bizonyítsuk be, hogy

(a) $\mathbf{x} - i\mathbf{z}$ és $i\mathbf{x} + \mathbf{z}$ pontosan akkor merőlegesek, ha $\mathbf{x} = i\mathbf{z}$;

(b) $\mathbf{x} + i\mathbf{z}$ és $i\mathbf{x} + \mathbf{z}$ pontosan akkor merőlegesek, ha $\|\mathbf{x}\| = \|\mathbf{z}\|$ és az $\mathbf{x}\cdot\mathbf{z}$ skalárszorzat tiszta képzetes.

8.3.3 Vizsgáljuk meg a 8.2.3 feladat állításait komplex euklideszi tér esetén.

8.3.4 Bizonyítsuk be a Cauchy–Bunyakovszkij–Schwarz egyenlőtlenséget komplex euklideszi térre.

8.3.5 A $\mathbf{C}^n$ szokásos euklideszi térben egy $\mathbf{x}$ vektor konjugáltját úgy kapjuk, hogy $\mathbf{x}$ minden komponensét konjugáljuk: ha $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, akkor $\overline{\mathbf{x}} = \begin{pmatrix} \overline{x_1} \\ \vdots \\ \overline{x_n} \end{pmatrix}$. Egy tetszőleges $H \subseteq \mathbf{C}^n$ részhalmazra legyen $\overline{H}$ a H-beli vektorok konjugáltjainak a halmaza. Végül egy vektort nevezzünk valósnak, ha minden komponense valós.

(a) Bizonyítsuk be, hogy $\mathbf{z}$ és $\overline{\mathbf{z}}$ akkor és csak akkor összefüggők, ha $\mathbf{z}$ egy valós vektor skalárszorosa.

(b) Mutassuk meg, hogy $\overline{H}$ akkor és csak akkor altér, ha H altér.

(c) Igazoljuk, hogy bármely U altérre $\overline{U}^{\perp} = \overline{U^{\perp}}$.

(d) Lássuk be, hogy egy $U \neq \mathbf{0}$ altérre $\overline{U} = U$ akkor és csak akkor teljesül, ha U-nak létezik valós vektorokból álló bázisa.

(e) Bizonyítsuk be, hogy akkor és csak akkor létezik olyan U altér, amelyre $U^{\perp} = \overline{U}$, ha n páros.

8.4. Transzformáció adjungáltja

Legyen V egy n-dimenziós (valós vagy komplex) euklideszi tér.

8.4.1 Tétel

Minden $\mathcal{A} \in \operatorname{Hom} V$ lineáris transzformációhoz pontosan egy olyan $\mathcal{A}^* \in \operatorname{Hom} V$ létezik, amellyel bármely $\mathbf{x}, \mathbf{z} \in V$ vektorra $(\mathcal{A}\mathbf{x})\cdot\mathbf{z} = \mathbf{x}\cdot(\mathcal{A}^*\mathbf{z})$ teljesül.

Ezt az $\mathcal{A}^*$ transzformációt az $\mathcal{A}$ transzformáció *adjungált*jának nevezzük. ♣

Külön felhívjuk a figyelmet arra, hogy az adjungált nemcsak az $\mathcal{A}$ transzformációtól, hanem a skalárszorzattól is függ. Ha tehát ugyanazon a V vektortéren egy másik skalárszorzatot veszünk (és így persze egy másik euklideszi teret kapunk), akkor ugyanannak a transzformációnak (általában) más lesz az adjungáltja.

Bizonyítás: Legyen $\mathbf{e}_1, \ldots, \mathbf{e}_n$ ortonormált bázis V-ben.

Tekintsük először a valós esetet. Ha vesszük az $\mathbf{e}_j$ bázisban $\mathcal{A}, \mathbf{x}$ és $\mathbf{z}$ mátrixát, akkor az $(\mathcal{A}\mathbf{x})\cdot\mathbf{z}$ skalárszorzatot a következőképpen írhatjuk fel:

$$(\mathcal{A}\mathbf{x})\cdot\mathbf{z} = [\mathcal{A}\mathbf{x}]^T[\mathbf{z}] = [\mathbf{x}]^T[\mathcal{A}]^T[\mathbf{z}]\,.$$

A keresett $\mathcal{A}^*$ transzformációval az $\mathbf{x}\cdot(\mathcal{A}^*\mathbf{z})$ skalárszorzatra ugyanígy

$$\mathbf{x}\cdot(\mathcal{A}^*\mathbf{z}) = [\mathbf{x}]^T[\mathcal{A}^*][\mathbf{z}]$$

adódik. A két skalárszorzat mindegyike ($\mathbf{x}$-ben és $\mathbf{z}$-ben) bilineáris függvény, ezért pontosan akkor azonosak, ha (ugyanabban a bázisban felírt) mátrixuk megegyezik, azaz $[\mathcal{A}]^T = [\mathcal{A}^*]$. Felhasználva a mátrixok és a lineáris leképezések közötti kölcsönösen egyértelmű megfeleltetést, innen azt nyerjük, hogy pontosan egy ilyen $\mathcal{A}^*$ transzformáció létezik.

A komplex esetben mindössze annyi a változás, hogy a transzponáltak helyett mindenütt az adjungált mátrixot (azaz a transzponált konjugáltját) kell venni. ■

A bizonyításból az is kiderült, hogyan kapjuk az adjungált transzformáció mátrixát ortonormált bázisban: valós esetben az $\mathcal{A}$ mátrix transzponáltját, a komplex esetben pedig az adjungáltját kell venni. Ezt fontossága miatt külön tételként is kimondjuk. Mivel valós mátrix transzponáltja és adjungáltja ugyanaz, ezért az egyöntetűség kedvéért a jövőben (a valós és a komplex esetben egyaránt) az adjungált mátrix elnevezést és jelölést fogjuk használni.

8.4.2 Tétel

Ortonormált bázisban $[\mathcal{A}^*] = [\mathcal{A}]^*$, azaz $\mathcal{A}^*$ mátrixát úgy kapjuk meg, hogy $\mathcal{A}$ mátrixát tükrözzük a főátlóra és (komplex esetben) konjugáljuk. ♣

A transzformációknál az adjungálás és a műveletek ugyanolyan kapcsolatban állnak, mint a mátrixoknál (lásd a 8.4.1 feladatot).

Valós euklideszi térben $\mathcal{A}$ és $\mathcal{A}^*$ karakterisztikus polinomja, minimálpolinomja és sajátértékei megyegyeznek, komplex esetben pedig egymás konjugáltjai lesznek (lásd a 8.4.7 feladatot).

Az invariáns alterekre vonatkozó alábbi egyszerű tétel a későbbiekben fontos szerepet játszik majd.

8.4.3 Tétel
U akkor és csak akkor invariáns altere $\mathcal{A}$-nak, ha $U^\perp$ invariáns altere $\mathcal{A}^*$-nak. ♣

Bizonyítás: Tegyük fel, hogy *U* invariáns altere $\mathcal{A}$-nak, és mutassuk meg, hogy $U^\perp$ invariáns altere $\mathcal{A}^*$-nak. Ehhez $\mathbf{z} \in U^\perp \Rightarrow \mathcal{A}^*\mathbf{z} \in U^\perp$ igazolandó, vagyis hogy $\mathbf{z}$-vel együtt $\mathcal{A}^*\mathbf{z}$ is merőleges tetszőleges $\mathbf{u} \in U$ vektorra. A kérdéses skalárszorzatot képezve valóban $\mathbf{u}\cdot(\mathcal{A}^*\mathbf{z}) = (\mathcal{A}\mathbf{u})\cdot\mathbf{z} = 0$ adódik, hiszen $\mathcal{A}\mathbf{u} \in U$ és $\mathbf{z} \in U^\perp$. A megfordítást ugyanígy (vagy az $(\mathcal{A}^*)^* = \mathcal{A}$ és $(U^\perp)^\perp = U$ összefüggésekből) kapjuk. ■

Feladatok

8.4.1 Igazoljuk az adjungált transzformáció alábbi tulajdonságait:
$(\mathcal{A}+\mathcal{B})^* = \mathcal{A}^*+\mathcal{B}^*$, $(\lambda\mathcal{A})^* = \overline{\lambda}\mathcal{A}^*$, $(\mathcal{A}\mathcal{B})^* = \mathcal{B}^*\mathcal{A}^*$, $(\mathcal{A}^*)^* = \mathcal{A}$.

8.4.2 Tekintsük a síkon a szokásos skalárszorzatot. Adjuk meg az alábbi transzformációk adjungáltját:

(a) tükrözés az x-tengelyre;
(b) tükrözés az origón átmenő tetszőleges egyenesre;
(c) az origó körüli (pozitív irányú) 90 fokos elforgatás;
(d) az origó körüli tetszőleges szögű elforgatás;
(e) merőleges vetítés az x-tengelyre;
(f) merőleges vetítés az origón átmenő tetszőleges egyenesre;
(g) az y-tengellyel párhuzamos vetítés a 45 fokos $y = x$ egyenesre;
(h) az a lineáris transzformáció, amely az x-tengely pontjait helybenhagyja, az y-tengely pontjait pedig -90 fokkal elforgatja.

8.4.3 Tekintsük a térben a szokásos skalárszorzatot, és legyen $\mathbf{c}$ egy rögzített vektor. Az $\mathcal{A}$ transzformáció egy $\mathbf{u}$ vektorhoz rendelje hozzá az $\mathbf{u} \times \mathbf{c}$ vektoriális szorzatot. Határozzuk meg $\mathcal{A}^*$-ot.

8.4.4 Tekintsük a 8.1.4 feladatban definiált euklideszi tereket, és határozzuk meg a kétszeri differenciálás (az $f \to f''$ lineáris transzformáció) adjungáltját.

8.4.5 Mutassuk meg, hogy ha $\mathcal{A}^2 = \mathcal{O}$, akkor minden $\mathbf{x}$-re $\mathcal{A}\mathbf{x} \perp \mathcal{A}^*\mathbf{x}$. Igaz-e az állítás megfordítása?

8.4.6 Tekintsük $\mathcal{A}$ és $\mathcal{A}^*$ egy-egy sajátvektorát. Bizonyítsuk be, hogy vagy a hozzájuk tartozó sajátértékek egymás konjugáltjai, vagy pedig a két sajátvektor merőleges egymásra.

8.4.7 Igazoljuk, hogy valós euklideszi térben $\mathcal{A}$ és $\mathcal{A}^*$ karakterisztikus polinomja, minimálpolinomja és sajátértékei megyegyeznek, komplex esetben pedig egymás konjugáltjai lesznek. (Egy polinom konjugáltján az együtthatók konjugálásával nyert polinomot értjük.)

8.4.8 Lássuk be, hogy $\operatorname{Ker}\mathcal{A}^* = (\operatorname{Im}\mathcal{A})^\perp$ és $\operatorname{Im}\mathcal{A}^* = (\operatorname{Ker}\mathcal{A})^\perp$.

8.4.9 Igazoljuk, hogy $\mathcal{A}$ és $\mathcal{A}^*$ kép-, illetve magterei azonos dimenziójúak.

8.4.10 Legyen $A \in \mathbf{C}^{k\times n}, \mathbf{b} \in \mathbf{C}^k$, és tekintsük az $A\mathbf{x} = \mathbf{b}$ lineáris egyenletrendszert (n ismeretlen, k egyenlet). Bizonyítsuk be, hogy ez akkor és csak akkor oldható meg, ha $\mathbf{b}$ merőleges az $A^*\mathbf{z} = \mathbf{0}$ homogén egyenletrendszer minden megoldására (a merőlegességet a $\mathbf{C}^k$ szokásos euklideszi térben értjük).

8.4.11

(a) Bizonyítsuk be, hogy ha $\mathcal{A}^*\mathcal{A} = \mathcal{O}$, akkor $\mathcal{A} = \mathcal{O}$.

(b) Mutassuk meg, hogy $\operatorname{Ker}(\mathcal{A}^*\mathcal{A}) = \operatorname{Ker}\mathcal{A}$ és $\operatorname{Im}(\mathcal{A}^*\mathcal{A}) = \operatorname{Im}\mathcal{A}^*$.

8.4.12 Tegyük fel, hogy $\mathcal{A}^*\mathcal{B} = \mathcal{O}$. Bizonyítsuk be, hogy

(a) $\operatorname{Im}\mathcal{A}$ és $\operatorname{Im}\mathcal{B}$ merőleges alterek;

(b) $\operatorname{Ker}(\mathcal{A}+\mathcal{B}) = \operatorname{Ker}\mathcal{A} \cap \operatorname{Ker}\mathcal{B}$.

Igaz-e az (a), illetve (b) állítás megfordítása?

*8.4.13 Mutassuk meg, hogy ha $\mathcal{A}^*\mathcal{B} = \mathcal{B}\mathcal{A}^* = \mathcal{O}$, akkor $\operatorname{Im}(\mathcal{A}+\mathcal{B}) = \operatorname{Im}\mathcal{A} \oplus \operatorname{Im}\mathcal{B}$.

M*8.4.14 Legyen V egy véges dimenziós vektortér a valós vagy a komplex test felett, és definiáljunk rajta különböző skalárszorzatokat.

(a) Melyek azok az $\mathcal{A} \in \operatorname{Hom} V$ transzformációk, amelyekre $\mathcal{A}^*$ nem függ a skalárszorzattól (tehát bármely skalárszorzat szerint ugyanaz)?

(b) Legyen S_1 és S_2 két skalárszorzat. Mutassuk meg, hogy akkor és csak akkor lesz minden $\mathcal{A} \in \operatorname{Hom} V$ transzformációnak az S_1 és S_2 szerint képzett adjungáltja ugyanaz, ha $S_1 = \lambda S_2$, ahol $\lambda \neq 0$.

8.5. Normális, önadjungált és unitér transzformációk

Ebben a pontban csak (véges dimenziós) *komplex* euklideszi terekkel foglalkozunk. Itt az adjungált segítségével jól le tudjuk írni, mikor létezik egy transzformációnak *ortonormált* sajátvektorokból álló bázisa. Más megfogalmazásban: mely transzformációkhoz található olyan *ortonormált* bázis, amelyben a transzformáció mátrixa diagonális. Ezután két fontos speciális esetet részletesen is megvizsgálunk. A valós euklideszi terekben kissé más a helyzet, ezt a következő pontban tárgyaljuk.

8.5.1 Definíció

Egy $\mathcal{A}$ transzformációt *normális*nak nevezünk, ha felcserélhető az adjungáltjával, azaz $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$. ♣

8.5.2 Tétel

Egy véges dimenziós komplex euklideszi térben akkor és csak akkor létezik az $\mathcal{A}$ transzformációnak *ortonormált* sajátvektorokból álló bázisa, ha $\mathcal{A}$ normális, azaz $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$. ♣

Bizonyítás: Először a feltétel elégségességét igazoljuk, tehát azt, hogy a normalitásból a kívánt bázis létezése következik.

Ha egy, a komplex test feletti vektortérben két transzformáció felcserélhető, akkor van közös sajátvektoruk. Vegyük ugyanis az egyik transzformáció egy sajátalterét. Ez a 6.4.6 feladat szerint a másik transzformációnak invariáns altere. Szorítsuk meg erre az altérre a másik transzformációt, és tekintsük egy tetszőleges sajátvektorát. Ez a két transzformációnak közös sajátvektora lesz.

Vegyük most a felcserélhető $\mathcal{A}$ és $\mathcal{A}^*$ transzformációk egy $\mathbf{e}$ közös sajátvektorát. Alkalmas skalárral beszorozva elérhetjük, hogy $\|\mathbf{e}\| = 1$ legyen. Ez lesz az ortonormált sajátbázis első eleme.

Tekintsük az $U = \langle \mathbf{e} \rangle^\perp$ merőleges kiegészítő alteret. Mivel $\langle \mathbf{e} \rangle$ invariáns altere volt $\mathcal{A}$-nak, illetve $\mathcal{A}^*$-nak, ezért (a 8.4.3 Tétel szerint) U invariáns altere $\mathcal{A}^*$-nak, illetve $\mathcal{A}$-nak. Ennek alapján a fenti eljárást az U altéren megismételhetjük stb. Így végül egy ortonormált sajátbázishoz jutunk.

A szükségességre rátérve, azt kell megmutatnunk, hogy ortonormált sajátbázis létezéséből $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$ következik. Vegyük $\mathcal{A}$ egy ortonormált sajátbázisát, ebben az $[\mathcal{A}]$ mátrix diagonális. Ekkor az ortonormáltság miatt $[\mathcal{A}^*] = [\mathcal{A}]^*$, tehát $[\mathcal{A}^*]$ is diagonális mátrix. Két diagonális mátrix pedig felcserélhető, és így a megfelelő transzformációk, azaz $\mathcal{A}$ és $\mathcal{A}^*$ is felcserélhetők. ■

A normális transzformációkra még egy érdekes karakterizációt adunk. További ekvivalens feltételeket a 8.5.10 feladat tartalmaz.

8.5.3 Tétel
Az $\mathcal{A}$ transzformáció akkor és csak akkor normális, ha $\mathcal{A}^*$ felírható az $\mathcal{A}$ polinomjaként, azaz van olyan $f \in \mathbf{C}[x]$, amellyel $\mathcal{A}^* = f(\mathcal{A})$. ♣

Bizonyítás: Ha $\mathcal{A}^* = f(\mathcal{A})$, akkor $\mathcal{A}\mathcal{A}^* = \mathcal{A}f(\mathcal{A}) = f(\mathcal{A})\mathcal{A} = \mathcal{A}^*\mathcal{A}$, hiszen $\mathcal{A}$ a hatványaival és $\mathcal{E}$-vel nyilván felcserélhető.

A megfordításhoz tegyük fel, hogy $\mathcal{A}\mathcal{A}^* = \mathcal{A}^*\mathcal{A}$. Az előző tétel szerint ekkor van olyan ortonormált bázis, amelyben az $[\mathcal{A}]$ mátrix diagonális és $[\mathcal{A}^*] = [\mathcal{A}]^*$. Legyenek $[\mathcal{A}]$ főátlójának elemei $\lambda_1, \ldots, \lambda_k$, ekkor $[\mathcal{A}^*]$ főátlójának elemei $\overline{\lambda_1}, \ldots, \overline{\lambda_k}$. Legyen n a különböző λ_j-k száma. Olyan $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_{n-1}x^{n-1}$ komplex együtthatós polinomot keresünk, amelyre $\mathcal{A}^* = f(\mathcal{A})$. Ezt a transzformációk helyett a diagonális mátrixokra felírva, az

$$\alpha_0 + \alpha_1\lambda_j + \ldots + \alpha_{n-1}\lambda_j^{n-1} = \overline{\lambda_j}, \quad j = 1, 2, \ldots, k$$

egyenletrendszer adódik (ahol az α_i-k az ismeretlenek). Az azonos λ-khoz tartozó egyforma egyenletekből csak egyet megtartva egy olyan $n \times n$-es egyenletrendszerhez jutunk, amelynek a determinánsa a különböző λ_j-k által generált Vandermonde-determináns. Mivel ez nem nulla, az egyenletrendszer (egyértelműen) megoldható, és így egy megfelelő f polinomot kapunk. (Hivatkozhattunk volna az interpolációs polinomokra bizonyított 3.2.4 Tételre is.) ■

A normális transzformációk két legfontosabb osztálya, amikor $\mathcal{A}^* = \mathcal{A}$, illetve $\mathcal{A}^* = \mathcal{A}^{-1}$, ezek az önadjungált, illetve az unitér transzformációk.

8.5.4 Definíció
Az $\mathcal{A}$ transzformáció *önadjungált*, ha $\mathcal{A}^* = \mathcal{A}$. ♣

Azonnal látszik, hogy egy önadjungált transzformáció normális, így létezik ortonormált sajátbázisa. A normális transzformációk közül pontosan azok önadjungáltak, amelyeknek a sajátértékei valósak (8.5.1 feladat).

8.5.5 Definíció
Az $\mathcal{A}$ transzformáció *unitér*, ha $\mathcal{A}^* = \mathcal{A}^{-1}$. ♣

Világos, hogy egy unitér transzformáció is normális, így létezik ortonormált sajátbázisa. A normális transzformációk közül pontosan azok unitérek, amelyeknek a sajátértékei egységnyi abszolút értékűek (8.5.3 feladat).

Az unitér transzformációk azzal jellemezhetők, hogy skalárszorzat-, norma-, illetve távolságtartók:

8.5.6 Tétel

Egy $\mathcal{A}$ transzformáció unitérsége az alábbi feltételek bármelyikével ekvivalens:

I. Skalárszorzattartás: $\mathbf{x}, \mathbf{z} \in V \Rightarrow (\mathcal{A}\mathbf{x})\cdot(\mathcal{A}\mathbf{z}) = \mathbf{x}\cdot\mathbf{z}$.

II. Normatartás: $\mathbf{x} \in V \Rightarrow \|\mathcal{A}\mathbf{x}\| = \|\mathbf{x}\|$.

III. Távolságtartás: $\mathbf{x}, \mathbf{z} \in V \Rightarrow \tau(\mathcal{A}\mathbf{x}, \mathcal{A}\mathbf{z}) = \tau(\mathbf{x}, \mathbf{z})$. ♣

Bizonyítás: (I.) $(\mathcal{A}\mathbf{x})\cdot(\mathcal{A}\mathbf{z}) = \mathbf{x}\cdot(\mathcal{A}^*\mathcal{A}\mathbf{z}) = \mathbf{x}\cdot\mathbf{z}$ minden $\mathbf{x}, \mathbf{z}$-re pontosan akkor teljesül, ha $\mathcal{A}^*\mathcal{A} = \mathcal{E}$.

(II.) A norma speciális skalárszorzat, így a skalárszorzattartásból a normatartás következik. A megfordításhoz azt kell felhasználni, hogy a norma segítségével is egyértelműen felírható a skalárszorzat.

(III.) A távolságot a norma segítségével definiáltuk, tehát a normatartásból következik a távolságtartás. A megfordítás az $\|\mathbf{u}\| = \tau(\mathbf{u}, \mathbf{0})$ összefüggésből adódik. ■

Feladatok

8.5.1

(a) Bizonyítsuk be, hogy egy normális transzformáció akkor és csak akkor önadjungált, ha a sajátértékei valósak.

(b) Igaz-e, hogy ha egy transzformáció sajátértékei valósak, akkor szükségképpen önadjungált?

8.5.2 Mutassuk meg, hogy egy $\mathcal{A}$ önadjungált transzformációra az $\mathcal{A}, \mathcal{A}^2, \ldots, \mathcal{A}^m, \ldots$ transzformációk vagy mind különbözők, vagy pedig legfeljebb két különböző van közöttük.

8.5.3

(a) Bizonyítsuk be, hogy egy normális transzformáció akkor és csak akkor unitér, ha a sajátértékei egységnyi abszolút értékűek.

(b) Igaz-e, hogy ha egy transzformáció sajátértékei egységnyi abszolút értékűek, akkor szükségképpen unitér?

8.5.4 Igaz-e, hogy egy véges dimenziós komplex vektortéren bármely $\mathcal{A}$ lineáris transzformáció normálissá tehető, azaz értelmezhető úgy egy skalárszorzat, hogy $\mathcal{A}$ normális legyen?

8.5.5 Tekintsük a $\mathbf{C}^4$ szokásos euklideszi teret. Az alábbi transzformációk közül melyek lesznek normálisak, önadjungáltak, illetve unitérek?

$$\mathcal{A}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} 0 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}; \quad \mathcal{B}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} u_4 \\ u_1 \\ u_2 \\ u_3 \end{pmatrix}; \quad \mathcal{C}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} u_1 \\ u_1 \\ u_1 \\ u_1 \end{pmatrix};$$

$$\mathcal{D}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} u_1+u_2+u_3+u_4 \\ u_1+u_2+u_3+u_4 \\ u_1+u_2+u_3+u_4 \\ u_1+u_2+u_3+u_4 \end{pmatrix}; \quad \mathcal{F}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} u_1-u_2 \\ u_2-u_3 \\ u_3-u_4 \\ u_4-u_1 \end{pmatrix}.$$

8.5.6 Legyen $\mathcal{A}$ és $\mathcal{B}$ önadjungált. Önadjungált lesz-e $\mathcal{A}+\mathcal{B}$, $\lambda\mathcal{A}$, $\mathcal{A}^2$, illetve $\mathcal{AB}$? Oldjuk meg a feladatot önadjungált helyett unitér, illetve normális transzformációkra is.

8.5.7

(a) Véleményezze az alábbi gondolatmenetet. Két önadjungált transzformáció szorzata is önadjungált, ugyanis: (i) egy transzformáció akkor és csak akkor önadjungált, ha van olyan ortonormált sajátvektorokból álló bázis, amely szerinti mátrixa diagonális és a főátló elemei valósak; (ii) két ilyen mátrix szorzata megint ilyen mátrixot ad; (iii) ha tehát a két önadjungált transzformáció megfelelő mátrixát felírjuk és összeszorozzuk, akkor a szorzat is ilyen típusú mátrix lesz, vagyis a szorzattranszformáció is önadjungált.

(b) Igazoljuk, hogy az $\mathcal{A}$ és $\mathcal{B}$ önadjungált transzformációk $\mathcal{AB}$ szorzata akkor és csak akkor önadjungált, ha $\mathcal{AB}=\mathcal{BA}$.

8.5.8 Mutassuk meg, hogy egy normális transzformáció sajátalterei páronként merőlegesek. Igaz-e az állítás megfordítása?

8.5.9 Legyen az $\mathcal{A}$ normális transzformáció mátrixa valamely $\mathbf{b}_1,\dots,\mathbf{b}_n$ bázisban A. Melyek igazak az alábbi állítások közül?

(a) Ha a $\mathbf{b}_1,\dots,\mathbf{b}_n$ bázis ortonormált, akkor $AA^*=A^*A$.

(b) Ha $AA^*=A^*A$, akkor a $\mathbf{b}_1,\dots,\mathbf{b}_n$ bázis ortonormált.

8.5.10 Bizonyítsuk be, hogy egy $\mathcal{A}$ transzformáció normalitása az alábbi feltételek bármelyikével ekvivalens.

(a) $\mathbf{x}\in V \Rightarrow \|\mathcal{A}\mathbf{x}\| = \|\mathcal{A}^*\mathbf{x}\|$.

(b) $\mathcal{A}$ és $\mathcal{A}^*$ sajátvektorai azonosak.

(c) Minden λ-ra $\operatorname{Ker}(\mathcal{A}-\lambda\mathcal{E}) = \operatorname{Ker}(\mathcal{A}^*-\overline{\lambda}\mathcal{E})$.

(d) Minden λ-ra $\operatorname{Im}(\mathcal{A}-\lambda\mathcal{E}) = \operatorname{Im}(\mathcal{A}^*-\overline{\lambda}\mathcal{E})$.
(e) Minden λ-ra $\operatorname{Ker}(\mathcal{A}-\lambda\mathcal{E}) \perp \operatorname{Im}(\mathcal{A}-\lambda\mathcal{E})$.

8.5.11 Bizonyítsuk be, hogy ha az $\mathcal{A}$ és $\mathcal{B}$ normális transzformációkra $\mathcal{AB}=\mathcal{O}$, akkor $\mathcal{BA}=\mathcal{O}$ is teljesül.

8.5.12 Mutassuk meg, hogy az $\mathcal{A}$ és $\mathcal{B}$ normális transzformációknak akkor és csak akkor létezik közös ortonormált sajátbázisa, ha $\mathcal{AB}=\mathcal{BA}$.

8.5.13 Lássuk be, hogy ha az $\mathcal{A}$ és $\mathcal{B}$ normális transzformációk felcserélhetők (azaz $\mathcal{AB}=\mathcal{BA}$), akkor $\mathcal{AB}$ is normális. Igaz-e az állítás megfordítása?

8.5.14 Bizonyítsuk be, hogy egy transzformáció akkor és csak akkor normális, ha felírható egy önadjungált és egy unitér transzformáció szorzataként, amelyek egymással felcserélhetők.

8.5.15 Mutassuk meg, hogy egy komplex euklideszi téren minden transzformációhoz létezik olyan ortonormált bázis, amelyben a transzformáció mátrixa felsőháromszög-mátrix.

8.5.16 Legyen V egy n-dimenziós komplex euklideszi tér és $\mathcal{A}$, illetve $\mathcal{A}^*\mathcal{A}$ karakterisztikus polinomjának gyökei (multiplicitással számolva) legyenek $\lambda_1,\dots,\lambda_n$, illetve $\mu_1,\dots,\mu_n$.
(a) Mutassuk meg, hogy $\mu_1,\dots,\mu_n$ nemnegatív valós számok.
(b) Bizonyítsuk be, hogy $\sum_{j=1}^n |\lambda_j|^2 \le \sum_{j=1}^n \mu_j$.
(c) A b)-beli egyenlőtlenségben pontosan akkor áll egyenlőség, ha $\mathcal{A}$ normális.

8.5.17 Bizonyítsuk be, hogy egy transzformáció akkor és csak akkor merőlegességtartó, ha egy unitér transzformáció skalárszorosa.

8.5.18 Írjuk fel egy unitér transzformáció mátrixát egy ortonormált bázisban. Bizonyítsuk be, hogy
(a) két különböző oszlopvektor szokásos $\mathbf{C}^n$-beli skalárszorzata 0, egy oszlopvektor önmagával vett skalárszorzata pedig 1;
(b) ugyanez érvényes oszlopok helyett sorokra is;
(c) a mátrix determinánsának abszolút értéke 1;
(d) a mátrix bármely elemének ugyanannyi az abszolút értéke, mint a hozzá tartozó előjeles aldeterminánsnak.

8.6. Szimmetrikus és ortogonális transzformációk

Most rátérünk a (véges dimenziós) *valós* euklideszi terek néhány transzformációtípusára. Itt már sokkal ritkább az ortonormált sajátbázis, azaz ortonormált bázis szerinti diagonális mátrix: pontosan az önadjungáltnak megfelelő szimmetrikus transzformációknál létezik ilyen. Ez az ún. főtengelytétel, amely többek között a geometriában a másodrendű görbék és felületek leírásánál is fontos szerepet játszik. Az unitérnek megfelelő ortogonális transzformációk esetén csak „kicsit csúnyább" mátrixot tudunk garantálni.

8.6.1 Definíció
Az $\mathcal{A}$ transzformáció *szimmetrikus*, ha $\mathcal{A}^* = \mathcal{A}$. ♣

8.6.2 Tétel (Főtengelytétel)
Egy $\mathcal{A}$ transzformációnak akkor és csak akkor létezik ortonormált sajátbázisa, ha $\mathcal{A}$ szimmetrikus. ♣

Bizonyítás: Ha létezik ortonormált sajátbázis, akkor $\mathcal{A}$-nak ebben felírt mátrixa diagonális, tehát nyilván szimmetrikus, és így $\mathcal{A}$ is szimmetrikus.

A megfordításhoz tegyük fel, hogy $\mathcal{A}$ szimmetrikus. Először belátjuk, hogy $\mathcal{A}$-nak létezik sajátvektora. Mivel a valós test fölött a minimálpolinom legfeljebb másodfokú irreducibilis tényezők szorzata, ezért a 6.5.5 Tétel szerint $\mathcal{A}$-nak létezik egy W legfeljebb 2-dimenziós invariáns altere. Ha $\dim W = 1$, akkor W (bármelyik) generátoreleme sajátvektor. Legyen tehát $\dim W = 2$, és írjuk fel $\mathcal{A}$ (W-re történő megszorításának) mátrixát egy ortonormált bázis szerint. Mivel $\mathcal{A}$ szimmetrikus, ezért ez a mátrix is az: $A = \begin{pmatrix} \alpha & \beta \\ \beta & \delta \end{pmatrix}$. Az $\mathcal{A}$ karakterisztikus polinomja $k_{\mathcal{A}} = x^2 - (\alpha + \delta)x + (\alpha\delta - \beta^2)$. Ennek a diszkriminánsa $(\alpha + \delta)^2 - 4(\alpha\delta - \beta^2) = (\alpha - \delta)^2 + 4\beta^2 \geq 0$, tehát $k_{\mathcal{A}}$-nak van (valós) gyöke. Ez a gyök $\mathcal{A}$-nak sajátértéke, így van sajátvektor is.

Legyen $\mathbf{e}_1$ az $\mathcal{A}$ egy egységnyi normájú sajátvektora. Ekkor az $U = \langle \mathbf{e}_1 \rangle^\perp$ merőleges kiegészítő altér invariáns altere $\mathcal{A}^* = \mathcal{A}$-nak. Ennek alapján a fenti eljárást az U altéren megismételhetjük stb. Így végül egy ortonormált sajátbázishoz jutunk. ■

A geometria szempontjából a szimmetrikus mátrixot egy szimmetrikus bilineáris függvény mátrixaként érdemes tekinteni. A főtengelytétel ekkor a következő állítással ekvivalens: egy szimmetrikus bilineáris függvény úgy is ortogonalizálható, hogy a bázis az (euklideszi térben eleve) adott skalárszorzatra nézve is ortonormált legyen. Ez speciálisan a közönséges sík, illetve tér má-

sodrendű görbéire, illetve felületeire vonatkozólag azt jelenti, hogy léteznek *merőleges* sajátirányok. Ezekkel felírva az adott görbének, illetve felületnek megfelelő kvadratikus alakot, az (konstans együtthatókkal — a sajátértékekkel — képezett) négyzetösszeg lesz.

A főtengelytétel előbbi alakja úgy is fogalmazható, hogy két szimmetrikus bilineáris függvény egyszerre is ortogonalizálható, ha legalább az egyikük skalárszorzat, azaz pozitív definit.

A főtengelytétel transzformációs és bilineáris függvényes alakjának ekvivalenciája némi meggondolást igényel, ugyanis más bázisra történő áttérésnél általában másképp változik egy transzformáció és másképp egy bilineáris függvény mátrixa. Jelen esetben ez azért nem okoz gondot, mert *ortonormált* bázisok szerepelnek, és ekkor egyformán módosulnak a mátrixok.

Most rátérünk az unitér transzformációk valós megfelelőjére.

8.6.3 Definíció

Az $\mathcal{A}$ transzformáció *ortogonális*, ha $\mathcal{A}^* = \mathcal{A}^{-1}$. ♣

8.6.4 Tétel

Egy $\mathcal{A}$ transzformáció akkor és csak akkor ortogonális, ha létezik olyan ortonormált bázis, amely szerint $\mathcal{A}$ mátrixa a főátlóra fűzött 2×2-es és 1×1-es blokkokból áll: a 2×2-es blokkok $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ alakúak, az 1×1-esek pedig ±1-ek (és a mátrix többi eleme 0). ♣

Másképp fogalmazva: V páronként ortogonális $\mathcal{A}$-invariáns „síkok” és „egyenesek” direkt összege, amelyek mindegyikén $\mathcal{A}$ valamilyen (origó körüli) forgatás.

Általában ortonormált sajátbázis nem létezik, hiszen pl. a sík (origó körüli) forgatása ortogonális transzformáció, de (ha a szög nem $k\pi$, akkor) nincs sajátvektora.

Bizonyítás: Ha létezik ilyen bázis, akkor egyszerű számolással adódik, hogy a fenti alakú mátrixot a transzponáltjával megszorozva az egységmátrixot kapjuk. Így a mátrix transzponáltja éppen az inverze, és ekkor (a bázis ortonormáltsága miatt) ugyanez érvényes a transzformációra is.

A megfordításhoz tegyük fel, hogy $\mathcal{A}$ ortogonális, azaz $\mathcal{A}^* = \mathcal{A}^{-1}$. Az előző tétel bizonyításához hasonlóan $\mathcal{A}$-nak létezik egy legfeljebb 2-dimenziós W invariáns altere. Ha $\dim W = 1$, akkor W (bármelyik) generátoreleme sajátvektor, és a hozzátartozó sajátérték az ortogonalitás miatt ±1.

Ha $\dim W = 2$, akkor írjuk fel $\mathcal{A}$ (W-re történő megszorításának) mátrixát

egy ortonormált bázis szerint. Mivel $\mathcal{A}^* = \mathcal{A}^{-1}$, ezért a mátrix transzponáltja egyben az inverze. Így $D = \det A = \det A^* = \det A^{-1} = 1/D$, tehát $D = \pm 1$.

Ha $A = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$, akkor $A^* = \begin{pmatrix} \alpha & \gamma \\ \beta & \delta \end{pmatrix}$, és az inverzre az előjeles aldeterminánsokkal adott képlet szerint $A^{-1} = \begin{pmatrix} \delta/D & -\beta/D \\ -\gamma/D & \alpha/D \end{pmatrix}$. Tehát

$$A^* = A^{-1} \iff \alpha = \delta/D, \gamma = -\beta/D, \beta = -\gamma/D, \delta = \alpha/D.$$

Ha $D = -1$, akkor $\beta = \gamma$ (és $\alpha = -\delta$). Mivel A szimmetrikus, a 8.6.2 Tétel szerint létezik ortonormált sajátbázisa. Továbbá, $k_A = x^2 - 1$ alapján a két sajátérték 1 és -1. (Más nem is lehetne, hiszen $\mathcal{A}$ ortogonális.)

A $D = 1$ esetben az adódik, hogy $A = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$ alakú, ahol $\alpha^2 + \beta^2 = 1$. Ez azt jelenti, hogy alkalmas θ-ra $A = \begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$.

Legyen most $U = W^\perp$. Ekkor U invariáns altere $\mathcal{A}^* = \mathcal{A}^{-1}$-nek. Mivel $\mathcal{A}$ és $\mathcal{A}^{-1}$ invariáns alterei könnyen láthatóan megegyeznek, ezért U invariáns altere $\mathcal{A}$-nak is. Ennek alapján a fenti eljárást az U altéren megismételhetjük stb. Így végül egy megfelelő ortonormált bázishoz jutunk. ■

Feladatok

8.6.1 Bizonyítsuk be, hogy ha $\mathcal{A}$ egyszerre szimmetrikus és ortogonális transzformáció, akkor $\mathcal{A}^2 = \mathcal{E}$. Igaz-e az állítás megfordítása?

8.6.2 Mutassuk meg, hogy egy szimmetrikus transzformáció sajátalterei páronként merőlegesek. Igazoljuk ugyanezt ortogonális transzformációkra is.

8.6.3 Tekintsük az $\mathbf{R}^4$ szokásos valós euklideszi teret. Az alábbi transzformációk közül melyek lesznek szimmetrikusak, illetve ortogonálisak? A szimmetrikusaknál adjunk meg ortonormált sajátbázist, és írjuk fel a megfelelő mátrixot. Az ortogonálisoknál adjunk meg egy, a 8.6.4 Tételben előírt ortonormált bázist, és itt is írjuk fel az ehhez tartozó mátrixot.

$$\mathcal{A}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} u_4 \\ u_3 \\ u_2 \\ u_1 \end{pmatrix}; \qquad \mathcal{B}\begin{pmatrix} u_1 \\ u_2 \\ u_3 \\ u_4 \end{pmatrix} = \begin{pmatrix} u_1 + u_2 \\ u_1 - u_2 \\ u_3 + u_4 \\ u_3 - u_4 \end{pmatrix};$$

$$\mathcal{C}\begin{pmatrix}u_1\\u_2\\u_3\\u_4\end{pmatrix}=\begin{pmatrix}u_4\\u_1\\u_2\\u_3\end{pmatrix};\qquad \mathcal{D}\begin{pmatrix}u_1\\u_2\\u_3\\u_4\end{pmatrix}=\begin{pmatrix}u_1+u_2+u_3+u_4\\u_1+u_2+u_3+u_4\\u_1+u_2+u_3+u_4\\u_1+u_2+u_3+u_4\end{pmatrix};$$

$$\mathcal{F}\begin{pmatrix}u_1\\u_2\\u_3\\u_4\end{pmatrix}=\begin{pmatrix}(u_1-u_2+u_3-u_4)/2\\(u_1-u_2-u_3+u_4)/2\\(u_1+u_2+u_3+u_4)/2\\(u_1+u_2-u_3-u_4)/2\end{pmatrix}.$$

8.6.4 Van-e olyan $\mathcal{A}$, amelyre $\mathcal{A}^*=-\mathcal{A}^{-1}$?

8.6.5 Melyek igazak az alábbi állítások közül?

(a) Ha $\mathcal{A}$ szimmetrikus, akkor $\mathcal{A}^2$ is szimmetrikus.

(b) Ha $\mathcal{A}^2$ szimmetrikus, akkor $\mathcal{A}$ is szimmetrikus.

(c) Ha $\mathcal{A}^2$ szimmetrikus, és $\mathcal{A}$-nak létezik (nem feltétlenül ortonormált bázis szerinti) diagonális mátrixa, akkor $\mathcal{A}$ is szimmetrikus.

(d) Ha $\mathcal{A}$ ortogonális, akkor $\mathcal{A}^2$ is ortogonális.

(e) Ha $\mathcal{A}^2$ ortogonális, akkor $\mathcal{A}$ is ortogonális.

8.6.6 Tegyük fel, hogy $\mathcal{A}\mathcal{A}^*=\mathcal{A}^*\mathcal{A}$ és $\mathcal{A}^k$ ortogonális valamilyen k-ra ($k>1$). Bizonyítsuk be, hogy ekkor $\mathcal{A}$ is ortogonális. Igaz-e hasonló állítás (ortogonális helyett) a szimmetrikus esetben?

8.6.7 Tegyük fel, hogy $\operatorname{Ker}\mathcal{A}=\mathbf{0}$ és $\mathcal{A}^*=\mathcal{A}^m$ valamilyen $m>1$-re. Bizonyítsuk be, hogy $\mathcal{A}$ ortogonális.

8.6.8 Legyen $(k,t)=1$, és tegyük fel, hogy $\mathcal{A}$-nak létezik inverze. Igazoljuk, hogy $\mathcal{A}^k$ és $\mathcal{A}^t$ akkor és csak akkor lesznek mindketten szimmetrikusak, ha $\mathcal{A}$ szimmetrikus. Lássuk be a hasonló állítást ortogonális transzformációkra is.

8.6.9 Igazoljuk a 8.5.17–8.5.18 feladatok megfelelőit ortogonális transzformációkra.

8.6.10 Jellemezzük geometriailag a sík és a tér szimmetrikus, illetve ortogonális transzformációit.

8.6.11 Mutassuk meg, hogy ha $\mathcal{A}^*$ felírható az $\mathcal{A}$ polinomjaként, akkor V előáll páronként ortogonális, legfeljebb 2-dimenziós $\mathcal{A}$-invariáns alterek direkt összegeként. Igaz-e az állítás megfordítása?

*8.6.12 Mutassuk meg, hogy $\mathcal{A}^*$ akkor és csak akkor írható fel az $\mathcal{A}$ polinomjaként, ha $\mathcal{A}\mathcal{A}^*=\mathcal{A}^*\mathcal{A}$.

9. KOMBINATORIKAI ALKALMAZÁSOK

A lineáris algebra alkalmazási területei igen szerteágazóak. Sokan azonban úgy vélik, hogy meglehetősen sok előismeretre van szükség mind lineáris algebrából, mind pedig az alkalmazási területről ahhoz, hogy az alkalmazásokhoz valóban el lehessen jutni. Ebben a fejezetben megmutatjuk, hogy számos kombinatorikai alkalmazás szinte semmilyen előismeretet sem igényel, és mégis komoly és meglepő eredményeket tudunk így elérni. Látni fogjuk, hogy sokszor csak az egyenletrendszerekre vonatkozó legalapvetőbb összefüggéseket kell felhasználni (Gauss-kiküszöbölés és következményei, 3.1 pont). Lesznek természetesen olyan részek is, amikor ennél jóval mélyebb dolgokra támaszkodunk (beleértve pl. még a véges testek szerkezetét is).

Az alkalmazásokat nemcsak a szoros értelemben vett kombinatorika és gráfelmélet területéről választottuk, hanem jónéhány számelméleti és geometriai problémát is tárgyalunk. A fejezet címében szereplő „kombinatorikai" jelző ennek megfelelően inkább az alkalmazások (nagyon tágan értelmezett) kombinatorikai *jelleg*ére utal. (A lineáris algebra más „típusú", de ugyancsak alapvetően fontos alkalmazásai leginkább az analízis különböző területeihez, pl. a differenciálegyenletek elméletéhez kapcsolódnak, ilyenekkel azonban ennek a könyvnek a keretein belül nem foglalkozunk.) A problémák válogatása és rendszerezése önkényesen történt, igyekeztünk sokféle témát és módszert bemutatni. Előnyben részesítettük az olyan kérdéseket, amelyek más érdekes — nem feltétlenül lineáris algebrai — összefüggésekhez is elvezetnek.

9.1. Szép polinomok

Bevezetésül egy polinomokra vonatkozó feladatot tárgyalunk, amelyről ránézésre egyáltalán nem látszik a lineáris algebrai kapcsolat.

9.1.1 Tétel
Minden nem nulla f polinomnak van olyan nem nulla $g = fh$ polinomszorosa, hogy g-ben minden tag kitevője prímszám. ♣

A tétel bármilyen test feletti polinomokra érvényes, de fennáll pl. egész együtthatós polinomokra is. Ez utóbbi a racionális együtthatós esetből azonnal következik: az (egész együtthatós) f-et racionális együtthatósként tekintve, az így kapott h-t végig kell szorozni az együtthatók nevezőinek a legkisebb közös többszörösével.

A tételre három különböző lineáris algebrai megoldást adunk egyenletrendszerek, alterek dimenziója, illetve a leképezések dimenziótétele segítségével.

A bizonyításokból látni fogjuk, hogy a tétel ugyanúgy igaz, ha a prímszámok helyett pozitív egészek tetszőleges végtelen sorozatát vesszük, és azt írjuk elő, hogy csak ilyen kitevőjű tagok forduljanak elő g-ben. (Az állítás nyilván akkor „mutatós", ha valamilyen érdekes sorozatot választunk, ki-ki ízlése szerint a prímeket, a Fibonacci-számokat, a kettőhatványokat stb., közben persze ügyelni kell arra, nehogy véletlenül az adott speciális sorozatra az állítás triviálisan adódjon.)

Első bizonyítás: Legyen $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_t x^t$, $\alpha_t \neq 0$, és keressük h-t $h = \beta_0 + \beta_1 x + \ldots + \beta_n x^n$ alakban, ahol n-et is később fogjuk alkalmasan megválasztani. Az fh szorzást elvégezve a nem prím kitevőjű tagok együtthatóira 0-t kell kapnunk; ez egy olyan homogén lineáris egyenletrendszert jelent a β_j-kre, ahol az együtthatók az α-k közül kerülnek ki. (Az első néhány egyenlet: $\alpha_0\beta_0 = 0, \alpha_0\beta_1 + \alpha_1\beta_0 = 0, \alpha_0\beta_4 + \ldots + \alpha_4\beta_0 = 0$ stb.) Itt az ismeretlenek száma $n+1$, az egyenletek száma pedig a $0, 1, 2, \ldots, n+t$ közül a nemprímek száma, azaz $n+t+1-\pi(n+t)$, ahol $\pi(s)$ az s-nél nem nagyobb (pozitív) prímek számát jelöli. Ha több az ismeretlen, mint az egyenlet, akkor a homogén lineáris egyenletrendszernek biztosan van nem triviális megoldása, ami éppen egy megfelelő h polinomot ad. Ez az $n+1 > n+t+1-\pi(n+t)$ egyenlőtlenség pontosan akkor teljesül, ha $\pi(n+t) > t = \deg f$. Ha tehát n-et ennek megfelelően választjuk, akkor ebből a kívánt tulajdonságú g létezése következik. ■

Második bizonyítás: Legyen s később alkalmasan megválasztandó pozitív egész és V a legfeljebb s-edfokú polinomok szokásos vektortere (beleértve a nulla polinomot is). Tekintsük V alábbi két részhalmazát: W_1 álljon azokból a (legfeljebb s-edfokú) polinomokból, amelyekben minden tag kitevője prímszám, W_2 pedig azokból, amelyek oszthatók f-fel. Nyilván W_1 és W_2 altér V-ben, továbbá $\dim V = s+1$, $\dim W_1 = \pi(s)$, $\dim W_2 = s-t+1$. Ha $\dim W_1 + \dim W_2 > \dim V$, akkor $W_1 \cap W_2 \neq \mathbf{0}$ (lásd a 4.6.6 feladatot), és $W_1 \cap W_2$ bármely nem nulla eleme megfelel g-nek. A $\dim W_1 + \dim W_2 > \dim V$ feltétel pedig pontosan akkor teljesül, ha $\pi(s) > t = \deg f$ (ami megegyezik az első bizonyításban kapott előírással). ■

Harmadik bizonyítás: Legyen W_1 és V ugyanaz, mint a második bizonyításban, és tekintsük azt az $\mathcal{A} : W_1 \to V$ lineáris leképezést, amely minden polinomnak megfelelteti az f polinommal történő maradékos osztásnál keletkező

maradékot. Ekkor $\operatorname{Ker}\mathcal{A}$ éppen az f-fel osztható és csupa prím kitevőjű tagból álló (legfeljebb s-edfokú) polinomok halmaza. Ha $\dim \operatorname{Im}\mathcal{A} < \dim W_1$, akkor a dimenziótétel szerint $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$, és így $\operatorname{Ker}\mathcal{A}$ bármely nem nulla eleme megfelel g-nek. Nyilván $\operatorname{Im}\mathcal{A}$ altér a legfeljebb $t-1$-edfokú polinomok vektorterében, tehát $\dim \operatorname{Im}\mathcal{A} \leq t$, továbbá $\dim W_1 = \pi(s)$. Így $\dim \operatorname{Im}\mathcal{A} < \dim W_1$ következik a (korábbi bizonyításoknál is látott) $\pi(s) > t = \deg f$ feltételből. ■

Feladatok

M 9.1.1 *Számkitalálás.*

(a) Micimackó gondolt húsz egész számot, ezek $x_1, x_2, \ldots, x_{20}$. Malacka megkérdezheti tőle bármely olyan kifejezés értékét, amelyet ezekből az összeadás és kivonás segítségével képezünk, pl. mennyi $x_1 + 8x_2 - -7x_3$. A következő kérdés mindig függhet az előzőre kapott választól. Legkevesebb hány kérdéssel tudja Malacka kitalálni a húsz számot?

*(b) Mennyiben változik a helyzet, ha Micimackó elárulta, hogy pozitív egészekre gondolt?

*(c) És ha szorozni is lehet (azaz Malacka az x_i-kből képezett bármilyen egész együtthatós polinom értékét is megkérdezheti, pl. mennyi $x_1 + 8x_2^3x_5$)?

M 9.1.2 *Súlyok.* Adott 13 súly. Akármelyiket is hagyjuk el, a maradék 12 darab beosztható két hatos csoportba úgy, hogy az egyes csoportokban levő súlyok összege megegyezik. Bizonyítsuk be, hogy mind a 13 súly egyenlő.

9.1.3 Igaz marad-e az előző feladat állítása akkor is, hogy nem követeljük meg, hogy a két egyenlő súlyú csoportban azonos számú súly szerepeljen?

M*9.1.4 *Unalmas vektorok.*

(a) Nevezzünk egy $\mathbf{R}^m$-beli vektort unalmasnak, ha a koordinátái között legfeljebb két különböző érték fordul elő (azaz például minden koordinátája -1 vagy $\sqrt{2}$). Legkevesebb hány unalmas vektor összegeként állítható elő (i) $\begin{pmatrix} 1 \\ 2 \\ \vdots \\ m \end{pmatrix}$; (ii) egy tetszőleges $\mathbf{R}^m$-beli vektor?

(b) Mi a helyzet, ha az unalmas vektor definícióját arra módosítjuk, hogy a koordinátái között legfeljebb k különböző érték fordulhat elő?

(c) Megváltoznak-e az előzőkben kapott eredmények, ha a valós számok helyett az F_p modulo p testet vesszük?

Megjegyzés: a (c) részben azért fogalmaztunk csak ilyen óvatosan, mert a (ii) kérdésnél nem látjuk, hogy az F_p testre vonatkozó minimumot hogyan lehetne minden esetre (azaz m és p bármely értékére) pontosan megadni.

M 9.1.5 *Vetélkedő.*

(a) Egy 32 fős osztály vetélkedősorozatot szervez. Minden fordulóban két csapat vetélkedik, tetszőleges létszámmal. Egy csapat állhat akár egy főből is, és nem szükséges, hogy minden diák minden fordulóban résztvegyen. Csak annyit követelünk meg, hogy a vetélkedősorozat folyamán bármely két diák legalább egyszer egymás ellenfele legyen (azaz legyen olyan forduló, amikor különböző csapatban szerepelnek). Legkevesebb hány fordulóban lehet a versenyt lebonyolítani?

*(b) Mennyi a fordulók minimális száma, ha a versenyt úgy kell megrendezni, hogy bármely két diák *pontosan* egy alkalommal legyen egymás ellenfele?

M*9.1.6 *Kicsi és nagy metszetek.*

(a) Létezik-e a pozitív egészeknek (a1) megszámlálhatóan végtelen; (a2) kontinuum sok olyan részhalmaza, amelyek közül bármely kettő metszete végtelen, de bármely három metszete véges?

(b) Oldjuk meg a feladatot, ha úgy módosul a második feltétel, hogy bármely három részhalmaz metszete az üres halmaz.

9.1.7 *Páratlan távolságok.* Létezik-e (a) a (közönséges háromdimenziós) térben; *(b) a síkon négy olyan pont, amelyek közül bármely kettő távolsága páratlan egész szám?

*9.1.8 *Cauchy-féle függvényegyenlet.* Tekintsük azokat a minden valós számon értelmezett f valós értékű függvényeket, amelyekre bármely a, b valós szám esetén fennáll az $f(a+b) = f(a) + f(b)$ egyenlőség.

(a) Mutassuk meg, hogy a racionális számok halmazán szükségképpen $f(x) = cx$ (alkalmas c konstanssal).

(b) Ha f legalább egy pontban folytonos, akkor $f(x) = cx$ minden valós x-re.

(c) Ha f egy akármilyen kis intervallumban korlátos, akkor $f(x) = cx$ minden valós x-re.

(d) Van olyan $f(x) \neq cx$ függvény, amely kielégíti a Cauchy-féle függvényegyenletet.

9.1.9 *Felezés*. Felbontható-e a pozitív (a) racionális; *(b) valós számok halmaza két olyan diszjunkt, nem üres részhalmazra, amelyek zártak az összeadásra?

*9.1.10 *Polinomok és periodikus függvények*.

(a) Felírható-e a (a1) $\mathbf{Q}$; (a2) $\mathbf{R}$ halmazon értelmezett $f(x) = x$ identitásfüggvény két (ugyanitt értelmezett) periodikus függvény összegeként?

(b) Felírható-e egy n-edfokú ($n \geq 1$) valós együtthatós polinomfüggvény (b1) n; (b2) $n+1$ darab (minden valós számon értelmezett) periodikus függvény összegeként?

9.2. Fibonacci-számok

Ebben a pontban a *Fibonacci-számok* képletét határozzuk meg, amelyet már a 4.6.8 feladatban is kitűztünk. Emlékeztetünk arra, hogy a Fibonacci-számok sorozatát a $\varphi_0 = 0, \varphi_1 = 1, \varphi_{j+1} = \varphi_j + \varphi_{j-1}, \quad j = 1, 2, \ldots$ rekurzióval definiáljuk. A sorozat első néhány tagja: $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, \ldots$

9.2.1 Tétel

$$\varphi_n = \frac{1}{\sqrt{5}}\left(\left(\frac{1+\sqrt{5}}{2}\right)^n - \left(\frac{1-\sqrt{5}}{2}\right)^n\right) \clubsuit$$

Megjegyzés: Ha már valahonnan tudjuk, hogy mi a bizonyítandó formula, akkor ezt egyszerűen igazolhatjuk teljes indukcióval. Így azonban nem kapunk magyarázatot arra, hogyan lehet a képletre rájönni (nem valószínű, hogy akár az első ezer tag felírása után sikerül ezt „megsejtenünk"). Az alábbi bizonyításokból a képlethez vezető út is kiderül.

A bizonyítások közül kettő lineáris algebrai, a harmadik pedig az analízis területéről a hatványsorokat veszi igénybe (bár céljainknak az ún. formális hatványsorok algebrai elmélete is megfelelne). Hasonló módszerekkel kezelhetők általában is a *rekurzív sorozatok*, amelyek a matematika számos ágában fontos szerepet játszanak.

Első bizonyítás: Nevezzük a Fibonacci-sorozat általánosításaként Φ-sorozatnak az olyan $\alpha_0, \alpha_1, \ldots$ valós számsorozatokat, amelyek kielégítik az $\alpha_{j+1} = = \alpha_j + \alpha_{j-1}, \quad j = 1, 2, \ldots$ feltételt (és az α_0, α_1 kezdőtagok tetszőleges valós

számok). Egy Φ-sorozat (valós) számszorosa és két Φ-sorozat összege nyilván ismét Φ-sorozat (két sorozat összegét, illetve egy sorozat számszorosát a szokásos módon elemenként képezzük).

Most megpróbáljuk magát az $F = (\varphi_0, \varphi_1, \ldots)$ Fibonacci-sorozatot olyan Φ-sorozatokból előállítani, amelyek tagjaira ismerünk egyszerű képletet. Könnyen adódik, hogy a számtani sorozatok közül csak az azonosan nulla lesz Φ-sorozat, ami nem segít a probléma megoldásában. A mértani sorozatoknál azonban már több szerencsével járunk: az $(\alpha, \alpha\rho, \alpha\rho^2, \ldots)$ mértani sorozat ($\alpha \neq 0$) pontosan akkor Φ-sorozat, ha $\rho^2 = \rho + 1$, ahonnan $\rho_1 = (1 + \sqrt{5})/2$, $\rho_2 = (1 - \sqrt{5})/2$.

Legyen $S_m = (1, \rho_m, \rho_m^2, \ldots)$, $m = 1, 2$, és keressük az F Fibonacci-sorozat előállítását $F = \gamma_1 S_1 + \gamma_2 S_2$ alakban. Mivel mindkét oldalon Φ-sorozat áll, ezért az egyenlőség pontosan akkor teljesül, ha a két kezdőtagra igaz, mert utána a rekurzió miatt öröklődik. A két kezdőtagra felírva ez a $\varphi_0 = 0 = \gamma_1 + \gamma_2, \varphi_1 = 1 = \gamma_1\rho_1 + \gamma_2\rho_2$ összefüggéseket jelenti. Ezt a lineáris egyenletrendszert megoldva $\gamma_1 = 1/\sqrt{5}, \gamma_2 = -1/\sqrt{5}$ adódik. Innen $\varphi_n = \gamma_1\rho_1^n + \gamma_2\rho_2^n$, ami (a ρ_m, γ_m konkrét értékek figyelembe vételével) éppen a tétel állítása. ■

Megjegyzés: Felmerül a kérdés, hol használtunk a megoldásban lineáris algebrát. A bizonyítás a fenti formájában természetesen középiskolai eszközökkel dolgozik, a lineáris algebra inkább a szemléletet, a hátteret adja. Itt tulajdonképpen arról van szó, hogy a Φ-sorozatok vektorterében keresünk alkalmas generátorrendszert, amelynek segítségével az F Fibonacci-sorozatot fel tudjuk írni. Ez a vektortér 2-dimenziós, hiszen a két kezdőtag választható szabadon, azaz a szabadsági fokok száma kettő. (Precízen: „természetes" bázis az 1,0-val és a 0,1-gyel kezdődő két Φ-sorozat; $(1, 0, 1, 1, 2, 3, 5, \ldots)$ és $(0, 1, 1, 2, 3, 5, 8, \ldots)$, ami mellesleg a Fibonacci-sorozat egy eltoltja és maga a Fibonacci-sorozat.) Ebben a 2-dimenziós vektortérben keresünk „szebb alakú" generátorrendszert. A mértani sorozatok közül a fent talált S_1 és S_2 megfelel, hiszen két lineárisan független elem biztosan bázist alkot.

Mindezek alapján nem kell kivételes szerencsének éreznünk, hogy az előállítás sikerült. A mértani sorozatok hányadosait ugyanis egy másodfokú egyenlet gyökeiként kaptuk és csak akkor lettünk volna gondban, ha az egyenletnek többszörös gyöke van. Azonban ez az eset (még a több tagból álló rekurziónál) is kezelhető, lásd a 9.2.3 feladatot.

Második bizonyítás: Legyen $\mathcal{F} : \mathbf{R}^2 \to \mathbf{R}^2$ az $\mathcal{F}\begin{pmatrix} a \\ b \end{pmatrix} = \begin{pmatrix} b \\ a+b \end{pmatrix}$ lineáris

transzformáció. Ekkor $\mathcal{F}\begin{pmatrix}\varphi_{j-1}\\ \varphi_j\end{pmatrix} = \begin{pmatrix}\varphi_j\\ \varphi_{j-1}+\varphi_j\end{pmatrix} = \begin{pmatrix}\varphi_j\\ \varphi_{j+1}\end{pmatrix}$, és így $\mathcal{F}^n\begin{pmatrix}0\\1\end{pmatrix} = \begin{pmatrix}\varphi_n\\ \varphi_{n+1}\end{pmatrix}$.

Tegyük fel, hogy $\mathbf{b}_1, \mathbf{b}_2$ olyan bázis $\mathbf{R}^2$-ben, ahol mindkét $\mathbf{b}_m$ sajátvektora $\mathcal{F}$-nek. Legyenek a megfelelő sajátértékek λ_1, λ_2, ekkor $\mathcal{F}^n\mathbf{b}_m = \lambda_m^n\mathbf{b}_m$, $m = 1, 2$. Ha

$$\begin{pmatrix}0\\1\end{pmatrix} = \delta_1\mathbf{b}_1 + \delta_2\mathbf{b}_2, \tag{9.2.1}$$

akkor

$$\begin{pmatrix}\varphi_n\\ \varphi_{n+1}\end{pmatrix} = \mathcal{F}^n\begin{pmatrix}0\\1\end{pmatrix} = \delta_1\lambda_1^n\mathbf{b}_1 + \delta_2\lambda_2^n\mathbf{b}_2, \tag{9.2.2}$$

és innen az első koordinátaként megkapjuk φ_n-et.

A sajátértékek meghatározásához írjuk fel $\mathcal{F}$ mátrixát pl. az $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}0\\1\end{pmatrix}$ bázisban: $[\mathcal{F}] = \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$. Innen a karakterisztikus polinom $k_\mathcal{F} = x^2 - x - 1$, a sajátértékek ennek a gyökei $\lambda_{1,2} = (1 \pm \sqrt{5})/2$ és a(z egyik) megfelelő sajátbázis $\mathbf{b}_{1,2} = \begin{pmatrix}1\\ (1 \pm \sqrt{5})/2\end{pmatrix}$. Ezt (9.2.1)-be beírva $\delta_1 = -\delta_2 = 1/\sqrt{5}$ adódik, és innen (9.2.2) alapján kapjuk a tétel állítását. ■

Harmadik bizonyítás: Tekintsük az $F(z) = \sum_{n=0}^{\infty}\varphi_n z^n$ hatványsort. Mivel a Fibonacci-számok definíciójából teljes indukcióval könnyen adódik $\varphi_n < 2^n$, emiatt az $F(z)$ hatványsor $|z| < 1/2$-re abszolút konvergens. Ez azért hasznos, mert abszolút konvergens végtelen sorokkal „ugyanúgy számolhatunk", mint ahogyan a véges összegek körében megszoktuk.

Írjuk le egymás alá az $F(z), zF(z)$ és $z^2F(z)$ hatványsorokat:

$$\begin{aligned} F(z) &= \varphi_0 + \varphi_1 z + \varphi_2 z^2 + \ldots + \quad \varphi_n z^n + \ldots \\ zF(z) &= \qquad \varphi_0 z + \varphi_1 z^2 + \ldots + \varphi_{n-1} z^n + \ldots \\ z^2F(z) &= \qquad\qquad + \varphi_0 z^2 + \ldots + \varphi_{n-2} z^n + \ldots \end{aligned}$$

Az első sorból kivonva a másik kettő összegét, a jobb oldalon majdnem minden tag kiesik, és azt kapjuk, hogy $(1 - z - z^2)F(z) = z$, azaz $F(z) = z/(1 - z - z^2)$.

Az $F(z)$-re kapott racionális törtfüggvényt parciális törtekre bontjuk és hatványsorba fejtjük. Legyenek a $z^2 + z - 1$ polinom gyökei μ_1 és μ_2: $\mu_{1,2} = (-1 \pm \sqrt{5})/2$. Ekkor alkalmas β_1, β_2-vel

$$F(z) = \frac{-z}{z^2 + z - 1} = \frac{\beta_1}{1 - \frac{z}{\mu_1}} + \frac{\beta_2}{1 - \frac{z}{\mu_2}} \tag{9.2.3}$$

alakban írható fel. A beszorzások elvégzése után az ezzel ($z \neq \mu_1, \mu_2$-re) ekvivalens $-z = \mu_1\beta_1(\mu_2 - z) + \mu_2\beta_2(\mu_1 - z)$ feltételhez jutunk, azaz $0 = \mu_1\mu_2(\beta_1 + \beta_2)$ és $\mu_1\beta_1 + \mu_2\beta_2 = 1$, ahonnan $\beta_1 = -\beta_2 = 1/\sqrt{5}$. Ezt (9.2.3) jobb oldalára beírva és az $(1 - z/\mu_m)^{-1}$ függvényeket végtelen mértani sorba fejtve kapjuk, hogy

$$F(z) = \beta_1 \sum_{n=0}^{\infty} \Big(\frac{z}{\mu_1}\Big)^n + \beta_2 \sum_{n=0}^{\infty} \Big(\frac{z}{\mu_2}\Big)^n = \sum_{n=0}^{\infty} \Big(\frac{\beta_1}{\mu_1^n} + \frac{\beta_2}{\mu_2^n}\Big) z^n \,.$$

Itt z^n együtthatójára — ami nem más mint φ_n — a tételben megadott értéket nyerjük. (A második bizonyítással összevetve könnyen adódik, hogy $\mu_m = 1/\lambda_m$ és $\beta_m = \delta_m$, $m = 1, 2$.) ■

Feladatok

9.2.1 Számítsuk ki α_{1000}-et, ha $\alpha_1 = \alpha_2 = 1$ és

(a) $\alpha_k = \alpha_{k-1} + 2\alpha_{k-2}$;

(b) $\alpha_k = 2\alpha_{k-1} + \alpha_{k-2}$.

9.2.2 Számítsuk ki α_{1111}-et, ha $\alpha_1 = 3, \alpha_2 = 7$ és

(a) $\alpha_k = 2\alpha_{k-1} - \alpha_{k-2}$;

(b) $\alpha_k = \alpha_{k-1} - \alpha_{k-2}$;

(c) $\alpha_k = \alpha_{k-1} - \alpha_{k-2} + \alpha_{k-3} - \alpha_{k-4}$.

*9.2.3 Tekintsük az $\alpha_k = \mu_1\alpha_{k-1} + \ldots + \mu_t\alpha_{k-t}$ feltételnek eleget tevő $\alpha_0, \alpha_1, \ldots$ komplex számsorozatokat, ahol t rögzített pozitív egész és $\mu_1, \ldots, \mu_t$ rögzített komplex számok, $\mu_t \neq 0$. Legyenek az $f = x^t - \mu_1 x^{t-1} - \ldots - \mu_t$ polinom különböző (komplex) gyökei $\lambda_1, \ldots, \lambda_r$, a multiplicitásuk rendre $s_1, \ldots, s_r$. Mutassuk meg, hogy ekkor $\alpha_n = \sum_{j=1}^{r} g_j(n)\lambda_j^n$, ahol g_j egy legfeljebb $s_j - 1$-edfokú polinom, $j = 1, 2, \ldots, r$, és g_j együtthatói csak az $\alpha_0, \ldots, \alpha_{t-1}$ kezdőértékektől függnek.

9.2.4 Használjuk az előző feladat jelöléseit. Mutassuk meg, hogy az $\alpha_0, \alpha_1, \ldots$ komplex számsorozat akkor és csak akkor lesz periodikus *bármilyen* $\alpha_0, \ldots, \alpha_{t-1}$ kezdőértékek mellett, ha f-nek nincs többszörös gyöke és minden gyöke egységgyök.

9.2.5 Határozzuk meg β_n-et, ha $\beta_k = \beta_{k-1} + \beta_{k-2} + 2, \quad \beta_0 = 0, \beta_1 = 1$.

9.2.6 Mutassuk meg, hogy az n-edik Fibonacci-szám, φ_n éppen a $\tau_n = (1/\sqrt{5})\big((1+\sqrt{5})/2\big)^n$ számhoz legközelebbi egész. Lássuk be azt

is, hogy φ_n és τ_n eltérése 0-hoz tart, ha $n \to \infty$ (azaz φ_n „majdnem" mértani sorozat).

9.2.7

(a) Hányféleképpen lehet egy $2 \times n$-es téglalapot 2×1-es dominókkal kirakni?

*(b) Hányféleképpen lehet egy $3 \times n$-es téglalapot 2×1-es dominókkal kirakni?

*(c) Jelöljük ψ_n-nel, ahányféleképpen egy $3 \times n$-es téglalapot 3×1-es dominókkal ki lehet rakni. Bizonyítsuk be, hogy minden elég nagy n-re $1,46^n < \psi_n < 1,47^n$.

9.2.8 Hány olyan részhalmaza van az $\{1, 2, \ldots, n\}$ számoknak, amelyben nem fordulnak elő szomszédos elemek?

9.2.9 Mutassuk meg, hogy minden pozitív egész felírható különböző Fibonacci-számok összegeként.

9.2.10 Igazoljuk a Fibonacci-számokra vonatkozó alábbi azonosságokat:

(a) $\varphi_{m+n} = \varphi_{m-1}\varphi_n + \varphi_m\varphi_{n+1}$;

(b) $\varphi_{2n-1} = \varphi_{n-1}^2 + \varphi_n^2$;

(c) $\varphi_1 + \varphi_2 + \ldots + \varphi_n = \varphi_{n+2} - 1$;

(d) $\varphi_1 + 2\varphi_2 + \ldots + n\varphi_n = (n+1)\varphi_{n+2} - \varphi_{n+4} + 2$;

(e) $\varphi_1^2 + \varphi_2^2 + \ldots + \varphi_n^2 = \varphi_n\varphi_{n+1}$;

(f) $\varphi_n^2 = \varphi_{n-1}\varphi_{n+1} + (-1)^{n+1}$;

(g) $\varphi_{3n} = 5\varphi_n^3 + 3(-1)^n\varphi_n$;

(h) $\varphi_n = \sum_{j=0}^{\lfloor (n-1)/2 \rfloor} \binom{n-j-1}{j}$;

(i) $\varphi_{2n} = \sum_{j=1}^{n} \binom{n}{j}\varphi_j$.

9.2.11 Bizonyítsuk be, hogy a szomszédos Fibonacci-számok relatív prímek. Mi a helyzet a másodszomszédokkal? És a harmadszomszédokkal?

9.2.12 Lássuk be, hogy minden m-re van végtelen sok m-mel osztható Fibonacci-szám.

*9.2.13 Igazoljuk, hogy $k \mid n \iff \varphi_k \mid \varphi_n$, sőt $\varphi_{(k,n)} = (\varphi_k, \varphi_n)$.

9.2.14

(a) Legyenek $a > b$ olyan pozitív egészek, amelyekre az euklideszi algoritmus *pontosan* n lépésből áll, és ezen belül b a lehető legkisebb. Határozzuk meg b-t.

*(b) Oldjuk meg a feladatot arra az esetre is, amikor az euklideszi algoritmust (a legkisebb nemnegatív maradékok helyett) a legkisebb abszolút értékű maradékokkal végezzük.

*9.2.15 Számítsuk ki a kettőhatvány indexű Fibonacci-számok reciprokaiból képezett végtelen sor összegét.

M**9.2.16 A többtényezős szorzatokat az asszociativitás miatt nem kell zárójelezni. Tekintsünk most egy nemasszociatív műveletet. Hányféle értékű lehet (azaz hányféleképpen zárójelezhető) ekkor egy n-tényezős szorzat?

**9.2.17 Hányféleképpen lehet egy konvex n-szöget a sokszög belsejében egymást nem metsző átlókkal háromszögekre bontani?

9.3. Négyzetszámok keresése

Ebben a pontban azt igazoljuk, hogy ha „elég sok" különböző pozitív egész egyikének sincs egy adott küszöbnél nagyobb prímosztója, akkor a számok közül kiválasztható néhány (esetleg csak egy, esetleg az összes), amelyek szorzata négyzetszám. (Ennek egy konkrét számokkal megfogalmazott változata a 3.3.12 feladatban szerepelt.) Ez a kérdés és annak lineáris algebrai megoldása meglepő módon a nagy számok prímtényezőkre bontásával kapcsolatban fontos szerepet játszik. A prímfelbontásra ugyanis nem ismeretes „gyors" algoritmus; egy (a gyakorlatban is használt) „viszonylag gyors" algoritmust éppen a szóban forgó feladat segítségével konstruálhatunk. (Mint tudjuk, a hatékony prímfelbontási algoritmus kérdése szorosan összefügg az ún. nyilvános jelkulcsú titkosírással, amelyet világszerte alkalmaznak a katonai, diplomáciai és üzleti életben egyaránt.) A feladat másik érdekessége, hogy a megoldásánál — az esetleg egyedül fontosnak hitt valós (vagy racionális vagy komplex) test helyett — természetes módon jelennek meg a modulo 2 maradékosztályok. További izgalmas és részben megoldatlan problémákhoz vezet, ha négyzetszámok helyett köbszámokat vagy tetszőleges magasabb hatványokat vizsgálunk.

9.3.1 Tétel

Legyenek $0 < p_1 < \ldots < p_k$ tetszőleges prímszámok és $0 < c_1 < \ldots < c_{k+1}$ olyan egészek, amelyek egyikének sincs a p_i-ktől különböző prímosztója. Ekkor a c_j számok közül kiválasztható néhány különböző (esetleg csak egy, esetleg az összes) úgy, hogy a szorzatuk négyzetszám legyen. ♣

Azonnal látszik, hogy a tétel $k+1$ helyett k darab c_j-re már nem igaz, legyen pl. $c_j = p_j$.

Első bizonyítás: Képezzük a c_j számainkból valahány különbözőnek a szorzatát minden lehetséges módon. Így $2^{k+1}-1$ szorzatot kapunk. Most vizsgáljuk meg, hogy egy (tetszőleges) szám hányféle lehet abból a szempontból, hogy prímtényezős felbontásában a p_i prímek kitevője páros vagy páratlan; ez 2^k lehetőség. A skatulyaelv alapján tehát a szorzataink között lesz két olyan, amelyekben az egyes prímek kitevői azonos paritásúak. Ha most ebből a két szorzatból elhagyjuk a közös tényezőket, és a megmaradtakat összeszorozzuk, akkor olyan szorzathoz jutunk, amely négyzetszám. ■

Második bizonyítás: Legyen $T = F_2$ a modulo 2 test, és a $c_1, \dots, c_{k+1}$ számoknak feleltessünk meg $\mathbf{c}_j \in T^k$ vektorokat a következőképpen:

$$\mathbf{c}_j = \begin{pmatrix} \gamma_{1j} \\ \vdots \\ \gamma_{kj} \end{pmatrix}, \qquad \gamma_{ij} = \begin{cases} 1, & \text{ha } c_j\text{-ben a } p_i \text{ prím kitevője páratlan;} \\ 0, & \text{ha } c_j\text{-ben a } p_i \text{ prím kitevője páros.} \end{cases}$$

Egy ilyen vektor tehát a számban szereplő prímek kitevőinek a paritását mutatja, és a $\mathbf{c}_j$ vektorok (modulo 2 vett) összeadása a c_j számok szorzásának felel meg. Ez a $k+1$ darab T^k-beli vektor szükségképpen lineárisan összefüggő (a modulo 2 test felett), tehát van olyan nem triviális lineáris kombinációjuk, amely $\mathbf{0}$-t ad. Szorozzuk össze azokat a c_j számokat, amelyeknek megfelelő $\mathbf{c}_j$ vektorok ebben a kombinációban nem nulla (azaz 1) együtthatóval szerepelnek. Mivel a megfelelő $\mathbf{c}_j$ vektorok összege nulla, ezért ez a szorzat négyzetszám. ■

A két bizonyítás közül a lineáris algebrát használó második felesleges nagyágyúnak tűnik. Mégis igen nagy a jelentősége, ugyanis ez egyben *gyors algoritmust* is ad egy jó szorzat megkeresésére (szemben a skatulyaelves első bizonyítással): a lineáris összefüggőségnél egy (homogén) lineáris egyenletrendszert kell megoldani, például Gauss-kiküszöböléssel. Ez a tény annál a fontos gyakorlati alkalmazásnál is lényeges szerepet játszik, amikor egy nagy összetett számot akarunk tényezőkre bontani. Erre a feladatra igazán gyors algoritmus nem ismeretes (szemben azzal, amikor csak a szám prím vagy összetett voltát szeretnénk eldönteni), de a jelenleg használt leggyorsabb módszerek általában a fentiekre (is) támaszkodnak.

Az alábbiakban ezt a faktorizációs eljárást vázoljuk. Legyen N egy nagy páratlan összetett szám, a feladat N-et (nem triviálisan) szorzattá bontani. A teljes hatványok felismerésére és felbontására egyszerűen adhatunk egy jó

algoritmust (lásd a 9.3.7 feladatot), így elég azt az esetet néznünk, amikor N-nek legalább két különböző prímosztója van.

Tegyük fel, hogy

$$(*)\ u^2 \equiv v^2 \pmod{N} \qquad \text{és} \qquad (**)\ u \not\equiv \pm v \pmod{N},$$

azaz $N \mid (u+v)(u-v)$, de $N \nmid u \pm v$. Ekkor N és $u+v$ legnagyobb közös osztója nyilván N-nek egy nem triviális osztója. Ezt a legnagyobb közös osztót az euklideszi algoritmus segítségével „gyorsan" meg tudjuk határozni.

Keressünk most a (*) és (**) feltételeket kielégítő u-t és v-t. Foglalkozzunk egyelőre csak (*)-gal. Először olyan b számokat próbálunk gyártani, amelyekre b^2-nek az N-nel vett (legkisebb pozitív) osztási maradéka, c, csak „kicsi" prímekkel osztható. Ilyen c-t remélhetünk, ha pl. $\sqrt{N}$-nél, $\sqrt{2N}$-nél stb. egy picit nagyobb számot választunk b-nek. Rögzítsünk le egy (N-től függő) R korlátot, és a b számot akkor tartsuk meg, ha c minden prímosztója R-nél kisebb, egyébként dobjuk el, majd próbáljunk ki egy újabb b értéket stb. Ily módon gyűjtsünk össze $k+1$ darab b_j, c_j párt, ahol $k = \pi(R)$ az R-ig terjedő prímek száma. Ekkor $b_j^2 \equiv c_j \pmod{N}$, $j = 1, 2, \ldots, k+1$. Közben mindig érdemes euklideszi algoritmussal kiszámítani b és N legnagyobb közös osztóját is, és ha ez 1-nél nagyobb (de N-nél kisebb), akkor máris megkaptuk N egy nem triviális osztóját. Azonban nem valószínű, hogy ekkora szerencsénk lenne. Így feltehetjük, hogy a kapott b_j-k (és így a c_j-k is) az N-hez relatív prímek.

A 9.3.1 Tételre adott második bizonyítás szerint a c_j-k közül *gyors algoritmussal* kiválasztható néhány olyan, amelyek szorzata egy v^2 négyzetszám. Az ezeknek megfelelő b_j-k szorzatát jelöljük u-val, ekkor a kongruenciák összeszorzásából a kívánt $u^2 \equiv v^2 \pmod{N}$ adódik.

Meg kell még vizsgálnunk, hogy (**), azaz $u \not\equiv \pm v \pmod{N}$ is teljesül-e. Azt állítjuk, hogy legalább $1/2$ valószínűséggel igen. Legyen N (általunk nem ismert, de azért létező) prímtényezős felbontása $N = q_1^{t_1} \ldots q_s^{t_s} (s \geq 2)$. Ekkor az $u^2 \equiv v^2 \pmod{N}$ kongruencia ekvivalens az $u^2 \equiv v^2 \pmod{q_j^{t_j}}$, $j = 1, 2, \ldots, s$ kongruenciarendszerrel. Egy q^t páratlan prímhatvány modulusra nézve az $u^2 \equiv v^2 \pmod{q^t}$ kongruencia pontosan akkor teljesül, ha $u \equiv \pm v \pmod{q^t}$. Ezalól csak az jelenthetne kivételt, ha $q \mid u+v$ és $q \mid u-v$ egyszerre állna fenn, de ekkor $q \mid (u+v)+(u-v) = 2u$, ahonnan $q > 2$ miatt $q \mid u$, ami $(u, N) = 1$ alapján lehetetlen. Így az $u^2 \equiv v^2 \pmod{q_j^{t_j}}$, $j = 1, 2, \ldots, s$ kongruenciarendszer 2^s-féleképpen valósulhat meg: minden egyes kongruenciában $u \equiv v$ vagy $u \equiv -v \pmod{q_j^{t_j}}$. Ebből a 2^s számú esetből összesen kettő olyan, amikor $u \equiv \pm v \pmod{N}$, nevezetesen amikor mindegyik kongruenciában „+", illetve mindegyik kongruenciában „−" áll. Az u és a v

kiválasztását (az $u^2 \equiv v^2 \pmod N$ feltétel megoldásai körében) tekinthetjük lényegében véletlenszerűnek, és emiatt az egyes eseteket egyforma valószínűnek képzelve azt nyerjük, hogy $1 - 2/2^s \geq 1/2$ valószínűséggel $u \not\equiv \pm v \pmod N$ is teljesül. Ennek megfelelően, előbb-utóbb (de inkább előbb) szinte biztosan találunk olyan u, v párt, amelyekre (**) is érvényes, és ezzel eljutottunk N egy valódi osztójához.

Miért nem igazán hatékony ez az algoritmus sem? Az ördög a mellőzött részletekben lakozik: hogyan keressük a b-ket és hogyan válasszuk meg az R korlátot. Az első kérdésnél mély számelméleti megfontolások segítenek némileg növelni annak az esélyét, hogy alkalmas b-t találjunk. Az R kijelölésénél pedig azzal a dilemmával kell szembenézni, hogy kis R esetén kevés b_j-t kell összegyűjteni, azonban ritkán akad jó b horogra, nagy R mellett pedig viszonylag gyakran találunk jó b-t, viszont igen sok kell belőlük. Itt is mély számelméleti tételek alapján lehet az optimális R-et megkapni.

A 9.3.1 Tételnek a négyzetszámok helyett köbszámokra, illetve magasabb hatványokra vonatkozó általánosításával a 9.3.1–9.3.4 feladatokban foglalkozunk.

Feladatok

9.3.1 *Köbszámok.* Legyenek $0 < p_1 < \ldots < p_k$ tetszőleges prímszámok és $0 < c_1 < \ldots < c_t$ olyan egészek, amelyek egyikének sincs a p_i-ktől különböző prímosztója.

(a) Mutassuk meg, hogy $t \leq 2k$ esetén nem feltétlenül tudunk kiválasztani néhány különböző c_j-t úgy, hogy ezek szorzata köbszám legyen.

(b) Bizonyítsuk be, hogy $t \geq 2 \cdot 3^k + 1$ esetén biztosan kiválasztható néhány különböző c_j úgy, hogy ezek szorzata köbszám legyen.

(c) Bizonyítsuk be, hogy $t \geq k + 1$ esetén biztosan kiválasztható néhány c_j úgy, hogy ezek szorzata köbszám legyen, és a tényezők között mindegyik c_j legfeljebb kétszer fordul elő.

M*9.3.2 *Chevalley tétele.* Legyen p egy pozitív prímszám és legyenek $f_i(x_1, x_2, \ldots, x_t)$, $i = 1, 2, \ldots, k$ olyan egész együtthatós, t-változós polinomok, amelyek konstans tagja 0 és $\sum_{i=1}^{k} \deg f_i < t$. Lássuk be, hogy az $f_i(x_1, x_2, \ldots, x_t) \equiv 0 \pmod p$, $i = 1, 2, \ldots, k$ kongruenciarendszernek létezik nem triviális megoldása. (Melyik ismert tételt kapjuk abban a speciális esetben, ha mindegyik polinom elsőfokú?)

*9.3.3 *Köbszámok újra.* Legyenek $0 < p_1 < \ldots < p_k$ tetszőleges prímszámok és $0 < c_1 < \ldots < c_t$ olyan egészek, amelyek egyikének sincs a p_i-ktől különböző prímosztója. Bizonyítsuk be, hogy $t \geq 2k + 1$

esetén biztosan kiválasztható néhány *különböző* c_j úgy, hogy ezek szorzata köbszám legyen.

*9.3.4 *Magasabb hatványok.* Általánosítsuk az előző feladatot köbszámok helyett q-adik hatványokra, ahol q tetszőleges prímszám.
Megjegyzés: A megfelelő állítás (más eszközökkel) igazolható arra az esetre is, amikor q prímhatvány, azonban tetszőleges q egészre a probléma megoldatlan.

9.3.5 *Összegek oszthatósága.*
(a) Mutassuk meg, hogy n egész számból mindig kiválasztható néhány, amelyek összege osztható n-nel.
*(b) Mutassuk meg, hogy $2n-1$ egész számból mindig kiválasztható n olyan, amelyek összege osztható n-nel.

9.3.6
(a) Mutassuk meg, hogy bármely $n > 1$-hez található három olyan egész szám, amelyek s négyzetösszegére $n \mid s$, de $n^2 \nmid s$.
(b) Lássuk be, hogy $(n, s/n) = 1$ is elérhető.

9.3.7 Adjunk gyors algoritmust a teljes hatványok felismerésére és felbontására.

9.3.8 *Faktorizáció.* Egy másik faktorizációs eljárás vázlata a következő. Próbáljuk meg az N nagy páratlan összetett számot $N = x^2 - y^2$ alakban előállítani. Ennek érdekében vizsgáljuk meg rendre az $x \geq \sqrt{N}$ számokra, hogy $x^2 - N$ négyzetszám-e. Ha felhasználjuk, hogy egy négyzetszám 3-mal, 5-tel, 7-tel, 8-cal stb. osztva csak speciális maradékot adhat, akkor ez jelentősen megkönnyíti az x keresését.
(a) Ha s darab különböző prím szerint nézzük $x^2 - N$ lehetséges maradékait, akkor körülbelül az x számok hányadrészéről derül ki, hogy $x^2 - N$ biztosan nem lehet négyzetszám?
(b) Ez a faktorizációs módszer mikor talál (viszonylag) gyorsan $N = de$ felbontást: ha d kicsi és e nagy vagy ha d és e közel egyforma?
(c) Bontsuk tényezőkre ezzel a módszerrel a 86519 és 584189 számokat. (Csak kalkulátort használjunk, és elegendő a 3 és 8 modulusokkal „szitálni”.)

9.4. Páratlanváros és Párosváros

Ebben a pontban azt vizsgáljuk, hogy egy k elemű halmaznak maximálisan hány olyan részhalmaza lehet, ahol az elemszámokra és a páronkénti met-

szetek elemszámára különféle feltételeket szabunk. Meglepő módon a feltételek minimális megváltoztatása az eredmény drámai megváltozását vonhatja maga után. Bevezetőként ezt az alábbi kis mesével illusztráljuk.

Hol volt, hol nem volt, az Óperenciás (Operációs?) tengeren túl, de a Nagy Prímszámtételen innen, Kombinatória kellős közepén volt egyszer egy icipici, 32 lakosú városka, amelynek a lakói imádtak egyesületeket alapítani. Kezdetben mindössze annyit kötöttek ki, hogy két egyesületnek nem lehet teljesen azonos a tagsága (hiszen akkor ez a kettő tulajdonképpen ugyanaz az egyesület, csak más néven). Még a „tagnélküli" egyesületet is bejegyezték, amelynek tehát senki sem tagja. (Ebben az egyesületben biztosan nem kerül sor éles vitákra!)

Szépen szaporodtak az egyesületek, mindenkinek több talicskányi tagkönyve volt már, azonban ettől a helyi nyomda kapacitása teljesen kimerült, és a polgárok rájöttek, hogy az egyesületek túlburjánzásának megakadályozására némi korlátozó intézkedéseket kell bevezetni. Két javaslat feküdt a nagytekintélyű szenátus előtt (amelynek természetesen mindenki tagja volt). Mindkét javaslat egyformán előírta, hogy ezentúl bármely két egyesületnek csak páros számú közös tagja lehet, és mindössze abban az apróságban mutatkozott eltérés, hogy emellett a Párosváros-pártiak azt akarták, hogy az egyesületek taglétszáma páros legyen, míg a Páratlanváros-pártiak a páratlan taglétszám mellett kardoskodtak. Mivel mindkét pártnak pontosan 16 képviselője volt a szenátusban, ezért nem tudván szavazással dönteni, segítségül hívták a szomszéd faluból a köztiszteletnek örvendő Lineáris Algebra apót, hogy mondjon véleményt. Az ő szavai most alább következnek.

9.4.1 Tétel (Páratlanváros)

Legyen $|X| = k$ és $H_1, \ldots, H_n$ olyan (különböző) részhalmazok X-ben, amelyekre mindegyik $|H_j|$ páratlan és $|H_t \cap H_j|$ páros, ha $t \neq j$. Ekkor $\max n = k$. ♣

9.4.2 Tétel (Párosváros)

Legyen $|X| = k$ és $H_1, \ldots, H_n$ olyan (különböző) részhalmazok X-ben, amelyekre mindegyik $|H_j|$ páros és $|H_t \cap H_j|$ páros, ha $t \neq j$. Ekkor $\max n = 2^{\lfloor k/2 \rfloor}$. ♣

Eszerint a mesebeli Párosvárosban $2^{16} = 65536$ egyesület alapítható, míg Páratlanvárosban mindössze 32.

A két tétel bizonyítása közös alapelven működik: a valósban megismert skalárszorzat és merőlegesség fogalmát kiterjesztjük a modulo 2 test feletti vektorterekre, és a részhalmazoknak, valamint a metszeteiknek az elemszámát

ennek segítségével fogjuk jellemezni. Egy másfajta megközelítést a 9.4.4 feladatban mutatunk.

Bizonyítás: Legyenek X elemei $x_1, \ldots, x_k$ és H tetszőleges részhalmaz X-ben. Feleltessünk meg H-nak egy k hosszúságú $\mathbf{h}$ vektort a következőképpen: $\mathbf{h}$-ban az i-edik komponens 1, ha $x_i \in H$, és 0, ha $x_i \notin H$.

Legyen $T = F_2$, ekkor $\mathbf{h}$-t tekinthetjük T^k-beli vektornak.

Definiáljuk T^k-ban a skalárszorzatot mint a koordináták szorzatösszegét (ugyanúgy, ahogy a valós test felett). Ez most is szimmetrikus bilineáris függvény lesz, csak a „pozitív definitségnek" persze nincs értelme, továbbá egy nem nulla vektor is lehet önmagára merőleges (lásd a 9.4.13–9.4.14 feladatokat).

Ha a H és H' részhalmazoknak a $\mathbf{h}$, illetve $\mathbf{h}'$ vektorok felelnek meg, akkor a $\mathbf{h}\cdot\mathbf{h}'$ skalárszorzat $H \cap H'$ elemszámát méri: annyi darab 1-est kell összeadni, ahány közös elem van H-ban és H'-ben. Ennélfogva $\mathbf{h}\cdot\mathbf{h}'$ aszerint 0, illetve 1, hogy $|H \cap H'|$ páros, illetve páratlan. Ez speciálisan $H = H'$ esetén is igaz, azaz $\mathbf{h}\cdot\mathbf{h}$ aszerint 0, illetve 1, hogy $|H|$ páros, illetve páratlan.

Térjünk most rá a Páratlanváros-tétel bizonyítására. Világos, hogy k darab ilyen H_j megadható, például az egyelemű részhalmazok megfelelnek a feltételnek. Most azt igazoljuk, hogy ennél több H_j már nem létezik. Ezt úgy látjuk be, hogy a H_j-knek megfeleltetett $\mathbf{h}_1, \ldots, \mathbf{h}_n$ vektorokról kimutatjuk, hogy lineárisan függetlenek. Mivel T^k-ban legfeljebb k darab lineárisan független vektor létezik, így valóban a kívánt $n \le k$ egyenlőtlenséget kapjuk.

Vegyünk egy $\delta_1\mathbf{h}_1 + \ldots + \delta_n\mathbf{h}_n = \mathbf{0}$ lineáris kombinációt. Ha mindkét oldalt skalárisan megszorozzuk $\mathbf{h}_j$-vel, akkor $\delta_1(\mathbf{h}_1\cdot\mathbf{h}_j) + \ldots + \delta_j(\mathbf{h}_j\cdot\mathbf{h}_j) + \ldots + \delta_n(\mathbf{h}_n\cdot\mathbf{h}_j) = 0$ adódik. Mivel $|H_j|$ páratlan, de minden $t \ne j$-re $|H_t \cap H_j|$ páros, ezért itt minden $\mathbf{h}_t\cdot\mathbf{h}_j$ skalárszorzat 0, kivéve $\mathbf{h}_j\cdot\mathbf{h}_j$-t, ami 1. Innen azonnal kapjuk, hogy $\delta_j = 0$. Mivel ez tetszőleges j-re teljesül, ezért a $\mathbf{h}_j$ vektorok valóban lineárisan függetlenek.

Rátérve a Párosváros-tétel bizonyítására, először lássuk be, hogy $2^{\lfloor k/2 \rfloor}$ ilyen részhalmaz megadható. Megfelelő, ha $\lfloor k/2 \rfloor$ darab (diszjunkt) elempárt veszünk, és az ezekből képezhető összes lehetséges halmazt tekintjük. (A mesebeli megfogalmazással, ha Párosvárosban 16 házaspár lakik, akkor bármely férj és feleség közösen lép vagy nem lép be egy egyesületbe.) Annak igazolása, hogy ez a maximum, további előkészületeket igényel.

Két $V = T^k$-beli vektor, $\mathbf{a}$ és $\mathbf{b}$ merőlegessége most is jelentse azt, hogy a skalárszorzatuk $\mathbf{a}\cdot\mathbf{b} = 0$, továbbá egy U altérre legyen $U^\perp$ az U összes elemére merőleges vektorok halmaza: $U^\perp = \{\mathbf{x} \in V \mid (\mathbf{u} \in U \Rightarrow \mathbf{u}\cdot\mathbf{x} = 0)\}$.

Könnyen adódik, hogy $U^\perp$ altér, azonban a 8.1.7 Tétel megfelelője általában már nem igaz: előfordulhat, hogy $U \cap U^\perp \ne \mathbf{0}$ és $\langle U, U^\perp\rangle \ne V$. A $\dim U + \dim U^\perp = \dim V$ összefüggés viszont továbbra is érvényes. Mindezt a

9.4.15 feladatban tárgyaljuk.

Visszatérve Párosvárosba, legyenek $H_1, \dots, H_n$ olyan részhalmazok X-ben, amelyekre minden $|H_j|$ és $|H_t \cap H_j|$ páros. Ez azt jelenti, hogy a H_j-knek megfelelő $\mathbf{h}_j$ vektorok ekkor önmagukra és egymásra is merőlegesek. Mivel (F_2 felett) $(\mathbf{a}+\mathbf{b})\cdot(\mathbf{a}+\mathbf{b}) = \mathbf{a}\cdot\mathbf{a} + 2(\mathbf{a}\cdot\mathbf{b}) + \mathbf{b}\cdot\mathbf{b} = \mathbf{a}\cdot\mathbf{a} + \mathbf{b}\cdot\mathbf{b}$, így a $\mathbf{h}_j$ vektorok által generált U altérben bármely két vektor merőleges egymásra. Emiatt $U \subseteq U^\perp$, tehát $\dim U \le \dim U^\perp$, és így a $\dim U + \dim U^\perp = \dim V$ összefüggésből $\dim U \le \lfloor \dim V/2 \rfloor = \lfloor k/2 \rfloor$ következik. Azaz valóban $n \le |U| = 2^{\dim U} \le 2^{\lfloor k/2 \rfloor}$, amint állítottuk. ■

Feladatok

9.4.1 Egy k elemű halmaznak hány olyan (különböző) részhalmaza van, amelyek elemszáma a) páros; b) 3-mal osztható?

9.4.2 Tekintsük a 9.4.1–9.4.2 Tételek bizonyításában bevezetett $H \mapsto \mathbf{h}$ megfeleltetést.

(a) A H és H' halmazok között milyen kapcsolat áll fenn, ha a $\mathbf{h}$ és $\mathbf{h}'$ vektorok minden komponensükben különböznek?

(b) A H és H' halmazok között milyen műveletet kell elvégezni, hogy az így kapott halmaznak éppen a $\mathbf{h}$ és $\mathbf{h}'$ vektorok (F_2 feletti) összege feleljen meg?

9.4.3 Adjunk új bizonyítást a Páratlanváros-tételre az F_2 test feletti függetlenség helyett a $\mathbf{Q}$ feletti függetlenségre támaszkodva.

9.4.4 Legyen $|X| = k$, $H_1, \dots, H_n$ (különböző) részhalmazok X-ben, és feleltessük meg a H_j-knek a $\mathbf{h}_1, \dots, \mathbf{h}_n$ vektorokat a 9.4.1–9.4.2 Tételek bizonyításában látott módon. Ekkor azt a $k \times n$-es A mátrixot, amelynek az oszlopai éppen a $\mathbf{h}_1, \dots, \mathbf{h}_n$ vektorok, a $H_1, \dots, H_n$ halmazrendszer *illeszkedési mátrix*ának (vagy *incidenciamátrix*ának) nevezzük.

(a) Mik lesznek a $B = A^T A$ szorzatmátrix elemei?

(b) A fentiek felhasználásával adjunk még egy bizonyítást a Páratlanváros és Párosváros tételekre.

9.4.5 A k lakosú Páratlanvárosban a 9.4.1 Tétel feltételei szerint alapítanak k egyesületet. A lehetőségek számát jelöljük ξ_k-val. Lássuk be, hogy

(a) $\xi_k > 1$, ha $k > 3$; (b) $\xi_k \to \infty$, ha $k \to \infty$;

*(c) $2^{k^2/8}/k! < \xi_k < 2^{k^2}/k!$.

9.4.6 *Fordított Páratlanváros.* Maximálisan hány egyesület alapítható a k lakosú Anti-Páratlanvárosban, ha itt bármely két egyesület közös tagjainak a száma páratlan, az egyesületek taglétszáma pedig páros?

9.4.7 *Kalandozások Számországban.*
(a) Hármashatárnak k lakója van, az egyesületek taglétszáma nem osztható 3-mal, bármely két egyesület közös tagjainak a száma viszont igen. Maximálisan hány egyesület létezhet Hármashatárban?
(b) Mi a helyzet Négyesföldön?
(c) Mutassuk meg, hogy Hatfaluban nem alapítható $2k$-nál több egyesület. *Megjegyzés*: Megoldatlan probléma, hogy egyáltalán k-nál több alapítható-e.

9.4.8
(a) Legyen $|X| = k$, ahol $3 \mid k$. Maximálisan hány olyan H_j részhalmaz adható meg X-ben, amelyekre $|H_j| \equiv 2 \pmod 3$ és $|H_t \cap H_j| \equiv 1 \pmod 3$, ha $t \neq j$?
(b) Oldjuk meg ugyanezt a feladatot $3 \nmid k$ esetén.

9.4.9 *Színes Páratlanváros.*
(a) A k lakosú Piros-Kék Páratlanvárosban n darab P_j piros és ugyanannyi K_j kék egyesületet alapítanak az alábbi feltételekkel: $|P_j \cap K_j|$ páratlan minden j-re és $|P_t \cap K_j|$ páros, ha $t \neq j$. Határozzuk meg n maximumát.
(b) Mutassuk meg, hogy az eredmény akkor sem változik, ha $|P_t \cap K_j|$ párosságát ($t \neq j$ helyett) csak $t < j$-re követeljük meg.

M*9.4.10 *Egyforma metszetek.* Egy k elemű halmaznak maximálisan hány olyan részhalmaza lehet, amelyek közül bármelyik kettőnek pontosan egy közös eleme van?

9.4.11 *Szigorú szabályok.* Álszabadiban az egyesületalapítási szabályok a következők: (i) Kevesebb egyesület van, mint ahány lakos; (ii) bármely két lakos ugyanannyi (éspedig pozitív számú) egyesületnek közös tagja; (iii) minden egyesületnek legalább két tagja van, és két egyesületnek nem lehet teljesen azonos a tagsága. Hány egyesület működik Álszabadiban?

M**9.4.12 *Korlátozott metszetek.* Egy k elemű halmazban maximálisan hány olyan részhalmaz adható meg, amelyek páronkénti metszeteinek az elemszáma legfeljebb m-féle lehet (azaz $t \neq j$-re a $|H_t \cap H_j|$ értékek között legfeljebb m különböző fordul elő, ahol $m \leq k$ egy rögzített nemnegatív egész)?

A 9.4.13–9.4.16 feladatokban legyen p egy pozitív prím, $T = F_p$, $V = T^k$ és U altér V-ben. A V-beli skalárszorzatot, merőlegességet és $U^\perp$-t ugyanúgy definiáljuk, mint a $p = 2$ esetben.

9.4.13 *Kicsi alterek.*

(a) Legyen $T = F_2$ és U olyan altér V-ben, amelyben csak a nullvektor merőleges önmagára. Bizonyítsuk be, hogy $|U| \leq 2$.

*(b) Legyen p páratlan prím és $T = F_p$. Maximálisan hány eleme lehet V-ben egy olyan U altérnek, amelyben csak a nullvektor merőleges önmagára?

9.4.14 *Izotrop vektorok.*

(a) Milyen p és k esetén létezik V-ben önmagára merőleges nem nulla vektor?

(b) Milyen p és k esetén alkotnak az önmagukra merőleges vektorok alteret V-ben? Hány dimenziós ez az altér?

9.4.15 *U és $U^\perp$.*

(a) Mutassunk példát arra, amikor $U \cap U^\perp \neq \mathbf{0}$, illetve $\langle U, U^\perp \rangle \neq V$.

(b) Bizonyítsuk be, hogy $\dim U + \dim U^\perp = \dim V$.

(c) Igazoljuk, hogy $U \cap U^\perp = \mathbf{0} \iff \langle U, U^\perp \rangle = V$.

9.4.16 *Belterjes merőlegesség.* Vizsgáljuk meg, hogy létezik-e V-ben olyan U altér, amelyre $U = U^\perp$, ha

(a) $p = 2$, $k = 10$; (b) $p = 5$, $k = 11$; (c) $p = 13$, $k = 30$;

(d) $p = 23$, $k = 2$; (e) $p = 43$, $k = 20$.

9.4.17 *Új egyesületek.*

(a) A k lakosú Páratlanvárosban a 9.4.1 Tétel feltételei szerint n egyesület működik. Igaz-e, hogy ha az egyesületek száma nem maximális (vagyis $n < k$), akkor a rendszer bővíthető, azaz a meglevők mellé további egyesület is alapítható?

(b) Mi a helyzet Párosvárosban?

M*9.4.18 *Liberalizált Párosváros.* Mutassuk meg, hogy páros k esetén akkor sem alapítható több egyesület Párosvárosban, ha a 9.4.2 Tétel feltételei közül a $|H_j|$ párosságára vonatkozót elejtjük, és páratlan k esetén is mindössze eggyel növelhető ekkor az egyesületek száma.

9.4.19 *Csupa Három.* Egy 9 elemű halmazban maximálisan hány olyan H_j részhalmaz van, amelyekre mindegyik $|H_j|$ és mindegyik $|H_t \cap H_j|$ is osztható 3-mal?

9.5. Szép gráfok

Ebben a pontban egy meglepő és szép gráfelméleti tételt igazolunk, az eddigieknél egy kicsit több lineáris algebra felhasználásával. Viccesen azonban akár úgy is fogalmazhatnánk, hogy mindennek az az oka, hogy a 15-nek a természetes számok körében nincs más osztója, mint az 1, a 3, az 5 és a 15.

Tekintsünk egy olyan (hurokél és többszörös él nélküli véges) gráfot, amelyben nincs ötnél rövidebb kör és minden csúcsból d él indul ki. Hány csúcsa lehet egy ilyen gráfnak?

Vegyünk egy tetszőleges csúcsot. Ebből d él indul ki, tehát újabb d csúcsot kapunk. Az új csúcsok mindegyikéből $d-1$ újabb él indul ki. Sem két ilyen él, sem a végpontjaik nem eshetnek egybe, mert akkor egy 3, illetve 4 hosszúságú körhöz jutnánk. Az élek végpontjai tehát újabb $d(d-1)$ csúcsot adnak. A gráfnak így összesen legalább d^2+1 csúcsa van.

Milyen d-kre állhat itt egyenlőség? Nyilván $d=1$ és $d=2$ megfelel (a gráf ekkor egyetlen él, illetve egy öt hosszúságú kör). Kicsit nehezebb $d=3$-ra egy jó gráfot mutatni, de van ilyen, az ún. Petersen-gráf (lásd a 9.5.1 feladatot). Viszont $d=4$, 5 és 6 egyike sem jó, amint ez növekvő nehézségű számolásokkal igazolható. Bravúros módon A. J. Hoffman és R. R. Singleton 1960-ban $d=7$-re ismét találtak egy jó gráfot; ezt egy csomó Petersen-gráf összeragasztásával nyerték. És mi a helyzet nagyobb d-kre?

9.5.1 Tétel (Hoffman–Singleton-tétel)
Tegyük fel, hogy egy gráf minden csúcsából d él indul ki, a gráfban nincs ötnél rövidebb kör és a gráfnak d^2+1 csúcsa van. Ekkor d értéke csak 1, 2, 3, 7 vagy 57 lehet. ♣

Megjegyzés: Sokáig megoldatlan volt, hogy mi a helyzet $d=57$-re. Végül 2020-ban igazolták, hogy nem létezik ilyen gráf.

Bizonyítás: Egy n csúcsú gráf *szomszédsági (adjacencia) mátrix*án azt az $n\times n$-es A mátrixot értjük, amelyben

$$\alpha_{ij}=\begin{cases}1, & \text{ha az } i\text{-edik és } j\text{-edik csúcs között van él;}\\ 0 & \text{egyébként,}\end{cases}\qquad i,j=1,2,\dots,n.$$

Könnyen látható, hogy egy gráf szomszédsági mátrixát négyzetre emelve a kapott $B=A^2$ mátrixban β_{ij} éppen az i-edik és j-edik csúcs közös szomszédainak a száma.

Vegyünk most egy, a tétel feltételeit kielégítő $n=d^2+1$ csúcsú G gráfot. A tétel kimondása előtti meggondolásokból adódik, hogy G-ben bármely két

csúcs vagy szomszédos, vagy pedig pontosan egy közös szomszédjuk van. Ezért a G gráf $n \times n$-es A szomszédsági mátrixára az

$$A^2 + A - (d-1)E = J \tag{9.5.1}$$

mátrixegyenlet teljesül, ahol E az ($n \times n$-es) egységmátrix, J pedig a csupa 1-ből álló mátrix.

Mivel A szimmetrikus mátrix, ezért $n = d^2+1$ független sajátvektora van (az $\mathbf{R}^n$ euklideszi térben, sőt ezek páronként ortogonálisak is). A (9.5.1) mátrixegyenletből könnyen adódik, hogy ha $\mathbf{v}$ sajátvektora A-nak λ sajátértékkel, akkor $\mathbf{v}$ sajátvektora J-nek is, éspedig

$$\mu = \lambda^2 + \lambda - (d-1) \tag{9.5.2}$$

sajátértékkel. Mivel a J-nek az n egyszeres sajátértéke, és minden további sajátértéke 0, ezért az A-nak (9.5.2) alapján a d egyszeres sajátértéke (ami közvetlenül is adódott volna), a további sajátértékei pedig kielégítik a $\lambda^2 + \lambda - (d-1) = 0$ egyenletet. Ezt megoldva kapjuk, hogy A további sajátértékei

$$\lambda_1 = \frac{-1+\sqrt{4d-3}}{2} \quad \text{és} \quad \lambda_2 = \frac{-1-\sqrt{4d-3}}{2}\,,$$

multiplicitásuk m_1, illetve m_2, ahol

$$m_1 + m_2 = n - 1 = d^2\,. \tag{9.5.3}$$

Írjuk fel az A mátrix nyomát. Ez egyrészt a főátlóbeli elemek összege, azaz 0, másrészt a sajátértékek (multiplicitással vett) összege. Tehát

$$0 = m_1\lambda_1 + m_2\lambda_2 + d = \frac{m_1 - m_2}{2}\sqrt{4d-3} - \frac{m_1+m_2}{2} + d \tag{9.5.4}$$

adódik. Ez csak úgy teljesülhet, ha $m_1 = m_2$ vagy pedig $s = \sqrt{4d-3}$ egész szám.

Az első esetben (9.5.3)-ból és (9.5.4)-ből kapjuk, hogy $d^2 = 2d$, azaz $d = 2$. A második esetben a $d = (s^2+3)/4$ összefüggést (4)-be beírva

$$-s^4 + 2s^2 + 16s(m_1 - m_2) + 15 = 0$$

adódik. Vagyis s osztója a 15-nek, tehát $s = 1$, 3, 5 vagy 15. Innen $d = 1$, 3, 7 vagy 57. ■

Feladatok

Gráfon a továbbiakban is hurokél és többszörös él nélküli véges gráfot értünk. Egy csúcs *fok*a a csúcsból kiinduló élek száma. Egy gráf *reguláris*, ha minden csúcs foka ugyanannyi.

Egy gráf *spektrum*a a szomszédsági mátrix sajátértékeinek a halmaza.

Legyen egy G gráfnak n csúcsa és m éle. A G gráf *illeszkedési (incidencia) mátrix*ának azt az $n \times m$-es C mátrixot nevezzük, amelyben $\gamma_{ij} = 1$, ha az i-edik csúcs illeszkedik a j-edik élre, és 0 egyébként.

9.5.1 A Petersen-gráf a következőképpen néz ki: Vegyük egy szabályos ötszög csúcsait, és ezt az öt pontból álló alakzatot a középpontból kicsinyítsük le (pl. fele méretűre). A külső pontok közül kössük össze a szomszédosakat (azaz ekkor egy szabályos ötszöget kapunk), a belső pontok mindegyikét kössük össze a másodszomszédaival (így egy csillagötszöget kapunk), végül mindegyik külső pontot kössük össze a neki megfelelő belső ponttal. Az így kapott gráfnak 10 csúcsa és 15 éle van.

(a) Ellenőrizzük, hogy ebben a gráfban valóban nincs ötnél rövidebb kör és minden csúcs foka 3.

(b) Adjuk meg a Petersen-gráf spektrumát.

9.5.2 Egy gráf csúcsaihoz rendeljük hozzá rendre az $x_1, \ldots, x_n$ valós (vagy komplex) számokat. Mutassuk meg, hogy az $\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ nem nulla vektor akkor és csak akkor sajátvektora a gráf szomszédsági mátrixának, ha bármely csúcsnál a szomszédaihoz rendelt x_i számok összege ugyanannyiszorosa a csúcshoz rendelt számnak.

9.5.3 Határozzuk meg az alábbi n csúcsú gráfok spektrumát:

(a) n csúcsú teljes gráf;

(b) $n = 2k$, és minden csúcsnak pontosan egy szomszédja van (ekkor a gráf diszjunkt élek egyesítése, ún. egyfaktor);

(c) $n = 2k$, az $a_1, \ldots, a_k$ csúcsok mindegyike össze van kötve a $b_1, \ldots, b_k$ csúcsok mindegyikével, és más él nincs (teljes páros gráf);

(d) $n - 1$ élű csillag (azaz a középpont a többi $n - 1$ pont mindegyikével össze van kötve, és más él nincs);

*(e) n hosszúságú kör.

9.5.4 Milyen kapcsolatban áll egy reguláris gráf spektruma a gráf komplementerének a spektrumával?

M*9.5.5 Legyen a G gráf szomszédsági mátrixa A. Mutassuk meg, hogy akkor és csak akkor van olyan f polinom, amelyre $f(A) = J$, ha G összefüggő és reguláris (J a csupa 1-ből álló mátrix).

9.5.6 Írjuk fel a 9.5.1 és 9.5.3 feladatokban szereplő gráfok illeszkedési mátrixát.

9.5.7 Legyen a G gráf illeszkedési mátrixa C. Mi a C^TC, illetve CC^T mátrixok elemeinek a kombinatorikai jelentése?

9.5.8 Melyek azok a gráfok, amelyeknél a(z alkalmasan választott) szomszédsági és illeszkedési mátrix egybeesik?

9.5.9 Legyen Λ a G gráf legnagyobb sajátértéke, δ és Δ pedig a G-ben előforduló legkisebb, illetve legnagyobb fokszám. Bizonyítsuk be, hogy $\delta \leq \Lambda \leq \Delta$.

M*9.5.10 Legyen Λ a G gráf legnagyobb sajátértéke. Mutassuk meg, hogy G csúcsai kiszínezhetők (legfeljebb) $\Lambda + 1$ színnel úgy, hogy bármely él két végpontja különböző színű.

9.5.11 Legyen $n \geq 2$. Egy X véges halmaz n-edrendű (nem elfajuló) *véges projektív sík*ot alkot, ha teljesülnek az alábbiak:

(i) az X elemeit pontoknak és bizonyos részhalmazait egyeneseknek nevezzük, és egy pont akkor van rajta egy egyenesen, ha a megfelelő részhalmaz tartalmazza az adott elemet;

(ii) bármely két egyenesnek egy közös pontja van, és bármely két ponton egy egyenes megy át;

(ii) minden egyenesen $n+1$ pont helyezkedik el, és minden ponton $n+1$ egyenes halad át.

Megmutatható, hogy ekkor mind a pontok, mind az egyenesek száma $|X| = n^2+n+1$. Az A.11.13 feladatban szerepel n-edrendű projektív sík konstrukciója, ha n tetszőleges prímhatvány. Megoldatlan, hogy más n-re is létezik-e n-edrendű projektív sík.

A véges projektív síkok szolgáltatták a nem triviális extremális megoldásokat a 9.4.10 feladattal kapcsolatban (lásd a feladat második bizonyítása utáni megjegyzést), és tulajdonképpen projektív síkok szerepelnek majd („inkognitóban”) a 9.6.2 Tétel bizonyításában is.

(a) Egy véges projektív sík minden pontjára egy-egy valós számot írunk. Mutassuk meg, hogy ha a számok összege minden egyenesen 0, akkor mindegyik szám 0.

*(b) Egy n-edrendű projektív sík pontjait tetszőlegesen kiszínezzük pirossal és kékkel. Bizonyítsuk be, hogy van olyan egyenes, ahol a színek közötti eltérés legalább $\sqrt{n}$.

9.6. Sidon-sorozatok

Sidon-sorozatoknak a természetes számok olyan $a_1 < a_2 < \dots$ véges vagy végtelen részsorozatait nevezzük, amelyeknél az $a_i + a_j$ összegek (vagy ami ugyanaz: az $a_i - a_j,\ i \neq j$ különbségek) mind különbözők. Az alábbiakban csak véges Sidon-sorozatokkal foglalkozunk.

Maximálisan hány eleme lehet egy Sidon-sorozatnak az $[1, n]$ intervallumban? Bebizonyítjuk, hogy ez a maximum „körülbelül" $\sqrt{n}$. Ez két állítást jelent: egyrészt azt, hogy 1 és n között valóban előfordul körülbelül $\sqrt{n}$ elemszámú Sidon-sorozat (alsó becslés a maximális elemszámra), másrészt azt, hogy az adott határok között ennél lényegesen hosszabb Sidon-sorozat már nem létezik (felső becslés a maximális elemszámra).

A kérdéskör vizsgálatában kiemelkedő érdemei vannak az 1996 szeptemberében elhunyt zseniális magyar matematikusnak, Erdős Pálnak. Turán Pállal közösen 1941-ben megmutatták, hogy a keresett maximum legfeljebb $n^{1/2} + 2n^{1/4}$. Ezt később B. Lindström más módszerrel $n^{1/2} + n^{1/4} + 1$-re javította, de ugyanez az eredmény az Erdős–Turán-bizonyítás pontosabb végigszámolásával is kiadódik (9.6.4 Tétel). J. Singer egy eredményének felhasználásával Erdős és tőle függetlenül S. Chowla 1944-ben azt is igazolták, hogy elég nagy n-re $n^{1/2} - n^{5/16}$ elemszámú Sidon-sorozat valóban meg is adható n-ig (9.6.3 Tétel). Ez a két eredmény együtt azt jelenti, hogy az $[1, n]$ intervallumban a Sidon-sorozatok maximális elemszáma nagyon pontos aszimptotikával $\sqrt{n}$. Máig is megoldatlan azonban a még jobb hibatagok kérdése. Az sejthető, hogy a maximális elemszámnak $\sqrt{n}$-től való eltérése egy n-től független korlát alatt marad. Ennek igazolásáért vagy cáfolásáért korábban Erdős Pál összesen 1000 dollárt ajánlott fel.

Jelöljük $s = s(n)$-nel az n-ig megadható leghosszabb Sidon-sorozat elemszámát. Próbáljunk először egyszerű felső becslést keresni s-re. Mivel egy 1 és n közötti Sidon-sorozatban az $a_i + a_j$ összegek mind különbözők, 2 és $2n$ közé esnek és számuk $\binom{s+1}{2}$, így $\binom{s+1}{2} < 2n$, azaz $s < 2\sqrt{n}$. Rögtön jobb becslést kapunk, ha az $a_i - a_j > 0$ különbségeket vizsgáljuk; ezek is mind különbözők, n-nél kisebbek, és számuk $\binom{s}{2}$, így $\binom{s}{2} < n$, azaz $s < \sqrt{2n} + 1$. A felső becslés-

nél tehát azonnal adódott a $\sqrt{n}$-es nagyságrend, „csak" a $\sqrt{n}$ együtthatóját kell 1-re leszorítani.

„Alulról nézve" sokkal kevésbé világos, hogyan érhető el a $\sqrt{n}$-es nagyságrend. A kettőhatványok példája csak $\log_2 n$-et ad, és a mohó algoritmussal is csak $\sqrt[3]{n}$ biztosítható (lásd a 9.6.1 feladatot). Egy szintén Erdőstől származó nagyon szép elemi konstrukcióval már $\sqrt{n/2}$ hosszú Sidon-sorozatot kapunk (lásd a 9.6.2 feladatot), és mint említettük, a $\sqrt{n}$ együtthatója „feltornázható" 1-re.

Lássunk akkor hozzá nagy elemszámú Sidon-sorozatok konstrukciójához. Ezt először bizonyos típusú n-ekre végezzük el, és ezek segítségével térünk majd át tetszőleges n-re.

9.6.1 Tétel

Legyen p tetszőleges prímszám. Ekkor $n = p^2 + p + 1$-re létezik olyan Sidon-sorozat az $[1, n]$ intervallumban, amelynek $\lceil \sqrt{n} \rceil = p + 1$ eleme van. ♣

A 9.6.1 Tétel helyett egy jóval élesebb és önmagában is nagyon érdekes és meglepő állítást igazolunk.

9.6.2 Tétel

Legyen p tetszőleges prímszám. Ekkor létezik $p + 1$ darab olyan a_i, amelyekre az $a_i - a_j,\ i \neq j$ különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo $p^2 + p + 1$. ♣

Megjegyzés: A 9.6.2 Tételben szereplő különbségek száma $p^2 + p$, és modulo $p^2 + p + 1$ éppen ennyi nem nulla maradék van. Vagyis az $a_i - a_j$ különbségek minden maradékot előállítanak, éspedig mindegyiket pontosan egyszer.

Nyilvánvaló, hogy a 9.6.2 Tételben az a_i-k maguk is páronként inkongruensek kell hogy legyenek, tehát választhatók 1 és $n = p^2 + p + 1$ közöttieknek, és így valóban azonnal adódik a 9.6.1 Tétel.

A 9.6.2 Tétel bizonyítása: A bizonyítás a véges testek segítségével történik, az ezek szerkezetére vonatkozó alapvető tételek (lásd az A.11 pontot) és egy kevés lineáris algebra felhasználásával.

Tekintsük a p^3 elemű T_3 véges testet, és ebben a p elemű T_1 résztestet. Legyen Δ a T_3 test multiplikatív csoportjának generáló eleme, azaz

$$T_3 = \{0, \Delta, \Delta^2, \ldots, \Delta^{p^3-1} = 1\}\,. \tag{9.6.1}$$

A T_1-beli nem nulla elemek T_3 multiplikatív csoportjának részcsoportját alkotják, melynek generátoreleme nyilván Δ^n, ahol $n = (p^3-1)/(p-1) = p^2+p+1$.

Vagyis

$$T_1 = \{0, \Delta^n, \Delta^{2n}, \ldots, \Delta^{(p-1)n} = \Delta^{p^3-1} = 1\}\,.$$

Tekintsük most T_3-at mint T_1 feletti vektorteret. Az előzőek alapján kapjuk, hogy T_3 két eleme, Δ^i és Δ^j pontosan akkor lineárisan összefüggő T_1 felett, ha

$$i \equiv j \pmod{n}\,. \tag{9.6.2}$$

A keresett a_i egészeket ezután a következőképpen adjuk meg. Vegyünk egy tetszőleges $\Theta \in T_3 \setminus T_1$ elemet és legyenek T_1 elemei $\gamma_1, \ldots, \gamma_p$. Írjuk fel a $\Theta + \gamma_i$ elemeket

$$\Theta + \gamma_i = \Delta^{a_i} \tag{9.6.3}$$

alakban. A (9.6.1) alapján ez megtehető, és így kijelöltünk p darab a_i egész számot, a $p+1$-ik pedig legyen $a_{p+1} = 0$.

Megmutatjuk, hogy ezek eleget tesznek a feltételnek, azaz az $a_i - a_j$ különbségek, vagy ami ugyanaz, az $a_i + a_j$ összegek páronként különböző maradékot adnak modulo $p^2 + p + 1$.

Tegyük fel, hogy $a_i + a_j \equiv a_k + a_l \pmod{p^2+p+1}$. Ekkor (9.6.2) és (9.6.3) alapján

$$(\Theta + \gamma_i)(\Theta + \gamma_j) - \gamma(\Theta + \gamma_k)(\Theta + \gamma_l) = 0$$

adódik valamely $\gamma \in T_1$ elemmel. Mivel Θ harmadfokú a T_1 test felett, ezért nem lehet gyöke egy legfeljebb másodfokú polinomnak. Vagyis csak $\gamma = 1$ és $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$ lehetséges, így a megfelelő a_i-k is egyenlők, ami éppen a bizonyítandó állítás volt.

A bizonyítás ugyanígy megy akkor is, ha $a_{p+1} = 0$ is szerepel a szóban forgó a_i-k között. ■

Megjegyzés: A 9.6.2 Tétel és a bizonyítás ugyanúgy érvényes akkor is, ha p egy prímszám hatványa. Mindez szoros kapcsolatban van a véges projektív síkokkal (lásd a 9.5.11 és A.11.13 feladatokat).

9.6.3 Tétel

Minden elég nagy n-re megadható olyan Sidon-sorozat az $[1, n]$ intervallumban, amelynek legalább $n^{1/2} - n^{5/16}$ eleme van. ♣

Bizonyítás: Vegyük azt a legnagyobb p prímszámot, amelyre $p^2+p+1 \le n$, és p^2+p+1-re készítsük el az előző ($p+1$ elemű) konstrukciót. Mivel $n^{1/2} - n^{5/16}$ és $n^{1/2}$ között elég nagy n-re mindig van prímszám, ezért $p > n^{1/2} - n^{5/16}$, amivel a tételt tetszőleges n-re igazoltuk. ■

Megjegyzés: A tetszőleges n-re történő áttérésnél azt használtuk fel, hogy a prímek elég „sűrűn" helyezkednek el. Ha tudjuk, hogy m és $m + m^c$ között elég nagy m-re mindig van prímszám, akkor a tételünkben a hibatag $n^{c/2}$ nagyságrendűnek vehető. A jelenleg bizonyított legjobb érték $c \approx 0{,}54$, ennek alapján tehát a hibatag kitevője 0,27-nek is vehető. (A tételben csak $c = 5/8$-dal dolgoztunk.) Ezek igen mély prímszámelméleti eredmények. Ha „csak" a prímszámtételre támaszkodnánk, akkor a 9.6.3 Tétel helyett csak annak $\sim \sqrt{n}$ aszimptotikus változatát kaptuk volna hibatag nélkül, ugyanis c értékét „pusztán" a prímszámtétel segítségével nem tudnánk 1 alá szorítani. A $c \approx 0{,}54$ „világrekord" tehát nem kis teljesítmény. Ugyanakkor jól tükrözi tudásunk korlátait is, ugyanis elérhetetlen messzeségben van tőle még az alábbi ártalmatlannak látszó és minden bizonnyal igaz állítás is: bármely két szomszédos négyzetszám közé esik prímszám. Ez lényegében a $c = 1/2$ esetnek felel meg, és még az ún. Riemann-sejtésből sem következik. Ráadásul a $c = 1/2$ sem határ, hanem minden valószínűség szerint c értéke akármilyen kicsinek választható, hogy az $[m, m + m^c]$ intervallum elég nagy m-re még mindig tartalmazzon prímszámot. Ez a sejtés azonban már végképp abba a kategóriába tartozik, amelyre Erdős azt szokta mondani, hogy biztosan igaz, de sohasem fogják tudni bebizonyítani.

A 9.6.3 Tétel más bizonyításaira nézve lásd a 9.6.3 és 9.6.4 feladatot.

Most rátérünk a Sidon-sorozatok elemszámának a(z éles) felső becslésére.

9.6.4 Tétel

Az $[1, n]$ intervallumba eső bármely Sidon-sorozatnak legfeljebb $n^{1/2} + n^{1/4} + 1$ eleme van. ♣

Első bizonyítás: Legyen t később alkalmasan megválasztandó egész szám, és toljunk végig egy $t - 1$ hosszúságú szakaszt a $[0, n]$ intervallumon, azaz tekintsük a $[-t + 1, 0], [-t + 2, 1], \ldots, [n, n + t - 1]$ intervallumokat. Tegyük fel, hogy az s elemű Sidon-sorozat elemszáma az egyes intervallumokban $A_1, A_2, \ldots, A_{n+t}$. Ekkor nyilván

$$\sum_{i=1}^{n+t} A_i = ts\,. \tag{9.6.4}$$

Számoljuk össze *multiplicitással* azokat az $\{a_i, a_j\}$, $i > j$ elempárokat, amelyek egy-egy ilyen intervallumba esnek, azaz mindegyik elempárt annyiszor vegyük, ahány intervallum azt tartalmazza. Legyen D ezek együttes száma.

Ekkor nyilván

$$D = \sum_{i=1}^{n+t} \binom{A_i}{2} = \sum_{i=1}^{n+t} \frac{A_i^2}{2} - \sum_{i=1}^{n+t} \frac{A_i}{2}\,. \tag{9.6.5}$$

Másrészt, ha egy ilyen elempárban az $a_i - a_j$ különbség d, akkor ez az elempár pontosan $t-d$ intervallumba esik bele. A Sidon-tulajdonság miatt minden d legfeljebb egyszer fordulhat elő, így

$$D \le \sum_{d=1}^{t-1}(t-d) = \frac{t(t-1)}{2}\,. \tag{9.6.6}$$

A (9.6.5) és (9.6.6) alapján

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \le t(t-1) \tag{9.6.7}$$

adódik. A számtani és négyzetes közép közötti egyenlőtlenség valamint (9.6.4) felhasználásával (9.6.7) bal oldalát a következőképpen becsülhetjük alulról:

$$\sum_{i=1}^{n+t} A_i^2 - \sum_{i=1}^{n+t} A_i \ge \frac{\left(\sum_{i=1}^{n+t} A_i\right)^2}{(n+t)} - ts = \frac{t^2 s^2}{n+t} - ts\,. \tag{9.6.8}$$

Így (9.6.7) és (9.6.8) összekapcsolásával azt nyerjük, hogy

$$s^2 - s\left(\frac{n}{t}+1\right) - \left(\frac{n}{t}+1\right)(t-1) \le 0\,.$$

Ezt a másodfokú egyenlőtlenséget megoldva

$$s \le \frac{n}{2t} + \frac{1}{2} + \sqrt{n+t+\frac{n^2}{4t^2} - \frac{n}{2t} - \frac{3}{4}}$$

adódik. Ha most t-nek a $t = \lfloor n^{3/4} \rfloor + 1$ értéket választjuk, akkor a tétel állítását kapjuk. ■

Második bizonyítás: Most bizonyos $a_i - a_j$ különbségek összegét fogjuk két oldalról megbecsülni. Legyen

$$K = \sum_{0<i-j\le r} a_i - a_j\,, \tag{9.6.9}$$

ahol r-et később alkalmasan megválasztjuk. A Sidon-tulajdonság miatt a (9.6.9)-beli összeg tagjai között nincs két azonos különbség, számuk

$$(s-1)+(s-2)+\cdots+(s-r)=rs-\frac{r(r+1)}{2}=rw\,,$$

ahol

$$w=s-\frac{r+1}{2}\,, \tag{9.6.10}$$

így K legalább akkora, mint az első rw darab pozitív egész összege, azaz

$$K\ge\frac{rw(rw+1)}{2}>\frac{r^2w^2}{2}\,. \tag{9.6.11}$$

Másrészt a (9.6.9)-beli összegnek része pl.

$$(a_s-a_{s-1})+(a_{s-1}-a_{s-2})+\cdots+(a_2-a_1)<a_s\le n$$

és számos más teleszkopikus összeg, amelyek hasonlóképpen becsülhetők felülről. Ezek általános alakja

$$(a_{s-\nu}-a_{s-\nu-\mu})+(a_{s-\nu-\mu}-a_{s-\nu-2\mu})+\cdots<a_{s-\nu}\le n\,,\quad 0\le\nu<\mu\le r\,.$$

Sőt az egész K ilyen teleszkopikus részösszegekre bontható, amelyeket úgy kapunk, hogy az indexek befutják az összes olyan 1 és s közötti (tovább már nem bővíthető) számtani sorozatot, amelynek differenciája legfeljebb r. Mivel μ differenciájú számtani sorozat éppen μ darab van, így a teleszkopikus részösszegek száma $1+2+\cdots+r=r(r+1)/2$, és mindegyik részösszeg értéke legfeljebb n, tehát

$$K\le\frac{nr(r+1)}{2}\,. \tag{9.6.12}$$

Egybevetve (9.6.11)-et és (9.6.12)-t, $2/r^2$-tel történő szorzás után a $w^2<n+n/r$ egyenlőtlenséget nyerjük. Innen gyökvonással és (9.6.10) felhasználásával kapjuk, hogy

$$s<\frac{r+1}{2}+\sqrt{n+\frac{n}{r}}\,.$$

Ha most r-nek az $r=\lfloor n^{1/4}\rfloor+1$ értéket választjuk, akkor a tétel állítását kapjuk. ■

Feladatok

9.6.1 Mutassuk meg, hogy a mohó algoritmussal 1 és n között egy legalább $\sqrt[3]{n}$ elemű Sidon-sorozatot kapunk.

Megjegyzés: A mohó algoritmussal ily módon egy olyan *végtelen* hosszú Sidon-sorozatot is nyerhetünk, amelynek *minden* n-re n-ig legalább $\sqrt[3]{n}$ eleme van. Meglepő, hogy ezt a nagyságrendet sokáig egyáltalán nem sikerült megjavítani. Csak 1981-ben igazolták Ajtai Miklós, Komlós János és Szemerédi Endre, hogy létezik olyan végtelen Sidon-sorozat, amelynek minden (elég nagy) n-re n-ig legalább $c\sqrt[3]{n \cdot \log n}$ eleme van, ahol c alkalmas pozitív konstans. 1997-ben Ruzsa Imre ezt $cn^{\sqrt{2}-1-\varepsilon}$-ra javította, azonban még ez az eredmény is igen messze van az Erdős által sejtett $n^{1/2-\varepsilon}$-os nagyságrendtől.

9.6.2 Legyen p prímszám és $a_i = 1 + 2ip + \langle i^2 \bmod p \rangle \quad i = 0, 1, \ldots, p-1$, ahol $\langle i^2 \bmod p \rangle$ az i^2 legkisebb nemnegatív maradékát jelöli modulo p. Lássuk be, hogy így $n = 2p^2$-re egy $\sqrt{n/2}$ elemszámú Sidon-sorozatot kapunk az $[1, n]$ intervallumban.

M*9.6.3 Legyen p tetszőleges prímszám. Ekkor létezik p darab olyan a_i, amelyekre az $a_i + a_j$ összegek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo $p^2 - 1$.

Megjegyzés: Az előzővel nyilván ekvivalens, hogy $i \neq j$-re az $a_i - a_j$ különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo $p^2 - 1$. A szereplő különbségek száma $p^2 - p$, és modulo $p^2 - 1$ összesen csak $p^2 - 2$ darab nem nulla maradék van. Vagyis az $a_i - a_j$ különbségek majdnem minden maradékot előállítanak. A bizonyításból leolvasható, hogy éppen a $p+1$-gyel osztható maradékok maradnak ki. — A feladatból a 9.4.3 Tétel hasonló módon vezethető le, mint ahogyan a 9.4.2 Tételből következett (ugyanez érvényes a következő feladatra is).

M*9.6.4 Legyen p tetszőleges prímszám. Ekkor létezik $p - 1$ darab olyan a_i, amelyekre az $a_i - a_j\,, \quad i \neq j$ különbségek (nemcsak hogy különbözők, hanem ráadásul) páronként inkongruensek modulo $p^2 - p$.

9.6.5 *Végtelen Sidon-sorozat*. Mutassuk meg, hogy bármely $\varepsilon > 0$-hoz található olyan végtelen Sidon-sorozat, amelynél *végtelen sok* n-re igaz, hogy n-ig legalább $(1/\sqrt{2} - \varepsilon)\sqrt{n}$ eleme van (vö. a 9.6.1 feladat utáni megjegyzéssel).

Megjegyzés: Megoldatlan, hogy ugyanez $1/\sqrt{2}$ helyett 1-gyel is igaz-e.

9.6.6 *Többtagú összegek.* Legyen $h \geq 2$ rögzített természetes szám, és az $[1, n]$ intervallumban tekintsünk most olyan sorozatokat, ahol az elemekből képezett h-tagú összegek mind különbözők. (A $h = 2$ eset éppen a Sidon-sorozatokat jelenti.)

*(a) Mutassuk meg, hogy van olyan sorozat, amelynek „körülbelül" $n^{1/h}$ eleme van.

(b) Lássuk be, hogy van olyan csak a h-tól függő $c = c(h)$ konstans, hogy minden ilyen sorozatnak legfeljebb $c(h)n^{1/h}$ eleme van.

Megjegyzés: Megoldatlan probléma, hogy $c(h)$ vajon $1 + \varepsilon$-ra csökkenthető-e, azaz bármely h-ra igaz-e, hogy a $h = 2$ esethez hasonlóan a maximális elemszám aszimptotikusan $n^{1/h}$. A 9.6.4 Tétel bizonyítása azért nem vihető át, mert $h \neq 2$-re a feltételt nem lehet összegekről különbségekre átjátszani.

9.6.7 *Minden összeg különböző.* Legyen $1 \leq a_1 < \ldots < a_s \leq n$, és tegyük fel, hogy a különböző a_i-kből képezett akárhány tagú összegek mind különbözők.

(a) Adjunk meg olyan sorozatot, amelynek elemszáma $s = 1 + \lfloor \log_2 n \rfloor$.

(b) Lássuk be, hogy bármely sorozat elemszámára
$$s \leq \log_2 n + \log_2 \log_2 n + 1.$$

M**(c) A b)-beli felső becslést javítsuk $s \leq \log_2 n + (\log_2 \log_2 n)/2 + 2$-re.

Megjegyzés: Meglepő módon az alsó becslés is javítható; az 1 helyett (elég nagy n-re) 2 írható. Erdős korábban 500 dollárt ajánlott fel annak eldöntésére, vajon a $\max s - \log_2 n$ eltérés n növekedésével korlátos marad-e. Megjegyezzük, hogy $\max s \geq \lfloor \log_2 n \rfloor + c$ bizonyításához (ahol c konstans) elég csak *egyetlen* $n = 2^\nu$-re ilyen elemszámú megfelelő sorozatot találni, ugyanis ezt 2^μ-vel megszorozva és a 2^ν-ig terjedő kettőhatványokkal kiegészítve egy kívánt elemszámú sorozatot kapunk $n = 2^{\nu+\mu}$-ig. Könnyen lehet azonban, hogy az említett alsó becslés már éles, vagyis c értéke már 2-ről 3-ra sem javítható.

**9.6.8 *Szorzatok.* Az $[1, n]$ intervallumban tekintsünk most olyan sorozatokat, ahol az elemekből képezett akárhány tényezős szorzatok mind különbözők. A prímek nyilván megfelelnek, tehát az elemszám lehet $\pi(n)$, az n-ig terjedő prímek száma. Mutassuk meg, hogy bármely ilyen sorozat elemszáma legfeljebb $\pi(n) + 2n^{2/3}$.

Megjegyzés: Belátható, hogy a maximális elemszámnak a $\pi(n)$-től való eltérése $\sqrt{n}/\log n$ nagyságrendű.

M**9.6.9 *Számtani sorozatok.* Mutassuk meg, hogy minden elég nagy n-re megadható 1 és n között $n/e^{c\sqrt{\log n}}$ olyan egész szám (ahol $c > 0$ alkalmas konstans), amelyek között nem fordul elő háromtagú számtani sorozat.

M*9.6.10 *Egyszínű számtani sorozatok.* Mutassuk meg, hogy az $1, 2, \ldots, 2000$ számok kiszínezhetők pirossal és kékkel úgy, hogy ne forduljon elő egyszínű 18-tagú számtani sorozat.

9.7. Hilbert harmadik problémája

Az 1900-as párizsi nemzetközi matematikai kongresszuson David Hilbert „Matematikai problémák" címmel tartott előadást, és ebben nagyszabású kutatási programot jelölt ki a XX. század matematikusai számára. Az itt felvázolt 23 problémakör jelentősen meghatározta a matematika fejlődési irányát, és a felvetett kérdések közül jónéhány ma is megoldatlan. Legkönnyebbnek a 3. probléma bizonyult, amely poliéderek átdarabolására vonatkozott, és amelyet M. Dehn néhány hónap alatt megoldott.

A probléma előzménye Bolyai Farkas és P. Gerwien tétele a sokszögek átdarabolhatóságáról: egymástól függetlenül bebizonyították, hogy két egyenlő területű sokszög mindig átdarabolható egymásba, azaz az egyiket szét lehet vágni egyenes vonalakkal véges sok részre úgy, hogy a kapott részekből a másik összerakható legyen. (Más szóval a két sokszöget páronként egybevágó részsokszögekre lehet felbontani, a bizonyítást lásd a 9.7.1 feladatban.)

Már Bolyai Farkas felvetette, vajon érvényes-e hasonló tétel azonos térfogatú poliéderekre is, és Hilbert ennek megválaszolását tűzte ki a 3. problémában, azt sejt(et)ve, hogy ez az átdarabolás a térben már nem mindig lehetséges. A válasz valóban negatív:

9.7.1 Tétel

Az egységnyi térfogatú kocka és szabályos tetraéder nem vágható szét véges sok poliéderre úgy, hogy az egyes darabokat alkalmas egybevágóságok átviszik egymásba. ♣

Bizonyítás: Tegyük fel indirekt, hogy a kocka és a tetraéder mégis egymásba darabolhatók lennének, és legyenek a felbontási eljárás során keletkező P poliéderek összes lapszögei $\beta_1, \ldots, \beta_m$. A β_i-k között szerepel a kocka és a tetraéder lapszöge is, az előbbi $\pi/2$, az utóbbit jelöljük α-val, ekkor $\cos\alpha = 1/3$.

Legyen V a valós számok szokásos vektortere a racionális test felett és ebben W a β_i-k által generált (legfeljebb m-dimenziós) altér. Mivel az α nem racionális számszorosa $\pi/2$-nek (lásd a 9.7.2 feladatot), vagyis $\pi/2$ és α lineárisan független vektorok W-ben, ezért α és $\pi/2$ kibővíthető a W bázisává. Ennélfogva megadható olyan $f : W \to \mathbf{Q}$ lineáris leképezés, amelyre $f(\pi/2) = 0$ és $f(\alpha) = 1$. A linearitás alapján bármely $\xi, \psi \in W$-re $f(\xi + \psi) = f(\xi) + f(\psi)$, valamint bármely r racionális számra $f(r\xi) = rf(\xi)$ érvényes, így speciálisan $f(r\pi) = 2rf(\pi/2) = 0$ is teljesül.

Vezessük be most a P poliéderekre az alábbi függvényt, az ún. Dehn-invariánst:

$$F(P) = \sum_e |e| \cdot f(\beta)\,,$$

ahol az összegezés a P poliéder összes e éle szerint történik, $|e|$ az e él hossza, β az e élnél levő lapszög és f az imént definiált függvény.

Megmutatjuk, hogy f „additív", azaz ha P-t szétvágjuk közös belső pont nélküli $P_1, P_2, \ldots, P_k$ poliéderekre, akkor

$$F(P) = \sum_{i=1}^{k} F(P_i). \tag{9.7.1}$$

Vegyük a bal oldalon az $F(P)$ összeg egy tetszőleges $|e| \cdot f(\beta)$ tagját. Ha az e él és a β lapszög a szétvágás után nem változott, akkor ez a tag a jobb oldalon érintetlenül szerepel pontosan az egyik P_i-ben. Ha az e él e_j szakaszokra esett szét, de a lapszög nem változott, akkor (9.7.1) jobb oldalán $\sum_j |e_j| \cdot f(\beta) = |e| \cdot f(\beta)$ jelenik meg. Ha a β lapszög lett β_s részekre vágva, akkor a jobb oldalon $\sum_s |e| \cdot f(\beta_s)$ szerepel, ami f linearitása miatt továbbra is $|e| \cdot f(\beta)$-val egyenlő. Ugyanígy adódik (9.7.1) a fenti esetek kombinációjakor is. Meg kell még mutatnunk, hogy ha a P-ben nem szereplő új élek keletkeznek P belsejében vagy valamelyik lapján, akkor (9.7.1) jobb oldalán az ezekből adódó tagok összege 0. Egy ilyen e élnél a hozzá tartozó P_t poliéderek β_t lapszögeinek összege 2π, illetve π. Így ez az él a (9.7.1) jobb oldalán álló $\sum_{i=1}^{k} F(P_i)$ összeghez

$$\sum_t |e| \cdot f(\beta_t) = |e| \cdot f(\sum_t \beta_t) = |e| f(r\pi) = 0 \text{ (ahol } r = 1 \text{ vagy } 2)$$

értékkel járul hozzá. Ezzel (9.7.1)-et teljes egészében beláttuk.

Ebből következik, hogy egymásba átdarabolható poliéderek Dehn-invariánsa meg kell hogy egyezzen. A K egységkockára $F(K) = 12f(\pi/2) = 0$. A megfelelő R szabályos tetraéder élhosszát b-vel jelölve ugyanakkor $F(R) =$

$= 6bf(\alpha) = 6b \neq 0$. Ez az ellentmondás igazolja, hogy K és R valóban nem darabolhatók át egymásba. ■

Megjegyzések: 1. A térbeli átdarabolhatóságnál tulajdonképpen tetszőleges egybevágóság helyett csak mozgásokat kellett volna megengedni, hiszen ha egy P poliédernek egy síkra vonatkozó tükörképe P', akkor P és P' a (háromdimenziós) térben általában „nem vihetők át ténylegesen" egymásba. Belátható azonban, hogy P és P' feldarabolhatók úgy, hogy az egyes részeket már mozgással is egymásba vihetjük, és így az átdarabolhatóság definíciójánál valóban mindegy, hogy tetszőleges egybevágóságokat vagy csak mozgásokat engedünk meg.

2. A síkbeli és térbeli helyzet eltérése világosan mutatja annak az okát, miért lehet a sokszögek területfogalmánál hatékonyan használni az átdarabolásokat (lásd Euklidész), ugyanakkor a poliéderek térfogatánál nemigen kerülhető meg valamiféle határátmenet.

3. Ha a geometriai, „rendes" szétvágások helyett tetszőleges részhalmazokra történő (diszjunkt) felosztásokat is megengedünk, akkor alapvetően megváltozik a helyzet. Megmutatható például, hogy egy gömb (ilyen halmazelméleti értelemben) átdarabolható két(!) ugyanekkora sugarú gömbbe. Egy sokáig megoldatlan probléma volt, hogy egy azonos területű négyzet és kör átdarabolható-e egymásba; ezt 1988-ban igazolta Laczkovich Miklós (ráadásul csak eltolásokra van szükség).

Feladatok

9.7.1 *Bolyai Farkas és P. Gerwien tétele*. Mutassuk meg, hogy két azonos területű sokszög mindig átdarabolható egymásba.

9.7.2 *Szögek és koszinuszok*.

(a) Mutassuk meg, hogy $\cos\alpha = 1/3$ esetén α/π irracionális szám.

(b) Lássuk be, hogy ha γ/π és $\cos\gamma$ is racionális, akkor $\cos\gamma = 0, \pm 1/2$ vagy ± 1.

*9.7.3 *Téglalap és négyzetek*. Igazoljuk, hogy egy téglalap akkor és csak akkor vágható szét véges sok (nem feltétlenül egyforma) négyzetre, ha az oldalainak az aránya racionális.

9.7.4 *Hasábok és tetraéderek*.

(a) Átdarabolható-e egymásba két azonos térfogatú hasáb (az alapok tetszőleges sokszögek lehetnek)?

*(b) Legyenek A, B, C, D ebben a sorrendben egy kocka alaplapjának szomszédos csúcsai és A', B', C', D' rendre a velük szomszédos csúcsok a fedőlapon. Átdarabolhatók-e egymásba az $ABCB'$ és $ABCC'$ (azonos alapú és magasságú) tetraéderek?

*9.7.5 *Négyzet és háromszög.* Mutassuk meg, hogy egy azonos területű négyzet és háromszög *csak eltolásokkal* nem darabolható át egymásba.

9.7.6 *Négyzetek és kockák.*

(a) Mutassuk meg, hogy egy négyzet akkor és csak akkor vágható szét pontosan n darab négyzetre, ha $n \neq 2$, 3 vagy 5.

(b) Mutassuk meg, hogy ha n elég nagy, akkor egy kocka szétvágható pontosan n darab kockára.

*(c) Igazoljuk az előző állítást minden $n \geq 48$-ra.

M*9.7.7 *Háromszögek.*

(a) Akkor és csak akkor bontható fel minden háromszög pontosan n darab *hasonló* háromszögre, ha $n \neq 2$, 3 vagy 5.

(b) Akkor és csak akkor bontható fel minden háromszög pontosan n darab *egybevágó* háromszögre, ha n négyzetszám.

(c) Ha n négyzetszám, két négyzetszám összege vagy egy négyzetszám háromszorosa, akkor létezik olyan háromszög, amely felbontható n darab egybevágó és az eredeti háromszöghöz is hasonló részre.

Megjegyzés: Megmutatható, hogy a (c) rész megfordítása is igaz. Ha azonban elhagyjuk azt a kikötést, hogy a kis (egybevágó) háromszögek az eredeti háromszöghöz hasonlók legyenek, akkor számos további megfelelő n érték adódik már a szabályos háromszögnél is.

9.8. Térfogat és determináns

Ebben a pontban megmutatjuk, hogy a determináns geometriai jelentése a(z előjeles) térfogat. Gondolatmenetünk bármilyen test feletti vektortérre érvényes, azonban a közvetlen geometriai kapcsolat miatt csak a valós test feletti vektorterekre fogunk szorítkozni.

A síkon bármely két vektor egy (esetleg elfajuló) paralelogrammát feszít ki, amelynek az egyik csúcsa az origó. A térben három vektor ugyanígy egy paralelogramma alapú hasábot, egy ún. paralelepipedont határoz meg. Ennek általánosításaként azt mondjuk, hogy egy $\mathbf{R}$ feletti n-dimenziós V vektortérben tetszőleges n darab vektor egy (n-dimenziós) *paralelepipedon*t feszít ki.

Ezt úgy kell „elképzelnünk”, hogy az élei a megadott vektorok, illetve azok eltolt példányai, a csúcsai pedig a vektorokból képezhető összegek „végpontjai” (a síkon $\mathbf{0}, \mathbf{a}_1, \mathbf{a}_2$ és $\mathbf{a}_1 + \mathbf{a}_2$, a térben $\mathbf{0}, \mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \mathbf{a}_1 + \mathbf{a}_2, \mathbf{a}_1 + \mathbf{a}_3, \mathbf{a}_2 + \mathbf{a}_3$ és $\mathbf{a}_1 + \mathbf{a}_2 + \mathbf{a}_3$). A csúcsok száma ennek megfelelően 2^n.

Értelmezni akarjuk a paralelepipedonok (előjeles) térfogatát. Ez azt jelenti, hogy minden vektor-n-eshez egy valós számot rendelünk hozzá, azaz egy $D : V^n \to \mathbf{R}$ függvényről van szó. Vizsgáljuk meg, milyen tulajdonságokat várunk el egy paralelepipedon térfogatától, azaz milyen feltételeket kell ennek a D függvénynek kielégítenie.

Az egyik követelményünk az, hogy ha egy paralelepipedon egyik élét — a többi él változatlanul tartása mellett — λ-szorosára változtatjuk, akkor a térfogat is a λ-szorosára változzék. Ugyanígy, ha az egyik $\mathbf{a}$ élt az $\mathbf{a}' + \mathbf{a}''$ összegre bontjuk, a többi élt változatlanul hagyjuk, akkor a keletkező két paralelepipedon térfogatának összege egyezzen meg az eredeti paralelepipedon térfogatával. Ez a két feltétel azt jelenti, hogy D (a bilineáris függvényekhez hasonlóan) mindegyik változójában *lineáris*, azaz összeg- és skalárszorostartó.

A következő elvárásunk az, hogy ha a paralelepipedon elfajuló, azaz az n darab vektor V-ben egy n-nél kisebb dimenziós alteret generál, akkor a térfogat legyen nulla. Ez más szavakkal azt jelenti, hogy ha az $\mathbf{a}_1, \ldots, \mathbf{a}_n$ vektorok összefüggők, akkor $D(\mathbf{a}_1, \ldots, \mathbf{a}_n) = 0$.

Végül azt szeretnénk, hogy az „egységkocka” térfogata 1 legyen. Ehhez rögzítsünk le V-ben egy $\mathbf{e}_1, \ldots, \mathbf{e}_n$ bázist, és írjuk elő a $D(\mathbf{e}_1, \ldots, \mathbf{e}_n) = 1$ feltételt.

9.8.1 Tétel

Legyen V egy n-dimenziós vektortér $\mathbf{R}$ felett és $\mathbf{e}_1, \ldots, \mathbf{e}_n$ egy rögzített bázis V-ben. Ekkor pontosan egy olyan $D : V^n \to \mathbf{R}$ függvény létezik, amely

(i) mindegyik változójában lineáris;

(ii) lineárisan összefüggő vektorokhoz 0-t rendel;

(iii) $D(\mathbf{e}_1, \ldots, \mathbf{e}_n) = 1$.

Ha az $\mathbf{a}_j$ vektornak az $\mathbf{e}_1, \ldots, \mathbf{e}_n$ bázis szerinti i-edik koordinátáját α_{ij}-vel jelöljük, akkor

$$D(\mathbf{a}_1, \ldots, \mathbf{a}_n) = \begin{vmatrix} \alpha_{11} & \alpha_{12} & \ldots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \ldots & \alpha_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_{n1} & \alpha_{n2} & \ldots & \alpha_{nn} \end{vmatrix}, \tag{9.8.1}$$

vagyis $D(\mathbf{a}_1, \ldots, \mathbf{a}_n)$ éppen annak a mátrixnak a determinánsa, amelynek az oszlopai az $\mathbf{a}_j$ vektorok (pontosabban ezek koordinátavektorai). ♣

A tétel alapján a paralelepipedon (előjeles) térfogatát az éleihez (a fenti módon) tartozó determinánssal adhatjuk meg.

Megjegyezzük még, hogy a tétel a determináns alternatív definiálására is alkalmas.

Bizonyítás: Először tegyük fel, hogy egy $D : V^n \to \mathbf{R}$ függvény rendelkezik az (i) – (iii) tulajdonságokkal. Ekkor (ii) speciális eseteként kapjuk, hogy

(iv) ha az $\mathbf{a}_j$ vektorok között van két azonos, akkor $D(\mathbf{a}_1, \dots, \mathbf{a}_n) = 0$.

Most megmutatjuk, hogy

(v) ha két vektort felcserélünk, akkor D értéke az ellentettjére változik („előjelet vált").

Cseréljük fel például $\mathbf{a}_1$-et és $\mathbf{a}_2$-t. Ekkor (i) és (iv) alapján

$$\begin{aligned} 0 &= D(\mathbf{a}_1 + \mathbf{a}_2, \mathbf{a}_1 + \mathbf{a}_2, \mathbf{a}_3, \dots, \mathbf{a}_n) = D(\mathbf{a}_1, \mathbf{a}_1, \mathbf{a}_3, \dots, \mathbf{a}_n) + \\ &+ D(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \dots, \mathbf{a}_n) + D(\mathbf{a}_2, \mathbf{a}_1, \mathbf{a}_3, \dots, \mathbf{a}_n) + D(\mathbf{a}_2, \mathbf{a}_2, \mathbf{a}_3, \dots, \mathbf{a}_n) = \\ &= D(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \dots, \mathbf{a}_n) + D(\mathbf{a}_2, \mathbf{a}_1, \mathbf{a}_3, \dots, \mathbf{a}_n)\,, \end{aligned}$$

tehát valóban $D(\mathbf{a}_2, \mathbf{a}_1, \mathbf{a}_3, \dots, \mathbf{a}_n) = -D(\mathbf{a}_1, \mathbf{a}_2, \mathbf{a}_3, \dots, \mathbf{a}_n)$.

Írjuk fel az $\mathbf{a}_j$-ket az $\mathbf{e}_i$ báziselemek lineáris kombinációjaként: $\mathbf{a}_j = \sum_{i=1}^{n} \alpha_{ij}\mathbf{e}_i$. Ennek alapján $D(\mathbf{a}_1, \dots, \mathbf{a}_n)$-et az (i) tulajdonság felhasználásával n^n darab

$$\alpha_{m_1 1}\alpha_{m_2 2} \dots \alpha_{m_n n} D(\mathbf{e}_{m_1}, \mathbf{e}_{m_2}, \dots, \mathbf{e}_{m_n}) \tag{9.8.2}$$

típusú tag összegére bonthatjuk. A (iii), (iv) és (v) feltételek alapján itt mindegyik $D(\mathbf{e}_{m_1}, \dots, \mathbf{e}_{m_n})$ érték egyértelműen meghatározott (0 vagy ± 1), és így $D(\mathbf{a}_1, \dots, \mathbf{a}_n)$ értéke is egyértelmű. Ezzel beláttuk, hogy legfeljebb egy ilyen D függvény létezik.

Az előzőkből (9.8.1) is azonnal következik. Először is (iv) alapján $D(\mathbf{e}_{m_1}, \dots, \mathbf{e}_{m_n}) = 0$, ha az $\mathbf{e}$-k között szerepel két azonos. Vegyünk most egy olyan tagot, ahol az $\mathbf{e}$-k mind különbözők, azaz $m_1, \dots, m_n$ az $1, \dots, n$ számok egy permutációja. Ekkor (iii) és (v) alapján $D(\mathbf{e}_{m_1}, \dots, \mathbf{e}_{m_n})$ aszerint 1 vagy -1, hogy az $m_1, \dots, m_n$ permutáció az $1, \dots, n$-ből páros vagy páratlan sok cserével keletkezett-e, más szóval az $m_1, \dots, m_n$ páros vagy páratlan permutáció-e. Ennek alapján $D(\mathbf{a}_1, \dots, \mathbf{a}_n)$ annak az $n!$ számú $(-1)^I \alpha_{m_1 1}\alpha_{m_2 2} \dots \alpha_{m_n n}$ tagnak az összege, ahol $m_1, \dots, m_n$ végigfut az $1, \dots, n$ számok összes permutációján és I az $m_1, \dots, m_n$ permutáció inverzió-száma. Ez pedig éppen az α_{ij} számokból képezett determináns értéke (pontosabban a transzponált mátrix determinánsának a definíció szerinti megadása). Ezzel (9.8.1)-et beláttuk.

Hátra van még annak az igazolása, hogy valóban létezik ilyen D függvény. Az előzőek szerint egyedül a determináns lehet megfelelő. Így azt kell megmutatni, hogy a determináns valóban rendelkezik az (i)–(iii) tulajdonságokkal. Ez pedig azonnal következik a determináns elemi tulajdonságaiból. ■

Megjegyzések: 1. A tétel bizonyítását a determináns tulajdonságaira történő hivatkozás nélkül is befejezhettük volna. Ugyanis láttuk, hogy egyedül az a D lehet jó, amelyre $D(\mathbf{a}_1, \dots, \mathbf{a}_n)$ éppen a (9.8.2)-ben szereplő n^n darab tag összege, ahol mindegyik $D(\mathbf{e}_{m_1}, \dots, \mathbf{e}_{m_n})$ érték egyértelműen meghatározott (0 vagy ± 1). Innen (iii) teljesülése nyilvánvaló, (i) és (iv) pedig egyszerű számolással adódik, és az utóbbi kettőből (ii) is könnyen levezethető (lásd a 9.8.1 feladatot). Persze mindezzel tulajdonképpen a megfelelő determinánstulajdonságok újbóli bizonyítását végeztük el.

Egy másik, kicsit kevesebb számolással járó lehetőség, ha megmutatjuk, hogy az (i) és (ii) tulajdonságnak eleget tevő függvények a természetesen adódó műveletekre nézve egy egydimenziós vektorteret alkotnak, és így a (iii) feltétel egyértelműen kijelöl ebben egy megfelelő D függvényt (vö. a 9.8.2 feladattal).

2. Mivel (adott test felett) bármely két n-dimenziós vektortér izomorf, ezért dolgozhattunk volna végig $V = \mathbf{R}^n$-nel is. Ekkor az $\mathbf{e}_1, \dots, \mathbf{e}_n$ bázisnak értelemszerűen a szokásos egységvektorokat célszerű választani.

Feladatok

9.8.1 Vezessük le a (ii) tulajdonságot (i)-ből és (iv)-ből.

9.8.2 Legyenek F_1 és F_2 olyan $V^n \to \mathbf{R}$ függvények, amelyekre (i) és (ii) teljesül és F_2 nem azonosan nulla. Mutassuk meg, hogy van olyan $\lambda \in \mathbf{R}$, amellyel $F_1 = \lambda F_2$.

9.8.3 Legyen az $\mathcal{A} \in \operatorname{Hom} V$ lineáris transzformáció mátrixa az $\mathbf{e}_1, \dots, \mathbf{e}_n$ bázisban A. Lássuk be, hogy az $F(\mathbf{v}_1, \dots, \mathbf{v}_n) = D(\mathcal{A}\mathbf{v}_1, \dots, \mathcal{A}\mathbf{v}_n)$ és a $G(\mathbf{v}_1, \dots, \mathbf{v}_n) = (\det A) \cdot D(\mathbf{v}_1, \dots, \mathbf{v}_n)$ függvények azonosan egyenlők.
Megjegyzés: A feladat alapján kapjuk, hogy a determináns tulajdonképpen az a skalár, ahányszorosára a transzformáció a térfogatot növeli.

9.8.4 Igazoljuk a determinánsok szorzástételét.

9.8.5
a) Legyen P_1, P_2 és P_3 a sík három pontja, P_j (szokásos Descartes-féle koordinátái) legyenek γ_{1j} és γ_{2j} $(j = 1, 2, 3)$. Bizonyítsuk be, hogy a

P_j pontok akkor és csak akkor esnek egy egyenesbe, ha $\begin{vmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} \\ 1 & 1 & 1 \end{vmatrix} = 0.$

b) Fogalmazzuk meg és lássuk be a megfelelő térbeli állítást: mikor esik négy pont egy síkba?

c) Igazak maradnak-e a fenti eredmények ferdeszögű koordinátarendszerben is?

10. KÓDOK

A kódelmélet feladata olyan eljárások kidolgozása, amelyek az elektronikus átvitelnél a (kis valószínűséggel, de esetleg mégis bekövetkező) hibákat kiszűrik, azaz a fogadó fél ezeket észreveszi („hibajelzés"), sőt akár rekonstruálni tudja a helyes üzenetet („hibajavítás"). Ennek érdekében az eredeti adatoknak megfelelő „közleményszavak" helyett kicsit hosszabb „kódszavak" kerülnek továbbításra. A kódolásnál általában az a cél, hogy minél kevesebb „ellenőrző jeggyel" minél több hiba jelzését, illetve javítását tudjuk elérni. Egy másik fontos követelmény, hogy a „kódolási" és „dekódolási" eljárások elvi és gyakorlati szempontból egyaránt (azaz mind a matematikai elméletet, mind pedig az elektronikai megvalósítást tekintve) nagy tömegű adatátvitel esetén is biztonságosan és hatékonyan működjenek.

Az alábbiakban az algebrai kódelmélet alapfogalmait tárgyaljuk, és bemutatunk néhány hatékony kódot. Megjegyezzük, hogy a kódoknak számos más (nem algebrai jellegű) típusa is létezik, valamint a kriptográfiában a titkosírásoknál is szokás a rejtjelezési eljárást kód(olás)nak nevezni, ezekkel azonban nem foglalkozunk.

10.1. Hibajelzés, hibajavítás

Az elektronikus eszközök az adatokat általában 0–1 sorozatokként tárolják. Bevezető illusztrációként szorítkozzunk arra a nagyon speciális esetre, amikor az átvitelnél *összesen* legfeljebb egyetlen bit továbbítása hibás, és nézzünk két egyszerű eljárást, hogyan lehet kideríteni, hogy valóban történt-e hiba, illetve hogyan lehet a hibás bitet megkeresni (azaz a hibát kijavítani).

Küldjük el a teljes üzenetet kétszer egymás után. Ha az átvitelnél legfeljebb egy bit továbbítása hibás, akkor a dupla üzenet két fele legfeljebb egyetlen jegytől eltekintve teljesen egyforma. Ezek szerint, ha a két rész egyforma, akkor nem történt hiba, ha pedig valahol eltérés van, akkor a továbbítás hibás volt. Sajnos azonban a hibát nem tudjuk kijavítani, hiszen lehet, hogy az éppen az „ellenőrző" részben keletkezett. Ezen úgy segíthetünk, ha az eredeti üzenetet még egyszer megismételjük, vagyis összesen háromszor küldjük el. Ekkor a három rész közül a feltevésünk szerint (legalább) kettő teljesen egyforma, és így ezek adják a helyes üzenetet.

Természetesen a fenti eljárások meglehetősen gazdaságtalanok. A kódelmélet egyik fő feladata éppen az, hogy olyan eljárásokat dolgozzon ki, amelyek

minél kevesebb „ellenőrző jeggyel" minél több hibát tudnak jelezni, illetve kijavítani (emellett természetesen az is fontos, hogy mindezt minél egyszerűbben és „automatikusabban" tegyék meg).

A bevezető után lássunk hozzá a megfelelő matematikai elmélet kiépítéséhez. Ezután is mindig feltesszük, hogy a továbbítandó adatok bináris formában, azaz 0–1 sorozatként állnak rendelkezésre. Tördeljük ezt a sorozatot n hosszúságú blokkokra, ezek lesznek a „közleményszavak". Minden közleményszó helyett egy $k > n$ hosszúságú 0–1 sorozat, a közleményszónak megfelelő „kódszó" kerül továbbításra.

10.1.1 Definíció

Legyen $n < k$, és jelöljük az n, illetve k hosszúságú 0–1 sorozatok halmazát T^n-nel, illetve T^k-val. Egy (k, n) paraméterű *kód*on T^k-nak egy 2^n elemű K részhalmazát értjük. A K kódoló függvénye egy olyan $\varphi : T^n \to T^k$ *injektív* (azaz különböző elemeket különböző képekbe vivő) leképezés, amelynek a képe $\operatorname{Im}\varphi = K$.

T^n elemeit *közleményszavak*nak, K elemeit pedig *kódszavak*nak nevezzük. ♣

A kódszavak tehát a T^k halmaznak egy 2^n elemű (egyelőre tetszőleges) részhalmazát alkotják.

Megjegyzés: A kiépítendő elmélet jelentős része (értelemszerű módosításokkal) átvihető lenne arra az esetre is, amikor a továbbítandó jelek a 0 és 1 helyett pl. a $0, 1, \ldots, p-1$ „jegyek" közül kerülnek ki, ahol p tetszőleges prím. Mi azonban csak az ún. *bináris kód*okkal, a $p = 2$ esettel foglalkozunk.

Legyen a továbbiakban $T = F_2$, a modulo 2 maradékosztályok teste. Ekkor az iménti T^n, illetve T^k jelölés összhangban van a korábbiakkal, azzal a kiegészítő megjegyzéssel, hogy mind a közleményszavakat, mind pedig a kódszavakat (egyelőre) általában nem oszlopvektorokkal, hanem inkább n, illetve k hosszúságú sorozatokkal fogjuk jelölni. (Ez az írásmód természetesebben felel meg a probléma jellegének, emellett kényelmesebb is.)

A következő ponttól kezdve majd azt is ki fogjuk használni, hogy T^n és T^k vektorterek T felett, és a kódok alterek lesznek T^k-ban, a φ kódoló függvények pedig alkalmas lineáris leképezések T^n-ről T^k-ba. Ennek megfelelően a közleményszavaknál és kódszavaknál oszlopvektoros jelölésre fogunk áttérni T^n-ben és T^k-ban.

Az egész fejezet során a szereplő vektorok, illetve mátrixok mindig automatikusan a $T = F_2$ test felettieknek értendők.

Most rátérünk a hibajelzés és hibajavítás pontos értelmezésére. Kezdjük a

hibajelzéssel. Tegyük fel, hogy egy $\mathbf{c} \in K$ kódszó továbbításakor hiba történt, azaz a $\mathbf{c}$ kódszó helyett egy tőle különböző $\mathbf{z} \in T^k$ vektor érkezett meg a fogadó félhez. Ha $\mathbf{z}$ maga is kódszó, akkor a hiba nem derül ki, azonban ha $\mathbf{z}$ nem kódszó, akkor világos, hogy hiba történt.

Mivel egy bit hibás továbbításának a valószínűsége igen kicsi (különben az egész átviteli rendszer gyakorlatilag használhatatlan lenne), ezért hiba esetén a $\mathbf{z}$ és $\mathbf{c}$ vektorok általában csak kevés komponensben különböznek. Így a hibajelzéshez elég azt biztosítani, hogy ha egy kódszóban csak „kevés jegyet" változtatunk meg, akkor nem kapunk (egy másik) kódszót.

10.1.2 Definíció

Egy kód *t-hibajelző*, ha akármelyik kódszavának (legalább 1, de) legfeljebb t tetszőleges komponensét megváltoztatva sohasem kapunk kódszót. ♣

A hibajelzés csak regisztrálja a tényt, hogy hiba történt. A hibajavítás azt jelenti, hogy ezen túlmenően azt is meg tudjuk határozni, melyik kódszó lett eltorzítva.

10.1.3 Definíció

Egy kód *t-hibajavító*, ha bármely két (különböző) kódszavának legfeljebb t tetszőleges komponensét megváltoztatva sohasem kapjuk ugyanazt a vektort. ♣

Nyilván a t-hibajavítás lényegesen erősebb követelmény a t-hibajelzésnél, és mindkettő szorosan összefügg a kódszavak „távolságával".

10.1.4 Definíció

Egy $\mathbf{v} \in T^k$ vektor *súly*a (vagy *Hamming-súly*a) a benne levő 1-esek száma, két vektor *távolság*a (vagy *Hamming-távolság*a) pedig azoknak a komponenseknek a száma, ahol a két vektor eltér. ♣

A távolság tehát a különbségvektor súlya. (Természetesen — $T = F_2$ miatt — különbségvektor helyett összegvektort is mondhattunk volna.)

Az $\mathbf{u}, \mathbf{v} \in T^k$ vektorok távolságát $\tau(\mathbf{u}, \mathbf{v})$-vel jelöljük. Az így definiált távolság valóban rendelkezik a távolság szokásos tulajdonságaival, és T^k erre a távolságra nézve metrikus tér (lásd a 8.2.6 Definíciót).

10.1.5 Tétel

Egy kód pontosan akkor t-hibajelző, ha a kódszavak közötti minimális távolság legalább $t+1$, és pontosan akkor t-hibajavító, ha a kódszavak közötti minimális távolság legalább $2t+1$. ♣

Bizonyítás: Mindkét állítás a 10.1.2–10.1.4 Definíciók közvetlen következménye. Ugyanis egy kód pontosan akkor t-hibajelző, ha bármely kódszóra igaz, hogy a tőle (legalább 1, de) legfeljebb t távolságra levő vektorok egyike sem kódszó. Hasonló módon egy kód pontosan akkor t-hibajavító, ha az egyes kódszavaktól legfeljebb t távolságra levő vektorok diszjunkt halmazokat alkotnak. ■

Példák kódokra

Kezdjük a sort a bevezetőben már jelzett két eljárással.

P1. *Kétszeri ismétlés*: A (megfelelő) kódszót úgy képezzük, hogy a közleményszót még egyszer megismételjük (tehát összesen kétszer írjuk le egymás után), azaz

$$\varphi : \alpha_1\alpha_2 \dots \alpha_n \mapsto \alpha_1\alpha_2 \dots \alpha_n\alpha_1\alpha_2 \dots \alpha_n \,.$$

Itt $k = 2n$, a kódszavak azok a vektorok, amelyeknek minden $1 \le j \le n$-re a j-edik és az $n + j$-edik komponense megegyezik. Ez a kód 1-hibajelző, a kódszavak minimális távolsága 2. (Természetesen a kód számos „többhibát" is jelez, de ha véletlenül pl. éppen az első és az $n + 1$-edik jegy volt hibás, akkor ez a 2-hiba nem derül ki, mert így egy másik kódszóhoz jutottunk.)

P2. *Háromszori ismétlés*: A (megfelelő) kódszót úgy képezzük, hogy a közleményszót összesen háromszor írjuk le egymás után, azaz

$$\varphi : \alpha_1\alpha_2 \dots \alpha_n \mapsto \alpha_1\alpha_2 \dots \alpha_n\alpha_1\alpha_2 \dots \alpha_n\alpha_1\alpha_2 \dots \alpha_n \,.$$

Itt $k = 3n$, a kódszavak azok a vektorok, amelyeknek minden $1 \le j \le n$-re a j-edik, az $n + j$-edik és a $2n + j$-edik komponense megegyezik. Ez a kód 1-hibajavító és 2-hibajelző, a kódszavak minimális távolsága 3.

Az előzőknél lényegesen „gazdaságosabb" az alábbi kód:

P3. *Paritásvizsgálat*: A (megfelelő) kódszót úgy képezzük, hogy a közleményszó után egyetlen további bitet írunk, éspedig a közleményszó jegyeinek az összegét, azaz 1-et vagy 0-t aszerint, hogy a közleményszóban páratlan vagy páros sok 1-es szerepelt:

$$\varphi : \alpha_1\alpha_2 \dots \alpha_n \mapsto \alpha_1\alpha_2 \dots \alpha_n\beta \,, \qquad \text{ahol } \beta = \sum_{i=1}^{n} \alpha_i \,.$$

Itt $k = n + 1$, a kódszavak azok a vektorok, amelyekben páros sok 1-es fordul elő, vagyis amelyeknek a súlya páros. Ez a kód is 1-hibajelző, a kódszavak minimális távolsága 2.

Az n, k és $s = k-n$ paraméterek szokásos elnevezéseit az alábbiakban foglaljuk össze:

10.1.6 Definíció

Egy (k, n) paraméterű kód esetén k a kód(szavak) *hossza*, n az *információs jegyek száma* vagy a kód *dimenziója* és $s = k - n$ az *ellenőrző jegyek száma*. ♣

A dimenzió elnevezést az magyarázza, hogy a legtöbb kód esetén a kódszavak alteret alkotnak T^k-ban (lásd a lineáris kódokat a következő pontban), és ekkor ennek az altérnek a dimenziója valóban n.

Egy kód hatékonyságát az méri, hogy egyrészt hány hibát tud (biztosan) jelezni, illetve javítani (azaz milyen nagy a kódszavak közötti minimális távolság), másrészt ezt milyen kis $s = k - n$ értékkel éri el. Az iménti P1 és P3 példa kódja is 1-hibajelző, ugyanakkor a kétszeri ismétlésnél az ellenőrző jegyek száma n, míg a paritásvizsgálatnál mindössze 1, tehát az utóbbi lényegesen hatékonyabb.

Nézzük most meg, legalább hány ellenőrző jegy szükséges az 1-hibajavításhoz. Minden kódszóhoz vegyük hozzá a tőle 1 távolságra levő vektorokat (azaz, amelyek a kódszótól egyetlen komponensben különböznek). Az így kapott $k+1$ elemű halmazok az 1-hibajavítás miatt szükségképpen diszjunktak, számuk 2^n, azaz $2^n(k+1) \leq 2^k$. Innen ($k = n+s$ felhasználásával) $2^s \geq n+s+1$ adódik. Ez pl. $n = 500$-ra $s \geq 9$-et jelent. A 10.3 pontban megmutatjuk, hogy itt elérhető az $s = 9$ egyenlőség (vö. a P2 példa háromszori ismétlés kódjából származó $s = 1000$ értékkel).

Feladatok

10.1.1 Tegyük fel, hogy minden egyes bit átvitelénél (egymástól függetlenül) p a hiba valószínűsége. Mi a valószínűsége annak, hogy egy k-jegyű kódszó átvitelénél

(a) nem történik hiba;
(b) pontosan 1 jegyben keletkezik hiba;
(c) több, mint 3 jegy lesz hibás?

(Érdekes és tanulságos a fenti valószínűségeket valamely konkrét k és p értékek, pl. $k = 20$ és $p = 10^{-4}$ esetén összehasonlítani.)

10.1.2 Tekintsük azokat a kódokat, ahol $n = 3$, a kódszó minden esetben a megfelelő 3-jegyű $\alpha_1\alpha_2\alpha_3$ közleményszóval kezdődik, majd ezt az alábbi ellenőrző jegy(ek) követi(k) (ezek száma rendre 1, 2, 2, 2, 3, 3, 3):

(a) $\alpha_1 + \alpha_2 + \alpha_3 + 1$; (b) $\alpha_1, \alpha_2 + \alpha_3$; (c) $\alpha_1, \max(\alpha_2, \alpha_3)$;

(d) α_1, γ ahol $\gamma = \begin{cases} \alpha_2, & \text{ha } \alpha_1 = 1 \\ \alpha_3, & \text{ha } \alpha_1 = 0; \end{cases}$ (e) $\alpha_1+\alpha_2, \alpha_1+\alpha_3, \alpha_2+\alpha_3$;

(f) $\alpha_1, \alpha_1 + \alpha_2, \alpha_1 + \alpha_2 + \alpha_3$; (g) α_1, $\alpha_1 \cdot \alpha_2$, $\alpha_1 \cdot \alpha_2 \cdot \alpha_3$.

A felsorolt kódok közül melyek lesznek 1-hibajelzők, illetve 1-hibajavítók?

10.1.3 Mutassuk meg, hogy a kód hibajelző, illetve hibajavító „ereje” nem változik meg, ha minden kódszóban

(a) az első jegyet az ellenkezőjére változtatjuk;
(b) az összes jegyet az ellenkezőjére változtatjuk;
(c) az első két jegyet felcseréljük.

Hogyan általánosíthatjuk ezeket az észrevételeket?

10.1.4

(a) Bizonyítsuk be, hogy három T^k-beli vektor páronkénti távolságainak az összege mindig páros szám.

(b) Mely m-ekre igaz, hogy m tetszőleges vektor páronkénti távolságainak az összege mindig páros szám?

10.1.5 Legyen az $\mathbf{u}, \mathbf{v} \in T^k$ vektorok távolsága $\delta(\mathbf{u}, \mathbf{v}) = d$. Adott q és r esetén hány olyan $\mathbf{w} \in T^k$ vektor létezik, amelyre $\delta(\mathbf{u}, \mathbf{w}) = q$ és $\delta(\mathbf{v}, \mathbf{w}) = r$?

10.1.6 Tegyük fel, hogy három T^k-beli vektor páronkénti távolsága d. Mutassuk meg, hogy d páros, és pontosan egy olyan vektor létezik, amely mindhárom adott vektortól $d/2$ távolságra esik.

10.1.7 Legyen egy (k, n) paraméterű kódban a kódszavak közötti minimális távolság d. Készítsünk egy $(k + 1, n)$ paraméterű K' kódot a következőképpen: minden páros súlyú kódszó után írjunk egy 0-t, minden páratlan súlyú kódszó után pedig egy 1-est. Mekkora a K' kódban a kódszavak közötti minimális távolság?

10.1.8 Lássuk be, hogy egy (k, n) paraméterű t-hibajavító kódban $\sum_{i=0}^{t} \binom{k}{i} \leq 2^{k-n}$.

10.1.9 Legyen $n = 2$. Minimálisan hány ellenőrző jegy szükséges az összes (A) 1; *(B) 2-hiba (a) jelzéséhez; (b) javításához?

Oldjuk meg a feladatot az $n = 3$ esetben is.

10.2. Lineáris kód

10.2.1 Definíció

Egy (k, n) paraméterű K kód lineáris, ha K (n-dimenziós) altér T^k-ban. ♣

Egy lineáris kódban a nullvektor mindig kódszó. Az előző pont P1–P3 példái és a 10.1.2 feladatban (b),(e) és (f) lineáris kódok.

Lineáris kód esetén sokkal egyszerűbben ellenőrizhetjük a t-hibajelzést, illetve t-hibajavítást:

10.2.2 Tétel

Egy lineáris kód pontosan akkor t-hibajelző, ha minden nem nulla kódszó súlya legalább $t + 1$, és pontosan akkor t-hibajavító, ha minden nem nulla kódszó súlya legalább $2t + 1$. ♣

Bizonyítás: Mivel lineáris kód esetén a kódszavak alteret alkotnak, ezért két kódszó különbsége is kódszó. Ennélfogva bármely két (különböző) kódszó távolsága egy alkalmas nem nulla kódszó súlya. Megfordítva, egy nem nulla kódszó súlya megegyezik ennek a kódszónak a nulla kódszótól való távolságával. Ezzel beláttuk, hogy a kódszavak közötti távolságok halmaza egybeesik a nem nulla kódszavak súlyainak a halmazával. Így speciálisan a kódszavak közötti minimális távolság megegyezik a nem nulla kódszavak súlyának minimumával. A tétel állításai ennek alapján a 10.1.5 Tételből következnek. ■

Így például egy lineáris kód pontosan akkor 1-hibajavító, ha minden nem nulla kódszó súlya legalább 3.

Ha K lineáris kód, akkor $\varphi : F^n \to F^k$ kódoló függvényként (injektív) lineáris leképezéseket használunk. Ennek megfelelően ezeket írott latin nagybetűkkel jelöljük és mátrixokkal jellemezzük:

10.2.3 Definíció

Legyen az $\mathcal{A} : T^n \to T^k$ lineáris leképezés a (k, n) paraméterű K lineáris kód kódoló függvénye. Írjuk fel az $\mathcal{A}$ leképezés $G = G_{\mathcal{A}} = [\mathcal{A}]$ mátrixát a természetes bázispár (azaz a T^n-beli, illetve T^k-beli egységvektorok) szerint. Ezt a $k \times n$-es G mátrixot a K kód *generátormátrix*ának nevezzük. ♣

A generátormátrix oszlopait tehát az egységvektorokhoz tartozó kódszavak alkotják. Az előző pont P3 példájának, a paritásvizsgálat-kódnak a generátormátrixa a következő $(n+1)\times n$-es mátrix:

$$\begin{pmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & 1 \\ 1 & 1 & \dots & 1 \end{pmatrix}$$

Ha minden kódszó magával a hozzá tartozó közleményszóval kezdődik, akkor a generátormátrix $G = \begin{pmatrix} E_{n\times n} \\ B_{s\times n} \end{pmatrix}$ alakú (ahol E az $n\times n$-es egységmátrix, B pedig egy $s\times n$-es mátrix).

Legyen $\mathbf{v}\in T^n$ egy tetszőleges közleményszó és $\mathbf{c} = \mathcal{A}\mathbf{v}$ a hozzá tartozó kódszó. Ha $\mathbf{v}$-t és $\mathbf{c}$-t most valóban oszlopvektornak, azaz $n\times 1$-es, illetve $k\times 1$-es mátrixnak tekintjük, akkor a kapcsolatuk a $\mathbf{c} = G_{\mathcal{A}}\mathbf{v}$ mátrixszorzat formájában is kifejezhető. A lineáris kódolást tehát a generátormátrixszal (balról) történő szorzás jelenti.

Megjegyezzük, hogy a lineáris kód helyett a *csoportkód* elnevezés is használatos. Ugyanis T^n és T^k tekinthető additív csoportnak, a lineáris kód T^k egy részcsoportjának, a hozzá tartozó kódoló függvény pedig csoporthomomorfizmusnak.

A pont hátralevő részében azt vizsgáljuk, hogyan lehet lineáris kód esetén a hibajavítást elvégezni. A későbbiekben erre lényegesen jobb módszert is mutatunk majd.

A hibajavítás azt jelenti, hogy minden $\mathbf{z}\in T^k$ vektorhoz megkeressük a hozzá legközelebbi (egyik) $\mathbf{c}$ kódszót, és ha az átvitelnél a fogadó félhez a $\mathbf{z}$ érkezett, akkor ezt a dekódoláskor $\mathbf{c}$-re javítja. Itt a $\mathbf{h} = \mathbf{z} - \mathbf{c}$ vektort *hibamintának* nevezzük, mert a $\mathbf{z}$ és $\mathbf{c}$ távolságának a minimalitása miatt ez a(z egyik) lehető legkisebb súlyú vektor, amelyet egy kódszóhoz hozzáadva a $\mathbf{z}$ vektort megkapjuk. (Ha $\mathbf{z}$ kódszó, akkor $\mathbf{h} = \mathbf{0}$.) A T^k elemeit ennek megfelelően a kódszavaknak a hibaminták szerinti eltoltjaiként érdemes felírni. Ez azt jelenti, hogy a kódszavak K alterének $\mathbf{h}+K$ eltoltjait kell tekinteni (lásd a 4.2.16 feladatot). Ily módon T^k-t 2^{k-n} darab diszjunkt osztályra bontottuk, amelyek mindegyike $|K| = 2^n$ vektort tartalmaz. Az osztályok között szerepel maga a K is (mint önmagának a $\mathbf{h} = \mathbf{0}$ vektorral történő eltoltja). A csoportelméleti megfogalmazásban ezek az osztályok éppen a K részcsoport szerinti mellékosztályokat jelentik. A továbbiakban az osztályokra ezt a mellékosztály elnevezést fogjuk használni.

A hibajavítást ezek után az alábbi *dekódolási tábla* segítségével végezhetjük el. Ennek első sorába felírjuk a kódszavakat (azaz K elemeit), kezdve a $\mathbf{0}$ kódszóval. Ezután a többi sorba rendre felírjuk az iménti mellékosztályokat, amelyekből mindig a legkisebb súlyú reprezentánst (azaz a hibamintát) választjuk, és rendre ezt adjuk hozzá a kódszavakhoz. A sorok elején álló „*osztályelső*" tehát maga a hibaminta, és dekódoláskor minden vektort a fölötte álló (első sorbeli) kódszóra korrigálunk. (Ezután a kódszóból természetesen meg kell még határoznunk a közleményszót. Ha a kódszó magával a közleményszóval kezdődik, akkor ez nem okoz nehézséget, egyéb esetben egy lehetséges módszert a 10.2.9 feladatban tárgyalunk.)

Ha a kód t-hibajavító, akkor a legfeljebb t darab 1-est tartalmazó hibaminták mind különböző mellékosztályba kerülnek, azaz különböző sorok osztályelsői.

Példa: Legyen $\mathcal{A} : \alpha_1\alpha_2 \mapsto \alpha_1\alpha_2\alpha_1\alpha_2\beta$, ahol $\beta = \alpha_1 + \alpha_2$. Ennek a lineáris kódnak a dekódolási táblája

00000	10101	01011	11110
10000	00101	11011	01110
01000	11101	00011	10110
00100	10001	01111	11010
00010	10111	01001	11100
00001	10100	01010	11111
11000	01101	10011	00110
01100	11001	00111	10010

Látjuk, hogy az egy darab 1-est tartalmazó hibaminták különböző sorokba kerültek, tehát a kód valóban 1-hibajavító. Például a 6. sor 3. helyén álló $\mathbf{z} = 01010$ esetén a helyes kódszó a $\mathbf{c} = 01011$. Az utolsó két sorban az osztályelső nem egyértelmű (a 7. sor elején állhatna pl. a 00110 is). Ez (is) mutatja, hogy az utolsó két sor a hibajavítás szempontjából nem használható, az itteni vektorok legalább 2-hibásak, és a kód a 2-hibákat nem tudja javítani.

A fenti eljárás meglehetősen kényelmetlen. A következő pontban a lineáris kódokat más módon fogjuk jellemezni, amellyel gyorsan és „automatikusan" lehet majd a hibajavítást elvégezni.

Feladatok

M*10.2.1 Legyen $k > n$. Melyek igazak az alábbi állítások közül?
(a) A lineáris kódok száma osztója az összes kód számának.
(b) A lineáris kódokhoz tartozó lineáris leképezés kódoló függvények száma osztója az összes kódhoz tartozó összes lehetséges kódoló függvények számának.

10.2.2 Írjuk fel a 10.1 pont P1 és P2 példájának, a kétszeri, illetve háromszori ismétlés kódnak a generátormátrixát.

10.2.3 A 10.1.2 feladatban szereplő kódok közül válasszuk ki a lineárisakat és írjuk fel ezek generátormátrixát, valamint dekódolási tábláját.

10.2.4 Legyen A egy $k \times n$-es 0–1 mátrix. Mutassuk meg, hogy akkor és csak akkor van olyan lineáris kód, amelynek a generátormátrixa A, ha az A-nak az F_2 test feletti rangja $r(A) = n$.

10.2.5 Bizonyítsuk be, hogy lineáris kód esetén a kódszavak éppen a generátormátrix oszlopainak összes lineáris kombinációi.

10.2.6 Mutassuk meg, hogy egy (k, n) paraméterű lineáris kód páros súlyú kódszavai alteret alkotnak T^k-ban. Hány dimenziós ez az altér?

10.2.7 Legyen K_1 és K_2 egy-egy (k_1, n_1), illetve (k_2, n_2) paraméterű kód, amelyekben a kódszavak minimális távolsága d_i és a $\varphi_i : T^{n_i} \to T^{k_i}$ kódoló függvények tartoznak hozzájuk $(i = 1, 2)$. A két kódból új kódokat képezünk az alábbi módon.

I. A közös közleményszavakat használjuk és a kódszavakat egymás után írjuk. Azaz feltesszük, hogy $n_1 = n_2 = n$ és egy $(k_1 + k_2, n)$ paraméterű K_3 kódot definiálunk a $\varphi_3 : T^n \to T^{k_1+k_2}$ kódoló függvénnyel, amely az $\mathbf{a} \in T^n$ közleményszóhoz a $\varphi_3(\mathbf{a}) = \varphi_1(\mathbf{a})|\varphi_2(\mathbf{a})$ kódszót rendeli.

II. Mindkét kód közleményszavait és kódszavait is egymás után írjuk. Azaz egy $(k_1 + k_2, n_1 + n_2)$ paraméterű K_4 kódot definiálunk a $\varphi_4 : T^{n_1+n_2} \to T^{k_1+k_2}$ kódoló függvénnyel, amely az $\mathbf{a}_1|\mathbf{a}_2$ közleményszóhoz (ahol $\mathbf{a}_i \in T^{n_i}$) a $\varphi_4(\mathbf{a}_1|\mathbf{a}_2) = \varphi_1(\mathbf{a}_1)|\varphi_2(\mathbf{a}_2)$ kódszót rendeli.

III. A közleményszavakat egymás után írjuk és a kódszavak aszimmetrikusan kombináljuk: Legyen $k_1 = k_2 = k$ és egy $(2k, n_1 + n_2)$ paraméterű K_5 kódot definiálunk a $\varphi_5 : F^{n_1+n_2} \to F^{2k}$ kódoló függvénnyel, amely az $\mathbf{a}_1|\mathbf{a}_2$ közleményszóhoz (ahol $\mathbf{a}_i \in T^{n_i}$) a $\varphi_5(\mathbf{a}_1|\mathbf{a}_2) = \varphi_1(\mathbf{a}_1)|\big(\varphi_1(\mathbf{a}_1) + \varphi_2(\mathbf{a}_2)\big)$ kódszót rendeli.

(a) Mit állíthatunk a K_3, K_4 és K_5 kódokban a kódszavak közötti d_3, d_4 és d_5 minimális távolságról?

(b) Ha C_1 és C_2 lineáris kódok, akkor K_3, K_4 és C_5 is azok. Hogyan kapjuk meg ezek G_3–G_5 generátormátrixait a K_1 és K_2 kódok G_1 és G_2 generátormátrixaiból?

10.2.8 Legyen $T = F_2$, és jelölje $T_m[x]$ a T feletti legfeljebb $m-1$-edfokú polinomok szokásos vektorterét. Ekkor az

$$\alpha_0\alpha_1 \ldots \alpha_{m-1} \mapsto \alpha_0 + \alpha_1 x + \ldots + \alpha_{m-1}x^{m-1}$$

megfeleltetés izomorfizmus a T^m és $T_m[x]$ vektorterek között. Legyen $k > n$, $s = k - n$. Ebben a feladatban a T^n, illetve T^k vektortereket a belőlük a fenti izomorfizmussal létesített $T_n[x]$, illetve $T_k[x]$ vektorterekkel azonosítjuk.

(a) Legyen $g \neq 0$ egy rögzített, legfeljebb s-edfokú polinom T felett. Legyen az $\mathcal{A} : T_n[x] \to T_k[x]$ leképezés a g polinommal történő szorzás, azaz $\mathcal{A}$ minden legfeljebb $n-1$-edfokú f polinomhoz a gf polinomot rendeli hozzá: $\mathcal{A}f = gf$. Mutassuk meg, hogy így egy lineáris kódot definiáltunk, és írjuk fel a generátormátrixát. Az ilyen kódokat *polinomkód*oknak, a g polinomot pedig a kód *generáló polinom*jának nevezzük.

(b) Legyen h egy k-adfokú, g pedig egy tetszőleges nem nulla polinom T felett. Az $\mathcal{A} : T_n[x] \to T_k[x]$ leképezés minden legfeljebb $n-1$-edfokú f polinomhoz rendelje hozzá a gf szorzatpolinom h-val való osztási maradékát. Mutassuk meg, hogy így akkor és csak akkor definiáltunk egy lineáris kódot, ha g és h legnagyobb közös osztójának a foka legfeljebb $s = k - n$.

(c) Tegyük fel, hogy a (b)-ben definiált K lineáris kódban g és h legnagyobb közös osztójának a foka pontosan s. Mutassuk meg, hogy ekkor K az (a)-beli értelemben vett polinomkód, amelynek a generáló polinomja osztója h-nak.

10.2.9 Tekintsünk egy (k, n) paraméterű K lineáris kódot. Mutassuk meg, hogy létezik olyan $n \times k$-as M 0–1 mátrix, hogy a kódszavakat M-mel balról megszorozva visszakapjuk a megfelelő közleményszavakat (azaz ha a $\mathbf{c}$ kódszó a $\mathbf{v}$ közleményszóból származott, akkor $M\mathbf{c} = \mathbf{v}$). Adjunk gyors algoritmust ilyen M megkeresésére.

10.3. Hamming-kód

Eddig a lineáris kódot egy lineáris leképezés *kép*tereként jellemeztük. Most ugyanezt egy másik lineáris leképezés *mag*tereként fogjuk tekinteni.

Egy (k, n) paraméterű K lineáris kód T^k-nak n-dimenziós altere. Legyen $k = n + s$ és $\mathcal{P} : T^k \to T^s$ olyan lineáris leképezés, amelynek a magtere $\operatorname{Ker}\mathcal{P} = K$. A dimenziótétel szerint ekkor $\mathcal{P}$ képtere az egész T^s.

Ilyen $\mathcal{P}$ lineáris leképezés megadásához a K altér egy $\mathbf{b}_1, \ldots, \mathbf{b}_n$ bázisát a $\mathbf{d}_1, \ldots, \mathbf{d}_s$ vektorokkal egészítsük ki T^k egy bázisává és legyen $\mathcal{P}\mathbf{b}_i = \mathbf{0}$, a $\mathcal{P}\mathbf{d}_j$ vektorok pedig legyenek tetszőleges független vektorok (azaz alkossanak bázist T^s-ben). Innen az is látszik, hogy a $\mathcal{P}$ leképezés általában nem egyértelmű.

10.3.1. Definíció

Legyen K egy (k, n) paraméterű lineáris kód, $k = n + s$, és $\mathcal{P} : T^k \to T^s$ olyan lineáris leképezés, amelynek a magtere K. Írjuk fel a $\mathcal{P}$ leképezés $P = [\mathcal{P}]$ mátrixát a természetes bázispár szerint. Ezt az $s \times k$ méretű P mátrixot a kód *paritásellenőrző mátrix*ának (vagy röviden, ellenőrző mátrixának) nevezzük. ♣

Az elnevezés magyarázatául gondoljuk végig, hogy mi történik, amikor a P mátrix egy sorát egy $\mathbf{z} \in T^k$ vektorral megszorozzuk. Ekkor eredményül $\mathbf{z}$ azon komponenseinek az összegét kapjuk, amely helyeken a P adott sorában 1-es áll, vagyis azt, hogy ezeken a helyeken $\mathbf{z}$-ben összesen páros vagy páratlan sok 1-es fordul-e elő. Ezt bármely sorral elvégezve pontosan a kódszavak esetén lesz minden ilyen összeg nulla. Azaz P valóban a vektorok bizonyos helyein álló 1-esek számának paritását ellenőrzi.

Mivel a $\mathcal{P}$ leképezés az esetek zömében nem egyértelmű, ezért egy kódnak általában több P paritásellenőrző mátrixa is létezik (vö. a 10.3.3–10.3.4 feladatokkal). Ezeket a definíció alapján azzal jellemezhetjük, hogy egy $\mathbf{z} \in T^k$ vektorra $P\mathbf{z} = \mathbf{0}$ akkor és csak akkor teljesül, ha $\mathbf{z}$ kódszó.

A már említett $\operatorname{Im}\mathcal{P} = T^s$ tulajdonság ekvivalens azzal, hogy $\dim \operatorname{Im}\mathcal{P} = s$, ami ugyanazt jelenti, hogy a P mátrix (F_2 feletti) rangja $r(P) = s$. Így egy paritásellenőrző mátrix rangja szükségképpen s. Sőt, ez a tulajdonság az előző bekezdés „akkor” részével kiegészítve már karakterizálja is a(z adott) kód paritásellenőrző mátrixait (lásd a 10.3.3 feladatot). Az is könnyen adódik, hogy ha egy 0–1 mátrixnak s sora, $k = n + s$ oszlopa van és a rangja s, akkor van olyan (k, n) paraméterű lineáris kód, amelynek éppen ez a paritásellenőrző mátrixa (lásd a 10.3.1 feladatot).

Illusztrációként nézzük a paritásvizsgálat-kódnak (a 10.1 pont P3 példájának) a paritásellenőrző mátrixát. Ez egyetlen „csupaegy” sorból áll (azaz olyan sorvektor, amelynek mind a k eleme 1-es): $P = (\,1 \quad 1 \quad 1 \quad \ldots \quad 1\,)$.

A G generátormátrixból általában könnyen megkaphatjuk a(z egyik) P paritásellenőrző mátrixot (lásd a 10.3.5 feladatot). Speciálisan, ha a kódszavak a hozzájuk tartozó közleményszavakkal kezdődnek, azaz a generátormátrix $G = \begin{pmatrix} E_{n\times n} \\ B_{s\times n} \end{pmatrix}$ alakú, akkor paritásellenőrző mátrixnak megfelel a $P = (\, B_{s\times n} \quad E_{s\times s}\,)$ mátrix.

Nézzük meg, hogyan használható a paritásellenőrző mátrix hibajavításra. Először is a definíció szerint $P\mathbf{z} = \mathbf{0}$ akkor és csak akkor teljesül, ha $\mathbf{z}$ kódszó. Ha az átvitelnél hiba történt és a kapott üzenet $\mathbf{z} = \mathbf{c} + \mathbf{h}$, ahol $\mathbf{c}$ a helyes kódszó, $\mathbf{h}$ pedig a hibaminta, akkor $P\mathbf{z} = P\mathbf{h}$. A $P\mathbf{z} \in T^s$ vektort a $\mathbf{z} \in T^k$ vektor *szindrómá*jának („tünetcsoportjának") nevezzük.

Ha a $\mathbf{h}$ hibamintában egyedül az i-edik helyen áll 1-es, akkor $P\mathbf{h}$ éppen a P mátrix i-edik oszlopa. Így a $\mathbf{z}$ vektor szindrómája a hibás helyeknek megfelelő P-beli oszlopok összege. Innen azonnal adódik az alábbi tétel:

10.3.2 Tétel

Egy lineáris kód pontosan akkor t-hibajavító, ha a P paritásellenőrző mátrixának bármely legfeljebb t darab oszlopát összeadva a kapott összegvektorok mind különbözők és egyikük sem nulla. ♣

Speciálisan, az 1-hibajavítás feltétele az, hogy P-ben minden oszlop különböző és egyik oszlop sem nulla.

A 10.1 pont végén láttuk, hogy ha egy 1-hibajavító kódnak s ellenőrző jegye van, akkor szükségképpen $n \le 2^s - s - 1$. Most megmutatjuk, hogy ennek a megfordítása is igaz:

10.3.3 Tétel

Legyen ($s \ge 2$ és) $n \le 2^s - s - 1$. Ekkor létezik $(s + n, n)$ paraméterű 1-hibajavító lineáris kód. ♣

Bizonyítás: Legyen P olyan $s \times (s+n)$-es mátrix, amelynek az oszlopai különböző nem nulla vektorok úgy, hogy ezek között található s darab lineárisan független. Ilyen P létezik, hiszen T^s-nek $2^s - 1 \ge n + s$ miatt elegendő számú nem nulla eleme van, a lineáris függetlenségi feltételt pedig biztosítja, ha pl. az utolsó s oszlopot az s darab egységvektornak választjuk.

Mivel P rangja s, ezért létezik olyan lineáris kód, amelynek P a paritásellenőrző mátrixa. Ez(ek) a kód(ok) a 10.3.2 Tétel, illetve az utána tett megjegyzés szerint 1-hibajavító(k). ■

Visszatérve a 10.1 pont végén említett $n = 500$ példára, a most bizonyított tételből következik, hogy az 1-hibajavítást mindössze $s = 9$ darab ellenőrző jeggyel meg tudjuk oldani (és ez a lehetséges minimum). Mindezt érdemes még egyszer összevetni a háromszori ismétlés kódjából adódó $s = 1000$ értékkel.

Az $n = 2^s - s - 1$ esetben a kódra külön elnevezést vezetünk be:

10.3.4 Definíció

Ha $n = 2^s - s - 1$ és $k = n + s = 2^s - 1$, akkor a (k, n) paraméterű 1-hibajavító lineáris kódokat *Hamming-kód*oknak nevezzük. ♣

Az előzőek szerint egy Hamming-kód azzal jellemezhető, hogy a paritásellenőrző mátrixában az oszlopok között a T^s vektortér összes nem nulla eleme pontosan egyszer fordul elő.

Feladatok

Valamennyi feladatban $n + s = k$, K egy (k, n) paraméterű lineáris kód, amelynek a generátormátrixa G, továbbá P egy $s \times k$ méretű 0–1 mátrix.

10.3.1 Igazoljuk, hogy egy 0–1 mátrixhoz akkor és csak akkor található olyan lineáris kód, amelynek ő a paritásellenőrző mátrixa, ha a sorai függetlenek, az oszlopai pedig összefüggők.

10.3.2 Írjuk fel a 10.1 pont P1 és P2 példájának, valamint a 10.1.2 feladatban szereplő kódok közül a lineárisaknak egy-egy paritásellenőrző mátrixát.

10.3.3 Mutassuk meg, hogy az alábbi három feltétel bármelyike ekvivalens azzal, hogy P a K kód (egyik) paritásellenőrző mátrixa:

I. $r(P) = s$ és bármely $\mathbf{c}$ kódszóra $P\mathbf{c} = \mathbf{0}$;

II. $r(P) = s$ és $PG = 0$;

III. P sorai bázist alkotnak az $(\operatorname{Im} \mathcal{A})^{\perp}$ altérben.

10.3.4

(a) Mutassuk meg, hogy egy kód paritásellenőrző mátrixa akkor és csak akkor egyértelmű, ha $s = 1$.

(b) Bizonyítsuk be, hogy egy kód paritásellenőrző mátrixainak a száma $\prod_{i=0}^{s-1}(2^s - 2^i)$.

10.3.5

(a) Ellenőrizzük, hogy ha $G = \begin{pmatrix} E_{n\times n} \\ B_{s\times n} \end{pmatrix}$ alakú, akkor paritásellenőrző mátrixnak valóban megfelel a $P = (\, B_{s\times n} \quad E_{s\times s}\,)$ mátrix.

(b) Adjunk általában is gyors algoritmust arra, hogyan lehet G ismeretében a paritásellenőrző mátrixo(ka)t megkapni.

10.3.6 Legyen Q egy olyan 0–1 mátrix, amelynek k oszlopa van és a magtere K. Bizonyítsuk be, hogy $r(Q) = s$, és Q bármely s független sora a K (egyik) paritásellenőrző mátrixát adja.

10.3.7 Mutassuk meg, hogy egy lineáris kódnál két T^k-beli vektor akkor és csak akkor kerül a dekódolási tábla azonos sorába, ha ugyanaz a szindrómájuk.

10.3.8 Egy lineáris kódban a kódszavak közötti minimális távolság pontosan akkor d, ha a(z egyik) paritásellenőrző mátrixban bármely $d-1$ oszlop lineárisan független, de van d olyan oszlop, amely összefüggő.

10.3.9 Egy lineáris kódban a kódszavak közötti minimális távolság legfeljebb 1-gyel lehet nagyobb az ellenőrző jegyek számánál.

10.3.10 Egy K kód *duális*a a $K^\perp$ merőleges kiegészítő altér. Mi a kapcsolat K-nak és duálisának a generátor- és paritásellenőrző mátrixai között?

10.3.11 Legyen $P = (\, B \quad E\,)$ a K lineáris kód paritásellenőrző mátrixa. Bizonyítsuk be, hogy K akkor és csak akkor duáisa önmagának, ha $B^T = B^{-1}$.

10.3.12 Mennyi egy Hamming-kódban a kódszavak közötti minimális távolság?

10.3.13 Bizonyítsuk be, hogy egy Hamming-kódban bármely kódszónak a komplementere is kódszó. (Két vektor egymás *komplementere*, ha minden komponensükben különböznek, vö. a 9.4.2a feladattal).

10.3.14 Legyen $s \geq 2, n = 2^s - s - 1$ és $k = 2^s - 1$. Legyen továbbá minden $0 \leq j \leq s-1$-re M_j azoknak a természetes számoknak a halmaza, amelyek kettes számrendszerbeli alakjában a 2^j együtthatója (azaz hátulról számítva a $j+1$-edik számjegy) 1. Nyilván bármely j-re $|M_j| = 2^{s-1}$.

Egy (k, n) paraméterű lineáris kódot fogunk megadni. A közleményszavak jegyeit azonban most nem a szokásos módon indexezzük, hanem az indexek közül a kettőhatványokat (beleértve az 1-et is) kihagyjuk (mint egyes szállodákban a szobaszámok közül kihagyják a

13-at, csak mi most a kettőhatványokra vagyunk „babonásak"). Így az indexekben (az $1, 2, \ldots, n$ számok helyett) rendre a $3, 5, 6, 7, 9, \ldots$, $k = n + s$ számok szerepelnek (hiszen éppen az $1, 2, 2^2, \ldots, 2^{s-1}$ kettőhatványokat kellett kihagynunk). Tekintsük ezek után a

$$\varphi : \alpha_3\alpha_5\alpha_6 \ldots \alpha_k \mapsto \alpha_3\alpha_5\alpha_6 \ldots \alpha_k\gamma_0\gamma_1 \ldots \gamma_{s-1}$$

kódoló függvényt, ahol $\gamma_j = \sum_{i \in M_j} \alpha_i$, $j = 0, 1, \ldots, s-1$. Mutassuk meg, hogy így egy Hamming-kódot kapunk.

10.4. BCH-kódok

A Hamming-kód a kódelmélet hajnalán, az 1940-es évek végén már megszületett. Ezután több, mint 10 évet kellett várni, míg az 1-hibajavítást sikerült hasonló hatékonyságú 2-hibajavításra fejleszteni. Az új kódokat közel egyidejűleg fedezte fel (vagy találta fel?) R. C. Bose és D. K. Ray-Chaudhuri (aki ekkor még Bose diákja volt), valamint tőlük függetlenül A. Hocquenghem. A kódokat a felfedezők nevének kezdőbetűiről BCH-kódoknak nevezik.

A BCH-kódokban a *véges testek* lényeges szerephez jutnak. (A véges testekre vonatkozó legfontosabb tudnivalókat az A.11 pont tartalmazza.)

Továbbra is n, k és $s = k - n$ jelöli a kód dimenzióját, hosszát, illetve az ellenőrző jegyek számát, és valamilyen adott t-vel t-hibajavító kódokat keresünk. Az eddigiekben az n-et tekintettük adottnak, és az s-et az n-hez képest igyekeztünk minimalizálni. Ezen a szemléletmódon egy picit változtatunk, mostantól kezdve $k = n + s$-t tekintjük rögzítettnek, és így szeretnénk minél kisebb s-et és vele együtt minél nagyobb n-et biztosítani.

Ennek alapján most T^k-ban egy minél nagyobb olyan K alteret keresünk, amelynek az elemei, a kódszavak, legalább $2t + 1$ távolságra esnek egymástól. Ez a K altér éppen a P paritásellenőrző mátrix magtere. A t-hibajavítás a P oszlopainak megfelelő tulajdonságából olvasható le, tehát a kódot egy megfelelő $s \times k$ méretű P mátrix kijelölésével adhatjuk meg. Az s minimalizálása azt jelenti, hogy P-nek minél kevesebb sora legyen.

Tekintsünk el egy pillanatra attól a követelménytől, hogy P sorai lineárisan függetlenek. Ha valamelyik sor függ a többitől, akkor ennek a sornak az elhagyása nyilván nem változtat sem a mátrix magterén, sem pedig az oszlopoknak a hibajavítással kapcsolatos tulajdonságain. Így a sorok számát mindaddig csökkenthetjük, amíg azok már függetlenek lesznek (vö. a 10.3.7 feladattal).

Ennek megfelelően olyan $m \times k$-as Q mátrixokat fogunk megadni, amelyekben bármely legfeljebb t oszlop összege mindig különböző és nem nulla

vektort eredményez (azaz bármely $2t$ oszlop lineárisan független), és m lehetőleg kicsi. Ekkor Q magtere éppen egy t-hibajavító lineáris kódot definiál. Ennél a kódnál az ellenőrző jegyek száma $s = r(Q) \leq m$, és egy P paritásellenőrző mátrixot úgy kaphatunk, hogy Q-nak csak s (tetszőlegesen választott) független sorát tartjuk meg. Magát a Q-t nevezhetjük a kód „*kvázi-paritásellenőrző mátrix*ának".

Mielőtt az általános t-hibajavító BCH-kódokra rátérnénk, nézzük meg külön a $t = 2$ speciális esetet. Ez a tárgyalásmód több előnnyel is jár, ugyanis a BCH-kódok meglehetősen bonyolult konstrukcióját így először mégiscsak egy könnyített változatban kell megértenünk, továbbá a t-hibajavítás bizonyítása is lényegesen egyszerűbb $t = 2$-re, mint az általános esetben.

Legyen $q \geq 3$ és $k = 2^q - 1$. A 10.1.8 feladatból következik, hogy 2-hibajavító kód esetén az ellenőrző jegyek száma szükségképpen $s \geq 2q - 1$. A 2-hibajavító BCH-kódok lényegében az alsó határt érik el, mert $s \leq 2q$-t biztosítanak. (Az is megmutatható, hogy ezeknél mindig pontosan $s = 2q$ teljesül.) Látjuk tehát, hogy azonos k mellett a Hamming-kódhoz képest egy 2-hibajavító BCH-kódnál kétszer annyi ellenőrző jegyre van szükség. Ez igen méltányos „ár", hiszen a nyújtott „szolgáltatás" formálisan nézve is „megduplázódott", valójában azonban a 2-hibaminták száma sokszorosa az 1-hibamintákénak ($\binom{k}{2}$, illetve k).

A 2-hibajavító BCH-kódot a(z egyik) P paritásellenőrző mátrixával adjuk meg. Ehhez először egy $2q \times k$ méretű Q kvázi-paritásellenőrző mátrixot definiálunk. Ennek első q sora legyen ugyanaz, mint a Hamming-kódnál, vagyis az oszlopok éppen T^q nem nulla elemei.

A Q alsó q sorának a megadásához a továbbiakban a T^q halmazt új szerepkörben, 2^q elemű testként fogjuk tekinteni. Ennek a testnek és a T^q vektortérnek az additív szerkezete megegyezik, ezért nem okoz zavart, ha a testet is T^q-val jelöljük. Legyen Δ a T^q test multiplikatív csoportjának egy generátoreleme, ekkor a T^q test nem nulla elemei felírhatók Δ-nak (a 0-tól a $2^q - 2$ kitevőig terjedő) hatványaiként. A Q felső felében ezek szerint az oszlopok éppen a Δ^j hatványok, $j = 0, 1, 2, \ldots, 2^q - 2$.

Ezután a Q mátrix alsó q sorát a következőképpen definiáljuk: az oszlopok alsó fele legyen mindig a felső rész köbe, azaz

$$Q = \begin{pmatrix} 1 & \Delta & \Delta^2 & \ldots & \Delta^j & \ldots \\ 1 & \Delta^3 & \Delta^6 & \ldots & \Delta^{3j} & \ldots \end{pmatrix}. \tag{10.4.1}$$

Megmutatjuk, hogy a Q mátrix magtere egy 2-hibajavító kód. Ehhez azt kell igazolni, hogy Q bármely legfeljebb 2 oszlopának az összege mindig más és más (és nem nulla) vektort eredményez. Ez könnyen láthatóan ekvivalens

azzal, hogy az

$$\mathbf{x}+\mathbf{z}=\mathbf{a}, \qquad \mathbf{x}^3+\mathbf{z}^3=\mathbf{b}$$

egyenletrendszernek $\mathbf{a}\neq\mathbf{0}$ esetén a T^q testben legfeljebb egy megoldása van ($\mathbf{x}$ és $\mathbf{z}$ szimmetriájától eltekintve).

Az első egyenletet köbre emelve, majd a második egyenletet ebből levonva $\mathbf{xz}(\mathbf{x}+\mathbf{z})=\mathbf{a}^3-\mathbf{b}$ adódik, vagyis $\mathbf{xz}=\mathbf{a}^2-\mathbf{b}/\mathbf{a}$. Azt kaptuk, hogy az $\mathbf{x}$ és $\mathbf{z}$ elemek összege és szorzata is ismert, és így pl. a gyökök és együtthatók közötti összefüggés alapján $\mathbf{x}$ és $\mathbf{z}$ csak egy adott másodfokú egyenlet (egyértelműen meghatározott) gyökei lehetnek (ha ez az egyenlet egyáltalán megoldható a T^q testben).

Mint már említettük, megmutatható, hogy Q rangja $2q$ (lásd a 10.4.4 feladatot), és így maga a Q lesz ennek a kódnak a(z egyik) paritásellenőrző mátrixa. (Ha nem így lenne, akkor „még jobban járnánk", hiszen akkor változatlan $k=2^q-1$ mellett $2q$-nál kevesebb ellenőrző jeggyel is biztosítani tudnánk a 2-hibajavítást.)

A kapott eredményt az alábbi tételben foglalhatjuk össze:

10.4.1 Tétel

Legyen $q\geq 3, n=2^q-2q-1, k=2^q-1$. A fenti módon a (10.4.1) képlettel megadott Q mátrix egy 2-hibajavító lineáris kódot definiál. Ezt a kódot 2-hibajavító *BCH-kód*nak nevezzük. ♣

Példa: Legyen $q=4$. A $2^4=16$ elemű testben meg kell keresnünk a nem nulla elemek multiplikatív csoportjának egyik generáló elemét. Az ilyen elemek száma $\varphi(15)=8$. Ezek bármelyike negyedfokú algebrai szám $T=F_2$ felett, tehát egy negyedfokú f irreducibilis polinomnak a gyöke. Mivel $f(0)\neq 0$, $f(1)\neq 0$, ezért f-ben páratlan sok tag fordul elő, azaz f az alábbi négy polinom valamelyike: $x^4+x+1, x^4+x^3+1, x^4+x^2+1, x^4+x^3+x^2+x+1$. A harmadik polinom $(x^2+x+1)^2$, tehát nem irreducibilis, a negyedik irreducibilis, azonban osztója az x^5-1-nek, tehát a gyökeinek már az ötödik hatványa 1, vagyis azok nem generálhatják a test multiplikatív csoportját. Az első két polinom megfelelő, ezek gyökeiként kapjuk a test multiplikatív csoportjának 8 generáló elemét. Válasszuk mondjuk az első polinom egyik gyökét Δ-nak. Ekkor a T^4 vektortér bázisa $1, \Delta, \Delta^2, \Delta^3$, ezek lesznek most az egységvektorok. A többi hatvány koordinátáit a minimálpolinomból adódó $\Delta^4=1+\Delta$ összefüggés ismételt alkalmazásával számíthatjuk ki. Ennek megfelelően az alábbi 8×15-ös

paritásellenőrző mátrixhoz jutunk:

$$\left(\begin{array}{cccccccccccccc}
1 & 0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\
0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 0 \\
0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 & 0 \\
0 & 0 & 0 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 1 & 1 \\
\hline
1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 \\
0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 1 \\
0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\
0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 1 & 1
\end{array}\right)$$

A t-hibajavító BCH-kódokra történő általánosítás a 2-hibajavító mintájára a következőképpen történik. Az eddigiekhez hasonlóan k értéke $k = 2^q - 1$, az ellenőrző jegyek számára most az $s \leq tq$ „méltányos" feltételt szabjuk (itt már az a szerencsés eset is előfordulhat, hogy s a jelzett korlátnál jóval kisebb lesz). A Q „kvázi-paritásellenőrző" mátrix t darab $q \times k$ méretű blokkból áll, ahol a felső blokk oszlopai továbbra is T^q nem nulla elemei, az i-edik blokk oszlopai pedig a felső blokkbeli vektoroknak (mint a T^q test elemeinek) a $2i-1$-edik hatványai, $i = 2, 3, \ldots, t$. (A köbök alatt tehát az ötödik, majd a hetedik hatványok következnek stb.) Ha Q sorai összefüggők, akkor válasszunk ki közülük egy maximális független rendszert, ezek alkotják a kód (egyik) P paritásellenőrző mátrixát. Mindezt pontosan az alábbi tételben mondjuk ki és bizonyítjuk be.

10.4.2. Tétel

Legyen q rögzített pozitív egész, amelyre $2^q - 1 > qt$, továbbá $k = 2^q - 1$, $m = tq$, Δ a T^q test multiplikatív csoportjának egy generátoreleme és Q az a $tq \times k$-as mátrix, amelynek a $j+1$-edik oszlopában egymás alatt rendre az alábbi t darab T^q-beli vektor áll: $\Delta^j, \Delta^{3j}, \Delta^{5j}, \ldots, \Delta^{(2t-1)j}$, azaz

$$Q = \begin{pmatrix}
1 & \Delta & \Delta^2 & \ldots & \Delta^j & \ldots \\
1 & \Delta^3 & \Delta^6 & \ldots & \Delta^{3j} & \ldots \\
1 & \Delta^5 & \Delta^{10} & \ldots & \Delta^{5j} & \ldots \\
\vdots & \vdots & \vdots & & \vdots & \\
1 & \Delta^{2t-1} & \Delta^{4t-2} & \ldots & \Delta^{(2t-1)j} & \ldots
\end{pmatrix}.$$

Ekkor $\operatorname{Ker} Q$ egy t-hibajavító lineáris kódot definiál, ahol az ellenőrző jegyek száma $s \leq tq$. Ezt a kódot t-hibajavító BCH-kódnak nevezzük. ♣

A tétel állítása az, hogy az így definiált kód valóban t-hibajavító. Ennek bizonyítása további előkészületeket igényel.

Először felelevenítjük a 10.2.8a feladatban bevezetett *polinomkód* fogalmát. Legyen $T = F_2$, és jelölje $T_m[x]$ a T feletti legfeljebb $m-1$-edfokú polinomok szokásos vektorterét. Ekkor az

$$\alpha_0\alpha_1\ldots\alpha_{m-1} \mapsto \alpha_0 + \alpha_1 x + \ldots + \alpha_{m-1}x^{m-1}$$

megfeleltetés izomorfizmus a T^m és $T_m[x]$ vektorterek között. Azonosítsuk a T^n, illetve T^k vektortereket a belőlük a fenti izomorfizmussal létesített $T_n[x]$, illetve $T_k[x]$ vektorterekkel.

10.4.3 Definíció

Legyen $g \neq 0$ egy rögzített s-edfokú polinom T felett. Legyen az $\mathcal{A} : T_n[x] \to T_k[x]$ leképezés a g polinommal történő szorzás, azaz $\mathcal{A}$ minden legfeljebb $n-1$-edfokú f polinomhoz a gf polinomot rendeli hozzá: $\mathcal{A}f = gf$. Az így definiált lineáris kódot *polinomkód*nak, a g polinomot pedig a kód *generáló polinom*jának nevezzük. ♣

A 10.2.8a feladatban megengedtük a $\deg g < s$ lehetőséget is, azonban ekkor minden kódszó végén $s - \deg g$ darab nulla áll, ami semmire sem használható. Így nyilván csak az az eset érdekes, amikor $\deg g = s$. Ekkor a kódszavak éppen g többszörösei (polinomszorosai).

Most megmutatjuk, hogy a Hamming-kód és a BCH-kódok is polinomkódok, és meghatározzuk a generáló polinomjaikat.

Tekintsük elsőként a Hamming-kódot. Itt paritásellenőrző mátrixnak vehető az s sorból és $k = 2^s - 1$ oszlopból álló $P = (\,1 \quad \Delta \quad \Delta^2 \quad \ldots \quad \Delta^{k-1}\,)$ mátrix. Legyen a $\mathbf{c} = \gamma_0\gamma_1\ldots\gamma_{k-1} \in T^k$ vektornak megfelelő polinom $C = \gamma_0 + \gamma_1 x + \ldots + \gamma_{k-1}x^{k-1} \in T_k[x]$. A $\mathbf{c}$ vektor pontosan akkor kódszó, ha $P\mathbf{c} = \mathbf{0}$, azaz $\sum_{j=0}^{k-1} \gamma_j \Delta^j = 0$. Ez azt jelenti, hogy a C polinomnak gyöke a Δ, vagyis $\mathbf{c}$ pontosan akkor kódszó, ha az m_Δ minimálpolinom osztója C-nek. Ennek megfelelően a Hamming-kód olyan polinomkód, amelynek a generáló polinomja $g = m_\Delta$.

Nézzük most a 2-hibajavító BCH-kódot. Az előzőkhöz hasonlóan adódik, hogy $\mathbf{c}$ pontosan akkor kódszó, ha m_Δ és m_{Δ^3} is osztója a C polinomnak, azaz a generáló polinom most Δ és Δ^3 minimálpolinomjának a legkisebb közös többszöröse: $g = [m_\Delta, m_{\Delta^3}]$.

Ugyanígy adódik az általános eset is:

10.4.4 Tétel

Jelöljük m_{Δ^j}-t m_j-vel. A 10.4.2 Tételben megadott általános t-hibajavító BCH-kód olyan polinomkód, amelynek a generáló polinomja $g_t = [m_1, m_3, \ldots, m_{2t-1}]$. ♣

Ennek alapján a kódban az ellenőrző jegyek száma éppen a g_t generáló polinom foka. Így $s = tq$ pontosan akkor teljesül, ha $\Delta, \Delta^3, \ldots, \Delta^{2t-1}$ mindegyike q-adfokú F_2 felett és semelyik kettőnek sem ugyanaz a minimálpolinomja (lásd a 10.4.2 feladatot).

Most már minden a rendelkezésünkre áll a 10.4.2 Tétel igazolásához: megmutatjuk, hogy az ott megadott kód valóban t-hibajavító.

A 10.4.2 Tétel bizonyítása: Először belátjuk, hogy bármely i-re $m_i = m_{2i}$. A T^q testben a négyzetre emelés izomorfizmus, amely a $T = F_2$ alaptest elemeit helybenhagyja. Ezért ha $\rho_0 + \rho_1\Theta + \ldots + \rho_v\Theta^v = 0$, akkor ugyanez Θ helyett Θ^2-re is teljesül. Ezzel igazoltuk, hogy $m_{2i} \mid m_i$. A másik irányú oszthatóság pl. abból adódik, hogy Θ-t is megkaphatjuk Θ^2-ből ismételt négyzetre emelésekkel.

A fentiek alapján $g_t = [m_1, m_2, \ldots, m_{2t}]$. Most megmutatjuk, hogy a kódban a minimális távolság legalább $2t + 1$, amiből a kívánt t-hibajavítás már következik.

Indirekt tegyük fel, hogy lenne egy legfeljebb $2t$ súlyú $\mathbf{c}$ kódszó. Az ennek megfelelő C polinom gyökei között szerepel Δ^i minden $i \leq 2t$-re. Írjuk fel ezt a $2t$ darab $C(\Delta^i) = 0$ egyenlőséget. Közben a C polinomból esetleg hagyjunk el 0 együtthatókat úgy, hogy pontosan $2t$ együttható maradjon.

Ekkor C-nek erre a $2t$ együtthatójára nézve egy $2t \times 2t$-es homogén lineáris egyenletrendszert kaptunk, amelynek van nem triviális megoldása (éppen C megfelelő együtthatói). Másrészt az egyenletrendszer determinánsa nem nulla, hiszen ez a különböző elemekkel generált $V(\Delta^{i_1}, \Delta^{i_2}, \ldots, \Delta^{i_{2t}})$ Vandermonde-determináns nem nulla konstansszorosa, ahol $i_1, i_2, \ldots, i_{2t}$ a C polinomban szereplő tagok fokszámai. Ekkor azonban az egyenletrendszernek csak triviális megoldása lehet, ami ellentmondás. ■

Feladatok

A feladatoknál is a szövegben használt jelöléseket alkalmazzuk, tehát s az ellenőrző jegyek száma, k a kód hossza, Δ a 2^q elemű véges test multiplikatív csoportjának a(z egyik) generátoreleme, m_i a Δ^i minimálpolinomja stb.

10.4.1 Írjuk fel $q = 5$-re egy 2-hibajavító BCH-kód paritásellenőrző mátrixát.

10.4.2 Mutassuk meg, hogy a q paraméterű t-hibajavító BCH-kódban $s = tq$ pontosan akkor teljesül, ha $\Delta, \Delta^3, \ldots, \Delta^{2t-1}$ mindegyike q-adfokú F_2 felett és semelyik kettőnek sem ugyanaz a minimálpolinomja.

M 10.4.3 Tekintsünk $q > 3$-ra egy 3-hibajavító BCH-kódot.

(a) Határozzuk meg s-et a $q = 4$ esetben.

*(b) Mutassuk meg, hogy ha q páratlan, akkor $s = 3q$.

*10.4.4 Bizonyítsuk be, hogy bármely q esetén egy 2-hibajavító BCH-kódban $s = 2q$.

M*10.4.5

(a) Igazoljuk, hogy $\deg m_i$ a legkisebb olyan v pozitív egész, amelyre $v \mid q$ és $(2^q - 1)/(2^v - 1) \mid i$.

(b) Mutassuk meg, hogy m_i összes gyökei a Δ-nak az $i \cdot 2^j$ kitevőjű hatványai, ahol $0 \leq j < \deg m_i$.

M*10.4.6 Lássuk be, hogy ha $t \leq 2^{q/2} - 1$, akkor a q paraméterű t-hibajavító BCH-kódban az $s = tq$ egyenlőség érvényes.

10.4.7 Legyen egy polinomkód generáló polinomja g. Bizonyítsuk be, hogy

(a) minden kódszó akkor és csak akkor páros súlyú, ha $1 + x \mid g$;

(b) minden páros súlyú vektor akkor és csak akkor kódszó, ha $g = 1 + x$.

10.4.8 Mutassuk meg, hogy egy BCH-kód generáló polinomja osztója $x^k - 1$-nek.

10.4.9 *Ciklikus*nak nevezzük az olyan lineáris kódokat, amelyeknél a kódszavak ciklikus permutációja is kódszó, tehát (T^k elemeit $\mathbf{z} = \gamma_0\gamma_1\gamma_2 \ldots \gamma_{k-1}$ alakban írva)

$$\gamma_0\gamma_1\gamma_2 \ldots \gamma_{k-1} \in K \Rightarrow \gamma_{k-1}\gamma_0\gamma_1 \ldots \gamma_{k-2} \in K.$$

M*(a) Bizonyítsuk be, hogy a ciklikus kódok lényegében speciális polinomkódokként jellemezhetők: egy kód akkor és csak akkor ciklikus, ha a kódszavainak a halmaza megegyezik egy olyan polinomkód kódszavainak a halmazával, amelynek a g generáló polinomjára $g \mid x^k - 1$ teljesül.

(b) Minden BCH-kód ciklikus.

M 10.4.10 Tegyük fel, hogy az $m < k$ és d számokra $\sum_{i=0}^{d-2} \binom{k-1}{i} < 2^m$. Ekkor létezik olyan lineáris kód, amelynek a hossza k, az ellenőrző jegyek száma legfeljebb m és a kódszavak közötti minimális távolság legalább d.

M*10.4.11 *Reed–Muller-kódok.*

(a) Legyen q adott, $n = q + 1$, $k = 2^q$ és a kód generátormátrixa a következő: soronként rendre a 2^q és $2^{q+1} - 1$ közötti számok kettes számrendszerbeli alakja szerepel. (A $q = 3$ esetre a mátrixot lásd a (b) rész után.) Mutassuk meg, hogy ebben a kódban a kódszavak közötti minimális távolság 2^{q-1}. Ezt a kódot *elsőrendű Reed–Muller-kód*nak nevezzük.

(b) Legyen $m < q$. Az *m-edrendű Reed–Muller-kód* esetén $n = \sum_{i=0}^{m} \binom{q}{i}$, $k = 2^q$ és a generátormátrix a következő: az első $q+1$ oszlop azonos az elsőrendű esetben látottal, a további oszlopokat pedig úgy kapjuk meg, hogy a 2-odik, 3-adik, ..., $q+1$-edik oszlop közül minden lehetséges módon kiválasztunk 2, 3, ..., m darabot és ezeket összeszorozzuk a komponensenkénti szorzással. Mutassuk meg, hogy ebben a kódban a kódszavak közötti minimális távolság 2^{q-m}.

Például $q = 3$-ra az első- és másodrendű Reed–Muller-kód generátormátrixai:

$$G(1,3) = \begin{pmatrix} 1 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 1 & 1 & 0 & 1 \\ 1 & 1 & 1 & 0 \\ 1 & 1 & 1 & 1 \end{pmatrix} \qquad G(2,3) = \begin{pmatrix} 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 1 & 0 & 0 & 1 & 0 & 0 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & 1 & 0 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 1 & 1 & 1 & 1 \end{pmatrix}$$

Itt $G(2,3)$ utolsó három oszlopa rendre a 2. és 3., a 2. és 4., illetve a 3. és 4. oszlop szorzata.

A. ALGEBRAI ALAPFOGALMAK

Ebben a „függelékben" összefoglaljuk a *könyvben felhasznált* legfontosabb algebrai alapfogalmakat és az ezekre vonatkozó főbb tételeket. Célunk az volt, hogy megfelelő algebrai hátteret biztosítsunk a *többi fejezet megértéséhez*. Ezzel összhangban most *bizonyos* témakörök *vázlatos* bemutatása, és nem az algebra egyes fejezeteinek átfogó, szisztematikus felépítése következik.

A fejezet két, egymástól lényegesen különböző jellegű, egy „elemi" és egy „haladó" részre tagozódik.

Az „elemi" A.1–A.7 pontokban minden szempontból alapvető ismereteket rendszerezünk, *viszonylag* részletes magyarázatokkal. Ennek a résznek az alapos elsajátítását (illetve átismétlését) nagyon melegen ajánljuk.

A „haladó" A.8–A.11 pontokkal kapcsolatban rögtön megjegyezzük, hogy a többi fejezetben csak kevés helyen támaszkodunk az itt tárgyalt anyagra, a könyv legnagyobb része enélkül is megérthető. Az itt bemutatott algebrai fogalmak általában lényegesen nehezebbek a korábbiaknál, és a nehézséget csak fokozza az eddig megszokotthoz képest jóval tömörebb tárgyalásmód, valamint az, hogy az eredményeket többnyire bizonyítás nélkül közöljük.

Az A.8–A.10 pontok elsősorban a véges testeknek az A.11 pontban sorra kerülő tárgyalását készítik elő. A véges testek számos alkalmazásnál igen fontos szerepet játszanak. Ezek egy részéhez tulajdonképpen csak a modulo p maradékosztályokra (sőt gyakran csak a $p = 2$ esetre) van szükség. A véges testek szerkezetének mélyebb vonásait elsősorban a 9.6 és 10.4 pontokban használtuk fel.

Természetesen a függelék nemcsak a könyv többi részének a tanulmányozását könnyít(het)i meg, hanem sok más szempontból is fontos és hasznos (és — reméljük — önmagában is érdekes) anyagot tárgyal.

A.1. Bemelegítés

1. Teljes indukció

A teljes indukció fontos módszer a tetszőleges pozitív egészre vonatkozó állítások bizonyítására. Ellenőrizzük, hogy

(i) az állítás igaz $n = 1$-re (kiinduló lépés), és

(ii) az igazsága öröklődik $n = k$-ról $n = k + 1$-re bármilyen k pozitív egész esetén (indukciós lépés).

Ekkor az állítás igaz minden n pozitív egészre.

Ez olyasmi, mint a dominóhatás: Ha végtelen sok dominó áll egymás mögött, és meglökjük az elsőt, akkor az meglöki a másodikat, ami meglöki a harmadikat stb., és végül mindegyik eldől.

Az indukciós lépésnél nem bizonyítjuk, hogy az állítás igaz k-ra (ha ezt közvetlenül bizonyítani tudnánk, nem lenne szükség indukcióra), csak feltesszük az érvényességét $n = k$ esetén, és ezt kihasználva igazoljuk, hogy akkor $k + 1$-re is fenn kell állnia.

A módszernek többféle változata is létezik: indulhatunk $n = 0$-ról vagy más kezdeti értékről; támaszkodhatunk arra, hogy $n = k$-ra és $n = k - 1$-re is igaz az állítás (ebben az esetben két szomszédos kinindulási értéket kell közvetlenül ellenőrizni); illeve feltehetjük, hogy minden, $n = k$-nál kisebb vagy egyenlő egészre fennáll.

P1 példa: Lássuk be, hogy $5^{n+2} + 6^{2n+1}$ minden $n \geq 0$ egészre osztható 31-gyel.

Bizonyítás: Kiinduló lépés: $n = 0$ esetén $31 \mid 5^2 + 6$.

Indukciós lépés: Feltesszük, hogy $31 \mid 5^{k+2} + 6^{2k+1}$, és belátjuk, hogy $31 \mid 5^{(k+1)+2} + 6^{2(k+1)+1}$. Célszerű átalakítással

$$5^{k+3} + 6^{2k+3} = 5(5^{k+2} + 6^{2k+1}) + 31 \cdot 6^{2k+1}.$$

A jobb oldal első tagja az indukciós feltevés szerint többszöröse a 31-nek, a második tagról ez közvetlenül látszik. Így az összegük is osztható 31-gyel.

2. Binomiális tétel

Az $\binom{n}{k}$ binomiális együttható egy n elemű halmaz k elemű részhalmazainak a számát jelenti. Más megfogalmazásban, hányféleképpen tudunk n elem közül k-t kiválasztani úgy, hogy minden elemet legfeljebb egyszer vehetünk, és az elemek kiválasztásának a sorrendje nem számít. Ennek képlete

$$\binom{n}{k} = \frac{n!}{k!(n-k)!} = \frac{n(n-1)\dots(n-k+1)}{k!} \tag{A.1.1}$$

ahol $j! = j(j-1)\dots 2 \cdot 1$ ha $j > 0$ és $0! = 1$. (A.1.1) igazolásához vegyük észre, hogy elsőnek tetszőlegesen választhatunk az n elem közül, másodiknak a maradék $n-1$ bármelyikét vehetjük stb., és végül k-adiknak a még megmaradt $n-(k-1)$ közül veszünk ki egyet. Ez összesen $n(n-1)\dots(n-k+1)$ lehetőség. Azonban, mivel a kiválasztás sorrendje nem számít, ezt el kell osztanunk a k elem összes lehetséges sorrendjének a számával. Így kapjuk az (A.1.1)-ben szereplő utolsó képletet. A nevezőt és a számlálót $(n-k)!$-sal bővítve adódik a középen álló kifejezés.

Például $\binom{8}{2} = 8 \cdot 7/2 = 28$, $\binom{n}{1} = n$, $\binom{n}{0} = 1$ (mivel az üres halmaz az egyetlen 0 elemű részhalmaz vagy pedig a képlet alapján, felhasználva, hogy $0! = 1$).

A.1.1 Tétel (Binomiális tétel)

$$(a+b)^n = \binom{n}{0}a^n + \binom{n}{1}a^{n-1}b + \binom{n}{2}a^{n-2}b^2 + \ldots + \binom{n}{n}b^n = \sum_{k=0}^{n}\binom{n}{k}a^{n-k}b^k. \clubsuit$$

Bizonyítás: Az $(a+b)(a+b)\ldots(a+b)$ szorzás elvégzésekor minden tényezőből az egyik tagot, a-t vagy b-t vesszük, ezeket összeszorozzuk, és az összes ilyen szorzatot összeadjuk. Például, ha mind az n zárójelből az a-t vesszük, akkor az a^n szorzat adódik; ha a-t veszünk az első két zárójelből és b-t a többi $n-2$-ből, ez a^2b^{n-2}-t eredményez stb. Vagyis $a^{n-k}b^k$ típusú szorzatokat kell összegeznünk, ahol $0 \leq k \leq n$. Egy ilyen $a^{n-k}b^k$ szorzat akkor keletkezik, ha k zárójelből veszünk b-t, a többi $n-k$ zárójelből pedig a-t. Így $\binom{n}{k}$ lehetőségünk van a b-k kiválasztására. Ennek megfelelően ez a tag $\binom{n}{k}$-szor fordul elő az összegben. ■

P2 példa: Igazoljuk, hogy $\sum_{k=0}^{n}\binom{n}{k} = 2^n$.

Első bizonyítás: A bal oldal egy n elemű halmaz össszes $(0, 1, \ldots, n$ elemű) részhalmazainak a száma. A jobb oldal ezt közvetlenül számolja meg: az n elem mindegyikére két lehetőség áll fenn aszerint, hogy benne van vagy nincs benne a részhalmazban.

Második bizonyítás: $2^n = (1+1)^n = \sum_{k=0}^{n}\binom{n}{k}1^{n-k} \cdot 1^k = \sum_{k=0}^{n}\binom{n}{k}$.

3. Logikai szitaformula

N tárgy mindegyike rendelkezhet a $P_1, \ldots, P_k$ tulajdonságok közül néhánnyal, akár az összessel, de esetleg eggyel sem. Ez utóbbiak számát jelölje N_0. Tudjuk, hány tárgyra érvényes P_1 függetlenül attól, hogy vannak-e ezeknek más tulajdonságaik. Ugyanígy tudjuk, hány tárgyra érvényes P_2, hányra teljesül (mondjuk) P_1, P_4 és P_6 mindegyike stb. Jelölje $N_{i_1 i_2 \ldots i_j}$ azon tárgyak számát, amelyekre fennáll $P_{i_1}, P_{i_2}, \ldots, P_{i_j}$ mindegyike (függetlenül a többi tulajdonság meglététől vagy hiányától). Ezekből ki tudjuk számítani N_0-t:

A.1.2 Tétel (Logikai szitaformula)

$$N_0 = N - \sum_{i=1}^{k} N_i + \sum_{1\le i_1<i_2\le k} N_{i_1 i_2} - \ldots + \\ + (-1)^j \sum_{1\le i_1<\ldots<i_j\le k} N_{i_1 i_2 \ldots i_j} + \ldots + (-1)^k N_{12\ldots k}. \ \clubsuit$$

Bizonyítás: Ha egy tárgy „tulajdonságmentes", akkor a jobb oldalon egyszer számoltuk, N-ben. Ha egy tárgy pontosan a $P_{i_1}, P_{i_2}, \ldots, P_{i_m}$ tulajdonságokkal rendelkezik, akkor $1 - \binom{m}{1} + \binom{m}{2} - \ldots + (-1)^m = (1-1)^m = 0$-szor szerepel a jobb oldalon. ■

P3 példa: Hányféleképpen fordulhat elő egy futóversenyen, hogy senkinek sem egyezik meg a helyezése a rajtszámával? (Holtverseny nincs.)

Megoldás: A verseny eredménye $N = n!$-féle lehet. Legyen P_i, $i = 1, 2, \ldots, n$ az a tulajdonság, hogy az i-edik rajtszámú versenyző az i-edik helyen végzett. Ekkor $N_i = (n-1)!$, mivel a többi versenyző sorrendje tetszőleges lehet. Ugyanígy, $N_{i_1 i_2} = (n-2)!$ stb. A logikai szitaformula szerint

$$N_0 = n! - n(n-1)! + \binom{n}{2}(n-2)! + \ldots + (-1)^n = n! \sum_{j=1}^{n} \frac{(-1)^j}{j!}.$$

Mivel a $\sum_{j=1}^{n}(-1)^j/j!$ összeg $1/e \approx 0{,}37$-hez tart, ha $n \to \infty$, így az ilyen eredmények aránya nagy n-re körülbelül 0,37.

4. Ekvivalenciareláció

Egy H halmazon értelmezett reláció bizonyos (a, b) párokat jelent (esetleg az összeset, esetleg egyet sem), ahol $a, b \in H$. Ha például $H = \{1, 2, 3\}$, akkor az $a < b$ reláció az $(1, 2), (1, 3)$ és $(2, 3)$ párokból áll.

Ha egy R relációban szerepel az (a, b) pár, akkor azt mondjuk, hogy a az R relációban van b-vel, és ezt aRb-vel jelöljük.

Az egyenlőség néhány alaptulajdonságával rendelkező relációkat *ekvivalenciarelációk*nak nevezzük:

A.1.3 Definíció

Egy H halmazon értelmezett R reláció ekvivalenciareláció, ha

(i) reflexív: aRa minden $a \in H$-ra,
(ii) szimmetrikus: $aRb \Rightarrow bRa$, és
(iii) tranzitív: $aRb, bRc \Rightarrow aRc$. ♣

Az ekvivalenciarelációk segítségével lehet egy halmazt diszjunkt részhalmazok egyesítésére bontani:

A.1.4 Tétel

Ha R ekvivalenciareláció a H halmazon, akkor a $C_a = \{b \in H \mid aRb\} \subseteq H$ részhalmazok vagy diszjunktak, vagy egybeesnek. Ezért H a különböző C_a részhalmazok diszjunkt egyesítése. ♣

A C_a részhalmazt az a elem által reprezentált ekvivalenciaosztálynak nevezzük. Egy ekvivalenciareláció tehát a H halmaz ekvivalenciaosztályokra történő partícióját hozza létre. Ennek a megfordítása is igaz: a H minden partíciója egy alkalmas ekvivalenciarelációból származik, nevezetesen aRb jelentse azt, hogy a partíciós felbontásban a és b ugyanabban a részhalmazban találhatók.

Bizonyítás: Azt kell megmutatnunk, hogy ha C_a és C_b nem diszjunktak, akkor $C_a = C_b$. Belátjuk, hogy $C_a \subseteq C_b$; a másik irányú tartalmazás hasonlóan igazolható, illetve azonnal következik a és b szerepének szimmetriájából.

Legyen $x \in C_a$, azaz aRx, és bRx-t kell igazolnunk. Legyen $d \in C_a \cap C_b$, tehát aRd and bRd. Mivel R szimmetrikus, $aRd \Rightarrow dRa$. A tranzitivitás miatt dRa-ból és aRx-ből adódik dRx. Ismét a tranzitivitás miatt bRd and dRx biztosítják bRx-et. ■

P4 példa: Álljon H a nem nulla valós számokból, és a akkor legyen relációban b-vel, ha a szorzatuk pozitív: $aRb \iff ab > 0$. Belátjuk, hogy R ekvivalenciareláció és meghatározzuk az ekvivalenciaosztályokat.

Megoldás: Reflexivitás: $a \cdot a = a^2 > 0$. Szimmetria: $ab = ba$, ezért $ab > 0 \Rightarrow ba > 0$. Tranzitivitás: Az $ab > 0$ és $bc > 0$ egyenlőtlenségeket összeszorozva kapjuk, hogy $acb^2 > 0$. Ezt $b^2 > 0$-val elosztva adódik a kívánt $ac > 0$.

Két ekvivalenciaosztály keletkezik, a pozitív és a negatív számok halmaza.

Feladatok

A.1.1 Igazoljuk az egyenlőségeket minden $n > 0$ egész számra.

(a) $\dfrac{1}{1\cdot 2} + \dfrac{1}{2\cdot 3} + \ldots + \dfrac{1}{n(n+1)} = \dfrac{n}{n+1}$.

(b) $1^2 + 2^2 + 3^2 + \ldots + n^2 = n(n+1)(2n+1)/6$.

A.1.2 Lássuk be az egyenlőtlenségeket minden $n > 0$ egész számra.

$$2\sqrt{n+1} - 2 < 1 + \frac{1}{\sqrt{2}} + \frac{1}{\sqrt{3}} + \ldots + \frac{1}{\sqrt{n}} \leq 2\sqrt{n} - 1.$$

A.1.3 Mutassuk meg, hogy $8 \mid 5^n + 4n + 7$ minden $n \geq 0$ egész számra.

A.1.4 Legyen $a_0 = 0$, $a_1 = 1$ és $a_{n+1} = 3a_n - 2a_{n-1}$, ha $n \geq 1$. Adjuk meg a_n-et explicit alakban.

A.1.5 „Belátjuk", hogy az összes valós szám egyenlő. Teljes indukcióval igazoljuk, hogy bármely n darab valós szám egyenlő. Ez nyilván teljesül $n = 1$-re. Feltesszük ennek igazságát $n-1$-re, és továbblépünk n-re. Legyenek $a_1, a_2, \ldots, a_n$ tetszőleges valós számok. Az indukciós feltevés szerint $a_1 = a_2 = \ldots = a_{n-1}$ és $a_2 = a_3 = \ldots = a_n$. Mivel a_{n-1} mindkétszer előfordul, ezért $a_1 = a_2 = \ldots = a_n$. Hol a hiba az okoskodásban?

A.1.6 Hányféleképpen írható fel a 2000 négy pozitív egész összegeként, ha a csak a tagok sorrendjében eltérő előállításokat is különbözőknek tekintjük?

A.1.7 Lássuk be:

(a) $\binom{n}{k} = \binom{n}{n-k}$;

(b) $\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k}$;

(c) $\binom{k}{k} + \binom{k+1}{k} + \ldots + \binom{n}{k} = \binom{n+1}{k+1}$;

(d) $\binom{n}{0}^2 + \binom{n}{1}^2 + \ldots + \binom{n}{n}^2 = \binom{2n}{n}$.

A.1.8 Adjuk meg az összegeket explicit alakban:

(a) $\binom{n}{0} + \binom{n}{2} + \binom{n}{4} + \binom{n}{6} + \ldots$;

(b) $\binom{n}{0} - 2\binom{n}{1} + 4\binom{n}{2} - 8\binom{n}{3} + \ldots$.

A.1.9

(a) Hány k-jegyű számot készíthetünk az $1, 2, \ldots, n$ számjegyekből úgy, hogy mind az n számjegy szerepeljen, ha (a1) $k < n$; (a2) $k = n$; (a3) $k > n$?

(b) Bizonyítsuk be:

$$n^k - n(n-1)^k + \binom{n}{2}(n-2)^k - \ldots$$
$$+(-1)^{n-2}\binom{n}{n-2}2^k + (-1)^{n-1}\binom{n}{n-1} = \begin{cases} 0, & \text{if } k < n; \\ n!, & \text{if } k = n. \end{cases}$$

A.1.10 Válasszuk ki az ekvivalenciarelációkat az alábbi, az egész számok halmazán definiált relációk közül, és adjuk meg az általuk indukált ekvivalenciaosztályokat.

(a) $aRb \iff 3 \mid a+b$;
(b) $aRb \iff 3 \mid a-b$;
(c) $aRb \iff 3 \mid 4a+5b$;
(d) $aRb \iff a^2 = b^2$;
(e) $aRb \iff ab \geq 0$;
(f) $aRb \iff |a-b| < 1000$.

A.1.11 Az alábbi gondolatmenet azt próbálja igazolni, hogy ha egy reláció szimmetrikus és tranzitív, akkor reflexív is. Legyen $a \in H$, és válasszunk olyan $b \in H$ elemet, amellyel aRb. Ekkor a szimmetria miatt bRa, és tranzitivitás miatt a kettőből aRa következik. Helyes ez a levezetés?

A.1.12 Egy n elemű halmazon hány (a) reláció; (b) reflexív reláció; (c) szimmetrikus reláció értelmezhető?

A.2. Oszthatóság és kongruenciák

Ebben a pontban minden betű egész számot jelöl. Először az oszthatóságra vonatkozó alapismereteket foglaljuk össze.

A.2.1 Definíció

Az a *osztó*ja b-nek, ha alkalmas c-vel $ac = b$ teljeül. Jelölés: $a \mid b$.

Az a és b *legnagyobb közös osztó*ja az a legnagyobb egész szám, amelynek a és b is többszöröse. Jelölés: (a, b) vagy lnko(a, b).

Két egész szám *relatív prím*, ha az lnko-juk 1.

A $p \neq \pm 1$ egész *felbonthatatlan*, ha nincs más osztója, mint ± 1 és $\pm p$. ♣

„Felbonthatatlan szám" helyett általában a „prím" vagy „prímszám" kifejezést használjuk, lásd alább.

A.2.2 Tétel

Maradékos osztás: Bármely $b \neq 0$ and a esetén pontosan egy olyan q és r létezik, amelyek $a = bq + r$ és $0 \leq r < |b|$.

A számelmélet alaptétele: Minden $c \neq 0, \pm 1$ felírható felbonthatatlan számok szorzataként, és ez a felírás a tényezők előjelétől és sorrendjétől eltekintve egyértelmű.

Kanonikus alak: Ha $n > 1$, akkor $n = p_1^{k_1} \dots p_r^{k_r}$ ahol a $p_j > 0$ pozitív prímszámok különbözők és $k_j > 0$. ♣

Az *euklideszi algoritmus* maradékos osztások sorozata:

$$a = bq_1 + r_1, \;\; b = r_1 q_2 + r_2, \;\; r_1 = r_2 q_3 + r_3, \;\; \dots .$$

Az utolsó nem nulla maradék az a és b lnko-ja. Ez gyors eljárás nagy számok lnko-jának a meghatározására. Emellett több fontos elméleti következménye van: (i) Az lnko nemcsak a legnagyobb a közös osztók között, hanem mindegyik közös osztónak többszöröse is. (ii) Ha $(a, b) = d$, akkor $d = au + bv$ alkalmas u és v egészekkel. (iii) Egy 0-tól és ± 1-től különböző egész akkor és csak akkor felbonthatatlan, ha rendelkezik a *prím*tulajdonsággal: csak úgy lehet osztója egy szorzatnak, ha legalább az egyik tényezőt osztja. Ezért a "prím" és "felbonthatatlan" ekvivalensek az egész számok körében. Ez a kulcslépés a számelmélet alaptételének a bizonyításában.

A következőkben néhány gyakran előforduló hiba elkerülésére hívjuk fel a figyelmet:

(A) Ha $a \mid bc$ és $a \not\mid b$, ebből **NEM** következik $a \mid c$, például $15 \mid 3 \cdot 20$, de $15 \not\mid 3$ és $15 \not\mid 20$.

Helyes következtetések:

(i) $a \mid bc,\ (a,b) = 1 \Rightarrow a \mid c$.

(ii) Ha a prímszám, akkor $a \mid bc,\ a \not\mid b \Rightarrow a \mid c$.

(B) Ha $a \mid c$ és $b \mid c$, ebből **NEM** következik $ab \mid c$, például $6 \mid 12$, $4 \mid 12$, de $24 \not\mid 12$.

Helyes következtetések:

(i) Ha $a \mid c,\ b \mid c$ és $(a,b) = 1$, akkor $ab \mid c$.

(ii) $a \mid c$ and $b \mid c \Rightarrow [a,b] \mid c$ (ahol $[a,b]$ az a és b legkisebb közös többszöröse).

A fenti tulajdonságok levezethetők például a számelmélet alaptételéből.

Most rátérünk a kongruenciákkal kapcsolatos alapismeretekre.

A.2.3 Definíció

Ha $m \mid a - b$ ahol $m > 0$, azaz a és b ugyanazt a maradékot adják m-mel osztva, akkor azt mondjuk, hogy „a kongruens b-vel modulo m”. Jelölés: $a \equiv b \pmod{m}$. Az m egész szám a kongruencia *modulus*a. ♣

A kongruenciareláció számos hasonló tulajdonsággal rendelkezik, mint az egyenlőség. Reflexív, szimmetrikus és tranzitív: bármely a, b, c esetén

$$a \equiv a; \qquad a \equiv b \Rightarrow b \equiv a; \qquad (a \equiv b \text{ and } b \equiv c) \Rightarrow a \equiv c \pmod{m}.$$

A kongruencia tehát ekvivalenciareláció (lásd az A.1.3 Definíciót). Egy-egy ekvivalenciaosztályba (lásd az A.1.4 Tételnél) azok az egész számok tartoznak, amelyek ugyanazt a maradékot adják m-mel osztva. Egy ilyen osztályt mod(ulo) m *maradékosztály*nak nevezünk. Például a $\{\ldots, -3, 7, 17, 27, \ldots\}$ halmaz egy mod 10 maradékosztály.

Kongruencuákat összeadhatunk, kivonhatunk és összeszorozhatunk:

$$a \equiv b \text{ and } c \equiv d \Rightarrow a + c \equiv b + d,\ a - c \equiv b - d,\ ac \equiv bd \pmod{m}.$$

Ezek ismételt alkalmazásával kapjuk, hogy $a \equiv b \Rightarrow a^t \equiv b^t \pmod{m}$ bármely $t > 0$ egészre, sőt $a \equiv b \Rightarrow f(a) \equiv f(b) \pmod{m}$ bármely f egész együtthatós polinomra.

Vigyáznunk kell az osztással: akkor sem szabad a kongruenciákat elosztani, ha a keletkező hányadosok egész számok. Például

$$24 \equiv 14 \pmod{10} \text{ and } 2 \equiv 2 \pmod{10}, \text{ de } 24/2 = 12 \not\equiv 14/2 = 7 \pmod{10}.$$

Helyes következtetések:

(i) $ac \equiv bc \pmod m$ és $(c,m)=1 \Rightarrow a \equiv b \pmod m$.

(ii) $ac \equiv bc \pmod m \Rightarrow a \equiv b \pmod{m/(c,m)}$.

Az Euler-féle φ-függvény központi szereoet játszik a számelméletben:

A.2.4 Definíció

$\varphi(n)$ az $1,2,\dots,n$ egészek közül az n-hez relatív prímek száma. ♣

A.2.5 Tétel

Ha az n kanonikus alapkja $n = p_1^{k_1}\dots p_r^{k_r}$ ahol a $p_j > 0$ számok különböző prímek és $k_j > 0$, akkor $\varphi(n) = p_1^{k_1-1}(p_1-1)\dots p_r^{k_r-1}(p_r-1)$. ♣

A.2.6 Tétel (Euler–Fermat-tétel)

$(c,m)=1 \Rightarrow c^{\varphi(m)} \equiv 1 \pmod m$. ♣

Ennek fontos speciális esete:

A.2.6A Tétel (Kis Fermat-tétel)

Ha p prím és $p \nmid c$, akkor $c^{p-1} \equiv 1 \pmod p$.

Ennek egy másik alakja: $c^p \equiv c \pmod p$ minden c-re teljesül. ♣

A.2.7 Definíció

Legyen $(c,m)=1$. A c *rend*je modulo m a legkisebb olyan $k>0$ kitevő, amelyre $c^k \equiv 1 \pmod m$. Ezt $o_m(c)$ jelöli, illetve $o(c)$, ha egyértelmű, melyik m modulusról van szó. ♣

A rend a legkisebb periódus, amely szerint a c hatványai ismétlődnek modulo m: $c^r \equiv c^s \pmod m \iff r \equiv s \pmod{o_c(m)}$. Az $s=0$ esetben kapjuk, hogy $c^r \equiv 1 \pmod m \iff o_m(c) \mid r$. Ebből az A.2.6 Tétel alapján $o_m(c) \mid \varphi(m)$ következik.

A kongruenciáknál imént definiált rend speciális esete a csoportbeli elemrend fogalomnak, lásd az A.8.2 Definíciót.

Az $Ax+By=C$ kétváltozós *lineáris diofantikus egyenlet*nél A,B,C adott egészek, A és B nem mindkettő nulla, és az x,y megoldásokat az egészek körében keressük.

A.2.8 Tétel

(i) Az $Ax + By = C$ lineáris diofantikus egyenlet akkor és csak akkor oldható meg, ha $(A, B) \mid C$. Ebben az esetben a megoldások száma végtelen.

(ii) Az euklideszi algoritmusból nyerhető egy (x_0, y_0) megoldás, és ebből az összes megoldás

$$x_t = x_0 + \frac{tB}{(A,B)}, \quad y_t = y_0 - \frac{tA}{(A,B)}, \quad t = 0, \pm 1, \pm 2, \ldots . \quad \clubsuit$$

Az $ax \equiv b \pmod{m}$ *lineáris kongruencia* esetén páronként inkongruens x megoldásokat keresünk.

A.2.9 Tétel

Az $ax \equiv b \pmod{m}$ lineáris kongruencia akkor és csak akkor oldható meg, ha $(a, m) \mid b$. Ekkor a páronként inkongruens megoldások száma (a, m). $\clubsuit$

Az $Ax+By = C$ egyenlet átalakítható az $Ax \equiv C \pmod{|B|}$ vagy $By \equiv C \pmod{|A|}$ kongruenciává (ha B, illetve A nem nulla). Megfordítva, az $ax \equiv b \pmod{m}$ kongruencia átalakítható az $ax - my = b$ egyenletté.

A szimultán kongruenciarendszer azt jelenti, hogy egyszerre több modulusra vonatkozó feltételeket szabunk ugyanarra az ismeretlenre.

A.2.10 Tétel Az $x \equiv c_1 \pmod{m_1}$, $x \equiv c_2 \pmod{m_2}$ szimultán kongruenciarendszer akkor és csak akkor oldható meg, ha $(m_1, m_2) \mid c_1 - c_2$. Megoldhatóság esetén egyetlen megoldás van mod $[m_1, m_2]$. $\clubsuit$

Speciálisan, ha m_1 és m_2 relatív prímek, akkor a rendszer bármely c_1 és c_2 mellett megoldható, és egyetlen megoldás van mod $m_1 m_2$. Ennek több modulusra vonatkozó általánosítása az

A.2.10A Tétel (Kínai maradéktétel)

Legyenek $m_1, \ldots, m_r$ páronként relatív prímek. Ekkor az $x \equiv c_i \pmod{m_i}$, $i = 1, 2, \ldots, r$ szimultán kongruenciarendszer bármely $c_1, \ldots, c_r$ esetén megoldható és egyetlen megoldás van mod $m_1 m_2 \ldots m_r$. $\clubsuit$

Az A.2.10A Tétel fontos következménye, hogy egy összetett modulusú kongruencia visszavezethető prímhatvány modulusú kongruenciákra: Ha az m kanonikus alakja $m = p_1^{\alpha_1} \ldots p_r^{\alpha_r}$, akkor az $f(x) \equiv 0 \pmod{m}$ kongruencia ekvivalens az $f(x) \equiv 0 \pmod{p_i^{\alpha_1}}$, $i = 1, 2, \ldots, r$ kongruenciarendszerrel.

Feladatok

A.2.1 Igazoljuk, hogy két páratlan négyzetszám különbsége mindig osztható 8-cal.

A.2.2 Melyek igazak az alábbi állítások közül?
(a) $(a \mid b \text{ and } a \mid c) \Longrightarrow a \mid 3b - 5c$;
(b) $a \mid b + c \Longrightarrow (a \mid b \text{ and } a \mid c)$;
(c) $ab \mid c \Longrightarrow (a \mid c \text{ and } b \mid c)$;
(d) $(a \mid c \text{ and } b \mid c) \Longrightarrow ab \mid c$;
(e) $(a \mid b \text{ or } a \mid c) \Longrightarrow a \mid bc$;
(f) $a \mid bc \Longrightarrow (a \mid b \text{ or } a \mid c)$;
(g) $(a \mid b + c \text{ and } a \mid b - c) \Longrightarrow (a \mid b \text{ and } a \mid c)$;
(h) $(a \mid 2b + 3c \text{ and } a \mid 3b + 5c) \Longrightarrow (a \mid b \text{ and } a \mid c)$.

A.2.3 Lássuk be az alábbi oszthatóságokat:
(i) $a - b \mid a^n - b^n$; (ii) $a + b \mid a^{2k+1} + b^{2k+1}$; (iii) $a + b \mid a^{2k} - b^{2k}$.

A.2.4 (A számjegyek tízes számrendszerben értendők.)
(a) Igazoljuk, hogy n akkor és csak akkor osztható 9-cel, ha a számjegyeinek az összege osztható 9-cel.
(b) Igazoljuk, hogy n akkor és csak akkor osztható 11-gyel, ha a számjegyeinek váltakozó előjellel vett összege osztható 11-gyel.
(c) Összeadtuk 2^{2000} számjegyeit, majd összeadtuk az így keletkezett szám számjegyeit stb., amíg végül egyjegyű számot kaptunk. Melyik ez az egyjegyű szám?
(d) Lássuk be, hogy bármely $n \geq 0$-ra $43 \mid 6^{n+2} + 7^{2n+1}$.

A.2.5 Melyek igazak az alábbi állítások közül? ($[k, n]$ a k és n legkisebb közös többszörösét jelöli.)
(a) $k \mid n,\ a \equiv b \pmod{n} \Longrightarrow a \equiv b \pmod{k}$;
(b) $k \mid n,\ a \equiv b \pmod{k} \Longrightarrow a \equiv b \pmod{n}$;
(c) $a \equiv b \pmod{n}$, $a \equiv b \pmod{k} \iff a \equiv b \pmod{kn}$;
(d) $a \equiv b \pmod{n}$, $a \equiv b \pmod{k} \iff a \equiv b \pmod{[k, n]}$;
(e) $a \equiv b \pmod{n} \iff ka \equiv kb \pmod{kn}$;
(f) $a \equiv b \pmod{n}$, $c \equiv d \pmod{k} \Longrightarrow ac \equiv bd \pmod{kn}$;
(g) $a^2 \equiv b^2 \pmod{n} \Longrightarrow a \equiv \pm b \pmod{n}$;
(h) $a^2 \equiv b^2 \pmod{101} \Longrightarrow a \equiv \pm b \pmod{101}$.

A.2.6 Tekintsünk egy egészekből álló tetszőleges $a_1, a_2, a_3, \ldots$ sorozatot. Bizonyítsuk be, hogy van végtelen sok olyan a_i, amelyek közül bármelyik kettőnek a különbsége osztható 11111-gyel.

A.2.7 Vegyük egész számok olyan maximális halmazát, amelyek mind különböző maradékot adnak n-nel osztva. Mi a maradéka ezek összegének?

A.2.8 Egy futóversenyen az n induló mindegyikénél összeadtuk a rajtszámot az elért helyezéssel (tehát ha például a 7-es rajtszámú futó második lett, akkor a $7 + 2 = 9$ összeget vettük). Észrevettük, hogy az így kapott n összeg csupa különböző maradékot ad n-nel osztva. Lehetséges-e ez, ha n értéke (a) 99; (b) 100?

A.2.9.

(a) Egy kör alakú tisztás mentén m fa áll, mindegyiken egy-egy mókus. A mókusok össze szeretnének gyűlni egy fán, de csak úgy változtathatják a helyüket, hogy két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára. Ezt a lépést akárhányszor ismételhetik. Milyen m esetén tudnak összegyűlni a mókusok?

(b) Mi a helyzet akkor, ha a megengedett lépést a következőképpen módosítjuk: két tetszőleges mókus egyidejűleg átugorhat egy-egy szomszédos fára, azonban ellenkező körüljárási irányba kell ugorniuk.

A.2.10

(a) Igazoljuk az A.2.5 Tételben a $\varphi(n)$-re adott képletet, ha n (prím vagy) prímhatvány.

(b) Mely n egészekre lesz $\varphi(n)$ (b1) páratlan; (b2) kettőhatvány?

A.2.11 Mi 1357^{8642} utolsó két jegye?

A.2.12 Bizonyítsuk be, hogy egy négyzetszám plusz 1 alakú számnak nem lehet $4k - 1$ alakú prímosztója.

A.2.13 Oldjuk meg a $8x \equiv 13 \pmod{11}$ kongruenciát.

A.2.14 Határozzuk meg 614^{4302} utolsó három számjegyét.

A.2.15 Hány 21-jegyű pozitív egésznek végződik minden hatványa ugyanarra a 20 számjegyre, mint az eredeti szám?

A.2.16 Bizonyítsuk be az A.2.8–A.2.10 tételeket.

A.3. Komplex számok

A komplex számokat eredetileg a harmadfokú egyenletnél tapasztalt paradox helyzet feloldására találták ki: a négyzetgyök alatt fellépő negatív számok

miatt a Cardano-képlet éppen abban az esetben mondott csődöt, amikor az egyenletnek három különböző valós gyöke van. Később kiderült, hogy a komplex számok a valós számok természetes kiterjesztései, és alapvető szerepet játszanak a matematika szinte minden ágán túl például a modern fizikában is.

A.3.1 Definíció

A komplex számok a $z = a+bi$ alakú kifejezések, ahol a és b valós számok és $i^2 = -1$. Az $a = \operatorname{Re} z$ és $b = \operatorname{Im} z$ (az i nélkül!) valós számokat a z komplex szám valós, illetve képzetes (vagy imaginárius) részének nevezzük. Egy komplex szám tiszta képzetes, ha a valós része 0.

A komplex számok összeadását és szorzását természetes módon definiáljuk:

$$(a+bi)+(c+di) = (a+c)+(b+d)i \quad \text{és} \quad (a+bi)(c+di) = (ac-bd)+(ad+bc)i.$$

Tehát a szorzásnál $a+bi$ mindkét tagját $c+di$ mindkét tagjával beszorozzuk, és az $i^2 = -1$ szabályt alkalmazzuk. ♣

A komplex számokat auonosíthatjuk a sík pontjaival: $z = a + bi$ az a és b koordinátájú pontnak felel meg. A komplex számokat az origóból induló helyvektorokkal is jellemezhetjük. Ekkor a komplex számok összeadása a megfelelő vektorok összeadását jelenti.

A.3.2 Definíció

Tekintsük a $z = a + bi$ komplex számot.

A z *konjugált*ja $\overline{z} = a - bi$, *abszolút érték*e $|z| = \sqrt{a^2 + b^2}$.

A $z \neq 0$ szöge *argumentum*a, *arkusz*a, $\arg(z)$ egy irányított szög (forgásszög), amely az x-tengely pozitív felét a z vektorra forgatja. Ez aszerint pozitív vagy negatív, hogy a forgatás az órmutató járásával ellentétes vagy azzal megegyező irányban történt. Egy nem nulla komplex számnak végtelen sok szöge van, ezek egymástól (radiánban mérve) 2π egész számú többszörösével térnek el egymástól. ♣

Például $\overline{-1+i} = -1-i$, $|-1+i| = \sqrt{2}$, $\arg(-1+i) = 3\pi/4$ (vagy $-5\pi/4$ stb.).

A $\overline{z}$ konjugált a z-nek a valós tengelyre vonatkozó tükörképe. Egyszerű számolással adódik $\overline{z+w} = \overline{z} + \overline{w}$, és hasonló érvényes a szorzásra, kivonásra és osztásra is.

A $|z|$ geometriai jelentése a z vektor hossza. A konjugáltat az abszolút értékkel a gyakran jól használható $|z|^2 = z \cdot \overline{z}$ azonosság kapcsolja össze.

A komplex számok összeadása és szorzása a valós vagy racionális számoknál megszokott tulajdonságokkal rendelkezik:

A.3.3 Tétel
A komplex számok testet alkotnak: a szorzás és összeadás asszociatív és kommutatív; a szorzás az összeadásra nézve disztributív; a 0 és az 1 az összeadás és szorzás egységeleme; létezik minden elemnek negatívja és minden nem nulla elemnek reciproka. ♣

A 0, 1, negatívok és reciprokok létezése ekvivalens a kivonás és osztás elvégezhetőségével. A fentieket tehát úgy foglalhatjuk össze, hogy a komplex számok körében elvégezhető a négy alapművelet és érvényesek a szokásos műveleti azonosságok.

Osztani legkényelmesebben a konjugált segítségével tudunk: ha $a+bi \neq 0$, akkor

$$\frac{c+di}{a+bi} = \frac{(c+di)(a-bi)}{(a+bi)(a-bi)} = \frac{(ac+bd)+(ad-bc)i}{a^2+b^2} = \frac{ac+bd}{a^2+b^2} + \frac{ad-bc}{a^2+b^2}\,i\,.$$

Egy komplex szám jellemezhető az abszolút értékével és a szögével is:

A.3.4 Tétel
Ha a $z \neq 0$ komplex szám szöge $\arg(z) = \varphi$, akkor $z = |z|(\cos\varphi + i\sin\varphi)$.
Komplex számok szorzásánál és osztásánál az abszolút értékek szorzódnak, illetve osztdnak, a szögek pedig összeadódnak, illetve kivonódnak. ♣

A z komplex számnak $a+bi$ az *algebrai* alakja, $|z|(\cos\varphi + i\sin\varphi)$ pedig a *trigonometrikus* alakja. Mivel a szögek úgy viselkednek, mint a kitevők, gyakran használjuk a $z = |z|e^{i\varphi}$ Euler-féle alakot is, ami a szorzásnak és az osztásnak természetes keretet ad. Ez az alak valójában nemcsak egy praktikus jelölés, hanem mélyebb komplex függvénytani megfontolások egyenes következménye.
Például $1 - i\sqrt{3} = 2(\cos(-\pi/3) + i\sin(-\pi/3) = 2e^{-i\pi/3}$.

Komplex számok egész kitevős hatványait a valós számoknál megszokott módon definiáljuk: Ha n pozitív egész, akkor

$$z^n = \underbrace{z\cdot\ldots\cdot z}_{n-\text{szer}}, \quad z^0 = 1 \quad \text{és} \quad z^{-n} = \frac{1}{z^n}, \text{ ha } z \neq 0.$$

Az A.3.4 Tétel második állításából azonnal következik a Moivre-formula: ha $z \neq 0$, akkor bármely k egészre

$$z^k = |z|^k(\cos(k\varphi) + i\sin(k\varphi)) = |z|^k e^{ik\varphi}.$$

Ha $n > 0$, akkor a z komplex szám *n-edik gyök*én az *összes* olyan $w = \sqrt[n]{z}$ komplex számot értjük, amelyre $w^n = z$. A $z = 0$-nak nyilván $w = 0$ az egyetlen n-edik gyöke. Ha $z \neq 0$, akkor z-nek pontosan n különböző n-edik gyöke van:

A.3.5 Tétel

Ha $z \neq 0$ és $\arg(z) = \varphi$, akkor

$$\sqrt[n]{z} = \sqrt[n]{|z|}(\cos\frac{\varphi + 2k\pi}{n} + i\sin\frac{\varphi + 2k\pi}{n}) = \sqrt[n]{|z|}e^{i(\varphi+2k\pi)/n},\ 0 \leq k \leq n-1.$$

Az n-edik gyökök tehát egy origó középpontú szabályos n-szög csúcsai. ♣

Az 1 komplex szám n-edik gyökei az n-edik *egységgyök*ök:

A.3.6 Definíció

Egy w komplex szám egységgyök, ha alkalmas $n > 0$ egészre $w^n = 1$. Ebben az esetben w-t n-edik egységgyöknek nevezzük.

A w komplex egységgyök *rend*je, $o(w)$ a legkisebb t pozitív egész kitevő, amelyre $w^t = 1$.

w *primitív* n-edik egységgyök, ha $o(w) = n$. ♣

Például $o(i) = 4$, tehát i primitív 4-edik egységgyök, továbbá 8-adik, 12-edik stb. (nem primitív) egységgyök is.

A rend hasonló a kongruenciáknál definiált rendhez, és mindkettő speciális esete egy csoportelem rendjének, lásd az A.8.2 Definíciót.

A.3.7 Tétel

Az n-edik egységgyökök $w_k = \cos(2k\pi/n) + i\sin(2k\pi/n) = e^{2\pi ki/n}$, $k = 0, 1, \ldots, n-1$.

w_k akkor és csak akkor promitív n-edik egységgyök, ha $(k, n) = 1$. A primitív n-edik egységgyökök száma tehát $\varphi(n)$ (ahol φ az Euler-féle φ-függvény, lásd az A.2.4 Definíciót).

Egy w komplex szám akkor és csak akkor egységgyök, ha az abszolút értéke 1 és a szöge a 2π-nek racionális többszöröse. Ha ez a racionális szorzó r/s, ahol $(r, s) = 1$ és $s > 0$, akkor $o(w) = s$.

Ha w egységgyök, akkor $w^t = w^m \iff t \equiv m \pmod{o(w)}$. Speciálisan $w^t = 1 \iff o(w) \mid t$. ♣

Feladatok

A.3.1 Számítsuk ki:

(a) $\dfrac{7+6i}{2+i} - \dfrac{5+i}{2+3i}$;

(b) i^{9999}

(c) $\sqrt{5-12i}$;

(d) $\sqrt[6]{8i}$;

(e) $\sqrt[5]{-3-i\sqrt{3}}$.

A.3.2 Adjuk meg a síkon azon pontok halmazát, amelyeknek megfelelő z komplex számokra

(a) $\operatorname{Im}(3i-5z)=7$;

(b) $\operatorname{Re}(2iz+5+8i)>9$;

(c) $|z-3+8i|\le 1$;

(d) $|z|=2\operatorname{Im} z$;

(e) $|z-5i|\ge|z+i|$;

(f) $(1+i)\overline{z}=z\sqrt{2}$;

(g) $(z+1)/(z+3)$ is imaginary.

A.3.3 Oldjuk meg az egyenleteket a komplex számok körében:

(a) $z^2+8=0$; (b) $z^2+2z+2=0$; (c) $z^2+(1+i)z+5i=0$.

A.3.4 Igazoljuk, hogy $|z_1+z_2|^2+|z_1-z_2|^2=2|z_1|^2+2|z_2|^2$ bármely z_1 és z_2 komplex számra teljesül. Mi ennek a geometriai jelentése?

A.3.5 Lássuk be, hogy ha két pozitív egész mindegyike két négyzetszám összege, akkor ez a szorzatukra is érvényes. Igaz-e a megfordítás? És mi a helyzet három négyzetszám összegére?

A.3.6 Hová kerül a $(3,4)$ pont az origó körüli (a) 90; (b) 60 fokos elforgatásnál?

A.3.7 Tegyük fel, hogy $z_1\ne z_2$. Lássuk be, hogy $(z_1+z_2)/(z_1-z_2)$ akkor és csak akkor tiszta képzetes, ha $|z_1|=|z_2|$.

A.3.8 Írjuk fel $\sin 5x$-et a $\sin x$ hatványainak a segítségével.

A.3.9

(a) Számítsuk ki $(1+i)^n$-et kétféleképpen: a trigonometrikus alakból, illetve a binomiális tétel alapján.

(b) Határozzuk meg az $\binom{n}{0}-\binom{n}{2}+\binom{n}{4}-\binom{n}{6}+\dots$ összeget.

A.3.10 Adjuk meg az összes (a) harmadik; (b) hatodik egységgyököt algebrai alakban.

A.3.11
(a) Mutassuk meg, hogy két egységgyök szorzata és hányadosa is egységgyök.
(b) Mely esetekben lesz két egységgyök összege vagy különbsége egységgyök?

A.3.12 Számítsuk ki az összes n-edik egységgyök összegét és szorzatát.

A.3.13 Legyen $o(z) = k$ és $o(w) = n$.
(a) Számítsuk ki $o(z^t)$ értékét.
(b) Mutassuk meg, hogy $o(zw) \mid [k, n]$.

A.3.14
(a) Számítsuk ki az összes primitív n-edik egységgyök szorzatát.
M (b) Határozzuk meg az összes primitív n-edik egységgyök összegét, ha $n = 7$, 27, illetve (**) tetszőleges pozitív egész.

A.3.15 Egy négyszög minden oldalára kifelé egy-egy négyzetet rajzolunk. Bizonyítsuk be, hogy a szemköztes négyzetek középpontjait összekötő szakaszok egyenlő hosszúak és merőlegesek egymásra.

M A.3.16 Adjuk meg a $\cos x + \cos(2x) + \ldots + \cos(nx)$ összeget egyszerűbb alakban.

A.4. Művelet

A.4.1 Definíció

Egy H nem üres halmazon értelmezett (kétváltozós) *művelet*en egy $H \times H \to H$ függvényt értünk, azaz egy olyan leképezést, amely bármely $a, b \in H$ elempárhoz egyértelműen hozzárendel egy H-beli elemet. ♣

A műveletet a legtöbbször szorzásnak nevezzük és az $a, b \in H$ elempárhoz hozzárendelt elemet ab-vel jelöljük. Összeadás esetén a jelölés $a + b$, további lehetséges jelölések $a * b$, $a \circ b$, $f(a, b)$ stb.

Példák műveletre

P1. A természetes, az egész, a racionális, a valós vagy a komplex számok körében az összeadás, illetve a szorzás.

P2. Az egész, a racionális, a valós vagy a komplex számok körében a kivonás. A természetes számok körében a kivonás nem művelet, hiszen pl. a $3 - 5$

különbség „nem létezik” (ugyanis nincs olyan m *természetes* szám, amelyre $m + 5 = 3$ teljesülne).

P3. A nem nulla racionális, valós vagy komplex számok körében az osztás.

P4. A modulo m maradékosztályok körében az összeadás, a kivonás és a szorzás.

P5. Az azonos alakú mátrixok körében az összeadás, a(z adott méretű) négyzetes mátrixok körében a szorzás.

P6. Az $\mathbf{R} \to \mathbf{R}$ vagy általánosan az $X \to X$ függvények körében a kompozíció (vagy függvényösszetétel, azaz a függvények egymás után alkalmazása).

P7. A sík egybevágósági (azaz távolságtartó) transzformációi körében a kompozíció.

P8. A térvektorok körében a vektoriális szorzat. Nem művelet azonban (az A.1.1 Definíció szerinti értelemben) a vektorok skalárszorzata (hiszen az eredmény nem vektor, hanem skalár), illetve a vektornak skalárral való szorzása (hiszen ekkor nem ugyanabból a halmazból vesszük a két elemet). Megfelelő általánosabb értelmezéssel azonban ezeket a (fontos) leképezéseket is besorolhatjuk a műveletek közé.

Megjegyzés: Szokás azt mondani, hogy a H halmaz a rajta értelmezett műveletre nézve „zárt”. Ez nem túl szerencsés szóhasználat, hiszen a művelet definíciójában már benne van, hogy bármely két elemre „a művelet eredménye”, azaz a hozzájuk rendelt elem szintén a H halmazhoz tartozik. A „zártság” elnevezésnek akkor van létjogosultsága, ha egy H halmazon már adott egy művelet és azt vizsgáljuk, hogy H valamely K részhalmaza zárt-e erre a műveletre nézve, azaz két K-beli elemre a H-beli adott műveletet elvégezve az eredmény ismét K-beli elem lesz-e. Ebben az értelemben K zártsága pontosan azt jelenti, hogy a H-beli művelet (pontosabban annak a K-ra történő megszorítása) a K (rész)halmazon is egy műveletet definiál.

Az ún. *műveleti azonosság*ok közül a legfontosabb az asszociativitás és a kommutativitás.

A.4.2 Definíció

Egy H-n értelmezett művelet *asszociatív*, ha bármely $a, b, c \in H$-ra $a(bc) = (ab)c$ teljesül. ♣

A.4.3 Definíció

Egy H-n értelmezett művelet *kommutatív*, ha bármely $a, b \in H$-ra $ab = ba$ teljesül. ♣

Az asszociativitás biztosítja azt, hogy a többtényezős szorzatok (zárójelek használata nélkül is) egyértelműek. Ha a művelet emellett még kommutatív is, akkor a tényezők egymás közötti sorrendje is tetszőlegesen változtatható.

Példák: A számok (polinomok, maradékosztályok stb.) összeadása és szorzása kommutatív és asszociatív. A mátrixok szorzása vagy a függvények kompozíciója asszociatív, de (általában) nem kommutatív. A (pl. valós) számok körében a számtani közép képzése kommutatív, de nem asszociatív. A számok kivonása vagy a vektorok vektoriális szorzata se nem kommutatív, se nem asszociatív.

Megjegyzések: 1. Az asszociativitásnál nem azt kell ellenőrizni, hogy $a(bc)$, illetve $(ab)c$ a H halmaz eleme, hiszen ez a művelet definíciójából következik. Most azt kell megvizsgálni, hogy ez a két elem **minden** esetben megegyezik-e.

2. Nincs értelme annak, hogy egy művelet „részben kommutatív/asszociatív". Ha van olyan a, b elempár, amelyre $ab \neq ba$, akkor a művelet *nem* kommutatív, ellenkező esetben pedig kommutatív. Természetesen, ha egy művelet nem kommutatív, attól még lehet (akár sok) olyan a, b elempár, amelyek *felcserélhető*k, azaz amelyekre $ab = ba$.

3. A számok összeadásánál és szorzásánál szerzett tapasztalatok alapján sokan úgy gondolhatják, hogy egy „normális" műveletnél az asszociativitás és a kommutativitás egyformán fontosak vagy pedig kettejük közül a kommutativitás az előbbre való. A valóságban azonban éppen fordított a helyzet, és inkább az asszociativitást kell hasznosabbnak tekintenünk. Ugyanis egyrészt sok olyan fontos művelet van, amely asszociatív, de nem kommutatív — gondoljunk pl. a matematika szinte valamennyi területén nélkülözhetetlen kompozícióra, másrészt számos alapvető műveleti tulajdonság éppen az asszociativitáson múlik — ilyen pl. egy elem inverzének az egyértelműsége (lásd az A.4.5 Definíció után) vagy az elemek inverze és az inverz művelet közötti kapcsolat (A.4.7 Tétel).

A.4.4 Definíció

*Bal oldali egységelem*nek egy olyan $e_B \in H$ elemet nevezünk, amelyre *minden* $a \in H$-val $e_B a = a$ teljesül.

Az e_J *jobb oldali egységelem*et értelemszerűen az $ae_J = a$ azonossággal definiáljuk.

Végül az $e \in H$ elem *egységelem* (vagy *kétoldali egységelem*), ha mind bal, mind pedig jobb oldali egységelem, azaz minden $a \in H$-ra $ea = ae = a$. ♣

Az „egységelem” szó önmagában tehát mindig kétoldali egységelemet jelent.

Az összeadás esetén az egységelemet *nullelem*nek vagy *nulla*nak nevezzük és 0-val jelöljük. Szorzásnál az egységelemet gyakran (az e helyett) egyszerűen 1-gyel jelöljük.

FIGYELEM! A bal oldali egységelem definíciója NEM azt jelenti, hogy minden a elemhez található egy (a-tól függő) e_B elem, amelyre $e_B a = a$, hanem azt, hogy van egy olyan „univerzális” e_B elem, amely minden a-hoz egyszerre „jó”. (Ennek nem mond ellent az sem, hogy esetleg több ilyen „univerzális” elem is létezhet, lásd alább.)

Egy műveletnél több bal oldali egységelem is lehet: pl. ha bármely két elem „szorzata” a második, akkor minden elem bal oldali egységelem. Ha azonban van e_J jobb oldali egységelem is, akkor $e_J = e_B e_J = e_B$ miatt $e_B = e_J$, tehát ekkor csak egyetlen bal oldali egységelem lehet (amely így kétoldali egységelem). Ebből az is következik, hogy az egységelem *egyértelmű*, azaz (egy adott műveletnél) legfeljebb egy (kétoldali) egységelem létezik.

A.4.5 Definíció

Tekintsünk egy *egységelemes* műveletet, jelöljük a (kétoldali) egységelemet e-vel. (Az előző bekezdésből tudjuk, hogy ez az e egyértelmű.)

Az $a \in H$ elem *bal oldali inverz*én (vagy röviden *balinverz*én) egy olyan $a_B \in H$ elemet értünk, amelyre $a_B a = e$.

Az $a \in H$ elem *jobb oldali inverz*ének (vagy röviden *jobbinverz*ének) értelemszerűen egy olyan $a_J \in H$ elemet nevezünk, amelyre $a a_J = e$.

Végül az $a \in H$ elem *inverz*e (vagy *kétoldali inverze*) egy olyan $a^{-1} \in H$ elem, amely az a-nak mind bal, mind pedig jobb oldali inverze, azaz $a^{-1}a = a a^{-1} = e$. ♣

Az egységelemnél elmondottakhoz hasonlóan itt is érvényes, hogy ha az „inverze” szó elé a valamelyik oldalra utaló jelzőt nem tesszük ki, akkor ez automatikusan az elem kétoldali inverzét jelenti.

Ha a művelet az összeadás, akkor az a elem inverzét az a *ellentett*jének vagy *negatív*jának hívjuk és $-a$-val jelöljük. Ha a művelet számok szorzása, akkor az a elem inverzét szokás az a *reciprok*ának is nevezni és (a^{-1} helyett) $1/a$-val jelölni.

Ne felejtsük el, hogy egy elem (bal, jobb vagy kétoldali) inverzéről eleve csak akkor beszélhetünk, ha a művelet egységelemes.

A „balinverz”, „jobb oldali inverz”, „inverzelem” stb. szavakat *önmagukban* lehetőleg ne használjuk, mindig pontosan meg kell mondani, hogy melyik elem bal, jobb vagy kétoldali inverzéről van szó. Ugyanígy értelmetlen azt mondani,

hogy egy műveletnél „nincs inverz”, hiszen általában egyes elemeknek van, másoknak pedig nincs inverze. A szélső eseteket nézve, az megvalósulhat, hogy minden elemnek van inverze (pl. ha a pozitív valós számok körében vesszük a szorzást), az ellenkező véglet azonban (egységelemes műveletnél) lehetetlen, hiszen (legalábbis) az egységelemnek mindig van inverze.

Az egységelemnél látottakhoz hasonlóan előfordulhat, hogy egy elemnek több balinverze létezik (lásd az A.4.6 feladatot). Ha azonban a művelet *asszociatív* és a-nak létezik a_J jobbinverze is, akkor

$$a_B = a_B e = a_B(aa_J) = (a_B a)a_J = ea_J = a_J$$

miatt az a bal- és jobbinverze szükségképpen megegyezik. Ebben az esetben tehát az a-nak csak egyetlen balinverze lehet (amely így az a kétoldali inverze). Ebből az is következik, hogy asszociatív művelet esetén egy elem inverze *egyértelmű*, azaz bármely elemnek legfeljebb egy (kétoldali) inverze létezik.

Most az *inverz művelet* fogalmát tárgyaljuk. A (pl. valós) számok kivonásánál $a - b$ azt a c számot jelentette, amelyre $c + b = a$. A kivonás azért művelet (a valós számok halmazán), mert bármely a, b esetén pontosan egy ilyen c szám létezik. Ugyanakkor pl. a természetes számok halmazán a kivonás *nem* művelet, hiszen nem minden a, b esetén található megfelelő c. Az tehát, hogy a kivonás elvégezhető-e vagy sem, az a szóban forgó összeadástól függ, annak egy tulajdonsága. Mindezeket az alábbi definícióban általánosítjuk:

A.4.6 Definíció

Legyen adott a H halmazon egy (szorzásként jelölt) művelet. Tegyük fel, hogy az $xb = a$ egyenlet minden $a, b \in H$-ra egyértelműen megoldható, azaz pontosan egy olyan $c \in H$ létezik, amelyre $cb = a$. Ekkor a $B(a, b) = c$ hozzárendelést a művelet bal oldali *inverz művelet*ének nevezzük.

Hasonlóan, ha minden $a, b \in H$-ra pontosan egy olyan $d \in H$ létezik, amelyre $bd = a$, akkor a $J(a, b) = d$ hozzárendelés a művelet jobb oldali *inverz művelet*e. ♣

Az összeadás (bármelyik oldali) inverz művelete tehát a kivonás, a nem nulla (pl. valós) számok szorzásának az inverz művelete pedig az osztás. Ha a(z eredeti) művelet kommutatív, akkor nyilván mindig $B = J$.

Tudjuk, hogy a számok körében a kivonás visszavezethető az összeadásra és az ellentettre: $a - b = a + (-b)$. Egy elem inverzének és az inverz műveletnek a fogalma bármely asszociatív műveletnél hasonlóképpen szorosan kapcsolódik egymáshoz:

A.4.7 Tétel

Legyen értelmezve H-n egy *asszociatív* művelet.

I. Ha a művelet egységelemes és a b elemnek létezik a b^{-1} (kétoldali) inverze, akkor az $xb = a$ és $by = a$ egyenletek bármely $a \in H$ esetén egyértelműen megoldhatók.

II. Ha az $xb = a$ és $by = a$ egyenletek bármely $a, b \in H$ esetén megoldhatók, akkor létezik egységelem és minden elemnek létezik inverze. ♣

Bizonyítás: I. Ha b-nek létezik inverze, akkor egy egyenlőséget b^{-1}-gyel akármelyik oldalról megszorozva az eredetivel ekvivalens egyenlőséget kapunk. Ugyanis egyrészt nyilván $h_1 = h_2 \Rightarrow h_1 b^{-1} = h_2 b^{-1}$, másrészt ha $h_1 b^{-1} = h_2 b^{-1}$, akkor ezt b-vel jobbról megszorozva $(h_1 b^{-1})b = (h_2 b^{-1})b$ adódik, amiből $(hb^{-1})b = h(b^{-1}b) = he = h$ felhasználásával a kívánt $h_1 = h_2$ egyenlőséget nyerjük.

Ennek alapján az $xb = a$ egyenlet ekvivalens $x = ab^{-1}$-gyel, tehát az egyenlet egyértelműen megoldható. Ugyanígy, a $by = a$ egyenlet egyetlen megoldása $y = b^{-1}a$.

II. Jelöljük (valamelyik $b \in H$-ra) a $bx = b$ egyenlet (egyik) megoldását g-vel. Megmutatjuk, hogy ez a (b-től látszólag függő) g jobb oldali egységelem. Vegyünk egy tetszőleges $a \in H$ elemet. Ekkor a feltétel szerint van olyan c, amelyre $cb = a$ és így $ag = (cb)g = c(bg) = cb = a$, tehát g valóban jobb oldali egységelem. Ugyanígy kapjuk, hogy létezik egy h bal oldali egységelem is. Korábban már láttuk, hogy ekkor $g = h$, vagyis létezik (kétoldali) egységelem.

Ezután egy tetszőleges b elem bal-, illetve jobbinverzét az $xb = e$, illetve $by = e$ egyenletek megoldása adja (ahol e az egységelem), és láttuk, hogy egy elem bal- és jobbinverze szükségképpen egyenlő, tehát minden elemnek létezik (kétoldali) inverze. ■

Feladatok

A.4.1 Válasszuk ki az alábbi hozzárendelések közül a műveleteket, és vizsgáljuk meg, hogy melyek kommutatívak, illetve asszociatívak. Határozzuk meg a bal, illetve jobb oldali egységelem(ek)et, és (kétoldali) egységelem létezése esetén adjuk meg, mely elemeknek létezik inverze.

(a) A páros számok körében (a1) az összeadás; (a2) a szorzás; (a3) a kivonás.

(b) A páratlan számok körében (b1) az összeadás; (b2) a szorzás.

(c) A pozitív egészek körében (c1) $\max(a, b)$; (c2) $\min(a, b)$; (c3) $\mathrm{lkkt}(a, b)$.

(d) A modulo m maradékosztályok körében a pozitív egész reprezentánsok segítségével definiált (d1) összeadás; (d2) szorzás; (d3) hatványozás; (d4) maximumképzés. (Ezt úgy kell érteni, hogy pl. a modulo 10 maradékosztályok körében a 8-at tartalmazó és a 13-at tartalmazó maradékosztályok maximuma a $\max(8, 13) = 13$-at tartalmazó maradékosztály.)

(e) A kompozíció (e1) a sík összes eltolásai körében; (e2) a sík összes (tetszőleges szögű és tetszőleges pont körüli) elforgatásai körében; (e3) a sík összes eltolásai és elforgatásai körében.

(f) Egy halmaz összes részhalmazai körében (f1) az egyesítés; (f2) a szimmetrikus differencia (azaz az egyesítésből elhagyjuk a metszetet).

(g) A valós számok körében legyen $a \circ b = 2a + 2b$.

(h) Az egész számokon legyen bármely a-ra $5 * a = a * 5 = a$ és $a * b = 5$, ha a és b egyike sem az 5.

(i) A mátrixszorzás azoknak a 2×2-es valós elemű mátrixoknak a körében, amelyeknek (i1) a második sora nulla; (i2) mind a négy eleme egyenlő; (i3) a négy elem összege nulla.

A.4.2 Legyen X egy tetszőleges (véges vagy végtelen) halmaz. Tekintsük az $X \to X$ függvények halmazát a szokásos függvényösszetételre (kompozícióra, egymás után alkalmazásra). Mi lesz itt az egységelem? Mely függvényeknek lesz bal-, illetve jobbinverzük és hány darab?

A.4.3 Egy n elemű halmazon hány művelet értelmezhető? Ezek közül hány lesz kommutatív? Hánynak lesz egységeleme?

A.4.4 Tekintsünk egy asszociatív, egységelemes műveletet. Bizonyítsuk be, hogy ha a-nak és b-nek is van (kétoldali) inverze, akkor ab-nek is létezik (kétoldali) inverze. Igaz-e az állítás megfordítása?

A.4.5 Melyek igazak az alábbi állítások közül?

(a) Ha van olyan $a, b \in H$, amelyre $ab = ba = b$, akkor a egységelem.

(b) Ha a művelet egységelemes, és valamely $a, b \in H$ elempárra $ab = = ba = b$, akkor a az egységelem.

(c) Ha a művelet egységelemes, valamely $a, b \in H$ elempárra $ab = ba = b$, és b-nek van inverze, akkor a az egységelem.

(d) Ha a művelet asszociatív, egységelemes, valamely $a, b \in H$ elempárra $ab = ba = b$, és b-nek van inverze, akkor a az egységelem.

A.4.6

(a) Mutassunk példát olyan asszociatív, egységelemes műveletre, amelynél valamelyik elemnek végtelen sok balinverze van.

(b) Lássuk be, hogy ha egy asszociatív, egységelemes műveletnél minden elemnek létezik balinverze, akkor minden elemnek pontosan egy balinverze van, amely az adott elemnek ráadásul kétoldali inverze.

(c) Bizonyítsuk be, hogy az egységelemnek (nemasszociatív művelet esetén is) pontosan egy balinverze és pontosan egy jobbinverze létezik.

(d) Mutassunk példát olyan (nemasszociatív) egységelemes műveletre, amelynél az egységelemen kívül minden elemnek végtelen sok bal- és jobbinverze létezik.

A.4.7 Hogyan módosul az A.4.7 Tétel I. része, ha b-re (a kétoldali inverz helyett) csak a bal oldali inverz létezését követeljük meg (és továbbra is feltesszük, hogy a művelet asszociatív és egységelemes)?

A.4.8 Bizonyítsuk be, hogy ha a művelet asszociatív és az $xb = a$ és $by = a$ egyenletek bármely $a, b \in H$ esetén megoldhatók, akkor ezeknek az egyenleteknek minden a, b-re pontosan egy megoldása van.

A.4.9 Mutassunk példát arra, hogy az A.1.7 Tétel egyik állítása sem marad igaz, ha a művelet asszociativitását nem követeljük meg.

A.5. Test

A kommutatív test fogalma a racionális, valós vagy komplex számoknak az összeadással és szorzással kapcsolatos tulajdonságait általánosítja.

A.5.1 Definíció

Egy T legalább kételemű halmazt *kommutatív test*nek nevezünk, ha

(i) értelmezve van T-n két művelet — az egyiket összeadásnak, a másikat szorzásnak hívjuk;

(ii) az összeadás asszociatív és kommutatív, létezik nullelem, és minden elemnek létezik ellentettje;

(iii) a szorzás asszociatív és kommutatív, létezik egységelem, és a nullelemen kívül minden elemnek létezik (a szorzásra vonatkozó, azaz multiplikatív) inverze;

(iv) bármely $a, b, c \in T$-re $a(b + c) = ab + ac$ teljesül. ♣

Az elnevezésben a „kommutatív” jelző a szorzás kommutativitására utal. Ha a szorzás kommutativitását nem kötjük ki, akkor *nem kommutatív test*ről vagy *ferdetest*ről beszélünk (ekkor azonban (iv)-ben a $(b + c)a = ba + ca$ azonosságot is előírjuk). Nem kommutatív testet alkotnak pl. a *kvaterniók*, lásd az 5.6 pont P5 példáját. A jelen fejezetben (és a könyv legnagyobb részében is) testen mindig kommutatív testet értünk.

Az (i)–(iv) követelményeket szokás *testaxiómák*nak is nevezni.

Az előző pontnak megfelelően egy testben a nullelemet 0-val, (a szorzásra vonatkozó) egységelemet 1-gyel, egy a elem ellentettjét $-a$-val, és ha $a \neq 0$, akkor az a (multiplikatív) inverzét a^{-1}-gyel (vagy $1/a$-val) jelöljük.

A (iv) azonosságot *disztributivitás*nak nevezzük. Általános szabály, hogy egy olyan algebrai struktúrában, amelynél egy halmazon egyszerre több művelet is értelmezve van, a különböző műveleteket egymással műveleti azonosság(ok) köti(k) össze.

Az A.4.7 Tétel alapján egy T testben a $b+x = a$ egyenlet minden $a, b \in T$-re egyértelműen megoldható, azaz elvégezhető a *kivonás*. Ugyanígy, a $bx = a$ egyenlet minden $b \neq 0$ és $a \in T$-re egyértelműen megoldható, azaz elvégezhető az *osztás* (a nullelemmel történő osztás kivételével). Sőt, az A.1.7 Tételből az is következik, hogy a test definíciójában a nullára és az ellentettre, illetve az egységelemre és az inverzre vonatkozó előírásokat akár ki is cserélhetjük a kivonás, illetve az osztás elvégezhetőségével. Ennek alapján a test fogalmát röviden abban a formában is összefoglalhatjuk, hogy „elvégezhető a négy alapművelet és a szokásos műveleti azonosságok érvényesek.”

Megjegyezzük még, hogy nem kommutatív test esetén nem osztásról, hanem külön bal és külön jobb oldali osztásról kell beszélnünk, hiszen (a nem nulla elemek körében) ekkor a szorzásnak két különböző inverz művelete van. (Kivonás azonban ekkor is csak „egyféle” létezik, mivel az összeadás mindenképpen kommutatív.)

Példák testre

P1. Mint már említettük, a test fogalmához a „modellt” elsősorban a racionális, a valós, illetve a komplex számok szolgáltatták. Ezeket a testeket rendre $\mathbf{Q}$, $\mathbf{R}$, illetve $\mathbf{C}$ jelöli.

P2. Testet alkotnak egy p prím modulus szerinti maradékosztályok a reprezentánsok segítségével definiált összeadásra és szorzásra nézve. Itt először is azt kell igazolni, hogy a műveletek egyáltalán értelmesek, vagyis az osztályokra a reprezentánsok segítségével definiált műveletek nem függnek a reprezentánsok választásától (vö. az A.4.1d feladattal). A multiplikatív inverz kivételével a többi tulajdonság az egész számokra vonatkozó megfelelő tulajdonságokból következik. A multiplikatív inverzre vonatko-

zó előírás a reprezentánsokra átfogalmazva azt jelenti, hogy bármely $a \not\equiv 0 \pmod{p}$ esetén az $ax \equiv 1 \pmod{p}$ lineáris kongruencia megoldható. Ez valóban igaz, hiszen p prím volta miatt $(a, p) = 1$.

A modulo p maradékosztályok testét F_p-vel jelöljük. Ennek p eleme van, tehát *véges test*. A véges testek általános leírását az A.11 pontban tárgyaljuk.

P3. Testet alkotnak az $a + b\sqrt{2}$ alakú valós számok, ahol a, b végigfutnak a racionális számokon. A multiplikatív inverz létezését a szokásos „gyöktelenítési" eljárással igazolhatjuk, a többi testaxióma pedig szinte azonnal adódik. Ha a $\sqrt{2}$ helyett $\sqrt[3]{5}$-tel szeretnénk hasonló konstrukciót elkészíteni, akkor az $a + b\sqrt[3]{5} + c\sqrt[3]{25}$ alakú valós számokat kell tekinteni, ahol a, b, c befutják a racionális számokat. Ez valóban test, bár a multiplikatív inverz meghatározása itt már ugyancsak komoly fejtörő elé állíthat bennünket. Az ilyen típusú testekkel általánosan az A.10 pontban foglalkozunk majd.

P4. Testet alkotnak a szokásos összeadásra és szorzásra nézve az ún. algebrai törtek vagy racionális törtfüggvények, azaz a valós együtthatós polinomokból (formálisan) képzett hányadosok.

Feladatok

A.5.1 Döntsük el, hogy az alábbi halmazok a szokásos összeadásra és szorzásra nézve kommutatív testet alkotnak-e.

(a) A valós számok következő részhalmazai: (a1) a páratlan nevezőjű törtek (az 1 is páratlan szám); (a2) az $a + b\sqrt{7}$ alakú számok, ahol a és b racionális; (a3) a nemnegatív racionális számok.

(b) A modulo $2m$ maradékosztályok közül a „párosak" (azaz a $0, 2, 4, 6, \ldots, 2m-2$ által reprezentáltak), ha (b1) $2m = 10$; (b2) $2m = 20$.

(c) Azok az $f : \mathbf{R} \to \mathbf{R}$ függvények, amelyekre (c1) $f(0) = 0$; (c2) $a \neq 0 \Rightarrow f(a) = 0$.

(d) Az alábbi alakú 2×2-es valós elemű mátrixok:

(d1) $\begin{pmatrix} 0 & 0 \\ a & 0 \end{pmatrix}$; (d2) $\begin{pmatrix} 0 & 0 \\ 0 & a \end{pmatrix}$; (d3) $\begin{pmatrix} a & 2a \\ 4a & 8a \end{pmatrix}$;

(d4) $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$; (d5) $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

A.5.2 Legyen $m > 1$ rögzített pozitív egész, és tekintsük azt az m^2 darab $a+bi$ „komplex számot", ahol az a és a b egy-egy modulo m maradékosztály. Definiáljuk az összeadást és a szorzást a komplex számoknál

látott műveletek mintájára [tehát pl. $m = 5$-re $(2 + 3i)(1 + 4i) = (2 - 12) + (3 + 8)i = i$]. Döntsük el, hogy testet kapunk-e, ha (a) $m = 2$; (b) $m = 3$; (c) $m = 5$.

A.5.3 Döntsük el, hogy az alábbi halmazok a megadott $\oplus$ összeadásra és $\odot$ szorzásra nézve kommutatív testet alkotnak-e. (A bekarikázatlan jelek a „szokásos" műveleteket jelentik.)

(a) A valós számok, ahol $a \oplus b = \sqrt[3]{a^3 + b^3}$ és $a \odot b = ab$ (vagyis a szorzás a szokásos).

(b) A valós számok, ahol $a \oplus b = 5(a + b)$ és $a \odot b = ab$.

(c) A valós számok, ahol $a \oplus b = a + b$ és $a \odot b = 5ab$.

(d) A valós számok, ahol $a \oplus b = a + b - 1$ és $a \odot b = a + b - ab$.

(e) A pozitív valós számok, ahol $a \oplus b = ab$ és $a \odot b = a^{\lg b}$.

(f) A komplex számok, ahol az összeadás a szokásos és $(a+bi)\odot(c+di) = ac + bdi$.

(g) A komplex számok, ahol az összeadás a szokásos és $(a+bi)\odot(c+di) = (ad + bc) + (bd - ac)i$.

A.5.4 Két testet egymással *izomorf*nak nevezünk, ha az elemeik *kölcsönösen egyértelműen* és *művelettartó* módon megfeleltethetők egymásnak, azaz ha létezik olyan $\varphi : T_1 \to T_2$ bijekció, amelyre $\varphi(a + b) = \varphi(a) + \varphi(b)$ és $\varphi(ab) = \varphi(a)\varphi(b)$ bármely $a, b \in T_1$ esetén teljesül. (Ez azt jelenti, hogy a két test „pontosan ugyanolyan", csak az elemek és a műveletek másképp vannak jelölve.)

(a) Mutassuk meg, hogy a $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ és F_p testek közül semelyik kettő sem izomorf.

*(b) Keressük meg az A.2.1 és A.2.3 feladat példái közül azokat, amelyek a $\mathbf{Q}$, $\mathbf{R}$, $\mathbf{C}$ és F_p testek valamelyikével izomorfak.

A.5.5 Egy T test *részteste*nek egy olyan $K \subseteq T$ részhalmazt nevezünk, amely maga is test a T-beli összeadásra és szorzásra (pontosabban azok megszorítására) nézve. Pl. $\mathbf{R}$ részteste $\mathbf{C}$-nek, illetve $\mathbf{Q}$ részteste $\mathbf{R}$-nek.

(a) Lássuk be, hogy $\mathbf{R}$-nek és $\mathbf{C}$-nek végtelen sok részteste van.

(b) Mutassuk meg, hogy $\mathbf{Q}$-nak, illetve az F_p testeknek nincsen valódi részteste (azaz ezekben a testekben az egyetlen résztest maga az eredeti test).

**(c) Bizonyítsuk be, hogy ha egy T testnek nincsen valódi részteste, akkor T vagy $\mathbf{Q}$-val, vagy pedig valamelyik F_p testtel izomorf.

(d) Igazoljuk, hogy $\mathbf{R}$-nek *nincs* olyan részteste, amely valamelyik F_p-vel izomorf.

*A.5.6 Definiálható-e az egész számok halmazán egy $\oplus$ összeadás, illetve egy $\odot$ szorzás úgy, hogy az egész számok testet alkossanak

(a) a $\oplus$ összeadásra és a szokásos szorzásra;
(b) a szokásos összeadásra és a $\odot$ szorzásra;
(c) a $\oplus$ összeadásra és a $\odot$ szorzásra?

A.6. Gyűrű

A gyűrű egy olyan kétműveletes algebrai struktúra, amelynél a szorzásra vonatkozóan csak kevesebbet követelünk meg, mint a testnél:

A.6.1 Definíció

Egy R nem üres halmazt *gyűrű*nek nevezünk, ha

(i) értelmezve van R-en két művelet — az egyiket összeadásnak, a másikat szorzásnak hívjuk;
(ii) az összeadás asszociatív és kommutatív, létezik nullelem, és minden elemnek létezik ellentettje;
(iii) a szorzás asszociatív;
(iv) bármely $a, b, c \in R$-re $a(b + c) = ab + ac$ és $(b + c)a = ba + ca$ teljesül. ♣

Látjuk tehát, hogy a fenti *gyűrűaxiómák*nál az (i), (ii) és (iv) kikötések azonosak a testnél előírtakkal, csak (iii)-nál engedtük el a szorzás kommutativitását, valamint az egységelemre, illetve az elemek inverzére vonatkozó feltételeket.

Mivel a szorzás nem (feltétlenül) kommutatív, ezért (iv)-ben mindkét oldali disztributivitást meg kell követelnünk. A két disztributivitás valóban független egymástól, pl. ha az $\mathbf{R} \to \mathbf{R}$ függvények körében az összeadást a szokásos módon, a szorzást pedig a kompozícióként definiáljuk, akkor minden gyűrűaxióma teljesül, kivéve az egyik disztributivitást.

A testnél látottak mintájára most is igaz, hogy a gyűrű definíciójában a nullelemre és az ellentettre vonatkozó előírások helyettesíthetők a kivonás elvégezhetőségével. Ennek megfelelően a gyűrű fogalmát röviden abban a formában is összefoglalhatjuk, hogy „elvégezhető az összeadás, a kivonás és a szorzás, továbbá érvényesek a szokásos műveleti azonosságok (eltekintve esetleg a szorzás kommutativitásától).”

Egy gyűrű *kommutatív*, ha a szorzás kommutatív, *egységelemes*, ha a szorzásnak van egységeleme. A *kommutatív test* ennek megfelelően egy olyan egységelemes, kommutatív gyűrűt jelent, amelyben minden nem nulla elemnek van inverze.

Egy R gyűrűben minden $a \in R$ elemre $0a = a0 = 0$ (lásd az A.6.4 feladatot), így egy legalább kételemű gyűrűben a nullelem és az egységelem szükségképpen különbözők. Az is adódik, hogy a 0-nak nem lehet (se bal, se jobb oldali) inverze.

Bizonyos gyűrűkben előfordul, hogy egy szorzat úgy is lehet 0, hogy egyik tényező sem 0, ez vezet el a *nullosztó*k fogalmához:

A.6.2. Definíció

Egy gyűrűben egy $a \neq 0$ elemet *bal oldali nullosztó*nak nevezünk, ha van olyan $b \neq 0$ elem, amellyel $ab = 0$ teljesül.

Hasonlóan, az $a \neq 0$ elem *jobb oldali nullosztó*, ha létezik olyan $c \neq 0$ elem, amelyre $ca = 0$. ♣

A.6.3 Tétel

Ha a gyűrű egységelemes és a-nak létezik bal oldali inverze, akkor a nem lehet bal oldali nullosztó. ♣

Az állítás természetesen úgy is igaz marad, ha a „bal” szó helyett (mindkétszer) a „jobb” szerepel.

Bizonyítás: Jelöljük e-vel az egységelemet és d-vel az a elem (egyik) balinverzét. Tegyük fel, hogy valamilyen b-vel $ab = 0$ teljesül. Azt kell igazolnunk, hogy ekkor szükségképpen $b = 0$. A $0 = ab$ egyenlőséget d-vel balról megszorozva $0 = d0 = d(ab) = (da)b = eb = b$ adódik. ■

Az A.6.3 Tétel megfordítása nem igaz, pl. az egész számok gyűrűjében nincsenek nullosztók (az ilyen gyűrűt *nullosztómentes*nek nevezzük), azonban csak az 1-nek és a -1-nek van inverze.

Az A.6.3 Tétel fontos következménye, hogy minden test nullosztómentes.

Példák gyűrűre

P1. Még egyszer megemlítjük, hogy minden test egyben gyűrű is.

P2. Az alábbi halmazok a szokásos összeadásra és szorzásra nézve egy kommutatív, egységelemes, nullosztómentes gyűrűt alkotnak: (A) az egész számok; (B) az $a + b\sqrt{2}$ alakú valós számok, ahol a, b egész; (C) a Gauss-egészek, azaz azok az $a + bi$ komplex számok, ahol a, b egész; (D) a valós együtthatós polinomok; (E) az egész együtthatós polinomok.

P3. Nem egységelemes (de kommutatív és nullosztómentes) gyűrűt alkotnak pl. a páros számok vagy a nulla konstans tagú polinomok (a műveletek a szokásosak).

P4. A valós számsorozatok az elemenkénti összeadásra és szorzásra, valamint az $\mathbf{R} \to \mathbf{R}$ függvények a szokásos függvényösszeadásra és szorzásra olyan kommutatív, egységelemes gyűrűt alkotnak, amelyben vannak nullosztók.

P5. A modulo m maradékosztályok a reprezentánsok segítségével definiált összeadásra és szorzásra nézve egy kommutatív, egységelemes gyűrűt alkotnak. Itt pontosan a redukált maradékosztályoknak van inverze, a többi nem nulla maradékosztály pedig nullosztó. Ez a gyűrű pontosan akkor test, ha m prím.

P6. Fontos gyűrű az $n \times n$-es (pl.) valós elemű mátrixok gyűrűje, lásd részletesen a 2.2 pontban. Ez egységelemes, de $n > 1$ esetén nem kommutatív. Inverze pontosan azoknak a mátrixoknak van, amelyeknek a determinánsa nem nulla, a többi mátrix a nullmátrix kivételével bal és jobb oldali nullosztó.

P7. Tekintsük egy H halmaz összes részhalmazait, és legyen az összeadás a szimmetrikus differencia, a szorzás pedig a metszet, azaz $A \oplus B = (A \setminus B) \cup (B \setminus A)$ és $A \odot B = A \cap B$. Így egy kommutatív, egységelemes gyűrűt kapunk. Inverze csak az egységelemnek van, az összes többi nem nulla elem nullosztó.

Feladatok

A.6.1 Ellenőrizzük, hogy a P1–P7 példákban valóban a mondott tulajdonságú gyűrűket definiáltunk.

A.6.2
(a) Mely elemeknek van inverze a P2 példában felsorolt gyűrűkben?
(b) Mely elemeknek van inverze és mely elemek nullosztók a P4 példában felsorolt gyűrűkben?
(c) Mi lesz a modulo 100 maradékosztályok gyűrűjében a 37 által reprezentált maradékosztály inverze?

A.6.3 Válasszuk ki az A.5.1–A.5.3 feladatok példái közül azokat a gyűrűket, amelyek nem alkotnak testet. Mindegyikben határozzuk meg a (bal, illetve jobb oldali) nullosztókat. Az egységelemes gyűrűknél keressük meg, mely elemeknek van inverze.

A.6.4 Bizonyítsuk be, hogy egy gyűrűben minden a elemre $0a = a0 = 0$ teljesül.

A.6.5

(a) Ellenőrizzük, hogy a P7 példa gyűrűje kommutatív, továbbá bármely elem ellentettje és négyzete önmaga.

(b) Van-e valamilyen kapcsolat általában is gyűrűkben az (a)-ban felsorolt három tulajdonság között?

A.6.6 Egy gyűrűben hogyan jellemezhetők azok a c elemek, amelyekkel lehet balról egyszerűsíteni (azaz, amelyekre $ca = cb$-ből szükségképpen $a = b$ következik)?

Mit jelent ez speciálisan egy testben, továbbá az egész számok, illetve a modulo m maradékosztályok gyűrűjében?

A.6.7 Legyenek c és d egy gyűrű elemei. Melyek igazak az alábbi állítások közül?

(a) Ha c jobb oldali nullosztó, akkor $cd = 0$ vagy cd is jobb oldali nullosztó.

(b) Ha cd jobb oldali nullosztó, akkor c is jobb oldali nullosztó.

**(c) Ha c és d közül legalább az egyik jobb oldali nullosztó, akkor $cd = 0$ vagy cd is jobb oldali nullosztó.

(d) Ha cd jobb oldali nullosztó, akkor c és d közül legalább az egyik jobb oldali nullosztó.

(e) Ha c és d jobb oldali nullosztó, akkor $c + d = 0$ vagy $c + d$ is jobb oldali nullosztó.

(f) Ha $c + d$ jobb oldali nullosztó, akkor c és d közül legalább az egyik jobb oldali nullosztó.

A.6.8 Bizonyítsuk be, hogy egy legalább kételemű, véges, nullosztómentes gyűrű szükségképpen test.

Megjegyzés: Belátható, hogy minden véges test kommutatív (Wedderburn tétele), tehát mindenképpen kommutatív testet kapunk.

*A.6.9 Mutassuk meg, hogy ha egy gyűrűben pontosan egy bal oldali egységelem létezik, akkor az (kétoldali) egységelem.

A.6.10 Egy R gyűrű *részgyűrű*jének egy olyan $S \subseteq R$ részhalmazt nevezünk, amely maga is gyűrű az R-beli összeadásra és szorzásra (pontosabban azok megszorítására) nézve. Pl. a páros számok részgyűrűt alkotnak az egész számok gyűrűjében.

Mutassuk meg, hogy egy részgyűrű nulleleme szükségképpen megegyezik az eredeti gyűrű nullelemével.

A.6.11 Legyen R egy egységelemes gyűrű és S részgyűrű R-ben, ahol S (és így R is) nem csak a nullelemből áll. Melyek igazak az alábbi állítások közül?

(a) S szükségképpen egységelemes.

(b) Ha S egységelemes, akkor S egységeleme szükségképpen megegyezik R egységelemével.

(c) Ha R nullosztómentes és S egységelemes, akkor S egységeleme szükségképpen megegyezik R egységelemével.

*A.6.12 Bizonyítsuk be, hogy ha egy legalább kételemű (nem feltétlenül kommutatív) gyűrűben az $xb = a$ egyenlet bármely $b \neq 0$ és a esetén megoldható, akkor a gyűrű egy nem feltétlenül kommutatív test.

A.7. Polinomok

Ebben a pontban igen vázlatosan (esetenként némi „pongyolaságot" is megengedve) áttekintjük a (kommutatív test feletti) polinomokkal kapcsolatos legfontosabb tudnivalókat.

1. Polinom

A precíz bevezetéssel kapcsolatos nehézségeket átugorva (T feletti) *polinom*on egy olyan $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ „formális kifejezést" értünk, ahol az α_i együtthatók a T kommutatív test elemei. Az $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ és $\beta_0 + \beta_1 x + \ldots + \beta_k x^k$ polinomokat akkor tekintjük azonosnak, ha „esetleges nulla együtthatójú tagoktól eltekintve a megfelelő együtthatók megegyeznek", azaz (pl. $k \geq n$-et feltételezve) $\alpha_0 = \beta_0, \alpha_1 = \beta_1, \ldots, \alpha_n = \beta_n, \beta_{n+1} = \ldots = \beta_k = 0$.

2. Polinomfüggvény

Maga a polinom *nem* függvény, de minden polinom természetes módon „létrehoz" egy ún. *polinomfüggvény*t: az $\alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ polinomhoz tartozó polinomfüggvény a $\gamma \mapsto \alpha_0 + \alpha_1 \gamma + \ldots + \alpha_n \gamma^n$ hozzárendeléssel definiált $T \to T$ függvény. A polinomot némi fantáziával a polinomfüggvény „alakjának" vagy „képletének" képzelhetjük. A két fogalom (a polinom és a polinomfüggvény) semmiképpen sem azonosítható, ugyanis egy függvénynek többféle „alakja" is lehet, ugyanazt a függvényt többféle „képlettel" is előállíthatjuk. Például a modulo p maradékosztályok F_p teste felett az x és x^p (egymástól különböző) polinomokhoz a „kis" Fermat-tétel szerint azonos polinomfüggvény tartozik, hiszen minden a-ra $a^p \equiv a \pmod{p}$. Belátható, hogy ez a „rendellenesség" csak *véges* testek esetén fordul elő (ott viszont „tipikus",

lásd az A.7.1 feladatot), végtelen test felett a polinom-polinomfüggvény kapcsolat bijektív.

A polinomot és a hozzá tartozó polinomfüggvényt általában ugyanúgy jelöljük, mindkettőt (pl.) f-fel (vagy ha az x „határozatlant", illetve „változót" hangsúlyozni akarjuk, akkor $f(x)$-szel). A jelölésen túlmenően legtöbbször a szóhasználatban sem teszünk különbséget közöttük; a polinomfüggvényre is a polinom szót használjuk. Ebben az értelemben pl. „egy f polinom helyettesítési értéke" természetesen az f polinomhoz tartozó polinom*függvény* helyettesítési értékét jelenti. A könyv többi részében mi is ezt a „közös" terminológiát követjük, ebben a pontban azonban szavakban is következetesen megkülönböztetjük a két fogalmat.

3. Műveletek

Az 1.-ben megadott két polinom *összege* definíció szerint az

$$(\alpha_0+\beta_0)+(\alpha_1+\beta_1)x+\ldots+(\alpha_n+\beta_n)x^n+\beta_{n+1}x^{n+1}+\ldots+\beta_kx^k$$

polinom (azaz a „megfelelő tagokat összeadjuk"), *szorzata* pedig az

$$\alpha_0\beta_0+(\alpha_0\beta_1+\alpha_1\beta_0)x+\ldots+(\sum_{i+j=m}\alpha_i\beta_j)x^m+\ldots+\alpha_n\beta_kx^{n+k}$$

polinom (azaz „minden tagot minden taggal megszorzunk").

Mindez összhangban van azzal, hogy a polinomokat tulajdonképpen (formális) összegként kezeljük és a műveleteket ennek megfelelően a számoknál megszokott „mintára" végezzük. Az így definiált műveletek jól kapcsolódnak a polinomfüggvények közötti (függvény)összeadáshoz és szorzáshoz is: ha minden polinomnak megfeleltetjük a hozzá tartozó polinomfüggvényt, akkor ez a megfeleltetés az összeadásra és a szorzásra nézve is *művelettartó*.

4. A $T[x]$ polinomgyűrű

A T feletti polinomok a 3.-ban értelmezett két műveletre nézve egy egységelemes, kommutatív, nullosztómentes gyűrűt alkotnak, amit $T[x]$-szel jelölünk. Ennek nulleleme a 0 polinom, amelynek minden együtthatója (a T-beli) 0.

Megjegyezzük, hogy a $T\to T$ polinom*függvények* is gyűrűt alkotnak a szokásos függvényösszeadásra és szorzásra, ez szintén egységelemes és kommutatív, azonban véges test esetén előfordulnak benne nullosztók (lásd az A.7.3 feladatot). Ha T végtelen test, akkor a polinom-polinomfüggvény megfeleltetés bijektív, továbbá az összeadásra és a szorzásra nézve is művelettartó, ezért ekkor a T feletti polinomok, illetve polinomfüggvények gyűrűje egymással *izomorf* (tehát ekkor pl. a polinomfüggvények körében sincsenek nullosztók).

5. Fokszám

Ha az $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ polinomban $\alpha_n \neq 0$, akkor az n (nemnegatív egész) számot az f polinom *fok*ának vagy *fokszám*ának nevezzük és $\deg f$-fel jelöljük (a jelölés az angol „degree" szóból származik). A 0 polinom kivételével minden polinomnak van foka. A fokszám és a műveletek definíciójából azonnal adódik, hogy ha f, g, illetve $f + g$ nem a nulla polinom, akkor $\deg(fg) = \deg f + \deg g$ és $\deg(f+g) \leq \max(\deg f, \deg g)$. Egy n-edfokú polinomban az x^n együtthatóját a polinom *főegyüttható*jának nevezzük.

Hangsúlyozzuk, hogy fokszáma a (nem nulla) polinomoknak, és nem a polinomfüggvényeknek van: például az F_p test felett az x polinom foka 1, az x^p polinom foka p, miközben ugyanaz a polinomfüggvény tartozik hozzájuk. (Végtelen test felett — a polinomok és polinomfüggvények közötti bijekió alapján — megengedhető egy polinomfüggvény fokáról is beszélni.)

6. Gyök

A $\gamma \in T$ elemet egy polinom*függvény gyök*ének nevezzük, ha a függvény γ helyen vett helyettesítési értéke 0(=a test nulleleme). Egy *polinom* gyökein a hozzá tartozó polinomfüggvény gyökeit értjük. Igen fontos az alábbi egyszerűen adódó ekvivalencia: egy f polinomhoz tartozó *polinomfüggvény*nek pontosan akkor gyöke a γ, ha az f *polinom*ból kiemelhető az $x-\gamma$ *gyöktényező*.

7. Multiplicitás

A $\gamma \in T$ elemet az f polinom(!) (pontosan) *k-szoros gyök*ének nevezzük, ha f-ből az $x - \gamma$ gyöktényező pontosan k-szor emelhető ki, azaz $f = (x - \gamma)^k g$, ahol a g polinomhoz tartozó polinomfüggvénynek a γ már nem gyöke. Ugyanezt úgy is mondhatjuk, hogy az f polinomban a γ gyök *multiplicitása* k. Ha $k \geq 2$, akkor γ-t az f polinom *többszörös gyök*ének nevezzük.

A fokszámnál elmondottakhoz hasonlóan itt is kiemeljük, hogy a gyökök multiplicitását a polinomokra, és nem a polinomfüggvényekre definiáltuk. Ismét az ottani példával élve, az F_p test felett a 0 az x polinomnak egyszeres, az x^p polinomnak pedig p-szeres gyöke, noha a két polinomhoz ugyanaz a polinomfüggvény tartozik.

8. A gyökök száma

A nulla polinomnak minden T-beli elem gyöke, bármely más polinomnak azonban multiplicitással számolva is legfeljebb annyi gyöke van, mint amennyi a foka. (Ez a tétel *nem kommutatív* test esetén nem érvényes, lásd az 5.6.23 feladatot.)

Az *algebra alaptétele* szerint a *komplex* test felett minden nem konstans polinomnak van (komplex) gyöke. Ebből következik, hogy a komplex test felett

minden nem nulla polinomnak a multiplicitást is figyelembe véve *pontosan* annyi gyöke van, mint amennyi a foka.

Egy *valós* együtthatós polinomnak egy *komplex* szám és a konjugáltja ugyanannyiszoros gyöke. Az algebra alaptételéből így az is következik, hogy minden valós együtthatós polinom felbontható legfeljebb másodfokú valós együtthatós polinomok szorzatára, és minden páratlan fokú valós együtthatós polinomnak van *valós* gyöke.

9. A gyökök meghatározása

Bármely T esetén az elsőfokú $\alpha_0 + \alpha_1 x$ polinom (ahol $\alpha_1 \neq 0$) egyetlen gyöke $-\alpha_0/\alpha_1$. A másodfokú polinomok gyökeinek megkeresésére „majdnem minden T" esetén alkalmazható a másodfokú egyenlet szokásos megoldóképlete.

A komplex vagy a valós test felett a harmad- és negyedfokú polinomok esetén hasonló univerzális megoldási módszer, *„megoldóképlet"* érvényes, amely a gyököket az együtthatókból a négy alapművelet és pozitív egész kitevőjű gyökvonások véges sokszori alkalmazásával állítja elő. Az ötöd- és magasabb fokú polinomok esetén ilyen általános módszer nem létezik, sőt olyan konkrét polinomok is megadhatók, amelyek gyökeit nem kaphatjuk meg az együtthatókból a fenti módon.

A racionális együtthatós polinomok racionális gyökeinek a meghatározására az alábbi egyszerű algoritmus alkalmazható. A polinomot az együtthatók nevezőinek a legkisebb közös többszörösével beszorozva egy olyan $a_0 + a_1 x + \\ + \ldots + a_n x^n$ egész együtthatós polinomot kapunk, amelynek a gyökei azonosak az eredeti polinom gyökeivel. Feltehető, hogy $a_n \neq 0$ és szükség esetén az x megfelelő hatványával végigosztva (ez a nem nulla gyökökön nem változtat) azt is elérhetjük, hogy $a_0 \neq 0$. Ha ennek az egész együtthatós polinomnak egy c/d racionális szám gyöke (ahol c és d relatív prím egész számok), akkor szükségképpen $c \mid a_0$ és $d \mid a_n$. Az így szóba jövő véges sok racionális számot végigpróbálva megkapjuk, hogy közülük melyek lesznek valóban gyökök.

Az F_p testek feletti polinomok gyökeinek a meghatározása, azaz a prím modulusú kongruenciák megoldása legrosszabb esetben az összes (véges sok!) testbeli elem végigpróbálásával történhet. Ha az f polinom foka p vagy annál nagyobb, akkor az alábbi redukciós eljárással f helyett elég egy legfeljebb $p-1$-edfokú polinom gyökeit megkeresni. Legyen f-nek az $x^p - x$ polinommal való osztási maradéka g (vagyis g-t úgy kapjuk, hogy f-ben mindenütt x^p helyére mindaddig x-et írunk, amíg ez csak lehetséges). Ekkor a g egy olyan legfeljebb $p-1$-edfokú (vagy esetleg a nulla) polinom, amelyhez ugyanaz a polinomfüggvény tartozik, mint az f-hez, ezért a gyökeik is megegyeznek.

10. Derivált polinom

A tetszőleges(!) T kommutatív test feletti $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n$ polinom *deriváltj*át a formális deriválási szabályok szerint definiáljuk: $f' = \alpha_1 + \ldots + n\alpha_n x^{n-1}$, ahol $j(\alpha_j x^{j-1})$ a j-szeri összeadást jelenti $T[x]$-ben.

Egyszerű számolással igazolható, hogy összeg, szorzat és hatvány deriválására a szokásos szabályok érvényben maradnak.

A derivált szorosan kapcsolódik a gyökök multiplicitásához: ha γ pontosan k-szoros gyöke f-nek ($k \geq 1$), akkor legalább $k-1$-szeres gyöke f'-nek. Itt a „legalább" nem mindig helyettesíthető a „pontosan" szóval, pl. F_2 felett az $f = x^5 + x = x(x+1)^4$ polinomnak a deriváltja $f' = x^4 + 1 = (x+1)^4$, tehát az 1 mindkettőnek pontosan négyszeres gyöke. Az is előfordulhat, hogy f' a nulla polinom lesz, vegyük pl. az F_p test felett az $f = x^p$ polinomot, ekkor $f' = px^{p-1} = 0$. Ha azonban a T testben $\alpha + \alpha + \ldots + \alpha = 0 \Rightarrow \alpha = 0$ teljesül, azaz egy nem nulla elemet önmagához akárhányszor hozzáadva sohasem kaphatunk nullát, akkor a fenti tétel úgy is érvényes marad, ha a „legalább" helyére a „pontosan" szót írjuk.

11. Összefüggés a gyökök és együtthatók között

Ha egy n-edfokú polinomnak multiplicitással számolva pontosan n gyöke van, legyenek ezek $\gamma_1, \ldots, \gamma_n$, akkor az

$$f = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n = \alpha_n \prod_{j=1}^{n} (x - \gamma_j)$$

egyenlőségből a $\sigma_m = (-1)^m \alpha_{n-m}/\alpha_n$, $m = 1, 2, \ldots, n$ összefüggéseket nyerjük, ahol σ_m a γ_j-kből képzett összes (azaz $\binom{n}{m}$ darab) m-tényezős szorzat összege. Speciálisan, a γ_i-k összege $-\alpha_{n-1}/\alpha_n$, a szorzatuk pedig $(-1)^n \alpha_0/\alpha_n$.

12. Polinomok számelmélete

Az oszthatóságot és a többi számelméleti fogalmat $T[x]$-ben pontosan ugyanúgy definiáljuk, mint bármely kommutatív, egységelemes, nullosztómentes gyűrűben.

Ennek megfelelően az *egység*ek (ne keverjük össze az egységelemmel!) azok a polinomok, amelyek minden polinomnak osztói, azaz, amelyeknek létezik (multiplikatív) inverzük. Ezek éppen a nem nulla konstans polinomok.

Egy polinom *irreducibilis* vagy *felbonthatatlan*, ha egyrészt ő maga nem egység, másrészt csak úgy bontható szorzattá, hogy valamelyik tényező egység (tehát csak az egységekkel és önmaga egységszereseivel osztható). A nullától és egységektől különböző, nem irreducibilis polinomokat *reducibilis*nek nevezzük.

$T[x]$-ben elvégezhető a *maradékos osztás*: bármely $g \neq 0$ és f polinomhoz létezik olyan h és r polinom, amelyekre $f = gh + r$ és $\deg r < \deg g$ vagy $r = 0$

(az is igaz, hogy h és r egyértelmű). Ez azt jelenti, hogy $T[x]$ *euklideszi gyűrű*, és így érvényes a *számelmélet alaptétele* (más szóval az *egyértelmű prímfaktorizáció*): a nulla polinomon és az egységeken kívül minden polinom felbomlik véges sok irreducibilis polinom szorzatára, és ez a felbontás a tényezők sorrendjétől és egységszeresétől eltekintve egyértelmű. Itt az egyértelműség azt jelenti, hogy ha $f = s_1 \cdot \ldots \cdot s_m = t_1 \cdot \ldots \cdot t_k$, ahol minden s_i és t_j irreducibilis, akkor $m = k$ és az s_i-k és t_j-k párba állíthatók úgy, hogy az egy párba tartozó polinomok egymás egységszeresei.

Két polinom *legnagyobb közös osztója* egy olyan polinomot jelent, amely közös osztó (azaz mindkét polinomnak osztója) és minden közös osztónak többszöröse. Az f és g polinomok legnagyobb közös osztóját (f, g)-vel vagy $\mathrm{lnko}(f, g)$-vel jelöljük. A maradékos osztás ismételt alkalmazásával adódó *euklideszi algoritmus*ból következik, hogy bármely két polinomnak létezik legnagyobb közös osztója, továbbá ez előállítható a két polinom alkalmas polinomszorosának összegeként: tetszőleges $f, g \in T[x]$-hez létezik olyan $u, v \in T[x]$, amellyel $(f, g) = fu + gv$ (az u és v nem egyértelmű). A legnagyobb közös osztó definíciója biztosítja, hogy két polinom legnagyobb közös osztója egységszerestől eltekintve egyértelmű, azaz ha d egy ilyen tulajdonságú polinom, akkor d minden egységszerese is ilyen tulajdonságú, és más megfelelő polinom nincs.

Egy polinom *prím*, ha egyrészt nem a nulla polinom és nem egység, másrészt két polinom szorzatának CSAK úgy lehet osztója, hogy a két tényező közül legalább az egyiknek osztója. A legnagyobb közös osztó felhasználásával igazolható, hogy egy polinom akkor és csak akkor prím, ha felbonthatatlan.

13. Irreducibilis polinomok

Mindig világosan jelezni kell, hogy egy adott polinomot melyik test felettinek tekintünk, hiszen például egy racionális együtthatós polinom egyben valós vagy komplex együtthatós polinom is, és így előfordulhat, hogy a racionális test felett irreducibilis, ugyanakkor a valós test felett reducibilis. (Az „f irreducibilis T felett" és az „f irreducibilis $T[x]$-ben" szóhasználat egyaránt helyes.)

Az algebra alaptételéből következik, hogy a komplex test felett a felbonthatatlanok éppen az elsőfokú polinomok, a valós test felett pedig az elsőfokúak és azok a másodfokúak, amelyeknek nincs valós gyökük.

A racionális test feletti irreducibilis polinomok jóval változatosabb képet mutatnak. Egy jól használható elégséges feltétel a *Schönemann–Eisenstein-kritérium*: ha $f = a_0 + a_1 x + \ldots + a_n x^n$ *egész* együtthatós és létezik olyan p prímszám, amely osztója az $a_0, a_1, \ldots, a_{n-1}$ együtthatók mindegyikének, de nem osztója a_n-nek és p^2 nem osztója a_0-nak, akkor f irreducibilis a *racionális*

test felett. Ebből azonnal adódik, hogy a racionális test felett minden n pozitív egészre létezik n-edfokú irreducibilis polinom.

Egy konkrét racionális együtthatós polinom irreducibilitásának eldöntéséhez először is szorozzuk be a polinomot az együtthatók nevezőinek a legkisebb közös többszörösével, majd az így keletkezett polinomot osszuk el az együtthatók legnagyobb közös osztójával. Ez a racionális test feletti irreducibilitást nem befolyásolja, hiszen csak egy konstanssal, azaz egységgel szoroztunk. Így egy olyan egész együtthatós polinomhoz jutottunk, amelynek az együtthatói relatív prímek, az ilyen polinomokat *primitív*eknek nevezzük. Igen fontos az alábbi két tétel, amelyeket *Gauss-lemmá(k)*nak szokás nevezni: I. Két primitív polinom szorzata is primitív; II. Ha egy F *egész* együtthatós polinom felírható a g és h *racionális* együtthatós polinomok szorzataként, $F = gh$, akkor F előáll $F = GH$ alakban is, ahol G és H olyan *egész* együtthatós polinomok, amelyek a g-nek, illetve a h-nak (racionális) konstansszorosai (tehát $\deg G = \deg g$ és $\deg H = \deg h$). Ennek alapján a racionális test feletti felbonthatóság kérdését arra vezettük vissza, hogy egy egész együtthatós polinom felírható-e (nem konstans) egész együtthatós polinomok szorzataként.

A racionális test feletti irreducibilis polinomok fontos osztályát alkotják a *körosztási polinomok*. Az m-edik körosztási polinom, Φ_m, az az 1 főegyütthatós polinom, amelynek gyökei az m-edik primitív komplex egységgyökök. Φ_m fokszáma tehát $\varphi(m)$. Például $\Phi_4 = x^2 + 1, \Phi_{11} = x^{10} + x^9 + \ldots + 1$. Az, hogy Φ_m egész együtthatós, az $x^m - 1 = \prod_{d|m} \Phi_d$ összefüggés felhasználásával adódik. Ha m prím vagy prímhatvány, akkor a racionális test feletti irreducibilitás egy alkalmas lineáris helyettesítés után a Schönemann–Eisenstein-kritérium segítségével igazolható, tetszőleges m-re a bizonyítás lényegesen nehezebb.

14. Egész együtthatós polinomok

A kommutatív test feletti polinomokra felsorolt tulajdonságok nagy része akkor is érvényben marad, ha az együtthatókat (a kommutatív test helyett) egy kommutatív, egységelemes, nullosztómentes gyűrűből vesszük (lásd az A.7.2 feladatot).

Az egyik legfontosabb eset az egész együtthatós polinomok vizsgálata. Itt most csak a számelméleti vonatkozásokra térünk ki. A kommutatív test feletti polinomokhoz képest két lényeges különbséget emelünk ki: az egész együtthatós polinomok körében csak a ± 1 egység, továbbá nincs maradékos osztás.

Vizsgáljuk meg részletesebben a maradékos osztás kérdését. Könnyen adódik, hogy ha pl. az $f = x$ polinomot a $g = 2$ polinommal akarjuk maradékosan elosztani, akkor nem tudjuk biztosítani, hogy az r maradék a nulla

polinom vagy az osztónál kisebb fokú polinom legyen. Ez azonban nyitva hagyja azt a lehetőséget, hogy a fokszám helyett valamilyen más euklideszi függvény szerint talán mégis létezik maradékos osztás. Megmutatjuk, hogy nem ez a helyzet. Ha ugyanis lenne maradékos osztás, akkor az x és 2 legnagyobb közös osztója, az 1, előállna $1 = xu + 2v$ alakban alkalmas u és v *egész* együtthatós polinomokkal. Ez azonban lehetetlen, hiszen a jobb oldal konstans tagja páros.

Noha nincs maradékos osztás, a számelmélet alaptétele mégis érvényes az egész együtthatós polinomokra. Ez lényegében abból következik, hogy a II. Gauss-lemma alapján egy egész együtthatós polinom pontosan akkor irreducibilis az egész együtthatós polinomok körében, ha vagy egy olyan p konstans polinom, ahol p prímszám, vagy pedig egy olyan primitív polinom, amely irreducibilis a racionális test felett. Ez ugyanis azt jelenti, hogy az egészek feletti irreducibilitás visszavezethető a racionálisok feletti irreducibilitásra, és így a racionális test feletti felbontás egyértelműségéből kapjuk, hogy ugyanez érvényes az egészek felett is.

Megjegyzés: Végül felhívjuk még a figyelmet a 3.2.4 Tételben tárgyalt *interpolációs polinom*okra és az ahhoz kapcsolódó 3.2.7–3.2.15 feladatokra.

Feladatok

T végig kommutatív testet jelöl.

A.7.1 Legyen T *tetszőleges* véges test.

(a) Bizonyítsuk be, hogy léteznek olyan T feletti különböző polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik.

(b) (Folytatás.) Sőt az is igaz, hogy *minden* polinomfüggvényhez *végtelen* sok olyan polinom található, amelyhez az adott polinomfüggvény tartozik.

A.7.2 Mutassuk meg, hogy az alábbi állítások az olyan polinomokra is igazak maradnak, amikor az együtthatókat (egy kommutatív test helyett) egy kommutatív, egységelemes, nullosztómentes gyűrűből vesszük.

I. Két polinom szorzatának a foka a tényezők fokszámának az összege.

II. Egy f polinomhoz tartozó polinomfüggvénynek pontosan akkor gyöke a γ, ha az f polinomból kiemelhető az $x - \gamma$ gyöktényező.

III. Egy n-edfokú polinomnak legfeljebb n gyöke van.

Melyik állítás(ok) marad(nak) igaz(ak) olyan kommutatív, egységelemes gyűrű esetén, amelyben nullosztók is előfordulnak?

A.7.3 Legyen T tetszőleges *véges* test.

(a) Ellenőrizzük, hogy a $T \to T$ polinomfüggvények valóban gyűrűt alkotnak a függvények szokásos összeadására és szorzására nézve.

(b) Mutassuk meg, hogy ebben a gyűrűben mindig találhatók nullosztók.

*(c) Határozzuk meg a nullosztók számát.

A.7.4 Mutassuk meg, hogy bármely T végtelen kommutatív test esetén létezik olyan $T \to T$ függvény, amely nem polinomfüggvény (vö. a 3.2.14 feladattal).

A.7.5 Egy G tizedfokú egész együtthatós polinomról tudjuk, hogy $G(n)$ minden egész n-re osztható 11-gyel. Bizonyítsuk be, hogy ekkor szükségképpen G minden együtthatója is osztható 11-gyel.

A.7.6

(a) A valós számok milyen részhalmazai léphetnek fel egy valós együtthatós polinomfüggvény értékkészleteként?

(b) A komplex számok milyen részhalmazai léphetnek fel egy komplex együtthatós polinomfüggvény értékkészleteként?

A.7.7 Adott egy tetszőleges $f = a_0 + a_1x + \ldots + a_nx^n$ egész együtthatós, legalább másodfokú polinom, amelyben $a_0 \neq 0, a_n \neq 0$. Megvizsgáljuk, hogy a polinom egyetlen együtthatójának a megváltoztatása hogyan befolyásolja azt, hogy létezik-e racionális gyök. Bizonyítsuk be az alábbi állításokat:

(a) Az a_0 helyére végtelen sok egész szám írható úgy, hogy a keletkező polinomnak legyen racionális gyöke.

(b) Az a_n helyére végtelen sok egész szám írható úgy, hogy a keletkező polinomnak legyen racionális gyöke.

(c) Bármely (rögzített) $1 \leq i \leq n-1$ esetén az a_i helyére legalább egy, de legfeljebb véges sok egész szám írható úgy, hogy a keletkező polinomnak legyen racionális gyöke.

(d) Bármely (rögzített) i esetén az a_i helyére végtelen sok *racionális* szám írható úgy, hogy a keletkező polinomnak legyen racionális gyöke.

(e) (Most két együtthatót változtatunk.) Bármely (rögzített) $i \neq j$ esetén az a_i és a_j helyére végtelen sok egész számpár írható úgy, hogy a keletkező polinomnak legyen racionális gyöke.

M*(f) Bármely (rögzített) i esetén az a_i helyére helyére végtelen sok egész szám írható úgy, hogy a keletkező polinomnak *ne* legyen racionális gyöke.

A.7.8 Bizonyítsuk be, hogy az $1+x+x^2/2+x^3/6+\ldots+x^n/(n!)$ polinomnak n különböző komplex gyöke van.

A.7.9 Adjunk (a gyakorlatban is megvalósítható elvi) eljárást olyan ötödfokú komplex együtthatós polinomok gyökeinek a (pontos) meghatározására, amelyeknek van többszörös gyökük.

A.7.10 Bizonyítsuk be, hogy egy, a racionális test felett irreducibilis polinomnak a komplex számok körében sem lehet többszörös gyöke.

A.7.11 Mutassuk meg, hogy egy f komplex együtthatós polinomnak akkor és csak akkor van többszörös gyöke, ha f és f' nem relatív prímek, azaz $(f, f') \neq 1$.

A.7.12 Jellemezzük azokat a komplex együtthatós polinomokat, amelyek oszthatók a deriváltjukkal.

A.7.13 Legyen F egy tetszőleges egész együtthatós, 28-adfokú polinom. Melyek igazak az alábbi állítások közül?

(a) F-nek biztosan van 17-edfokú osztója $\mathbf{C}[x]$-ben.
(b) F-nek biztosan van 17-edfokú osztója $\mathbf{R}[x]$-ben.
(c) F-nek biztosan van 18-adfokú osztója $\mathbf{R}[x]$-ben.
(d) F-nek biztosan van 18-adfokú osztója $\mathbf{Q}[x]$-ben.

A.7.14

(a) Legyen f és g minden együtthatója egész szám. Ekkor f-et és g-t tekinthetjük akár egész, akár racionális, akár komplex, akár F_2-beli együtthatós polinomnak. Így az $f \mid g$-nek négy különböző értelmezése van. Milyen kapcsolatban állnak egymással ezek az oszthatóságok?

(b) Mennyiben változik a helyzet, ha f és g minden együtthatója 0 vagy 1?

A.7.15 Bizonyítsuk be, hogy bármely m, n, k természetes számokra

$$x^2 + x + 1 \mid x^{3m} + x^{3n+1} + x^{3k+2}\,.$$

A.7.16 Határozzuk meg az $x^n - 1$ és $x^k - 1$ polinomok legnagyobb közös osztóját.

A.7.17 Van-e olyan 10-edfokú valós együtthatós polinom, amelynek az x^5+2 és $2x^6 + 3x + 1$ polinomokkal való osztási maradéka megegyezik?

A.7.18 A következő „diofantikus” egyenletet vizsgáljuk: adottak az $f, g, h \in T[x]$ polinomok, és olyan $u, v \in T[x]$ polinomokat keresünk,

amelyekre $fu+gv=h$. Mi a megoldhatóság feltétele, hány megoldás van, és hogyan kapjuk meg az összes megoldást?

A.7.19 Legyen f racionális együtthatós polinom. Igazak-e az alábbi állítások?

I. Ha f irreducibilis $\mathbf{Q}$ felett, akkor f-nek nincs racionális gyöke.

II. Ha f-nek nincs racionális gyöke, akkor f irreducibilis $\mathbf{Q}$ felett.

Mennyiben változik a helyzet, ha f fokszámára alkalmas pótlólagos kikötéseket teszünk?

A.7.20 Bontsuk fel az x^4+1 polinomot irreducibilisek szorzatára az alábbi testek fölött:

(a) $\mathbf{C}$; (b) $\mathbf{R}$; (c) $\mathbf{Q}$; (d) F_2; (e) F_3.

A.7.21 Adjunk meg olyan c pozitív egészt, amelyre az 1^4+c, 2^4+c, 3^4+c, …, n^4+c, … számok valamennyien összetettek.

A.7.22 Az alábbi polinomok közül melyek irreducibilisek a racionális test felett:

(a) x^2+2500; (b) x^4+2500; (c) x^4+3000; (d) $x^4+100000$.

*A.7.23 Bizonyítsuk be, hogy ha $a_1,\dots,a_k$ különböző egész számok, akkor az $(x-a_1)\cdot\ldots\cdot(x-a_k)-1$ polinom irreducibilis a racionális test felett.

A.7.24 Hogyan kapjuk meg Φ_m-ből Φ_{2m}-et (ahol Φ_j a j-edik körosztási polinomot jelöli)?

*A.7.25 Bizonyítsuk be, hogy az m-edik körosztási polinom

$$\Phi_m=\frac{(x^m-1)\cdot\prod_{p,q}(x^{m/pq}-1)\cdot\ldots}{\prod_p(x^{m/p}-1)\cdot\prod_{p,q,r}(x^{m/pqr}-1)\cdot\ldots}$$

alakba írható, ahol $p,q,r,\dots$ az m különböző prímosztói.

A.7.26

(a) Adjuk meg az $f=x^{4k}+x^{3k}+x^{2k}+x^k+1$ polinom gyökeit.

(b) Milyen k értékekre lesz f valamelyik körosztási polinom?

*A.7.27 Az egységsugarú körbe írt szabályos n-szögben mennyi az egyik csúcsból kiinduló összes (azaz $n-1$ darab) oldal és átló hosszának a szorzata?

A.7.28 Tegyük fel, hogy az $f=x^n+\alpha_{n-1}x^{n-1}+\ldots+\alpha_0$ valós együtthatós polinomban $\alpha_{n-1}^2-2\alpha_{n-2}<0$. Bizonyítsuk be, hogy f-nek van olyan komplex gyöke, amely nem valós.

A.7.29 Adjunk szükséges és elégséges feltételt arra, hogy az ax^3+bx^2+cx+ $+d=0$ $(a\neq 0)$ komplex együtthatós harmadfokú egyenlet (komplex) gyökei számtani sorozatot alkossanak.

A.7.30 Egy egész együtthatós polinom főegyütthatója 1 és minden (komplex) gyök 1-nél kisebb abszolút értékű. Adjuk meg a polinom többi együtthatóját.

A.8. Csoport

A.8.1 Definíció

Egy G nem üres halmazt *csoport*nak nevezünk, ha értelmezve van G-n egy asszociatív művelet, létezik egységelem és minden elemnek van inverze.

♣

Ugyanehhez a fogalomhoz jutunk, ha — a testnél és gyűrűnél látottakhoz hasonlóan, az A.4.7 Tétel alapján — az egységelemre és inverzre vonatkozó kikötés helyett a művelet (mindkét oldali) invertálhatóságát írjuk elő.

A csoport egységelemét általában e-vel, egy g csoportelem inverzét g^{-1}-gyel jelöljük. Ha a művelet kommutatív, akkor *kommutatív csoport*ról vagy *Abel-csoport*ról beszélünk.

Példák csoportra

P1. Bármely gyűrű (így speciálisan bármely test is) az összeadásra nézve kommutatív csoportot alkot. Ennek megfelelően Abel-csoportot alkotnak a szokásos összeadásra az egész, a páros, a racionális, a valós vagy a komplex számok, a (megfelelő) mátrixok, polinomok, függvények, a modulo m maradékosztályok stb.

P2. Bármely (akár nem kommutatív) test nem nulla elemei a szorzásra csoportot alkotnak. Ennek megfelelően a **nem nulla(!)** racionális, valós vagy komplex számok, a nem nulla maradékosztályok modulo p (ahol p prím) stb. a szokásos szorzásra csoportot alkotnak.

P3. Egységelemes gyűrű esetén csoportot alkotnak a szorzásra azok az elemek, amelyeknek létezik inverze. Ennek a testre vonatkozó speciális esete éppen a P2 példa. Két másik fontos speciális esetet kapunk a négyzetes mátrixok, illetve a modulo m maradékosztályok gyűrűjéből: csoportot alkotnak a szorzásra egy T test feletti $n\times n$-es invertálható mátrixok, illetve a modulo m redukált maradékosztályok, tehát amelyek elemei relatív prímek m-hez.

P4. A komplex számoknak sok olyan részhalmaza van, amely a szorzásra nézve csoport, tekintsük pl. az n-edik egységgyököket, az összes egységgyököt, illetve az 1 abszolút értékű komplex számokat.

P5. Az $\{1, 2, \ldots, n\}$ halmaz önmagára történő kölcsönösen egyértelmű leképezései (azaz bijekciói) csoportot alkotnak a kompozícióra (összetételre, egymás után alkalmazásra) nézve. Ezt a csoportot n-edfokú *szimmetrikus csoport*nak nevezzük és S_n-nel jelöljük. Az S_n csoport tehát az $1, 2, \ldots, n$ elemek *permutáció*iból áll, $|S_n| = n!$.

P6. A sík vagy a tér összes egybevágóságai, illetve hasonlóságai (azaz a távolságtartó, illetve aránytartó transzformációk) a kompozícióra nézve csoportot alkotnak. Szintén csoportot kapunk, ha csak speciális egybevágóságokat tekintünk, pl. a síkban az összes eltolást, egy adott pont körüli összes forgatást stb. (a művelet továbbra is a kompozíció).

P7. Egy sík-, illetve térbeli alakzat *szimmetriacsoport*ját azok a sík-, illetve téregybevágóságok alkotják, amelyek az adott alakzatot önmagába viszik át, a művelet pedig a kompozíció. Például egy szabályos n-szög szimmetriacsoportja az n darab szimmetriatengelyre történő tükrözésből és a középpont körüli $2k\pi/n$ szögű elforgatásokból áll, ahol $k = 0, 1, \ldots, n-1$. A 0 szögű elforgatás a helybenhagyás vagy identikus leképezés, ami a csoport egységeleme. Ezt a csoportot D_n-nel jelöljük és *diédercsoport*nak nevezzük, $|D_n| = 2n$. Ha a $2\pi/n$ szögű forgatást f-fel és az egyik szimmetriatengelyre történő tükrözést t-vel jelöljük, akkor D_n elemei egyértelműen felírhatók $t^i f^j, 0 \le i \le 1, 0 \le j \le n-1$ alakban és a szorzást a $t^2 = f^n = e$ és $ft = tf^{n-1}$ szabályok szerint kell végezni.

Egy csoportban bármely elem tetszőleges *egész kitevőjű hatvány*ait a szokásos módon definiáljuk: ha n pozitív egész, akkor g^n egy olyan n-tényezős szorzat, amelynek minden tényezője g, továbbá $g^0 = e$ és $g^{-n} = (g^n)^{-1}$. (A racionális, valós stb. kitevőjű hatványozásnak egy csoportban általában *nincs értelme*.) Az $a^m a^k = a^{m+k}$ és $(a^m)^k = a^{mk}$ hatványazonosságok csoportban is érvényesek (ahol a a csoport tetszőleges eleme, a k és m kitevők pedig tetszőleges egész számok, negatívak és nullák is lehetnek), azonban $(ab)^m = a^m b^m$ már nem mindig teljesül, hiszen a szorzás nem feltétlenül kommutatív.

A.8.2 Definíció

Egy G csoportban egy g *elem rendje* az a *legkisebb* olyan n *pozitív* egész szám, amelyre $g^n = e$ (ahol e a csoport egységeleme), illetve ha nincs ilyen n, akkor g rendje végtelen. ♣

A g elem rendjét $o(g)$-vel jelöljük (ezt „ordo g”-nek olvassuk). Például

D_n-ben $o(f) = n, o(t) = 2$, az egész számok additív csoportjában a nullán kívül minden elem rendje végtelen.

A rendfogalom két fontos speciális esetét kapjuk, ha a nem nulla komplex számok, illetve a modulo m redukált maradékosztályok multiplikatív csoportját tekintjük. A második esetben ezzel pontosan a kongruenciáknál tanult rendfogalomhoz jutunk. Az első csoportban a véges rendű elemek éppen az egységgyökök lesznek.

Bármely csoportban érvényes, hogy egy n-edrendű elem két hatványa akkor és csak akkor egyenlő, ha a kitevők kongruensek modulo n, egy végtelen rendű elemnek pedig csak az azonos kitevőjű hatványai egyeznek meg. Ebből következik, hogy minden elemnek pontosan annyi különböző hatványa van, mint amennyi a rendje.

A.8.3 Definíció

Egy csoport *ciklikus*, ha egyetlen elem (összes egész kitevőjű) hatványaiból áll. Egy ilyen elemet a ciklikus csoport *generátorelem*ének nevezünk. ♣

A g által generált ciklikus csoportot $\langle g \rangle$-vel jelöljük. A rendnél elmondottak szerint $|\langle g \rangle| = o(g)$. Így ha $o(g) = n$, akkor $\langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ (és a felsorolt elemek mind különbözők). Ha $o(g) = \infty$, akkor a g-nek minden hatványa különböző (beleértve a negatív egész kitevőjű hatványokat is).

Ciklikus csoportot alkotnak az egész számok vagy a modulo m maradékosztályok az összeadásra, (az egyik) generátorelem az 1. Ugyancsak ciklikus az n-edik egységgyökök, valamint ha p prím, akkor a modulo p redukált maradékosztályok multiplikatív csoportja. Az előbbi generátorelemei a *primitív n-edik egységgyök*ök, az utóbbié pedig a modulo p *primitív gyök*ök.

Mivel egy elem hatványai egymással felcserélhetők, ezért egy ciklikus csoport biztosan kommutatív. Így egy nem kommutatív csoport sohasem lehet ciklikus.

A kommutatív csoportok közül nem ciklikus pl. a racionális, a valós vagy a komplex számok additív csoportja, illetve a nem nulla racionális, valós vagy komplex számok multiplikatív csoportja, vagy a véges csoportok körében a téglalap szimmetriacsoportja, az F_p test feletti véges dimenziós vektorterek additív csoportja, a modulo 15 redukált maradékosztályok multiplikatív csoportja stb. Belátható, hogy a modulo m redukált maradékosztályok multiplikatív csoportja akkor és csak akkor ciklikus (azaz akkor és csak akkor létezik primitív gyök modulo m), ha $m = 2, 4, p^k$ vagy $2p^k$, ahol p egy páratlan prím és $k \geq 1$.

A.8.4 Definíció

Egy G csoport *részcsoport*jának egy olyan $H \subseteq G$ részhalmazt nevezünk, amely maga is csoport a G-beli műveletre (pontosabban annak megszorítására) nézve. ♣

Belátható, hogy G-nek egy H nem üres részhalmaza akkor és csak akkor részcsoport, ha zárt a G-beli műveletre és inverzképzésre nézve (azaz $r, s \in H \Rightarrow rs \in H, r^{-1} \in H$).

Példák: A valós együtthatós polinomok additív csoportjában részcsoportot alkotnak az egész együtthatós polinomok, a legfeljebb ötödfokú polinomok (ideértve a 0 polinomot is), az $x^2 + 1$-gyel osztható polinomok stb. Bármely G csoportban részcsoport maga a G, valamint a csak az egységelemből álló részhalmaz (ezt a továbbiakban $\{e\}$ helyett röviden e-vel jelöljük); ezeket *triviális részcsoport*oknak nevezzük. Bármely elem összes (egész kitevőjű) hatványai is részcsoportot alkotnak, ez az adott elem által generált ciklikus részcsoport.

A.8.5 Definíció

Legyen H részcsoport G-ben és $g \in G$ tetszőleges elem. Ekkor a $gH = \{gh \mid h \in H\}$ halmazt H szerinti *bal oldali mellékosztály*nak nevezzük. ♣

Belátható, hogy két, H szerinti bal oldali mellékosztály vagy diszjunkt, vagy egybeesik, továbbá a bal oldali mellékosztályok egyesítése éppen G. A (különböző) bal oldali mellékosztályok számát a H részcsoport G-beli *index*ének nevezzük és $|G : H|$-val jelöljük.

Hasonló módon definiálhatók a H szerinti *jobb* oldali mellékosztályok is. Ezek általában nem esnek egybe a bal oldali mellékosztályokkal, azonban megmutatható, hogy a számuk ugyanannyi, azaz $|G : H|$.

Legyen a továbbiakban G véges csoport. Mivel minden (pl. bal oldali) mellékosztály elemszáma $|H|$, az előzőekből következik, hogy $|G| = |H| \cdot |G : H|$. Innen azonnal adódik:

A.8.6 Tétel (Lagrange tétele)

Egy véges csoport bármely részcsoportjának elemszáma osztója a csoport elemszámának. ♣

Egy csoport elemszámát a csoport rendjének is szokás nevezni.

Mivel egy elem rendje megegyezik az általa generált ciklikus részcsoportnak az elemszámával, ezért a Lagrange-tétel alapján bármely g-re $o(g) \,\big|\, |G|$

is teljesül. Ez a rend tulajdonságai alapján $g^{|G|} = e$-vel ekvivalens. Ha speciálisan G a modulo m redukált maradékosztályok multiplikatív csoportja, akkor így éppen az Euler–Fermat-tételt kapjuk.

Végül megemlítjük, hogy más algebrai struktúrákhoz hasonlóan két csoportot akkor nevezünk *izomorf*nak, ha létezik közöttük művelettartó(!) bijekció. Például a valós számok additív és a pozitív valós számok multiplikatív csoportja izomorf, ugyanis az $x \mapsto 2^x$ megfeleltetés bijektív és művelettartó. Két ciklikus csoport pontosan akkor izomorf, ha azonos az elemszámuk.

Feladatok

G végig csoportot jelöl.

*A.8.1 Hány eleműek a szabályos testek szimmetriacsoportjai?

A.8.2 Bizonyítsuk be, hogy G akkor és csak akkor kommutatív, ha minden $a, b \in G$ esetén $(ab)^2 = a^2b^2$. Igaz-e hasonló állítás, ha a négyzetek helyett $(ab)^4 = a^4b^4$ teljesül (minden $a, b \in G$-re)?

A.8.3 Bizonyítsuk be, hogy kommutatív csoportban $o(ab) \,\big|\, [o(a)\,,\, o(b)]$.

A.8.4 Lehet-e két véges rendű elem szorzata végtelen rendű?

A.8.5 Melyek igazak az alábbi állítások közül?

(a) Ha $|G| < \infty$, akkor G minden eleme véges rendű.

(b) Ha G minden eleme véges rendű, akkor $|G| < \infty$.

(c) Ha $2 \,\big|\, |G|$, akkor G-ben van másodrendű elem.

(d) Ha $4 \,\big|\, |G|$, akkor G-ben van negyedrendű elem.

A.8.6 Lássuk be, hogy bármely $k, s > 1$ egész számokra $s \,|\, \varphi(k^s - 1)$, ahol $\varphi(n)$ az Euler-féle φ-függvény.

*A.8.7 Mivel egyenlő egy véges kommutatív csoport elemeinek a szorzata? Melyik nevezetes kongruenciatételt általánosítja ez a feladat?

A.8.8 Melyek izomorfak az alábbi csoportok közül?

(a) A modulo 15 redukált maradékosztályok a szorzásra;

(b) a modulo 16 redukált maradékosztályok a szorzásra;

(c) a modulo 24 redukált maradékosztályok a szorzásra;

(d) a modulo 16 nem redukált maradékosztályok az összeadásra;

(e) a nyolcadik komplex egységgyökök a szorzásra;

(f) a $\pm 1, \pm i, \pm j, \pm k$ kvaterniók a szorzásra (lásd az 5.6 pont P5 példáját);

(g) a modulo 4 maradékosztályok feletti $\begin{pmatrix} 1 & c \\ 0 & \pm 1 \end{pmatrix}$ alakú mátrixok a szorzásra;

(h) T^3 az összeadásra, ahol T az F_2 test;

(i) a négyzet szimmetriacsoportja;

(j) a(z általános) téglatest szimmetriacsoportja.

*A.8.9

(a) Bizonyítsuk be, hogy ha $|G_1| = |G_2|$ és mindkét csoportban az egységelemen kívül minden elem rendje 2, akkor G_1 és G_2 izomorf.

(b) Az előző állítás nem marad igaz, ha az elemek rendje 3.

M A.8.10

(a) Melyek azok a csoportok, amelyeknek csak triviális részcsoportjaik vannak?

(b) Melyek azok a csoportok, amelyeknek csak véges sok részcsoportjuk van?

A.8.11 Mutassunk példát olyan csoportra, amely előáll három valódi részcsoportjának az egyesítéseként. Van-e ilyen tulajdonságú páratlan elemszámú csoport is?

*A.8.12 Hány részcsoportja van (a) egy n elemű ciklikus csoportnak; (b) D_n-nek?

*A.8.13 Lássuk be, hogy egy csoportban egy M nem üres részhalmaz akkor és csak akkor lesz valamely részcsoport szerinti bal oldali mellékosztály, ha $a, b, c \in M \Rightarrow ab^{-1}c \in M$.

A.9. Ideál és maradékosztálygyűrű

A.9.1 Definíció

Egy R gyűrűben egy nem üres $I \subseteq R$ részhalmazt az R *ideál*jának nevezünk, ha

(i) I zárt az (R-beli) összeadásra és ellentettképzésre, azaz

$$i, j \in I \Rightarrow i + j \in I, -i \in I;$$

(ii) bármely I-beli elemet egy tetszőleges R-beli elemmel akármelyik oldalról megszorozva ismét I-beli elemet kapunk, azaz

$$i \in I, r \in R \Rightarrow ri \in I, ir \in I. \ \clubsuit$$

Az ideál fogalma könnyen láthatóan ekvivalens azzal, hogy I olyan részgyűrű, ahol egy I-beli és egy I-n kívüli elem szorzata *is* I-beli (a részgyűrű definícióját lásd az A.6.10 feladatban).

Példák: Ideált alkotnak az egész számok gyűrűjében az m-mel osztható számok, a valós együtthatós polinomok gyűrűjében egy adott g-vel osztható polinomok, az egész együtthatós polinomok gyűrűjében azok a polinomok, amelyeknek a konstans tagja páros szám. Nem alkotnak ideált (de részgyűrűt igen) a valós együtthatós polinomok gyűrűjében a konstans polinomok vagy az egész együtthatós polinomok. Testben csak a két triviális ideál létezik (maga a test és a csak a nullából álló részhalmaz).

Az ideálok legegyszerűbb és egyben legfontosabb típusát az egyetlen elem által generált ideálok, más néven *főideál*ok jelentik. Ezek vizsgálatánál kényelmi okokból csak kommutatív és egységelemes gyűrűkre szorítkozunk.

A.9.2 Definíció

Legyen R kommutatív és egységelemes gyűrű, $a \in R$ tetszőleges. Ekkor az $\{ra \,|\, r \in R\}$ halmazt az a által generált *főideál*nak nevezzük és (a)-val jelöljük. ♣

Az a által generált (a) főideál tehát az a elem „többszöröseiből" áll.

A definícióban szereplő „a által generált" és „ideál" szóhasználat jogosságát az alábbi tétel mutatja:

A.9.3 Tétel

Egy R kommutatív és egységelemes gyűrűben az $(a) = \{ra \,|\, r \in R\}$ halmazra az alábbi tulajdonságok teljesülnek:

(i) (a) ideál R-ben;
(ii) $a \in (a)$;
(iii) ha I ideál R-ben és $a \in I$, akkor szükségképpen $(a) \subseteq I$. ♣

Az (a) főideál tehát az a elemet tartalmazó *legszűkebb* ideál.

Az A.9.1 Definíció utáni három példa közül a harmadik nem főideál (lásd az A.9.9c feladatot), az első kettő viszont igen, (egyik) generátorelemük az m, illetve a g. Nem is meglepő, hogy az ebből a két gyűrűből választott ideálpéldáink főideálok voltak, ugyanis érvényes az alábbi tétel:

A.9.4 Tétel

Az egész számok gyűrűjében, illetve a T kommutatív test feletti $T[x]$ polinomgyűrűben minden ideál főideál. ♣

Az A.9.4 Tétel állítása minden olyan kommutatív, nullosztómentes, egységelemes gyűrűben igaz, ahol elvégezhető a maradékos osztás (azaz minden *euklideszi gyűrű* egyben *főideálgyűrű* is — ezeknek a fogalmaknak a pontos definiálását az Olvasóra bízzuk).

Az eddigiekből is érezhető, hogy az ideálok szorosan kapcsolódnak a számelmélethez. Valójában onnan is származnak: eredetileg a Fermat-sejtés kapcsán vezette be Kummer német matematikus az „ideális szám" fogalmát. Néhány számelméleti vonatkozást az A.9.10 feladatban tárgyalunk.

Most rátérünk az ideál szerinti faktorgyűrű konstrukciójára. Ez a fogalom a modulo m maradékosztályok gyűrűjének az általánosítása.

Mint láttuk, az egész számok $\mathbf{Z}$ gyűrűjében az m-mel osztható számok egy I ideált alkotnak. Ekkor a c egész számot tartalmazó modulo m maradékosztály éppen a $c+I = \{c+i \mid i \in I\} = \{c+km \mid k \in \mathbf{Z}\}$ halmaz, itt a c ennek a maradékosztálynak egy reprezentánsa. A maradékosztályok összeadását és szorzását a reprezentánsok segítségével értelmeztük, ami ebben a felírásban a következőket jelenti: $(c+I)+(d+I) = (c+d)+I, (c+I)(d+I) = cd+I$. Be kellett látni, hogy ezek a hozzárendelések az *osztályokra* valóban műveleteket definiálnak, azaz az eredményül kapott osztály *egyértelmű*, *nem függ* attól, hogy az egyes osztályokból melyik *reprezentáns*okat választottuk. Ha végigelemezzük ennek a bizonyítását, akkor kiderül, hogy a szóban forgó egyértelműséget éppen I ideál volta biztosítja. Mindezek alapján a következő általánosítást kapjuk.

A.9.5 Tétel

Legyen I ideál az R gyűrűben. Ekkor az I szerinti (különböző) $c+I = \{c+i \mid i \in I\}$ *maradékosztály*ok a

$$(c+I)+(d+I) = c+d+I, \qquad (c+I)(d+I) = cd+I$$

módon definiált összeadásra és szorzásra nézve gyűrűt alkotnak. Ezt a gyűrűt az R-nek az I szerinti *maradékosztálygyűrű*jének vagy *faktorgyűrű*jének nevezzük és R/I-vel jelöljük. ♣

A faktorgyűrű nulleleme nyilván a $0+I$ maradékosztály, azaz maga az I ideál.

Megjegyezzük, hogy egy $c+I$ maradékosztály éppen az R additív csoportjának az I additív részcsoport szerinti egyik mellékosztálya (mindegy, hogy melyik oldali, hiszen a gyűrűben az összeadás mindig kommutatív). Ennek megfelelően az I szerinti (különböző) maradékosztályok az R-nek egy diszjunkt felbontását adják.

A továbbiakban egy T kommutatív test feletti $T[x]$ polinomgyűrű faktorgyűrűit vizsgáljuk. Az A.9.4 Tétel szerint $T[x]$-ben minden ideál főideál. Legyen $I = (g)$, ahol $g \neq 0$. Ekkor éppen azok a polinomok kerülnek egy maradékosztályba, amelyek ugyanazt a maradékot adják g-vel osztva. Ily módon — az egész számoknál tapasztaltakhoz teljesen hasonlóan — minden maradékosztály egyértelműen jellemezhető egy „maradékkal", azaz egy legfeljebb $\deg g - 1$-edfokú polinommal (idesorolva a 0 polinomot is, amely magát az I-t reprezentálja). A $T[x]/(g)$ maradékosztálygyűrűben tulajdonképpen ezekkel a maradékokkal számolunk, azaz pl. két maradékosztály szorzásakor ezeket a maradékokat összeszorozzuk és vesszük a szorzatnak a g-vel való osztási maradékát (pontosan ugyanúgy, ahogy pl. modulo 15 a 7-nek és a 6-nak a szorzata 12).

Tekintsük példaként az $\mathbf{R}[x]/(x^2+1)$ maradékosztálygyűrűt. Itt minden maradékosztályt egyértelműen reprezentálhatunk egy legfeljebb elsőfokú $a+bx$ (valós együtthatós) polinommal, amelyet az x^2+1 polinommal való osztási maradéknak tekintünk. Ennek megfelelően az összeadást az

$$(a+bx)+(c+dx) = (a+c)+(b+d)x,$$

a szorzást pedig az

$$\begin{aligned}(a+bx)(c+dx) &= ac+(ad+bc)x+bdx^2 = \\ &= ac+(ad+bc)x-bd+bd(x^2+1) = (ac-bd)+(ad+bc)x\end{aligned}$$

szabály szerint kell végezni, azaz pontosan ugyanúgy, ahogyan a komplex számoknál (képzeljünk az „x" betű helyére mindenhol „i" betűt). Ezzel beláttuk, hogy az $\mathbf{R}[x]/(x^2+1)$ maradékosztálygyűrű test és izomorf $\mathbf{C}$-vel.

Az alábbi tétel pontos választ ad arra, hogy egy $T[x]/(g)$ maradékosztálygyűrű mikor test.

A.9.6 Tétel

Legyen T kommutatív test és $g \in T[x]$ tetszőleges polinom. A $T[x]/(g)$ maradékosztálygyűrű akkor és csak akkor test, ha g irreducibilis T felett. ♣

Feladatok

A.9.1 Tekintsünk egy tetszőleges additív Abel-csoportot, és definiáljuk ebben a szorzást úgy, hogy bármely két elem szorzata a nullelem legyen. Bizonyítsuk be, hogy így egy gyűrűt kapunk. Mik lesznek az ideálok? (Az ilyen gyűrűket *zérógyűrű*nek nevezzük.)

A.9.2 Melyek azok az m természetes számok, amelyekre a modulo m maradékosztályok gyűrűjében a nullosztók és a nulla egy ideált alkotnak?

A.9.3

(a) Vegyünk egy nullosztómentes gyűrűben akárhány (de véges sok) nem nulla ideált (azaz az ideálok egyike se álljon csak magából a nullelemből). Lássuk be, hogy ekkor az ideálok metszete sem nulla.

(b) Mutassunk példát olyan gyűrűre, amelyben előfordul, hogy két nem nulla ideál metszete nulla.

(c) Adjunk meg olyan gyűrűt is, amelyben vannak nullosztók, de véges sok nem nulla ideál metszete sohasem lehet nulla.

A.9.4

(a) Igazoljuk, hogy egy testnek csak triviális ideáljai vannak.

(b) Tegyük fel, hogy az R kommutatív gyűrűben csak triviális ideálok vannak, és van két olyan elem, amelyek szorzata nem nulla (azaz R nem zérógyűrű). Bizonyítsuk be, hogy R test.

(c) Mutassuk meg, hogy a $T^{n\times n}$ mátrixgyűrűnek csak triviális ideáljai vannak. [Ebből látszik, hogy (b)-ben a kommutativitási feltétel lényeges szerepet játszik.]

A.9.5 Jelöljük a modulo m maradékosztályok gyűrűjét $\mathbf{Z}_m$-mel.

(a) Bizonyítsuk be, hogy $\mathbf{Z}_m$-ben minden ideál főideál.

*(b) Legyen $k \mid m$. Mi a szükséges és elégséges feltétele annak, hogy a (k) főideál mint gyűrű izomorf legyen $\mathbf{Z}_{m/k}$-val? [Itt (k) értelemszerűen azt a főideált jelöli $\mathbf{Z}_m$-ben, amelyet a k-t tartalmazó modulo m maradékosztály generál.]

*(c) Bizonyítsuk be, hogy bármely $k \mid m$ esetén a $\mathbf{Z}_m/(k)$ faktorgyűrű izomorf $\mathbf{Z}_k$-val.

A.9.6 Bizonyítsuk be az A.9.3–A.9.6 Tételeket

A.9.7 A főideál általánosításaként bevezetjük a *végesen generált ideál* fogalmát. Legyen R kommutatív, egységelemes gyűrű, $a_1, \dots, a_k \in R$, és legyen $(a_1, \dots, a_k) = \{\sum_{i=1}^{k} r_i a_i \mid r_i \in R\}$. Fogalmazzuk meg és bizonyítsuk be az A.9.3 Tétel megfelelőjét az $a_1, \dots, a_k$ elemek által generált $(a_1, \dots, a_k)$ ideálra.

A.9.8 Jelöljük az A.6 pont P7 példájában szereplő gyűrűt R_H-val.

(a) Jellemezzük a főideálokat R_H-ban.

(b) Mutassuk meg, hogy ha H véges, akkor R_H-ban minden ideál főideál.

(c) Bizonyítsuk be, hogy végtelen H esetén H összes véges részhalmaza olyan ideált alkot R_H-ban, amely nem főideál, sőt nem is végesen generált ideál.

(d) Legyen $A \subseteq H$ tetszőleges. Igazoljuk, hogy az $R_H/(A)$ faktorgyűrű $R_{H\setminus A}$-val izomorf.

A.9.9 Adjuk meg egyszerűbb alakban az alábbi, két elemmel generált ideálokat. Melyek lesznek közülük főideálok? Határozzuk meg a szerintük vett faktorgyűrűket is.

(a) Az egész számok gyűrűjében $(30, 42)$.

(b) A modulo 100 maradékosztályok gyűrűjében $(30, 42)$.

(c) Az egész együtthatós polinomok gyűrűjében $(2, x)$.

A.9.10 Legyen R kommutatív, nullosztómentes, egységelemes gyűrű, és definiáljuk az oszthatóságot, az egységeket és a legnagyobb közös osztót a szokásos módon. A kerek zárójelek most mindig a generált ideált, a, b, d pedig az R gyűrű elemeit jelölik. [Tehát (a, b) az a és b által generált ideál, nem pedig az a és b legnagyobb közös osztója — bár a két fogalom között szoros kapcsolat áll fenn, lásd a feladat (c)–(e) részét.] Bizonyítsuk be az alábbi állításokat:

(a) $a \mid b \iff (b) \subseteq (a)$.

(b) $(a) = (b) \iff a$ és b egymás egységszeresei.

(c) Ha $(a, b) = (d)$, akkor d az a és b legnagyobb közös osztója.

(d) Az egész számok gyűrűjében vagy egy T kommutatív test feletti $T[x]$ polinomgyűrűben a (c)-beli állítás megfordítása is igaz.

(e) Az egész együtthatós polinomok gyűrűjében a (c)-beli állítás megfordítása nem igaz.

A.9.11 Legyen R az egész elemű 2×2-es mátrixok gyűrűje. Mutassuk meg, hogy ebben a csupa páros elemből álló mátrixok egy I ideált alkotnak. Hány elemű az R/I faktorgyűrű? Milyen ismert gyűrűvel izomorf R/I?

A.9.12 Legyen R az összes valós függvények szokásos gyűrűje és f a következő függvény: $f(x) = x$, ha $x \geq 5$ és $f(x) = 0$, ha $x < 5$.

(a) Mely függvények alkotják az (f) főideált?

(b) Bizonyítsuk be, hogy az $R/(f)$ faktorgyűrű izomorf R-rel.

A.9.13 Legyen I az R gyűrű egy nem triviális ideálja. Melyek igazak az alábbi állítások közül?

(a) Ha R kommutatív, akkor R/I is kommutatív.

(b) Ha R/I kommutatív, akkor R is kommutatív.

(c) Ha R egységelemes, akkor R/I is egységelemes.

(d) Ha R/I egységelemes, akkor R is egységelemes.

(e) Ha R nullosztómentes, akkor R/I is nullosztómentes.

(f) Ha R/I nullosztómentes, akkor R is nullosztómentes.

A.9.14 Az alábbi faktorgyűrűk közül melyek alkotnak testet?

(a) $\mathbf{R}[x]/(x^2)$; (b) $\mathbf{C}[x]/(x^2+1)$; (c) $\mathbf{Q}[x]/(x^6-2)$;

(d) $F_2[x]/(x^4+x+1)$.

A.10. Testbővítés

Ebben a pontban — a fejezet többi részével összhangban — testen mindig *kommutatív* testet értünk.

A.10.1 Definíció

Az M testet az L test *bővítés*ének nevezzük, ha L *részteste* M-nek, azaz $L \subseteq M$ és az L testben a műveletek éppen az M-beli műveletek megszorításai. ♣

Ennek a kapcsolatnak a szokásos jelölése $M \mid L$, de mivel ez könnyen félreérthető és nem is igazán tükrözi az L és M viszonyát, ezért inkább az $M : L$ jelölést fogjuk alkalmazni.

Ha M bővítése L-nek, akkor M egyben vektortér is L felett a „természetesen” adódó műveletekre. Ezek a *vektortér*műveletek az M *test* műveleteiből származnak: két M-beli „*vektor*t” mint az M *test* két elemét adjuk össze, továbbá egy L-beli „*skalár*ral” úgy szorzunk meg egy M-beli „vektort”, hogy az M *test*nek ezt a két elemét összeszorozzuk.

Az M-nek mint az L test feletti vektortérnek a *dimenzió*jára külön elnevezést és jelölést vezetünk be:

A.10.2 Definíció

Ha M bővítése L-nek, akkor az M-nek mint L feletti vektortérnek a dimenzióját a testbővítés *fok*ának nevezzük és $\deg(M : L)$-lel jelöljük. ♣

Például $\deg(\mathbf{C} : \mathbf{R}) = 2$, $\deg(\mathbf{R} : \mathbf{Q}) = \infty$.

Alapvetően fontos tétel, hogy az egymás utáni testbővítések esetén a fokszámok összeszorzódnak:

A.10.3 Tétel (Testbővítések fokszámtétele)
Az $L \subseteq M \subseteq N$ bővítéslánc esetén $\deg(N : L) = \deg(N : M) \cdot \deg(M : L)$. ♣

A testbővítések legegyszerűbb és egyben legfontosabb típusát az egyetlen elem által generált bővítések jelentik. Ezt rögtön tetszőleges testekre vizsgáljuk, de melegen ajánljuk, hogy az Olvasó az alábbiakat először az $L = \mathbf{Q}$, $M = \mathbf{C}$ speciális esetben gondolja végig, és ezen keresztül „szokja meg" ezt a fogalmat.

Előrebocsátjuk, hogy az $M : L$ testbővítés esetén az L test elemeit görög kisbetűkkel, az M elemeit pedig görög nagybetűkkel fogjuk jelölni.

Legyen L részteste M-nek és $\Theta \in M$ tetszőleges elem. Ekkor az L-nek a Θ-val történő *egyszerű bővítés*én az L-ből és a Θ-ból a(z M) testbeli műveletek (és inverzeik) segítségével előálló elemek halmazát fogjuk érteni. Ehhez elkészítjük minden lehetséges módon az $\alpha_0 + \alpha_1\Theta + \ldots + \alpha_n\Theta^n \in M$ elemeket, ahol n *tetszőleges* nemnegatív egész és az α_i-k az L test elemei, majd vesszük ilyenek hányadosait. Az $\alpha_0 + \alpha_1\Theta + \ldots + \alpha_n\Theta^n$ elem nem más mint a $g = \alpha_0 + \alpha_1 x + \ldots + \alpha_n x^n \in L[x]$ polinomnak a $\Theta \in M$ helyen vett $g(\Theta) \in M$ helyettesítési értéke. A szóban forgó hányadosok tehát $g(\Theta)/h(\Theta)$ alakú M-beli elemek, ahol g és h tetszőleges $L[x]$-beli polinomok és természetesen $h(\Theta) \neq 0$. Az ily módon kapott elemek a Θ-t és az L-et tartalmazó *legszűkebb* résztestet alkotják M-ben. Mindezt pontosan az alábbi definícióban és tételben fogalmazzuk meg.

A.10.4 Definíció
Legyen L részteste M-nek és $\Theta \in M$ tetszőleges elem. Ekkor a

$$\left\{ \frac{g(\Theta)}{h(\Theta)} \;\middle|\; g, h \in L[x],\ h(\Theta) \neq 0 \right\},$$

illetve ugyanezt részletesen kiírva, a

$$\left\{ \frac{\sum_{i=0}^{n} \alpha_i \Theta^i}{\sum_{j=0}^{k} \beta_j \Theta^j} \;\middle|\; \alpha_i, \beta_j \in L,\ \sum_{j=0}^{k} \beta_j \Theta^j \neq 0, \quad n, k = 0, 1, 2, \ldots \right\}$$

M-beli részhalmazt az L-nek a Θ-val történő *egyszerű bővítés*ének nevezzük és $L(\Theta)$-val jelöljük. ♣

A.10.5 Tétel

$L(\Theta)$ az M testnek az a *legszűkebb* részteste, amely a Θ elemet és az L testet tartalmazza, azaz

(i) $L(\Theta)$ az M testnek részteste;
(ii) $\Theta \in L(\Theta)$, $L \subseteq L(\Theta)$;
(iii) ha T részteste M-nek és $\Theta \in T$, $L \subseteq T$, akkor szükségképpen $L(\Theta) \subseteq T$. ♣

Bizonyos esetekben $L(\Theta)$ elemei egyszerűbb alakban is felírhatók. Ehhez szükségünk lesz az *algebrai elem* fogalmára.

A.10.6. Definíció

Legyen L részteste M-nek. A $\Theta \in M$ elem *algebrai* az L test felett, ha létezik olyan nem nulla $f \in L[x]$ polinom, amelynek a Θ gyöke, azaz $f(\Theta) = 0$. ♣

A már említett $L = \mathbf{Q}, M = \mathbf{C}$ speciális esetben ez az *algebrai szám* fogalmát jelenti: egy Θ komplex szám akkor *algebrai szám*, ha létezik olyan racionális együtthatós, nem nulla polinom, amelynek a Θ gyöke. Így például a $\sqrt{2}$, a $\sqrt[3]{5}$ vagy az $i\sqrt[7]{10}$ algebrai számok, megfelelő polinomok az $x^2 - 2$, az $x^3 - 5$, illetve az $x^{14} + 100$.

A nem algebrai komplex számokat *transzcendens szám*oknak nevezzük, ilyenek pl. a π, az e (a természetes logaritmus alapszáma), $\lg 2$, $\sin 1$ (a szöget radiánban mérve). Az algebrai számok csak megszámlálható sokan vannak, tehát a komplex számok „túlnyomó többsége" transzcendens. Ennek ellenére általában igen nehéz kérdés egy adott komplex számról eldönteni, hogy algebrai-e vagy transzcendens. Megoldatlan például, hogy $e+\pi$ algebrai-e vagy transzcendens, sőt azt sem tudjuk, hogy racionális-e vagy irracionális.

Egy Θ algebrai elem esetén több olyan $f \in L[x]$ polinom is létezik, amelynek a Θ gyöke, hiszen például egy ilyen polinom bármely polinomszorosa is rendelkezik ezzel a tulajdonsággal. Ezek között a polinomok között a(z egyik) legalacsonyabb fokúnak kitüntetett szerepe van:

A.10.7 Definíció

Az L felett algebrai $\Theta \in M$ elem *minimálpolinom*jának a(z egyik) legalacsonyabb fokú $L[x]$-beli polinomot nevezzük, amelynek a Θ gyöke. A Θ minimálpolinomját m_Θ-val jelöljük. ♣

A.10.8 Tétel
(i) m_Θ egy (L-beli) konstans szorzótól eltekintve egyértelmű.
(ii) Legyen $f \in L[x]$. Ekkor $f(\Theta) = 0 \iff m_\Theta \mid f$.
(iii) m_Θ irreducibilis L felett.
(iv) Ha f irreducibilis L felett és $f(\Theta) = 0$, akkor $f = m_\Theta$. ♣

Megjegyezzük, hogy az m_Θ jelölés a Θ *akármelyik* minimálpolinomját jelentheti, de ez nem okoz problémát, hiszen ezek a polinomok egymástól az (i) állítás alapján csak egy konstans szorzóban különböznek. Ha valaki (nagyon) egyértelműsíteni akar, akkor választhatja pl. azt az alakot, amelynek a főegyütthatója 1. Ekkor természetesen a (iv) állításban az $f = \gamma m_\Theta$ következtetés írható, ahol γ egy L-beli konstanst jelöl.

A.10.9 Definíció
Az L felett algebrai $\Theta \in M$ elem *fok*ának a minimálpolinomja fokszámát nevezzük: $\deg \Theta = \deg m_\Theta$. ♣

A korábbi ($L = \mathbf{Q}, M = \mathbf{C}$-re vonatkozó) példáinkban szereplő algebrai számok esetén a megadott polinomok $\mathbf{Q}$ felett irreducibilisek voltak, tehát a $\sqrt{2}$ minimálpolinomja $x^2 - 2$, a $\sqrt[3]{5}$-é $x^3 - 5$, az $i\sqrt[7]{10}$-é pedig $x^{14} + 100$, és így a három szám foka rendre 2, 3, illetve 14. (Az $i\sqrt[7]{10}$-re vonatkozó állítást a legkevesebb számolással az A.10.3 és a nemsokára következő A.10.11 Tételek segítségével lehet igazolni.) Az elsőfokú algebrai számok az elsőfokú racionális együtthatós polinomok gyökei, azaz maguk a racionális számok. Általában, tetszőleges L felett is az elsőfokú algebrai elemek pontosan az L elemei lesznek.

Most rátérünk arra, hogyan írhatók fel egy Θ *algebrai* elemmel történő bővítés esetén az $L(\Theta)$ elemei az A.10.4 Definícióban megadottnál egyszerűbb alakban.

Tekintsük példaként a racionális testnek a $\sqrt{2}$-vel vett $\mathbf{Q}(\sqrt{2})$ bővítését. Ez nem más, mint az $\alpha_0 + \alpha_1\sqrt{2}$ alakú számok T halmaza, ahol $\alpha_i \in \mathbf{Q}$ (lásd az A.5 pont P3 példáját), ugyanis T egy olyan test, amely a $\sqrt{2}$-t és a racionális számokat tartalmazza és nyilván a legszűkebb. Ez azt jelenti, hogy az A.10.4 Definícióban felírt alakhoz képest nincs szükség osztásra és a $\sqrt{2}$-nek az egynél magasabb kitevőjű hatványaira. Ha a $\sqrt{2}$ helyett a $\sqrt[3]{5}$-tel történő $\mathbf{Q}(\sqrt[3]{5})$ bővítést tekintjük, akkor itt $\sqrt[3]{5}$ legfeljebb második hatványaira van szükség, mert a harmadik és magasabb hatványok kifejezhetők ezekkel (és alkalmas racionális számokkal).

Az általános esetben a következő tétel érvényes:

A.10.10 Tétel
Ha $\Theta \in M$ egy n-edfokú algebrai elem az L test felett, akkor $L(\Theta)$ elemei *egyértelműen* felírhatók $\alpha_0 + \alpha_1\Theta + \ldots + \alpha_{n-1}\Theta^{n-1}$ alakban, ahol $\alpha_i \in L$. ♣

A tétel más megfogalmazásban azt jelenti, hogy az $1, \Theta, \ldots, \Theta^{n-1}$ elemek bázist alkotnak $L(\Theta)$-ban mint L feletti vektortérben. Így ennek a vektortérnek a dimenziója, azaz az $L(\Theta) : L$ testbővítés foka n. Ezt a fontos tényt külön tételként is kimondjuk:

A.10.11 Tétel
Ha $\Theta \in M$ algebrai elem az L test felett, akkor $\deg\big(L(\Theta) : L\big) = \deg\Theta$. ♣

Az A.10.10–A.10.11 Tételeket kiegészíthetjük azzal, hogy ha Θ nem algebrai elem (azaz *transzcendens*) L felett, akkor az $L(\Theta)$ elemei *nem* adhatók meg az A.10.4 Definícióban leírtnál egyszerűbb alakban, és az $L(\Theta) : L$ testbővítés foka ekkor *végtelen*.

Az $L(\Theta)$ test egy másik megközelítését adja az alábbi tétel:

A.10.12 Tétel
Ha $\Theta \in M$ algebrai elem az L test felett, akkor az $L(\Theta)$ test izomorf az $L[x]/(m_\Theta)$ faktorgyűrűvel. ♣

Tekintsük példaként a valós számoknak az i-vel történő bővítését, ekkor nyilván a komplex számokat kapjuk, azaz $\mathbf{C} = \mathbf{R}(i)$. Az i minimálpolinomja $m_i = x^2 + 1$, tehát az A.10.12 Tétel értelmében $\mathbf{C} = \mathbf{R}(i)$ izomorf az $\mathbf{R}[x]/(x^2 + 1)$ faktorgyűrűvel — ezt az eredményt már az A.9 pontban is megkaptuk.

Az A.10.12 Tétel alapján az $L(\Theta)$ elemeit az m_Θ polinom szerinti osztási maradékokként képzelhetjük el.

A tételt kiegészíthetjük azzal, hogy ha Θ *transzcendens* elem L felett, akkor az $L(\Theta)$ test az L feletti *algebrai törtek*, azaz az $L[x]$-beli polinomok formálisan képzett hányadosainak testével izomorf.

Végül megjegyezzük, hogy az A.10.12 Tétel segítségével „akkor is megkonstruálhatjuk $L(\Theta)$-t, ha nincs eleve adva egy bővebb M test”, lásd az A.10.18 feladatot.

Feladatok

M A.10.1 Tegyük fel, hogy az $M : L$ testbővítés foka véges, legyen $\deg(M : L) = n$. Bizonyítsuk be, hogy ekkor egy tetszőleges $\Theta \in M$ elem algebrai L felett, $\deg\Theta \leq n$, sőt $\deg\Theta \mid n$.

A.10.2 Mi az oka annak, hogy egy algebrai elem minimálpolinomja mindig irreducibilis, ugyanakkor egy lineáris transzformáció minimálpolinomja (lásd a 6.3 pontban) lehet reducibilis is az adott test felett?

A.10.3 Bizonyítsuk be az A.10.3, 5, 8, 10 és 12 Tételeket.

Az A.10.4–A.10.17 feladatok az algebrai számokra (azaz a komplex számok közül a $\mathbf{Q}$ felett algebrai elemekre) vonatkoznak.

A.10.4 Mutassuk meg, hogy egy $f \neq 0$ *komplex* együtthatós polinomhoz akkor és csak akkor létezik olyan $g \neq 0$ *racionális* együtthatós polinom, amelyre $f \mid g$, ha f minden (komplex) gyöke algebrai szám.

A.10.5 Bizonyítsuk be, hogy egy algebrai számból pozitív egész kitevős gyököt vonva ismét algebrai számot kapunk.

*A.10.6 Lássuk be, hogy az algebrai számok a komplex számok egy résztestét alkotják.

A.10.7 Mit állíthatunk egy algebrai és egy transzcendens szám összegéről, illetve két transzcendens szám összegéről (algebrai–transzcendens szempontból)?

A.10.8

(a) Jelöljük két komplex szám összegét S-sel, a szorzatukat pedig P-vel. Mi mondható a(z eredeti) két számról (algebrai–transzcendens szempontból), ha
(i) S algebrai, P transzcendens; (ii) S transzcendens, P algebrai;
(iii) S és P is transzcendens; (iv) S és P is algebrai?

(b) Mennyiben változik a helyzet, ha az „algebrai”, illetve „transzcendens” szavak helyére a „racionális”, illetve „irracionális” szavakat írjuk?

A.10.9 Legyen egy $z(\neq 0)$ komplex szám algebrai alakja $z = a + bi$, trigonometrikus alakja $z = r(\cos\varphi + i\sin\varphi)$. Bizonyítsuk be, hogy z akkor és csak akkor algebrai, ha

(a) a és b algebrai; illetve
(b) r és $\cos\varphi$ algebrai.

A.10.10 Az alábbi komplex számok közül melyek algebraiak és mennyi a fokuk?

(a) $\sqrt[100]{3000}$; (b) $\sqrt{2}+\sqrt{3}$; (c) $e+\pi i$;
(d) $\pi^{1000}+3\pi^9+7$; (e) $\sqrt[3]{2}+\sqrt[3]{4}$; (f) $\cos 20^\circ$;
(g) egy 101-edik egységgyök; (h) egy 6-odik egységgyök;
(i) egy primitív n-edik egységgyök; *(j) $\cos 1^\circ$.

*A.10.11 Van-e az egységkörön az egységgyökökön kívül algebrai szám?

*A.10.12 Határozzuk meg az egységkörön az összes páratlan fokú algebrai számot.

A.10.13 Legyen Θ algebrai szám, $\deg\Theta = k$. Mik $\deg(\Theta^2)$ lehetséges értékei?

A.10.14 Mutassuk meg, hogy
(a) $\mathbf{Q}(\sqrt{8}) = \mathbf{Q}(\sqrt{18})$; (b) $\mathbf{Q}(\sqrt[9]{2}) \cap \mathbf{Q}(\sqrt[6]{2}) = \mathbf{Q}(\sqrt[3]{2})$.

A.10.15 Bizonyítsuk be, hogy létezik olyan *racionális* együtthatós polinom, amely az $1 + 3\sqrt[7]{25} + 11\sqrt[7]{125} + 1000\sqrt[7]{625}$ helyen a $\sqrt[7]{5}$ értéket veszi fel.

M*A.10.16 Bizonyítsuk be, hogy ha $|z| = 1$, akkor $\mathbf{Q}(z) \cap \mathbf{R} = \mathbf{Q}(\operatorname{Re} z)$.

M*A.10.17 Bizonyítsuk be, hogy ha egy $f \in \mathbf{C}[x]$ polinom minden együtthatója algebrai szám, akkor f minden (komplex) gyöke is algebrai szám.

Megjegyzés: Jelöljük az algebrai számok testét A-val. Ekkor a feladat állítása úgy is fogalmazható, hogy minden nem konstans $f \in A[x]$ polinomnak van A-ban gyöke (illetve — ami ezzel ekvivalens — minden f-nek multiplicitással számolva pontosan annyi gyöke van A-ban, mint amennyi a foka). Ez azt jelenti, hogy — a komplex testhez hasonlóan — az algebrai számok testére is érvényes az „algebra alaptétele". Az ilyen tulajdonságú testeket *algebrailag zárt* testeknek nevezzük.

*A.10.18 Legyen L tetszőleges (kommutatív) test és f egy irreducibilis polinom L felett. Konstruáljunk egy olyan M testet, amely rendelkezik az alábbi tulajdonságokkal:

(i) M-nek van az L-lel izomorf L^* részteste;
(ii) ha $f^* \in L^*[x]$ az a polinom, amelynek az együtthatóit az f együtthatóiból az $L \to L^*$ izomorfizmus szerint kapjuk, akkor f^*-nak van egy $\Theta \in M$ gyöke;
(iii) $M = L^*(\Theta)$.

Megjegyzés: Ennek a konstrukciónak az alapján akkor is tudjuk az L-et egy irreducibilis polinom — még nem is létező(!) — gyökével bővíteni, ha nincs eleve adva egy, az L-et tartalmazó test.

A.11. Véges testek

A véges testek közül már számos esetben foglalkoztunk a modulo p maradékosztályok F_p testével, ahol p prím. Néhány másfajta véges test is szerepelt, pl. egy 9 elemű az A.5.2b és egy 16 elemű az A.9.14d feladatban.

Ebben a pontban a véges testek többféle általános jellemzését is megadjuk.

Mindenekelőtt megjegyezzük, hogy a szorzás kommutativitását nem kell külön hangsúlyoznunk, mert Wedderburn nevezetes (és nehéz) tétele szerint véges nem kommutatív test nem létezik.

Előrebocsátjuk még, hogy ebben a pontban egy (általános) véges test elemeit görög nagybetűkkel, a nullelemet 0-val, az egységelemet 1-gyel, magát a testet pedig M-mel fogjuk jelölni.

1. Elemszám

A szisztematikus tárgyalást az elemszámok leírásával kezdjük.

A.11.1 Tétel

(i) Minden véges test elemszáma prímhatvány (beleértve az első hatványokat, azaz magukat a prímeket is).

(ii) Bármely p^k prímhatványhoz izomorfiától eltekintve pontosan egy M véges test létezik, amelyre $|M| = p^k$. ♣

Ennek alapján pl. 100 elemű test nem létezik, 81 elemű viszont igen. A tételből az is következik, hogy két azonos elemszámú véges test szükségképpen izomorf, tehát pl. ha p prímszám, akkor nincs másfajta p elemű test, mint a modulo p maradékosztályok teste.

2. Összeadás

A következő tétel leírja a véges testek additív csoportjának a struktúráját.

A.11.2 Tétel

Legyen az M véges test elemszáma $|M| = p^k$. Ekkor M az összeadásra nézve izomorf az F_p test feletti (akármelyik) k-dimenziós vektortér, azaz (pl.) F_p^k additív csoportjával. ♣

Ennek alapján M elemeit olyan k-dimenziós vektoroknak képzelhetjük, amelyek minden komponense F_p-beli, azaz minden komponens egy-egy modulo p maradékosztály és az összeadást ennek megfelelően kell végezni. Ebből következik, hogy bármely $\Theta \in M$ elemet önmagával p-szer összeadva mindig 0-t kapunk. Ezt úgy is fogalmazhatjuk, hogy az M additív csoportjában a nem nulla elemek (additív) rendje p.

3. Szorzás

A véges testek multiplikatív szerkezete is nagyon szép:

A.11.3 Tétel

Egy véges test nem nulla elemei a szorzásra nézve *ciklikus* csoportot alkotnak. ♣

Ugyanezt úgy is megfogalmazhatjuk, hogy létezik olyan $\Delta \in M$ elem, amelynek a hatványaiként az M összes nem nulla elemét megkapjuk. Mivel ekkor Δ multiplikatív rendje $o(\Delta) = |M| - 1 = p^k - 1$, ezért az M nem nulla elemei egyértelműen felírhatók Δ^j alakban, ahol $j = 0, 1, 2, \ldots, p^k - 2$. Ha speciálisan $|M| = p$, azaz $M = F_p$, akkor ez éppen azt jelenti, hogy Δ *primitív gyök* modulo p.

Megjegyezzük még, hogy a p^k elemű test multiplikatív csoportjának — a ciklikus csoportokra érvényes általános eredménynek megfelelően — (nemcsak egy, hanem pontosan) $\varphi(p^k - 1)$ darab generátoreleme van.

Egy véges test multiplikatív csoportjának (akármelyik) generátorelemét a test *primitív elem*ének nevezzük. A p^k elemű véges testben tehát $\varphi(p^k - 1)$ primitív elem található.

4. Vektortér

A továbbiakban fontos szerepe lesz annak, hogy bármely véges test tartalmaz egy F_p típusú testet. Ez éppen az 1 egységelem által generált résztest lesz, amely az $1, 1+1, \ldots, 1+1+\ldots+1$ alakú elemekből áll. Ha $|M| = p^k$, akkor az A.8.2 Tétel szerint az 1 additív rendje (is) p, tehát p darab ilyen alakú (különböző) elem van. Könnyen látható, hogy ezek egy, az F_p-vel izomorf testet alkotnak.

Ennek megfelelően az M-et felfoghatjuk mint az F_p test *bővítés*ét. Ez többek között azt is jelenti, hogy M egy k-dimenziós *vektortér* F_p felett, tehát az A.8.2 Tételbeli izomorfia nemcsak az additív csoportok, hanem a megfelelő vektorterek között is fennáll.

Mindezt az alábbi tételben foglaljuk össze:

A.11.4 Tétel

Legyen az M véges test elemszáma $|M| = p^k$. Ekkor M tartalmaz egy F_p-vel izomorf résztestet és e felett a részteste felett M egy k-dimenziós vektorteret alkot. ♣

5. Testbővítés

Most megvizsgáljuk az imént bevezetett $M : F_p$ testbővítés további vonatkozásait (itt erősen támaszkodunk majd az A.10 pontra).

Mivel $\deg(M : F_p) = k$, ezért az A.7.1 feladat alapján minden $\Theta \in M$ *algebrai* elem F_p felett és $\deg \Theta \mid k$.

Megmutatjuk, hogy $M : F_p$ *egyszerű* bővítés. Legyen az M multiplikatív csoportjának a(z egyik) generátoreleme Δ. Ekkor a Δ-t tartalmazó legszűkebb résztest csak a teljes M lehet (hiszen minden nem nulla elemet már pusztán a szorzással is megkapunk), tehát $F_p(\Delta) = M$.

Ebből az is következik, hogy $k = \deg(M : F_p) = \deg\big(F_p(\Delta) : F_p\big) = \deg m_\Delta$, azaz a Δ-nak az F_p test feletti foka pontosan k.

Ekkor az M-nek mint F_p feletti vektortérnek az $1, \Delta, \Delta^2, \ldots, \Delta^{k-1}$ elemek egy bázisát alkotják (itt az 1 az F_p és M testek közös egységelemét jelöli).

Természetesen a multiplikatív csoport generátorelemein, azaz a primitív elemeken kívül más $\Theta \in M$ elemekre is fennáll(hat) $M = F_p(\Theta)$; ez pontosan a(z F_p felett) k-adfokú Θ-kra teljesül.

A fentiek lényegét az alábbi tételben foglaljuk össze:

A.11.5 Tétel

Legyen az M véges test elemszáma $|M| = p^k$, Δ a multiplikatív csoport (egyik) generátoreleme és F_p az M-ben levő p elemű test. Ekkor

(i) $M = F_p(\Delta)$;
(ii) $1, \Delta, \Delta^2, \ldots, \Delta^{k-1}$ bázis M-ben mint F_p feletti vektortérben;
(iii) bármely $\Theta \in M$-re $\deg \Theta \mid k$;
(iv) $\Theta \in M$, $\deg \Theta = k \iff M = F_p(\Theta)$. ♣

6. Faktorgyűrű

Az $M = F_p(\Delta)$ előállításból az A.10.12 Tétel szerint kapjuk, hogy M izomorf az $F_p[x]/(m_\Delta)$ faktorgyűrűvel. Ezt az A.9.6 Tétellel is összevetve a véges testek alábbi igen hasznos jellemzését nyerjük:

A.11.6 Tétel

A p^k elemű véges testet megadhatjuk mint az $F_p[x]/(f)$ faktorgyűrűt, ahol f egy k-adfokú irreducibilis polinom F_p felett. ♣

Ez azt jelenti, hogy a p^k elemű test elemeinek tekinthetjük a legfeljebb $k-1$-edfokú $F_p[x]$-beli polinomokat és ezekkel mint az f irreducibilis polinom szerinti osztási maradékokkal kell a műveleteket végezni.

Az A.11.1(ii) és A.11.6 Tételekből az is adódik, hogy az F_p test felett tetszőleges k-ra létezik k-adfokú irreducibilis polinom. Ugyanez érvényes bármely

véges test felett is, sőt képletet is tudunk adni az adott fokú irreducibilis polinomok darabszámára (lásd az A.11.12b feladatot és az útmutatásnál szereplő megjegyzést).

Az F_p feletti k-adfokú irreducibilis polinomok között kitüntetett szerepe van azoknak, amelyek a p^k elemű véges test *primitív elem*einek, azaz a multiplikatív csoport generátorelemeinek a minimálpolinomjai. Ezeket (F_p felett) *primitív polinom*oknak nevezzük. (Ennek a fogalomnak semmi köze sincs a Gauss-lemmában szereplő, az egész számok feletti primitív polinomokhoz.)

7. Példa

Illusztrációként megkonstruáljuk a 125 elemű testet.

Ehhez az F_5 test felett kell egy harmadfokú irreducibilis polinomot találnunk. Mivel egy harmadfokú polinom pontosan akkor irreducibilis, ha nincs gyöke az adott testben (ez magasabb fokszám esetén nem igaz, lásd az A.7.19 feladatot!), ezt könnyen tudjuk ellenőrizni, hiszen csak az F_5 test összesen 5 darab elemét kell behelyettesítenünk. Így pl. $f = x^3 + x + 1$ megfelel.

Az A.11.6 Tétel értelmében ekkor M elemeit a legfeljebb másodfokú $\alpha_0 + \alpha_1 x + \alpha_2 x^2$ polinomoknak vehetjük, ahol $\alpha_i \in F_5$ és ezekkel a polinomokkal mint az $x^3 + x + 1$ szerint vett osztási maradékokkal kell számolni.

Például a $3+4x$ és $3+x^2$ elemek összege és szorzata $(3+4x)+(3+x^2) = = 1+4x+x^2$, illetve

$$(3+4x)(3+x^2) = 4+2x+3x^2+4x^3 = 4+2x+3x^2+4(-1-x) = 3x+3x^2.$$

Az M elemeit F_5^3-beli vektorokkal is jelölhetjük, ekkor bázisnak az $1, x, x^2$ maradékokat célszerű választani. Ezzel a jelöléssel a fenti vektorok és a velük végzett műveletek a következőképpen festenek:

$$\begin{pmatrix}3\\4\\0\end{pmatrix} + \begin{pmatrix}3\\0\\1\end{pmatrix} = \begin{pmatrix}1\\4\\1\end{pmatrix} \quad \text{és} \quad \begin{pmatrix}3\\4\\0\end{pmatrix}\begin{pmatrix}3\\0\\1\end{pmatrix} = \begin{pmatrix}0\\3\\3\end{pmatrix}.$$

Jól látszik, hogy ez a fajta felírás kényelmessé teszi az összeadást, a szorzás elvégzésében azonban nem segít; a szorzáshoz mindenképpen a polinomos alakban kell gondolkodnunk, és a minimálpolinom szerinti redukciót kell felhasználnunk.

Hogyan kaphatjuk meg a test multiplikatív csoportjának egy generátorelemét? A fenti konstrukcióban az x (vagy a második jelölésmóddal, a $\begin{pmatrix}0\\1\\0\end{pmatrix}$ vektor) akkor lesz megfelelő, ha a (multiplikatív) rendje $|M|-1 = 124$. Mivel

a Lagrange-tétel alapján a csoport bármely elemének a 124-edik hatványa az egységelem, így csak azt kell ellenőriznünk, hogy kisebb (pozitív) kitevőjű hatványként megkapjuk-e az 1-et. Mivel $124 = 2^2 \cdot 31$, ezért elég a 4-edik és a 62-edik hatványt megvizsgálni: ha ezek egyike sem az egységelem, akkor a rend ezek egyikének sem osztója, és így csak 124 lehet.

Az $x^3 = -1 - x$ összefüggés alapján $x^4 = -x - x^2 \neq 1$, tehát $o(x) \not| 4$. Azt, hogy $x^{62} = 1$ teljesül-e, a leggyorsabban a következőképpen dönthetjük el. Mivel (kommutatív) testben vagyunk, ezért (a nullosztómentesség, valamint $x \neq 0$ alapján)

$$1 = x^{62} = (x^{31})^2 \iff x^{31} = \pm 1 \iff x^{32} = \pm x\,.$$

Az $x^4 = -(x + x^2)$ egyenlőséget négyzetre emelve

$$x^8 = x^2 + 2x^3 + x^4 = x^2 - (2 + 2x) - (x + x^2) = -(2 + 3x)$$

adódik, majd ezt a binomiális tétellel negyedik hatványra emelve kapjuk, hogy

$$x^{32} = (2 + 3x)^4 = 2^4 + 4 \cdot 2^3 \cdot 3x + 6 \cdot 2^2 \cdot 3^2 x^2 + 4 \cdot 2 \cdot 3^3 x^3 + 3^4 x^4 = \\ = 1 + x + x^2 + x^3 + x^4 = 1 + x + x^2 - (1 + x) - (x + x^2) = -x.$$

Mint láttuk, ebből $x^{62} = 1$ következik, tehát az x nem primitív elem.

Ekkor nyilván bármely m-re $(x^m)^{62} = 1$, és így az x hatványai sem lehetnek primitív elemek. Emellett a(z összesen) két darab negyedrendű elem sem primitív. Mindezeket kiszűrve, bármelyik más elem viszont már megfelel a multiplikatív csoport generátorának.

Egy másik lehetőség, hogy keresünk F_5 felett egy másik harmadfokú irreducibilis polinomot, amely már primitív, ilyen pl. az x^3+3x+2, és az e szerinti faktorgyűrűként írjuk fel a 125 elemű testet. Ekkor az x (mint az $x^3 + 3x + 2$ polinom szerinti maradék) generátorelem lesz a multiplikatív csoportban.

Feladatok

A11.1 Mutassuk meg, hogy egy p^k elemű testben szabad tagonként p-edik hatványra emelni, azaz $(\Theta + \Psi)^p = \Theta^p + \Psi^p$.

A.11.2 Mivel egyenlő egy véges test összes nem nulla elemének a szorzata, illetve összege?

A.11.3 Hány gyöke van a p^k elemű testben az $x^m - 1$ polinomnak?

A.11.4 A 13^k elemű testben hány olyan $\Theta \neq \Psi$ elempár létezik, amelyek egymás köbgyökei?

A.11.5

(a) Tegyük fel, hogy egy nullosztómentes gyűrűben létezik olyan nem nulla elem, amelyet önmagával valahányszor összeadva a nullelemet kapjuk. Bizonyítsuk be, hogy ekkor létezik egy olyan egyértelműen meghatározott p prímszám, hogy a gyűrű bármely elemét p-szer önmagával összeadva mindig a nullelem adódik.

(b) Mutassunk példát olyan *végtelen* testre, amely rendelkezik ezzel a tulajdonsággal.

Megjegyzés: Ezt a p-t a nullosztómentes gyűrű *karakterisztikájának* nevezzük. A p^k elemű test karakterisztikája tehát p. — Ha nincs ilyen p, azaz egy nem nulla elemet önmagával akárhányszor összeadva sohasem kapjuk a nullelemet, akkor a (nullosztómentes) gyűrűt *0-karakterisztikájú*nak vagy *végtelen karakterisztikájú*nak nevezzük. Így pl. $\mathbf{Q}$, $\mathbf{R}$ és $\mathbf{C}$ karakterisztikája 0.

A.11.6 Hogyan konstruálhatunk 169, illetve 81 elemű testet?

A.11.7 Mutassuk meg, hogy a p^k elemű M test éppen az $x^{p^k} - x$ polinom gyökeiből áll [azaz $x^{p^k} - x = \prod_{\Theta \in M}(x - \Theta)$].

M*A.11.8 Legyen f irreducibilis polinom F_p felett. Igazoljuk, hogy $f \mid x^{p^k} - x$ akkor és csak akkor teljesül, ha $\deg f \mid k$.

A.11.9 Bizonyítsuk be, hogy a p^k elemű test akkor és csak akkor tartalmaz p^n elemű résztestet, ha $n \mid k$.

A.11.10 Lássuk be, hogy egy véges test bármely két (különböző) részteste különböző elemszámú.

*A.11.11 Legyen $f = x^k + \alpha_{k-1}x^{k-1} + \ldots + \alpha_1 x + \alpha_0$ egy primitív polinom F_p felett, és legyen A a következő $k \times k$-as mátrix:

$$A = \begin{pmatrix} 0 & 0 & 0 & \ldots & 0 & -\alpha_0 \\ 1 & 0 & 0 & \ldots & 0 & -\alpha_1 \\ 0 & 1 & 0 & \ldots & 0 & -\alpha_2 \\ \vdots & \vdots & \vdots & & \vdots & \vdots \\ 0 & 0 & 0 & \ldots & 1 & -\alpha_{k-1} \end{pmatrix}.$$

Mutassuk meg, hogy az A (különböző) hatványai és a nullmátrix a mátrixösszeadásra és a mátrixszorzásra nézve egy p^k elemű testet alkotnak.

M*A.11.12 Hány k-adfokú, 1 főegyütthatójú
(a) primitív; (b) irreducibilis
polinom létezik F_p felett?

A.11.13 Tekintsük a p^3 elemű M testet mint F_p feletti (3 dimenziós) vektorteret. Nevezzük az M egydimenziós altereit *pont*oknak, a kétdimenziós altereit pedig *egyenes*eknek. Egy pont akkor van rajta egy egyenesen, ha a megfelelő alterek tartalmazzák egymást. Mutassuk meg, hogy így egy p-edrendű nem elfajuló projektív síkot kapunk (lásd a 9.5.11 feladatot):

(a) Bármely két egyenesnek egy közös pontja van, és bármely két ponton egy egyenes megy át.
(b) Mind a pontok, mind az egyenesek száma $p^2 + p + 1$.
(c) Minden egyenesen $p + 1$ pont helyezkedik el, és minden ponton $p + 1$ egyenes halad át.

Megjegyzések: Ugyanez a konstrukció a p prím helyett egy p^m prímhatvánnyal is elvégezhető, ekkor a p^{3m} elemű véges testet kell a benne levő p^m elemű test feletti vektortérnek tekinteni. Ahogy a 9.5.11 feladatban említettük, megoldatlan probléma, hogy egy véges projektív sík pontjainak a száma lehet-e más, mint $p^{2m} + p^m + 1$, ahol p prím.

A geometriai kapcsolat talán „szemléletesebbé" válik, ha a pontokat definiáló (egydimenziós) alterekből figyelmen kívül hagyjuk a nullvektort. Ekkor az egy pontot jellemző vektorok éppen egymás nem nulla skalárszorosai. Ezt úgy is felfoghatjuk, hogy egy „síkbeli" pontot *homogén koordináták*kal jellemzünk, azaz ugyanazt a pontot kapjuk, ha mindhárom koordinátát egy tetszőleges nem nulla skalárral megszorozzuk. Ez teljesen összhangban van a valós test feletti projektív sík megadásával. [A valós projektív síkot az euklideszi sík *ideális pontok*kal történő kibővítésével kapjuk, ahol az ideális pontok az adott irányú párhuzamos egyenesek metszéspontjai, és ezek egy ideális egyenest alkotnak. Az euklideszi sík (a_1, a_2) koordinátájú „közönséges" pontjának a projektív síkon azok a homogén koordinátás $(\alpha_1, \alpha_2, \alpha_3)$ számhármasok felelnek meg, amelyekre $\alpha_1/\alpha_3 = a_1, \alpha_2/\alpha_3 = a_2$.]

A.11.14 Tekintsük az előző feladatbeli M-et, a pontok továbbra is legyenek az egydimenziós alterek, azonban most az egyeneseknek is az egydimenziós altereket válasszuk. Az illeszkedés definícióját úgy módosítjuk, hogy egy pont akkor van rajta egy egyenesen, ha a pontnak, illetve az egyenesnek megfelelő két (egydimenziós) altér merőleges egymásra. Mutassuk meg, hogy most is teljesülnek az előző feladat állításai.

EREDMÉNYEK ÉS ÚTMUTATÁSOK

1. Determinánsok

1.1.

1.1.1

(a) A legkevesebb inverzió az $1, 2, 3, \ldots, n$ permutációban van, a legtöbb pedig az $n, n-1, \ldots, 2, 1$ permutációban.

(b) Lássuk be, hogy a természetes $1, 2, 3, \ldots, n$ sorrendből kiindulva szomszédos elemek cseréjével el lehet jutni a fordított $n, n-1, \ldots, 1$ sorrendhez. Mivel az inverziószám minden lépésben 1-gyel változik, ezért minden, a 0 és $\binom{n}{2}$ közé eső értéket fel kell vennie.

1.1.2 (a) 2500; (b) 2550; (c) 4270; (d) 5000.

1.1.3 $n = 4k$ vagy $n = 4k + 1$ alakú.

1.1.4 $(n + 1)/2$ (csak páratlan n esetén van ilyen permutáció).

1.1.5

(a) $2n - 3$. Ez akkor és csak akkor lép fel, ha az 1-et és az n-et cseréljük fel, és közülük az egyik az első, a másik pedig az utolsó helyet foglalja el.

(b) $2\lceil (n-4)/5 \rceil + 1$, ahol $\lceil x \rceil$ az x szám felső egész részét jelenti, azaz a legkisebb olyan egész számot, amely $\geq x$.

1.1.6

(a) $\binom{n}{2}$.

(b) $n - 1$.

(c) $\lfloor (3n-3)/2 \rfloor$, azaz $n = 2k + 1$ esetén $3k$, $n = 2k$ esetén pedig $3k - 2$.

1.1.7

(a) Páros n-re.

(b) Az $n = 5$ kivételével minden $n > 2$-re.

(c) Páratlan k esetén minden páros $n > k$-ra, páros $k \neq 0$ esetén $n = 2k + 1$ kivételével minden $n > k$-ra, $k = 0$ esetén minden $n > 0$-ra.

1.1.8

(a) Aszerint számoljuk össze a permutációkat, hogy az 1 hányadik helyen áll.

(b) Alkalmazzuk az előző eredményt k-ra és $k - 1$-re.

(c) $n!$

(d) $\binom{n}{2} n!/2$.

(e) Használjuk a skatulyaelvet.

(f) A „középső” k érték(ek)re.

1.2.

1.2.1 (a) 90. (b) -192.

1.2.2 Igaz: (a), (d), (g).

1.2.3
(a) 0.
(b) $\alpha_{11}\alpha_{22}\dots\alpha_{nn}$ (azaz a főátlóbeli elemek szorzata).
(c) $(-1)^{n(n-1)/2}\,\alpha_{1,n}\alpha_{2,n-1}\dots\alpha_{n,1}$.

1.2.4 (a) $(-1)^{n-1}$. (b) 0. (c) $(-1)^{n/2}$, ha n páros, és 0, ha n páratlan.

1.2.5 Útmutatás: bármely n-tényezős szorzatnál az adott k sort tekintve csak $n-m<k$ oszlopból van lehetőség nem nulla elem választására.

1.2.6 Ha a két elem ugyanabban a sorban vagy oszlopban áll, akkor $(n-2)(n-1)!$, egyébként pedig $(n^2-3n+4)(n-2)!$. Ugyanez az eredmény érvényes akkor is, ha a szorzatok előjelezését is figyelembe vesszük.

1.2.7 Minden esetben elegendő már *egyetlen* elem alkalmas megváltoztatása. Útmutatás: Ha a determináns definíciójában az α_{11} elemet az őt tartalmazó szorzatokból kiemeljük, akkor a determináns $\alpha_{11}\beta+\gamma$ alakba írható. Ha $\beta\neq 0$, akkor az $\alpha'_{11}=-\gamma/\beta$ változtatás megfelel. Egyébként próbálkozzunk ugyanígy az első sor többi elemével. Ha egyik esetben sem járunk sikerrel, akkor a determináns már eleve 0 volt.

1.2.8 A legegyszerűbb, ha az első egyenletet α_{21}-gyel, a másodikat pedig α_{11}-gyel beszorozzuk, és ezután x_1-et kiejtve kifejezzük x_2-t. Hasonlóan kaphatjuk meg x_1-t is. Ezzel beláttuk, hogy csak a feladatban megadott értékek szolgáltathatnak megoldást. Az, hogy ez valóban megoldás, behelyettesítéssel ellenőrizhető.
Analóg állítás érvényes n ismeretlen és egyenlet esetén is, ez az ún. Cramer-szabály, amelyet a 3.2 pontban tárgyalunk.

1.2.9 A legegyszerűbben úgy érhetünk célt, ha a paralelogrammát olyan, vele azonos területű paralelogrammába toljuk át, amelynek egyik oldala valamelyik tengelyre esik.
Analóg állítás érvényes a térben (sőt magasabb dimenziókban is) a paralelepipedonok térfogatára (lásd a 9.8 pontot).

1.2.10 $2^{\lfloor n/2\rfloor}$.

1.2.11 A determináns definíciójában szereplő szorzatok között pontosan egy páratlan szám fordul elő, a többi páros, és így ezek (előjeles) összege is páratlan szám.

1.3.

1.3.1 Ha $n = 4k$ vagy $4k+1$ alakú, akkor nem változik, egyébként pedig előjelet vált.

1.3.2 Ha a determináns nem nulla, akkor n ilyen szám van: a (-1)-ből vont n-edik gyökök. Ha a determináns 0, akkor bármely komplex szám megfelel.

1.3.3 (a) 30. (b) 100.
Útmutatás: sorok, illetve oszlopok alkalmas kivonogatásával olyan determináns keletkezik, amelyben szebb és kisebb számok szerepelnek.

1.3.4 Hasonlóan okoskodhatunk, mint az 1.3.1/III Tétel bizonyításánál.

1.3.5 Az 1.3.3 Tétel bizonyításánál látottakhoz hasonló gondolatmenetet kell alkalmazni.

1.3.6 Az adott két sor cseréjénél a determináns egyrészt nem változik, másrészt előjelet vált, tehát csak 0 lehet. Ez a gondolatmenet pl. a modulo 2 test esetére nem alkalmazható, hiszen ott „$1 = -1$”.

1.3.7
(a) A determinánsok egyenlők.
(b) Az új determináns a réginek $\alpha^{n(n+1)}$-szerese.

1.3.8 (a) $(n-1)!$ (b) 1. (c) 0, ha $n > 1$. (d) 0, ha $n > 2$.
(e) 0, ha $n > 2$.

1.3.9 0, ha $n > 2$.

1.3.10 Útmutatás:
(a) A 3-mal való oszthatóságnál adjuk hozzá az utolsó oszlophoz a többi oszlopot.
(b) Az általános esetben az utolsó oszlophoz az utolsó előtti oszlop 10-szeresét, az azt megelőző oszlop 100-szorosát stb. érdemes hozzáadni.

1.3.11 0, ha $n > 2$.

1.3.12 Eredmény: $[\gamma + (n-1)\delta](\gamma - \delta)^{n-1}$.
Útmutatás: Adjuk hozzá az első sorhoz a többi sort, emeljük ki az első sor közös $\gamma + (n-1)\delta$ értékét, majd vonjuk le a többi sorból az első sor δ-szorosát. — Másik lehetőség: alulról kezdve, minden sorból vonjuk le a fölötte levő sort, majd jobbról balra haladva, minden oszlopot adjunk hozzá az előtte álló oszlophoz.

1.3.13 Válasz: 0.
Útmutatás: tükrözzünk a főátlóra.

1.3.14 Ha egy sornak többször is szerepel a konjugáltja, akkor van két egyező sor, tehát $D = 0$. Ha egy sornak önmaga a konjugáltja, akkor a sorban minden elem valós. A konjugált sorpárokat kivonogatásokkal átalakíthatjuk úgy,

hogy az egyik sorban csak valós, a másikban csak tiszta képzetes számok maradjanak.

1.3.15 Eredmény: 1.
Általánosítás: a mátrix a Pascal-háromszög egy (elforgatott) darabja. Az általános determináns is 1. Ennek igazolásához azt használjuk fel, hogy a mátrixban bármely elem a fölötte és előtte álló elem összege.

1.3.16
(a) $(-1)^n(n-2)$.
Útmutatás: az első sorból vonjuk le a többi sort.
(b) $(-1)^{n-1}(n-1)!$
Útmutatás: az első oszlopot vigyük hátra, és vonjuk le az első sort a többi sorból.

1.3.17 $n!$

1.3.18 Eredmény: 0, ha $n > 2$.
Útmutatás: Az addiciós képletek beírása után bontsuk a determinánst az 1.3.2 Tétel ismételt alkalmazásával 2^n darab determináns összegére. Az 1.3.3A Tétel alapján ezek mindegyike 0, ha $n > 2$.

1.3.19 Útmutatás: adjuk hozzá az utolsó oszlophoz a többi oszlopot.
Páros n esetén csak az $n/2$-lel való oszthatóság következik.

1.3.20 Az előző feladathoz hasonló gondolatmenetet kell alkalmazni.

1.3.21 Útmutatás: ha $(i, n) = 1$, akkor az i-edik és az $(n-i)$-edik sort összeadva mindig egy $n, n, \ldots, n, 2n$ alakú sort kapunk.

1.4.

1.4.1 nD.

1.4.2 Eredmény: 0.
Útmutatás: az első két sorra vett ferde kifejtés a feltétel szerint egybeesik az egyik sor szerinti (rendes) kifejtéssel.

1.4.3 A régi és az új determinánst is fejtsük ki az első sor szerint.

1.4.5 Eredmény: $\delta^{n-1} - (n-1)\beta\gamma\delta^{n-2}$ (ha $n \geq 2$).
Útmutatás: Jelöljük a determinánst D_n-nel és fejtsük ki az utolsó sora szerint. Az A_{n1} aldeterminány könnyen meghatározható és így a $D_n = \delta D_{n-1} - \beta\gamma\delta^{n-2}$ rekurzió adódik. Néhány kis n értékre D_n-et kiszámolva (már ezt is a rekurzió felhasználásával érdemes csinálni!) az eredmény könnyen megsejthető, és ezután a rekurzió alapján teljes indukcióval igazolható.

A feladat rekurzió nélkül is megoldható: ha $\delta = 0$, akkor a determináns 0, egyébként pedig a főátló fölött csupa 0 elérhető, ha az első sorból levonjuk a többi sor alkalmas többszörösét.

1.4.6 $(\gamma^2 - \delta^2)^k$.

1.4.7 Eredmény: $\gamma^n + \gamma^{n-1}\delta + \gamma^{n-2}\delta^2 + \ldots + \delta^n$.
Útmutatás: valamelyik szélső sor vagy oszlop szerint kifejtve a $D_n = (\gamma + \delta)D_{n-1} - \gamma\delta D_{n-2}$ rekurzió adódik.

1.4.8 Eredmény: egy ilyen γ van, ha az eredeti determináns összes aldeterminánsának összege nem nulla, és nincs ilyen γ, ha ez az összeg 0.
Útmutatás: A γ hozzáadásával kapott determinánst bontsuk 2^n darab determináns összegére. Ezeknek a tagoknak a legtöbbje 0 lesz.

1.4.9 Az utolsó sor szerinti kifejtést felhasználva teljes indukcióval bizonyítsunk.

1.4.10 $1 - \sum_{i=1}^{n} \beta_i^2$.

1.4.11

(a) Először az azonos sorhoz (vagy oszlophoz) tartozó aldeterminánsok egyenlőségét igazoljuk. Pl. A_{11} és A_{1j} az előjeltől eltekintve egyetlen oszlopban tér el egymástól. Használjuk fel, hogy minden sorban az elemek összege 0, és innen fejezzük ki az első oszlop elemeit.

(b) Használjuk a kifejtési tételt.

1.4.12 Ha $\beta = \delta$, akkor lásd az 1.3.12 feladatot, ha pedig $\beta \neq \delta$, akkor az eredmény $[\beta(\gamma - \delta)^n - \delta(\gamma - \beta)^n]/(\beta - \delta)$.
Útmutatás: A jobb alsó sarokban álló elemet írjuk $\beta + (\gamma - \beta)$ alakba, és bontsuk a determinánst az utolsó sor szerint két determináns összegére. Ezzel D_n-et kifejezhetjük D_{n-1} segítségével. Innen a leggyorsabban úgy érünk célt, ha ebből a rekurzióból β és δ szimmetriáját kihasználva egy másik rekurziót is felírunk. A két egyenlőségből D_n azonnal kifejezhető.

1.4.13 (a) n. (b) $n^2 - n + 1$. (ca) 1. (cb) $n(n-1)/2 + 1$.

1.4.14 Létezik.

1.4.15 Az 1.4.2 Tétel bizonyítását kell értelemszerűen módosítani.

1.5.

1.5.1 (a) $(-1)^{n(n-1)/2}\, V$. (b) $(-1)^{n(n-1)/2}\, V^2$.

1.5.2 Ha a γ_i-k között vannak azonosak, akkor minden komplex szám megoldás. Ha a γ_i-k mind különbözők, akkor a $V(x, \gamma_2, \ldots, \gamma_n) = 0$ egyenlet összes gyöke $x = \gamma_i$, tehát $n-1$ megoldás van. Több megoldás más δ esetén sem lehet, ugyanis, ha a γ_i-k mind különbözők, akkor $V(x, \gamma_2, \ldots, \gamma_n) - \delta$ az

x-nek pontosan $n-1$-edfokú polinomja. Innen az is látszik, hogy $n-1$-nél kevesebb megoldás előfordulhat, mégpedig akkor, ha ennek a polinomnak van többszörös gyöke.

1.5.3 Ha az i-edik sorban szereplő mértani sorozat első eleme δ_i, hányadosa pedig γ_i, akkor a determináns $\delta_1 \dots \delta_n V(\gamma_1, \dots, \gamma_n)$.

1.5.4 $n!(n-1)! \dots 1! = n(n-1)^2(n-2)^3 \dots 1^n$.

1.5.5

(a) $V(\gamma_1, \dots, \gamma_n)$-nek és a polinomok főegyütthatóinak a szorzata.

(b) 0.

1.5.6 $\prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)(\beta_j - \beta_i)$.

1.5.7 $\binom{n-1}{1}\binom{n-1}{2} \dots \binom{n-1}{n-1} \prod_{1 \le i < j \le n} (\alpha_j - \alpha_i)(\beta_i - \beta_j)$.

1.5.8 A hányados mindig $2^{(n-1)(n-2)/2}$.
Útmutatás: $\cos(r\phi)$ kifejezhető a $\cos\phi$-nek r-edfokú polinomjaként, határozzuk meg itt a főegyütthatót, majd alkalmazzuk az 1.5.5a feladat eredményét.

1.5.9 (a) Előjelet vált. (b) Pontosan a páros permutációk.

1.5.10 $\binom{n+2}{3}$.

1.5.11

(a) A skatulyaelv szerint minden $k < n$-hez található olyan $i \neq j$, hogy a_i és a_j ugyanazt a maradékot adja k-val osztva.

(b) $V(a_1, \dots, a_n)$ nem változik, ha a_i^j helyére $j!\binom{a_i}{j}$-t írunk.

1.5.12 Eredmény: $(-1)^{(p+1)/2}$, azaz 1, ha $p = 4k-1$ alakú, és -1, ha $p = 4k+1$ alakú.
Útmutatás: a $k!(p-1-k)!$ típusú szorzatok maradékának megállapításához használjuk a Wilson-tételt.

1.5.13 Eredmény: $(\gamma_1 + \gamma_2 + \dots + \gamma_n)V(\gamma_1, \dots, \gamma_n)$.
Útmutatás: az $n+1$-edrendű $f(x) = V(\gamma_1, \gamma_2, \dots, \gamma_n, x)$ determinánst fejtsük ki az utolsó sora szerint.

2. Mátrixok

2.1.

2.1.1 Az összeg egy olyan $k \times n$-es mátrix, amelynek minden eleme $6 \cdot 3^{kn-1}$.

2.1.2 α/β nem valós (és $\alpha, \beta \neq 0$).

2.1.3 A.

2.1.4 (a) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$. (b) $\begin{pmatrix} 2 & -3 \\ 1 & -2 \end{pmatrix}$. (c) $\begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$.

2.1.5 (a) $\begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$. (b) $\begin{pmatrix} \cos n\alpha & -\sin n\alpha \\ \sin n\alpha & \cos n\alpha \end{pmatrix}$.

(c) páratlan n-re: $\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix}$, páros n-re: $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$.

2.1.6 (a) $\begin{pmatrix} b & 1-b \\ b & 1-b \end{pmatrix}$. (b) $\begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$.

2.1.7 Nullmátrix.

2.1.8 Igaz: (a), (d).

2.1.9 Az állítás hamis, ellenpélda $A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$. A hibás indoklásban a szorzás kommutativitásának a feltételezése van elbújtatva.

2.1.10 A B-vel balról, illetve jobbról történő szorzás hatására A első sora, illetve oszlopa 5-tel szorzódik.
C balról: az első sorhoz hozzáadódik a második sor 6-szorosa.
C jobbról: a második oszlophoz hozzáadódik az első oszlop 6-szorosa.

2.1.11 A sorok, illetve oszlopok permutálódnak.

2.1.12 0.

2.1.14 1.

2.1.15 Útmutatás: A^2-ben a közvetlenül a főátló felett álló elemek is 0-k, A^3-ben az ezek felett állók is stb.

2.1.16 $A^p = E$(= a 2.1.3 feladatbeli egységmátrix).
Útmutatás: Írjuk fel a mátrixot $A = E + B$ alakban, és a hatványozásnál használjuk fel (most jogosan) a binomiális tételt és az előző feladatot.

2.1.17 Útmutatás: szorozzunk be $A - E$-vel.

2.1.18 $A = \lambda E$.

2.1.19 γ_{im} azt mutatja, hogy az i-edik termékhez az m-edik anyagból mennyit kell felhasználni.

2.1.20 A skalárszorosra vonatkozó azonosság az adjungáltnál $(\lambda A)^* = \overline{\lambda} A^*$ alakra módosul.

2.1.21 $A = 0$.
A komplex esetben (a transzponált helyett) az adjungálttal kell szorozni.

2.2.

2.2.1 Igaz: (a), (b).

2.2.2 Igaz: (a), (b), (g).

2.2.3 Igaz: (a), (c).

2.2.4 (a) és (d) invertálható, az inverzük

$$\begin{pmatrix} -2 & 1 \\ 3/2 & -1/2 \end{pmatrix}, \text{ illetve } \begin{pmatrix} -3/2 & 5/2 & -1 \\ 1/2 & -7/2 & 2 \\ 1/2 & 3/2 & -1 \end{pmatrix}.$$

(b) és (c) nullosztók, egy-egy (mindkét oldali) nullosztópár

$$\begin{pmatrix} 6 & -2 \\ -3 & 1 \end{pmatrix}, \text{ illetve } \begin{pmatrix} 1 & 3 & -2 \\ -2 & -6 & 4 \\ 1 & 3 & -2 \end{pmatrix}.$$

2.2.5 A determinánsuk ± 1.
Útmutatás: kövessük a 2.2.2 Tétel bizonyításának a gondolatmenetét.

2.2.6 Pontosan akkor van inverze, ha a főátlóban egyik elem sem nulla. Az inverze is felsőháromszög-mátrix lesz.

2.2.7 Igaz: (a), (c), (f).
Útmutatás (f)-hez: Ha $\det A \neq 0$, akkor A^{-1} segítségével kaphatjuk meg X-et. Ha $\det A = 0$, akkor alkalmas $C \neq 0$-val $AC = 0$ és így bármely X-re $AX = A(X + C)$.

2.2.8 1.5.5: Általánosan, ha $f_i = \beta_{i,0} + \beta_{i,1}x + \ldots + \beta_{i,n-1}x^{n-1}$, akkor a keresett determináns a β_{ij}-kből $(0 \leq i, j \leq n-1)$ képzett determinánsnak és a $V(a_1, \ldots, a_n)$ Vandermonde-determinánsnak a szorzata.
1.5.6: $V(\alpha_1, \ldots \alpha_n)V(\beta_1, \ldots, \beta_n)$.
1.5.7:

$$\begin{vmatrix} 1 & \binom{n-1}{1}\alpha_1 & \binom{n-1}{2}\alpha_1^2 & \ldots & \alpha_1^{n-1} \\ 1 & \binom{n-1}{1}\alpha_2 & \binom{n-1}{2}\alpha_2^2 & \ldots & \alpha_2^{n-1} \\ \vdots & \vdots & \vdots & & \vdots \\ 1 & \binom{n-1}{1}\alpha_n & \binom{n-1}{2}\alpha_n^2 & \ldots & \alpha_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} \beta_1^{n-1} & \beta_2^{n-1} & \ldots & \beta_n^{n-1} \\ \beta_1^{n-2} & \beta_2^{n-2} & \ldots & \beta_n^{n-2} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \ldots & 1 \end{vmatrix}$$

2.2.9 $A^2 = E$ pontosan azt jelenti, hogy $A = A^{-1}$, a másik feltétel pedig azt, hogy $\hat{A} = \pm A$. Használjuk fel a 2.2.2 Tételből az inverzre kapott képletet, valamint a 2.2.3 Lemmát és a determinánsok szorzástételét.

2.2.10 Alkalmazzuk a 2.2.3 Lemmát A-ra, majd $\hat{A}$-ra is. A kérdéses mátrix az A mátrix $(\det A)^{n-2}$-szerese lesz.

2.2.11 Írjuk fel a 2.2.3 Lemmát A-ra és B-re is.
Komplex esetben $A = \rho \cdot B$, ahol ρ egy $n-1$-edik komplex egységgyök.

2.2.12

(a),(b) „Ugyanaz", mint a valós test.

(c) Kommutatív, egységelemes, azoknak az elemeknek van inverze, amelyekre $a \neq \pm b$, a többi (nem nulla) elem pedig kétoldali nullosztó.

(d) „Ugyanaz", mint a komplex test.

(e) Nem kommutatív, minden $\begin{pmatrix} 1 & b \\ 0 & 0 \end{pmatrix}$ mátrix bal oldali egységelem, jobb oldali egységelem nincs, minden (nem nulla) elem jobb oldali nullosztó, a bal oldali nullosztók pedig a $\begin{pmatrix} 0 & b \\ 0 & 0 \end{pmatrix}$ mátrixok ($b \neq 0$).

2.2.14 $3 \mid n$.
Szükségesség: használjuk a determinánsok szorzástételét.
Elégségesség: $n = 3$-ra megfelel egy olyan 0, 1 és 2 elemű mátrix, amellyel egy mátrixot balról megszorozva permutálja annak sorait és közben az egyik sort 2-vel is megszorozza (vö. a 2.1.10 és 2.1.11 feladattal). Tetszőleges $3 \mid n$ esetén a mátrixot rakjuk össze ilyen hármas blokkokból.

3. Lineáris egyenletrendszerek

3.1.

3.1.2 Ekvivalens változtatások: (a), (d).
Más test felett esetleg (d) ekvivalenciája sem marad érvényben, ilyen T pl. a modulo 2 test.

3.1.3

(a) $x = 1, y = -1, z = 2$.

(b) Nincs megoldás.

(c) $x = -2 + \nu, y = 5 - \nu, z = \nu$, ahol ν tetszőleges valós szám.

3.1.4 25.

3.1.5

(a) $x_1 = -i\nu$, $x_2 = \nu$, $x_3 = i$, ahol ν tetszőleges komplex szám.

(b) $x_1 = 0$, $x_2 = 1$, $x_3 = i$, $x_4 = -1$, $x_5 = -i$.

3.1.6 Ha n páratlan, akkor $x_1 = x_2 = \ldots = x_n = 1/2$. Ha n páros, akkor $x_1 = x_3 = \ldots = x_{n-1} = 1-\nu$, $x_2 = x_4 = \ldots = x_n = \nu$, ahol ν tetszőleges valós szám.

3.1.7 m és n relatív prímek.

3.1.8 $x_1 = n+1$, $x_2 = x_3 = \ldots = x_{n-1} = 0$, $x_n = -1$.

3.1.9 (a) p^{n-2}. (b) p^2.

3.1.10 (d)-hez legyen T a modulo 7 test.
A második résznél (b) és (d) nem lehetséges.

3.1.11 Az ismeretlenek száma a vezéregyesek és a szabad paraméterek számának az összege.

3.1.12 Útmutatás: az RLA segítségével lássuk be, hogy legalább $n-k$ szabad paraméter van.

3.1.13 Útmutatás: Ha H egynél több elemű, akkor van olyan $\mathbf{x}'$ és $\mathbf{x}''$ megoldás, amelynél $x_1' \neq x_1''$. Ha (i) $\lambda_1+\lambda_2 = 1$, akkor $\mathbf{x}^* = \lambda_1\mathbf{x}'+\lambda_2\mathbf{x}''$ is megoldás, és (ii) $x_1^* = \lambda_1 x_1' + \lambda_2 x_1''$. Lássuk be, hogy tetszőlegesen előírt x_1^*-hoz lehet olyan λ_i-ket találni, amelyek (i)-et és (ii)-t kielégítik.
Másik lehetőség (továbbra is feltesszük, hogy H egynél több elemű): használjuk fel az RLA segítségével x_1-re kapott paraméteres előállítást.
Még ügyesebben és minden számolás nélkül is célhoz érhetünk, ha a Gauss-kiküszöbölést úgy végezzük, hogy x_1-et vesszük utolsó ismeretlennek, ekkor ugyanis x_1 biztosan szabad paraméter lesz, amire az állítás nyilvánvaló.

3.1.14 A kétismeretlenes egyenleteknek a koordinátageometria alapján a sík egyenesei felelnek meg, megoldás pedig ezek metszéspontja. Egy egyenletrendszer tehát pontosan akkor oldható meg, ha az összes egyenesnek van közös pontja. Hasonló módon a háromismeretlenes egyenleteknek a tér egy-egy síkja felel meg. Háromnál több ismeretlen és/vagy más test esetén nincs lehetőség ilyen közvetlen geometriai megfeleltetésre.

3.1.15 A mátrixműveletek tulajdonságai alapján

$$A\mathbf{x}'' = A\mathbf{x}' \iff A(\mathbf{x}''-\mathbf{x}') = \mathbf{0}.$$

3.1.16 Igaz: (a), (c), (f).

3.1.17 Ábel nem tudja kitalálni Béla számainak a paritását.
Béla ki tudja találni Ábel számainak a paritását és 5 a minimális kérdésszám.

3.1.18 Igaz: (a), (b).
Útmutatás (b)-hez: ha az együtthatók (beleértve a jobb oldalon álló konstansokat is) racionálisak, akkor a Gauss-kiküszöbölés során nem lépünk ki a racionális számok köréből.

3.1.19 Igaz: (b).
Útmutatás (b)-hez: egy nem triviális racionális megoldást a nevezők legkisebb közös többszörösével beszorozva, majd az így kapott egész számok legnagyobb közös osztójával végigosztva egy olyan egész megoldást kapunk, amelynek nem minden komponense osztható 11-gyel, és így a modulo 11 test felett tekintve is nem triviális megoldást jelent.

3.2.

3.2.1 A megoldás során érdemes különválasztani a valós és a képzetes részeket. A Cramer-szabályt itt a legjobban úgy lehet „alkalmazni", hogy az együtthatómátrix determinánsáról megmutatjuk, hogy nem nulla (lásd az 1.3.15 feladatot), tehát egyetlen megoldás van, és megpróbáljuk kitalálni ezt a megoldást. (Kitalálás helyett a képletbeli determinánsok kiszámítása sem okoz nehézséget, azonban ebben az esetben a Gauss-kiküszöbölés már gyorsabban célhoz vezet.)
Eredmény: $x_1 = x_3 = 1$, $x_2 = 2i$, $x_4 = 0$.

3.2.2 $x_1 = \ldots = x_n = 1$.

3.2.3 (a) $x_1 = \ldots = x_{n-1} = 0$, $x_n = n$. (b) $x_j = \prod_{i \neq j}(\beta - \alpha_i)/(\alpha_j - \alpha_i)$.

3.2.4 Igaz: (a).

3.2.5 Útmutatás: A feltételekből következik, hogy mindkét egyenletrendszernek mindig pontosan egy megoldása van.
(a) Ekkor bármely $\mathbf{x} \in T^n$-re $A_1\mathbf{x} = A_2\mathbf{x}$. Válasszuk $\mathbf{x}$-et rendre „egységvektoroknak", azaz legyen $\mathbf{x}$ egyik komponense 1, a többi 0.
(b) Lássuk be, hogy mindkét feltétel azzal ekvivalens, hogy $(A_1 - A_2)\mathbf{x} = \mathbf{0}$-nak csak triviális megoldása van.

3.2.6 Útmutatás:
(a) Térjünk át a modulo 7 testre. Ekkor egy olyan homogén lineáris egyenletrendszert kapunk, amelynek csak triviális megoldása van.
(b) Tetszőleges K-ra a helyes feltétel az, hogy a determináns (nemcsak hogy nem osztható K-val, hanem) relatív prím K-hoz. A bizonyítást először a prímhatvány esetre végezzük el a kitevő szerinti teljes indukcióval, majd lássuk be, hogy ha az állítás két, egymáshoz relatív prím K-ra igaz, akkor ezek szorzatára is teljesül.

3.2.7 Némi töprengés árán ki is találhatjuk a polinomokat! A 3.2.4 Tétel mellett a 3.2.10 és 3.2.11 feladatokban leírt módszereket is alkalmazhatjuk.
Eredmények: (a) $-x+11$; (b) $2x^2+1$; (c) ix;
(d) $2(x+1)(x^2+1)+1 = 2x^3+2x^2+2x+3$.

3.2.8
(a) 0 vagy 1.
(b) Végtelen test esetén végtelen sok, t elemű véges test esetén $t-1$.
Útmutatás (b)-hez: Ha g egy ilyen polinom, akkor $g-f$-nek mindegyik γ_i gyöke.
Másik lehetőség: Az eddigiekhez vegyünk hozzá egy új $\gamma_{n+1} \in T$ helyet, itt írjunk elő tetszőleges β_{n+1} értékeket, és vegyük az így keletkező interpolációs polinomokat. (Ez a módszer nem működik, ha T véges test és elemszáma éppen n.)

3.2.9 Ha két különböző polinom is lenne, akkor a különbségük is legfeljebb $n-1$-edfokú, ugyanakkor a különbségnek mind az n darab γ_i gyöke, ami ellentmondás.

3.2.10 Rendre behelyettesítve $\gamma_1, \dots, \gamma_n$-et, sorban meghatározhatjuk a $\nu_0, \dots, \nu_{n-1}$ együtthatókat. Ezzel beláttuk az interpolációs polinom *létezés*ét, továbbá azt, hogy a *feladatban megadott alakú* polinomok körében csak egyetlen megfelelő f van. Az interpolációs polinom *egyértelműség*ének bizonyításához (a ν_i együtthatók egyértelműségén kívül) még azt is igazolni kell, hogy más alakú polinom nem jöhet szóba, mégpedig azért nem, mert minden legfeljebb $n-1$-edfokú polinom előállítható (ráadásul egyértelműen) a szóban forgó alakban.

3.2.11
(a) Az L_i polinomban mindegyik $x-\gamma_j$, $j \neq i$ gyöktényező szerepel, és így a fokszámkorlátozás miatt L_i csak ezen gyöktényezők szorzatának a konstansszorosa lehet. A konstans szorzót az $L_i(\gamma_i) = 1$ feltételből kapjuk meg.
Eredmény: $L_i = \prod_{j \neq i}(x-\gamma_j)/(\gamma_i-\gamma_j)$.

3.2.12 (a) 1. (b1) 1. (b2) 0.

3.2.13
(a) Hamis. Ellenpélda: $x(x+1)/2$.
(b) Igaz. Útmutatás: elegendően sok helyet és helyettesítési értéket véve állítsuk elő a polinomot interpoláció segítségével (bármelyik módszerrel), és vegyük észre, hogy egyik eljárás sem vezet ki abból a testből, ahonnan a helyek és a felvett értékek valók.

3.2.14 A test *összes* elemével és a Φ függvény ezeken felvett értékeivel készítsük el a megfelelő interpolációs polinomot.

3.2.15 Ali Baba egy olyan 24-edfokú f polinomot választott, amelynek a konstans tagja a kulcsszám, és az i-edik rablónak az $f(i)$ értéket súgta meg.

3.3.

3.3.1
(i) Összefüggők, és bármelyik vektor kifejezhető a másik kettővel, pl. $\mathbf{u}_1 = 3\mathbf{u}_3 - 2\mathbf{u}_2$.
(ii) Függetlenek.

3.3.2 Csak a (ii)-beli vektorok függetlenek, a modulo 3 test felett tekintve pedig ezek sem.

3.3.3 Igaz: (b).

3.3.4 Igaz: (a), (c).

3.3.5 Csak $\mathbf{v} = \mathbf{0}$ lehetséges.

3.3.6 Szükségképpen függetlenek.

3.3.7 (a) Igen. (b) Nem.

3.3.8 Függetlenek: (a), (d), a többiek összefüggők.
A módosított feladatban az (a)-beliek lehetnek függetlenek is és összefüggők is, a többiek szükségképpen összefüggők.

3.3.9 (aα), (bα), (bβ) szükségképpen összefüggők, a többi három esetben lehetnek akár összefüggők, akár függetlenek.

3.3.11
(a) Használjuk fel az előző feladatot.
(b) A sorekvivalens átalakítások nem változtatnak azon, hogy a megfelelő homogén lineáris egyenletrendszernek van-e nem triviális megoldása.

3.3.12 Lásd a 9.3.1 Tételt.

3.4.

3.4.1 Az oszlopoknál a 3.3.5/II Tételt, az aldeterminánsoknál a kifejtési tételt érdemes felhasználni.

3.4.2 $\binom{k}{h}\binom{n}{h}$.

3.4.3 (i) 2. (ii) 3. (iii) 1.

3.4.4 (a) 0 vagy 1. (b) 0, 1 vagy 2.

3.4.5 A rang a sorok és oszlopok számának a minimuma.

3.4.6 (b) és (c) hamis, (d) igaz.

3.4.8 A valós és a racionális test szerinti rang megegyezik, a mod 2 szerinti rang pedig legfeljebb ekkora (lehet sokkal kisebb is, lásd a 4.6.16 feladatot).

3.4.9 Igaz: (a).

3.4.11 Igaz: (a), (d).

3.4.12 Az „akkor” részt az igazolja, hogy elemi sor- és oszlopekvivalens átalakításokkal a rang nem változik. A „csak akkor” onnan következik, hogy mindkét mátrix olyan alakra hozható, ahol a „főátló” rangnyi számú egyessel kezdődik és minden más elem nulla; hozzuk az egyik mátrixot ilyen alakra, majd alkalmazzuk a másik mátrixból idevezető lépések inverzét.

3.4.13

(a) Vegyünk pl. egy olyan A mátrixot, amelynek az első négy oszlopa négy tetszőleges független vektor és $\mathbf{a}_5 = \mathbf{a}_1$, $\mathbf{a}_6 = \mathbf{a}_2$, $\mathbf{a}_7 = \mathbf{a}_3$.

(b) Útmutatás: bármelyik további oszlop előáll az r független oszlop közül akármelyik $r-1$ lineáris kombinációjaként.

(c) Felhasználhatjuk a 3.4.5 feladatot.

3.4.14

(a) Legyen pl. az első három oszlopból álló rész olyan, hogy ennek a résznek bármelyik 3 sora független, a többi oszlop pedig egyezzen meg az első oszloppal.

(b) Útmutatás: először a nem nulla aldeterminánsoraiban és oszlopaiban levő további elemekre igazoljuk az állítást.

(c) Felhasználhatjuk az 1.5.6 feladatot.

3.4.15 Igaz: (a), (d), (e).

3.4.16 11.

3.4.17 (a) Ha $r(A) \leq n-2$, akkor lássuk be, hogy $B = 0$. Ha $r(A) = n-1$, akkor használjuk fel, hogy egyrészt a kifejtési tételek szerint B bármely sorvektora kielégíti az $A\mathbf{x} = \mathbf{0}$ homogén egyenletrendszert, másrészt ennek az egyenletrendszernek a megoldásai $n-r(A) = 1$ szabad paraméterrel írhatók fel.

3.4.18 Igen: (c).

3.4.19 (a) k. (b) Ha $k > n$, akkor 1, ha pedig $k \leq n$, akkor $n-k+2$.

3.5.

3.5.1 (a) $\begin{pmatrix} 1 & 1 & 0 & -1 \\ 1 & 2 & -1 & -1 \\ 0 & -1 & 0 & 1 \\ -1 & -1 & 1 & 1 \end{pmatrix}$; (b) $\begin{pmatrix} 4 & -6 & 4 & -1 \\ -6 & 14 & -11 & 3 \\ 4 & -11 & 10 & -3 \\ -1 & 3 & -3 & 1 \end{pmatrix}$.

3.5.2

$$A^{-1} = \begin{pmatrix} n & -1 & -1 & \dots & -1 \\ -1 & 1 & 0 & \dots & 0 \\ -1 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \dots & 1 \end{pmatrix}; \quad B^{-1} = \begin{pmatrix} 1 & -2 & 1 & \dots & 0 \\ 0 & 1 & -2 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix};$$

$$C^{-1} = \begin{pmatrix} 2 & -1 & 0 & \dots & 0 & 0 \\ -1 & 2 & -1 & \dots & 0 & 0 \\ 0 & -1 & 2 & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 2 & -1 \\ 0 & 0 & 0 & \dots & -1 & 1 \end{pmatrix}.$$

3.5.3

(a) X minden oszlopa és Y minden sora $\lambda(1, 1, -1, -1)$ alakú.

(b) X minden oszlopa $(\lambda + 2\mu, -2\lambda - 3\mu, \lambda, \mu)$ alakú, Y minden sora $(\lambda - \mu, -2\lambda - \mu, \lambda, \mu)$ alakú.

3.5.4 Legyen pl. B a csupa 1-ből álló mátrix.

3.5.5 Páratlan n-re invertálható, és ($n > 1$-re) az inverz minden eleme $\pm 1/2$, mégpedig a főátlóban az előjel mindig $+$, innen soronként jobbra haladva és ciklikusan a főátlóhoz visszatérve a többi $n - 1$ elemnél váltakozva $-$ és $+$ (tehát a főátló előtt is mindig $+$).
Páros n-re nullosztó; $AB = 0$, illetve $CA = 0$ pontosan akkor teljesül, ha B minden oszlopa, illetve C minden sora $\lambda(1, -1, 1, -1, \dots, 1, -1)$ alakú.

3.5.6

(a) A 2.2.2 Tételre a 3.5 pontban adott új bizonyítás gondolatmenetét kell megfelelően módosítani.

(b) Pl. az előző két feladat segítségével gyárthatunk ilyen példát.

3.5.7 Nem következik. Ellenpéldát a 3.5.4 vagy 3.5.5 feladatból nyerhetünk.

3.5.8

(a) Lásd pl. a 3.5.3b feladatot.

(b) Legyen az $A\mathbf{x} = \mathbf{0}$, illetve $A^T\mathbf{y} = \mathbf{0}$ egyenletrendszer egy-egy (egyparaméteres) megoldásserege $\mathbf{x} = \begin{pmatrix} \lambda_1\gamma \\ \vdots \\ \lambda_n\gamma \end{pmatrix}$, illetve $\mathbf{y} = \begin{pmatrix} \mu_1\delta \\ \vdots \\ \mu_n\delta \end{pmatrix}$, ahol $\gamma, \delta \in T$ tetszőleges. Ekkor a B mátrix megfelel, ha $\beta_{ij} = \lambda_i\mu_j$.

(c) Csak $A = 0$ ilyen.

4. Vektorterek

4.1.

4.1.1 Vektortér: (b), (d), (e), (f), (h), (i), (j).

4.1.2 Vektortér: (a), (c), (d), (e), (j), (l), (m), (o).

4.1.3 Vektortér: (a), (b), (f), (g), (k).

4.1.4 P7: legyen T_1 a T_2 test részteste, ekkor $V = T_2$ vektortér a T_1 felett a T_2-beli műveletekre. Sőt, az is elég, hogy T_2 olyan kommutatív gyűrű, amelynek az egységeleme megegyezik a T_1 test egységelemével.

4.1.5 Igen. (Ennek „mélyebb" magyarázatát lásd az 5.2.2 feladatban.)

4.1.6 Igen. (Ennek „mélyebb" magyarázatát lásd az 5.2.2 feladatban.)

4.1.7 Nem.

4.1.8

(a) Nem. Útmutatás: pl. $\lambda = 1/2$, $v = 3$ bajt okoz.

(b) Nem. Útmutatás: az (a)-beli gondolatmenetet csak olyan testeknél kell módosítani, amelyekben „nincs $1/2$".

(c) Igen. Útmutatás: van az egész számokkal azonos számosságú halmaz, amely jól ismert vektorteret ad.

(d) Nem. Útmutatás: lássuk be, hogy V számossága nem lehet kisebb T számosságánál.

(e) Igen. Útmutatás: a valós számsorozatokat próbáljuk meg komplex számsorozatokként tekinteni.

(f) Igen. A megoldáshoz komolyabb lineáris algebrai meggondolások kellenek, amelyekkel azt a meglepő tényt lehet megmutatni, hogy a komplex számok az összeadásra nézve és a valós számok az összeadásra nézve *izomorf* struktúrát (csoportot) alkotnak. Tekintsük ugyanis a valós számokat és a komplex számokat a racionális test feletti szokásos vektorterekként.

Ekkor számossági megfontolások alapján ezek (Hamel-)bázisa azonos számosságú, tehát a két vektortér dimenziója megegyezik, és így izomorfak — lásd a 4.5 és 5.2 pontok végén szereplő megjegyzéseket is.

4.1.9 Mindegyik esetben csak egyetlen axióma nem teljesül, ezek: (a) (S1); (b) (S1); (c) (S4); (d) (S3).

4.1.10

(ii) Induljunk ki a $(0+\lambda)\mathbf{v} = \lambda\mathbf{v}$ összefüggésből.

(iii) Induljunk ki az $(1+(-1))\mathbf{v} = 0\mathbf{v}$ összefüggésből.

(iv) Ha $\lambda \neq 0$, akkor $\lambda\mathbf{v} = \mathbf{0}$ mindkét oldalát szorozzuk meg a λ^{-1} skalárral.

4.1.11 Igaz: (a), (b).

4.1.12 (S4)-ből (a) triviálisan következik, (b) pedig éppen a 4.1.2 Tétel (iv) állítása. A megfordításokhoz az (a) esetben $1\mathbf{v} = 1(\lambda\mathbf{v})$ jobb oldalát alakítsuk tovább, a (b) esetben pedig induljunk ki az $1(1\mathbf{v}+(-\mathbf{v}))$ kifejezésből.

4.1.13 Bontsuk fel kétféleképpen az $(1+1)(\mathbf{u}+\mathbf{v})$ kifejezést.

4.1.14 Néhány ilyen példát ad a 4.1.9 feladat.
Az összeadási axiómák függetlenségének bizonyításához jól használható a következő észrevétel: ha minden $\mathbf{v}$-re $\mathbf{v}+\mathbf{v} = \mathbf{v}$ és a skalárral való szorzás $\lambda\mathbf{v} = \mathbf{v}$-vel van definiálva, akkor a skalárral való szorzásra vonatkozó axiómák valamennyien teljesülnek.
Legnehezebb az (S2) függetlenségének az igazolása, ehhez útmutatás: legyen $V = \mathbf{C}^2$, $T = \mathbf{C}$, az összeadás a szokásos és a skalárral való szorzásnál $\lambda\mathbf{v}$ értékét $\mathbf{v}$ bizonyos tulajdonságaitól függően hol a λ-val, hol pedig a $\overline{\lambda}$-tal történő szokásos szorzással definiáljuk.

Elvi problémákat vet fel az (Ö3), és még inkább az (Ö), illetve az (S) axiómák függetlenségének a kérdése. Ha (Ö3) nem teljesül, akkor az (Ö4) tulajdonképpen értelmetlen, hiszen ellentettről csak akkor beszélhetünk, ha van nullelem. Ennek ellenére *formálisan* felvethetjük (Ö3) függetlenségét is a következő módon: nincs nullelem, de létezik egy olyan **0**-val *jelölt* [és az (Ö4)-en kívül más axiómában szerepet nem játszó] elem, hogy (Ö4) igaz [és persze (Ö3) kivételével az összes többi axióma is].

Még erőltetettebb a többi axióma megfelelő értelmezése, ha az (Ö), illetve az (S) axióma nem teljesül, hiszen ha gond van magával a művelettel, akkor nem szoktuk ennek a tulajdonságait vizsgálni. Előfordulhat azonban olyan eset, amikor azért a „legtöbb" elempárhoz megtörtént az egyértelmű hozzárendelés, ilyen például az osztás a valós számoknál. Ezért (Ö3)-nak és (Ö4)-nek még akkor is lehet értelme, ha (Ö) „csak parciálisan teljesül", az azonosságokat pedig (nagyon mesterkélten) úgy lehet felfogni, hogy minden olyan esetben érvényesek, amikor mindkét oldal valóban létezik.

4.2.

4.2.1 Mindhárom feladat egy-egy adott vektortér bizonyos részhalmazairól azt kérdezi, hogy azok alteret alkotnak-e.

4.2.2 Altér: (a), (b), (h), (i), (j).

4.2.3 A magtér meghatározása egy homogén lineáris egyenletrendszer megoldását jelenti. A képtér esetében azt kell eldönteni, hogy egy adott együtthatómátrixú egyenletrendszer a „jobb oldal" mely értékeire oldható meg. Ehhez a jobb oldalt célszerű paraméterként tekinteni, és így elvégezni a Gauss-kiküszöbölést. Az adott A mátrixra

$$\operatorname{Ker} A = \left\{\lambda \begin{pmatrix} 2 \\ -3 \\ 0 \\ 1 \end{pmatrix} + \mu \begin{pmatrix} 1 \\ -2 \\ 1 \\ 0 \end{pmatrix}\right\}, \qquad \operatorname{Im} A = \left\{\alpha \begin{pmatrix} -1 \\ 0 \\ 1 \end{pmatrix} + \beta \begin{pmatrix} 2 \\ 1 \\ 0 \end{pmatrix}\right\},$$

ahol λ, μ, α, $\beta \in T$. (Mindkét altér másfajta paraméterezésekkel vagy más egyéb formában is megadható.)

4.2.4 Az F_p testek felett (a) nem valósulhat meg.

4.2.5 Válasz: (a), (b), (c), (e).
Az (a), (b) és (c) feltételek bármelyike *ekvivalens* azzal, hogy W altér, az (e) feltétel pedig pontosan a $W = V$ esetben teljesül.

4.2.6 Igaz: (b), (c).

4.2.7

(a) $\mathbf{u}$ és $\mathbf{v}$ vagy mindketten W-beliek, vagy egyikük sem az.
(b) $\mathbf{u}$ és $\mathbf{v}$ közül legfeljebb az egyik W-beli.
(c) $\mathbf{u}$ és $\mathbf{v}$ mindketten W-beliek.
(d) $\mathbf{u}$ és $\mathbf{v}$ egyike sem W-beli.
(e) $\mathbf{u}$ és $\mathbf{v}$ közül legfeljebb az egyik W-beli. (Ne felejtsük el megmutatni, hogy megvalósulhat az az eset is, amikor pontosan az egyikük W-beli, és az is, amikor egyikük sem esik W-be.)

Más test felett: pl. F_{11} esetén (c) úgy is teljesülhet, ha $\mathbf{u}$ és $\mathbf{v}$ egyike sem W-beli.

4.2.8 $5\mathbf{u} + 3\mathbf{v} + \mathbf{w} \notin W$, $6\mathbf{u} + 3\mathbf{v} + \mathbf{w} \in W$.

4.2.9 Egyetlen vektor skalárszorosaiból állnak.

4.2.10 Ha V a síkvektorok szokásos vektortere, akkor az origón átmenő egyenesek megfelelnek. Ezt a következőképpen általánosíthatjuk tetszőleges vektortérre: ha $\mathbf{a} \neq \mathbf{0}$ és $\mathbf{b}$ nem skalárszorosa $\mathbf{a}$-nak, akkor a

$\mathbf{c}_\mu = \mathbf{a} + \mu\mathbf{b}$ vektor összes skalárszorosai minden $\mu \in T$ esetén más és más alteret adnak.

4.2.11 5; $p + 3$.

4.2.12

(b) Valamelyik tartalmazza a másikat.
(c) Nem.
(d) Általában nem, de az F_2 test feletti vektorterekben előfordulhat.
(g) Útmutatás: F_2^2-re ez a 4.2.11 feladatból következik. Ugyanígy igazolható bármely T felett T^2-re is. Az általános esetet úgy vezethetjük vissza erre, hogy V-ben veszünk egy „nagy" alteret, amelyet egy „2-dimenziós" altérrel „kibővítve" megkapjuk az egész V-t.

4.2.14 V nem vektortér.

4.2.15 Csak (d) helyes.

4.2.16

(a) A térvektoroknál a pontok, az egyenesek, a síkok és maga a tér.
(c) Legyen $\mathbf{u}$ közös eleme a két sokaságnak. Lássuk be, hogy $\mathbf{v}$ pontosan akkor lesz ilyen közös elem, ha $\mathbf{v} - \mathbf{u}$ benne van a két altér metszetében.
(d) Ha $\mathbf{a} = \mathbf{u} + \mathbf{w}_1$, $\mathbf{b} = \mathbf{u} + \mathbf{w}_2$, $\mathbf{c} = \mathbf{u} + \mathbf{w}_3$, $\mathbf{w}_i \in W$, akkor az altér tulajdonságainak felhasználásával adódik, hogy $\mathbf{a} + \lambda(\mathbf{b} - \mathbf{c})$ is ilyen alakú. A megfordításhoz próbáljuk meg L elemeiből előállítani a megfelelő W-t, és a feltétel segítségével igazoljuk, hogy ez valóban altér.

4.2.17 A fő problémát az jelenti, hogy az $\mathbf{u} + W$ sokaság nem határozza meg egyértelműen magát az $\mathbf{u}$ vektort. Ezért először azt kell igazolni, hogy a műveletek nem függnek attól, hogy a sokaságot melyik $\mathbf{u}$-val „reprezentáltuk".

4.3.

4.3.1 Csak a (c) generátorrendszer.

4.3.2 A 4.1. pont példái közül: P1, P2, P3, P7. — A 4.1.1 feladatban: (b). — A 4.1.2 feladatban: (c), (l), (m). — A 4.1.3 feladatban: nincs ilyen.

4.3.3 Igaz: (a), (d), (e).

4.3.4 Igaz: (a), (c), (e).

4.3.6 Igaz: (c), (e).

4.3.7 Csak $\mathbf{c} = \mathbf{0}$ lehetséges.

4.3.8 Ha két altér mindegyike kielégíti a feltételeket, akkor (iii) alapján ezek kölcsönösen tartalmazzák egymást, tehát egyenlőek.

4.3.9 Lássuk be, hogy ez a metszet kielégíti a 4.3.4 Tétel (i)–(iii) követelményeit.

4.3.10 (a), (b), (d), (e) V. (c) $\{f \mid f(x) = 0, \text{ ha } x \neq 5,\ x \neq 6\}$.
Direkt összeg: (a), (c), (d).

4.3.12
(a) $\langle W_1, W_2\rangle \cap W_3 \supseteq \langle W_1 \cap W_3\,,\ W_2 \cap W_3\rangle$.
(b) $\langle W_1 \cap W_2\,,\ W_3\rangle \subseteq \langle W_1, W_3\rangle \cap \langle W_2, W_3\rangle$.
Az (a) és (b) résznél általában *nem* áll fenn egyenlőség. Ez is mutatja, hogy a generátum és az egyesítés tulajdonságai alapvetően eltérnek egymástól.
(c) A két altér egyenlő.

4.3.13 (a) Nem ($W \cap Z \neq \mathbf{0}$). (b) és (c) Igen. (d) Nem (Z nem altér).
(e) Igen. (f) Nem ($\langle W, Z\rangle \neq V$).

4.3.14 Több altér által generált altér (egyik lehetséges) definíciója:

$$\langle W_1, \ldots, W_k\rangle = W_1 + \ldots + W_k = \{w_1 + \ldots + w_k \mid w_i \in W_i\}.$$

A 4.3.6 Tétel általánosítása: az elemek ilyen előállítása akkor és csak akkor egyértelmű, ha

$$W_i \cap \langle W_1, \ldots, W_{i-1}\,,\ W_{i+1}\,,\ \ldots\,,\ W_k\rangle = \mathbf{0}, \quad i = 1, 2, \ldots, k.$$

Ebben az esetben a W_i-k által generált alteret a W_i-k direkt összegének hívjuk. Jelölés: $W_1 \oplus \ldots \oplus W_k$. Ez sokkal erősebb megkötést jelent, mint az, hogy az összes altér metszete $\mathbf{0}$, például a sík *nem* direkt összege három, az origón átmenő különböző egyenesnek.

4.3.15 Ha a részhalmaz altér, akkor az általa generált altér nyilván önmaga. A többi esetben:
4.1.1: (a) a legfeljebb 100-adfokú polinomok és a 0; (c), (g), (k), (l), (m) az összes polinom.
4.1.2: (b), (g), (h), (i) az összes sorozat; (f) a konvergens sorozatok; (k) a (j)-beli sorozatok.
4.1.3: (c) a (b)-beli függvények; (d), (e), (i), (j), (l), (m) az összes függvény.

4.3.16 (a) $f \in \langle H \rangle$. (b) $g \notin \langle H \rangle$. (c) Nem változik a helyzet.
Útmutatás (c)-hez: A feladat átfogalmazható arra, hogy egy racionális együtthatós, végtelen sok egyenletből álló, de csak véges sok ismeretlent tartalmazó egyenletrendszernek van-e megoldása. A Gauss-kiküszöbölés segítségével igazoljuk, hogy ez nem függ attól, hogy az ismeretleneket a racionális vagy a valós számok körében keressük.

4.3.17 Csak (c) generátorrendszer.
Útmutatás (b)-hez: Nem állítható elő például egy olyan sorozat, melynek az elemei egy *transzcendens* szám különböző hatványai. (A transzcendens szám definícióját lásd az A.10 pontban, az A.10.6 Definíció után.) Ennek igazolásához írjuk fel a feladatot egy (végtelen sok egyenletet, de csak véges sok ismeretlent tartalmazó) egyenletrendszer formájában, és alkalmazzuk a Gauss-kiküszöbölést vagy az algebrai bővítések elemi tulajdonságait (lásd az A.10 pontot).

4.4.

4.4.1 Igaz: (b), (e), (g), (i), (j).

4.4.2 (a) Összefüggő. (b) Független.
(c) Lehet összefüggő, lehet független.

4.4.3 Következik.

4.4.4 A 4.4.3 Tétel III. állításának bizonyításához hasonlóan adódik.

4.4.5 Ha $s \geq 2$ és $\mathbf{v}$, $\mathbf{u}_1$, …, $\mathbf{u}_{m-s}$ lineárisan független, akkor megfelel például $\lambda_1\mathbf{v}$, …, $\lambda_s\mathbf{v}$, $\mathbf{u}_1$, …, $\mathbf{u}_{m-s}$, ahol λ_1, …, λ_s különböző $\neq 0$ skalárok.

4.4.6 Igaz: (a), (c).

4.4.7 Függetlenek.

4.4.8 Csak $\mathbf{d} = \mathbf{0}$ lehetséges.

4.4.9 Független: (a), (d). Összefüggő: (b), (c), (f).
Lehet összefüggő, lehet független: (e), (g).

4.4.10 (a) m páratlan. (b) $(k\,,\,m) = 1$.

4.4.11 Csak (c) nem igaz.

4.4.12 Használjuk fel (a) a számelmélet alaptételét; (b) a transzcendens szám definícióját.

4.5.

4.5.1 A bázisok elemszáma:
(a) 11; (b) 18; (c) 19; (d) 20; (e) 20; (f) 20; (g) 19.

4.5.2 Bázis: (a), (d). Független, de nem bázis: (f).
Generátorrendszer, de nem bázis: (b).

4.5.3 Mindkét fogalom azonos a bázissal. (Használjuk fel a 4.5.3 Tételt.)

4.5.4 Alkalmazzuk a 4.5.4 Tételt.

4.5.6 Összefüggő.

4.5.7 Igaz: (b), (c), (f).

4.5.8 (a) Egyik sem. (b) Független, de nem generátorrendszer.
(c) Bázis, ha n páratlan, és egyik sem, ha n páros.
(d) Bázis. (e) Generátorrendszer, de nem független.

4.5.9 Elég a függetlenséget vizsgálni.

4.5.11 Útmutatás: Írjuk fel a $\mathbf{v}_i$-ket a 4.5.10 feladat szerint. Lássuk be, hogy van olyan j, amelyre $\beta_{ij} \neq 0$, valamint a β_{rs}-ekből képezett determinánsban az A_{ij} előjeles aldeterminánsa sem nulla. Ekkor $\mathbf{v}_j$ kielégíti a feladat feltételeit.

4.5.12
(a) Van.
(b) Nincs. (Írjuk fel a vektortér elemeit egy bázis segítségével.)
(c) Lássuk be, hogy minden véges test tartalmaz egy F_p testet, és fölötte vektortér (vö. az A.11 ponttal).
(d) Használjuk fel (c) eredményét.

4.5.13 Útmutatás: használjuk fel pl. a 4.5.7 Tételt.

4.5.14 Útmutatás (a)-hoz és (b)-hez: F_p^n-ben az első báziselem $(p^n - 1)$-féleképpen választható, a következő $(p^n - p)$-féleképpen stb. Az eredmény éppen a (c) részben a jobb oldali szorzat.

4.6.

4.6.1 (a) 2. (b) ∞. (c) $n(n+1)/2$. (d) ∞.
(e) p. Útmutatás: használjuk fel a 3.2.14 feladat állítását is.
(f) 84. (g) 210. (h) 20. (i) $n - r$. (j) Oszlopszám – rang.
(k) Rang.

4.6.2 Bázis: (a), (b), (c).
Útmutatás (d)-hez: már az első 8 vektor is lineárisan összefüggő.

4.6.3 Vegyünk k független vektor által generált alteret.

4.6.4 Használjuk fel, hogy A minden oszlopára ugyanaz a feltétel adódik.

4.6.5 Induljunk ki abból, hogy W_1 és W_2 bázisának egyesítése már összefüggő.

4.6.6

(a) W_1 és W_2 bázisának egyesítése generátorrendszer $\langle W_1, W_2\rangle$-ben.

(c) $W_1 \cap W_2$ bázisát bővítsük ki W_1, illetve W_2 bázisává.

4.6.7 (a) ∞. (b) 101, 101, 102.

4.6.8 $\varphi_n = \frac{1}{\sqrt{5}}\Big(\big(\frac{1+\sqrt{5}}{2}\big)^n - \big(\frac{1-\sqrt{5}}{2}\big)^n\Big)$.
Az útmutatás szerinti részeredmények: (i) 2; (ii) keressünk mértani sorozatokat.
A részletes levezetést lásd a 9.2.1 Tétel első bizonyításában és az utána szereplő megjegyzésben.

4.6.9 A kilenc ismeretlenre adódó összefüggéseket felírva egy olyan egyenletrendszert kapunk, amelyben 3 szabad paraméter lesz. Szabadon választhatjuk pl. az α_{11}, α_{12} és α_{22} elemeket. Így bázist alkotnak azok a bűvös négyzetek, amelyekben a fenti elemek egyike 1, a másik kettő 0, a többi elem pedig a feltételekből egyértelműen meghatározható. Ezzel a paraméterezéssel az összes bűvös négyzet alakja

$$\begin{pmatrix} \beta & \gamma & 3\delta-\gamma-\beta \\ 4\delta-\gamma-2\beta & \delta & 2\beta+\gamma-2\delta \\ \beta+\gamma-\delta & 2\delta-\gamma & 2\delta-\beta \end{pmatrix}$$

4.6.10 (a) 3. (b) 3. (c) 4.

4.6.11 Útmutatás: az összegvektorok $k \geq 4$ esetén már összefüggők.

4.6.13 Vizsgáljuk az oszlopvektorok által generált alterek kapcsolatát.

4.6.14 Ha $r > 0$, akkor egy r-dimenziós alteret r független vektorral generálhatunk. Így azonban ugyanazt az alteret sokszor megkapjuk, mégpedig bármelyik bázisa szerint. Eredmény:

$$\frac{(p^n-1)(p^n-p)\dots(p^n-p^{r-1})}{(p^r-1)(p^r-p)\dots(p^r-p^{r-1})}\,.$$

4.6.15 Nyilván elég a $0 < r \leq \min(k,n)$ esettel foglalkozni. Legkevesebb számolással úgy érhetünk célba, ha T^k-ban kiválasztunk egy r-dimenziós alteret és ebben egy n elemű generátorrendszert. Eredmény:

$$\frac{(p^k-1)(p^k-p)\dots(p^k-p^{r-1})(p^n-1)(p^n-p)\dots(p^n-p^{r-1})}{(p^r-1)(p^r-p)\dots(p^r-p^{r-1})}\,.$$

4.6.16 (c) 1010.

4.7.

4.7.1
(a) A két megfelelő koordináta is felcserélődik.
(b) Az adott koordináta $1/\lambda$-val szorzódik.
(c) Az eredeti α_i és α_j koordinátákból α_i és $\alpha_j - \lambda\alpha_i$ lesz.

4.7.2 Csak a $\mathbf{0}$ ilyen.

4.7.3 Érdemes felhasználni a három vektorból képezett mátrix inverzét.
Eredmény: Az $\begin{pmatrix}1\\0\\0\end{pmatrix}$ vektornak a megadott bázis szerinti koordinátái 26, -21, 19, azaz

$$\begin{pmatrix}1\\0\\0\end{pmatrix} = 26\begin{pmatrix}1\\2\\5\end{pmatrix} - 21\begin{pmatrix}3\\7\\8\end{pmatrix} + 19\begin{pmatrix}2\\5\\2\end{pmatrix}.$$

A $\begin{pmatrix}0\\1\\0\end{pmatrix}$ vektor koordinátái: -10, 8, -7. A $\begin{pmatrix}0\\0\\1\end{pmatrix}$ vektor koordinátái: -1, 1, -1.

4.7.4 A $\mathbf{v}$ skalárszorosain kívül bármi lehet.

4.7.5 (a) Életben marad. (b) Nem marad életben.

5. Lineáris leképezések

5.1.

5.1.1 Nem lineáris leképezés: (b), (f), (h), (j), A többi lineáris leképezés, a magtér és képtér után zárójelben a dimenzió szerepel.
(a) Mag: konstans polinomok (1), kép: legfeljebb 99-edfokú polinomok (100).
(c) Mag: $\{\gamma x\}$ (1), kép: $\{f \mid \alpha_1 = 0\}$ (100).
(d) Mag: konstans polinomok (1), kép: legfeljebb 99-edfokú polinomok (100).
(e) Mag: x-szel osztható polinomok (100), kép: $\{\gamma x\}$ (1).
(g) Mag: azok a polinomok, amelyeknek az 1 gyöke (100), kép: $\{\gamma(x + x^2)\}$ (1).
(i) Mag: az x^7+4x+1-gyel osztható polinomok (94), kép: legfeljebb 6-odfokú polinomok (7).

5.1.2 Nem lineáris leképezés: (b), (c), (d), (g). A többi lineáris leképezés, a magtér és képtér után zárójelben a dimenzió szerepel.
(a) Mag: tiszta képzetes számok (1), kép: valós számok (1).
(e) Mag: a 0 (0), kép: $\mathbf{C}$ (2).
(f) Mag: a 0 (0), kép: $\mathbf{C}$ (2), kivéve ha a 0-val szoroztunk, amikor a mag: $\mathbf{C}$ (2), a kép a 0 (0).
(h) Mag: a 0 (0), kép: $\mathbf{C}$ (2).

5.1.3 Nem lineáris leképezés: (b), (d), (f). A többi lineáris leképezés, a magtér és képtér után zárójelben a dimenzió szerepel.
(a) Mag: azok a mátrixok, amelyeknek a középső oszlopa nulla (6), kép: T^3 (3).
(c) Mag: azok a mátrixok, amelyekben a főátló elemeinek az összege nulla (8), kép: a „csupaegy” vektor skalárszorosai (1).
(e) Mag: azok a mátrixok, amelyekben minden sor összege nulla (6), kép T^3 (3).

5.1.4 A magtér és képtér után zárójelben a dimenzió szerepel.
(a) Mag: 0 (0), kép: a 0-val kezdődő sorozatok (∞).
(b) Mag: azok a sorozatok, amelyekben legfeljebb a kezdő elem nem nulla (1), képt: minden sorozat (∞).
(c) Mag: 0 (0), kép: azok a sorozatok, amelyekben $\alpha_{2k} = \alpha_{2k+1}$, $k = 0, 1, 2, \ldots$ (∞).
(d) Mag: azok a sorozatok, amelyekben $\alpha_{10k} = 0$, $k = 0, 1, 2, \ldots$ (∞), kép: minden sorozat (∞).
(e) Mag: azok a sorozatok, amelyeknek minden eleme egyenlő (1), képtér: minden sorozat ∞.
(f) Mag: 0 (0), kép: minden sorozat ∞.
(g) Mag: a (γ, $-\gamma$, $-\gamma$, γ, γ, $-\gamma$, $-\gamma$, γ, ...) sorozatok (1), kép: azok a sorozatok, ahol $\alpha_{4k} + \alpha_{4k+1} = \alpha_{4k+2} + \alpha_{4k+3}$, $k = 0, 1, 2, \ldots$ (∞).

5.1.5 Nem.

5.1.6 Útmutatás (b)-hez: legyen $T = \mathbf{C}$.

5.1.7 $\dim V \leq 1$.

5.1.8 A valós test felett nem igaz.

5.1.9 Igaz: (b), (d).

5.1.10 Alkalmazzuk a 4.6.6 Tételt.

5.1.12 101^k, $k = 0, 1, 2, \ldots$ vagy ∞.

5.1.13 Útmutatás: $\mathbf{u}_i - \mathbf{u}_1 \in \operatorname{Ker} \mathcal{A}$, $i = 2, 3, \ldots, k$.

5.1.14 Útmutatás: ha egy tetszőleges $\mathbf{c}_1, \ldots, \mathbf{c}_n$ bázisra például $\mathcal{A}\mathbf{c}_1 \neq \mathbf{0}$ és $\mathcal{A}\mathbf{c}_i = \mathbf{0}$, akkor $\mathbf{c}_i$ helyett vegyük $\mathbf{c}_i + \mathbf{c}_1$-et.

5.1.16
(a) $\mathcal{A}U \cap \mathcal{A}Z \supseteq \mathcal{A}(U \cap Z)$, és általában nem áll fenn egyenlőség.
(b) $\mathcal{A}\langle U, Z\rangle = \langle \mathcal{A}U\,,\, \mathcal{A}Z\rangle$.

5.2.

5.2.1 5.1.1: nincs. 5.1.2: (e), (f) (kivéve, ha a 0-val szoroztunk), (h).
5.1.3: nincs. 5.1.4: (f).

5.2.2 4.1.5 a valós számok szokásos vektorterével, 4.1.6 pedig a komplex számok $\mathbf{Q}$ feletti, a szokásos műveletek szerinti vektorterével izomorf. A megfelelő izomorfizmusok $v \mapsto \lg v$, illetve $v \mapsto v + 1$.

5.2.3 (c), (d).

5.2.4 Használjuk az 5.2.5 Tételt.

5.2.5 $n + 1$.

5.2.6 (a), (b), (d), (f), (g), (i), (j) és (k) (ezek mind 8-dimenziósak);
(e) és (h) (ezek 43-dimenziósak).

5.3.

5.3.1 W egy bázisát egészítsük ki V egy bázisává, és ezen a bázison definiáljuk alkalmasan a transzformációt.

5.3.2 Ilyen a $\mathcal{O}$ leképezés akármilyen V_1 és V_2 esetén. Ezen kívül még a modulo 2 maradékosztályok teste felett $\dim V_1 = 1$ esetén a képtér, $\dim V_2 = 1$ esetén a magtér meghatározza a leképezést. Minden más esetben bármely leképezéshez van vele azonos magterű, illetve képterű tőle különböző leképezés (sőt néhány további kivételtől eltekintve olyan is, amelynek *mind* a képtere, *mind* pedig a magtere megegyezik az adott leképezés kép-, illetve magterével).

5.3.3
(a) 0 vagy 1. Ha az $\mathbf{u}_1, \ldots, \mathbf{u}_n$ generátorrendszer nem bázis, akkor mindig megadhatók a $\mathbf{c}_i$-k úgy, hogy ne létezzen ilyen leképezés, és úgy is, hogy pontosan egy ilyen leképezés létezzen.
(b) Legalább 1, és ha $\mathbf{u}_1, \ldots, \mathbf{u}_n$ nem bázis, akkor mindig több ilyen leképezés létezik, mégpedig legalább $|T|$ számosságú.

5.3.4 (a) 0. (b) 1. (c) ∞.

5.3.5 p^{kn}.

5.3.6 Útmutatás: ha $\dim V_1 \leq \dim V_2$, akkor a bázisok segítségével olyan $\mathcal{A}$ definiálható, amelyre $\operatorname{Ker}\mathcal{A} = \mathbf{0}$, ha pedig $\dim V_1 \geq \dim V_2$, akkor olyan, amelyre $\operatorname{Im}\mathcal{A} = V_2$.

5.4.

5.4.1 Pontosan a páros dimenziósak ilyenek.

5.4.2 (a), (b).

5.4.3 Igen.

5.4.4 Akármelyik feltételből következik az izomorfizmus.

5.4.5 Útmutatás: (i)-ből $\dim \operatorname{Im} \mathcal{A} \leq 3$, (ii)-ből pedig $\dim \operatorname{Ker} \mathcal{A} \leq 5$ következik.

5.4.6 Útmutatás: írjuk fel $\mathcal{A}$-ra is és $\mathcal{B}$-re is a dimenziótételt, és használjuk fel a véges dimenziós tér alterének dimenziójáról szóló 4.6.4 Tételt.

5.4.7 Útmutatás: alkalmazzuk a dimenziótételt és a direkt összeg dimenziójára vonatkozó 4.6.6b feladatot.

5.5.

5.5.2 (a) $\mathcal{O}$. (b) $\mathcal{E}$. (c) $\mathcal{E}$. (d) $(2\cos\Phi)\mathcal{E}$. (e) Forgatva nyújtás az origóból, a forgatás szöge $+45$ fok, a nyújtás aránya $\sqrt{2}$.

5.5.3 Altér: (c), (d); valamint (a), ha $V_1 = U_1$; (b), ha $\dim V_1 \leq 1$ vagy $\dim V_2 \leq 1$; (e), ha a V_2-beli megadott vektor nullvektor.

5.5.4 Kivételes esetektől eltekintve általában egyik sem altér.

5.5.5 Igaz: (a).

5.5.6 Útmutatás: Lássuk be, hogy bármely $\mathcal{A} \in \operatorname{Hom}(V_1, V_2)$ egyértelműen írható fel a $\mathcal{C}_{ij}$ leképezések lineáris kombinációjaként. Ehhez használjuk fel, hogy az $\mathcal{A}$ leképezés jellemezhető az $\mathbf{a}_j$ báziselemek képével, a képek pedig egyértelműen előállíthatók a $\mathbf{b}_i$ báziselemek segítségével. (Vö. az 5.7 ponttal.)

5.5.7 Azonnal következik az előző feladatból. (Vö. az 5.7.5 Tétellel.)

5.5.8 Csak (a) igaz.

5.5.9 (c) 7.

5.6.

5.6.1 Igen: (c), (d).

5.6.2 $\mathcal{AB}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix}=\begin{pmatrix}\alpha_3\\ \alpha_1\\ \alpha_2\end{pmatrix}$, $\mathcal{BA}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\end{pmatrix}=\begin{pmatrix}\alpha_2\\ \alpha_3\\ \alpha_1\end{pmatrix}$, $\mathcal{A}^{101}=\mathcal{A}$, $(\mathcal{AB})^{101}=\mathcal{BA}$.

5.6.3 $\mathcal{A}=\lambda\mathcal{E}$.

5.6.4 $\dim V\le 1$.

5.6.5 $\operatorname{Ker}\mathcal{AB}\supseteq\operatorname{Ker}\mathcal{B}$, $\operatorname{Im}\mathcal{AB}\subseteq\operatorname{Im}\mathcal{A}$.

5.6.6 Az első disztributivitást igazoljuk. $\mathcal{A}(\mathcal{B}+\mathcal{C})=\mathcal{AB}+\mathcal{AC}$ bármelyik oldala pontosan akkor értelmes, ha $\mathcal{A}\in\operatorname{Hom}(V_2\,,V_3)$, $\mathcal{B},\mathcal{C}\in\operatorname{Hom}(V_1\,,V_2)$. Bármely $\mathbf{x}\in V_1$-re a bal oldal

$$[\mathcal{A}(\mathcal{B}+\mathcal{C})]\mathbf{x}=\mathcal{A}[(\mathcal{B}+\mathcal{C})\mathbf{x}]=\mathcal{A}(\mathcal{B}\mathbf{x}+\mathcal{C}\mathbf{x})=\mathcal{A}(\mathcal{B}\mathbf{x})+\mathcal{A}(\mathcal{C}\mathbf{x})\,,$$

itt az utolsó lépésben felhasználtuk $\mathcal{A}$ linearitását. Ha a jobb oldalt alkalmazzuk egy $\mathbf{x}\in V_1$ vektorra, akkor ez a leképezések összeadásának és szorzásának definíciója alapján azonnal ugyanerre az alakra hozható.

5.6.7 Útmutatás: alkalmazzuk a dimenziótételt a $\mathcal{B}$ leképezésnek az $\operatorname{Im}\mathcal{A}$ altérre történő megszorítására.

5.6.8 Útmutatás: Lássuk be, hogy $\operatorname{Ker}\mathcal{A}^2\supseteq\operatorname{Ker}\mathcal{A}$, illetve $\operatorname{Im}\mathcal{A}^2\subseteq\operatorname{Im}\mathcal{A}$ mindig teljesül. Ezután írjuk fel a dimenziótételt $\mathcal{A}$-ra és $\mathcal{A}^2$-re is. Innen a dimenzió végességét még egyszer kihasználva kapjuk az első és a második feltétel ekvivalenciáját. Az első és a harmadik feltétel ekvivalenciája közvetlenül adódik (vagy felhasználhatjuk hozzá az előző feladat eredményét).

5.6.9 Legyen $V=\mathbf{R}^5$ és legyen $\mathcal{A}\mathbf{x}=A\mathbf{x}$ minden $\mathbf{x}\in V$-re. Nyilván $\operatorname{Im}\mathcal{A}^{k+1}\subseteq\subseteq\operatorname{Im}\mathcal{A}^k$, és ha valamilyen k-ra egyenlőség áll fenn, akkor onnantól kezdve

$$U=\operatorname{Im}\mathcal{A}^k=\operatorname{Im}\mathcal{A}^{k+1}=\operatorname{Im}\mathcal{A}^{k+2}=\dots$$

Mivel az egyenlőség a feladat feltétele szerint $U=\mathbf{0}$-val teljesül, továbbá a

$$V\supseteq\operatorname{Im}\mathcal{A}\supseteq\operatorname{Im}\mathcal{A}^2\supseteq\operatorname{Im}\mathcal{A}^3\supseteq\dots$$

láncban a dimenzió mindig legalább eggyel csökken, amíg U-hoz nem jutunk, így legkésőbb az ötödik lépésben szükségképpen már $\mathbf{0}$ lesz az eredmény. Ennek alapján $\mathcal{A}^5=\mathcal{O}$, és innen $A^5=0$. (A feladatra egy másik megoldást a *minimálpolinom* segítségével adhatunk, lásd a 6.3 pontot.)

5.6.10 $\mathcal{A}$-nak végtelen sok balinverze van, nincs jobbinverze, jobb oldali nullosztó, nem bal oldali nullosztó. $\mathcal{B}$-re a „bal" és „jobb" felcserélésével kapott analóg eredmények érvényesek. (Figyeljük meg, hogy $\mathcal{BA} = \mathcal{E}$, de $\mathcal{AB}$ nem az!)

5.6.11 (a) és (c) Az $\mathcal{A}$ és $\mathcal{C}$ transzformációnak nincs egyik oldala inverze sem, és kétoldali nullosztók, pl. $\mathcal{AC} = \mathcal{CA} = \mathcal{O}$.
(b) A $\mathcal{B}$ transzformáció nem nullosztó, és

$$\mathcal{B}^{-1} : \mathbf{b}_1 \mapsto \mathbf{b}_1,\ \mathbf{b}_2 \mapsto -\mathbf{b}_1 + \mathbf{b}_2,\ \ldots,\ \mathbf{b}_n \mapsto -\mathbf{b}_1 + \mathbf{b}_n\,.$$

5.6.12 $\dim V \leq 1$.

5.6.13 $\dim V \leq 1$.

5.6.14 (a) $\dim V \geq 2$. (b) Nincs ilyen $V(\neq \mathbf{0})$.

5.6.15 Bővítsük ki $\operatorname{Im}\mathcal{A}$ bázisát V bázisává, és definiáljuk $\mathcal{B}$-t ezen a bázison.

5.6.16 Igaz: (a), (b), (c).

5.6.17 $\dim B = \dim J = \dim V \cdot \dim \operatorname{Ker}\mathcal{A}$.

5.6.18
(a) Projekció például a síkon tetszőleges egyenesre történő vetítés.
(b) Projekció=vetítés.
(c) Csak az $\mathcal{E}$-nek.
(e) Például a modulo 2 test felett az „akkor" rész nem igaz.
(f) Lássuk be, hogy $\operatorname{Ker}(\mathcal{P} + \lambda\mathcal{E}) = \mathbf{0}$, illetve $\operatorname{Im}(\mathcal{P} + \lambda\mathcal{E}) = V$, vagy pedig keressük az inverzet $\alpha\mathcal{P} + \beta\mathcal{E}$ alakban.
(g) A megfelelő alterek $U_1 = \operatorname{Im}\mathcal{P}$ és $U_2 = \operatorname{Ker}\mathcal{P}$. Az „akkor" rész közvetlenül verifikálható, a „csak akkor" rész igazolásához használjuk fel a $\mathbf{v} = \mathcal{P}\mathbf{v} + {}$ $+(\mathbf{v} - \mathcal{P}\mathbf{v})$ felírást.

5.6.19 Útmutatás: a lényeg az, hogy a $\mathcal{B}$ transzformáció $\operatorname{Im}\mathcal{A}$ egy bázisához ezeknek a báziselemeknek egy-egy $\mathcal{A}$ szerinti ősképét rendelje hozzá.
Megjegyzés: az is elérhető, hogy egyúttal $\mathcal{BAB} = \mathcal{B}$ is teljesüljön.

5.6.20 Algebra: (a), (c), (d), (e), (g), (i) (ez utóbbi a kvaternióalgebrával izomorf).

5.6.21 (a) 0. (b) 3^{50}. (c) 8.

5.6.22

$$v\overline{v} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2, \qquad v^{-1} = \frac{1}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2}\overline{v} \quad (v \neq 0)\,.$$

5.6.23 Végtelen sok (az összes megoldás: $\alpha_1 i + \alpha_2 j + \alpha_3 k$, ahol $\alpha_1^2 + \alpha_2^2 + \alpha_3^2 = {}$ $= 1$). — A szóban forgó tétel *kommutatív* test felett érvényes.

5.6.24 n.
Útmutatás: ha a v kvaternió nem valós, akkor az $\alpha+\beta v$ alakú kvaterniók, ahol α, β valós, a komplex számokkal izomorf testet alkotnak.

5.6.25 Útmutatás: Legyen $c \neq 0$ tetszőleges rögzített eleme az A algebrának, és tekintsük a c-vel történő szorzást mint az A (vektortér) lineáris transzformációját, azaz legyen $\mathcal{C} : x \mapsto cx$ (ahol $x \in A$), ekkor $\mathcal{C} \in \operatorname{Hom} A$. A nullosztómentesség alapján $\operatorname{Ker}\mathcal{C} = 0$, így a véges dimenzió miatt $\operatorname{Im}\mathcal{C} = A$. Ez azt jelenti, hogy a $cx = d$ egyenlet bármely $d \in A$ esetén megoldható.

5.7.

5.7.1 (a)
$$\begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 3 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 4 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 5 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 6 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$
(b) és (c): van. [A (c) rész általánosítását lásd az 5.8.7b feladatban.]
(d) és (e): nincs.

5.7.4
(a) Az első két oszlop felcserélődik.
(b) Az első két sor felcserélődik.ű
(c) A harmadik oszlop λ-val szorzódik.
(d) A harmadik sor $1/\lambda$-val szorzódik.
(e) A harmadik oszlophoz hozzáadódik a második oszlop μ-szöröse.
(f) A második sorból levonódik a harmadik sor μ-szöröse.
Általában megfigyelhetjük, hogy az $\mathbf{a}_j$-knél történő változtatás hatása a mátrix *oszlop*aiban hasonló jellegű, ún. *„kovariáns"* változásként jelenik meg, ugyanakkor a $\mathbf{b}_i$-knél történő változtatás eredménye a mátrix *sor*aiban ellentétes jellegű, ún. *„kontravariáns"* változás lesz.

5.7.5 Van: (b), (c), (d).

5.7.6 Útmutatás: V_1-ben $\operatorname{Ker}\mathcal{A}$ egy bázisának kiegészítésével készítsünk bázist, V_2-ben pedig a $\operatorname{Ker}\mathcal{A}$-n kívüli báziselemek képeit egészítsük ki bázissá.

5.7.8 Útmutatás: ha $\mathbf{c} \notin \operatorname{Ker}\mathcal{A}$, akkor az $\mathcal{A}\mathbf{c}$, $\mathbf{c}$ bázis megfelel.

5.7.9 $\mathcal{A} = \lambda\mathcal{E}$.

5.7.10 Útmutatás: Egy nem nulla négyzetes mátrix akkor és csak akkor egyik vagy másik vagy mindkét oldali nullosztó, ha a determinánsa 0. A transz-

formációk és a mátrixok közötti megfeleltetést használva, ez utóbbi feltétel — a homogén lineáris egyenletrendszereknél tanultak alapján — azonnal a $\operatorname{Ker}\mathcal{A} \neq \mathbf{0}$ feltételre vezethető vissza.

5.7.11 Útmutatás: az „oszlopvektorok" által generált altér minden esetben éppen $\operatorname{Im}\mathcal{A}$.

5.7.12 Útmutatás: térjünk át a megfelelő leképezésekre, használjuk fel az előző feladatot, és alkalmazzuk a dimenziótételt az (b) részben $\mathcal{A}$-ra, az (a) részben pedig az $\mathcal{A}$-nak az $\operatorname{Im}\mathcal{B}$-re történő megszorítására.

5.7.13 Nem igaz, mert a síkon is van az identitáson kívül ilyen tulajdonságú lineáris transzformáció (keressük ezt a forgatások között).

5.7.14 (a) Vegyük minden báziselem λ-szorosát. (b) Pl. $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

5.8.

5.8.1 (a) $\begin{pmatrix} 1/2 & 3/2 & 1 \\ -1/2 & 1/2 & 1 \\ 1/2 & -1/2 & -1 \end{pmatrix}$; (b) $\begin{pmatrix} 1 & -1 & 1 \\ 1 & -2 & 1 \\ 1 & -3 & 1 \end{pmatrix}$; (c) $\begin{pmatrix} 0 & 1 & 0 \\ 1 & 0 & -1 \\ 0 & 1 & 0 \end{pmatrix}$.

5.8.3 Alkalmazzuk az 5.8.1A Tételt $\mathcal{A} = \mathcal{S}$-re.

5.8.4 Használjuk fel az 5.8.1A Tételt és a determinánsok szorzástételét.

5.8.5 (a) és (b) hamis, mindkettőre ellenpélda a legfeljebb elsőfokú polinomok vektortere és a deriválás. (c) és (d) igaz.

5.8.7 (a) $\mathcal{A} \neq \mathcal{O}$. (b) $\mathcal{A} \neq \lambda\mathcal{E}$.

5.8.8 Ha $\mathcal{A} = \lambda\mathcal{E}$, akkor bármely bázis megfelel, egyébként pedig keressük a kísérő transzformációt $\mathcal{S} = \mathcal{A} - \lambda\mathcal{E}$ alakban.

6. Sajátérték, minimálpolinom

6.1.

6.1.1 Sé=sajátérték, sv=sajátvektor (a 0 polinomot eleve kizárjuk), sd=sajátaltér dimenziója, dm=diagonális mátrix.

(a) Sé: 0, sv: konstans polinomok, sd: 1, dm: nincs.

(b) Sé: $0, 1, \ldots, 6$, sv: „egytagúak", sd: mindegyiké 1, dm: van.

(c) Sé: 0, 6^6, sv: $x-6$-tal osztható polinomok, illetve γx^6 alakú polinomok, sd: 6, illetve 1, dm: van.

(d) Sé: $0, 1$, sv: x^2+2x+3-mal osztható polinomok, illetve legfeljebb elsőfokú polinomok, sd: 5, illetve 2, dm: van.

6.1.2 Következik: $\mu\mathcal{A}$-ra, $\mathcal{A}^2$-re, illetve $\mathcal{A}^{-1}$-re, a megfelelő sajátértékek rendre $\mu\alpha$, α^2, illetve α^{-1}.

6.1.3 Mindegyik következik. Ha $\mathbf{v}$-hez $\mathcal{A}$-nál az α, $\mathcal{B}$-nél a β sajátérték tartozik, akkor a megfelelő sajátérték $\mathcal{A}+\mathcal{B}$-nél $\alpha+\beta$, $\mathcal{AB}$-nél $\alpha\beta$, a többi esetben pedig az előző feladatban megadott érték.

6.1.4 Igaz: (b), (c).
Útmutatás c)-hez: ha $\mathcal{A}^2\mathbf{v} = \mu^2\mathbf{v}$, akkor $(\mathcal{A}+\mu\mathcal{E})[(\mathcal{A}-\mu\mathcal{E})\mathbf{v}] = \mathbf{0}$ miatt vagy $\mathbf{v}$ sajátvektor μ sajátértékkel, vagy pedig $(\mathcal{A}-\mu\mathcal{E})\mathbf{v}$ sajátvektor $-\mu$ sajátértékkel.

6.1.5 Igaz: (a), (d), (e).

6.1.6 Pl. egy (origón átmenő) tengely körüli (nem $k\pi$ szögű) forgatás, egy (origón átmenő) síkra történő tükrözés, illetve a három tengely irányában eltérő mértékű nagyítás.

6.1.7 $\mathbf{u}$-hoz és $\mathbf{v}$-hez azonos sajátérték tartozik, de $\mathbf{u} \neq -\mathbf{v}$.

6.1.8 $\lambda\mathcal{E}$.

6.1.9 Bizonyítsunk k szerinti teljes indukcióval.

6.1.10 Következik az előző feladatból.

6.1.11 A magtér kétdimenziós, ezenkívül észre lehet venni egy, a 3 sajátértékhez tartozó sajátvektort is.

6.1.12
(a) A 0 pontosan akkor sajátérték, ha a megfelelő transzformáció nem invertálható és ez $\mathcal{AB}$-re és $\mathcal{BA}$-ra egyszerre teljesül. Egyébként, az $(\mathcal{AB})(\mathbf{x}) = \lambda\mathbf{x}$ egyenlőségre alkalmazzuk a $\mathcal{B}$ transzformációt.
(b) Következik (a)-ból az $\mathcal{A} = \mathcal{B}\mathcal{B}^{-1}\mathcal{A}$ felírás alapján.

6.2.

6.2.1 (a) $(-x)^7$. (b) $-x(x-1)(x-2)\dots(x-6)$. (c) $-x^6(x-6^6)$. (d) $-x^5(x-1)^2$.

6.2.2 (a) x^2-1. (b) x^2-x. (c) x^2+1. (d) x^2-x+1. (e) $(x-1)^2$. (f) $(x+1)^2$. (g) $(x-5)^2$.

6.2.3 $g(x) = k_{\mu\mathcal{A}}(x) = \mu^n f(x/\mu)$, ahol $n = \dim V$. Azaz, ha

$$f(x) = (-1)^n x^n + \alpha_{n-1}x^{n-1} + \ldots + \alpha_1 x + \alpha_0,$$

akkor

$$g(x) = (-1)^n x^n + \mu\alpha_{n-1}x^{n-1} + \ldots + \mu^{n-1}\alpha_1 x + \mu^n\alpha_0\,.$$

6.2.4 6.1.10: Egy polinomnak legfeljebb annyi gyöke lehet, mint amennyi a foka. 6.1.9: Ha összefüggők lennének, akkor az általuk generált altér k-nál kisebb dimenziós lenne, és ha a transzformációt erre az altérre megszorítjuk, akkor k (vagy több) sajátértéke lenne, ami az előzőek alapján lehetetlen.

6.2.5 Az algebra alaptétele szerint a karakterisztikus polinomnak van gyöke.

6.2.6 (a) Van. b) Nincs.

6.2.7 Kp=karakterisztikus polinom, sé=sajátérték, sv=sajátvektor (a $\mathbf{0}$-t eleve kizárjuk közülük), dm=diagonális mátrix.

(a) Kp: x^4-1, sé: $1,-1$, sv: $\langle \mathbf{b}_1+\mathbf{b}_2+\mathbf{b}_3+\mathbf{b}_4\rangle$, $\langle \mathbf{b}_1-\mathbf{b}_2+\mathbf{b}_3-\mathbf{b}_4\rangle$, dm: nincs.

(b) Kp: $x(x+1)(x-1)^2$, sé: $0,1,-1$, sv: $\langle \mathbf{b}_3-\mathbf{b}_4\rangle, \langle \mathbf{b}_4, \mathbf{b}_1+\mathbf{b}_2\rangle, \langle \mathbf{b}_1-\mathbf{b}_2\rangle$, dm: van.

(c) Kp: $(1-x)^4-1$, sé: $0,2$, sv: $\langle \mathbf{b}_1-\mathbf{b}_2+\mathbf{b}_3-\mathbf{b}_4\rangle$, $\langle \mathbf{b}_1+\mathbf{b}_2+\mathbf{b}_3+\mathbf{b}_4\rangle$, dm: nincs.

A komplex test felett az (a) és (c) esetben további két sajátérték adódik, és létezik diagonális mátrix.

6.2.8 Ahány különböző (esetleg ismétléses) permutációja létezik a főátlóban levő elemeknek. (Azért nincs több, mert a karakterisztikus polinomban az egyes sajátértékek multiplicitása egyértelmű.)

6.2.9 Használjuk a karekterisztikus polinomra a gyökök és együtthatók közötti összefüggést.

6.2.10 Érdemes megvizsgálni a mátrixok nyomát, determinánsát, a karakterisztikus polinomot és ezzel együtt a sajátértékeket, valamint azt, hogy létezik-e diagonális mátrix.

6.2.11 Használjuk az 1.3.6 Tételt.

6.3.

6.3.1 6.1.1: (a) x^7. (b) $x(x-1)(x-2)\dots(x-6)$. (c) x^2-6^6x. (d) x^2-x.
6.2.2: (a) x^2-1. (b) x^2-x. (c) x^2+1. (d) x^2-x+1.
(e) $x-1$. (f) $x+1$. (g) $x-5$.
6.2.7: (a) x^4-1. (b) x^3-1. (c) $(1-x)^4-1$.

6.3.2 $\lambda\mathcal{E}$.

6.3.3 A konstans tag nem nulla.

6.3.4 Az $m_{\mathcal{A}}(\mathcal{A})=\mathcal{O}$ egyenlőséget szorozzuk be $\mathcal{A}^{-1}$-gyel.

6.3.5 Ha $m_{\mathcal{A}}=\alpha_0+\ldots+\alpha_k x^k$, akkor $m_{\mathcal{A}^{-1}}=\alpha_k+\ldots+\alpha_0 x^k$.

6.3.6 Igaz: (b), (c), (e), (f).

6.3.7 A minimálpolinomra is érvényes az algebra alaptétele.

6.3.8 A mátrixnak megfelelő transzformáció minimálpolinomja osztója x^{1000}-nek és legfeljebb ötödfokú, tehát x^k alakú, ahol $k \leq 5$.

6.3.9

(a) Van (pl. a síkban a 72 fokos forgatás mátrixa).

(b) Nincs (mert a keresett mátrixnak megfelelő transzformáció minimálpolinomja egyrészt másodfokú, másrészt osztója az $x^5 - 1$ polinomnak, ami a racionális test fölött lehetetlen).

6.3.10 Vagy megegyeznek, vagy pedig az egyik a másiknak az x-szerese.
Útmutatás: Ha $\alpha_0\mathcal{E}+\alpha_1\mathcal{AB}+\alpha_2(\mathcal{AB})^2+\ldots+\alpha_k(\mathcal{AB})^k = \mathcal{O}$, akkor ezt az egyenlőséget balról $\mathcal{B}$-vel, jobbról pedig $\mathcal{A}$-val megszorozva $\alpha_0\mathcal{BA} + \alpha_1(\mathcal{BA})^2 + \alpha_2(\mathcal{BA})^3 + \ldots + \alpha_k(\mathcal{BA})^{k+1} = \mathcal{O}$ adódik.

6.3.11 Ha $m_{\mathcal{A}} = f$ és $m_{\mathcal{B}^{-1}\mathcal{AB}} = g$, akkor $f(\mathcal{B}^{-1}\mathcal{AB}) = \mathcal{B}^{-1}f(\mathcal{A})\mathcal{B} = \mathcal{O}$ miatt $g \mid f$, és a másik irányú oszthatóság is hasonlóan adódik.

6.3.12 Ha a minimálpolinom j-edfokú ($j \leq n$), akkor $\operatorname{Hom} V$-ben $\mathcal{A}$ minden hatványa, így $\mathcal{A}^k$ is előállítható $\mathcal{E}, \mathcal{A}, \ldots, \mathcal{A}^{j-1}$ lineáris kombinációjaként.

6.3.13 Az altér dimenziója éppen a minimálpolinom foka.
Útmutatás: Ha a minimálpolinom j-edfokú, akkor $\mathcal{E}, \mathcal{A}, \ldots, \mathcal{A}^{j-1}$ bázist alkot a szóban forgó altérben. (Vö. a 6.5.4 Tétellel.)

6.3.14 Bármely $k/2$ és k közötti egész szám, a határokat is beleértve.
Útmutatás: Legyen $\mathcal{A}^2$ minimálpolinomja $\beta_0 + \beta_1 x + \ldots + \beta_s x^s$. Ebbe $\mathcal{A}^2$-et behelyettesítve azonnal adódik, hogy $\mathcal{A}$ gyöke a $\beta_0 + \beta_1 x^2 + \ldots + {} + \beta_s x^{2s}$ polinomnak, vagyis $k \leq 2s$. A másik irányú becslés: $\operatorname{Hom} V$-ben minden j-re $\mathcal{A}^j \in \langle \mathcal{E}, \mathcal{A}, \ldots, \mathcal{A}^{k-1} \rangle$, tehát $\mathcal{A}$-nak, és így $\mathcal{A}^2$-nek is bármely $k+1$ hatványa lineárisan összefüggő. Innen $s \leq k$ adódik. Azt, hogy ezek az értékek valóban fel is lépnek, az alábbi típusú példákkal igazolhatjuk: a transzformációnak legyen csupa különböző sajátértéke (k darab), amelyek közül néhánynak szerepel az ellentettje is.

6.3.15 Útmutatás: Legyen egy tetszőleges r polinom esetén $r^*(x) = r(x^2)$. Használjuk fel, hogy $r(\mathcal{A}^2) = \mathcal{O} \iff m_{\mathcal{A}} \mid r^*$, továbbá, hogy ha $\lambda \neq 0$, akkor az r-nek a λ^2 pontosan ugyanannyiszoros gyöke, mint az r^*-nak a λ.

6.3.16 Útmutatás: Ha $(h, m_{\mathcal{A}}) = d \neq 1$, akkor $h(\mathcal{A})(m_{\mathcal{A}}/d)(\mathcal{A}) = \mathcal{O}$ miatt $h(\mathcal{A})$ nullosztó (vagy nulla), tehát nem létezik inverze. Ha $(h, m_{\mathcal{A}}) = 1$, akkor alkalmas r és s polinomokkal $1 = hr + sm_{\mathcal{A}}$, és így $h(\mathcal{A})r(\mathcal{A}) = \mathcal{E}$.

6.3.17 A minimálpolinomok és (így szükségképpen) a sajátértékek egybeesnek, a karakterisztikus polinomok azonban nem is azonos fokúak.

6.3.18 Ha $f = \alpha_0 + \alpha_1 x + \ldots + \alpha_k x^k$, akkor legyen V bázisa $\mathbf{b}_1, \ldots, \mathbf{b}_k$ és

$$\mathcal{A}\mathbf{b}_1 = \mathbf{b}_2, \ldots, \mathcal{A}\mathbf{b}_{k-1} = \mathbf{b}_k, \mathcal{A}\mathbf{b}_k = \sum_{i=0}^{k-1} (-\alpha_i/\alpha_k)\mathbf{b}_{i+1}\,.$$

6.3.19 Attól, hogy a minimálpolinomnak és a karakterisztikus polinomnak is pontosan a sajátértékek a gyökei, lehetne, hogy valamelyik gyöktényező a minimálpolinomban magasabb hatványon szerepel, és akkor a minimálpolinom nem lenne osztója a karakterisztikus polinomnak.

Abból, hogy a minimálpolinom osztója a karakterisztikus polinomnak, következik, hogy a minimálpolinom gyökei, azaz a sajátértékek mind gyökei a karakterisztikus polinomnak, de ez utóbbinak lehetnének más gyökei is. Visszafelé ugyanígy, az oszthatóság csak azt biztosítja, hogy a minimálpolinom gyökei a karakterisztikus polinom gyökei, azaz a sajátértékek közül kerülnek ki, de nem adódik, hogy minden sajátérték valóban előfordul közöttük.

6.3.20 Igazoljuk, hogy bármely $f \in T[x]$ polinomra $S^{-1}f(A)S = f(S^{-1}AS)$.

6.3.21 Az, hogy A nem gyöke egy legfeljebb k-adfokú, nem nulla $f \in T[x]$ polinomnak, azzal ekvivalens, hogy $E, A, A^2, \ldots, A^k$ lineárisan függetlenek a mátrixok $T^{n\times n}$ vektorterében. Ez utóbbi azt jelenti, hogy a megfelelő homogén lineáris egyenletrendszernek csak triviális megoldása létezik. Mivel a Gauss-kiküszöbölésnél nem lépünk ki az együtthatók által meghatározott testből, ezért valós együtthatók esetén ugyanahhoz a redukált lépcsős alakhoz jutunk akkor is, ha az együtthatókat komplex számoknak tekintjük.

Megjegyzés: Ugyanígy adódik általánosan is, hogy ha K részteste a T testnek, azaz $K \subseteq T$ és K maga is test a T-beli műveletek megszorításaira, akkor egy $A \in K^{n\times n}$ mátrixnak a K feletti minimálpolinomja egyben T feletti mininálpolinom is. Az analóg állítás a karakterisztikus polinomra is igaz, ez a definícióból azonnal következik.

6.3.22

(a) Mivel $m_A \mid k_A$, ezért m_A minden irreducibilis tényezője szerepel k_A felbontásában. Megfordítva, legyen f a k_A egy irreducibilis tényezője. Tekintsük az A mátrixot komplex elemű A' mátrixnak, ekkor $k_{A'} = k_A$ és $m_{A'} = m_A$ (ez k_A-ra a definícióból adódik, m_A-ra pedig a 6.3.21 feladat mintájára igazolható). Az algebra alaptétele szerint f (egy konstans szorzótól eltekintve) gyöktényezők szorzatára bomlik és az irreducibilitás miatt ezek a gyökök mind különbözők (A.4.10 feladat). Ezek mind gyökei

$k_{A'} = k_A$-nak, tehát sajátértékei A'-nek, így gyökei $m_{A'} = m_A$-nak is. Ezért ugyanezek a gyöktényezők m_A-ban is szerepelnek, vagyis $f \mid m_A$.

(b) Szükségesség: Az $A \in \mathbf{Q}^{n\times n}$ mátrix gyöke az $x^3 - 2$ polinomnak, ami irreducibilis, tehát ez a minimálpolinom. A karakterisztikus polinom így csak ennek hatványa lehet, ezért a fokszáma, azaz n csak a 3 többszöröse lehet. Elégségesség: Megfelelő mátrixot $n = 3$-ra pl. a 6.3.18 feladat útmutatásából kapunk, tetszőleges n-re pedig ilyen 3×3-as blokkokból kell a mátrixot összerakni.

6.4.

6.4.2 Igaz: (a), (c), (d).
Útmutatás d)-hez: az $\mathcal{A}$ transzformáció U-ra történő megszorításának a magtere a feltétel szerint $\mathbf{0}$, tehát a képtere az egész U.

6.4.3 Az első k oszlop utolsó $n - k$ eleme nulla.

6.4.4

(a) Egy ilyen transzformáció skalárszorosa, két ilyen transzformáció összege és szorzata is ilyen tulajdonságú.

(b) $n^2 - nk + k^2$. Útmutatás: a transzformációk helyett tekintsük a mátrixukat egy olyan bázisban, amelynek első k eleme U-beli.

6.4.5 (a) $\lambda\mathcal{E}$. b) Ha $\dim V > 13$, akkor $\lambda\mathcal{E}$.
Útmutatás (b)-hez: a 6.4.1 feladat alapján a 13-nál kisebb, illetve nagyobb dimenziójú alterek invarianciája is igazolható.

6.4.6 Útmutatás: Legyen U sajátaltere $\mathcal{A}$-nak. Ha $\mathbf{u} \in U$, azaz $\mathcal{A}\mathbf{u} = \lambda\mathbf{u}$ valamely rögzített λ-ra, akkor $\mathcal{A}(\mathcal{B}\mathbf{u}) = \mathcal{B}(\mathcal{A}\mathbf{u}) = \mathcal{B}(\lambda\mathbf{u}) = \lambda(\mathcal{B}\mathbf{u})$, tehát $\mathcal{B}\mathbf{u} \in U$.

6.4.7 (b) Nem, pl. $[\mathcal{A}] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 2 \end{pmatrix}$, $[\mathcal{B}] = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 3 \end{pmatrix}$.

6.4.8 $n + 2$.
Útmutatás: Lássuk be, hogy ha egy polinom eleme egy invariáns altérnek, akkor minden nála nem nagyobb fokú polinom is benne van ebben az altérben.

6.4.9

(b) Legyen $(f, m_{\mathcal{A}}) = d$. Először azt igazoljuk, hogy $\operatorname{Ker} f(\mathcal{A}) = \operatorname{Ker} d(\mathcal{A})$, itt az egyik irányhoz használjuk fel, hogy d felírható $d = sf + tm_{\mathcal{A}}$ alakban. Ezután lássuk be, hogy ha d_1 és d_2 a minimálpolinom két osztója és $\operatorname{Ker} d_1(\mathcal{A}) = \operatorname{Ker} d_2(\mathcal{A})$, akkor d_1 és d_2 egymás konstansszorosa. Ezt $(d_1\,,\, d_2)$ segítségével visszavezethetjük a $d_1 \mid d_2$ esetre. Ha most

$m_{\mathcal{A}} = d_2 h = r d_1 h$, akkor a feltétel alapján már $d_1(\mathcal{A})h(\mathcal{A}) = \mathcal{O}$, tehát a minimálpolinom definíciója miatt r csak konstans lehet.

(c) A (b) rész szerint ennyi különböző $\operatorname{Ker} f(\mathcal{A})$ típusú altér létezik.

(d) Az $\mathcal{A}$-nak akkor és csak akkor nincs nem triviális invariáns altere, ha $m_{\mathcal{A}}$ irreducibilis (T felett) és $\deg m_{\mathcal{A}} = \dim V$. A Cayley–Hamilton-tétel alapján ez azzal ekvivalens, hogy $k_{\mathcal{A}}$ irreducibilis (T felett).

6.4.10 Az előző feladathoz hasonló gondolatmeneteket alkalmazzunk.

6.4.11 (a) Igaz. (b) Hamis, pl. $[\mathcal{A}] = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$, $f = g = x$.

6.4.13 0: $\mathbf{u} = \mathbf{0}$, 1: $\mathbf{u}$ sajátvektor. (Vö. a 6.5.4 Tétellel.)

6.4.14 Pl. megfelel maga a V, ha $\dim \operatorname{Im} \mathcal{A} \leq \dim V - 2$, vagy egy legalább kétdimenziós altér, ha $\mathcal{A} = \mathcal{E}$.

6.4.15 Igaz: (a), (c), (e).

6.5.

6.5.1

(a) Ha $\lambda \neq 0$, akkor $o(\mathbf{u}) = o(\lambda \mathbf{u})$.

(b) $o(\mathcal{A}\mathbf{u}) = o(\mathbf{u})/x$ vagy $o(\mathbf{u})$ attól függően, hogy $o(\mathbf{u})$ konstans tagja nulla vagy nem nulla.

(c) $o[f(\mathcal{A})\mathbf{u}] = o(\mathbf{u})/\big(o(\mathbf{u}), f\big)$.

6.5.2 A rend létezéséhez és a fokszámára adott becsléshez azt használjuk fel, hogy az $\mathbf{u}, \mathcal{A}\mathbf{u}, \ldots, \mathcal{A}^n\mathbf{u}$ vektorok lineárisan összefüggők.
Egy másik lehetőség, ha a minimálpolinom megfelelő tulajdonságaira támaszkodunk.

6.5.3 $o_{\mathcal{A}}(\mathbf{u})$.

6.5.4 Használjuk fel az előző feladat eredményét, valamint a minimálpolinom és a sajátértékek kapcsolatát.

6.5.5 Járjunk el a 6.5.7 Lemma bizonyításában a (iii)-nál megadott útmutatás szerint: lássuk be, hogy ha $f = gh$, akkor $g = o[h(\mathcal{A})\mathbf{v}]$.

6.5.6 Igaz: (a), (c).

6.5.7 Útmutatás: Ha $i > 0$, akkor $\mathcal{A}^i\mathbf{u} \in \operatorname{Im} \mathcal{A}$.
Válasz a kérdésre: A 6.5.6 Tétel alapján ugyanez a korlát érvényes a minimálpolinomra.

6.5.8 Legyen $\mathbf{u}_1, \ldots, \mathbf{u}_n$ a $\lambda_1, \ldots, \lambda_n$ sajátértékekhez tartozó egy-egy sajátvektor, ezek bázist alkotnak. Az $\mathbf{u}_i$-k tetszőleges részhalmaza által generált (összesen 2^n darab) altér invariáns (a $\mathbf{0}$ alteret az üres halmaz generálja). Azt kell igazolni, hogy nincs több invariáns altér. Ehhez azt mutassuk meg, hogy ha egy $\mathbf{v} = \beta_1\mathbf{u}_1 + \ldots + \beta_n\mathbf{u}_n$ vektor eleme egy U invariáns altérnek és $\beta_i \neq 0$, akkor $\mathbf{u}_i \in U$. E célból alkalmazzuk $\mathbf{v}$-re az $f_i(\mathcal{A})$ transzformációt, ahol $f_i = m_{\mathcal{A}}/(x - \lambda_i)$.

6.5.9 A minimálpolinom minden osztója valamely $\mathbf{u}$ vektor rendje, és páronként nem-egységszeres osztók esetén az ezekhez tartozó $\langle \mathbf{u}, \mathcal{A}\rangle$ alterek mind különbözők.

6.5.10 A feladatnak az említett (i) állítás az $\big(o(\mathbf{u}), o(\mathbf{v})\big) = 1$ speciális esete, és a bizonyítás is az ott látottak mintájára adódik.

6.5.11 Ha $\lambda \neq 0$, akkor $o_{\lambda\mathcal{A}}(\mathbf{u})$ foka megegyezik $o_{\mathcal{A}}(\mathbf{u})$ fokával. A másik kérdésnél a helyzet analóg a minimálpolinomnál látottakkal (6.3.14 feladat). A bizonyítás is történhet az ottani mintára, egy másik lehetőség az, ha a 6.5.6 Tétel alapján csak az ottani eredményeket használjuk fel, egy harmadik út pedig, ha a 6.5.4 Tételre támaszkodunk.

6.5.12 (c) $\mathbf{R}$ és $\mathbf{C}$ felett is megfelel pl. $[\mathcal{A}] = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix}, [\mathcal{B}] = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$. Egyszerűbb példa $\mathbf{R}$ felett a síkon az origó körüli 120 fokos, illetve 240 fokos forgatás vagy bármely két olyan transzformáció, amelynek azonos irreducibilis polinom a minimálpolinomja.

6.6.

6.6.1 Az elégségességhez használjuk fel a 6.6.2 Tételt.

6.6.2

(a) $\mathcal{A}$-nak a különböző sajátértékekhez tartozó sajátvektorai bázist alkotnak, és ezek $\mathcal{B}$-nek is sajátvektorai.

(b) Az $\mathcal{A}$-val felcserélhető transzformációk n-dimenziós alteret alkotnak $\operatorname{Hom} V$-ben, ennek része $\mathcal{A}$ polinomjainak az altere, amely szintén n-dimenziós, tehát a két altér egybeesik. Ezeket a legkönnyebben úgy láthatjuk be, ha a transzformációk helyett az $\mathcal{A}$ sajátvektorai szerinti bázisban felírt mátrixokkal dolgozunk. Egy másik lehetőség, ha az interpolációs polinomot (lásd a 3.2.4 Tételt) használjuk fel.

6.6.3 A megszorítás minimálpolinomja osztója az eredeti minimálpolinomnak. A karakterisztikus polinomoknál is ugyanez a helyzet.

6.6.4

(a) Használjuk pl. a 6.5.3 Tételt.

(b) Ha pl. $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ rendre az 1, 1, 2 sajátértékhez tartozó lineárisan független sajátvektorok, és $U_1 = \langle \mathbf{b}_1, \mathbf{b}_3 \rangle$, $U_2 = \langle \mathbf{b}_2, \mathbf{b}_3 \rangle$, akkor $m_\cap = (x-2) \neq$ $\neq (m_1, m_2) = (x-1)(x-2)$.

6.6.5 (a) és (b) Pl. $\mathcal{A} = \mathcal{E}$ esetén sem áll általában egyenlőség.

(c) $U_1 \cap U_2$ bázisát egészítsük ki U_1, illetve U_2 bázisává, ez együttesen $\langle U_1, U_2 \rangle$ bázisát adja, és a karakterisztikus polinomok kiszámításához $\mathcal{A}$ mátrixát ebben a bázisban írjuk fel.

6.6.6 Először azt igazoljuk, hogy ha $\deg m_\mathcal{A} < \dim V$, akkor végtelen test esetén végtelen sok invariáns altér van. Mivel bármely $\mathbf{u}$-ra $\dim\langle \mathbf{u}, \mathcal{A} \rangle = \deg o(\mathbf{u}) \leq \deg m_\mathcal{A} < \dim V$, ezért mindegyik $\langle \mathbf{u}, \mathcal{A} \rangle$ valódi altér. Ezek egyesítése nyilván kiadja V-t, és mivel végtelen test esetén véges sok valódi altér egyesítése nem lehet V, így szükségképpen végtelen sok ($\langle \mathbf{u}, \mathcal{A} \rangle$ alakú) invariáns altér van. (Véges test esetén annyi mondható, hogy biztosan van nem $\langle \mathbf{u}, \mathcal{A} \rangle$ alakú altér, pl. a V, és emiatt a 6.5.9 feladat szerint több invariáns altér van, mint ahány páronként nem-egységszeres osztója van a minimálpolinomnak.)

Most megmutatjuk, hogy ha $\deg m_\mathcal{A} = \dim V$, akkor (akár véges, akár végtelen test esetén) minden invariáns altér $\operatorname{Ker} f(\mathcal{A})$ alakú. Ezzel készen leszünk, hiszen az ilyen alterek száma a 6.4.9 feladat szerint a minimálpolinom páronként nem-egységszeres osztóinak a számával egyenlő.

Legyen $\mathbf{v}$ olyan vektor, amelyre $o(\mathbf{v}) = m_\mathcal{A}$. Ekkor $\dim\langle \mathbf{v}, \mathcal{A} \rangle =$ $= \deg o(\mathbf{v}) = \deg m_\mathcal{A} = \dim V$, tehát $\langle \mathbf{v}, \mathcal{A} \rangle = V$.

Legyen $f \mid m_\mathcal{A}$, azaz $m_\mathcal{A} = fg$. Ekkor $\operatorname{Im} f(\mathcal{A}) = \langle f(\mathcal{A})\mathbf{v}, \mathcal{A} \rangle$, tehát $\dim \operatorname{Im} f(\mathcal{A}) = \deg o[f(\mathcal{A})\mathbf{v}] = \deg g$. A dimenziótétel szerint így $\dim \operatorname{Ker} f(\mathcal{A}) = \deg f$.

Vegyünk most egy tetszőleges U invariáns alteret, és jelöljük az $\mathcal{A}$ transzformáció U-ra történő megszorításának a minimálpolinomját f-fel. Belátjuk, hogy $U = \operatorname{Ker} f(\mathcal{A})$.

Legyen $\mathbf{u} \in U$ olyan vektor, amelyre $o(\mathbf{u}) = f$. Ekkor $\langle \mathbf{u}, \mathcal{A} \rangle \subseteq U \subseteq$ $\subseteq \operatorname{Ker} f(\mathcal{A})$. Továbbá $\dim \langle \mathbf{u}, \mathcal{A} \rangle = \dim \operatorname{Ker} f(\mathcal{A}) = \deg f$, tehát valóban $U = \operatorname{Ker} f(\mathcal{A})$.

6.6.7 Az előzőn kívül használjuk fel a 6.4.9, 6.4.10 és 6.5.9 feladatokat is.

6.6.8

(a) $\lambda\mathcal{E}$.

(d) Nem, legyen pl. $\mathcal{D} = -\mathcal{A}$, illetve $\mathcal{D} = \mathcal{A}^{-1}$.

(f) A megfordítás hamis, pl. a $\begin{pmatrix}1&0&0&0\\1&1&0&0\\0&0&1&0\\0&0&0&1\end{pmatrix}$ és $\begin{pmatrix}1&0&0&0\\1&1&0&0\\0&0&1&0\\0&0&1&1\end{pmatrix}$ mátrixokhoz tartozó transzformációk karakterisztikus polinomja és minimálpolinomja megegyezik, azonban nem hasonlók, mert a(z 1 sajátértékhez tartozó) sajátalterek dimenziója eltér.

6.6.9 $\lambda\mathcal{E}$.

Útmutatás: kombináljuk az előző feladat (a) és (f) pontjának eredményét.

6.6.10 (a) $\begin{pmatrix}2&0&0\\0&2&0\\0&0&0\end{pmatrix}$; (b) $\begin{pmatrix}1&0&0\\0&\omega&0\\0&0&\omega^2\end{pmatrix}$; (c) $\begin{pmatrix}2&0&0\\1&2&0\\0&0&0\end{pmatrix}$;

(d) $\begin{pmatrix}1&0&0\\1&1&0\\0&0&1\end{pmatrix}$, ahol ω primitív harmadik egységgyök.

6.6.11

(a),(d) Közvetlenül a főátló alatt 1-ek állnak, minden más elem 0 (az egész mátrix egyetlen Jordan-alblokk).

(b) Diagonális mátrix, a főátlóban az n-edik egységgyökök állnak.

(c) Közvetlenül a főátló alatt az $\lfloor(n+2)/2\rfloor$-edik sor kivételével 1-ek állnak, minden más elem 0 (az egész mátrix egyetlen Jordan-blokk, amely egy $\lfloor n/2\rfloor$ és egy $\lfloor(n+1)/2\rfloor$ méretű alblokkból áll).

(e) A bal felső sarokban n, az összes többi helyen 0 áll.

(f) Diagonális mátrix, a főátlóban $\lfloor(n+1)/2\rfloor$ darab 1 és $\lfloor n/2\rfloor$ darab -1 áll.

6.6.12 A blokkok (és azon belül az alblokkok) egymástól függetlenül hatványozódnak. Egy $k\times k$-as $A=\begin{pmatrix}\lambda&0&0&\dots&0\\1&\lambda&0&\dots&0\\0&1&\lambda&\dots&0\\\vdots&\vdots&\vdots&\ddots&\vdots\\0&0&0&\dots&\lambda\end{pmatrix}$ Jordan-féle alblokk m-edik hatványában a főátló fölött minden elem 0, a főátlóban minden elem λ^m, közvetlenül alatta minden elem $m\lambda^{m-1}$, az eggyel lejjebbi „ferde szinten” minden elem $\binom{m}{2}\lambda^{m-2}$, és általában, bármely $j<k$-ra a főátló alatti j-edik ferde szinten minden elem $\binom{m}{j}\lambda^{m-j}$.

Hasonló módon kapjuk meg tetszőleges f polinom esetén $f(\mathcal{A})$-t is.

6.6.13 Legyen λ_i multiplicitása a főátlóban (azaz a λ_i-hez tartozó blokk mérete) s_i, és az ezen a blokkon belüli legnagyobb alblokk mérete t_i. Ekkor

$$k_{\mathcal{A}}=\prod(x-\lambda_i)^{s_i},\qquad m_{\mathcal{A}}=\prod(x-\lambda_i)^{t_i}\,.$$

Megjegyzés: Ebből azonnal adódik $k_{\mathcal{A}} \mid m_{\mathcal{A}}$, és így új bizonyítást nyertünk a 6.3.5 Cayley–Hamilton-tételre a komplex test esetén. Ugyanez működik bármely algebrailag zárt testre, azaz amelyben bármely nem konstans polinomnak van gyöke. Innen tetszőleges testre is adódik az oszthatóság, ha áttérünk a test algebrai lezártjára és felhasználjuk, hogy ez nem befolyásolja sem a karakterisztikus, sem a minimálpolinomot (lásd az Útmutatásoknál a 6.3.21 feladat utáni megjegyzést).

6.6.14 Használjuk a Jordan-alakot.

6.6.15

(a) $\deg m_{\mathcal{A}} = 1$ vagy $\deg m_{\mathcal{A}} = n(= \dim V)$ vagy $m_{\mathcal{A}} = (x-\lambda)^{n-1}$.

(b) A karakterisztikus polinom csupa különböző gyöktényező szorzata.

(c) A karakterisztikus polinom bármely gyöktényezőjének a multiplicitása a minimálpolinomban vagy ugyanannyi, mint a karakterisztikus polinomban, vagy eggyel kevesebb, vagy pedig 1.

6.6.16 Használjuk fel a Jordan-alakot, és azt, hogy a Jordan-alak hasonló a transzponáltjához. Ez utóbbi a báziselemek sorrendjének a megváltoztatásával egyszerűen adódik.

6.6.17

(a) Tekintsük az A mátrixot egy $\mathcal{A}$ lineáris transzformáció mátrixának. A karakterisztikus polinomból kapjuk, hogy létezik sajátbázis, ebben tehát $\mathcal{A}$ mátrixa egy C diagonális mátrix. Az 5.8.1A Tétel alapján $C = S^{-1}AS$, ahol S az új bázisra áttérés mátrixa. Innen $A = SCS^{-1}$, amiből $A^n = SC^nS^{-1}$. Diagonális mátrixokat elemenként lehet hatványozni, továbbá S és S^{-1} is könnyen meghatározható, amiből megkapjuk A^n-et. Eredmény: $A^n = \frac{1}{3}\begin{pmatrix} 5^n + 2^{n+1} & 5^n - 2^n \\ 2\cdot 5^n - 2^{n+1} & 2\cdot 5^n + 2^n \end{pmatrix}$.

(b) Most annyi a különbség, hogy nincs sajátbázis, mert a karakterisztikus polinomnak kétszeres gyöke van. Így a Jordan-alakot használjuk C-nek, amelynek a hatványait a 6.6.12 feladat alapján számolhatjuk. Eredmény: $B^n = \begin{pmatrix} n2^{n-1} + 2^n & n2^{n-1} \\ -n2^{n-1} & 2^n - n2^{n-1} \end{pmatrix}$.

7. Bilineáris függvények

7.1.

7.1.1 (a) és (b) nem bilineáris függvény. (c) $\alpha_{ij} = 2^{j-1}$.
(d) $\alpha_{ij} = (i-1)2^{j-1}$. (e) $\alpha_{ij} = 1$, ha $i + j = 4$, és 0 egyébként.

7.1.2 P2: E. P3: $\alpha_{12} = 1, \alpha_{21} = 2$, a többi $\alpha_{ij} = 0$, illetve $\alpha_{11} = 1$, $\alpha_{22} = -3$, a többi $\alpha_{ij} = 0$. P4: nullmátrix.

7.1.3 A nulla függvény értékkészlete csak a nullából áll, minden más bilineáris függvény értékkészlete az *összes* valós szám.

7.1.4

(a) Legfeljebb egy $\mathbf{A}$ létezik.

(b) Ha nem bázis, akkor végtelen sok $\mathbf{A}$ létezik.

7.1.5 Ha $\dim V = n$, akkor a keresett dimenzió n^2.
Útmutatás: lássuk be, hogy a szóban forgó vektortér izomorf $T^{n\times n}$-nel.

7.1.6

(a) Az első és második sor, valamint az első és második oszlop felcserélődik.

(b) A harmadik sor és oszlop λ-val szorzódik, emiatt speciálisan α_{33} a λ^2-szeresére változik.

(c) A harmadik sorhoz, illetve oszlophoz hozzá kell adni a második sor, illetve oszlop μ-szörösét, emiatt speciálisan az új harmadik sor harmadik eleme $\alpha'_{33} = \alpha_{33} + \mu\alpha_{23} + \mu\alpha_{32} + \mu^2\alpha_{22}$ lesz.

7.1.7 Csak a $\mathbf{0}$ bilineáris függvény ilyen.

7.1.8 Útmutatás (c)-hez: használjuk fel (b)-t.

7.1.9 (a) 1 (kivéve ha $\mathbf{A} = \mathbf{0}$). (b) Az $\mathbf{A}$ mátrixának a rangja.

7.2.

7.2.1 Ha $\mathbf{A}$ antiszimmetrikus, akkor $\mathbf{A}(\mathbf{u},\mathbf{v}) = -\mathbf{A}(\mathbf{v},\mathbf{u})$-ben $\mathbf{u}$ és $\mathbf{v}$ helyére is $\mathbf{x}$-et írva $\mathbf{A}(\mathbf{x},\mathbf{x}) = -\mathbf{A}(\mathbf{x},\mathbf{x})$ adódik, ahonnan $\mathbf{A}(\mathbf{x},\mathbf{x}) = 0$. A megfordításhoz „fejtsük ki” $\mathbf{A}(\mathbf{u}+\mathbf{v},\mathbf{u}+\mathbf{v})$-t (lásd a 7.2.3 Tétel második bizonyításának az elejét).

7.2.2 Útmutatás: Legyen $\mathbf{B}$ egy tetszőleges bilineáris függvény és tegyük fel, hogy létezik egy $\mathbf{B}(\mathbf{u},\mathbf{v}) = \mathbf{S}(\mathbf{u},\mathbf{v}) + \mathbf{A}(\mathbf{u},\mathbf{v})$ előállítás, ahol $\mathbf{S}$ szimmetrikus, $\mathbf{A}$ pedig antiszimmetrikus. Felcserélve $\mathbf{u}$-t és $\mathbf{v}$-t és beírva a definíciókat egy újabb összefüggést kapunk. A két egyenlőségből $\mathbf{S}$ és $\mathbf{A}$ egyértelműen kifejezhető $\mathbf{B}$ segítségével. Ezzel kiderült, hogy legfeljebb az így kapott $\mathbf{S}$ és $\mathbf{A}$ jöhet szóba. Ahhoz, hogy ez a függvénypár valóban megfelel, meg kell még mutatni, hogy az így megadott $\mathbf{S}$, illetve $\mathbf{A}$ tényleg szimmetrikus, illetve antiszimmetrikus. [A számolásokból $\mathbf{S}(\mathbf{u},\mathbf{v}) = (1/2)\big(\mathbf{B}(\mathbf{u},\mathbf{v})+\mathbf{B}(\mathbf{v},\mathbf{u})\big)$ és $\mathbf{A}(\mathbf{u},\mathbf{v}) = (1/2)\big(\mathbf{B}(\mathbf{u},\mathbf{v})-\mathbf{B}(\mathbf{v},\mathbf{u})\big)$ adódik.]

7.2.3

(b) Ha $\dim V = n$, akkor $\dim S = n(n+1)/2$ és $\dim A = n(n-1)/2$.

(c) Ez lényegében az előző feladat.

7.2.4 Igaz: (a).

7.2.5 Minden altérnél csak egy lehetséges példát adunk meg.

(a) $\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\1\\0\end{pmatrix}$; (b) $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}-3\\-1\\1\\3\end{pmatrix}$;

(c) $\begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}$.

7.2.6 dm=a(z egyik) diagonális mátrix főátlója, **A**-OB=(az egyik) **A**-ortogonális bázis.

(a) dm: $1,0,0,0,0$. **A**-OB: 1, $x-1$, x^2-1, x^3-1, x^4-1.

(b) dm: $1,1,-1,0,0$. **A**-OB: x, $1/2+x^2$, $1/2-x^2$, x^3, x^4.

(c) dm: $1,1,1,1,1$. **A**-OB: $f_i = \lambda_i F/(x-i)$, ahol $F = \prod_{i=1}^{5}(x-i)$ és a λ_i-k alkalmas skalárok.

7.2.7 dm=a(z egyik) diagonális mátrix főátlója, **A**-OB=(az egyik) **A**-ortogonális bázis.

(a) dm: $1,0,0$. **A**-OB: $\mathbf{b}_1$, $\mathbf{b}_2 - 2\mathbf{b}_1$, $\mathbf{b}_3 - 3\mathbf{b}_1$.

(b) dm: $1,-1,0$. **A**-OB: $\mathbf{b}_1$, $\mathbf{b}_2 - 2\mathbf{b}_1$, $\mathbf{b}_3 - 2\mathbf{b}_2 + \mathbf{b}_1$.

7.2.8 Keressük $\mathbf{w}$-t $\mathbf{w} = \mathbf{u} + \lambda\mathbf{v}$ alakban. Másik lehetőség: a feltételek alapján alkalmas diagonális mátrix főátlójában szükségképpen előfordul $+1$ és -1 is. Az ezeknek megfelelő bázisvektorok összege jó $\mathbf{w}$-t ad.

7.2.9 A dimenzió n vagy $n-1$.

7.2.10 $(n+2)(n+1)/2$.

7.3.

7.3.1

(a) Következik a 7.2.1 feladatból.

(b) „Fejtsük ki” $\mathbf{A}(\mathbf{u}+\mathbf{v}, \mathbf{u}+\mathbf{v})$-t. Így szimmetrikus **A**-ra $\mathbf{A}(\mathbf{u},\mathbf{v})$-t egyértelműen kifejezhetjük a kvadratikus alakból. Ezzel kaptuk, hogy minden kvadratikus alak legfeljebb egy szimmetrikus bilineáris függvényből származtatható. Meg kell még mutatni, hogy tényleg van ilyen tulajdonságú szimmetrikus bilineáris függvény. Ehhez azt kell belátni, hogy a kvadratikus alakból a jelzett módon kifejezett bilineáris függvény valóban szimmetrikus, ami egyszerű számolással ellenőrizhető. [A szimmetrikus bilineáris függvényre az $\mathbf{A}(\mathbf{u},\mathbf{v}) = (1/2)\big(\tilde{\mathbf{A}}(\mathbf{u}+\mathbf{v}) - \tilde{\mathbf{A}}(\mathbf{u}) - \tilde{\mathbf{A}}(\mathbf{v})\big)$ előállítás adódik a kvadratikus alakból.]

7.3.2 7.2.5: PD. 7.2.6: (a) PSZ. (b) I. (c) PD. 7.2.7: (a) PSZ. (b) I.

7.3.3 PD, PSZ: nemnegatív valós számok. ND, NSZ: nempozitív valós számok. I: összes valós szám. $\mathbf{0}$: csak a nulla.
Ha csak a nem nulla vektorokon felvett értékeket nézzük, akkor PD: pozitív valós számok, ND: negatív valós számok, a többi változatlan (az indefinitnél ehhez fel kell használni a 7.2.8 feladat állítását is).

7.3.4 (a) $\tilde{\mathbf{A}}(\lambda\mathbf{x}) = \lambda^2\tilde{\mathbf{A}}(\mathbf{x})$. (b) Az $\mathbf{x}$ és $\mathbf{z}$ vektorok $\mathbf{A}$-ortogonálisak.

7.3.5

(a) Ha $\lambda > 0$, akkor $\mathbf{A}$ és $\lambda\mathbf{A}$ jellege megegyezik. Ha $\lambda < 0$, akkor az indefinitnél nincs változás, a többinél a jelleg „előjelet vált”. Ha $\lambda = 0$, akkor $\lambda\mathbf{A} = \mathbf{0}$.

(b) PD+PD=PD; PD+PSZ=PD; PSZ+PSZ=PD vagy PSZ;
PD+I, PSZ+I és PD+NSZ: PD vagy PSZ vagy I; további hat esetet kapunk a fentiekből a P és N betűk cseréjével; PSZ+NSZ: PSZ vagy NSZ vagy I vagy $\mathbf{0}$; végül I+I, PD+ND: bármi lehet.

7.3.6 A sokféle lehetséges felírásból mindig csak egyet adunk meg.

(a) $[(x_1 + x_2)/2]^2 - [(x_1 - x_2)/2]^2$.

(b) $[(x_1 + x_2 + x_3)/2]^2 - [(x_1 - x_2 + x_3)/2]^2$.

(c) $[(x_1 + 2x_2 + x_3)/2]^2 - [(x_1 - x_3)/2]^2 - x_2^2$.

(d) $(x_1 - x_2 + x_3)^2 - (x_2 + 2x_3)^2$.

(e) $(x_1 + 2x_2 + x_3)^2 - (x_2\sqrt{3} + x_3/\sqrt{3})^2 + (x_3\sqrt{7/3})^2$.

7.3.7 A sokféle lehetséges felírásból mindig csak egyet adunk meg.

(a) $(x_1 + x_2 + x_3 + x_4)^2$.

(b) $[(x_1 + x_2 + x_3)/2]^2 - [(x_1 - x_2 + x_3)/2]^2 + [(x_3 + x_4)/2]^2 - [(x_3 - x_4)/2]^2$.

(c) $[(x_1 + x_2 + x_3 + x_4)/2]^2 - [(x_1 - x_2 + x_3 - x_4)/2]^2$.

(d) $[(x_1 + x_2 + 2x_3 + 2x_4)/2]^2 - [(x_1 - x_2)/2]^2 - [(2x_3 + x_4)/2]^2 - (x_4\sqrt{3}/2)^2$.

7.3.8 A tehetetlenségi tétel olyan előjeles négyzetösszegekre vonatkozik, amelyben egy ($\mathbf{A}$-ortogonális) *bázis* szerinti koordináták négyzetei szerepelnek. A feladatbeli négyzetösszegekre ez nem lehet igaz, hiszen egy kétdimenziós kvadratikus alak ilyen felírásában legfeljebb *két* négyzet előjeles összege állhat. A szóban forgó alak (egyik lehetséges) „helyes” felírása: $(x_1\sqrt{2} + x_2/\sqrt{2})^2 + (x_2\sqrt{3/2})^2$.

7.3.9 Pl. az egyik báziselemet λ-szorosára változtatva a determináns λ^2-tel szorzódik.
A második állításhoz használjuk fel, hogy a 7.2.3 Tétel harmadik bizonyításában végzett elemi ekvivalens átalakítások során a determináns

előjele nem változik, továbbá ilyen átalakításokkal a függvény bármely mátrixából kiindulva diagonális mátrixhoz juthatunk, amelyben a determináns előjele a tehetetlenségi tétel miatt egyértelmű.

7.3.10 Igaz: (a).

7.3.11 PD, ND: 1; PSZ, NSZ: $n-1$; I: $n(n-1)/2$. (A $\mathbf{0}$ függvény egyik osztályba sem tartozik, ezért a megadott számoknak az összege eggyel kisebb, mint a 7.2.10 feladat eredménye.)

7.3.12 **A** (pozitív vagy negatív) definit.

7.3.13 **A** *nem* indefinit.

7.3.14

(a) **A** *nem* indefinit.

(b) **A** indefinit vagy $\mathbf{A} = \mathbf{0}$.

(c) PD, ND: 0; PSZ, NSZ: a diagonális mátrix főátlójában a nullák száma; I, $\mathbf{0}$: $\dim V$.

(d) Csak I-nél van változás (c)-hez képest, a válasz: $\dim V - \max(r, s)$, ahol r, illetve s a diagonális mátrix főátlójában a pozitív, illetve negatív elemek száma. (Ez a képlet egyébként a többi alakra is helyes.)

7.4.

7.4.1 Ha az $\mathbf{u}$, illetve $\mathbf{v}$ vektorok koordinátái $u_1, \dots, u_n$, illetve $v_1, \dots, v_n$, akkor legyen $\mathbf{u}\cdot\mathbf{v} = \sum_{j=1}^{n} \overline{u_j} v_j$. Ez pozitív definit ermitikus bilineáris függvény lesz.

7.4.2 Csak a $\mathbf{0}$ ilyen.

7.4.3 Igaz: (a).

7.4.4 A valós esethez képest csak annyi a változás, hogy (b)-ben és (c)-ben a soroknál a skalár helyett a skalár konjugáltjával kell operálni. Részletesen:

(b) A harmadik sor $\overline{\lambda}$-val, a harmadik oszlop λ-val szorzódik, emiatt speciálisan α_{33} a $|\lambda|^2$-szeresére változik.

(c) A harmadik sorhoz a második sor $\overline{\mu}$-szörösét, a harmadik oszlophoz pedig a második oszlop μ-szörösét kell hozzáadni, emiatt speciálisan az új harmadik sor harmadik eleme $\alpha'_{33} = \alpha_{33} + \overline{\mu}\alpha_{23} + \mu\alpha_{32} + |\mu|^2\alpha_{22}$ lesz.

7.4.5 Figyeljünk oda, hogy időnként konjugálni kell, és a szimmetrikus helyett az ermitikus tulajdonságra van szükség.

7.4.6 Olyan diagonális mátrixokat választunk, amelyekben a főátló elemei az 1, a -1 és a 0 közül kerülnek ki. Az általunk megadott **A**-ortogonális bázisokat „le kell normálni” (azaz alkalmas skalárokkal be kell szorozni), hogy pontosan ezeknek a mátrixoknak feleljenek meg.

(a) $\begin{pmatrix}1&0\\0&0\end{pmatrix}$, **A**-ortogonális bázis (az eredeti bázis szerinti koordinátavektorokként felírva): $\begin{pmatrix}1\\0\end{pmatrix}, \begin{pmatrix}1\\i\end{pmatrix}$, $\tilde{\mathbf{A}}(\mathbf{x}) = |x_1 + ix_2|^2$, PSZ.

(b) $\begin{pmatrix}1&0\\0&-1\end{pmatrix}$, **A**-OB: $\begin{pmatrix}1\\-i\end{pmatrix}, \begin{pmatrix}1\\i\end{pmatrix}$,
$\tilde{\mathbf{A}}(\mathbf{x}) = |(x_1 + ix_2)/\sqrt{2}|^2 - |(x_1 - ix_2)/\sqrt{2}|^2$, I.

(c) $\begin{pmatrix}1&0&0\\0&0&0\\0&0&0\end{pmatrix}$, **A**-OB: $\begin{pmatrix}1\\\rho^2\\\rho\end{pmatrix}, \begin{pmatrix}1\\\rho\\\rho^2\end{pmatrix}, \begin{pmatrix}1\\1\\1\end{pmatrix}$,
$\tilde{\mathbf{A}}(\mathbf{x}) = |x_1 + \rho x_2 + \rho^2 x_3|^2$, PSZ.

7.4.7 Ermitikus kvadratikus alak értékkészlete négyféle lehet: összes valós szám, nemnegatív valós számok, nempozitív valós számok, illetve csak a 0.
Az általános esetben a keresett példák már alkalmas diagonális mátrixokkal is megvalósíthatók.

7.4.8
(a) A mátrix megegyezik az adjungáltjának a negatívjával.
(b) Ellenőrizzük, hogy egyrészt egy ermitikus függvény i-szerese valóban ferdén ermitikus, másrészt pedig egy ferdén ermitikus függvény $1/i$-szerese ermitikus.
(c) A kvadratikus alak értékkészlete csak imaginárius számokat tartalmaz.
(d) Hasonlóan kell eljárni, mint a 7.2.2 feladatnál.

7.4.9 Igaz: (c).

7.4.10 Közvetlenül ellenőrizhető, hogy az ermitikus függvények skalárszorosai rendelkeznek a szóban forgó tulajdonsággal. A megfordításhoz próbáljunk először olyan δ-t választani, amelyre $\mathbf{A}(\mathbf{u}, \mathbf{v} - \delta\mathbf{u}) = 0$, majd használjuk ki a feltett tulajdonságot. Kisebb átalakítások után $\mathbf{A}(\mathbf{u}, \mathbf{v}) = \theta\overline{\mathbf{A}(\mathbf{v}, \mathbf{u})}$ adódik, ahol θ nem függ $\mathbf{v}$-től. Ezután némi ügyeskedéssel megmutatható, hogy $\mathbf{u}$-tól sem függ. Végül $|\theta| = 1$ alapján kapjuk, hogy $(1/\sqrt{\theta})\mathbf{A}$ ermitikus.

A megfordítást „szervezettebben” is végiggondolhatjuk az alábbi „trükk” felhasználásával: $\mathbf{A}\big(\mathbf{u}, \mathbf{A}(\mathbf{u}, \mathbf{v})\mathbf{u} - \mathbf{A}(\mathbf{u}, \mathbf{u})\mathbf{v}\big) = 0$.

Harmadik út a megfordításhoz: Végezzünk (módosított) Gauss-kiküszöbölést az **A** (egyik) mátrixán. A feltételből következik, hogy egy oszlop „kinullázása” után a megfelelő sor is magától kinullázódott. Így diagonális mátrixhoz jutunk. Emeljük ki a főátló egy nem nulla elemét. Azt kell még igazolni, hogy ekkor a főátlóban (is) csupa valós szám marad.

8. Euklideszi terek

8.1.

8.1.1 Legegyszerűbben úgy érünk célhoz, ha a második négy vektorról megmutatjuk, hogy az első négy által definiált skalárszorzatra nézve ortonormált bázist alkotnak.

8.1.2 A $\sum_{j=1}^{k} \lambda_j \mathbf{a}_j = \mathbf{0}$ egyenlőség mindkét oldalának az $\mathbf{a}_j$-vel vett skalárszorzatát képezve $\lambda_j = 0$ adódik.

8.1.3 Pl. a Gram–Schmidt ortogonalizációból következik.

8.1.4 Ortonormált bázis:

(a) $1/\sqrt{2}, x\sqrt{3/2}, (x^2 - 1/3)\sqrt{45/8}$;

(b) $1, x - 1, (x - 1)^2/2$;

(c) $1/3, x/\sqrt{60}, (x^2 - 20/3)/\sqrt{308}$;

(d) $1/3, (x - 5)/\sqrt{60}, [(x - 5)^2 - 20/3]/\sqrt{308}$.

8.1.6 A 8.1.7 Tételből, illetve annak első bizonyításából következik.

8.1.7 (a) $W_1^\perp = \{\mathbf{v} \mid v_3 = v_4 = v_5 = 0\}$. (b) $W_2^\perp = \{\mathbf{v} \mid \sum_{j=1}^{5} v_i = 0\}$.
(c) $W_3^\perp = \{\mathbf{v} \mid v_1, \dots, v_5$ számtani sorozat$\}$.

8.1.8 A második feltételből $W \subseteq U^\perp$, az elsőből pedig $\dim W \geq \dim U^\perp$ következik.

8.1.9 Útmutatás (c)-hez: alkalmazzuk (b)-t U_i helyébe $U_i^\perp$-t írva, majd vegyük mindkét oldal merőleges kiegészítőjét.

8.1.10 Útmutatás (b)-hez: legyenek pl. $\mathbf{v}_j$ koordinátái egy ortonormált bázisban $j, j^2, \dots, j^n$.

8.1.11 Mivel $i \neq j$-re $\mathbf{b}_i \cdot \mathbf{c}_j = 0$, így $\mathbf{c}_j$ eleme a $\langle \mathbf{b}_1, \dots, \mathbf{b}_{j-1}, \mathbf{b}_{j+1}, \dots, \mathbf{b}_n \rangle^\perp$ egydimenziós altérnek. Ezután a $\mathbf{b}_j \cdot \mathbf{c}_j = 1$ kikötés egyértelműen kijelöli $\mathbf{c}_j$-t. Azt, hogy a $\mathbf{c}_j$-k lineárisan függetlenek, a 8.1.2 feladathoz hasonlóan kell igazolni.

8.1.12 Képezzük a skalárszorzatot V olyan bázisa szerint, amely U és W bázisának egyesítéséből keletkezett. Végtelen sok ilyen skalárszorzat létezik.

8.1.13 Útmutatás (b)-hez: Legyen $\mathbf{e}_1, \dots, \mathbf{e}_n$ ortonormált bázis. Ekkor pontosan az a $\mathbf{c}$ vektor felel meg, amelynek koordinátái a $\Psi(\mathbf{e}_i)$ értékek.

8.1.14 Tudjuk, hogy a dimenziók egyenlősége szükséges és elégséges feltétel a vektorterek izomorfiájához. Így csak azt kell igazolni, hogy azonos dimenzió esetén létezik olyan vektortérizomorfizmus, amely még a skalárszorzatot is tartja. Erre bármely olyan lineáris leképezés megfelel, amely ortonormált bázist ortonormált bázisba visz át.

8.1.15

(a) Az egyetlen nehézséget annak az igazolása jelenti, hogy két V-beli sorozat összege is V-beli. Ehhez lássuk be a $\sum_{j=1}^{\infty}(\alpha_j + \beta_j)^2 \leq$ $\leq 2\sum_{j=1}^{\infty}\alpha_j^2 + 2\sum_{j=1}^{\infty}\beta_j^2$ egyenlőtlenséget.

(b) Ne felejtsük el megmutatni, hogy $\sum_{j=1}^{\infty}\alpha_j\beta_j$ konvergens.

(c) $\mathbf{0}$.

8.1.16

(b) Az $\Rightarrow$ irány hamis, lásd pl. a 8.1.15c feladatot.

(c) Pl. a 8.1.15c feladat U-jára nem teljesül az egyenlőség.

(d) Az egyik irányú tartalmazáshoz vegyük a (c)-beli összefüggés mindkét oldalának merőleges kiegészítőjét, a másik irányú tartalmazáshoz pedig alkalmazzuk (c)-t U helyett $U^{\perp}$-re.

8.1.17 A 8.1.7 Tétel állítása hamis, a 8.1.9 feladat (b) része igaz, az (a) egyik iránya és a (c) rész hamis. Ellenpéldákat a 8.1.15c feladat felhasználásával gyárthatunk.

8.2.

8.2.1 $\sqrt{2}$.

8.2.2 $60°$.

8.2.3

(a) Pitagorasz-tétel és megfordítása.

(b) Egy paralelogramma pontosan akkor rombusz, ha az átlói merőlegesek.

(c) Egy paralelogrammában az átlók négyzetösszege megegyezik az oldalak négyzetösszegével.

8.2.4 Normált tér: (b), (d), (e).
Útmutatás (e)-nél a háromszögegyenlőtlenséghez: Először lássuk be, hogy nemnegatív a_j, b_j-kre

$$a_1b_1 + \ldots + a_nb_n \leq (a_1^3 + \ldots + a_n^3)^{\frac{1}{3}} \cdot (b_1^{3/2} + \ldots + b_n^{3/2})^{\frac{2}{3}} \qquad \text{(E.8.1)}$$

teljesül. Az a_j-ket, illetve a b_j-ket alkalmas pozitív számmal végigszorozva ekvivalens egyenlőtlenség adódik, így feltehetjük, hogy a jobb oldalon mindkét tényező 1. Az $a^3, b^{3/2}, b^{3/2}$ számokra a számtani és mértani közép közötti egyenlőtlenséget felírva $ab \leq a^3/3 + 2b^{3/2}/3$ adódik. Ezt az összes a_j, b_j párra összegezve éppen a kívánt $a_1b_1 + \ldots + a_nb_n \leq 1$

egyenlőtlenséget kapjuk. Rátérve a háromszögegyenlőtlenségre, elég nemnegatív c_j, d_j-kre

$$S = \left(\sum_{j=1}^{n}(c_j + d_j)^3\right)^{\frac{1}{3}} \le \left(\sum_{j=1}^{n} c_j^3\right)^{\frac{1}{3}} + \left(\sum_{j=1}^{n} d_j^3\right)^{\frac{1}{3}} = T + U$$

fennállását igazolni. A bal oldal köbét $S^3 = \sum_{j=1}^{n} c_j(c_j + d_j)^2 + + \sum_{j=1}^{n} d_j(c_j+d_j)^2$ alakban írva mindkét összegre alkalmazzuk az (E.8.1) egyenlőtlenséget $b_j = (c_j + d_j)^2$ és $a_j = c_j$, illetve d_j szereposztással. Ekkor éppen $S^3 \le TS^2 + US^2$, azaz a kívánt $S \le T + U$ adódik.

Megjegyezzük, hogy a köbök helyett bármilyen $p > 1$ kitevőjű hatvánnyal hasonló módon definiálhatunk normát. Az erre vonatkozó háromszögegyenlőtlenséget *Minkowski-egyenlőtlenség*nek, az (E.8.1)-nek megfelelő

$$a_1b_1 + \ldots + a_nb_n \le (a_1^p + \ldots + a_n^p)^{\frac{1}{p}} \cdot (b_1^q + \ldots + b_n^q)^{\frac{1}{q}}$$

összefüggést pedig, ahol $1/p + 1/q = 1$, *Hölder-egyenlőtlenség*nek nevezzük. A $p = 2$ speciális esetben a Hölder-egyenlőtlenség éppen a CBS-t adja. A $p = 3$-ra most vázolt bizonyítás tetszőleges racionális p-re átvihető.

8.2.5

(a) Az előző feladat példái megfelelnek.

(b) Az egyik irány a 8.2.3c feladat. A megfordításhoz fejezzük ki két vektor skalárszorzatát a norma segítségével: $\mathbf{x}\cdot\mathbf{z} = (1/4)(\|\mathbf{x} + \mathbf{z}\|^2 - -\|\mathbf{x}-\mathbf{z}\|^2)$, és lássuk be, hogy az így kapott függvény a feltétel teljesülése esetén valóban skalárszorzatot definiál. Itt a (bi)linearitás igazolása okoz nehézséget. A feltételt írjuk fel az $\mathbf{x} = \mathbf{u}+\mathbf{v}$ és $\mathbf{z} = \mathbf{w}$, valamint $\mathbf{x} = \mathbf{u}-\mathbf{v}$ és $\mathbf{z} = \mathbf{w}$ vektorpárokra, majd a két egyenlőséget kivonva eljuthatunk az első változó szerinti összegtartáshoz. A skalárszorostartást egész, majd racionális skalárokra az öszegtartásból vezethetjük le. Tetszőleges valós λ-ra innen ez úgy következik, hogy az $f(\lambda) = (\lambda\mathbf{x})\cdot\mathbf{z} - \lambda(\mathbf{x}\cdot\mathbf{z})$ függvényről kimutatjuk, hogy mindenütt folytonos. Ez a második tagra nyilvánvaló. Az elsőt írjuk fel a normákkal: $(\lambda\mathbf{x})\cdot\mathbf{z} = (1/4)(\|\lambda\mathbf{x} + \mathbf{z}\|^2 - \|\lambda\mathbf{x} - \mathbf{z}\|^2)$. Nyilván elég $\|\lambda\mathbf{x} + \mathbf{z}\|$ folytonosságát belátni (a másik tagra ugyanúgy megy). Ezt a háromszögegyenlőtlenség és a skalárkiemelési tulajdonság felhasználásával a következőképpen kapjuk:

$$\|\lambda\mathbf{x} + \mathbf{z}\| - \|\mu\mathbf{x} + \mathbf{z}\| \le \|(\lambda - \mu)\mathbf{x}\| = |\lambda - \mu| \cdot \|\mathbf{x}\|\,.$$

8.2.6 Metrikus tér: (b), (c).

8.2.7 Az előző feladat (c) példája megfelel.

8.2.8 A CBS második bizonyításában legyen minden $z_j = 1$. Egyenlőség akkor teljesül, ha minden x_j egyenlő és nemnegatív.

8.2.9 Igaz: (a).

8.2.10 (a) 30°. (b) 120°. (c) 45°.

8.2.11 (a) 16, 32, illetve 8. (b) 2. (c) 60°. (d) 60°, 90° vagy 120°. (e) 1, illetve $1/2$.

8.2.12 Két részhalmaz távolságán a pontjaik távolságainak az infimumát értjük. Lássuk be, hogy (a geometriából megszokott tapasztalatunkkal összhangban) egy $\mathbf{v}$ vektorhoz egy U altérben a $\mathbf{v}$ vektor merőleges vetülete van a legközelebb. A konkrét példában a vektor és az altér távolsága 5.

8.2.13 A keresett $\mathbf{z}$-(ke)t az $A\mathbf{z} = \mathbf{b}'$ egyenletrendszer megoldása(i)ként kapjuk, ahol $\mathbf{b}'$ az az $\operatorname{Im} A$-beli vektor, amely a legközelebb van $\mathbf{b}$-hez. Ez a $\mathbf{b}'$ éppen a $\mathbf{b}$-nek az $\operatorname{Im} A$ altérbe eső merőleges vetülete. Az $A\mathbf{z} = \mathbf{b}'$ egyenletrendszer megoldásait az eredeti egyenletrendszerbe behelyettesítve így lesz a jobb oldali értékektől (azaz a $\mathbf{b}$ megfelelő komponenseitől) való eltérések négyzetösszege minimális. A konrét egyenletrendszernél $\mathbf{b}' = \begin{pmatrix} 0 \\ 3 \\ 6 \end{pmatrix}$, $\mathbf{z} = \begin{pmatrix} -3 + \mu + 2\nu \\ 3 - 2\mu - 3\nu \\ \mu \\ \nu \end{pmatrix}$, ahol μ és ν tetszőleges valós számok, és ezeket behelyettesítve az eltérések (lehető legkisebb) négyzetösszege 6.

8.2.14
(a) Az $\mathbf{x} = \sum_{j=1}^{n} \lambda_j \mathbf{e}_j$ egyenlőség két oldalának $\mathbf{e}_i$-vel vett skalárszorzatából kapjuk, hogy $\lambda_i = \mathbf{x}\cdot\mathbf{e}_i$.
(b) Az (a)-beli előállítások segítségével képezzük az $\mathbf{x}\cdot\mathbf{z}$ skalárszorzatot.
(c) Alkalmazzuk (b)-t $\mathbf{z} = \mathbf{x}$-szel.
Mindhárom állítást közvetlenül is leolvashatjuk a koordinátás felírásokból.

8.2.15 Az egyenlőtlenség a 8.2.14c feladatból következik. Egyenlőség pontosan akkor teljesül, ha $\mathbf{x} \in \langle \mathbf{c}_1, \ldots, \mathbf{c}_k \rangle$.

8.2.16 A CBS-re adott második és harmadik bizonyítás (minimális módosításokkal) átvihető a szemidefinit esetre is. Megjegyezzük, hogy a szemidefinit esetben egyenlőség akkor is előfordulhat, ha a két vektor lineárisan független.

8.2.17 (a) n. (b) 3 (ha $n \geq 2$).

8.2.18 Az első és a harmadik bizonyítás átvihető a végtelen dimenziós esetre is.

8.3.

8.3.1 A valósban adott bizonyítások szinte változtatás nélkül érvényesek. [A 8.2.14–8.2.15 feladatoknál figyeljünk oda, hogy a(z általában nem valós értékű) skalárszorzatokban most a tényezők sorrendje lényeges, valamint a skalárszorzatok *abszolút érték*ének a négyzete szerepel.]

8.3.2

(a) Használjuk fel, hogy $i\mathbf{x}+\mathbf{z}=i(\mathbf{x}-i\mathbf{z})$.

(b) Az $(\mathbf{x}+i\mathbf{z})\cdot(i\mathbf{x}+\mathbf{z})$ skalárszorzatot kifejtve válasszuk külön a valós és a képzetes részt.

8.3.3 Az (a)-ban csak az $\Rightarrow$, (b)-ben csak a $\Leftarrow$ rész igaz, (c) továbbra is érvényes.

8.3.4 A 8.2.8 Tételre adott második bizonyítás adaptálása: Az ortonormált bázis szerinti koordinátákkal a négyzetre emelt egyenlőtlenség az

$$|\overline{x_1}z_1+\ldots+\overline{x_n}z_n|^2\le(|x_1|^2+\ldots+|x_n|^2)(|z_1|^2+\ldots+|z_n|^2)$$

módon írható fel. Kihasználva a $|w|^2=\overline{w}w$ összefüggést, ez a

$$0\le\sum_{1\le i<j\le n}|x_iz_j-x_jz_i|^2$$

alakra hozható.

A harmadik bizonyítás adaptálása: Most is a minden (komplex) λ-ra érvényes

$$0\le\|\lambda\mathbf{x}+\mathbf{z}\|^2=(\lambda\mathbf{x}+\mathbf{z})\cdot(\lambda\mathbf{x}+\mathbf{z})=|\lambda|^2(\mathbf{x}\cdot\mathbf{x})+2\mathrm{Re}[\lambda(\mathbf{z}\cdot\mathbf{x})]+\mathbf{z}\cdot\mathbf{z}$$

egyenlőtlenségből indulunk ki. Legyen speciálisan $\lambda=\mu\rho$, ahol μ tetszőleges valós szám, ρ pedig olyan egységnyi abszolút értékű komplex szám, amellyel $\rho(\mathbf{z}\cdot\mathbf{x})$ pozitív valós. (Ez csak $\mathbf{z}\cdot\mathbf{x}=0$ esetén nem érhető el, de akkor a CBS triviálisan igaz.) A λ fenti előállítását a kiindulási egyenlőtlenségünkbe beírva minden μ valós számra $0\le\mu^2(\mathbf{x}\cdot\mathbf{x})+2\mu|\mathbf{z}\cdot\mathbf{x}|+\mathbf{z}\cdot\mathbf{z}$ adódik. Ezután a bizonyítást ugyanúgy fejezhetjük be, mint a valós esetben.

8.3.5

(a) Ha $\mathbf{z}\neq\mathbf{0}$, akkor $\mathbf{z}$-ből valamelyik nem nulla komponensét kiemelve $\mathbf{z}=\alpha\mathbf{w}$ alakban írható, ahol $\mathbf{w}$ egyik komponense 1. Ha $\mathbf{w}$ és $\overline{\mathbf{w}}$ egymás skalárszorosai, akkor ez a skalár csak 1 lehet, tehát $\mathbf{w}=\overline{\mathbf{w}}$, azaz $\mathbf{w}$ valós vektor.

(b) A skalárszorosnál ügyeljünk arra, hogy $\overline{\mu\mathbf{x}}=\overline{\mu}\cdot\overline{\mathbf{x}}(\neq\mu\overline{\mathbf{x}})$.

(d) Az elégségességhez írjuk fel U elemeit ebben a valós vektorokból álló bázisban. A szükségességhez egy tetszőleges $\mathbf{0} \neq \mathbf{z} \in U$ vektorból kiindulva $\overline{\mathbf{z}} \in U$ és így $\mathbf{v} = \overline{\mathbf{z}} + \mathbf{z} \in U$ adódik. Itt $\mathbf{v}$ valós vektor. Ha $\mathbf{v} = \mathbf{0}$, akkor $i\mathbf{z}$ valós vektor. Mindenképpen találtunk U-ban egy nem nulla $\mathbf{b}$ valós vektort. Ez lesz a keresett bázis első eleme. Legyen W a $\langle \mathbf{b} \rangle$ altér U-beli merőleges kiegészítője. Megmutatjuk, hogy $\overline{W} = W$, és így az előző eljárást W-re megismételve végül U egy valós (ráadásul akár ortonormált) bázisához jutunk. A $\overline{W} = W$ tulajdonság igazolásához konjugáljuk az $U = \langle \mathbf{b} \rangle \oplus W$ felírást: $\overline{U} = \overline{\langle \mathbf{b} \rangle} \oplus \overline{W}$. Itt $\overline{U} = U$, illetve $\mathbf{b}$ valós volta miatt a bal oldalon, illetve a jobb oldal első tagjánál a konjugált jel elhagyható. A merőleges kiegészítő altér egyértelműségéből kapjuk, hogy valóban $\overline{W} = W$.

(e) A dimenziók közötti összefüggésekből adódik, hogy n csak páros lehet. Páros n-re válasszuk U bázisának azokat a vektorokat, amelyek $2j-1$-edik komponense 1, a $2j$-edik i, a többi pedig 0, $j = 1, 2, \ldots, n/2$.

8.4.

8.4.1 A szorzatra vonatkozó azonosság igazolása: $((\mathcal{AB})\mathbf{x})\cdot\mathbf{z} = (\mathcal{A}(\mathcal{B}\mathbf{x}))\cdot\mathbf{z} = (\mathcal{B}\mathbf{x})\cdot(\mathcal{A}^*\mathbf{z}) = \mathbf{x}\cdot((\mathcal{B}^*(\mathcal{A}^*\mathbf{z})) = \mathbf{x}\cdot((\mathcal{B}^*\mathcal{A}^*)\mathbf{z})$. Az egyenlőségsorozat elejét és végét tekintve, az $(\mathcal{AB})^*$ adjungált definíciójából (és egyértelműségéből) kapjuk a kívánt $(\mathcal{AB})^* = \mathcal{B}^*\mathcal{A}^*$ állítást. Ugyanígy látható be a feladat többi része is.
Másik lehetőség: ortonormált bázis szerinti mátrixokra áttérve felhasználhatjuk a mátrixokra vonatkozó hasonló azonosságokat (2.1.20 feladat).

8.4.2 (a), (b), (e), (f): $\mathcal{A}^* = \mathcal{A}$. (c), (d): $\mathcal{A}^* = A^{-1}$.
(g) és (h) egymás adjungáltjai.
A legegyszerűbben (alkalmas) ortonormált bázisban felírt mátrixokkal okoskodhatunk.

8.4.3 $\mathcal{A}^* = -\mathcal{A}$.

8.4.4

(a) Legyen $h = \beta_0 + \beta_1 x + \beta_2 x^2$ és $\mathcal{A}^* h = r$.
Ha $f = 1$, akkor $\mathcal{A}f = f'' = 0$, tehát $0 = (\mathcal{A}f)\cdot h = f\cdot(\mathcal{A}^* h) = \int_{-1}^{+1} r(t)dt$.
Ugyanígy az $f = x$ polinommal $0 = \int_{-1}^{+1} tr(t)dt$ adódik.
Az integrálásokat elvégezve kapjuk, hogy $r = \alpha(-3x^2 + 1)$ alakú.
Tekintsük végül $f = x^2$-et. Legyen $g = 1$-re $\mathcal{A}^* g = \alpha_0(-3x^2 + 1)$. Ekkor $(\mathcal{A}f)\cdot g = \int_{-1}^{+1} 2dt = 4$ és $f\cdot(\mathcal{A}^* g) = \int_{-1}^{+1} t^2\alpha_0(-3t^2 + 1)dt = -8\alpha_0/15$.

Innen $\alpha_0 = -15/2$, tehát $\mathcal{A}^*1 = 15(3x^2-1)/2$. Hasonlóan kapjuk az x és x^2 polinom képét is: $\mathcal{A}^*x = 0$ és $\mathcal{A}^*x^2 = 5(3x^2-1)/2$. Ebből a fenti általános h-ra $\mathcal{A}^*h = (15\beta_0 + 5\beta_2)(3x^2-1)/2$ adódik.

(b) $\mathcal{A}^*h = (\beta_0+\beta_1+\beta_2)(x-1)^2/2$.

(c),(d) $\mathcal{A}^*h = (3\beta_0 + 20\beta_2)(3x^2-20)/154$.

8.4.5 $(\mathcal{A}^*\mathbf{x})\cdot(\mathcal{A}\mathbf{x}) = \mathbf{x}\cdot(\mathcal{A}^2\mathbf{x}) = 0$.
A megfordítás komplex euklideszi térben igaz, valósban hamis. Ha ugyan is az $\mathbf{x}\cdot(\mathcal{A}^2\mathbf{x})$ kvadratikus alak azonosan nulla, akkor ebből $\mathbf{C}$ felett a 7.4.3 Tétel szerint következik, hogy az $\mathbf{u}\cdot(\mathcal{A}^2\mathbf{v})$ bilineáris függvény is azonosan nulla, tehát $\mathcal{A}^2 = \mathcal{O}$. A valós test felett a 7.3.1a feladat szerint csak $\mathbf{u}\cdot(\mathcal{A}^2\mathbf{v}) = -\mathbf{v}\cdot(\mathcal{A}^2\mathbf{u})$ adódik, ami pl. a síkon akkor is teljesül, ha $\mathcal{A}$ a 45 fokos forgatás (az origó körül). Valós euklideszi térben $\mathcal{A}^2 + (\mathcal{A}^*)^2 = \mathcal{O}$ a „helyes" szükséges és elégséges feltétel arra, hogy minden $\mathbf{x}$-re $\mathcal{A}\mathbf{x} \perp \mathcal{A}^*\mathbf{x}$ teljesüljön.

8.4.6 Legyen $\mathcal{A}\mathbf{x} = \mu\mathbf{x}, \mathcal{A}^*\mathbf{z} = \nu\mathbf{z}$. Ekkor $\overline{\mu}(\mathbf{x}\cdot\mathbf{z}) = (\mu\mathbf{x})\cdot\mathbf{z} = (\mathcal{A}\mathbf{x})\cdot\mathbf{z} = \mathbf{x}\cdot(\mathcal{A}^*\mathbf{z}) = \mathbf{x}\cdot(\nu\mathbf{z}) = \nu(\mathbf{x}\cdot\mathbf{z})$. Innen vagy $\mathbf{x}\cdot\mathbf{z} = 0$ vagy $\overline{\mu} = \nu$.

8.4.7 A karakterisztikus polinomot ortonormált bázis szerint írjuk fel. A minimálpolinomra a definíciót és a 8.4.1 feladatot használjuk fel. A sajátértékekre vonatkozó állítást a karakterisztikus (vagy a minimál)polinomra nyert eredményből kapjuk. (Vigyázat, $\mathcal{A}$ és $\mathcal{A}^*$ saját*vektor*ai között általában nincs szoros kapcsolat!)

8.4.8 $\operatorname{Ker}\mathcal{A}^* = (\operatorname{Im}\mathcal{A})^\perp$ igazolása:
$\mathcal{A}^*\mathbf{z} = \mathbf{0} \iff \forall\mathbf{x}\ \ \mathbf{x}\cdot(\mathcal{A}^*\mathbf{z}) = 0 \iff \forall\mathbf{x}\ \ (\mathcal{A}\mathbf{x})\cdot\mathbf{z} = 0 \iff \mathbf{z} \perp \operatorname{Im}\mathcal{A}$.

8.4.9 Használjuk fel az előző feladatot. Másik lehetőség: írjuk fel egy ortonormált bázis szerint a mátrixokat, és hasonlítsuk össze a rangjukat.

8.4.10 Használjuk fel a 8.4.8 feladat első egyenlőségét.

8.4.11 (b) Ha $\mathcal{A}\mathbf{x} = \mathbf{0}$, akkor $(\mathcal{A}^*\mathcal{A})\mathbf{x} = \mathcal{A}^*\mathbf{0} = \mathbf{0}$. Megfordítva, ha $(\mathcal{A}^*\mathcal{A})\mathbf{x} = \mathbf{0}$, akkor $0 = \mathbf{x}\cdot((\mathcal{A}^*\mathcal{A})\mathbf{x}) = (\mathcal{A}\mathbf{x})\cdot(\mathcal{A}\mathbf{x})$, tehát $\mathcal{A}\mathbf{x} = \mathbf{0}$. A képterekre vonatkozó állítás az egyik irányú tartalmazásból és a magteres állításból adódó dimenzióegyenlőségből következik.

8.4.12

(a) Az $(\mathcal{A}\mathbf{x})\cdot(\mathcal{B}\mathbf{z}) = \mathbf{x}\cdot((\mathcal{A}^*\mathcal{B})\mathbf{z})$ összefüggés igazolja az állítást és a megfordítást is.

(b) Ha $\mathcal{A}\mathbf{x} = \mathcal{B}\mathbf{x} = \mathbf{0}$, akkor nyilván $(\mathcal{A}+\mathcal{B})\mathbf{x} = \mathcal{A}\mathbf{x} + \mathcal{B}\mathbf{x} = \mathbf{0}$. A másik irányú tartalmazás: Ha $(\mathcal{A}+\mathcal{B})\mathbf{x} = \mathbf{0}$, akkor $\mathcal{A}\mathbf{x} = -\mathcal{B}\mathbf{x}$. Itt a bal oldal $\operatorname{Im}\mathcal{A}$-ban, a jobb oldal pedig $\operatorname{Im}\mathcal{B}$-ben van, és így az (a)

rész felhasználásával mindkét oldal csak a nullvektor lehet. A (b) állítás megfordítása nem igaz (ami nem meglepő, hiszen a $\operatorname{Ker}(\mathcal{A}+\mathcal{B}) = \operatorname{Ker}\mathcal{A}\cap\operatorname{Ker}\mathcal{B}$ feltétel független a skalárszorzattól).

8.4.13 Az $\mathcal{A}^*\mathcal{B}=\mathcal{O}$ feltételből az előző feladat szerint $\operatorname{Im}\mathcal{A}\cap\operatorname{Im}\mathcal{B}=\mathbf{0}$ következik. Meg kell még mutatni, hogy $\operatorname{Im}(\mathcal{A}+\mathcal{B}) = \langle\operatorname{Im}\mathcal{A},\operatorname{Im}\mathcal{B}\rangle$. Itt az egyik irányú tartalmazás világos, a másikhoz azt igazoljuk, hogy $\operatorname{Im}\mathcal{A},\operatorname{Im}\mathcal{B}\subseteq \subseteq \operatorname{Im}(\mathcal{A}+\mathcal{B})$. A $\mathcal{B}\mathcal{A}^*=\mathcal{O}$ egyenlőséget adjungálva $\mathcal{A}\mathcal{B}^*=\mathcal{O}$ adódik, tehát ez a feltétel is szimmetrikus $\mathcal{A}$-ban és $\mathcal{B}$-ben, így elég $\operatorname{Im}\mathcal{A}$-val foglalkoznunk. Fusson végig $\mathbf{x}$ az $\operatorname{Im}\mathcal{A}^*$ altéren. Ekkor $\mathcal{B}\mathbf{x}=\mathbf{0}$ miatt $(\mathcal{A}+\mathcal{B})\mathbf{x}=\mathcal{A}\mathbf{x}$, tehát $\operatorname{Im}(\mathcal{A}+\mathcal{B})\supseteq\operatorname{Im}(\mathcal{A}\mathcal{A}^*)=\operatorname{Im}\mathcal{A}$ (felhasználva a 8.4.11b feladatot is).

8.4.14 (a) $\mathcal{A}=\lambda\mathcal{E}$.

8.5.

8.5.1

(a) Használjuk fel, hogy egy (ortonormált) sajátbázis szerinti mátrixban a sajátértékek éppen a főátló elemei.

(b) Hamis. Lehet, hogy a transzformációnak egyáltalán nincs diagonális mátrixa, illetve ha van is, az nem képezhető ortonormált bázis szerint.

8.5.2 Ha valamely $0<s<t$-re $\mathcal{A}^s=\mathcal{A}^t$, akkor $\mathcal{A}$ gyöke az x^t-x^s polinomnak, így sajátértékei (amelyek az előző feladat szerint valósak) csak 0 és ±1 lehetnek. Innen egy ortonormált sajátbázis szerinti mátrix segítségével kapjuk, hogy $\mathcal{A}^3=\mathcal{A}$. (Hasonlóan érhetünk célhoz, ha az önadjungált transzformáció helyett rögtön áttérünk egy valós elemű diagonális mátrixra.)

8.5.3 Lásd a 8.5.1 feladathoz adott útmutatásokat.

8.5.4 Az állítás hamis. Pontosan azok a transzformációk tehetők normálissá, amelyeknek létezik diagonális mátrixuk.

8.5.5 A legegyszerűbben (a szokásos) ortonormált bázis szerinti mátrixokon ellenőrizhetjük a feltételek teljesülését. Eredmények: $\mathcal{A}$ és $\mathcal{C}$ nem normális, $\mathcal{B}$ unitér, $\mathcal{D}$ önadjungált és $\mathcal{F}$ normális (de nem önadjungált és nem unitér).

8.5.6 Ha $\mathcal{A},\mathcal{B}$ önadjungált, akkor $\mathcal{A}+\mathcal{B}$ és $\mathcal{A}^2$ is önadjungált, de $\lambda\mathcal{A}$ és $\mathcal{A}\mathcal{B}$ nem feltétlenül az: $\lambda\mathcal{A}$ csak valós λ-ra (vagy $\mathcal{A}=\mathcal{O}$-ra) lesz önadjungált, $\mathcal{A}\mathcal{B}$ pedig csak az $\mathcal{A}\mathcal{B}=\mathcal{B}\mathcal{A}$ esetben (lásd a 8.5.7 feladatot).
Ha $\mathcal{A},\mathcal{B}$ unitér, akkor $\mathcal{A}\mathcal{B}$ és így $\mathcal{A}^2$ is unitér, de $\lambda\mathcal{A}$ és $\mathcal{A}+\mathcal{B}$ nem feltétlenül az.

Ha $\mathcal{A}, \mathcal{B}$ normális, akkor $\lambda\mathcal{A}$ és $\mathcal{A}^2$ is normális, de $\mathcal{A}+\mathcal{B}$ és $\mathcal{AB}$ nem feltétlenül az.

8.5.7

(a) A gondolatmenet helyességéhez az kellene, hogy a két transzformációhoz *közös* ortonormált sajátbázist találjunk, ilyen azonban általában nincs. Maga az állítás sem igaz, a (b) pont alapján könnyen gyárthatunk ellenpéldát.

(b) Ha $\mathcal{A}$ és $\mathcal{B}$ önadjungált, akkor $(\mathcal{AB})^* = \mathcal{B}^*\mathcal{A}^* = \mathcal{BA}$.

8.5.8 Használjuk fel ortonormált sajátbázis létezését.
A megfordítás hamis, mert lehet, hogy nem létezik sajátbázis.

8.5.9 Igaz: (a).

8.5.10

(a) $\|\mathcal{A}\mathbf{x}\|^2 = (\mathcal{A}\mathbf{x})\cdot(\mathcal{A}\mathbf{x}) = \mathbf{x}\cdot(\mathcal{A}^*\mathcal{A}\mathbf{x})$. Ugyanígy $\|\mathcal{A}^*\mathbf{x}\|^2 = \mathbf{x}\cdot(\mathcal{A}\mathcal{A}^*\mathbf{x})$. Mindkét függvény $\mathbf{x}$-ben kvadratikus alak, így — mivel a komplex test felett vagyunk — pontosan akkor egyenlők, ha a megfelelő bilineáris függvények egyenlők. Ez utóbbiak egyenlősége pedig a 8.4.1 Tétel bizonyításának végén látott gondolatmenet szerint ekvivalens az $\mathcal{AA}^* = \mathcal{A}^*\mathcal{A}$ normalitási feltétellel.

(b) Ha $\mathcal{A}$ és $\mathcal{A}^*$ sajátvektorai közösek, akkor a 8.5.2 Tétel bizonyítását követve juthatunk ortonormált sajátbázishoz. A megfordításhoz tekintsük $\mathcal{A}$ egy ortonormált sajátbázisát és írjuk fel ebben a bázisban $\mathcal{A}$ és $\mathcal{A}^*$ mátrixát; a sajátvektorok ezekből a mátrixokból jól áttekinthetők.

(c) Ez a (b)-beli feltétel átfogalmazása (felhasználva a megfelelő sajátértékek kapcsolatát is).

(d),(e) A 8.4.8 feladat alapján visszavezethetők (c)-re.

8.5.11 $\mathcal{AB} = \mathcal{O} \Rightarrow \operatorname{Im}\mathcal{B} \subseteq \operatorname{Ker}\mathcal{A} \Rightarrow \operatorname{Im}\mathcal{B}^* \subseteq \operatorname{Ker}\mathcal{A}^* \Rightarrow$
$\Rightarrow (\operatorname{Ker}\mathcal{B})^\perp \subseteq (\operatorname{Im}\mathcal{A})^\perp \Rightarrow \operatorname{Ker}\mathcal{B} \supseteq \operatorname{Im}\mathcal{A} \Rightarrow \mathcal{BA} = \mathcal{O}$.
(A második lépésnél az előző feladat (c) és (d) részét alkalmaztuk $\lambda = 0$-val, a harmadik lépésnél pedig a 8.4.8 feladatot használtuk fel.)

8.5.12 A 8.5.2 Tétel bizonyításának gondolatmenetét kell megfelelően módosítani, kihasználva közben a 8.5.10b feladatot is.

8.5.13 Alkalmazzuk az előző feladatot. A megfordítás hamis, unitér transzformációk körében könnyen találunk ellenpéldát.

8.5.14 Az elégségességhez használjuk fel az előző feladatot. A szükségességhez tekintsük a normális transzformáció egy ortonormált sajátbázis szerinti diagonális mátrixát. A főátló elemeit bontsuk fel egy valós szám és egy egységnyi abszolút értékű komplex szám szorzatára, és a mátrixot írjuk fel ennek megfelelően két diagonális mátrix szorzataként.

8.5.15 Olyan $\mathbf{e}_1, \dots, \mathbf{e}_n$ ortonormált bázist keresünk, hogy $\langle \mathbf{e}_1, \dots, \mathbf{e}_k \rangle$ minden k-ra $\mathcal{A}$-nak invariáns altere legyen. Válasszuk $\mathbf{e}_n$-nek az $\mathcal{A}^*$ transzformáció egy (egységnyi normájú) sajátvektorát, ekkor $U_n = \langle \mathbf{e}_n \rangle^\perp$ az $\mathcal{A}$-nak invariáns altere. Ismételjük meg most az eljárást U_n-re (vigyázat, most az $\mathcal{A}$ transzformáció U_n-re történő megszorítása szerinti $\mathcal{A}^*$-ot kell tekinteni, ami általában nem az eredeti $\mathcal{A}^*$ megszorítása, hiszen U_n legtöbbször nem is invariáns altere az eredeti $\mathcal{A}^*$-nak), ezzel megkapjuk $\mathbf{e}_{n-1}$-et stb.

8.5.16

(a) A μ_j-k az $\mathcal{A}^*\mathcal{A}$ transzformáció sajátértékei. Ha $\mathbf{x} \neq \mathbf{0}$ és $\mathcal{A}^*\mathcal{A}\mathbf{x} = \mu\mathbf{x}$, akkor $\overline{\mu}\|\mathbf{x}\|^2 = (\mu\mathbf{x})\cdot\mathbf{x} = (\mathcal{A}^*\mathcal{A}\mathbf{x})\cdot\mathbf{x} = \|\mathcal{A}\mathbf{x}\|^2$, és innen $\mu \geq 0$.

(b) Vegyünk olyan ortonormált bázist, amelyben $\mathcal{A}$ mátrixa felsőháromszög-mátrix. Ekkor a főátlóban éppen a λ_j sajátértékek állnak. Ebben a bázisban $\mathcal{A}^*$ mátrixa alsóháromszög-mátrix és a főátlóban a $\overline{\lambda_j}$-k szerepelnek. Ebben a bázisban $\mathcal{A}^*\mathcal{A}$ mátrixa a két mátrix szorzata, és a főátlóban levő elemek összege, azaz a szorzatmátrix nyoma éppen az $[\mathcal{A}]$-beli elemek abszolút értékeinek négyzetösszege, ami így legalább $\sum_{j=1}^n |\lambda_j|^2$. Másrészt a szorzatmátrix nyoma $\sum_{j=1}^n \mu_j$.

(c) Az előző gondolatmenetből látszik, hogy egyenlőség pontosan akkor teljesül, ha a felsőháromszög-mátrixnak a főátlóján kívül minden eleme nulla.

8.5.17 Elégségesség: Ha $\mathcal{A}$ unitér és $\mathbf{u} \perp \mathbf{v}$, akkor

$$((\lambda\mathcal{A})\mathbf{u})\cdot((\lambda\mathcal{A})\mathbf{v}) = (\lambda(\mathcal{A}\mathbf{u}))\cdot(\lambda(\mathcal{A}\mathbf{v})) = |\lambda|^2(\mathcal{A}\mathbf{u}\cdot\mathcal{A}\mathbf{v}) = |\lambda|^2(\mathbf{u}\cdot\mathbf{v}) = 0.$$

A szükségességhez legyen $\mathcal{A}$ merőlegességtartó, és legyenek $\mathbf{u}$ és $\mathbf{v}$ merőleges egységvektorok. Megmutatjuk, hogy $\|\mathcal{A}\mathbf{u}\| = \|\mathcal{A}\mathbf{v}\|$. Mivel $\mathbf{u} \perp \mathbf{v}$ és $\|\mathbf{u}\| = \|\mathbf{v}\|$, ezért $\mathbf{u}+\mathbf{v} \perp \mathbf{u}-\mathbf{v}$, és így a merőlegességtartás miatt $0 = (\mathcal{A}(\mathbf{u}+\mathbf{v}))\cdot(\mathcal{A}(\mathbf{u}-\mathbf{v})) = \|\mathcal{A}\mathbf{u}\|^2 - \|\mathcal{A}\mathbf{v}\|^2$ (az utolsó egyenlőségnél $(\mathcal{A}\mathbf{u}) \perp (\mathcal{A}\mathbf{v})$-t is kihasználtuk). Legyen most $\mathbf{e}_j$ egy ortonormált bázis és az $\|\mathcal{A}\mathbf{e}_j\|$ normák közös értéke λ. Ha $\lambda \neq 0$, akkor $(1/\lambda)\mathcal{A}$ unitér lesz, ha pedig $\lambda = 0$, akkor $\mathcal{A} = \mathcal{O}$, ami triviálisan egy (tetszőleges) unitér transzformáció nullaszorosa.

8.5.18

(a),(b) Ez az $\mathcal{A}^*\mathcal{A} = \mathcal{E}$, illetve $\mathcal{A}\mathcal{A}^* = \mathcal{E}$ egyenlőség mátrixos átfogalmazása.

(c) $1 = \det E = (\det[\mathcal{A}]) \cdot (\det[\mathcal{A}]^*) = (\det[\mathcal{A}]) \cdot \overline{(\det[\mathcal{A}])} = |\det[\mathcal{A}]|^2$.

(d) Használjuk fel (c)-t és a mátrix inverzére az előjeles aldeterminánsokkal adott képletet.

8.6.

8.6.1 Az $\mathcal{A}^2 = \mathcal{E}$ egyenlőséget $(\mathcal{A}^* =)\mathcal{A} = \mathcal{A}^{-1}$ biztosítja. A megfordítás hamis, vegyünk például a síkon két nem párhuzamos, különböző hosszúságú vektort, és legyen $\mathcal{A}$ az a transzformáció, amely ezeket egymásba viszi. A „helyes" megfordítás a következő (beleértve az eredeti állítást is): egy $\mathcal{A}$ transzformációra a három feltétel közül bármelyik kettőből következik a harmadik: (i) $\mathcal{A}$ szimmetrikus; (ii) $\mathcal{A}$ ortogonális; (iii) $\mathcal{A}^2 = \mathcal{E}$.

8.6.2 Szimmetrikus transzformációkra az állítás a 8.4.6 feladatból (vagy az ott látott gondolatmenet mintájára) adódik. Ortogonális transzformációkra is hasonlóan okoskodhatunk, közben használjuk fel azt is, hogy ekkor legfeljebb ± 1 lehetnek a sajátértékek.

8.6.3 S=ortonormált sajátbázis, O=a 8.6.4 Tételben előírt ortonormált bázis.

(a) $\mathcal{A}$ szimmetrikus és ortogonális,
S: az $\begin{pmatrix}1\\0\\0\\1\end{pmatrix}, \begin{pmatrix}0\\1\\1\\0\end{pmatrix}, \begin{pmatrix}1\\0\\0\\-1\end{pmatrix}, \begin{pmatrix}0\\1\\-1\\0\end{pmatrix}$ vektorok $1/\sqrt{2}$-szerese, a megfelelő diagonális mátrix főátlója: $1, 1, -1, -1$.

(b) $\mathcal{B}$ szimmetrikus,
S: a $\begin{pmatrix}-1\\1+\sqrt{2}\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\-1\\1+\sqrt{2}\end{pmatrix}, \begin{pmatrix}-1\\1-\sqrt{2}\\0\\0\end{pmatrix}, \begin{pmatrix}0\\0\\-1\\1-\sqrt{2}\end{pmatrix}$ vektorok skalárszorosai, a diagonális mátrix főátlója: $-\sqrt{2}, -\sqrt{2}, \sqrt{2}, \sqrt{2}$.

(c) $\mathcal{C}$ ortogonális,
O: az $\begin{pmatrix}1\\1\\1\\1\end{pmatrix}, \begin{pmatrix}1\\-1\\1\\-1\end{pmatrix}, \begin{pmatrix}1\\-1\\-1\\1\end{pmatrix}, \begin{pmatrix}1\\1\\-1\\-1\end{pmatrix}$ vektorok $1/2$-szerese, a megfelelő mátrix: $\begin{pmatrix}1&0&0&0\\0&-1&0&0\\0&0&0&-1\\0&0&1&0\end{pmatrix}$ (a jobb alsó 2×2-es blokk a 90 fokos forgatásnak felel meg).

(d) $\mathcal{D}$ szimmetrikus,
S: a $\mathcal{C}$-beli, a megfelelő diagonális mátrix főátlója: $4, 0, 0, 0$.

(e) $\mathcal{F}$ ortogonális, O: az $\begin{pmatrix}1\\0\\1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\-1\end{pmatrix}, \begin{pmatrix}1\\0\\-1\\0\end{pmatrix}, \begin{pmatrix}0\\1\\0\\1\end{pmatrix}$ vektorok $1/\sqrt{2}$-szerese, a megfelelő mátrix ugyanaz, mint $\mathcal{C}$-nél.

8.6.4 Nincs. A feltételből ugyanis ($\mathbf{x} \neq \mathbf{0}$-ra) $0 \leq (\mathcal{A}\mathbf{x})\cdot(\mathcal{A}\mathbf{x}) = \mathbf{x}\cdot(\mathcal{A}^*\mathcal{A}\mathbf{x}) = = \mathbf{x}\cdot(-\mathbf{x}) < 0$ következne.

8.6.5 Igaz: (a), (d).

8.6.6 A feltételekből $(\mathcal{A}^*\mathcal{A})^k = \mathcal{E}$ adódik. Így $\mathcal{A}^*\mathcal{A}$ sajátértékei egységnyi abszolút értékűek. Emellett $\mathcal{A}^*\mathcal{A}$ (mindig) szimmetrikus és a sajátértékei nemnegatív valósak, tehát most minden sajátérték 1, ezért csak $\mathcal{A}^*\mathcal{A} = \mathcal{E}$ lehetséges.
Az állítás szimmetrikus analogonja hamis, legyen pl. $\mathcal{A}$ egy 90 fokos forgatás a síkon és $k = 4$.

8.6.7 A feltételből $\mathcal{A} = (\mathcal{A}^m)^* = \mathcal{A}^{m^2}$, és így $\operatorname{Ker}\mathcal{A} = \mathbf{0}$ miatt $\mathcal{A}^{m^2-1} = \mathcal{E}$. Innen $(\mathcal{A}^{m-1})^* = \mathcal{A}^{m^2-m} = (\mathcal{A}^{m-1})^{-1}$. Ezután alkalmazzuk az előző feladatot.

8.6.8 A csak akkor rész igazolásához állítsuk elő az lnko-t $1 = (k,t) = kq - tr$ alakban $(q, r > 0)$.

8.6.9 A komplex esethez hasonlóan kell okoskodni.

8.6.10 Szimmetrikus transzformációk: a síkon kettő, a térben három (páronként) merőleges irányban (esetleg különböző mértékben) „nyújtunk" (vagy összenyomunk), emellett esetleg még tükrözünk is (egy vagy több) olyan egyenesre (a síkon), illetve síkra (a térben), amely valamelyik irányra merőleges.
Ortogonális transzformációk a síkon: (az origón átmenő) tengelyre történő tükrözések és (az origó körüli tetszőleges szögű) elforgatások.
Ortogonális transzformációk a térben: (az origón átmenő) síkra történő tükrözések, (az origón átmenő) tengely körüli (tetszőleges szögű) elforgatások, esetleg a tengelyre merőleges síkra történő tükrözéssel kombinálva (ebbe beletartozik az origóra történő tükrözés is).

8.6.11 Kövessük a 8.6.4 Tétel bizonyításának a gondolatmenetét.
A megfordítás hamis, pl. a sík önmaga már eleve a kívánt tulajdonságú (al)tér, ugyanakkor a szokásos ortonormált bázisban a $\begin{pmatrix}0 & 1\\0 & 0\end{pmatrix}$ mátrixszal jellemzett $\mathcal{A}$ transzformációnál az adjungált nem írható fel az $\mathcal{A}$ polinomjaként.

8.6.12 Írjuk fel a mátrixokat egy ortonormált bázis szerint, ekkor elég az ekvivalenciát a mátrixokra kimutatni. Ha ezeket a (valós elemű) mátrixokat komplex eleműeknek tekintjük, akkor a 8.5.3 Tétel mátrixos változata igazolja az ekvivalenciát. Ezután már csak azt kell megmutatni, hogy ha egy valós elemű A mátrixra az A^T transzponált előáll az A komplex együtthatós polinomjaként, akkor valós együtthatós polinomjaként is előáll. Ez onnan következik, hogy a kívánt előállítás egy lineáris egyenletrendszert jelent, ahol az ismeretlenek a keresett polinom együtthatói, az egyenletrendszer együtthatói az A hatványainak elemei, a jobb oldali konstansok pedig A^T elemei. Mivel az egyenletrendszer együtthatói (és a jobb oldali konstansok) valósak, ezért ha van komplex megoldás, akkor (pl. a Gauss-kiküszöbölés alapján) valós megoldásnak is kell lennie.

9. Kombinatorikai alkalmazások

9.1.

9.1.1 A minimális kérdésszám: (a) 20; (b) 2; (c) 1.

9.1.2 Igazoljuk az állítást először teljes indukcióval pozitív egész súlyokra, ezután tetszőleges egészekre, majd racionálisokra. Az igazi nehézséget a valós számokra történő áttérés jelenti. Erre a megoldásoknál négy bizonyítást is közlünk, most ezekhez adunk útmutatást.

Első bizonyítás: Tekintsük a 13 valós szám által generált alteret a valós számoknak a racionálisok feletti szokásos vektorterében, és térjünk át (akármilyen bázis szerinti) koordinátákra.

Második bizonyítás: A feltételt felírhatjuk egy ($0, \pm 1$ együtthatós) homogén lineáris egyenletrendszerként. Érdemes az egyik ismeretlent 0-nak rögzíteni, ekkor azt kell belátni, hogy az egyenletrendszernek csak triviális megoldása létezik. Mutassuk meg, hogy ha a racionális számok körében csak triviális megoldás létezik, akkor a valós számok körében is ugyanez a helyzet.

Harmadik bizonyítás: Az előző egyenletrendszert nézzük a modulo 2 test felett, majd innen térjünk át a valós számokra.

Negyedik bizonyítás: Lássuk be és használjuk fel, hogy a valós számok jól közelíthetők racionálisakkal: tetszőleges véges sok valós számhoz és előre megadott ε-hoz találhatók olyan azonos nevezőjű törtek, hogy mindegyik valós számnak a megfelelő törttől való eltérése legfeljebb a nevező reciprokának az ε-szorosa.

9.1.3 Nem marad igaz, ellenpélda: 12 darab 1-es és 1 darab 11-es (sok más ellenpélda is adható).

9.1.4

(a) (i): $\lceil \log_2 m \rceil$, ahol $\lceil x \rceil$ az x szám felső egész részét (azaz az x-nél nem kisebb egész számok minimumát) jelöli. (ii): $m-1$ (ha $m \geq 2$).

(b) (i): $\lceil \log_k m \rceil$. (ii): $\lceil (m-1)/(k-1) \rceil$ (ha $m \geq k$).

(c) Tekintsük csak az (a)-beli probléma megfelelőjét (azaz amikor $k=2$), a (b)-beli általános kérdés (azaz amikor k tetszőleges) hasonlóan tárgyalható. Az (i)-re adott válasz $p < m$ esetén változik: ekkor $\lceil \log_2 m \rceil$ helyett $\lceil \log_2 p \rceil$ lesz a keresett minimum. A (ii)-nél is változás van, ha p nem túl nagy m-hez képest: mivel $\lceil \log_2 p \rceil$ unalmas vektor mindenképpen elegendő, ezért $p \leq 2^{m-2}$ esetén $m-1$-nél kisebb lesz a keresett minimum. Ha viszont p elegendően nagy m-hez képest, akkor ugyanúgy $m-1$ a minimum, mint a valós (vagy bármilyen végtelen) test felett.

9.1.5 (a) 5. (b) 31.

9.1.6

(a) Mindkét kérdésre igenlő a válasz. A kontinuum sok részhalmaz konstrukciójánál segít a lineáris algebra.

(b) Megszámlálhatóan végtelen sok részhalmaz megadható, de annál több nem.

9.1.7

(a) Igen, pl. megfelel egy egységnyi oldalú szabályos tetraéder négy csúcsa.

(b) A síkon nincs 4 ilyen pont. Az indirekt bizonyításhoz legyen az egyik pont az origó, az ebből a másik három pontba mutató vektor pedig $\mathbf{a} = (a_1, a_2), \mathbf{b} = (b_1, b_2)$ és $\mathbf{c} = (c_1, c_2)$. A távolságokat a skalárszorzat segítségével felírva, lássuk be, hogy az $\mathbf{a}\cdot\mathbf{a}, \mathbf{b}\cdot\mathbf{b}, \mathbf{c}\cdot\mathbf{c}, 2\mathbf{a}\cdot\mathbf{b}, 2\mathbf{a}\cdot\mathbf{c}$ és $2\mathbf{b}\cdot\mathbf{c}$ skalárszorzatok mindegyike $8k+1$ alakú egész szám. Mutassuk meg, hogy

$$M = \begin{pmatrix} \mathbf{a}\cdot\mathbf{a} & \mathbf{a}\cdot\mathbf{b} & \mathbf{a}\cdot\mathbf{c} \\ \mathbf{b}\cdot\mathbf{a} & \mathbf{b}\cdot\mathbf{b} & \mathbf{b}\cdot\mathbf{c} \\ \mathbf{c}\cdot\mathbf{a} & \mathbf{c}\cdot\mathbf{b} & \mathbf{c}\cdot\mathbf{c} \end{pmatrix} = \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \\ c_1 & c_2 \end{pmatrix} \begin{pmatrix} a_1 & b_1 & c_1 \\ a_2 & b_2 & c_2 \end{pmatrix}.$$

Így az M rangja az 5.7.12a feladat alapján legfeljebb 2, tehát $\det M = 0$. Ezért $\det(2M) = 8 \det M = 0$. Ugyanakkor

$$\det(2M) \equiv \begin{vmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{vmatrix} = 4 \pmod 8,$$

ami ellentmondás.

9.1.8

(a) Nyilván $c = f(1)$. Az állítást lássuk be először a pozitív egészekre, majd a pozitív racionálisokra, a 0-ra és végül a negatív racionálisokra.

(b) Mutassuk meg, hogy f ekkor mindenütt folytonos, majd támaszkodjunk az a)-beli eredményre.

(c) Ekkor a 0 körül is van olyan intervallum, amelyben f korlátos, és innen az is következik, hogy f a 0-ban folytonos.

(d) Ha a valós számokat mint a racionális test feletti V vektorteret tekintjük, akkor a feltétel azt jelenti, hogy f lineáris transzformáció V-n. A bázis fogalmának (és létezésének) végtelen dimenziós térre történő kiterjesztésével (Hamel-bázis) a lineáris transzformációk továbbra is a báziselemek képeivel jellemezhetők, azaz egy Hamel-bázison f-et tetszőlegesen előírhatjuk, ez mindig egyértelműen meghatároz egy minden valós számon értelmezett megfelelő f függvényt. (Ezeket az f-eket természetesen „nem látjuk".)

9.1.9

(a) Nem. Ha $r_1 = a_1/b_1$ és $r_2 = a_2/b_2$ a két részhalmaz egy-egy eleme, akkor az összeadási zártság miatt $a_1a_2 = a_2b_1r_1 = a_1b_2r_2$ mindkét részhalmaznak eleme.

(b) Igen. A valós számokat $\mathbf{Q}$ feletti vektortérnek tekintve, írjuk fel a pozitív számokat egy (végtelen) bázis segítségével. Az egyik, illetve másik részhalmazba azok a számok kerüljenek, amelyek felírásában egy rögzített báziselem együtthatója nemnegatív, illetve negatív. (Az is megfelel, hogy az együtthatók összege legyen nemnegatív, illetve negatív.)

9.1.10

(a1) Nem. Lássuk be, hogy $\mathbf{Q}$ esetén két periodikus függvény összege is periodikus, mert létezik közös periódusuk.

(a2) Igen. A valós számoknak $\mathbf{Q}$ feletti vektorterében 1 és $\sqrt{2}$ lineárisan függetlenek, tehát kiegészíthetők a vektortér bázisává. Így minden s valós szám egyértelműen felírható $s = r_1 + r_2\sqrt{2} + t$ alakban, ahol r_1 és r_2 racionális számok és t a többi báziselem által generált altér eleme. Ekkor a $h_1(s) = r_1$ és $h_2(s) = r_2\sqrt{2} + t$ függvények periodikusak $\sqrt{2}$, illetve 1 periódussal, továbbá $s = h_1(s) + h_2(s)$.

(b1) Nem. Bizonyítsunk a fokszám szerinti indukcióval. Használjuk ki, hogy ha az $f(x)$ polinom k darab periodikus függvény összege, akkor az eggyel alacsonyabb fokú $g(x) = f(x) - f(x-1)$ polinom $k-1$ darab periodikus függvény összege.

(b2) Igen. Az identitásfüggvénynél látott konstrukció általánosításaként $\mathbf{R}$-ben mint a $\mathbf{Q}$ feletti (végtelen dimenziós) vektortérben a $b_1, \ldots, b_{n+1}$ lineárian független elemeket egészítsük ki a tér bázisává. Így minden

s valós szám egyértelműen előáll $s = \sum_{i=1}^{n+1} r_i b_i + t$ alakban, ahol $r_i \in \mathbf{Q}$ és t a többi báziselem által generált altér eleme. Ezt k-adik hatványra emelve s^k olyan k-tényezős szorzatok összege, amelyekben minden tényező az $n+1$ darab $r_i b_i$ valamelyike vagy t. Ha $k \le n$, akkor valamelyik $r_i b_i$ biztosan kimarad. Írjuk fel most ennek alapján az adott n-edfokú $f(s)$ polinomot, és legyen $h_1(s)$ azoknak a tagoknak az összege, amelyekben nem szerepel $r_1 b_1$, a maradékból legyen $h_2(s)$ azoknak a tagoknak az összege, amelyekben nem szerepel $r_2 b_2$ stb. A legvégén maradt tagokban nem szerepel $r_{n+1} b_{n+1}$, ezek összege legyen $h_{n+1}(s)$. Ekkor $h_i(s)$ periodikus b_i periódussal és $f(s) = \sum_{i=1}^{n+1} h_i(s)$.

9.2.

9.2.1 (a) $(2^{1000} - 1)/3$. (b) $\big((1+\sqrt{2})^{999} + (1-\sqrt{2})^{999}\big)/2$.

9.2.2 (a) 4443. (b) 3. (c) 3.
Útmutatás (c)-hez: az

$$f = x^4 - x^3 + x^2 - x + 1 = \big(x^{10} - 1\big)\big/\big((x^5 - 1)(x + 1)\big)$$

polinom (komplex) gyökei különböző 10-edik egységgyökök (éspedig éppen a primitív 10-edik egységgyökök, azaz f a 10-edik körosztási polinom), ezért a sorozat (bármilyen kezdőértékek mellett) mindenképpen periodikus 10 hosszúságú periódussal.

9.2.3 A Fibonacci-számoknál látott mindhárom bizonyítás megfelelő módosítása alkalmas az állítás igazolására, ehhez adunk némi útmutatást.
Első bizonyítás: Használjuk ki, hogy λ_i az f első $s_i - 1$ deriváltjának is gyöke.
Második bizonyítás: A diagonális mátrix helyett a Jordan-alakot lehet felhasználni.
Harmadik bizonyítás: a parciális törtekre bontásnál a nevezőkben a megfelelő gyöktényezők magasabb hatványai is megjelennek, ezek sorbafejtése a mértani sor (első vagy magasabb) deriváltjainak segítségével történhet.

9.2.4 Használjuk fel az előző feladatot.

9.2.5 A β_n sorozatot egy alkalmas konstanssal eltolva a zavart okozó 2-es tag eltűnik, és egy Fibonacci-típusú sorozatot kapunk.
Válasz: $\beta_n = \varphi_{n+3} - 2$ (ahol φ_n az n-edik Fibonacci-szám).

9.2.6 A φ_n képletében szereplő másik tag 0-hoz tart.

9.2.7

(a) φ_{n+1}.

(b) Nyilván csak $n = 2k$ esetén létezik ilyen kirakás, és a lehetőségek száma ekkor $\big((3+\sqrt{3})(2+\sqrt{3})^k + (3-\sqrt{3})(2-\sqrt{3})^k\big)/6$.
Útmutatás: Jelöljük T_{2k}-val a $3 \times (2k)$-as téglalapot és H_{2k-1}-gyel azt a $3 \times (2k-1)$-es téglalapot, amelynek hiányzik az egyik sarka. Legyen μ_{2k} és ϑ_{2k-1} a T_{2k} és H_{2k-1} alakzatok 2×1-es dominókkal való kirakásainak a száma. Ekkor $\mu_{2k} = 2\vartheta_{2k-1} + \mu_{2k-2}$ és $\vartheta_{2k-1} = \mu_{2k-2} + \vartheta_{2k-3}$. A második összefüggés többszöri alkalmazásával $\vartheta_{2k-1} = \mu_{2k-2} + \mu_{2k-4} + \ldots + \mu_2 + 1$ adódik. Ezt az elsőbe beírva, majd az így a μ_{2k}-ra és μ_{2k-2}-re kapott egyenlőségeket egymásból kivonva a $\mu_{2k} = 4\mu_{2k-2} - \mu_{2k-4}$ rekurziót nyerjük.

(c) A $\psi_n = \psi_{n-1} + \psi_{n-3}$ rekurziónak megfelelő $f = x^3 - x^2 - 1$ polinom (komplex) gyökei legyenek ρ_1, ρ_2, ρ_3. A szokásos függvényvizsgálattal könnyen adódik, hogy f-nek egyetlen valós gyöke van és ez 1-nél nagyobb: $\rho_1 > 1$. Ekkor $\rho_3 = \overline{\rho_2}$, továbbá mivel a gyökök szorzata 1, ezért $|\rho_2| = |\rho_3| < 1$. A ψ_n-re adódó $\psi_n = \gamma_1\rho_1^n + \gamma_2\rho_2^n + \gamma_3\rho_3^n$ képletben emiatt az utolsó két tag 0-hoz tart, ha n tart a végtelenhez. Az állítás ezután $1{,}46 < \rho_1 < 1{,}47$-ből következik.

9.2.8 φ_{n+2}. Útmutatás: a rekurziót aszerint írjuk fel, hogy a legnagyobb elem hiányzik-e vagy szerepel-e a részhalmazban. (Vö. a 9.2.10h feladattal.)

9.2.9 Használjuk a mohó algoritmust, azaz összeadandónak minden lépésben rendre a rendelkezésre álló legnagyobb Fibonacci-számot vegyük.
A feladat állítása egyébként a Fibonacci-számok helyett bármely olyan, pozitív egészekből álló végtelen számsorozatra is igaz, amelynek az 1 eleme, és a sorozat minden eleme az előző elemnek legfeljebb a duplája.

9.2.10

(a) Teljes indukció n szerint.

(b) Az előző azonosságból következik alkalmas helyettesítéssel.

(c) Teljes indukció vagy a $\varphi_{k+1} - \varphi_k = \varphi_{k-1}$ egyenlőségek összegzése $k = 1, 2, \ldots, n+1$-re.

(d) Teljes indukció vagy a $(k-2)\varphi_{k+1} - (k-2)\varphi_k = (k-2)\varphi_{k-1}$ egyenlőségek összegzése $k = 3, 4, \ldots, n+1$-re és némi átrendezés.

(e) Teljes indukció vagy a $\varphi_k^2 = \varphi_k\varphi_{k+1} - \varphi_k\varphi_{k-1}$ egyenlőségek összegzése $k = 1, 2, \ldots, n$-re.

(f) Az (a)-ból nyerhető $\varphi_{2n-1} = \varphi_{n-2}\varphi_n + \varphi_{n-1}\varphi_{n+1}$ egyenlőséget (b)-vel összevetve átrendezés után $\varphi_n^2 - \varphi_{n-1}\varphi_{n+1} = -(\varphi_{n-1}^2 - \varphi_{n-2}\varphi_n)$ adódik. Ezután ugyanezt az összefüggést alkalmazzuk n helyett rendre az $n-1, n-2, \ldots$ számokkal.

(g) Az (a) azonosságot alkalmazzuk a $\varphi_{n+2n}, \varphi_{n+n}$ és $\varphi_{(n+1)+n}$ számok felbontásához, így φ_{3n}-et kifejezhetjük φ_n és φ_{n-1} segítségével. Használjuk fel még az (f)-beli azonosságot is.

(h) Teljes indukció vagy használjuk fel a 9.2.8 feladatot.

(i) A $\varphi_t = \varphi_{t-1} + \varphi_{t-2}$ azonosság ismételt alkalmazásával bármely k-ra a $\varphi_{2n} = \sum_{j=0}^{k} \binom{k}{j} \varphi_{2n-2k+j}$ összefüggést nyerjük. Ennek $k = n$ speciális esete a bizonyítandó állítás.

9.2.11 A másodszomszédok is relatív prímek. A harmadszomszédok közül a 3-mal osztható indexűek legnagyobb közös osztója 2, a többiek relatív prímek. (Vö. a 9.2.13 feladattal.)

9.2.12 Jelöljük φ_k-nak m-mel való osztási maradékát r_k-val. Az (r_k, r_{k+1}) párok csak m^2 különböző értéket vehetnek fel, ezért lesz olyan $t > s$, amelyre $(r_t, r_{t+1}) = (r_s, r_{s+1})$. Lássuk be, hogy ekkor bármely k-ra $(r_k, r_{k+1}) = (r_{k+t-s}, r_{k+t-s+1})$, azaz az r_n maradékok periodikusan ismétlődnek ($t-s$ periódus szerint). Mivel $r_0 = 0$, ezért bármely j-re $r_{j(t-s)} = 0$, azaz $m \mid \varphi_{j(t-s)}$.

9.2.13 Útmutatás: Használjuk fel a 9.2.10a feladatot. A $k \mid n \Rightarrow \varphi_k \mid \varphi_n$ állítást az n/k szerinti teljes indukcióval igazolhatjuk. A megfordításhoz és a legnagyobb közös osztóra vonatkozó állításhoz lássuk be, hogy ha $a = bq + r$, akkor $(\varphi_a, \varphi_b) = (\varphi_b, \varphi_r)$.
Egy másik lehetőség: Mutassuk meg, hogy bármely m-re az m-mel osztható Fibonacci-számok indexei éppen a legkisebb ilyen tulajdonságú nem nulla Fibonacci-szám indexének a többszörösei.

9.2.14

(a) φ_{n+1}.

(b) $\big((1+\sqrt{2})^n - (1-\sqrt{2})^n\big)/(2\sqrt{2})$, ami az $\alpha_{i+1} = 2\alpha_i + \alpha_{i-1}, \alpha_0 = 0$, $\alpha_1 = 1$ rekurzió megoldása (ezeket a számokat szokás Lucas-sorozatnak nevezni).

9.2.15 Legyen $\rho = (1+\sqrt{5})/2$, ekkor $\varphi_n = \big(\rho^n - (-1/\rho)^n\big)/\sqrt{5}$. A szóban forgó sor első m tagjának az összegét „teleszkopikus” összeggé alakíthatjuk át:

$$\sqrt{5}\sum_{k=1}^{m} \frac{\rho^{2^k}}{\rho^{2^{k+1}}-1} = \sqrt{5}\sum_{k=1}^{m}\Big(\frac{1}{\rho^{2^k}-1} - \frac{1}{\rho^{2^{k+1}}-1}\Big) = \sqrt{5}\Big(\frac{1}{\rho^2-1} - \frac{1}{\rho^{2^{m+1}}-1}\Big).$$

Mivel a második tag 0-hoz tart, így a keresett sorösszeg $\sqrt{5}/(\rho^2-1) = (5-\sqrt{5})/2$.

9.2.16 Eredmény: $\binom{2n-2}{n-1}/n$. A megoldásoknál ezt három különböző módon vezetjük le, most ezekhez adunk útmutatást.
Első megoldás: $n-1$ darab (kéttényezős) szorzást kell végrehajtani. Minden egyes szorzásnál jelöljük meg a nyitó zárójelet $+1$-gyel és a szorzat első tényezőjét -1-gyel; ha ez az első tényező maga is egy többtényezős szorzat, akkor annak utolsó tényezőjét jelöljük meg a -1-gyel. Könnyen láthatóan ekkor az $a_1, a_2, \ldots, a_{n-1}$ tényezők mindegyike pontosan egyszer van -1-gyel megjelölve, továbbá bármely $k \leq n-1$-re a_k előtt legalább k nyitó zárójelnek (azaz $+1$-nek) kell szerepelnie. Ennek a megfordítása is igaz, minden ilyen ± 1-ekből álló sorozat egy szorzási útnak felel meg. Így $n-1$ darab $+1$-ből és $n-1$ darab -1-ből álló sorozatokat képezünk, amelyekben az elejétől számítva akárhány tag összege nemnegatív. Minden sorozat elejére még egy $+1$-et odaírva, olyan, most már n darab $+1$-ből és $n-1$ darab -1-ből álló sorozatokra fogalmaztuk át a problémát, amelyekben az elejétől számítva akárhány tag összege pozitív. Lássuk be, hogy a „rossz" sorozatok száma a -1-gyel kezdődő sorozatok számának a duplája.
Második megoldás: Az utoljára elvégzett szorzás az első k és a maradék $n-k$ tényezőből (valahogyan) elkészített szorzatokat szorozza össze, $k = 1, 2, \ldots, n-1$, így a feladatnak az $\alpha_n = \sum_{k=1}^{n-1} \alpha_k \alpha_{n-k}$, $\alpha_1 = 1$ rekurzió felel meg. Ebből az $A(z) = \sum_{n=1}^{\infty} \alpha_n z^n$ hatványsorra az $A^2(z) = A(z) - z$ egyenletet kapjuk.
Harmadik megoldás: Egyszerűbb rekurziót kapunk, ha az elemek egymás közötti cseréjét is figyelembe vesszük. A rekurziót megoldva, az így meghatározott β_n értékből nyilván $\alpha_n = \beta_n/n!$.

9.2.17 Az egyik oldalt rögzítsük, és aszerint csoportosítsuk az eseteket, hogy az ezen oldalt tartalmazó háromszög harmadik csúcsa hová esik. Az így kapott rekurzió lényegében azonos az előző feladat második megoldásában tárgyalt rekurzióval.
Eredmény: $\binom{2n-4}{n-2}/(n-1)$.

9.3.

9.3.1

(a) Pl. megfelelnek a p_i-k első és negyedik hatványai.

(b) A skatulyaelv szerint biztosan lesz három olyan c_j, amelyekben mindegyik p_i kitevőjének modulo 3 vett maradéka ugyanannyi. Ennek a három c_j-nek a szorzata köbszám.

(c) Az állítás a 9.3.1 Tételre adott bármelyik bizonyítás értelemszerű módosításával igazolható.

9.3.2 Okoskodjunk indirekt, ekkor a kis-Fermat-tétel felhasználásával kapjuk, hogy a

$$\prod_{i=1}^{k}\bigl(1-f_i^{p-1}(x_1,x_2,\ldots,x_t)\bigr)\equiv\prod_{j=1}^{t}(1-x_j^{p-1})\pmod p$$

kongruencia azonosság (azaz minden $x_1,\ldots,x_t$ esetén teljesül). Mutassuk meg, hogy a fokszámok összegére tett feltétel miatt ez nem lehetséges. Ha speciálisan mindegyik polinom elsőfokú, akkor (az F_p test felett) egy homogén lineáris egyenletrendszert kapunk, amelyben az ismeretlenek száma nagyobb az egyenletek számánál, tehát van nem triviális megoldás. A Chevalley-tétel tehát ennek a jól ismert eredménynek az általánosításaként is tekinthető.

9.3.3 A c_j számban a p_i prím kitevője legyen γ_{ij} $(1\le i\le k, 1\le j\le t)$. Az $f_i(x_1,\ldots,x_t)=\sum_{j=1}^{t}\gamma_{ij}x_j^2$ polinomokra és $p=3$-ra alkalmazzuk a Chevalley-tételt.

9.3.4 Itt $t\ge(q-1)k+1$ a megfelelő feltétel.

9.3.5

(a) Tekintsük a $c_1, c_1+c_2,\ldots,c_1+c_2+\ldots+c_n$ számok n-nel való osztási maradékait.

(b) Először azt igazoljuk, hogy ha az állítás igaz $n=r$-re és $n=s$-re, akkor teljesül $n=rs$-re is. A $2rs-1$ számból vegyünk tetszőleges $2r-1$-et, ekkor az r-re vonatkozó állítás szerint kiválaszthatunk r olyat, amelyek összege osztható r-rel. A maradék $2rs-1-r$ számból ismét vegyünk tetszőleges $2r-1$-et, ezek között is van r darab olyan, amelyek összege osztható r-rel. Lássuk be, hogy ily módon $2s-1$ darab olyan r-es csoport keletkezik, ahol minden csoport elemeinek az összege osztható r-rel. Alkalmazzuk ezután az s-re vonatkozó állítást ezen összegek r-edrészére.

Ennek alapján elég az $n=p=$ prím esettel foglalkozni. Legyen $f_1=\sum_{j=1}^{2p-1}c_jx_j^{p-1}$, $f_2=\sum_{j=1}^{2p-1}x_j^{p-1}$, és alkalmazzuk a Chevalley-tételt.

9.3.6

(a) A kínai maradéktétel szerint elegendő a problémát egy p^m prímhatvány modulusra megoldani. Ha $m>1$, akkor az $x_1=x_2=x_3=p^{\lceil m/2\rceil}$ választás megfelelő. Ha $m=1$, akkor (pl. a Chevalley-tétel alapján) az $x_1^2+x_2^2+x_3^2\equiv 0\pmod p$ kongruenciának van nem triviális megoldása. Itt feltehető $|x_i|\le p/2$, ezért $0<x_1^2+x_2^2+x_3^2<p^2$, tehát az $x_1^2+x_2^2+x_3^2$ összeg (amely a feltétel szerint p-vel osztható) p^2-tel már nem lehet osztható.

(b) Az (a)-beli eljárást kell egyetlen esetben finomítani: ha $m>1$ és páratlan, akkor legyen $x_i=p^{(m-1)/2}y_i$, és az y_i-kre alkalmazzuk az előbb $m=1$-re látott gondolatmenetet.

9.3.7 Képezzük a kérdéses N számnak minden lehetséges k-ra a (közelítő, valós) k-adik gyökét, és az ehhez legközelebbi n_k egész számra ellenőrizzük le, nem teljesül-e $n_k^k = N$. Mivel a szóba jöhető legkisebb hatványalap a 2, ezért $k \leq \log_2 N$, tehát ez valóban gyors algoritmus.

9.3.8

(a) Az egyes prímek egymástól függetlenül durván a számok felét selejtezik ki, tehát a garantáltan rossz számok aránya s darab prím esetén körülbelül $(2^s - 1)/2^s$ (azaz nagyjából minden 2^s-edik számot kell csak x-ként kipróbálni).

(b) Az a jó, ha d és e közel egyforma.

(c) $86519 = 241 \cdot 359$, $584189 = 613 \cdot 953$. Az $N = 86519 = x^2 - y^2$ keresésénél $x \geq \sqrt{86519}$, azaz x legkisebb szóba jöhető értéke 295. Az $y^2 = x^2 - N$ egyenlőséget modulo 8 vizsgálva a bal oldal lehetséges értéke $0, 1$ vagy 4, a jobb oldalé $0-7, 1-7$ vagy $4-7$, ezek egyetlen közös értéke $1 = 0-7$, azaz $8 \mid x^2$. Innen kapjuk, hogy az x szükségképpen osztható 4-gyel. Modulo 3 vizsgálva hasonlóan adódik, hogy $3 \mid x$. Így a legkisebb kipróbálandó érték az $x = 300$, ami rögtön meg is felel, hiszen $\sqrt{300^2 - 86519} = 59$ egész szám. Az $N = 584189$ esetében azt kapjuk, hogy x páratlan és 3-mal osztható, így a kipróbálandó számok az $x = 765, 771, \ldots$, itt $x = 783$-ra járunk szerencsével.

Megjegyzés: Mielőtt egy nagy szám felbontását megkíséreljük, mindenképpen célszerű egy gyors prímteszttel meggyőződni arról, hogy a szám valóban összetett. Azt se felejtsük el, hogy igazán gyors faktorizációs algoritmus nem ismeretes, nagy (pl. háromszázjegyű) számokra a feladatban jelzett faktorizációs módszer is reménytelenül lassú.

9.4.

9.4.1

(a) 2^{k-1}.
Az első $k-1$ elem mindegyikénél szabadon döntünk, hogy bevesszük-e az adott elemet a részhalmazba vagy sem, és ekkor az utolsó elemnél egyértelműen adódik, hogy bevegyük vagy sem. Egy másik lehetőség: a keresett szám $\sum_{i=0}^{\lfloor k/2 \rfloor} \binom{k}{2i} = \big((1+1)^k + (1-1)^k\big)/2$.

(b) $\big(2^k + 2\cos(k\pi/3)\big)/3$. Ezt átírhatjuk más alakba is aszerint, hogy k milyen maradékot ad 6-tal osztva: $(2^k + 2)/3$, ha $k \equiv 0 \pmod 6$; $(2^k + 1)/3$, ha $k \equiv \pm 1 \pmod 6$; $(2^k - 2)/3$, ha $k \equiv 3 \pmod 6$; és végül $(2^k - 1)/3$, ha $k \equiv \pm 2 \pmod 6$.

Útmutatás: Jelölje α_k, β_k, illetve γ_k egy k elemű halmaz azon részhalmazainak a számát, amelyek elemszáma 0, 1, illetve 2 maradékot ad 3-mal osztva. Célunk α_k meghatározása. Nyilván $\alpha_i + \beta_i + \gamma_i = 2^i$. Ennek felhasználásával $\alpha_k = 2^{k-1} - \beta_{k-1}$, $\beta_{k-1} = 2^{k-2} - \gamma_{k-2}$, valamint $\gamma_{k-2} = 2^{k-3} - \alpha_{k-3}$, ahonnan az $\alpha_k + \alpha_{k-3} = 3 \cdot 2^{k-3}$, majd az $\alpha_k = \alpha_{k-6} + 21 \cdot 2^{k-6}$ rekurzió adódik. Ezt tovább bontva az $\alpha_k = = 21 \cdot 2^{k-6} + 21 \cdot 2^{k-12} + \ldots$ képletet nyerjük, amely az utolsó tagjától eltekintve egy 2^6 hányadosú mértani sor összege.

Másik lehetőségként az

$$\alpha_k = \sum_{i=0}^{\lfloor k/3 \rfloor} \binom{k}{3i} = \big((1+1)^k + (1+\omega)^k + (1+w^2)^k\big)/3$$

összefüggéssel dolgozhatunk, ahol ω egy harmadik primitív komplex egységgyök.

9.4.2
(a) H és H' egymás komplementerei.
(b) H és H' szimmetrikus differenciáját kell képezni.

9.4.3 Indirekt okoskodva tegyük fel, hogy létezik egy $\delta_1\mathbf{h}_1 + \ldots + \delta_n\mathbf{h}_n = \mathbf{0}$ racionális együtthatós nem triviális lineáris kombináció. Az együtthatók nevezőinek legkisebb közös többszörösével beszorozva, majd a kapott egész együtthatók legnagyobb közös osztójával végigosztva elérhetjük, hogy a δ_j-k relatív prím egész számok legyenek. Mindkét oldalt skalárisan megszorozva $\mathbf{h}_j$-vel, most is $\delta_1(\mathbf{h}_1 \cdot \mathbf{h}_j) + \ldots + \delta_j(\mathbf{h}_j \cdot \mathbf{h}_j) + + \ldots + \delta_n(\mathbf{h}_n \cdot \mathbf{h}_j) = 0$ adódik. Mivel $|H_j|$ páratlan, de minden $t \neq j$-re $|H_t \cap H_j|$ páros, ezért itt minden $\mathbf{h}_t \cdot \mathbf{h}_j$ skalárszorzat páros, kivéve $\mathbf{h}_j \cdot \mathbf{h}_j$-t, ami páratlan. Innen azonnal kapjuk, hogy δ_j szükségképpen páros. Mivel ez tetszőleges j-re teljesül, ezért valamennyi δ_j páros, ami ellentmond annak, hogy a δ_j számok relatív prímek voltak.

9.4.4
(a) $\beta_{ij} = |H_i \cap H_j|$ modulo 2 maradéka.
(b) Páratlanváros: Ekkor a $B = A^T A$ szorzat az $n \times n$-es egységmátrix, így az 5.7.12a feladat alapján $n = r(B) \leq r(A) \leq k$.
Párosváros: Most B az $n \times n$-es nullmátrix, ezért az 5.7.12b feladat szerint $k \geq r(A) + r(A^T) = 2r(A)$, azaz $r(A) \leq \lfloor k/2 \rfloor$. Ez azt jelenti, hogy A oszlopainak száma $n \leq 2^{r(A)} \leq 2^{\lfloor k/2 \rfloor}$.

9.4.5

(a) Az egyelemű részhalmazok mindig jók. Emellett $k = 4$-re (vagy bármely páros k-ra) megfelelnek az egyelemű részhalmazok komplementerei is. A többi k-ra a kétféle eljárás kombinációjával kapjuk a kívánt eredményt.

(b) Az (a) részben jelzett kombináció ezt is biztosítja.

(c) A felső becslés nagyjából k tetszőleges részhalmaz összes lehetséges kiválasztásának a száma. Az alsó becsléshez a legkönnyebben úgy jutunk el, ha a 9.4.4 feladatban látott módszert alkalmazzuk. Az egyszerűség kedvéért legyen k páros, $k = 2t$. Ha C egy tetszőleges $t \times t$-es szimmetrikus 0–1 mátrix, E_t pedig a $t \times t$-es egységmátrix, akkor a $k \times k$-as $A = \begin{pmatrix} C + E_t & C \\ C & C + E_t \end{pmatrix}$ mátrixra $B = A^T A$ a $k \times k$-as egységmátrix, tehát A egy alkalmas H_j halmazrendszer illeszkedési mátrixa. Az ilyen A-k (azaz C-k) száma $2^{k(k+2)/8}$. A $k!$-sal az oszlopcserékkel egymásba vihető halmazrendszerek azonossága miatt kell leosztani. (Ha az izomorf halmazrendszerektől is el akarunk tekinteni, tehát azoktól, amelyek egymásból a városlakók valamilyen permutációjával nyerhetők, akkor ez a sorcseréknek felel meg, és ekkor még egyszer le kell osztani $k!$-sal. Azonban még így is igen nagy számot kapunk, pl. elég nagy k-ra alulról becsülhetjük $2^{k^2/9}$-cel.) Mindez azt mutatja, hogy Páratlanvárosban nagyon sok különböző módon alapíthatunk k megfelelő egyesületet.

9.4.6 Eredmény: k, ha k páratlan és $k - 1$, ha k páros.
Útmutatás: páratlan k-ra a $k - 1$ elemű részhalmazok, páros k-ra pedig például az x_1-et tartalmazó kételemű részhalmazok megfelelnek. Annak igazolására, hogy ennél több részhalmaz már nem létezik, a Páratlanváros-tétel eredeti vagy a 9.4.4 feladatban jelzett bizonyítása adaptálható. Páros k esetén azt lehet kihasználni, hogy az illeszkedési mátrix (F_2 feletti) rangja legfeljebb $k - 1$, hiszen a sorok összege 0.

9.4.7

(a) A Páratlanváros-tétel bármelyik bizonyítása átvihető (értelemszerűen az F_2 test helyett F_3-mal kell dolgozni). Válasz: k.

(b) A válasz most is k, azonban csak a 9.4.3 feladatban ajánlott bizonyítás működik.

(c) Mivel $|H_t \cap H_j|$ osztható 6-tal, ezért $|H_t \cap H_j|$ osztható 2-vel és 3-mal is, ugyanakkor $|H_j|$ nem osztható 6-tal, tehát $|H_j|$ a 2 és a 3 közül legalább az egyikkel nem osztható. Így $2k + 1$ darab Hatfalus egyesület között vagy lenne $k + 1$ darab Páratlanvárosos, vagy pedig lenne $k + 1$ darab Hármashatáros, és mindkettő lehetetlen.

Megjegyzés: Általánosan a következő problémáról van szó. Legyen s rögzített pozitív egész. Maximálisan hány olyan H_j részhalmaza lehet egy k elemű X halmaznak, amelyekre $s \not| |H_j|$, de $t \neq j$ esetén $s \,\big|\, |H_t \cap H_j|$? Mindig meg lehet adni k ilyen részhalmazt; az egyeleműeket. A Páratlanváros-tételben láttuk, hogy $s = 2$ esetén ez a maximum. Ugyanígy elintézhető minden olyan eset, amikor s prímszám. Az állítás akkor is igaz marad, ha s egy prímszám hatványa (a bizonyítást ekkor a 9.4.3 feladat ajánlása szerint lehet elvégezni). A többi s-re a probléma *megoldatlan*; csak annyi adódik, hogy a maximum legfeljebb $\omega(s) \cdot k$, ahol $\omega(s)$ az s különböző prímosztóinak a száma. Ezt a felső becslést eddig csak igen minimális mértékben sikerült javítani, pl. $s = 6$-ra $n \leq 2k$ helyett csak a hajszálnyival jobb $n \leq 2k - 2\log_2 k$ az ismert legjobb eredmény. Ugyanakkor egyetlen s-re sem találtak k-nál több megfelelő részhalmazt.

9.4.8 (a) k. (b) $k - 1$.

9.4.9 Válasz: k.
A Páratlanváros-tétel eredeti bizonyítását kövessük. A K_j halmazoknak megfelelő $\mathbf{k}_j$ vektorok függetlenségét úgy láthatjuk be, ha a $\delta_1\mathbf{k}_1 + \ldots + {} + \delta_n\mathbf{k}_n = \mathbf{0}$ lineáris kombináció mindkét oldalát skalárisan megszorozzuk rendre a P_t halmazoknak megfelelő $\mathbf{p}_t$ vektorokkal.

9.4.10 Válasz: k.
Útmutatás a felső becsléshez: lássuk be, hogy a megfelelő vektorok a valós test felett lineárisan függetlenek.

9.4.11 Válasz: 1 (és ennek minden városlakó tagja).
Az előző feladatnál használt lineáris algebrai gondolatmenethez hasonlóan okoskodhatunk.

9.4.12 $\sum_{i=0}^{m} \binom{k}{i}$.

9.4.13 (b) Válasz: p^2, azaz az altér maximálisan 2-dimenziós lehet.
Először példát mutatunk ilyen altérre. Legyen $0 < r < p$ egy kvadratikus nemmaradék modulo p, ekkor megfelel T^{p-r+1}-ben az $U = \left\langle \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 1 \end{pmatrix} \right\rangle$ altér. (Megjegyezzük, hogy már T^3-ban is mindig található a kívánt tulajdonságú altér, sőt ha $p \equiv 3 \pmod 4$, akkor maga a T^2 vektortér is megfelel.)
Most megmutatjuk, hogy egy (legalább) háromdimenziós altérben mindig található önmagára merőleges nem nulla vektor. Az ortogonalizációs eljárással előállíthatunk $\mathbf{b}_1, \mathbf{b}_2, \mathbf{b}_3$ páronként merőleges vektorokat, legyen

$\mathbf{b}_i \cdot \mathbf{b}_i = \beta_i, \quad i = 1, 2, 3$. Egy $\mathbf{v} = \sum_{i=1}^{3} \gamma_i \mathbf{b}_i$ vektor akkor és csak akkor merőleges önmagára, ha

$$0 = \mathbf{v} \cdot \mathbf{v} = (\sum_{i=1}^{3} \gamma_i \mathbf{b}_i) \cdot (\sum_{i=1}^{3} \gamma_i \mathbf{b}_i) = \sum_{i=1}^{3} \gamma_i^2 \beta_i$$

teljesül. A γ_i-ket ismeretleneknek tekintve ennek az egyenletnek pl. a Chevalley-tétel (9.3.2 feladat) szerint van nem triviális megoldása.

9.4.14

(a) Ha $p \equiv 3 \pmod 4$, akkor $k \geq 3$ esetén, egyébként $k \geq 2$-re. Ugyanis a $z_1^2 + z_2^2 \equiv 0 \pmod p$ kongruenciának pontosan $p \not\equiv 3 \pmod 4$ mellett van nem triviális megoldása, a $z_1^2 + z_2^2 + z_3^2 \equiv 0 \pmod p$ kongruencia pedig már minden p-re nem triviálisan megoldható.

(b) Ha csak a nullvektor merőleges önmagára, azaz ha $k = 1$ és p tetszőleges vagy $k = 2$ és $p \equiv 3 \pmod 4$, akkor ez triviálisan altér (dimenziója 0). Ettől eltekintve csak $p = 2$-re kapunk alteret, de k tetszőleges lehet. Ennek a dimenziója $k - 1$. (Azokból a vektorokból áll, amelyeknek páros sok koordinátája 1-es.)

9.4.15

(a) Pl. legyen $p = k = 2$ és $U = \left\langle \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\rangle$.

(b) Egy $\mathbf{x} \in V$ vektor pontosan akkor merőleges U-ra, ha U egy bázisának minden elemére merőleges. Ez a feltétel egy $\dim U$ egyenletből álló, $\dim V$ ismeretlenes homogén lineáris egyenletrendszert jelent, amelynek a rangja $\dim U$ (mert a sorok, amelyek az U báziselemeiből származnak, lineárisan függetlenek). A megoldásoknál így a szabad paraméterek száma $\dim U^\perp = \dim V - \dim U$.

(c) A (b) részből és a 4.6.6 feladatból következik.

9.4.16 Létezik: (a), (c), (e).
Útmutatás: A $\dim U + \dim U^\perp = \dim V$ összefüggés alapján k szükségképpen páros. Használjuk fel a 9.4.14a feladatot is.

9.4.17

(a) Nem igaz, vegyünk pl. egy nagy páratlan elemszámú részhalmazt és a tőle diszjunkt egyelemű részhalmazokat.

(b) Igaz. A Párosváros-tétel bizonyítását követve tekintsük a H_j halmazoknak megfelelő $\mathbf{h}_j$ vektorok által generált U alteret. Ha ennek az U-nak nem minden eleme szerepel a $\mathbf{h}_j$-k között, akkor egy ilyen hiányzó vektorral bővíthetjük a rendszert. Ha U minden eleme szerepel, de az elemszám nem maximális, akkor $\dim U < \lfloor \dim V/2 \rfloor$ és így $\dim U^\perp \geq \dim U + 2$.

Egészítsük ki U bázisát $U^\perp$ bázisává a $\mathbf{w}_1, \mathbf{w}_2, \ldots$ vektorokkal. Ekkor $\mathbf{w}_1, \mathbf{w}_2$ és $\mathbf{w}_1 + \mathbf{w}_2$ mindegyike merőleges U-ra és közülük legalább az egyik önmagára is merőleges, és ekkor ezzel a vektorral bővíthetjük a rendszert.

9.4.18 Útmutatás: Válasszuk külön a páros és páratlan tagszámú egyesületeket, és mutassuk meg, hogy a nekik megfelelő vektorok által generált alterek diszjunktak. Ha ezek dimenziója s, illetve t, akkor $2s + t \leq k$, és így $n \leq t + 2^{\lfloor (k-t)/2 \rfloor}$.

9.4.19 Válasz: 8.
Útmutatás: Lássuk be először, hogy 6 elemű halmaz esetén 4 a maximum. Rátérve a 9 elemű halmaz esetére, igazoljuk, hogy ha a H_i részhalmazok megfelelnek, akkor a komplementereik is a kívánt tulajdonságúak. Ennek alapján feltehető, hogy $|H_1| = 3$. Ekkor valamennyi H_i-re $H_i \cap H_1 = \emptyset$ vagy $H_i \supseteq H_1$. A H_i-knek a H_1-be eső része tehát kétféle lehet, a H_1-en kívül eső részekre pedig a 6 elemű halmaznál látottak szerint négy lehetőség adódik.

9.5.

9.5.1 (b) A 3 egyszeres, az 1 ötszörös és a -2 négyszeres sajátérték. Ezt a legegyszerűbben a 9.5.1 Tétel bizonyításából olvashatjuk le a $d = 3$ speciális esetben.

9.5.2 Az állítás a szomszédsági mátrix és a sajátvektor definíciójából következik.

9.5.3 A sajátértékeket a szomszédsági mátrix karakterisztikus polinomjának a gyökeiként kaphatjuk meg, azonban gyakran kevesebb számolással is célhoz érhetünk, ha az előző feladatra támaszkodunk. Eredmények:
(a) Az $n-1$ egyszeres, a -1 pedig $n-1$-szeres sajátérték.
(b) Az 1 és a -1 mindketten k-szoros sajátértékek.
(c) A k és a $-k$ egyszeres, a 0 pedig $n-2$-szeres sajátérték.
(d) A $\sqrt{n-1}$ és a $-\sqrt{n-1}$ egyszeres, a 0 pedig $n-2$-szeres sajátérték.
(e) A sajátértékek $2\cos(2j\pi/n)$, $0 \leq j \leq n-1$.

9.5.4 Legyen G, illetve $\overline{G}$ szomszédsági mátrixa A, illetve A'. Ekkor a csupa 1 komponensű $\mathbf{j}$ vektor a regularitás miatt mind G-nek, mind pedig $\overline{G}$-nek sajátvektora, a megfelelő sajátérték d, illetve $n-1-d$. Legyen $\mathbf{j}, \mathbf{v}_2, \ldots, \mathbf{v}_n$ az A-nak egy ortonormált sajátbázisa (az $\mathbf{R}^n$ euklideszi térben), a megfelelő sajátértékek legyenek $d, \lambda_2, \ldots, \lambda_n$. Mivel a J-nek a $\mathbf{j}$-től független sajátvektorai éppen $\langle \mathbf{j} \rangle^\perp$ nem nulla elemei, és ezekhez a 0 sajátérték tartozik, ezért a $\mathbf{v}_i$-k a J-nek is sajátvektorai 0 sajátértékkel. Ekkor az $A' = J - E - A$ összefüggés alapján a $\mathbf{v}_i$-k az

A'-nek is sajátvektorai, a megfelelő sajátértékek pedig $-1-\lambda_i$. Az A' sajátértékei tehát $n-1-d, -1-\lambda_2, \ldots, -1-\lambda_n$.

9.5.5 Mutassuk meg, hogy mindkét feltétel ekvivalens azzal, hogy A minden sajátvektora J-nek is sajátvektora.

9.5.6 A Petersen-gráf illeszkedési mátrixa 10×15-ös, ez 6 darab 5×5-ös C_{ij} blokkból áll ($i = 1, 2$, $j = 1, 2, 3$), ahol $C_{12} = C_{21} = 0$, $C_{13} = C_{23} = E$,

$$C_{11} = \begin{pmatrix} 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 \end{pmatrix} \qquad \text{és} \qquad C_{22} = \begin{pmatrix} 1 & 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 1 & 0 & 1 \end{pmatrix}.$$

A továbbiakban a 9.5.3 feladat számozását használjuk.

(a) Egy $n \times n(n-1)/2$-es mátrix, amelynek oszlopaiban minden lehetséges módon előfordul két darab 1-es.

(b) Két $k \times k$-as egységmátrix egymás alatt.

(c) Egy $2k \times k^2$-es mátrix, amelynek oszlopaiban minden lehetséges módon előfordul két darab 1-es úgy, hogy az egyik a felső k sorból, a másik pedig az alsó k sorból van.

(d) Egy $(n-1) \times (n-1)$-es egységmátrix fölött egy csupa 1 sor.

(e) Egy $n \times n$-es mátrix, ahol a főátlóban, közvetlenül a főátló alatt és a jobb felső sarokban áll 1-es, máshol pedig 0.

9.5.7 $M = C^T C$ olyan $m \times m$-es mátrix, ahol a főátló minden eleme 2 és $i \neq j$-re μ_{ij} aszerint 1, illetve 0, hogy az i-edik és j-edik élnek van-e közös csúcsa vagy sem.
$N = CC^T$ olyan $n \times n$-es mátrix, ahol a főátlóban ν_{ii} az i-edik csúcs foka és $i \neq j$-re ν_{ij} aszerint 1, illetve 0, hogy az i-edik és j-edik csúcs össze van-e kötve éllel vagy sem.

9.5.8 Diszjunkt háromszögek egyesítése.

9.5.9 A szokásos jelölésekkel az $A\mathbf{j}$ vektor i-edik koordinátája éppen d_i, az i-edik csúcs foka. Legyen $\mathbf{b}_1, \ldots, \mathbf{b}_n$ ortonormált sajátbázis, $\lambda_1, \ldots, \lambda_n$ a megfelelő sajátértékek és $\mathbf{j} = \sum_{i=1}^{n} \rho_i \mathbf{b}_i$. Ekkor

$$\delta n \leq d_1 + \ldots + d_n = \mathbf{j} \cdot (A\mathbf{j}) = \sum_{i=1}^{n} \lambda_i \rho_i^2 \leq \Lambda \sum_{i=1}^{n} \rho_i^2 = \Lambda(\mathbf{j} \cdot \mathbf{j}) = \Lambda n,$$

azaz valóban $\delta \leq \Lambda$. A $\Lambda \leq \Delta$ egyenlőtlenség bizonyításához legyen $\mathbf{v}$ a Λ-hoz tartozó olyan sajátvektor, amelynek a(z egyik) legnagyobb

koordinátája 1, legyen ez pl. az első koordináta. Az $\mathbf{x} \leq \mathbf{z}$ jelentse azt, hogy minden koordinátára $x_i \leq z_i$. Ekkor $\Lambda\mathbf{v} = A\mathbf{v} \leq A\mathbf{j} \leq \Delta\mathbf{j}$, és az első koordináták összehasonlításával kapjuk, hogy $\Lambda \leq \Delta$.

9.5.10 Először igazoljuk az alábbi segédállításokat. Legyenek A és A' nemnegatív elemű szimmetrikus mátrixok, a maximális sajátértékek Λ, illetve Λ'.

(i) Ha egy nem nulla $\mathbf{x}$ vektor koordinátái nemnegatívak (azaz $\mathbf{x} \geq \mathbf{0}$) és $A\mathbf{x} \geq \tau\mathbf{x}$, akkor $\Lambda \geq \tau$.

(ii) Ha az A és A' minden elemére $\alpha_{ij} \geq \alpha'_{ij}$, akkor $\Lambda \geq \Lambda'$.

Ezután a feladat állítását bizonyítsuk a csúcsok száma szerinti teljes indukcióval; a gráfból hagyjuk el a legkisebb fokszámú csúcsot a hozzá tartozó élekkel és használjuk fel (ii)-t.

Megjegyzés: belátható, hogy a legnagyobb sajátértékhez mindig tartozik nemnegatív sajátvektor, sőt ez bármely nemnegatív elemű (nem feltétlenül szimmetrikus) mátrixra is igaz (Frobenius–Perron-tétel).

9.5.11

(a) Összeadva az összes egyenesre az összegeket azt kapjuk, hogy az összes pontra írt szám összege is 0. Ezután használjuk ki, hogy ha egy adott pontot tartalmazó összes egyenesre nézzük az összeget, akkor ebben a többi pont egyszer szerepel, az adott pont pedig $n+1$-szer.

Célhoz érhetünk a 9.4.4 feladatban definiált illeszkedési mátrix segítségével is, amelyben az i-edik sor j-edik eleme aszerint 1 vagy 0, hogy az i-edik pont rajta van-e a j-edik egyenesen vagy sem. Lássuk be erről az $(n^2+n+1 \times n^2+n+1$-es) A mátrixról, hogy A^TA főátlójának minden eleme $n+1$ és az összes többi elem 1. Az 1.3.12 feladat szerint ekkor $0 \neq \det(A^TA) = (\det A)^2$, ezért $A^T\mathbf{v} = \mathbf{0} \Rightarrow \mathbf{v} = \mathbf{0}$. Legyen $\mathbf{v}$-ben az i-edik koordináta az i-edik pontra írt szám, ekkor $A^T\mathbf{v}$-ben a j-edik koordináta a j-edik egyenesen levő pontokra írt számok összege, ami a feltétel szerint 0. Ezért az előbbiek alapján $\mathbf{v} = \mathbf{0}$, azaz minden ponton csak a 0 szám lehet.

(b) Legyen P, ill. K a piros, illetve kék pontok száma ($P + K = n^2+n+1$), és hasonlóan, P_i, illetve K_i az i-edik egyenesen a piros, illetve kék pontok száma ($P_i + K_i = n+1$). Elég belátni, hogy a $|P_i - K_i|$ eltérések átlaga az n^2+n+1 egyenesen legalább $\sqrt{n}$, azaz

$$\sum_{i=1}^{n^2+n+1} (P_i - K_i)^2 \geq n(n^2+n+1). \tag{E.9.1}$$

A négyzetre emelést elvégezve a bal oldal

$$\sum_{i=1}^{n^2+n+1} P_i^2 + \sum_{i=1}^{n^2+n+1} K_i^2 - 2 \sum_{i=1}^{n^2+n+1} P_i K_i. \qquad \text{(E.9.2)}$$

Az első összeg (E.9.2)-ben azon rendezett piros pontpárok száma, amelyek egy egyenesen vannak. Ha a két pont különböző, akkor egy ilyen egyenes van, ha azonos, akkor $n+1$ egyenes. Ebből adódik, hogy az első összeg $P(P-1)+(n+1)P = P^2+nP$. Ugyanígy adódik, hogy a második összeg K^2+nK. A harmadik összeg pedig a piros-kék pontpárok száma, ami PK. Ezért (E.9.2) átírható a $P^2+K^2+n(P+K)-2PK = (P-K)^2+n(n^2+n+1)$ alakba, ami igazolja (E.9.1)-et.
Célhoz érhetünk egy $(n^2+n+1 \times n^2+n+1$-es) B módosított illeszkedési mátrix segítségével is: $b_{ij} = 1$, ha az i-edik pont piros és rajta van a j-edik egyenesen; -1, ha az i-edik pont kék és rajta van a j-edik egyenesen; és 0 egyébként. Igazoljuk, hogy most is B^TB főátlójának minden eleme $n+1$ és az összes többi elem 1. Legyen $\mathbf{w}$ a csupa 1 koordinátájú vektor, ekkor azt kell belátni, hogy $\mathbf{z} = B^T\mathbf{w}$-nek van legalább $\sqrt{n}$ abszolút értékű koordinátája. Ez következik abból, ha a koordináták négyzetének átlaga legalább n, azaz $\mathbf{z}$-nek önmagával vett skalárszorzata legalább $n(n^2+n+1)$. Ez a skalárszorzat

$$(B^T\mathbf{w})^T(B^T\mathbf{w}) = \mathbf{w}^TBB^T\mathbf{w}. \qquad \text{(E.9.3)}$$

Lássuk be, hogy BB^T főátlójának is minden eleme $n+1$, a többi elem pedig aszerint 1 vagy -1, hogy a sor- és oszlopindexeknek megfelelő pontok azonos vagy különböző színűek. Így $BB^T = nE+H$, ahol H főátlójában 1 áll, minden más elem pedig ± 1. Ezért (E.9.3) átírható $n\mathbf{w}^T\mathbf{w}+\mathbf{w}^TH\mathbf{w}$ alakba. Itt az első tag $n(n^2+n+1)$, a második tagról pedig lássuk be, hogy $(P-K)^2$. Mivel ez utóbbi nemnegatív, ezért az (E.9.3)-beli $\mathbf{z}^T\mathbf{z}$ skalárszorzat valóban legalább $n(n^2+n+1)$.

9.6.

9.6.1 A mohó algoritmussal mindig a legelső olyan elemet választjuk, amelyik nem rontja el a Sidon–tulajdonságot. Tegyük fel, hogy $a_1 < a_2 < \ldots < a_s < n$ már megvan. Egy d elem akkor rossz, ha valamilyen $i, j, k \le s$-re $d + a_i = a_j + a_k$, azaz $d = a_j + a_k - a_i$. Ezzel legfeljebb s^3 (sőt tulajdonképpen kevesebb mint $s^3/2$) elemet zártunk ki, azaz $s < n^{1/3}$ esetén még találunk n-nél kisebb további jó elemet.

9.6.2 A Sidon-tulajdonság igazolásához tegyük fel, hogy $a_i + a_j = a_k + a_l$, azaz $2p(i+j-k-l)+(\langle i^2 \bmod p\rangle+\langle j^2 \bmod p\rangle-\langle k^2 \bmod p\rangle-\langle l^2 \bmod p\rangle)=0$.

Itt a második tag osztható $2p$-vel, de abszolút értéke $2p$-nél kisebb, tehát csak 0 lehet. Emiatt az első tag is 0. Vagyis $i-k=l-j$ és $i^2-k^2\equiv l^2-j^2 \pmod p$. Innen egyszerű számolással adódik, hogy vagy $i=k$ és $j=l$ vagy pedig $i=l$ és $j=k$.

9.6.3 A p^2 elemű testtel és a benne levő p elemű résztesttel hasonlóan (csak egyszerűbben) kell okoskodni, mint a 9.6.2 Tétel bizonyításában tettük.

9.6.4 Vegyünk egy g primitív gyököt modulo p, és legyen a_i az $x \equiv i \pmod{p-1}$, $x \equiv g^i \pmod p$ szimultán kongruenciarendszer megoldása modulo $p(p-1)$, $i=1,2,\dots,p-1$.

9.6.5 A 9.6.1 Tétel szerint vegyünk 1 és n_1 között egy kb. $\sqrt{n_1}$ elemszámú S_1 Sidon-sorozatot. Legyen n_2 jóval nagyobb n_1-nél. Az $[n_1, n_1+n_2]$ intervallumban ne vegyünk elemeket, viszont n_1+n_2 és n_1+2n_2 között helyezzünk el egy kb. $\sqrt{n_2}$ elemszámú Sidon-halmazt, és abból hagyjuk el azokat az elempárokat, amelyeknek a különbsége $< n_1$, a maradékot jelölje S_2. (Megfelelne céljainknak az is, ha minden elempárból csak az egyik elemet hagynánk el.) A Sidon-tulajdonság miatt az elhagyott elemek száma $< 2n_1$. Így n_1+2n_2-ig összesen kb. $\sqrt{n_2}+\sqrt{n_1}-2n_1 \approx \approx \sqrt{n_2}$ elemünk van. Lássuk be, hogy $S_1 \cup S_2$ Sidon-tulajdonságú. Ezután válasszunk egy, az n_1+2n_2-nél jóval nagyobb n_3-at, $n_1+2n_2+n_3$ és $n_1+2n_2+2n_3$ között helyezzünk el egy kb. $\sqrt{n_3}$ elemszámú Sidon-halmazt, abból töröljük azokat az elemeket, amelyeknek a különbsége $< n_1+2n_2$ stb. Az eljárást folytatva a feladat feltételeit teljesítő végtelen Sidon-sorozatot kapunk.

9.6.6
(a) Általánosítsuk a 9.6.3 feladat módszerét a p^h elemű testre.
(b) Az elemekből képezhető h-tagú összegek egyrészt mind különbözők, másrészt valamennyien 1 és nh közé esnek.

9.6.7
(a) A kettőhatványok ilyenek.
(b) Vizsgáljuk meg, hány összeg keletkezik és ezek milyen határok közé esnek.
(c) A keletkező összegeket egy (klasszikus) valószínűségi változónak tekintve alkalmazzuk a Csebisev-egyenlőtlenséget.

9.6.8 Legyen C az 1 és $n^{2/3}$ közötti egész számok halmaza, továbbá D a C-nek az n-ig terjedő prímszámokkal való egyesítése. Először lássuk be, hogy n-ig minden szám felírható $n=cd$ alakban, ahol $c \in C$, $d \in D$ (a felírás általában nem egyértelmű). Az a_i számoknak rögzítsük egy ilyen

$a_i = c_i d_i$ előállítását, majd készítsünk el egy $|C| + |D| \leq \pi(n) + 2n^{2/3}$ csúcsú páros gráfot, amelynél a csúcsok egyik csoportja a C halmaz, a másik pedig a D, és az a_i számnak a c_i és d_i csúcsot összekötő él felel meg. Ha az élek száma legalább annyi, mint a csúcsok száma, akkor a gráfban van kör. A párosság miatt ennek a körnek páros sok éle van, és a konstrukció alapján a minden második élnek megfelelő a_i-k szorzata megegyezik a kör többi élének megfelelő a_j-k szorzatával (hiszen mindkét szorzat a kör összes csúcsaiban szereplő számok szorzata).

9.6.9 Írjuk fel a számokat d alapú számrendszerben, ahol d értékét később alkalmasan megválasztjuk. Tekintsük most azokat a számokat n-ig, amelyek felírásában minden számjegy $< d/2$ és a számjegyek négyzetösszege egy adott q érték. Mutassuk meg, hogy egy ilyen számhalmazban nem fordul elő háromtagú számtani sorozat, továbbá q és d alkalmas megválasztásával elérhető, hogy a halmaz elemszáma a feladat állításának megfelelően nagy legyen.

9.6.10 *Első megoldás*: A „rossz" színezések számát ügyesen felülről becsülve mutassuk meg, hogy ez kisebb, mint az összes színezések száma.
Második megoldás: Tekintsük a p prímmel a 2^p elemű T véges testet, legyen Δ a multiplikatív csoport generátoreleme és W egy $p-1$-dimenziós altér T-ben (mint F_2 feletti vektortérben). A színezés: k akkor piros, ha $\Delta^k \in W$. Az $1, 2, \ldots, p(2^p - 1)$ számokat ily módon kiszínezve nem fordul elő $p+1$-tagú egyszínű számtani sorozat.
Harmadik megoldás: Legyenek pirosak azok a számok, amelyek a 7 és a 17 közül pontosan az egyikkel oszthatók.
Negyedik megoldás: Legyenek pirosak azok a számok, amelyek a 2, a 3, az 5 és a 7 közül páratlan sokkal oszthatók.
Ötödik megoldás: Nevezzünk A-nak, illetve B-nek egy olyan, 17 egymás után következő számból álló blokkot, amelynek az első 16 eleme piros, az utolsó eleme pedig kék, illetve fordítva, és tekintsük az alábbi színezést: 15 darab A után vegyünk 15 darab B-t és ezt ismételjük (összesen 16-szor lehet).

9.7.

9.7.1 Az alábbi lépésekben igazolhatjuk a tételt:

(i) Két egyenlő alapú és magasságú paralelogramma egymásba darabolható. Legyen a közös alap AB, a vele párhuzamos oldalegyenesen a csúcsok legyenek CD, illetve $C'D'$. Ha pl. D a $D'C'$ szakaszon van, akkor az $ABCD$ paralelogrammából vágjuk le a BCC' háromszöget, és ezt a vele

egybevágó ADD' háromszög helyére illesztve megkapjuk az $ABC'D'$ paralelogrammát. Ha a CD és $C'D'$ szakaszoknak nincs közös pontja, akkor mindkét paralelogrammát vágjuk szét az alapjukkal párhuzamosan olyan „alacsonyabb" paralelogrammákra, amelyekre már alkalmazhatjuk az előző gondolatmenetet.

(ii) Egy téglalap átdarabolható olyan téglalappá, melynek egyik oldala adott. A téglalapot szükség esetén vékonyabb csíkokra vágva és a csíkokat a rövidebb élek mentén összeragasztva olyan ABCD téglalapot kapunk, amelynek (mondjuk) a BC oldala kisebb, az AB oldala pedig nagyobb az adott x szakasznál. A B középpontú x sugarú kör messe a CD oldalt a C' pontban, és legyen D' a B pont tükörképe az AC' szakasz felezőpontjára, ezzel egy $ABC'D'$ paralelogrammát kapunk. A C' és B pontok merőleges vetülete a $D'A$ egyenesen legyen X, illetve Y, így egy $BC'XY$ téglalaphoz jutunk, amelynek BC' oldala éppen az előírt x hosszúságú. Ekkor az $ABCD$ téglalap és a $BC'XY$ téglalap is azonos alapú és magasságú, mint az $ABC'D'$ paralelogramma, ezért az (i) rész alapján a két téglalap — az $ABC'D'$ paralelogramma „közvetítésével" — egymásba darabolható.

(iii) Végül egy tetszőleges sokszöget háromszögekre bonthatunk, mindegyik háromszöget téglalappá alakíthatjuk, a kapott téglalapokból pl. egységnyi alapú téglalapokat gyárthatunk, és ezeket egymás mellé téve egyetlen, egységnyi alapú téglalappá daraboltuk át a sokszöget. Ezt két azonos területű sokszögre elvégezve két egybevágó téglalaphoz jutunk, tehát a két sokszög egymásba is átdarabolható.

9.7.2

(a) Valamely δ pontosan akkor lesz a π-nek racionális számszorosa, ha van olyan n pozitív egész, amelyre $n\delta$ a 2π-nek egész számú többszöröse, azaz $\cos(n\delta) = 1$. A

$$\cos(n\alpha) = 2\cos\big((n-1)\alpha\big)\cos\alpha - \cos\big((n-2)\alpha\big)$$

összefüggés alapján igazoljuk teljes indukcióval, hogy $\cos(n\alpha)$ egy 3^n nevezőjű (tovább már nem egyszerűsíthető) tört, és így nem lehet az értéke 1.

(b) Az előzőkhöz hasonlóan igazoljuk teljes indukcióval, hogy $2\cos(n\gamma)$ a $2\cos\gamma$-nak egész együtthatós, normált polinomja. Így ha $\cos(n\gamma) = 1$, akkor $2\cos\gamma$ gyöke egy egész együtthatós, normált polinomnak. Egy ilyen polinom racionális gyökei csak egészek lehetnek, tehát $2\cos\gamma$ egész szám. Ezt a $|\cos\gamma| \le 1$ feltétellel összevetve kapjuk az állítást.

9.7.3 Ha egy T téglalap a és b oldalának aránya az $a/b = r/s$ racionális szám, akkor T szétvágható rs darab egybevágó $a/r = b/s$ oldalú négyzetre. A megfordításhoz definiáljunk a téglalapok halmazán egy, a területre emlékeztető függvényt: legyen f egy tetszőleges valós függvény, amely kielégíti a Cauchy-féle $f(x+y) = f(x) + f(y)$ függvényegyenletet (lásd a 9.1.8 feladatot), és ha egy U téglalap oldalai c és d, akkor legyen $F(U) = f(c)f(d)$. Speciálisan, ha U egy négyzet, akkor $F(U) \geq 0$. Mutassuk meg, hogy ha az U téglalapot az U_i téglalapokra vágjuk szét, akkor $F(U) = \sum_i F(U_i)$. Tegyük fel indirekt, hogy a és b nem egymás racionális számszorosai és mégis szétvágtuk az a és b oldalú T téglalapot négyzetekre: $T = \cup N_i$ (ahol az N_i négyzeteknek nincs közös belső pontjuk). Ekkor $F(T) = \sum F(N_i)$ jobb oldala nemnegatív, ugyanakkor $F(T) < 0$, ha $f(a) = 1$ és $f(b) = -1$, ami elérhető, mert a és b lineárisan függetlenek $\mathbf{Q}$ felett.

9.7.4

(a) Átdarabolhatók, ennek igazolása a Bolyai–Gerwien-tétel bizonyításának a mintájára (szinte arra támaszkodva) végezhető el (9.7.1 feladat).

(b) Nem darabolhatók egymásba: az $ABCC'$ tetraéder átdarabolható egy hasábba és így egy vele azonos térfogatú kockába is, az $ABCB'$ tetraéder viszont nem. Ez utóbbi egyik lapszöge $\pi/2$, a másikat ϑ-val jelölve $\cos\vartheta = 1/\sqrt{3}$. Mutassuk meg, hogy ϑ/π irracionális, és ezután kövessük a 9.7.1 Tétel bizonyításának a gondolatmenetét.

9.7.5 A megfelelő invariáns legyen a sokszögnek egy adott irányba eső élhosszainak (valamely körüljárás szerinti) előjeles összege.

9.7.6

(a) Ha $n = 2k > 2$, akkor egy k oldalhosszúságú négyzetben vegyünk egy $k-1$ oldalú négyzetet és a megmaradt sávokban a $2k-1$ darab egységnégyzetet. Ha $n = 2k+3 > 5$, akkor vegyük az előző konstrukciót, majd valamelyik négyzetet vágjuk fel 4 egybevágó részre. A megfordításhoz használjuk ki, hogy az eredeti négyzet minden sarkára kell illeszkednie egy kis négyzetnek, tehát n eleve nem lehet 2 vagy 3, az $n = 5$ esetben pedig a nagy négyzet egyik oldalára 3, a többi oldalra 2 kis négyzet illeszkedne, ami egyszerű esetszétválasztás után szintén ellentmondásra vezet.

(b) Mivel egy kockából könnyen csinálhatunk 8, illetve 27 kis kockát, ezek egymás utáni alkalmazásával egy kocka $1 + 7x + 26y$ részre is bontható, ahol x és y tetszőleges nemnegatív egészek. Felhasználva, hogy a 7 és a 26 relatív prímek, lássuk be, hogy minden elég nagy n előállítható ilyen alakban.

(c) Mivel egy kockát 8 részre vágva, a kis kockák számát mindig tudjuk 7-tel növelni, ezért elég az állítást a 48 és 54 közötti n-ekre igazolni.

48: $48 = 27 + 3 \cdot 7$, azaz a kockát vágjuk 27 részre, majd 3 kis kockát 8-8 részre.

49: egy 6 oldalú kocka alsó felét bontsuk 4 darab 3 oldalú kockára, a felső sorát 36 darab egységkockára, a fennmaradó két sort pedig 9 darab 2 oldalú kockára.

50: $50 = 7 \cdot 7 + 1$.

51: egy 6 oldalú kocka alsó felét és még egy nyolcadát bontsuk 5 darab 3 oldalú kockára, a megmaradt részből kiválaszthatunk 5 darab 2 oldalú kockát és marad még 41 darab egységkocka.

52: egy 4 oldalú kockából vegyünk ki egy 3 oldalú részt, ekkor marad 37 egységkocka, ezekből kettőt 8-8 részre osztva összesen 52 kockára bontottuk az eredeti kockát.

53: $53 = 1 + 2 \cdot 19 + 2 \cdot 7$ alapján elég olyan eljárást mutatni, amely 19-cel növeli a kockák darabszámát; egy 3 oldalú kockát bontsunk egy 2 oldalúra és a megmaradó 19 egységkockára.

54: egy 8 oldalú kocka háromnegyedét bontsuk 6 darab 4 oldalú kockára, a maradékból leválasztható 2 darab 3 oldalú és 4 darab 2 oldalú kocka, valamint marad 42 darab egységkocka.

9.7.7

(a) Ha $n \neq 2$, 3 vagy 5, akkor a 9.7.6a feladathoz hasonló konstrukciót alkalmazhatunk. A megfordítás $n = 2$-re most is egyszerű, azonban $n = 3$-ra és 5-re a négyzethez képest bonyolítja a helyzetet, hogy a kis háromszögek az eredeti háromszög szögeit is elvághatják. Itt jó szolgálatot tesz az alábbi, önmagában is érdekes észrevétel: Ha egy H háromszög szögei a racionális test felett lineárisan függetlenek, akkor H csak úgy bontható fel hasonló háromszögekre, ha azok H-hoz is hasonlók, továbbá ekkor H felbontásánál a kis háromszögek H szögeit nem vághatják el.

(b) Ha $n = k^2$, akkor egy háromszög minden oldalát k egyenlő részre osztva a háromszöget nyilván n egybevágó kis háromszögre bontottuk. A megfordításhoz vegyünk egy olyan háromszöget, amelyben nemcsak a szögek, hanem az oldalak is lineárisan függetlenek. Mutassuk meg, hogy valóban létezik ilyen háromszög, továbbá egy ilyen háromszöget nem lehet n egybevágó háromszögre felbontani, ha $\sqrt{n}$ irracionális.

(c) Ha $n = k^2 + m^2$, akkor vegyünk egy olyan derékszögű háromszöget, amelynek a befogói k és m. Ha $n = 3k^2$, akkor egy szabályos háromszög „fele” lesz megfelelő.

9.8.

9.8.1 Ha pl. $\mathbf{a}_n = \sum_{j=1}^{n-1} \lambda_j \mathbf{a}_j$, akkor (i) miatt $D(\mathbf{a}_1, \mathbf{a}_2 \ldots, \mathbf{a}_n) =$
$= \sum_{j=1}^{n-1} \lambda_j D(\mathbf{a}_1, \mathbf{a}_2 \ldots, \mathbf{a}_j)$, és itt (iv) szerint mindegyik tag 0.

9.8.2 A 9.8.1 Tétel bizonyításának mintájára következik, hogy $F_i(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ már teljesen meghatározza F_i-t.

9.8.3 Használjuk fel az előző feladatot és az $F(\mathbf{e}_1, \ldots, \mathbf{e}_n) = G(\mathbf{e}_1, \ldots, \mathbf{e}_n)$ egyenlőséget.

9.8.4 Támaszkodjunk az előző feladatra.

9.8.5

(a) A determináns értéke nem változik, ha az első két oszlopból kivonjuk a harmadik oszlopot és a harmadik sora szerint kifejtjük. Az ennek megfelelő $\begin{vmatrix} \gamma_{11}-\gamma_{13} & \gamma_{12}-\gamma_{13} \\ \gamma_{21}-\gamma_{23} & \gamma_{22}-\gamma_{23} \end{vmatrix}$ determináns a P_3-ból P_1-be, illetve P_2-be mutató vektorok által kifeszített paralelogramma előjeles területe. Ez a paralelogramma pontosan akkor fajul el, ha a pontok egy egyenesbe esnek.

(b) A négy pont akkor és csak akkor van egy síkban, ha a koordinátáikból képezett $\begin{vmatrix} \gamma_{11} & \gamma_{12} & \gamma_{13} & \gamma_{14} \\ \gamma_{21} & \gamma_{22} & \gamma_{23} & \gamma_{24} \\ \gamma_{31} & \gamma_{32} & \gamma_{33} & \gamma_{34} \\ 1 & 1 & 1 & 1 \end{vmatrix}$ determináns nulla.

(c) Az eredmények tetszőleges koordinátarendszerben érvényesek, ugyanis a 9.8.1 Tétel szerint tetszőleges bázist választhatunk.

10. Kódok

10.1.

10.1.1 (a) $(1-p)^k$. (b) $kp(1-p)^{k-1}$. (c) $1 - \sum_{i=0}^{3} \binom{k}{i} p^i (1-p)^{k-i}$.

10.1.2 1-hibajelző: (a), (b), (e), (f). 1-hibajavító: (e).

10.1.3 Az általánosítás: (i) tetszőleges számú rögzített helyen a jegyeket megváltoztathatjuk, azaz minden kódszóhoz ugyanazt a vektort hozzáadhatjuk (a kódszavakat „eltoljuk"); (ii) a kódszavak jegyeit tetszőlegesen (de azonos módon) permutálhatjuk; valamint (i)-et és (ii)-t kombináltan is alkalmazhatjuk (azaz vehetjük a kétféle transzformáció kompozícióját). Az így nyert kódokat az eredetivel *ekvivalens*eknek nevezzük.

10.1.4 (b) Pontosan a páratlan m-ek ilyenek.

10.1.5 Legyen A, illetve B azoknak a helyeknek a halmaza, ahol az $\mathbf{u}$ és $\mathbf{v}$ vektorok jegyei azonosak, illetve ellentétesek. A feltétel szerint $|A| = k - d, |B| = d$. Jelöljük j-vel, ahány A-beli helyen a $\mathbf{w}$ vektor jegye nem ugyanaz, mint a másik két vektoré. Ekkor B-ben az $\mathbf{u}$ és $\mathbf{w}$ vektorok $q - j$, a $\mathbf{v}$ és $\mathbf{w}$ vektorok pedig $r - j$ jegyben kell hogy különbözzenek, és nyilván $(q - j) + (r - j) = d$. Innen $j = (r + q - d)/2$, tehát nincs megfelelő $\mathbf{w}$, ha $r + q - d$ páratlan szám és $\binom{k-d}{j}\binom{d}{q-j}$ ilyen $\mathbf{w}$ van, ha $r + q - d$ páros.

10.1.6 Az előző feladathoz hasonló gondolatmenetet kell alkalmazni.

10.1.7 Ha d páratlan volt, akkor a minimális távolság eggyel nő, páros d-re pedig nem változik.

10.1.8 A $t = 1$ speciális esetre látott gondolatmenetet kell adaptálnunk. Jelöljük $H(\mathbf{c})$-vel a $\mathbf{c}$ kódszó t sugarú környezetét, azaz a tőle legfeljebb t távolságra levő T^k-beli vektorok halmazát (beleértve magát a $\mathbf{c}$ vektort is). Mivel a $\mathbf{c}$-től (illetve bármelyik T^k-beli vektortól) pontosan i távolságra $\binom{k}{i}$ darab vektor található, ezért a tőle legfeljebb t távolságra levő vektorok száma $|H(\mathbf{c})| = \sum_{i=0}^{t}\binom{k}{i}$. A feltétel szerint a $H(\mathbf{c})$ halmazok páronként diszjunktak és a számuk 2^n, így az egyesítésük elemszáma $2^n|H(\mathbf{c})| \leq |T^k| = 2^k$.

10.1.9 $n = 2$: (aA) 1. (aB) 3. (bA) 3. (bB) 6.

$n = 3$: (aA) 1. (aB) 3. (bA) 3. (bB) 7.

Az $n = 2$ esetre és a 2-hibajavításra részletezzük a bizonyítást (a t-hibajavítás tetszőleges t-re ennek mintájára tárgyalható, és hasonlóan kell okoskodni — csak jóval több számolgatás kíséretében — $n = 3$ mellett is a 2-hibajavításnál). Hat ellenőrző jegy valóban elég, mert megfelel például a $\varphi : \alpha_1\alpha_2 \mapsto \alpha_1\alpha_2\alpha_1\alpha_2\alpha_1\alpha_2\beta\beta$ kód, ahol $\beta = \alpha_1 + \alpha_2$. Azonnal látszik, hogy a négy kódszó közül bármelyik kettőnek a távolsága legalább 5, tehát a kód valóban 2-hibajavító. Ugyanakkor öt ellenőrző jegy még nem lehet elég a 2-hibajavításhoz, mert T^7-ben már három olyan vektor sem található, amelyek közül bármelyik kettő távolsága legalább 5. Ha ugyanis $\mathbf{c}_2 - \mathbf{c}_1$-ben és $\mathbf{c}_3 - \mathbf{c}_2$-ben is a hét jegy között legalább öt darab 1-es szerepel, akkor ezek közül legalább három azonos helyen fordul elő, és így $\mathbf{c}_3 - \mathbf{c}_1 = (\mathbf{c}_3 - \mathbf{c}_2) + (\mathbf{c}_2 - \mathbf{c}_1)$-ben ezeken a helyeken 0 áll, vagyis $\mathbf{c}_3 - \mathbf{c}_1$-ben legfeljebb négy 1-es található.

10.2.

10.2.1 Igaz: (b).

10.2.2 Két, illetve három $n \times n$-es egységmátrix egymás alatt.

10.2.3 Lineáris: (b), (e) és (f). Generátormátrixok:

$$\text{(b)}\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 1 \end{pmatrix} \qquad \text{(e)}\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 1 & 0 \\ 1 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix} \qquad \text{(f)}\ \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \\ 1 & 1 & 0 \\ 1 & 1 & 1 \end{pmatrix}$$

A dekódolási táblát csak (e)-re adjuk meg (a másik két kód nem is lesz 1-hibajavító):

000000	100110	010101	001011	110011	101101	011110	111000
100000	000110	110101	101011	010011	001101	111110	011000
010000	110110	000101	011011	100011	111101	001110	101000
001000	101110	011101	000011	111011	100101	010110	110000
000100	100010	010001	001111	110111	101001	011010	111100
000010	100100	010111	001001	110001	101111	011100	111010
000001	100111	010100	001010	110010	101100	011111	111001
100001	000111	110100	101010	010010	001100	111111	011001

10.2.4 Egy $\mathcal{A} : T^n \to T^k$ lineáris leképezés injektivitása ekvivalens azzal, hogy $\dim \operatorname{Im} \mathcal{A} = n$, továbbá $\dim \operatorname{Im} \mathcal{A}$ éppen az $\mathcal{A}$ mátrixának a rangja.

10.2.6 A dimenzió $n-1$ vagy n.

10.2.7

(a) $d_3 \geq d_1 + d_2$; $\quad d_4 = \min(d_1, d_2)$; $\quad d_5 = \min(2d_1, d_2)$.

(b) $G_3 = \begin{pmatrix} G_1 \\ G_2 \end{pmatrix}$; $\quad G_4 = \begin{pmatrix} G_1 & 0 \\ 0 & G_2 \end{pmatrix}$; $\quad G_5 = \begin{pmatrix} G_1 & 0 \\ G_1 & G_2 \end{pmatrix}$.

10.2.8

(a) Legyen $g = \sum_{i=0}^{s} \delta_i x^i$, ekkor a generátormátrix j-edik oszlopában a $j+i$-edik elem δ_i, $i = 0, 1, \ldots, s$, a többi elem pedig 0 (tehát a „főátló" minden eleméről „lelóg" a g polinom egy-egy példánya).

(b) Az injektivitással lehet baj. Legyen g és h legnagyobb közös osztója d, ekkor

$$h \,|\, gf_1 - gf_2 = g(f_1 - f_2) \iff \frac{h}{d} \,\Big|\, \frac{g}{d}(f_1 - f_2) \iff \frac{h}{d} \,\Big|\, f_1 - f_2\,.$$

Ebből a $\deg f_i \leq n-1$ feltétel figyelembevételével akkor és csak akkor következik $f_1 = f_2$, ha $n \leq \deg(h/d) = k - \deg d$, azaz $\deg d \leq s$.

(c) Legyen $d = (g, h)$ és D a d-vel osztható legfeljebb $k-1$-edfokú polinomok halmaza. Ekkor $|D| = 2^{k-\deg d} = 2^n$, tehát D éppen a d által generált polinomkód kódszavaiból áll, továbbá nyilván $d \mid h$. A gf polinom h-val való osztási maradéka mindenképpen osztható d-vel, tehát $K \subseteq D$. Mivel emellett $|K| = |D|$, ezért $K = D$.

10.2.9 Legyen a kód generátormátrixa G, ekkor olyan H kell, amelyre $HG = E_{n\times n}$. Ez n darab, n egyenletből álló és k ismeretlenes lineáris egyenletrendszert jelent, amelyek mindegyikének az együtthatómátrixa G^T. Mivel G rangja n, ezért ezek az egyenletrendszerek megoldhatók. A megoldásokat pl. Gauss-kiküszöböléssel gyorsan meg is tudjuk határozni. A megoldások ($k > n$ miatt) nem egyértelműek, de akármelyikből adódó H megfelel. Ugyanezt az eljárást alkalmaztuk a négyzetes mátrixok inverzének a meghatározására (tulajdonképpen megfelelő értelmezés mellett most is a G mátrix egy bal oldali inverzéről van szó).

10.3.

10.3.1 A sorok függetlenségének a feltételezése mellett az oszlopok összefüggősége ekvivalens azzal, hogy több oszlop van, mint sor. A paritásellenőrző mátrixról tudjuk, hogy a rangja megegyezik a sorok számával, tehát a sorai függetlenek, az oszlopok pedig többen vannak, mint a sorok. A megfordításhoz vegyünk egy olyan P mátrixot, amelynek s sora és k oszlopa van, ahol $k-s = n > 0$ és $r(P) = s$. A dimenziótétel szerint $\operatorname{Ker} P$ egy $k - s = n$-dimenziós K altér T^k-ban, tehát P a (k, n) paraméterű K lineáris kód paritásellenőrző mátrixa.

10.3.2 Mivel mindegyik esetben $G = \begin{pmatrix} E_{n\times n} \\ B_{s\times n} \end{pmatrix}$ alakú, ezért paritásellenőrző mátrixnak megfelel $P = \begin{pmatrix} B_{s\times n} & E_{s\times s} \end{pmatrix}$ (vö. a 10.3.5a feladattal).

10.3.3 I. A második tulajdonság azt fejezi ki, hogy $\operatorname{Ker} \mathcal{P} \supseteq K$. Itt egyenlőség pontosan akkor teljesül, ha $n = \dim K = \dim \operatorname{Ker} \mathcal{P} = \dim T^k - r(P) = k - r(P)$, azaz ha $r(P) = s$.
II. Az I.-beli második tulajdonság ekvivalens $PG = 0$-val.
III. A $PG = 0$ mátrixegyenlőség azt jelenti, hogy P sorai merőlegesek $\operatorname{Im} \mathcal{A}$-ra, $r(P) = s$ pedig azt, hogy ezek a sorok függetlenek. Használjuk fel, hogy $\dim(\operatorname{Im} \mathcal{A})^\perp = \dim T^k - \dim \operatorname{Im} \mathcal{A} = k - n = s$.

10.3.4 Használjuk az előző feladat III. részét, valamint (b)-hez még a 4.5.14a feladatot is.

10.3.5 Útmutatás (b)-hez: Használjuk a 10.3.3 feladat II. részét. A $PG = 0$ feltétel s darab, k ismeretlenes és n egyenletből álló homogén egyenletrendszert jelent, amelyek közös együtthatómátrixa G^T. Mivel a szabad paraméterek száma $k - r(G^T) = k - n = s$, ezért a megoldások egy s-dimenziós alteret alkotnak T^k-ban, tehát kiválasztható s darab független megoldás. Az egyenletrendszert pl. Gauss-kiküszöböléssel oldhatjuk meg, és biztosan független megoldásokhoz jutunk, ha rendre egy-egy szabad paramétert 1-nek, a többit pedig 0-nak választunk.

10.3.6 Ha egy sor lineárisan függ a többitől, akkor ennek a sornak az elhagyása a mátrix magterét nem változtatja meg.

10.3.8 Hasonlóan okoskodhatunk, mint a 10.3.2 Tétel bizonyításánál.

10.3.9 Használjuk fel az előző feladatot.
Másik lehetőség: A paritásellenőrző mátrix helyett a generátormátrixszal is dolgozhatunk. Ha a kódszavak a megfelelő közleményszóval kezdődnek, akkor egy egységvektorhoz tartozó kódszó súlya legfeljebb $1 + s$, tehát készen vagyunk.
Ugyanezt a gondolatot tetszőleges lineáris kód esetén a következőképpen valósíthatjuk meg: vegyünk a generátormátrixban n független sort, és lássuk be, hogy van olyan kódszó, amelynek az ebbe az n sorba eső része egy (tetszőleges) egységvektor.

10.3.10 Az egyik kód generátormátrixának a transzponáltja a másiknak egy paritásellenőrző mátrixa és viszont.

10.3.11 Használjuk fel az előző feladatot.

10.3.12 Válasz: 3. Az 1-hibajavítás miatt a minimális távolságnak legalább 3-nak kell lennie, nagyobb pedig azért nem lehet, mert — mint már a 10.1 pont végén is láttuk — ekkor a kódszavak 1 sugarú környezetei kitöltik az egész T^k-t.

10.3.13 Először mutassuk meg, hogy ha egy lineáris kódban van olyan kódszó, amelynek a komplementere is kódszó, akkor ez minden kódszóra teljesül. Ezután elég például a $\mathbf{0}$ kódszó komplementéről, a $\mathbf{j}$ csupaegy vektorról belátni, hogy kódszó. Ez pontosan azt jelenti, hogy a paritásellenőrző mátrix minden sorában páros sok 1-es szerepel.

10.3.14 A megadásból leolvasható, hogy lineáris kódot definiáltunk. Írjuk fel a G generátormátrixot. Ennek az egységmátrix alatti $s \times (2^s - 1)$ méretű B részében az oszlopok rendre azoknak a 2^s-nél kisebb természetes számoknak a kettes számrendszerbeli alakjai, amelyek nem kettőhatványok. Így éppen azok az oszlopok fordulnak elő B-ben, éspedig mindegyik egyszer, amelyekben legalább két darab 1-es áll. Láttuk, hogy a P paritásellenőrző

mátrixot megkaphatjuk úgy, hogy B mögött egy $s \times s$ méretű egységmátrixot helyezünk el, azaz B oszlopai mögé az s darab egységvektort is odatesszük. Így P oszlopait úgy kapjuk, hogy T^s minden nem nulla vektorát pontosan egyszer vesszük, azaz valóban egy Hamming-kódról van szó.

A paritásellenőrző mátrix felírása nélkül közvetlenül is beláthatjuk, hogy a kód 1-hibajavító, tehát Hamming-kód. Ehhez azt kell igazolni, hogy minden nem nulla kódszóban legalább három 1-es szerepel. Ha már a közleményszóban legalább három 1-es áll, akkor ezek a kódszóban is megmaradnak, tehát készen vagyunk. Ha a közleményszóban egyetlen 1-es fordul elő, mondjuk α_m, akkor az m kettes számrendszerbeli jegyeinek megfelelő γ-k értéke is 1, tehát a kódszóban ekkor is megvan a (legalább) három 1-es. Végül, ha a közleményszóban két 1-es található, mondjuk α_m és α_q, akkor m és q kettes számrendszerbeli felírása legalább egy jegyben különbözik, és egy ilyen helyiértéknek megfelelő γ értéke szükségképpen 1, azaz most is találtunk (legalább) három 1-est a kódszóban.

10.4.

10.4.1 A 32 elemű test multiplikatív csoportjának elemszáma 31, ami prímszám, ezért ezt a csoportot az egységelemen kívül bármelyik eleme generálja. Így generátorelemnek egy tetszőleges ötödfokú irreducibilis polinom, például az x^5+x^2+1 egyik gyökét vehetjük. Ekkor a $\Delta^5 = 1+\Delta^2$ számolási szabályt kell ismételten alkalmazni. Ennek alapján a paritásellenőrző mátrixnak például a 3. oszlopa a következő lesz: a felső részbe Δ^2, az alsóba $\Delta^6 = \Delta + \Delta^3$ kerül, azaz a felső öt elem rendre 0,0,1,0,0, az alsó öt pedig 0,1,0,1,0.

10.4.2 Láttuk, hogy $s = \deg g_t$, ahol $g_t = [m_1, m_3, \ldots, m_{2t-1}]$. Mivel mindegyik m_i irreducibilis, ezért g_t a fenti m_i-k közül a különbözőknek a szorzata, továbbá $\deg m_i \le q$. Így $s = \deg g_t = tq$ pontosan akkor teljesül, ha az m_i-k mind különbözők és mindegyiknek a foka q.

10.4.3

(a) A 16 elemű testet a 10.4.1 Tétel utáni példa mintájára kezeljük, és használjuk ki, hogy $(\Delta^3)^5 = (\Delta^5)^3 = 1$.

(b) Mutassuk meg, hogy Δ^3 és Δ^5 is generátorelem a T^q test multiplikatív csoportjában, és így a minimálpolinomjuk szükségképpen q-adfokú. Ezután igazolnunk kell még a három minimálpolinom különbözőségét, ehhez lássuk be, hogy m_i összes gyökei a Δ-nak az $i \cdot 2^j$ kitevőjű hatványai, ahol $0 \le j < q$.

10.4.4 Az előző feladathoz hasonlóan kapjuk, hogy $m_3 \neq m_1$, és így $s = \deg g = \deg m_1 + \deg m_3 = q + \deg(\Delta^3)$. Ha Δ^3 nem lenne q-ad-fokú, akkor a foka valódi osztója lenne a q-nak, és így $\deg(\Delta^3) \leq q/2$, tehát $s \leq 3q/2$ következne. Ugyanakkor tudjuk, hogy $s \geq 2q - 1$, ami ellentmondás.

10.4.5

(a) Használjuk fel, hogy minden $v \mid q$-ra a T^q testnek pontosan egy 2^v elemű részteste van, és ennek nem nulla elemei a Δ-nak a $j(2^q - 1)/(2^v - 1)$ kitevőjű hatványai.

(b) Lássuk be, hogy ezek mind gyökei m_i-nek, továbbá páronként különbözők. Ez utóbbihoz használjuk fel, hogy Δ két hatványa pontosan akkor egyenlő, ha a kitevők különbsége osztható $2^q - 1$-gyel.

10.4.6 Meg kell mutatni, hogy teljesülnek a 10.4.2 feladat feltételei. Támaszkodjunk a 10.4.5 feladatra is.

10.4.7

(a) A $\mathbf{c} = \gamma_0 \dots \gamma_{k-1} \in T^k$ vektor akkor és csak akkor páros súlyú, ha $\gamma_0 + \gamma_1 + \dots + \gamma_{k-1} \equiv 0 \pmod 2$, azaz az 1 gyöke a $C = \gamma_0 + \gamma_1 x + \dots + \gamma_{k-1} x^{k-1}$ polinomnak, vagyis $x - 1 = x + 1 \mid C$. Mivel a kódszavak K halmaza pontosan g többeseiből áll, ezért a feltétel ekvivalens azzal, hogy $1 + x \mid g$.

(b) A páros súlyú elemek száma éppen $|T^k|/2$, azaz ekkor az ellenőrző jegyek száma $s = 1$. Ezt (a)-val összevetve kapjuk az állítást.

10.4.8 A T^q test multiplikatív csoportjának bármely elemét a $|T^q| - 1 = 2^q - 1 = k$-adik hatványra emelve az egységelemet kapjuk. Ez azt jelenti, hogy a multiplikatív csoport bármely eleme gyöke az $x^k - 1$ polinomnak, és így mindegyik m_i minimálpolinom osztja $x^k - 1$-et. Ekkor viszont a legkisebb közös többszörösük, azaz a generáló polinom is osztja $x^k - 1$-et.

10.4.9

(a) Lássuk be, hogy egy ciklikus kód kódszavai ideált alkotnak az $R_k = T[x]/(x^k - 1)$ maradékosztálygyűrűben, és ezt az ideált egy olyan g polinom generálja, amely osztója $x^k - 1$-nek.

(b) Az (a) részből és az előző feladatból következik.

10.4.10 Olyan (kvázi-)paritásellenőrző mátrixot kell gyártani, amelynek bármelyik $d-1$ oszlopa független. Ha már az első j oszlopot elkészítettük, akkor a $j + 1$-ediket úgy kell megválasztani, hogy az ne legyen felírható az első j oszlop közül semelyik legfeljebb $d - 2$-nek a lineáris kombinációjaként. A feltétel alapján ez még $j = k - 1$-re is megvalósítható.

10.4.11 Az (a) résznél q szerinti, a (b) résznél pedig (pl.) $q+m$ szerinti teljes indukcióval bizonyítsunk.

A. Algebrai alapfogalmak

A.1.

A.1.1

(a) Indukciós lépés: A bal oldali összeg $n+1$-re csak az utolsó tagban különbözik az n-es összegtől. Tehát a képlet helyességét n-re feltéve az $\dfrac{n}{n+1}+\dfrac{1}{(n+1)(n+2)}=\dfrac{n+1}{n+2}$ egyenlőséget kell belátnunk.
Közvetlen bizonyítás: $\dfrac{1}{k(k+1)}=\dfrac{1}{k}-\dfrac{1}{k+1}$ alapján teleszkopikus összeget kapunk.

(b) Az (a)-hoz hasonlóan, az indukciós lépésben az

$$\frac{n(n+1)(2n+1)}{6}+(n+1)^2=\frac{(n+1)(n+2)(2n+1)}{6}$$

egyenlőséget kell ellenőriznünk.
Közvetlen bizonyítás: adjuk össze a $(k+1)^3-k^3=3k^2+3k+1$ egyenlőségeket $1\le k\le n$-re.

A.1.2 A felső becsléshez az indukciós lépésben elég ellenőrizni

$$2\sqrt{n}-1+\frac{1}{\sqrt{n+1}}\le 2\sqrt{n+1}-1$$

fennállását. Ehhez használjuk fel a $\sqrt{n+1}-\sqrt{n}=1/(\sqrt{n+1}+\sqrt{n})$ azonosságot. Az alsó becslést hasonlóan bizonyíthatjuk.
Közvetlen bizonyítás: becsüljük az összeget az $\int_1^n dx/\sqrt{x}$ integrállal.

A.1.3 Kövessük a P1 példa módszerét.
Közvetlen bizonyítás: mutassuk meg, hogy 8-cal osztva 5^n maradéka páros n-re 1, páratlan n-re pedig 5.

A.1.4 Az első néhány értéket kiszámolva megsejtjük, hogy $a_n=2^n-1$. Az indukciós lépésben feltesszük ennek helyességét $n-1$-re és n-re, és ebből vezetjük le $n+1$-re: $a_{n+1}=3a_n-2a_{n-1}=3(2^n-1)-2(2^{n-1}-1)=$
$=2^{n+1}-1$.
Az ilyen típusú rekurziók közvetlen megoldási módszereit a 9.2 pontban tárgyaljuk.

A.1.5 Az indukciós lépés nem működik $n=1$-ről $n+1=2$-re.

A.1.6 Válasz: $\binom{1999}{3}$.
Útmutatás: Mérjük fel a tagokat egymás után egy 2000 hosszúságú szakaszra.

A.1.7 Az elegáns bizonyítások a képlet helyett a kombinatorikai jelentésen alapulnak.
(a) Egy k elemű részhalmaz egyértelműen meghatározza az $n-k$ elemű komplementerét.
(b) Az $\{1, 2, \ldots, n+1\}$ halmaz k elemű részhalmazait aszerint osztályozzuk, hogy az $n+1$ elemet tartalmazzák-e vagy sem.
(c) Az $\{1, 2, \ldots, n+1\}$ halmaz $k+1$ elemű részhalmazait a legnagyobb elemük szerint rakjuk külön csoportokba.
(d) Van n piros és n kék golyónk, és n golyót kell közülük kiválaztani.

A.1.8
(a) Használjuk a binomiális tételt $(1-1)^n$-re és a P2 példát.
(b) Alkalmazzuk a binomiális tételt $(1-2)^n$-re.

A.1.9 .
(a) (a1) 0. (a2) $n!$.
(a3) A tulajdonságok legyenek azok, hogy bizonyos számjegyek hiányoznak a számból, és alkalmazzuk a logikai szitát. Eredményül a (b) bal oldalán álló összeget kapjuk. (Ez $k < n$ and $k = n$ esetén is érvényes, de akkor sokkal egyszerűbb a direkt meggondolás.)
(b) Az (a) rész alapján mindkét oldal az $1, 2, \ldots, n$ számjegyekből készíthető k-jegyű pozitív egészek számát adja.
Tanulság: időnként hasznos lehet valamit elbonyolítani, mert ezt a közvetlen módszerrel adódó egyszerű eredménnyel összevetve szép azonossághoz juthatunk.

A.1.10 Ekvivalenciareláció: (b), (c), (d). Ekvivalenciaosztályok:
(b) Három végtelen osztály: a 3 szerinti maradékosztályok.
(c) Megegyezik (b)-vel $4a + 5b = 3(a + 2b) + a - b$ miatt.
(d) Egy-egy osztályt alkot egy szám és a negatívja, tehát végtelen sok kételemű osztály van plusz a $\{0\}$ egyelemű osztály.

A.1.11 A gondolatmenet nem működik, ha a egyetlen elemmel sincs relációban.

A.1.12 (a) 2^{n^2}. (b) 2^{n^2-n}. (c) $2^{n(n+1)/2}$.

A.2.

A.2.1 $(2s+1)^2 - (2t+1)^2 = 4(s(s+1) - t(t+1))$, és két szomszédos egész szorzata mindig páros szám.

Másik lehetőség: a^2 maradéka csak a maradékától függ, ugyanis $(8k+r)^2 = 8(8k^2+2kr)+r^2$. Mivel $(8k\pm 1)^2 = 8L+1$ és $(8k\pm 3)^2 = = 8M+9 = 8N+1$, egy páratlan négyzetszám 8-as maradéka mindig 1. Ez a módszer a 8 helyett tetszőleges egészre és négyzetek helyett bármilyen hatványra általánosítható. A kongruenciák segítségével az eljárás még jobban formalizálható.

A.2.2 Igaz: (a), (c), (e), (h).

A.2.3 Igazoljuk az $a^n - b^n = (a-b)(a^{n-1} + a^{n-2}b + a^{n-3}b^2 + \ldots + b^{n-1})$ azonosságot, ebből kapjuk (i)-et. Ide b helyére $-b$-t írva adódik (ii) és (iii) attól függően, hogy n páratlan vagy páros.
Másik lehetőség: emeljük n-edik hatványra az $a \equiv b \pmod{a-b}$ és $a \equiv -b \pmod{a+b}$ igaz kongruenciákat.

A.2.4

(a) A $10 \equiv 1 \pmod 9$ kongruenciát hatványozva $10^k \equiv 1 \pmod 9$, és így

$$\begin{aligned}\overline{a_s a_{s-1}\ldots a_1 a_0} =& a_s 10^s + a_{s-1}10^{s-1} + \ldots + a_1 10 + a_0 \equiv \\ \equiv& a_0 + a_1 + a_2 + \ldots + a_s \pmod 9.\end{aligned}$$

Ezzel azt az általánosabb észrevételt bizonyítottuk, hogy egy pozitív egész számnak és a számjegyei összegének ugyanaz a 9-es maradéka.

(b) A $10 \equiv -1 \pmod{11}$ kongruenciával járjunk el (a)-hoz hasonlóan.

(c) A válasz (a) alapján 2^{2000}-nek a 9-es maradéka. A $2^3 \equiv -1 \pmod 9$ kongruenciát 666-odik hatványra emelve $2^{1998} \equiv 1 \pmod 9$ adódik, tehát a keresett maradék $1 \cdot 4 = 4$.

(d) Indukcióval is célhoz érhetünk, de egyszerűbb, ha kongruenciákat használunk: $36 \equiv -7$ és $49 \equiv 6 \pmod{43}$, tehát

$$6^{n+2} + 7^{2n+1} = 36 \cdot 6^n + 7 \cdot 49^n \equiv -7 \cdot 6^n + 7 \cdot 6^n = 0 \pmod{43}.$$

A.2.5 Igaz : (a), (d), (e), (h).

A.2.6 Az állítás igaz 11111 helyett tetszőleges $n > 0$ egészre. Az n-nel való osztásnál n maradék lehetséges, ezért a skatulyaelv alapján a sorozat végtelen sok a_i elemének ugyanaz lesz a maradéka. Ezek közül bármelyik kettő különbsége osztható n-nel.

A.2.7. Mivel n lehetséges maradék van, ezért a szóban forgó összeg

$$\begin{aligned}S =& k_0 n + (k_1 n + 1) + (k_2 n + 2) + \ldots + (k_{n-1} n + n - 1) = \\ =& kn + (1 + 2 + \ldots + (n-1)) = kn + n(n-1)/2.\end{aligned}$$

Ha n páratlan, akkor $(n-1)/2$ egész szám, így S osztható n-nel, tehát a maradék 0. Ha n páros, akkor

$$n(n-1)/2 = n^2/2 - n/2 = n((n/2)-1) + (n/2),$$

vagyis a maradék $n/2$.

A.2.8

(a) Lehetséges $n = 99$-re, pl. ha mindenki helyezési száma megegyezik a rajtszámával.

(b) Nem fordulhat elő $n = 100$-ra. Legyen az i-edik versenyző helyezési száma h_i, rajtszáma r_i és ezek összege $t_i = r_i + s_i$. Az A.2.7 feladat szerint $\sum_{i=1}^{100} r_i \equiv \sum_{i=1}^{100} s_i \equiv 50 \pmod{100}$, így $\sum_{i=1}^{100} t_i \equiv 0 \pmod{100}$. Ha a t_i-k maradékai mind különbözők, akkor $\sum_{i=1}^{100} t_i \equiv 50 \pmod{100}$, ami ellentmondás.

A.2.9

(a) Egyszerű és természetes eljárás adódik ha m páratlan vagy osztható 4-gyel. Az $m = 4k+2$ esetben az összes ugrások száma páratlan lenne, ez tehát nem lehetséges.

(b) Páratlan m-re működik az (a)-beli természetes algoritmus. Páros m-re nem tudnak összegyűlni, ehhez cimkézzük meg a fákat sorban az $1, 2, \ldots, m$ számokkal, és tekintsük az $S_k = j_1 + \ldots + j_m$ összeg maradékát modulo m, ahol j_i annak a fának a sorsszáma, ahová az i-edik mókus a k-adik lépés után kerül. Mutassuk meg, hogy S_k nem változik az ugrálás során, de a kezdeti értéke különbözik attól, amikor az összes mókus egy fán található.

A.2.10

(a) Egy p^k prímhatvány esetén $(c, p^k) = 1$ akkor és csak akkor teljesül, ha c nem osztható p-vel. Az $1, 2, \ldots, p^k$ egészek között a p-nek p^{k-1} többszöröse van: $p, 2p, 3p, \ldots, p^k = p^{k-1}p$. Így $\varphi(p^k) = p^k - p^{k-1}$.

(b1) $n = 1, 2$.

(b2) $n = 2^k p_1 \ldots p_r$ ahol $k \geq 0$, $r \geq 0$ és p_i különböző $2^s + 1$ alakú prímek.

A.2.11 Válasz: 49.
Útmutatás: Az utolsó két jegy egy modulo 100 kongruenciát jelent. Mivel $(1357, 100) = 1$, az Euler–Fermat-tétel szerint $1357^{k\varphi(100)} \equiv 1 \pmod{100}$.

A.2.12 Ha egy $p = 4k-1$ prímre $n^2 \equiv -1 \pmod{p}$, akkor a kongruenciát a $(p-1)/2$-edik hatványra emelve ellentmondásra jutunk az Euler–Fermat-tétellel.

A.2.13 $x \equiv 3 \pmod{11}$.

A.2.14 Válasz: 496.
Útmutatás: A modulo 1000 kongruencia helyett tekintsük a megfelelő szimultán kongruenciarendszert modulo 125 és modulo 8. Egy c^k hatványt modulo egy p^s prímhatvány nézve a k kitevőt az Euler–Fermat-tétellel tudjuk redukálni, ha $(c, p^s) = 1$, illetve $c^k \equiv 0 \pmod{p^s}$, ha $p \mid c$ és $k \geq s$.

A.2.15 Válasz: 36.
Útmutatás: Az $x^2 \equiv x \pmod{10^{20}}$ kongruencia helyett tekintsük a megfelelő prímhatvány modulusokra vonatkozó szimultán kongruenciarendszert. Lássuk be, hogy az $x(x-1) \equiv 0$ kongruenciának bármely prímhatvány modulus esetén csak 2 megoldása van.

A.2.16 A.2.8 Tétel: Ha (x, y) megoldás, akkor (A, B) osztja A-t és B-t, így $(A, B) \mid Ax + By = C$. A megfordításhoz használjuk fel az euklideszi algoritmus következményét, hogy az lnko előáll $(A, B) = Au + Bv$ alakban alkalmas u és v egészekkel. Ez egyben hatékony algoritmust is szolgáltat egy (x_0, y_0) megoldás megkereséséhez. Utána ellenőrizzük, hogy a képlet további megoldásokat szolgáltat. Annak igazolásához, hogy nincs más megoldás, vegyünk egy (x, y) megoldást:

$$\begin{aligned} Ax + By = Ax_0 + By_0 &\iff A(x - x_0) = B(y_0 - y) \iff \\ &\iff \frac{A}{(A,B)}(x - x_0) = \frac{B}{(A,B)}(y_0 - y), \end{aligned}$$

és használjuk fel, hogy $A/(A, B)$ és $B/(A, B)$ relatív prímek.

A.2.9 Tétel: Alakítsuk át a lineáris kongruenciát lineáris diofantikus egyenletté a tétel kimondása után jelzett módon.

A.2.10 Tétel: A feltétel átírható az $x = m_1 y_1 + c_1 = m_2 y_2 + c_2$ alakba. Alkalmazzuk az A.2.8 Tételt a második egyenlőségből adódó lineáris diofantikus egyenletre.

A.3.

A.3.1 Válaszok: (a) $3 + 2i$. (b) $-i$. (c) $\pm(3 - 2i)$.
(d) $\sqrt{2}e^{i(1+4k\pi)/12}$, $0 \leq k \leq 5$. (e) $\sqrt[10]{12}e^{i(7+12k\pi)/30}$, $0 \leq k \leq 4$.
Útmutatás (c)-hez:

$$5 - 12i = (x + yi)^2 \iff x^2 - y^2 = 5, 2xy = -12, \text{ ahol } x, y \in \mathbf{R}.$$

(Ez a módszer nem működik általában n-edik gyökökre, mert nem létezik megoldóképlet a négynél magasabb fokú egyenletekre.)

A.3.2 A $z = a + bi$ algebrai alak alapján koordinátageometriai feladatokról van szó. A keletkező egyenletek és egyenlőtlenségek kezelésénél figyeljünk arra, hogy végig ekvivalens lépéseket végezzünk. Sokszor azonban egyszerűbb és elegánsabb a közvetlen geometriai interpretációt használni.

(a) A feltétel $3 - 5b = 7$, innen $b = -4/5$. Ez egy vízszintes egyenes az x-tengely alatt $4/5$ egységgel.

(b) A feltétel $-2b + 5 > 9$, innen $b < -2$. Ez egy nyitott félsík, amelyet felülről az x-tengely alatt 2 egységgel haladó vízszintes egyenes határol.

(c) A z pont távolsága a $(3, -8)$ ponttól kisebb vagy egyenlő, mint 1. Ez tehát egy $(3, -8)$ középpontú és 1 sugarú zárt körlap.

(d) Ha $z \neq 0$, akkor a feltétel $\sin(\arg z) = 1/2$, tehát $\arg z = \pi/6$ vagy $5\pi/6$. Így két, az origóból induló zárt félegyenest kapunk.

(e) A z az $5i$ ponntól legalább olyan messze van, mint a $-i$ ponttól. Ez tehát egy, a $-i$-t tartalmazó zárt félsík, amelyet az $5i$ és $-i$ szakaszfelező merőlegese, a $b = 2$ vízszintes egyenes határol.

(f) Ha $z \neq 0$, akkor a trigonometrikus alakból $\pi/4 - \arg z = \arg z + 2k\pi$, $k \in \mathbf{Z}$, azaz $\arg z = \pi/8 + k\pi$ adódik. Ez tehát egy, az origón átmenő egyenes.

(g) A feltétel szerint a tört valós része 0. A $z = a + bi$ alakból az osztás elvégzése után $\dfrac{(a+1)(a+3)+b^2}{(a+3)^2+b^2} = 0$ adódik. Itt a számláló akkor és csak akkor 0, ha $(a+2)^2 + b^2 = 1$. Ez tehát egy $(-2, 0)$ középpontú és 1 sugarú körvonal a $z = -3$ (vagy $(-3, 0)$) pont nélkül, hiszen a nevező nem lehet 0.
Másik lehetőség: A tört szöge, vagyis a számláló és nevező szögének a különbsége $\pm\pi/2$, tehát a -1-ből z-be mutató vektor merőleges a -3-ból a z-be mutató vektorra. Ez azt jelenti, hogy az $A = (-1, 0)$, $B = (-3, 0)$ és $C = z$ csúcsú háromszögben C-nél derékszög van. Thalész tétele szerint a C pontok egy körön helyezkednek el, amelynek középpontja az AB szakasz felezőpontja és átmérője ez a szakasz. Az A pontot be kell vennünk, a B-t azonban ki kell zárnunk.

A.3.3 Válaszok: (a) $\pm 2\sqrt{2}i$. (b) $-1 \pm i$. (c) $1 - 2i$ és $-2 + i$.
Útmutatás: (b)-nél és (c)-nél használjuk a másodfokú egyenlet megoldóképletét.

A.3.4 Használjuk a $z_j = a_j + b_j i$ algebrai alakot vagy a $|w|^2 = w \cdot \overline{w}$ azonosságot.
Geometriai jelentés: Egy paralelogrammában az oldalak négyzetösszege megegyezik az átlók négyzetösszegével.

A.3.5 Útmutatás: $a^2+b^2=|a+bi|^2$ és $|z|\cdot|w|=|zw|$.
Másik lehetőség: az $(a^2+b^2)(c^2+d^2)=(ac)^2+(bd)^2+(ad)^2+(bc)^2$ egyenlőség jobb oldalán adjunk hozzá az első két tag összegéhez egy új tagot, majd ugyanezt vonjuk le az utolsó két tag összegéből úgy, hogy a keletkező háromtagú összegek teljes négyzetek legyenek.
A megfordítás hamis, például $3\neq a^2+b^2$, de $3\cdot 3=3^2+0^2$ (vagy $3\cdot 75=9^2+12^2$).
A három négyzetszámra vonatkozó analóg állítás hamis, például $3=1^2+1^2+1^2$ and $5=2^2+1^2+0^2$, de $15\neq a^2+b^2+c^2$.

A.3.6 Válaszok: (a) $(-4,3)$. (b) $\big((3-4\sqrt{3})/2,(4+3\sqrt{3})/2\big)$.
Útmutatás: Szorozzuk meg $3+4i$-t i-vel, illetve $e^{i\pi/3}$-mal. Általánosan, egy w komplex számmal történő szorzás geometriai jelentése az origóból történő $\arg w$ szögű forgatva nyújtás $|w|$-szeresre.

A.3.7 A $z_j=a_j+b_ji$ algebrai alakot használva a tört valós része pontosan akkor 0, ha $|z_1|=|z_2|$.
Egy egyszerű geometriai bizonyítás: a paralelogramma átlói akkor és csak akkor merőlegesek egymásra, ha az oldalak egyenlők, azaz a paralelogramma rombusz.

A.3.8 Válasz: $16(\sin x)^5-20(\sin x)^3+5\sin x$.
Útmutatás: Legyen $z=\cos x+i\sin x$, és számítsuk ki z^5-t kétféleképpen; a trigonometrikus alakból és a binomiális tétellel. Hasonlítsuk össze a képzetes részeket és írjunk $(\cos x)^2$ helyére $1-(\sin x)^2$-et.

A.3.9

(b) Válasz: $2^{n/2}\cos(n\pi/4)$.
Útmutatás: Hasonlítsuk össze az (a)-ban kapott kétféle előállítás valós részét.

A.3.10 (a) $1,(-1\pm i\sqrt{3})/2$. (b) $\pm1,(\pm1\pm i\sqrt{3})/2$.

A.3.11

(a) Ha $z^n=w^k=1$, akkor $(zw)^{[n,k]}=(z/w)^{[n,k]}=1$.
Másik lehetőség: Használjuk az egységgyököknek az abszolút értékükkel és szögükkel történő jellemzését.

(b) Válasz: A két szög különbsége $\pm2\pi/3$.
Útmutatás: A két egységgyök által kifeszített rombusz két oldala és rövidebb átlója egyenlő oldalú háromszöget alkot.

A.3.12 Ha $w=e^{2\pi i/n}$, akkor $1,w,w^2,\dots,w^{n-1}$ az összes n-edik egységgyök.
Összeg: $S_n=\sum_{k=0}^{n-1}w^k=(w^n-1)/(w-1)=0$, ha $n>1$.
Szorzat: $P_n=\prod_{k=0}^{n-1}w^k=w^{n(n-1)/2}$. Így $P_n=(w^n)^{(n-1)/2}=1$, ha n páratlan, és $P_n=(w^{n/2})^{n-1}=(-1)^{n-1}=-1$, ha n páros.

Másik lehetőség: Egy n-edik egységgyök reciproka is az. A szorzat tényezőit párosítsuk ennek megfelelően: $z \cdot (1/z) = 1$. Külön kell vizsgálnunk a $z = 1/z$ vagyis $z^2 = 1$ esetet, ez $z = \pm 1$-et jelenti. Mivel $(-1)^n = 1$ pontosan a páros n-ekre igaz, ezért a szorzat páratlan n-re 1, páros n-re pedig -1.

A.3.13

(a) $(z^t)^s = 1 \iff z^{ts} = 1 \iff k = o(z) \mid ts \iff k/(k,t) \mid s$, tehát a legkisebb s kitevő $k/(k,t)$.

(b) Lásd az A.3.11a feladat útmutatását.

A.3.14

(a) Válasz: 1, ha $n \neq 2$, és -1, ha $n = 2$.
Útmutatás: képezzünk $z, 1/z$ párokat.

(b) Jelölje T_n a primitív n-edik egységgyökök összegét. Ekkor $T_7 = -1$, $T_{27} = 0$ és $T_n = (-1)^r$, ha az n szám r különböző prímszám szorzata, $T(1) = 1$, és $T_n = 0$ minden más n-re.

A.3.15 Legyenek a négyszög csúcsai az óramutató járásával ellentése körüljárás szerint az A, B, C és D komplex számok, és legyen O_1 az AB oldalra támaszkodó négyzet középpontja. Az $\overrightarrow{AO_1}$ vektorhoz úgy jutunk, hogy az $\overrightarrow{AB}$ vektort $-\pi/4$-gyel elforgatjuk, és a hosszát $\sqrt{2}$-vel elosztjuk. Ez az $e^{-i\pi/4}/\sqrt{2} = (1-i)/2$-vel történő szorzásnak felel meg. Mivel $\overrightarrow{AB} = B - A$ és $\overrightarrow{AO_1} = O_1 - A$, ezért

$$O_1 = (O_1 - A) + A = \frac{(B-A)(1-i)}{2} + A = \frac{B(1-i)}{2} + \frac{A(1+i)}{2}.$$

A másik három négyzet középpontját hasonló módon kifejezve, az $O_4 - O_2 = i(O_3 - O_1)$ egyenlőséget kell ellenőriznünk.

A.3.16 Válasz: $\dfrac{\sin(nx/2)\cos((n+1)x/2)}{\sin(x/2)}$, ha $x \neq 2m\pi$, és n, ha $x = 2m\pi$ valamilyen m egész számra.
Útmutatás: Ha $z = \cos x + i \sin x$, a $\sum_{k=1}^{n} z^k$ mértani sorozat összegének valós részét kell mghatároznunk. A szebb alakhoz érdemes ezt $w = \cos(x/2) + i \sin(x/2)$ segítségével átírni.
Másik lehetőség: Sorozzuk meg az összeget $\sin(x/2)$-lel és alkalmazzuk a $\sin\beta\cos\alpha = \dfrac{\sin(\alpha+\beta) - \sin(\alpha-\beta)}{2}$ azonosságot.

A.4.

A.4.1 Nem művelet: (b1), (d3), (d4), (e2), (i3).

Kommutatív: (a1), (a2), (b2), (c1), (c2), (c3), (d1), (d2), (e1), (f1), (f2), (g), (h), (i2).

Asszociatív: (a1), (a2), (b2), (c1), (c2), (c3), (d1), (d2), (e1), (e3), (f1), (f2), (i1), (i2).

Egységelem és inverz:

(a1) $e = 0$ és minden elemnek van inverze.
(a3) a 0 jobb oldali egységelem.
(b2) $e = 1$ és csak a ± 1-nek van inverze.
(c1) és (c3): $e = 1$ és csak az 1-nek van inverze.
(d3) $e = 0$ és minden elemnek van inverze.
(e1) és (e3): e a helybenhagyás és minden elemnek van inverze.
(f1) $e = \emptyset$ és csak az e-nak van inverze.
(f2) $e = \emptyset$ és minden elem önmaga inverze.
(h) $e = 5$, az 5 inverze önmaga, és az összes többi elem közül mindegyik inverze mindegyiknek.
(i1) Minden olyan mátrix bal oldali egységelem, amelynek a bal felső eleme 1.
(i2) $e = \begin{pmatrix} 1/2 & 1/2 \\ 1/2 & 1/2 \end{pmatrix}$ és minden nem nulla mátrixnak van inverze.

A.4.2 Az egységelem az identitás (amely minden elemnek önmagát felelteti meg). Kétoldali inverze pontosan a *bijekció*knak (az X halmazt önmagára kölcsönösen egyértelmű módon leképező függvényeknek) létezik. Az aszszociativitás miatt az inverz egyértelmű. Véges X esetén más függvénynek nincs bal- vagy jobbinverze sem. A továbbiakban legyen $|X| = \infty$, és az f és g függvények fg kompozíciója a szokásos módon jelentse azt, hogy először a g-t alkalmazzuk és utána az f-et. Ekkor balinverze pontosan az *injektív* függvényeknek létezik (azoknak a függvényeknek, amelyeknél különböző elemek képe különböző), és (a bijekciókon kívül) minden ilyen függvénynek végtelen sok balinverze van. Hasonlóan, jobbinverze pontosan a *szürjektív* függvényeknek létezik (azoknak a függvényeknek, amelyeknél X minden eleme fellép képként), és (a bijekciókon kívül) minden ilyen függvénynek végtelen sok jobbinverze van.

A.4.3 Műveletek száma: mind az n^2 elempárhoz n-féle értéket rendelhetünk, tehát n^{n^2} művelet értelmezhető.
Kommutatív műveletek száma: mivel az a, b és b, a elempárhoz ugyanazt rendeljük, ezért $n + \binom{n}{2} = n(n+1)/2$ elempáron választhatjuk meg

szabadon a függvényértéket (a többi helyen a hozzárendelés ezekből már egyértelműen adódik), tehát $n^{n(n+1)/2}$ kommutatív művelet értelmezhető.
Egységelemes műveletek száma: az egységelem az n elem bármelyike lehet, ezután az ezzel akármelyik oldalról történő szorzás egyértelműen meghatározott, a maradék $(n-1)^2$ elempáron viszont tetszőleges a hozzárendelés, így n^{n^2-2n+2} egységelemes művelet értelmezhető.
Mindezeket a *műveleti tábl*áról is kényelmesen leolvashatjuk. Legyenek X elemei $a_1, \ldots, a_n$, és készítsünk el egy $n \times n$-es táblázatot, amelynek a felső és bal oldali margójára írjuk fel rendre az a_i elemeket, és a táblázat i-edik sorának j-edik eleme legyen $a_i a_j$ (azaz a megfelelő sorban és oszlopban álló elemek szorzata). A művelet megadását a tábla kitöltése jelenti. Minden helyre az X halmaz n eleme közül bármelyiket beírhatjuk, n^2 darab hely van, tehát a lehetőségek száma n^{n^2}. A művelet kommutativitását az jelzi, hogy a műveleti tábla a főátlóra szimmetrikus, az egységelem pedig onnan látszik, hogy ennek az elemnek a sora és oszlopa megegyezik a felső, illetve bal oldali margóval.
Megjegyezzük még, hogy a műveletek összeszámolásánál két műveletet akkor is különbözőnek tekintettünk, ha az elemek alkalmas permutálásával egymásba vihetők (ezek tulajdonképpen „ugyanolyan" műveletek, csak a halmaz elemei másképp vannak indexezve — a kétféle művelet által létrehozott algebrai struktúra *izomorf*).

A.4.4 $(ab)^{-1} = b^{-1}a^{-1}$.
A megfordítás hamis, ellenpéldát (többek között) az A.4.2 feladat felhasználásával készíthetünk.

A.4.5 Csak (d) igaz.

A.4.6
(a) Lásd pl. az A.4.2 feladatot.
(b) Legyen a tetszőleges és b az a-nak egy balinverze, azaz $ba = e$. Elég megmutatni, hogy b az a-nak jobbinverze is, mert ekkor az asszociativitás miatt $b = a^{-1}$ és a-nak nem lehet más balinverze sem. Az $ab = e$ igazolásához legyen c a b-nek egy balinverze és számítsuk ki kétféleképpen a $cbab$ szorzatot.
(c) Az egységelemnek önmaga az egyetlen bal-, illetve jobbinverze.
(d) Lásd pl. az A.4.1h feladatot.

A.4.7 Ekkor csak arra következtethetünk, hogy az $xb = a$ egyenletnek legalább egy, a $by = a$ egyenletnek pedig legfeljebb egy megoldása létezik.

A.4.8 Alkalmazzuk az A.4.7 Tétel II., majd I. állítását.

A.4.9 Az A.4.1 feladat (h), illetve (g) része ellenpélda I.-re, illetve II.-re.

A.5.

A.5.1 Test: (a2), (b1), (c2), (d2), (d3), (d5).

A.5.2 Csak $m = 3$-ra kapunk testet.

A.5.3 Test: (a), (c), (d), (e), (g).

A.5.4

(a) Az F_p-k közül bármely kettőnek az elemszáma különböző és véges, tehát ezek a testek sem egymással, sem pedig egy végtelen testtel nem lehetnek izomorfak (hiszen még bijekció sem létesíthető). A racionális számok halmaza megszámlálható, a valós, illetve komplex számoké viszont ennél nagyobb számosságú, tehát $\mathbf{Q}$ és $\mathbf{R}$, illetve $\mathbf{Q}$ és $\mathbf{C}$ között sem létezik bijekció. Végül az $\mathbf{R}$ és $\mathbf{C}$ testek (noha a két halmaz között megadható bijektív megfeleltetés) azért nem izomorfak, mert a szorzás számos tulajdonsága eltér, pl. az egységelem negatívjából (azaz a -1-ből) $\mathbf{C}$-ben lehet négyzetgyököt vonni, $\mathbf{R}$-ben viszont nem.

(b) A.5.1: F_5-tel izomorf (b1); $\mathbf{R}$-rel izomorf (c2), (d2), (d3); $\mathbf{C}$-vel izomorf (d5).
A.5.3: $\mathbf{R}$-rel izomorf (a), (c), (d), (e); $\mathbf{C}$-vel izomorf (g).

A.5.5

(a) Pl. vehetjük a $T_p = \{a + b\sqrt{p} \,|\, a, b \in \mathbf{Q}\}$ résztesteket, ahol p végigfut a (pozitív) prímeken.

(b) A feltételezett résztest egy tetszőleges nem nulla elemét önmagával elosztva megkapjuk az egységelemet, és az egységelemből kiindulva a négy alapművelettel a $\mathbf{Q}$, illetve F_p test minden eleméhez eljutunk.

(c) Mutassuk meg, hogy az egységelemből kiindulva a négy alapműveletet segítségével mindig egy résztesthez jutunk, és ez a résztest $\mathbf{Q}$-val vagy valamelyik F_p-vel izomorf.

(d) F_p-ben bármely elemet p-szer összeadva mindig a nullelemet kapjuk, ugyanakkor $\mathbf{R}$-ben a 0-n kívül egyetlen ilyen tulajdonságú elem sem található.

Megjegyzés: ez a példa jól illusztrálja, hogy egy testnek lehet olyan részhalmaza, ami test, mégsem résztest. A $H = \{0, 1, 2, \ldots, p-1\}$ halmaz részhalmaza $\mathbf{R}$-nek, és ha a H halmazon az összeadást, illetve a szorzást mint a számok összegének, illetve szorzatának a modulo p vett (legkisebb nemnegatív) maradékát értelmezzük, akkor egy testet kapunk, amely izomorf F_p-vel. A H tehát a valós számoknak egy olyan részhalmaza, amely az így definiált összeadásra és szorzásra nézve testet alkot. Ez azonban $\mathbf{R}$-nek *nem részteste*, ugyanis ebben a testben másképp végezzük a műveleteket, mint a valós számok körében, hiszen pl. $p = 7$-re most $3 + 5 = 1$, míg az $\mathbf{R}$ testben $3 + 5 = 8$. (A fenti okoskodást azért nem

mondtuk el közvetlenül az F_p-re és azért kellett a H halmaz „közvetítő” szerepét igénybe vennünk, mert maga az F_p nem igazán tekinthető az $\mathbf{R}$ részhalmazának sem. Az F_p elemei ugyanis tulajdonképpen *nem* számok, hanem inkább maradékosztályok, azaz az F_p minden egyes eleme egy egész számokból álló végtelen halmaz.)

A.5.6 Csak a (c) esetben kaphatunk testet. Útmutatás:

(a) Mivel a szorzás a szokásos, ezért (pl.) a 2-nek nem lesz multiplikatív inverze.

(b) Legyen $1 \odot 1 = c$ és mutassuk meg, hogy ekkor $a \odot b = abc$. Innen leolvasható, hogy ha $c \neq \pm 1$, akkor nincs egységelem, ha pedig $c = \pm 1$, akkor a legtöbb elemnek nincs inverze.

(c) Használjuk fel, hogy az egész számok és a racionális számok között bijekció létesíthető.

A.6.

A.6.2

(a) (A): ± 1. (B): amelyekre $a^2 - 2b^2 = \pm 1$. (C): $\pm 1, \pm i$.
(D): a nem nulla konstans polinomok. (E): ± 1.

(b) Azoknak a sorozatoknak van inverze, amelyeknek egyik eleme sem nulla, a többi sorozat pedig a csupa nulla sorozat kivételével nullosztó. Hasonló a helyzet a valós függvényeknél is: azoknak van inverze, amelyek sehol sem veszik fel a 0 értéket, a többi függvény pedig az azonosan nulla függvény kivételével nullosztó.

(c) Válasz: a $\{\ldots, -127, -27, 73, 173, \ldots\}$ maradékosztály.
A $37x \equiv 1 \pmod{100}$ lineáris kongruenciát (vagy a vele ekvivalens $37x - 100y = 1$ lineáris diofantikus egyenletet) kell megoldani.

A.6.3 A nullelemet eleve kizártuk a nullosztók közül és inverze sem lehet, ezért csak a nem nulla elemek vizsgálatára szorítkozunk.
A.5.1: (a1) Nullosztómentes, inverze azoknak a törteknek van, amelyeknek a számlálója is páratlan. — (b2) Minden elem nullosztó, nincs egységelem. — (c1) Azok a függvények nullosztók, amelyeknek a 0-n kívül más gyöke is van, a többi függvénynek pedig létezik inverze. — (d1) Itt bármely két elem szorzata nulla, tehát minden elem nullosztó és nincs egységelem. — (d4) Nincs egységelem (de bal oldali egységelem végtelen sok van, mégpedig azok a mátrixok, amelyekre $a + b = 1$). Minden elem jobb oldali nullosztó, a bal oldali nullosztók pedig azok a mátrixok, amelyekre $a + b = 0$.

A.5.2: (a) Inverze az 1-nek és az i-nek van, az $1+i$ pedig nullosztó. — (c) Azok lesznek nullosztók, amelyekre $5 \mid a^2+b^2$ (nyolc darab ilyen nem nulla elem van), a többi (tizenhat) elemnek pedig létezik inverze.
A.5.3: (f) Az $a+bi$ akkor nullosztó, ha a és b közül (pontosan) az egyik nulla, a többi elemnek létezik inverze.

A.6.4 Az $ab = a(b+0) = ab + a0$ egyenlőséghez adjuk hozzá ab ellentettjét, és használjuk fel az összeadás asszociativitását.

A.6.5 (b) Az utolsóból következik a másik kettő. (Az ilyen tulajdonságú gyűrűket *Boole-gyűrű*knek nevezzük.)

A.6.6 $c \neq 0$ és c nem bal oldali nullosztó.
Ennek alapján egy nullosztómentes gyűrűben (így egy testben vagy az egész számok körében is) bármely nem nulla elemmel lehet egyszerűsíteni, a modulo m maradékosztályok körében pedig pontosan a redukált maradékosztályokkal. [Ez utóbbi annak az átfogalmazása, hogy a $ca \equiv cb \pmod{m}$ kongruenciából a $(c,m)=1$ feltétel mellett következik $a \equiv b \pmod{m}$.]

A.6.7 Igaz: (a), (d).

A.6.8 Ha a gyűrű egy nem nulla elemét a gyűrű összes elemével (valamelyik oldalról) végigszorozzuk, akkor a nullosztómentesség miatt csupa különböző elemet kapunk. Így a végesség miatt ezek a gyűrű minden elemét kiadják. Ez éppen azt jelenti, hogy az $xb = a$ és $by = a$ egyenletek bármely $b \neq 0$ és a esetén egyértelműen megoldhatók.

A.6.9 Legyen c az egyetlen bal oldali egységelem. Azt kell igazolnunk, hogy bármely b esetén $bc = b$, azaz $bc - b = 0$ is teljesül. Ehhez lássuk be, hogy $c + bc - b$ is bal oldali egységelem, majd használjuk fel, hogy csak egyetlen bal oldali egységelem létezik.

A.6.10 Legyen az R gyűrű nulleleme 0_R, az S részgyűrűé pedig 0_S, és vegyünk egy tetszőleges $s \in S$ elemet. Ekkor $s = 0_R + s = 0_S + s$. A második egyenlőség mindkét oldalához az s elem R-beli(!) ellentettjét (jobbról) hozzáadva az asszociativitás felhasználásával a jobb oldalon

$$(0_S + s) + (-s) = 0_S + \big(s + (-s)\big) = 0_S + 0_R = 0_S,$$

a bal oldalon pedig ugyanígy 0_R adódik.
Megjegyzés: vegyük észre, hogy a bizonyításhoz erősen felhasználtuk az ellentettet is!

A.6.11 Csak (c) igaz.
Az (a) állítást pl. az A.6 pont P4 példájában szereplő (rész)gyűrűk, a (b) állítást pedig az A.5.1 feladat (b1), (d2) vagy (d3) konstrukciója segítségével cáfolhatjuk meg.

A (c) igazolásához legyen e_R, illetve e_S az R, illetve S egységeleme és vegyünk egy tetszőleges $s \neq 0$ elemet az S-ből. Ekkor $s = e_R s = e_S s$ és (az R-beli!) nullosztómentesség miatt itt s-sel egyszerűsíthetünk.

A.6.12 Először lássuk be, hogy a gyűrű nullosztómentes. Ennek felhasználásával mutassuk meg, hogy egy tetszőleges $b \neq 0$ elemet véve az $xb = b$ egyenlet (egyik) $x = e$ megoldása egy jobb(!) oldali egységelem. Ekkor $be = b$ alapján ugyanígy következik, hogy e bal oldali egységelem is. Ezután az $xb = e$ egyenlet (egyik) $x = c$ megoldása a b-nek balinverze. Azt, hogy $bc = e$ is teljesül, többféleképpen is igazolhatjuk, lássuk be például, hogy $(e - bc)b = 0$ és használjuk fel a nullosztómentességet.

A.7.

A.7.1

(a) Végtelen sok polinom van, de csak véges sok (polinom)függvény.

(b) Ha az $f \neq g$ polinomokhoz ugyanaz a polinomfüggvény tartozik, akkor bármely h és t polinomokra h-hoz és $h + t(f - g)$-hez is ugyanaz a polinomfüggvény tartozik.
Másik lehetőség: h-hoz és $h + t\prod_{\gamma\in T}(x-\gamma)$-hoz ugyanaz a polinomfüggvény tartozik.

A.7.2 Ha a nullosztómentesség feltételét elejtjük, akkor csak II. marad igaz. (A III.-ra könnyen találunk ellenpéldát a modulo m maradékosztályok feletti polinomok, azaz az összetett modulusú kongruenciák körében.)

A.7.3

(b) Pl. az $f = x$ és $g = \prod_{0\neq\gamma\in T}(x - \gamma)$ szorzata a nulla polinom*függvény*.

(c) Használjuk fel a 3.2.14 feladatot is. Válasz: $|T|^{|T|} - (|T| - 1)^{|T|} - 1$.

A.7.4 Pl. bármely olyan nem azonosan nulla függvény megfelel, amelynek végtelen sok gyöke van.

A.7.5 Tekintsük G-t az F_{11} test feletti polinomnak.

A.7.6

(a) Az egyeleműek, a $H^a = \{x \geq a\}$ és $H_a = \{x \leq a\}$ típusú részhalmazok, valamint a teljes $\mathbf{R}$. (Szemléletesen fogalmazva: a számegyenesen a pontok, a zárt félegyenesek és maga a számegyenes.)

(b) Csak az egyelemű részhalmazok és a teljes $\mathbf{C}$. (Használjuk fel az algebra alaptételét.)

A.7.7

(a) Helyettesítsünk be a polinomfüggvénybe egy tetszőleges egész számot és módosítsuk a_0-t úgy, hogy a helyettesítési érték nulla legyen.

(b) Most egy egész szám reciprokát helyettesítsük be.

(c) Egyrészt el tudjuk érni, hogy az 1 gyök legyen, másrészt viszont csak véges sok racionális gyök jöhet szóba.

(d) Az (a) és (b) mintájára most tetszőleges racionális szám behelyettesítésével célhoz érünk.

(e) Végtelen sokféleképpen el tudjuk érni, hogy az 1 gyök legyen.

(f) A (c) alapján elég csak az $i = 0$ és $i = n$ esettel foglalkoznunk. Ezek is visszavezethetők egymásra az $x \mapsto 1/x$ helyettesítéssel. Ezután az $i = 0$ eset igazolásához okoskodjunk indirekt. Gondoljuk meg, hogy (a_0-tól függetlenül) milyen alakú racionális számok lehetnek gyökök, és fogalmazzuk át az indirekt feltételt arra, hogy ekkor az ilyen alakú racionális számokat a $g = a_1x+a_2x^2+\ldots+a_nx^n$ polinomfüggvénybe behelyettesítve véges sok kivételtől eltekintve minden egész számot meg kellene kapnunk. Használjuk ki, hogy elég nagy x-re a $g(x)$ függvényérték konstansszor x^n nagyságrendű, és így az összes $|g(x)| < M$ függvényérték előállításához lényegében csak az $|x| < cM^{1/n}$ számok jöhetnek szóba (ahol c egy M-től független konstans). Ezek az x-ek azonban (ha M-et megfelelően választjuk) „kevesen" vannak ahhoz, hogy a $g(x)$ helyettesítési értékek majdnem az összes, M-nél kisebb abszolút értékű egész számot kiadják.

A.7.8 Mutassuk meg, hogy f-nek és f'-nek nincs közös gyöke.

A.7.9 Keressük meg (a negyedfokú) f' gyökeit, ezek valamelyike gyöke f-nek is, és ezzel a gyöktényezővel f-et (akár kétszer) leosztva a hányados már (ötnél) alacsonyabb fokú.

Elegánsabb és gyorsabb, ha euklideszi algoritmussal meghatározzuk f és f' legnagyobb közös osztóját, ennek a $d = (f, f')$ polinomnak a gyökei éppen f többszörös gyökei az eredetinél eggyel kisebb multiplicitással. Ennek megfelelően az f/d polinom gyökei megegyeznek f gyökeivel, de mindegyik gyök most egyszeres. Így $g = (d, f/d)$ gyökei az f többszörös gyökei, de egyszeres multiplicitással. Ezután rendre g, d/g és pl. $f/(dg)$ gyökeit meghatározva megkapjuk f gyökeit és azok multiplicitását.

A.7.10 $d = (f, f') \mid f$, $\deg d < \deg f$, így az irreducibilitás miatt d csak konstans lehet.

A.7.11 Az előző két feladathoz hasonló gondolatmenetet kell alkalmazni.

A.7.12 $f = \alpha_n(x - \gamma)^n$.

A.7.13 Igaz: (a), (c).

A.7.14

(a) A $\mathbf{Q}$ és $\mathbf{C}$ feletti oszthatóság ekvivalens. Az egészek feletti oszthatóságból bármelyik másik következik, de ennek a megfordítása egyik esetben sem igaz („univerzális" ellenpélda: $f = 3x$ és $g = 5x$). Az F_2 és a $\mathbf{Q}$, illetve $\mathbf{C}$ feletti oszthatóság között nincs kapcsolat.

(b) Ekkor a $\mathbf{Q}$, a $\mathbf{C}$ és az egészek feletti oszthatóság ekvivalens és ezekből következik az F_2 feletti oszthatóság, de a megfordítás nem igaz. (A változásnál csak az játszott szerepet, hogy f főegyüttható 1 lett.)

A.7.15 Mutassuk meg, hogy a bal oldal (komplex) gyökei a jobb oldalnak is (legalább ugyanannyiszoros) gyökei.
Másik lehetőség: a jobb oldalt írjuk át

$$(x^{3m} - 1) + x(x^{3n} - 1) + x^2(x^{3k} - 1) + (x^2 + x + 1)$$

alakba.
Harmadik lehetőség: alkalmazzunk teljes indukciót (pl.) $m+n+k$ szerint.
Megjegyzés: az előző feladat szerint ez az oszthatóság egyformán érvényes $\mathbf{Q}[x]$-ben, $\mathbf{C}[x]$-ben vagy az egész együtthatós, sőt akár az F_2 test feletti polinomok körében.

A.7.16 Válasz: $x^{(n,k)} - 1$.
Megjegyzés: Itt is mindegy, hogy a két polinom legnagyobb közös osztóját a racionális, a valós vagy a komplex test fölött nézzük, sőt ez megegyezik az egészek vagy akár az F_2 felett vett lnko-val is (bár az utóbbi két állítás nem teljesen nyilvánvaló).
Többféle megoldáshoz is adunk útmutatást:
(A) A komplex test felett okoskodva a közös (komplex) gyöktényezőket kell kiválasztani.
(B) Gondoljuk végig, hogy a megadott két polinomra elvégzett euklideszi algoritmus lépései éppen a kitevőkkel (az egész számok körében) végzett euklideszi algoritmus lépéseinek felelnek meg.
(C) Közvetlenül belátható, hogy $x^{(n,k)} - 1$ valóban közös osztó. Legyen most h egy tetszőleges közös osztó, ekkor $h \mid (x^{un} - 1) - (x^{vk} - 1) = x^{vk}(x^{un-vk} - 1)$, ahonnan u és v alkalmas megválasztásával kapjuk, hogy $h \mid x^{(n,k)} - 1$.
(D) Használjuk fel a körosztási polinomokat.

A.7.17 Nincs. A tizedfokú polinomból a feltételezett közös maradékot levonva egy olyan tizedfokú polinomot kapnánk, amely a két polinomnak közös többszöröse lenne. A relatív prímség miatt azonban a két polinomnak már a legkisebb közös többszöröse is tizenegyedfokú.

A.7.18 Mivel a T feletti polinomok számelmélete a maradékos osztás megléte miatt teljesen analóg az egész számok számelméletével, így a feladatra adott válasz és annak igazolása is teljesen ugyanaz, mint az egész számok körében vizsgált („igazi") diofantikus egyenleteknél. A megoldhatóság szükséges és elégséges feltétele: $(f, g) \mid h$, a megoldásszám végtelen, egy u_0, v_0 megoldást (pl.) az euklideszi algoritmusból nyerhetünk, és az összes megoldást az $u = u_0 + wg/(f, g)$, $v = v_0 - wf/(f, g)$ képlet szolgáltatja, ahol $w \in T[x]$ tetszőleges polinom.

A.7.19 Mindkét állítás hamis. Az I. igazzá válik, ha feltesszük, hogy $\deg f \geq 2$. A II. viszont csak a $\deg f = 2$ vagy 3 esetben lesz igaz.

A.7.20

(a) $\mathbf{C}[x]$-ben: $\prod_{k=1}^{4}(x - \vartheta_k)$, ahol $\vartheta_k = e^{i(2k+1)\pi/4}$.
(b) $\mathbf{R}[x]$-ben: $(x^2 + x\sqrt{2} + 1)(x - x\sqrt{2} + 1)$.
(c) $\mathbf{Q}[x]$-ben: irreducibilis $(= \Phi_8)$.
(d) $F_2[x]$-ben: $(x + 1)^4$.
(e) $F_3[x]$-ben: $(x^2 + x - 1)(x^2 - x - 1)$.

A.7.21 Keressünk olyan c-t, amelyre az $x^4 + c$ polinom reducibilis $\mathbf{Q}$ felett. Arra is vigyázni kell, nehogy olyan c-t válasszunk, amellyel valamilyen n-re az egyik tényező helyettesítési értéke ± 1, a másiké pedig egy prímszám.

A.7.22 Irreducibilisek: (a), (c), (d).

A.7.23 Ha $(x - a_1) \cdot \ldots \cdot (x - a_k) - 1 = gh$, ahol a II. Gauss-lemma alapján feltehető, hogy g és h egész együtthatós, akkor bármely i-re $g(a_i)h(a_i) = -1$, tehát $g(a_i) + h(a_i) = 0$, $i = 1, 2, \ldots, k$. Ha a felbontás nem volt triviális, akkor $\deg(g + h) < k$, tehát csak $g + h = 0$, azaz $g = -h$ lehetséges. Ekkor viszont gh főegyütthatója negatív lenne, ami ellentmond a kiindulási feltételnek.

A.7.24 Ha m páros, akkor $\Phi_{2m}(x) = \Phi_m(x^2)$, ha pedig m páratlan, akkor $\Phi_{2m}(x) = \Phi_m(-x)$ [illetve $m = 1$ esetén $-\Phi_m(-x)$].

A.7.26

(a) Azok az $5k$-adik komplex egységgyökök, amelyek *nem* k-adik egységgyökök is egyúttal.
(b) $k = 5^s$, $s = 0, 1, 2, \ldots$

A.7.27 n.

A.7.28 A megadott negatív szám a gyökök négyzetösszege.

A.7.29 $2b^3 - 9abc + 27a^2d = 0$.
Útmutatás: a gyökök összegét érdemes nézni. (Ne felejtsük el *mindkét* irányt igazolni!)

A.7.30 Az összes többi együttható 0.
Útmutatás: vizsgáljuk a gyökök szorzatát, majd osszunk le az így adódó egyik gyöktényezővel, és ismételjük meg az eljárást.

A.8.

A.8.1 Tetraéder: 24, kocka és oktaéder: 48, dodekaéder és ikozaéder: 120.
Útmutatás: vizsgáljuk meg, hogy két szomszédos csúcs hány helyre kerülhet és az ő helyzetük mennyire határozza meg a test elhelyezkedését. Meg kell még mutatnunk, hogy az így kiszámolt valamennyi lehetőség valóban meg is valósul alkalmas egybevágósági transzformációkkal.
Megjegyzés: A kocka és oktaéder, illetve a dodekaéder és ikozaéder esetén nemcsak az elemszámok azonosak, hanem a két csoport izomorf is. Ez egyszerűen igazolható közvetlen geometriai megfontolásokkal, ha a két testet egymáshoz viszonyítva ügyesen helyezzük el.

A.8.2 A kérdéses $abab = aabb$ egyenlőséget balról a^{-1}-gyel, jobbról b^{-1}-gyel beszorozva egy vele ekvivalens egyenlőséget kapunk.
Kommutatív csoportban nyilván lehet tényezőnként negyedik hatványra (is) emelni, a megfordítás azonban nem igaz, tekintsük pl. D_4-et.

A.8.4 Lehet, vegyünk például a síkon két olyan tengelyes tükrözést, ahol a tengelyek (fokban mérve) irracionális szöget zárnak be egymással. (Az előző feladat szerint csak nem kommutatív csoportban találhatunk ilyen elemeket.)

A.8.5 Igaz: (a), (c).

A.8.6 Megfelelő G csoport megfelelő g elemére alkalmazzuk az $o(g) \,\big|\, |G|$ összefüggést.

A.8.7 Ha a csoportban pontosan egy másodrendű elem van, akkor a csoportelemek szorzata ezzel egyenlő, egyébként pedig az egységelemmel.
Ha speciálisan G a modulo p maradékosztályok multiplikatív csoportja, akkor ez éppen a Wilson-tétel.
Útmutatás: Párosítsunk minden elemet az inverzével. Gondot okoz, ha több másodrendű elem is van, ekkor ezek körében csináljunk egy másféle párosítást.

A.8.8 Valamennyi csoport 8 elemű, azonban öt különböző „típusú” van közöttük: ab — chj — de — f — gi. [Tehát pl. (c), (h) és (j) közül bármelyik kettő izomorf, de ezek nem izomorfak a többi csoport egyikével sem.]
A nem-izomorfak megkülönböztetése valamilyen eltérő műveleti tulajdonság alapján történhet (pl. kommutativitás, elemek rendje), az izomorfak

„azonosításához" pedig mutassuk meg, hogy mindkét csoportban pontosan „ugyanazok a számolási szabályok" (ha másképp nem megy, akkor írjuk fel és hasonlítsuk össze a két műveleti táblát).
Megjegyzés: Belátható, hogy „másféle" 8 elemű csoport nem is létezik, azaz minden 8 elemű csoport a megadott csoportok valamelyikével izomorf.

A.8.9

(a) Először lássuk be, hogy egy ilyen csoport szükségképpen kommutatív. Ezután mutassuk meg, hogy az elemei $e, a, b, ab, c, ac, bc, abc, \ldots$ formában állíthatók elő. Végül ennek alapján igazoljuk, hogy egy ilyen csoport szerkezetileg szükségképpen azonos egy, az F_2 feletti véges dimenziós vektortér additív csoportjával.

(b) Ellenpélda: legyen G_1 az F_3 test feletti 3 dimenziós vektortér additív csoportja és G_2 az (ugyancsak az) F_3 feletti, olyan 3×3-as felsőháromszögmátrixok multiplikatív csoportja, amelyekben a főátló mindhárom eleme 1.

A.8.10

(a) Válasz: amelyek elemszáma 1 vagy prím.
Útmutatás: az egyik irányhoz használjuk a Lagrange-tételt, a másik irányhoz tekintsünk ciklikus részcsoportokat.

(b) Válasz: a véges csoportok.
Útmutatás: Azt kell igazolni, hogy egy végtelen csoportban mindig végtelen sok részcsoport van. Két esetet különböztessünk meg aszerint, hogy van-e a csoportban végtelen rendű elem vagy nincs, és a gondolatmenethez most is ciklikus részcsoportokat vegyünk igénybe.

A.8.11 A téglalap szimmetriacsoportja megfelel. Páratlan elemszámú csoport nem lehet ilyen, ennek igazolásához használjuk fel a Lagrange-tételt.

A.8.12

(a) Válasz: $d(n)$, azaz n pozitív osztóinak a száma.
Útmutatás: mutassuk meg, hogy a részcsoportok is ciklikusak, és választható bennük olyan g^d generátorelem, ahol $d \mid n$ (itt g az eredeti csoport valamelyik rögzített generátorelemét jelöli).

(b) $d(n) + \sigma(n)$, ahol $\sigma(n)$ az n pozitív osztóinak az összege.

A.8.13 Ha $M = gH$ és $a, b, c \in M$, akkor $ab^{-1}c = (gh_1)(gh_2)^{-1}(gh_3) = = gh_1h_2^{-1}g^{-1}gh_3 = gh_1h_2^{-1}h_3 = gh_4 \in M$. A megfordításhoz lássuk be, hogy a feltétel teljesülése esetén a $\{b^{-1}c \mid b, c \in M\}$ halmaz részcsoport.

A.9.

A.9.1 Az ideálok pontosan az additív csoport részcsoportjai lesznek.

A.9.2 Akkor és csak akkor kapunk ideált, ha m prímhatvány. (Ez igaz a prímek első hatványára, azaz magukra a prímekre is, ekkor a nulla ideálról van szó, hiszen a modulo p maradékosztályok körében nincsenek nullosztók.)

A.9.3

(a) Ha i_j eleme az I_j ideálnak, akkor a $\prod_j i_j$ szorzat eleme az I_j ideálok metszetének.

(b),(c) Az A.9.1–A.9.2 feladatok a segítségünkre lehetnek ilyen példák konstrukciójánál.

A.9.4

(a) Használjuk fel, hogy ha $a \neq 0$, akkor ra alakban a test minden eleme előáll.

(b) Bármely $b \in R$-re az $I_b = \{rb \mid r \in R\}$ halmaz ideál, tehát a feltétel szerint $I_b = 0$ vagy $I_b = R$. Mutassuk meg, hogy azok a $b \in R$ elemek, amelyekre $I_b = 0$, szintén egy I ideált alkotnak, így $I = 0$ vagy $I = R$. Az utóbbi esetben R bármely két elemének a szorzata nulla lenne, tehát $I = 0$. Ez az előbbiekkel együtt azt jelenti, hogy bármely $b \neq 0$-ra az rb alakú elemek az egész R-et kiadják, azaz lehet osztani és így R test.
Megjegyzések: A kommutativitást ott használtuk ki lényegesen, hogy az I_b halmaz valóban ideál. Az I_b helyett azért nem írhattunk eleve (b)-t, mert egységelem létezését nem tettük fel, és így előfordulhatott volna, hogy $b \notin I_b$ (például zérógyűrűben valóban ez a helyzet), amikor is jogtalan lenne a „b által generált ideál" elnevezés.

(c) Legyen I egy nem nulla ideál, azt kell igazolni, hogy I az összes mátrixot tartalmazza. Induljunk ki egy tetszőleges $A \neq 0$, $A \in I$ mátrixból, és ezt szorozzuk meg balról, majd jobbról egy-egy olyan mátrixszal, amelyben csak egyetlen helyen áll nem nulla elem. Lássuk be, hogy az ily módon kapott mátrixok összegeként minden mátrixot elő tudunk állítani. Mivel ezek a lépések nem vezettek ki az ideálból, adódik, hogy I valóban csak a teljes $T^{n\times n}$ mátrixgyűrű lehet.

A.9.5

(a) Válasszuk minden modulo m maradékosztályból a legkisebb nemnegatív reprezentánst (azaz a $0, 1, \ldots, m-1$ maradékokat), ekkor egy nem nulla ideál generátorelemének megfelel az ideál legkisebb pozitív eleme.

(b) A feltétel az, hogy k és m/k relatív prímek legyenek.

(c) Lássuk be, hogy a (k) főideál szerinti maradékosztályokat egyértelműen jellemezhetjük a $0, 1, \ldots, k-1$ „maradékokkal", és ezekkel éppen úgy kell végezni a műveleteket, ahogyan „modulo k számolunk" velük.

A.9.6 A.9.3 Tétel: A kommutativitást az (i), az egységelemet a (ii) tulajdonság igazolásánál kell felhasználni.

A.9.4 Tétel: Egy nem nulla ideál generátorelemének az egész számok esetén válasszuk az ideál (egyik) legkisebb abszolút értékű, a polinomok esetén pedig (egyik) legkisebb fokszámú nem nulla elemét. A bizonyításnál használjuk fel a maradékos osztást.

A.9.5 Tétel: A fő nehézséget annak az igazolása jelenti, hogy noha az osztályokra a műveleteket a reprezentánsok segítségével definiáltuk, az eredmény független a reprezentánsok választásától. Az azonosságok, illetve kitüntetett elemek létezése az eredeti gyűrű megfelelő tulajdonságaiból következik.

A.9.6 Tétel: Ha $g = 0$, akkor $T[x]/(g)$ izomorf $T[x]$-szel, ha g egység, akkor $T[x]/(g)$ egyedül a nullelemből áll, tehát ezekben az esetekben nem test. Ha g reducibilis, $g = rs$, ahol $\deg r < \deg g$, $\deg s < \deg g$, akkor az $r + (g)$ és $s + (g)$ maradékosztályok egyike sem a nulla maradékosztály, azonban a szorzatuk $\big(r+(g)\big)\big(s+(g)\big) = g+(g) = (g)$, ami a faktorgyűrű nulleleme, vagyis a faktorgyűrűben nullosztók vannak, tehát semmiképpen sem lehet test. Végül megmutatjuk, hogy ha g irreducibilis, akkor valóban testet kapunk. A szorzás kommutatív, egységelem az $1 + (g)$ maradékosztály, tehát azt kell még belátni, hogy ha $h + (g)$ nem a nulla maradékosztály, akkor létezik inverze. A feltétel azt jelenti, hogy $h \notin (g)$, azaz $g \nmid h$. A $h + (g)$ inverze egy olyan $u + (g)$ maradékosztályt jelent, amelyre $\big(h + (g)\big)\big(u + (g)\big) = 1 + (g)$, azaz alkalmas v polinommal $hu+vg = 1$ teljesül. Mivel a g irreducibilitása és $g \nmid h$ miatt g és h relatív prímek, így ennek a (polinomokra vonatkozó) „diofantikus" egyenletnek létezik u, v megoldása (lásd az A.7.18 feladatot).

A.9.7 Az A.9.3 Tétel megfelelője röviden így foglalható össze: $(a_1, \ldots, a_k)$ az a_i elemeket tartalmazó legszűkebb ideál.

A.9.8

(a) Az (A) főideál az A részhalmazaiból áll.

(b) Legyen I ideál, $A = \cup_{B\in I} B$, ekkor $I = (A)$.

(c) Az (a) részből következik, hogy ez nem főideál. Végesen generált pedig azért nem lehet, mert a (b) rész mintájára igazolható, hogy R_H-ban minden végesen generált ideál szükségképpen főideál.

(d) Lássuk be, hogy az R_H gyűrű két eleme, azaz H két részhalmaza pontosan akkor kerül az (A) főideál szerint ugyanabba a maradékosztályba, ha a két szóban forgó részhalmaznak az „A-n kívül eső része" azonos. Ennek megfelelően minden maradékosztály egyértelműen jellemezhető $H \setminus A$ egy részhalmazával. Ne felejtsük el a művelettartást is ellenőrizni!

A.9.9

(a) $I = (6)$, azaz I a 6-tal osztható számokból áll, R/I pedig a modulo 6 maradékosztálygyűrű.

(b) $I = (2)$, azaz I a modulo 100 „páros" maradékosztályokból áll, R/I pedig (izomorf) az F_2 test(tel).

(c) I-t azok a(z egész együtthatós) polinomok alkotják, amelyeknek a konstans tagja páros szám. Megmutatjuk, hogy I nem főideál. Tegyük fel indirekt, hogy $I = (g)$, ekkor $g \mid 2$ és $g \mid x$ teljesül, azaz g (az egész együtthatós polinomok körében) közös osztója a 2 és az x polinomoknak. Ezért csak $g = \pm 1$ lehet, azonban $\pm 1 \notin I$, hiszen a ± 1 polinomok konstans tagja páratlan. Ez az ellentmondás biztosítja, hogy I nem főideál. Az R/I faktorgyűrűt úgy kapjuk, hogy az egész együtthatós polinomoknak vesszük a „maradékait mind a 2, mind pedig az x szerint". Így összesen a 0 és az 1 által reprezentált maradékosztályok lesznek különbözők és R/I izomorf F_2-vel.

A.9.10

(c) Az $(a) \subseteq (a, b) = (d)$ tartalmazásból az (a) rész alapján $d \mid a$ következik, és $d \mid b$ is hasonlóan adódik, tehát d közös osztója a-nak és b-nek. Legyen most c tetszőleges közös osztó, azaz $c \mid a$ és $c \mid b$. Mivel $d \in (d) = (a, b)$, így d felírható $d = au + bv$ alakban, ahonnan kapjuk, hogy $c \mid d$ is teljesül.

(d) Használjuk fel, hogy az a és b legnagyobb közös osztója felírható $au + bv$ alakban.

(e) Ellenpéldát kaphatunk pl. az A.9.9c feladatból.

A.9.11 $|R/I| = 16$ és R/I izomorf az F_2 test feletti 2×2-es mátrixok gyűrűjével.

A.9.12

(a) Azok a függvények vannak az (f) főideálban, amelyeknek minden, 5-nél kisebb valós szám gyöke.

(b) Az R gyűrű két eleme, azaz két valós függvény akkor és csak akkor kerül az (f) főideál szerint ugyanabba a maradékosztályba, ha a két szóban forgó függvénynek minden $x < 5$-re ugyanaz a helyettesítési értéke (a többi helyettesítési érték „nem számít"). Ennek megfelelően minden maradékosztály egyértelműen jellemezhető az 5-nél kisebb helyeken felvett függvényértékekkel. A művelettartás ellenőrzése után így azt kapjuk, hogy az $R/(f)$ faktorgyűrű izomorf az 5-nél kisebb valós számokon értelmezett valós függvények szokásos gyűrűjével. Végül ez utóbbi azért izomorf magával az R-rel, azaz az összes valós függvények gyűrűjével, mert a két értelmezési tartomány (vagyis az 5-nél kisebb valós számok halmaza, illetve az összes valós számok halmaza) között bijekció létesíthető.

A.9.13 Igaz: (a), (c).

A.9.14 Test: (c), (d). (Használjuk az A.9.6 Tételt.)

A.10.

A.10.1 Az algebraiság és $\deg\Theta \le n$ igazolásához használjuk fel, hogy az $1, \Theta, \Theta^2, \dots, \Theta^n$ elemek biztosan lineárisan összefüggők, $\deg\Theta \mid n$ bizonyításánál pedig alkalmazzuk a fokszámtételt és az A.10.11 Tételt.

A.10.2 Az M test nullosztómentes, ugyanakkor $\operatorname{Hom} V$-ben vannak nullosztók.

A.10.3 A.10.3 Tétel: Legyen M-nek L feletti bázisa $\Theta_1, \dots, \Theta_m$, N-nek M feletti bázisa $B_1, \dots, B_n$, ekkor lássuk be, hogy a $\Theta_i B_j$ elemek az N-nek L feletti bázisát adják. Ne felejtsük el a végtelen dimenziós esetet is meggondolni.

A.10.5 Tétel: (i) Azt kell igazolni, hogy $L(\Theta)$ zárt az (M-beli) összeadásra, szorzásra, ellentett- és reciprokképzésre nézve. Nézzük például az összeadást:

$$g_1(\Theta)/h_1(\Theta) + g_2(\Theta)/h_2(\Theta) = [(g_1h_2 + g_2h_1)(\Theta)]/[(h_1h_2)(\Theta)].$$

(ii) Ha $g = x$, $h = 1$, akkor $g(\Theta)/h(\Theta) = \Theta$. $L \subseteq L(\Theta)$ hasonlóan igazolható.
(iii) Mivel T test, ezért T-nek a Θ-val és az L elemeivel együtt az ezekből a „négy alapművelet" segítségével előálló elemeket is tartalmaznia kell.

A.10.8 Tétel: (ii) Ha $f = m_\Theta g$, akkor $f(\Theta) = m_\Theta(\Theta)g(\Theta) = 0 \cdot g(\Theta) = 0$. A megfordításhoz tegyük fel, hogy $f(\Theta) = 0$, és írjuk fel f-nek az m_Θ-val való maradékos osztását: $f = m_\Theta h + r$, ahol $\deg r < \deg m_\Theta$ vagy $r = 0$. Ekkor $r(\Theta) = f(\Theta) - m_\Theta(\Theta)h(\Theta) = 0 - 0 = 0$, és így a minimálpolinom definíciója miatt csak $r = 0$ lehetséges.
(iii) Ha indirekt $m_\Theta = gh$, ahol $\deg g < \deg m_\Theta, \deg h < \deg m_\Theta$, akkor $0 = m_\Theta(\Theta) = g(\Theta)h(\Theta)$, és M nullosztómentessége miatt $g(\Theta) = 0$ vagy $h(\Theta) = 0$, de mindkettő ellentmond a minimálpolinom definíciójának.
(iv) A (ii) alapján $m_\Theta \mid f$, továbbá m_Θ nem konstans, így az f irreducibilitása miatt m_Θ csak az f (konstansszorosa) lehet.

A.10.10 Tétel: Ha egy elemnek többféle ilyen előállítása lenne, akkor ezeket egymásból kivonva azt kapnánk, hogy Θ gyöke egy legfeljebb $n-1$-edfokú polinomnak, ami ellentmondás. Azt, hogy létezik ilyen előállítás, két lépésben bizonyítjuk: (i) $g(\Theta)/h(\Theta)$ alkalmas $f \in L[x]$ polinommal átírható $f(\Theta)$ alakba; (ii) elérhető $\deg f < n$ is. Az (i) igazolásához lássuk be, hogy $g(\Theta)/h(\Theta) = f(\Theta)$ *ekvivalens* a $g = hf + m_\Theta u$ „diofantikus" egyenlettel, ami megoldható, mert h és m_Θ relatív prímek. (ii) Legyen f-nek az m_Θ-val való osztási maradéka r, ekkor $f(\Theta) = r(\Theta)$.

A.10.12 Tétel: Az $\alpha_0+\alpha_1\Theta+\ldots+\alpha_{n-1}\Theta^{n-1}$ elemekkel pontosan ugyanúgy kell számolni, mint az m_Θ polinom szerinti osztási maradékokkal.

A.10.4 Egy $g\neq 0$ racionális együtthatós polinomnak minden gyöke definíció szerint algebrai szám, tehát ez g bármely osztójára is teljesül. Megfordítva, ha f minden gyöke algebrai szám, akkor megfelelő g-t kapunk, ha vesszük az f gyökei minimálpolinomjainak a szorzatát.

A.10.5 $\sqrt[k]{\Theta}$ gyöke az $f(x)=m_\Theta(x^k)$ polinomnak.

A.10.6 Azt kell igazolni, hogy két algebrai szám összege és szorzata, valamint egy algebrai szám ellentetteje és reciproka is algebrai. Nézzük például az összeget. Ha Θ és Ψ algebrai, akkor legyen $M=\mathbf{Q}(\Theta)$, $N=M(\Psi)$, ekkor $\Theta+\Psi\in N$. Ezután alkalmazzuk a fokszámtételt és az A.10.11 Tételt.

A.10.7 Egy algebrai és egy transzcendens szám összege mindig transzcendens, két transzcendens szám összege lehet algebrai is és transzcendens is (mutassunk mindkét esetre példát).

A.10.8

(a) (i) Mindkét szám transzcendens.
(ii) Mindkét szám transzcendens, vagy pedig az egyik 0 és a másik transzcendens.
(iii) Legalább az egyik szám transzcendens (mutassunk példát, amikor mindkettő transzcendens, illetve amikor csak az egyik az).
(iv) Mindkét szám algebrai.
Útmutatás (iv)-hez: fejezzük ki az eredeti számokat S-sel és P-vel.

(b) Csak (iv)-nél van változás, itt előfordulhat az is, hogy a két eredeti szám (speciális) irracionális szám.
Megjegyzés: az eltérés oka az, hogy (i)–(iii) esetén csak a testtulajdonságok játszottak szerepet, (iv)-nél viszont a (négyzet)gyökvonás is.

A.10.9

(a) Ha a és b algebrai, akkor mivel i algebrai és algebrai számok összege és szorzata is az, ezért $a+bi$ is algebrai. Megfordítva, tegyük fel, hogy $z=a+bi$ algebrai, először lássuk be, hogy $\overline{z}=a-bi$ is az (ugyanaz a minimálpolinomja), ezután fejezzük ki a-t és b-t z-vel és $\overline{z}$-vel.

(b) Használjuk fel az (a) részt, valamint azt, hogy ha $\cos\varphi$ és $\sin\varphi$ közül az egyik algebrai, akkor szükségképpen a másik is az.

A.10.10 Transzcendens: (c), (d), a többi algebrai. A fokszámok: (a) 100; (b) 4; (e) 3; (f) 3; (g) Az 1 foka 1, a többié 100; (h) A ±1 foka 1, a többié 2; (i) $\varphi(n)$; (j) 48.
Útmutatás: (b)-nél és (e)-nél kevés számolással is célhoz érhetünk, ha a fokszámtételt felhasználjuk; (j)-nél alkalmazzunk az A.10.12 feladat megoldásához hasonló gondolatmenetet.

A.10.11 Van.
Útmutatás: Az egységgyökök minimálpolinomjai a körosztási polinomok, amelyek egész együtthatósak és a főegyüttható 1, ugyanakkor könnyen készíthető olyan 1 abszolút értékű komplex szám, amelynek nincs ilyen alakú minimálpolinomja.

A.10.12 Csak a ± 1 ilyen.
Útmutatás: Legyen $z = \cos\varphi + i\sin\varphi$. Mutassuk meg, hogy $\mathbf{Q}(z)$-nek eleme $\overline{z} = 1/z$ és így $\cos\varphi$ és $i\sin\varphi$ is. Legyen $M = \mathbf{Q}(\cos\varphi)$ és $N = M(i\sin\varphi)$, ekkor $N = \mathbf{Q}(z)$ és $\deg(N : M) = 2$.

A.10.13 Válasz: $\deg(\Theta^2) = k$ vagy $k/2$.
Útmutatás: $\mathbf{Q} \subseteq \mathbf{Q}(\Theta^2) \subseteq \mathbf{Q}(\Theta)$ és itt a második bővítés legfeljebb másodfokú.

A.10.14
(a) $\sqrt{18}/\sqrt{8}$ racionális szám.
(b) Mutassuk meg, hogy a jobb oldal része a metszetnek, majd használjuk a fokszámtételt.

A.10.15 Legyen $\Psi = 1+3\sqrt[7]{25}+11\sqrt[7]{125}+1000\sqrt[7]{625}$. Ekkor $\Psi \in \mathbf{Q}(\sqrt[7]{5})$, és mivel a 7 prím, továbbá $\Psi \notin \mathbf{Q}$, ezért $\mathbf{Q}(\Psi) = \mathbf{Q}(\sqrt[7]{5})$, így $\sqrt[7]{5} \in \mathbf{Q}(\Psi)$.

A.10.16 Használjuk fel, hogy $|z| = 1$ esetén $\operatorname{Re} z = (z + 1/z)/2$. Ne feledkezzünk el arról az esetről sem, amikor z transzcendens.

A.10.17 Vegyük azt a bővítésláncot, ahol $\mathbf{Q}$-t egymás után bővítjük a polinom együtthatóival, majd a végén az egyik gyökével.

A.10.18 Az A.10.12 Tétel alapján legyen $M = L[x]/(f)$. Ekkor M az A.9.6 Tétel szerint test, továbbá a konstans$+(f)$ maradékosztályok halmaza megfelel L^*-nak, az $x + (f)$ maradékosztály pedig Θ-nak.

A.11.

A.11.1 Vegyük észre, hogy a binomiális együtthatók annyiszor történő összeadást jelentenek, továbbá mindegyik 1-nél nagyobb binomiális együttható osztható p-vel.

A.11.2 A szorzat értéke -1 (ez $p = 2$ esetén ugyanaz, mint az 1). Az összeg a kételemű test kivételével 0.
Útmutatás: A szorzatnál párosítsunk minden elemet az inverzével és használjuk ki, hogy legfeljebb egy darab másodrendű elem van. (A párosítás helyett az elemeket a generátorelem hatványaiként felírva is célhoz érünk.) Az összegnél páratlan p esetén párosítsunk minden elemet az ellentettjével, p=2-re pedig tekintsük a vektorteres felírást (ez utóbbi páratlan p-re is alkalmazható).

A.11.3 Válasz: $(m, p^k - 1)$.
Útmutatás: A gyökök azok a Θ-k, amelyekre $o(\Theta) \mid m$. Használjuk ki azt is, hogy $o(\Theta) \mid p^k - 1$.

A.11.4 Válasz: 1, ha k páratlan, és 3, ha k páros (a (Θ, Ψ) és (Ψ, Θ) párt ugyanannak tekintjük).
Útmutatás: vezessük vissza az előző feladatra.

A.11.5

(a) Ha $0 = a + a + \ldots + a$, akkor ezt tetszőleges b-vel beszorozva $0 = (a + a + \ldots + a)b = ab + ab + \ldots + ab = a(b + b + \ldots + b)$ adódik, és mivel $a \neq 0$, ezért a második tényező 0. Ebből következik, hogy ha egy nem nulla elemet k-szor összeadva nullát kapunk, akkor ugyanez valamennyi nem nulla elemre érvényes. Tekintsük a legkisebb ilyen k-t. Ha k összetett lenne, $k = rs$, ahol $r < k, s < k$, akkor a k darab a összegét bontsuk r hosszúságú csoportokra és jussunk ellentmondásra. Tehát a legkisebb ilyen k egy p prím. Több prím azért nem jöhet szóba, mert minden más k ennek a minimális darabszámnak a többszöröse.

(b) Tekintsük pl. az F_p test feletti polinomhányadosokat (algebrai törteket).

A.11.6 F_{13}, illetve F_3 felett keresendő egy-egy irreducibilis polinom, amelynek a foka 2, illetve 4.

A.11.7 A multiplikatív csoportra alkalmazzuk a Lagrange-tételt, és ebből olvassuk le, hogy a nem nulla elemek valóban gyökei a megadott polinomnak (a nulla meg nyilvánvalóan gyök). A polinomnak ezzel megkaptuk annyi (különböző) gyökét, mint amennyi a foka, tehát több gyök nem lehet.

A.11.8 A „csak akkor" részhez használjuk fel az előző feladatot és azt, hogy a p^k elemű test bármely elemének a foka osztója k-nak. A megfordításnál induljunk ki az $F_p[x]/(f)$ testből.

A.11.9 Az állítás lényegében ekvivalens az előző feladattal.

A.11.10 Tekintsük a test multiplikatív csoportját, és használjuk fel, hogy egy (véges) ciklikus csoport bármely két (különböző) részcsoportja különböző elemszámú.

A.11.11 Tekintsük A-t egy $\mathcal{A}$ lineáris transzformáció mátrixának, és mutassuk meg, hogy az $\mathcal{A}$ minimálpolinomja éppen f (vö. a 6.3.18 feladattal). Ennek megfelelően az A mátrix hatványai „ugyanúgy viselkednek", mint az $F_p[x]/(f)$ faktorgyűrűben az x maradékosztály hatványai.

A.11.12

(a) $\varphi(p^k-1)/k$.

(b) Válasz: $(1/k)\sum_{d\,|\,k}\mu(d)p^{k/d}$, ahol $\mu(n)$ a *Möbius-függvény*: $\mu(1)=1$, $\mu(n)=(-1)^s$, ha az n szám s darab különböző prím szorzata és $\mu(n)=$ $=0$ minden más n-re.
Megjegyzés: Általánosan is, egy tetszőleges q elemű véges test felett a k-adfokú irreducibilis polinomok számára ugyanez a képlet érvényes, csak p helyére q-t kell írni. A bizonyítás is teljesen analóg a $q=p$ esettel.
Útmutatás (b)-hez: Jelöljük a keresett darabszámot I_k-val. Az A.11.8 feladat alapján $x^{p^k}-x$ az összes olyan d-edfokú, F_p felett irreducibilis polinom szorzata, ahol $d\,|\,k$. Ebben az egyenlőségben a két oldal fokszámát összehasonlítva, I_k-ra egy rekurzív összefüggést kapunk. Innen I_k-t az ún. Möbius-féle megfordítási formulával fejezhetjük ki.

A.11.13

(a) A két egyenes közös pontja egy olyan egydimenziós altér, amely benne van a két kétdimenziós altér metszetében. Mivel a vektortér háromdimenziós, ez a metszet nem lehet nulla, tehát maga a metszet egy egydimenziós altér. Hasonlóképpen, a két pontot tartalmazó egyenes a két egydimenziós altér által generált (kétdimenziós) altér lesz.

(b) Pontok: az egydimenziós altereknek a nullvektoron kívüli részei $p-1$ eleműek és diszjunktak, a számuk tehát $(p^3-1)/(p-1)=p^2+p+1$. Egyenesek: a kétdimenziós U altereknek bijektíven megfeleltethetők az $U^\perp$ egydimenziós alterek (vö. az A.41.14 feladattal), vagy közvetlenül is leszámolhatók a bázisok szerint. (A pontokra és az egyenesekre vonatkozó állítás is a 4.6.14 feladat speciális esete.)

(c) A (b) részhez hasonló gondolatmenetet kell alkalmazni.

A.11.14 Az előző feladatra úgy vezethető vissza, hogy minden egyenest most a „normálvektorával” jellemeztünk, azaz egy kétdimenziós U altér helyett az egydimenziós $U^\perp$-t vettük.

MEGOLDÁSOK

1. Determinánsok

• **1.1.5(b)** *Válasz*: $2\lceil (n-4)/5\rceil + 1$, ahol $\lceil x\rceil$ az x szám felső egész részét jelenti, azaz a legkisebb olyan egész számot, amely $\geq x$.

Bizonyítás: Egy rögzített permutációban tekintsünk egy $a < b$ elempárt, és jelöljük $m(a,b)$-vel azoknak a c elemeknek a számát, amelyek a és b között helyezkednek el és amelyekre $a < c < b$. Az ilyen c-ket az adott cserénél fontos elemeknek fogjuk nevezni. [Pl. a 3165472 permutációban $m(2,6) = 2$, mert az 5 és a 4 a fontos elemek.] Ekkor az a és b cseréjénél az inverziószám $2m(a,b)+1$-gyel változik, ugyanis az a-nak és a b-nek az egymáshoz és a fontos elemekhez való viszonya változik meg.

Legyen egy adott permutációban M az összes $m(a,b)$ érték maximuma. A bizonyítandó állítás az előzőek alapján azzal ekvivalens, hogy (i) bármely permutációra $M \geq \lceil (n-4)/5\rceil$, és (ii) van olyan permutáció, amelyre $M = \lceil (n-4)/5\rceil$.

Először (i)-et igazoljuk. Vegyünk egy tetszőleges permutációt. Azzal az esettel foglalkozunk, amikor az 1 és n számok egyike sem az első vagy utolsó elem. A fennmaradó esetekben ugyanis hasonló (csak egyszerűbb) meggondolásokat kell alkalmazni (és kiderül, hogy akkor még nagyobb M adódik), ezt nem részletezzük.

Tegyük fel, hogy az első, illetve az utolsó helyen álló elem a k, illetve az r, továbbá az n (mondjuk) előrébb áll, mint az 1, azaz a permutáció $k \ldots n \ldots 1 \ldots r$ alakú.

Megmutatjuk, hogy a k, az n, az 1 és az r kivételével minden elem fontos az alábbi öt csere közül legalább az egyiknél: (A) k és n; (B) k és 1; (C) n és 1; (D) n és r; (E) 1 és r.

Valóban, a permutációban a k és az n között álló elemek közül a k-nál nagyobbak (A)-nál fontosak, a k-nál kisebbek pedig (B)-nél. Az n és az 1 között állók valamennyien fontosak (C)-nél [emellett esetleg (B)-nél és/vagy (D)-nél is]. Végül, az 1 és az r között álló elemek közül az r-nél nagyobbak (D)-nél, az r-nél kisebbek pedig (E)-nél fontosak.

Így $n-4 \leq m(k,n)+m(1,k)+m(1,n)+m(r,n)+m(1,r) \leq 5M$, ahonnan $M \geq \lceil (n-4)/5\rceil$, amint állítottuk.

Rátérve (ii)-re, nyilván elég az $n = 5t+4$ esettel foglalkozni. Könnyű ellenőrizni, hogy az (i)-beli gondolatmenet alapján megsejthető

$$3t{+}3, \ldots, 4t{+}3 \,\big|\, t{+}1, t, \ldots, 1 \,\big|\, 2t{+}3, \ldots, 3t{+}2 \,\big|\, 5t{+}4, \ldots, 4t{+}4 \,\big|\, t{+}2, \ldots, 2t{+}2$$

konstrukció egy megfelelő permutációt szolgáltat.

• **1.1.7(c)** *Válasz*: páratlan k esetén minden páros $n > k$, páros $k \neq 0$ esetén $n = 2k + 1$ kivételével minden $n > k$, $k = 0$ esetén minden $n > 0$.

Szükségesség: (i) $n > k$ nyilvánvaló. (ii) Az összes inverziószám $nk/2$, tehát páratlan k esetén n páros kell hogy legyen. (iii) Az első elem pontosan akkor áll k másikkal inverzióban, ha k darab nála kisebb van, tehát ha az első elem $k + 1$. Hasonlóan az utolsó elem $n - k$. Ez $n = 2k + 1 > 1$-re nyilván lehetetlen.

Elégségesség: Jelöljük $/s, t\backslash$-vel, ha az $1, 2, \ldots, s$ számoknak létezik olyan permutációja, amelyben minden elem pontosan t másikkal áll inverzióban. Az alábbi két összefüggést fogjuk felhasználni:

(A) $/c, k - d\backslash, /d, k - c\backslash \Rightarrow /c + d, k\backslash$;

(B) $/f, k\backslash, /g, k\backslash \Rightarrow /uf + vg, k\backslash$, ahol u, v tetszőleges pozitív egészek.

(A) igazolásához legyenek a $/c, k - d\backslash$, illetve $/d, k - c\backslash$ feltételt biztosító permutációk $i_1, \ldots, i_c$, illetve $j_1, \ldots, j_d$, ekkor megfelel a $d+i_1, \ldots, d+i_c, j_1, \ldots, j_d$ permutáció. (B) esetében az egyik kiindulási permutációt az $1, 2, \ldots, f$, majd az $f + 1, \ldots, 2f$ stb. $(u - 1)f + 1, \ldots, uf$ blokkokra, utána pedig a másikat az $uf + 1, \ldots, uf + g$ stb. blokkokra kell alkalmazni.

Az állítást k szerinti teljes indukcióval bizonyítjuk. Ha $k = 0$ vagy 1, akkor az állítás nyilvánvaló. Tegyük fel, hogy az állítás igaz minden $k' < k$-ra és tetszőleges megfelelő n-re. Tekintsük most k-t, és legyen először $k < n \leq 2k$ és kn páros. Legyen $n = c + d$, $1 \leq c, d \leq k$ és c páros (általában n-nek több ilyen $c + d$ előállítása is van). Ekkor $c > k - d$ és $d > k - c$, tehát $/c, k - d\backslash$ mindenképpen igaz és $d(k - c) \equiv kn \equiv 0 \pmod 2$ miatt $/d, k - c\backslash$ is fennáll, ezért (A) alapján $/c + d, k\backslash = /n, k\backslash$ is érvényes. (A $/d, k - c\backslash$-vel baj van, ha éppen $d = 2(k - c) + 1$, azonban ekkor vehetjük n-nek egy másik $c + d$ előállítását, illetve ha csak egy van, akkor az $/n, k\backslash$ állítás könnyen igazolható közvetlenül.) Ezután az $n > 2k$ eseteket a már bizonyított $n \leq 2k$-ból (B) felhasználásával láthatjuk be.

Megjegyezzük még, hogy (A) helyett a „fordított” permutációból adódó $/n, k\backslash \iff /n, n - 1 - k\backslash$ tulajdonsággal is dolgozhattunk volna.

• **1.4.13(a)** Ha M a nullmátrixot választja, akkor nyilván n lépésre van szükség. Megmutatjuk, hogy minden más esetben már kevesebb lépés is elég. Legyen r az a maximális szám, hogy az A mátrixból kiválasztható r oszlop és r sor úgy, hogy az ezek metszéspontjaiban álló (r^2 darab elemből képzett) $r \times r$-es determináns nem nulla. Ekkor $n - r$ lépés elegendő. Tegyük fel, hogy például a bal felső sarokban álló $r \times r$-es D_r determináns nem nulla. Vegyük ekkor a bal felső sarokban az eggyel nagyobb méretű $(r + 1) \times (r + 1)$-es D_{r+1} determinánst, és fejtsük ki az utolsó (azaz $r + 1$-edik) sora szerint. Ebben a kifejtésben $\alpha_{r+1,r+1}$ együtthatója (a sorok és oszlopok más elhelyezkedése ese-

tén esetleg előjeltől eltekintve) éppen D_r, tehát nem nulla. Ezért $\alpha_{r+1,r+1}$-et meg tudjuk úgy változtatni, hogy az így keletkező D'_{r+1} már ne legyen nulla. Most D'_{r+1}-t bővítsük ki egy $(r+2)\times(r+2)$-es determinánssá A következő sorából és oszlopából az első $r+2$ elem hozzávételével, és ismételjük meg az előző gondolatmenetet $\alpha_{r+2,r+2}$-re. Az eljárást folytatva $n-r$ lépés után egy $(n\times n$-es) nem nulla determinánsú A' mátrixot kapunk. (A megoldásban tulajdonképpen a mátrix determinánsrangját használtuk, lásd a 3.4 pontot. Ha csak azt akartuk volna igazolni, hogy n lépés mindig elég, akkor teljes indukcióval és a fenti gondolatmenet egyszerűsített változatával is célhoz érhettünk volna.)

• **(b)** Ha M olyan mátrixot választ, amelynek az első oszlopa csupa nulla, akkor n^2-n lépés kevés, ugyanis M kijelölheti a mátrix többi elemét. Indukcióval megmutatjuk, hogy n^2-n+1 lépés mindig elég. Az $n=1$ esetben ez nyilvánvaló. Legyen $n>1$, és tekintsük az M által megadott tetszőleges $n\times n$-es A mátrixot és a kijelölt n^2-n+1 helyet. Kell lennie olyan sornak, ahol C bármely elemet megváltoztathat (hiszen különben csak legfeljebb $n(n-1)$ kijelölt hely lenne), továbbá van olyan oszlop, ahol nem minden elem változtatható (hiszen a mátrixban nem minden hely van kijelölve). Ha pl. az első sor és első oszlop ilyen, akkor cserélje C az első sor első elemét 1-re, az első sor többi elemét pedig 0-ra. Mivel az első sor és oszlop összesen $2n-1$ eleme közül nem mindegyik van kijelölve, ezért az első sor és oszlop elhagyásával keletkező $(n-1)\times(n-1)$-es B mátrixban legalább $(n^2-n+1)-(2n-2)=(n-1)^2-(n-1)+1$ kijelölt hely van. Az indukció alapján B átalakítható nem nulla determinánsú B' mátrixszá. Legyen most A' az az $n\times n$-es mátrix, amelynek első sora A első sorából a korábban jelzett változtatással keletkezik, első oszlopa az első elemtől eltekintve megegyezik A első oszlopával, a többi elemet pedig B' alkotja. Ekkor A'-t az első sor szerint kifejtve kapjuk, hogy $\det A'=\det B'\neq 0$.

• **(ca)** Azonos az 1.2.7 feladattal.

• **(cb)** Ha M olyan mátrixot választ, amelynek a főátlója csupa egyes, a főátló fölött pedig minden elem nulla, akkor $(n^2-n)/2$ lépés kevés, ugyanis M kijelölheti a mátrix többi elemét. Indukcióval megmutatjuk, hogy $1+(n^2-n)/2$ lépés mindig elég. Az $n=1$ esetben ez nyilvánvaló. Legyen $n>1$, és tekintsük az M által megadott tetszőleges $n\times n$-es A mátrixot és a kijelölt $1+(n^2-n)/2$ helyet.

Ha minden oszlopban van legalább egy kijelölt hely, akkor ezeket változtassuk meg úgy, hogy minden oszlopban az elemek összege 0 legyen. Ekkor minden sort az utolsó sorhoz hozzáadva egy csupa 0 sor keletkezik, tehát a determináns nulla.

Ha pl. az első oszlopban egyetlen hely sincs kijelölve, de minden elem nulla, akkor semmit sem kell változtatnunk.

Ha az első oszlopban egyetlen hely sincs kijelölve és pl. $\alpha_{11} \neq 0$, akkor minden sorból vonjuk ki az első sor megfelelő többszörösét, hogy az első oszlop többi eleme nullává váljon. Most hagyjuk el az első sort és oszlopot, az így keletkező $(n-1) \times (n-1)$-es B_1 mátrixban legalább

$$1 + (n^2 - n)/2 - (n-1) = 1 + [(n-1)^2 - (n-1)]/2$$

kijelölt hely van, így az indukció alapján ez átalakítható nulla determinánsú B' mátrixszá. „Vezessük át" az ennek megfelelő változtatást az eredeti A mátrixba. Az így kapott A' mátrixot az első oszlop „kinullázása" után az első sor szerint kifejtve a kívánt $\det A' = \det B' = 0$ adódik.

• **1.4.14** Megfelel bármely olyan mátrix, amelynek a determinánsa nulla, de egyik A_{ij} előjeles aldeterminánsa sem nulla, ugyanis α_{ij}-t megváltoztatva az i-edik sor (vagy a j-edik oszlop) szerinti kifejtés értéke biztosan megváltozik. Ilyen mátrixot pl. úgy gyárthatunk, hogy veszünk egy $(n-1) \times (n-1)$-es mátrixot, amelynek a determinánsa nem nulla és kiegészítjük egy n-edik sorral és oszloppal úgy, hogy a keletkező $n \times n$-es mátrixban minden sor és minden oszlop összege nulla legyen (vö. az 1.4.11 feladattal).

• **1.5.6** A mértani sorozat összegképletét használva az i-edik sor j-edik eleme $1 + \alpha_i\beta_j + \ldots + \alpha_i^{n-1}\beta_j^{n-1}$, tehát minden sor egy n-tagú összeg. Ennek alapján a determinánst n^n darab determináns összegére bonthatjuk, amelyek mindegyikében az i-edik sor j-edik eleme $\alpha_i^k\beta_j^k$ alakú, ahol $0 \leq k \leq n-1$. Az így keletkező determinánsok közül igen sokban lesz két egyforma sor, ezek értéke nulla. A fennmaradó determinánsokban a j-edik oszlop elemei rendre $\alpha_1^{\pi(1)}\beta_j^{\pi(1)}, \alpha_2^{\pi(2)}\beta_j^{\pi(2)}, \ldots, \alpha_n^{\pi(n)}\beta_j^{\pi(n)}$, ahol $\pi(1), \ldots, \pi(n)$ a $0, 1, \ldots, n-1$ számok valamilyen permutációja. Az $\alpha_1^{\pi(1)}, \ldots, \alpha_n^{\pi(n)}$ számoknak a sorokból történő kiemelése és $I(\pi)$ számú sorcsere után éppen $V(\beta_1, \ldots, \beta_n)$ marad. Az eredeti determinánsunk értéke így $V(\beta_1, \ldots, \beta_n) \sum (-1)^{I(\pi)} \alpha_1^{\pi(1)} \cdot \ldots \cdot \alpha_n^{\pi(n)} =$ $= V(\beta_1, \ldots, \beta_n) V(\alpha_1, \ldots, \alpha_n)$. — Egy másik megoldási lehetőség a determinánsok szorzástételének (2.2.4 Tétel) alkalmazása (lásd a 2.2.8 feladatot).

2. Mátrixok

• **2.1.18** Pontosan az $A = \lambda E$ mátrixok ilyenek. Ezek nyilván megfelelnek. Tegyük fel megfordítva, hogy $AB = BA$ minden B-re teljesül. Legyen $i \neq j$ és B az a mátrix, amelyben az i-edik sor j-edik eleme 1, minden más elem pedig 0. Ekkor az AB mátrixban a j-edik oszlop az A mátrix i-edik oszlopával azonos, minden más elem nulla, a BA mátrixban pedig az i-edik sor az A mátrix j-edik

sorával azonos, minden más elem nulla. Az $AB = BA$ egyenlőségből kapjuk, hogy $\alpha_{ii} = \alpha_{jj}$, $k \neq i \Rightarrow \alpha_{ki} = 0$ és $m \neq j \Rightarrow \alpha_{jm} = 0$. Mivel ez minden $i \neq j$ esetén fennáll, ezért A-ban a főátló elemei egyenlők, minden más elem pedig 0, azaz valóban $A = \lambda E$.

• **2.2.13** Ha A valamelyik sorában vagy oszlopában csupa nulla áll, akkor $\det A = 0$, és így nem létezhet inverz. Ellentmondásra jutunk akkor is, ha valamelyik sorban vagy oszlopban (legalább) két nem nulla elem előfordul. Legyen mondjuk $\alpha_{24} > 0$ és $\alpha_{27} > 0$. Szorozzuk meg A második sorát A^{-1} első, harmadik, negyedik stb. oszlopával. Ekkor $AA^{-1} = E$ alapján mindig nullát kell kapnunk, ez azonban a nemnegativitási feltétel miatt csak úgy lehetséges, ha A^{-1} ezen oszlopaiban a 4. és a 7. elem szükségképpen nulla. Vagyis A^{-1}-nek a 4. és 7. sora a második oszlopbeli elemek kivételével csupa nulla, és így $\det A^{-1} = 0$, ami ellentmondás.

3. Lineáris egyenletrendszerek

• **3.1.17** Ábel nem tudja kitalálni, mert pl. ugyanúgy mindig „páros" választ kap, akár csupa párosra, akár csupa páratlanra gondolt Béla. Béla viszont ki tudja találni, pl. a következő 5 kérdéssel (minden modulo 2 értendő):

$$x_5 + x_1 + x_2 =? = b_1,\ x_1 + x_2 + x_3 =? = b_2,\ x_2 + x_3 + x_4 =? = b_3,$$
$$x_3 + x_4 + x_5 =? = b_4,\ x_4 + x_5 + x_1 =? = b_5.$$

Ez az egyenletrendszer ugyanis egyértelműen megoldható. Ez adódik a determináns (modulo 2) kiszámításával, de közvetlenül is:

$$b_1 + b_2 + b_3 + b_4 + b_5 = 3(x_1 + x_2 + x_3 + x_4 + x_5) = x_1 + x_2 + x_3 + x_4 + x_5,$$

innen $b_2 + b_4 = x_1 + x_2 + 2x_3 + x_4 + x_5 = b_1 + b_2 + b_3 + b_4 + b_5 + x_3$, azaz $x_3 = b_1 + b_3 + b_5$, és a többi x_i-t is hasonlóan kapjuk. 4 kérdés viszont nem elég, mert akkor a 4 egyenletből álló 5 ismeretlenes rendszernek nem lehet egyértelmű megoldása, mivel az ismeretlenek száma nagyobb az egyenletek számánál.

• **3.2.12(a)** Az n darab Lagrange-féle alappolinom összege az $f(\gamma_1) = \ldots = f(\gamma_n) = 1$ feltételt kielégítő interpolációs polinom. Az $f = 1$ polinom kielégíti ezt a feltételt, és mivel csak egy ilyen (legfeljebb $n-1$-edfokú) polinom van, ezért $\sum_{i=1}^{n} L_i = 1$.

• **(b)** A (b1)-beli kifejezés a $\sum_{i=1}^{n} L_i = 1$ polinomnak a ν helyen vett helyettesítési értéke, azaz 1, a (b2)-beli összeg pedig ugyanebben a polinomban az $n-1$-edfokú tag együtthatója, azaz 0.

• **3.4.13(c)** Legyenek $\gamma_1, \ldots, \gamma_n$ különböző valós számok és $\alpha_{ij} = \gamma_j^{i-1}$, ha $i \leq r$, és 0 egyébként. Ennek a $k \times n$-es A mátrixnak a (sor)rangja legfeljebb r, hiszen csak r darab nem nulla sora van. Vegyünk most tetszőleges r oszlopot, ezek lineáris függetlenségéhez azt kell megmutatni, hogy az ezek alkotta $k \times r$-es B mátrix (oszlop)rangja r. A B mátrix rangján nem változtat, ha a csupa nulla sorait elhagyjuk, így egy $r \times r$-es C mátrixhoz jutunk. A C mátrix determinánsa egy csupa különböző elemmel generált Vandermonde-determináns, tehát nem nulla, ezért C (determináns)rangja r.

• **3.4.14(c)** Legyenek $\gamma_1, \ldots, \gamma_n$, illetve $\delta_1, \ldots, \delta_k$ különböző valós számok és legyen $\alpha_{ij} = 1 + (\delta_i\gamma_j) + \ldots + (\delta_i\gamma_j)^{r-1}$. Az 1.5.6 feladat alapján ebben a mátrixban minden $r \times r$-es aldeterminány két, csupa különböző elemmel generált Vandermonde-determináns szorzata, tehát nem nulla. Be kell még látni, hogy minden $(r+1) \times (r+1)$-es D aldeterminány értéke nulla. Ha egy ilyen D determinánst a sorai szerint r^{r+1} darab D_m determináns összegére bontunk, akkor a skatulyaelv szerint a kapott D_m determinánsok mindegyikében lesz két olyan sor, amelyek egymás számszorosai. Ezért mindegyik $D_m = 0$, és így $D = 0$, amint állítottuk.

• **3.4.18(a)** Ilyen mátrixok összege is ilyen típusú, tehát nyilván nem kapunk meg minden mátrixot.

• **(b)** Az (a) rész alapján elég olyan $B + C$ összegeket vizsgálni, ahol B-nek minden sora, C-nek pedig minden oszlopa számtani sorozat, azaz $\beta_{ij} = x_i + (j-1)y_i$ és $\gamma_{ij} = v_j + (i-1)z_j$, $1 \leq i \leq k, 1 \leq j \leq n$. Az $A = B + C$ előállítás az $\alpha_{ij} = x_i + (j-1)y_i + v_j + (i-1)z_j$ egyenletrendszer megoldhatóságát jelenti, az ismeretlenek x_i, y_i, v_j és z_j. Az ismeretlenek száma $2k + 2n$, ami (általában) kisebb, mint az egyenletek száma (kn), ezért az egyenletrendszer nem lehet minden α_{ij} esetén megoldható, tehát nem áll elő minden A mátrix a kívánt alakban.

• **(c)** Legyenek $\gamma_1, \ldots, \gamma_n$ tetszőleges különböző valós számok. Megmutatjuk, hogy bármely $k \times n$-es valós mátrix előáll n darab olyan M_r mátrix összegeként $(r = 1, 2, \ldots, n)$, ahol M_r minden sora egy γ_r hányadosú mértani sorozat. Ekkor M_r-ben pl. az első sor elemei rendre $x_r, x_r\gamma_r, \ldots, x_r\gamma_r^{n-1}$. Egy tetszőleges mátrix első sorának előállításához az $\alpha_{1j} = \sum_{r=1}^{n} x_r\gamma_r^{j-1}$, $1 \leq j \leq n$ egyenletrendszert kell megoldani (az ismeretlenek az $x_1, \ldots, x_n$). Az egyenletrendszer determinánsa $V(\gamma_1, \ldots, \gamma_n) \neq 0$, tehát az egyenletrendszer megoldható. Ugyanígy okoskodhatunk a többi sorra is. [Ha az esetleg előforduló és

problematikusnak tekinthető $x_r = 0$ esetet, azaz azt, amikor valamelyik mértani sorozat minden eleme nulla, nem akarjuk megengedni, akkor egy ilyen mátrixot két másik összegével helyettesíthetünk, amelyekben a csupa nulla sor(ok) helyett egy-egy olyan mértani sorozat áll, amelyek egymás negatívjai, a többi („rendes") sorba pedig az eredetileg szereplő mértani sorozatoknak az 1/2-szerese kerül.]

• **3.4.19(a)** k lépés mindig elég, hiszen megfelel, ha C a jobb oldali konstansok mindegyikét nullára változtatja. Ennyi lépés kell is, ha az egyenletrendszerben minden együttható nulla, de a jobb oldalon egyetlen elem sem nulla.

• **(b)** Ha $k > n$, akkor elég a jobb oldalon egyetlen elem megváltoztatása. Tudjuk, hogy van olyan i, amelyre az $A\mathbf{x} = \mathbf{e}_i$ egyenletrendszernek nincs megoldása ($\mathbf{e}_i$ az i-edik egységvektor, azaz amelynek i-edik komponense 1, a többi pedig 0). Ha az R által adott $A\mathbf{x} = \mathbf{b}$ egyenletrendszer megoldható volt, akkor a jobb oldalon az i-edik elemhez 1-et hozzáadva a kapott $A\mathbf{x} = \mathbf{b} + \mathbf{e}_i$ egyenletrendszer biztosan nem oldható meg.

Megmutatjuk, hogy $k \leq n$ esetén $n - k + 2$ a keresett lépésszám. Ennyire valóban szükség van, ha R olyan egyenletrendszert adott meg, amelyben az együtthatómátrix bármelyik k oszlopa lineárisan független és a jobb oldalon minden elem 0. Ugyanis ekkor C-nek legalább $n-k+1$ oszlopot el kell rontania, hogy csak $k-1$ független oszlop maradjon (különben az egyenletrendszernek bármilyen jobb oldal esetén van megoldása), és ezután még a jobb oldalon is legalább egy 0-t meg kell változtatnia.

Azt, hogy $n - k + 2$ lépés mindig elég is, lényegében ugyanezzel a gondolatmenettel mutathatjuk meg. Technikailag ezt a legegyszerűbben úgy kezelhetjük, hogy vesszük az R által adott egyenletrendszernek a Gauss-kiküszöböléssel *leghamarabb* adódó („redukálatlan") lépcsős alakját (tehát a redukálást már nem hajtjuk végre). Ehhez az alakhoz „felülről lefelé haladva" jutunk, és így az utolsó sor skalárszorosait *nem* adjuk hozzá más sorokhoz. Ennélfogva, ha ebben a lépcsős alakban csak az utolsó soron változtatunk, akkor az ezeknek a változásoknak az eredeti egyenletrendszerben megfelelő módosítások is csak az (eredeti) utolsó sort befolyásolják, a többi (eredeti) sort nem. Így valóban elegendő a lépcsős alakokra szorítkoznunk.

Tekintsük tehát egy lépcsős alak utolsó sorát, ebből fogunk legfeljebb $n - k + 2$ elem módosításával tilos sort gyártani. Először is a jobb oldali konstanst (ha nulla volt) változtassuk nem nullára. Ha az utolsó sorban nincs vezéregyes, akkor ez az egyetlen lépés elegendő is. Ha az utolsó sorban is van vezéregyes, akkor pedig a vezéregyes és az utána következő együtthatók (összesen legfeljebb $n - k + 1$ elem) helyére írjunk 0-t.

• **3.5.8(c)** Az $A\mathbf{x} = \mathbf{0}$ egyenletrendszer megoldásában valamelyik (pl. az első) ismeretlen szabad paraméter, azaz az $AB = 0$-t kielégítő B mátrixok első sora tetszőleges $\mathbf{s}$ vektor lehet. Ha $BA = 0$ is teljesül, akkor itt csak B első sorának az A-val vett szorzatát tekintve így bármely $\mathbf{s}$-re $\mathbf{s}A = \mathbf{0}$ áll fenn. Ez azonban csak $A = 0$ esetén lehetséges.

4. Vektorterek

• **4.2.12(e)** Indirekt, tegyük fel, hogy $V = \cup_{i=1}^{k} W_i$, ahol a W_i-k valódi alterei a V-nek. Feltehetjük, hogy k a minimális lehetséges darabszám. Ekkor $W_1 \not\subseteq \cup_{i=2}^{k} W_i$, hiszen különben W_1-et elhagyva $V = \cup_{i=2}^{k} W_i$ is teljesülne. Legyenek $\mathbf{u}$ és $\mathbf{v}$ olyan vektorok, amelyekre $\mathbf{u} \in W_1$, de $\mathbf{u} \notin W_i$, ha $i > 1$, továbbá $\mathbf{v} \notin W_1$. Tekintsük a $\mathbf{v} + \lambda\mathbf{u}$ ($\lambda \in T$) végtelen sok vektort. A feltétel szerint ezek valamennyien elemei a véges sok W_j közül valamelyiknek, tehát van olyan $1 \le i \le k$ és olyan $\lambda \ne \lambda'$, amelyre $\mathbf{v} + \lambda\mathbf{u} \in W_i$, $\mathbf{v} + \lambda'\mathbf{u} \in W_i$. Itt $i \ne 1$, mert különben $\mathbf{v} \in W_1$ következne. A két W_i-beli vektort kivonva kapjuk, hogy $(\mathbf{v} + \lambda\mathbf{u}) - (\mathbf{v} + \lambda'\mathbf{u}) = (\lambda - \lambda')\mathbf{u} \in W_i$, ahonnan $\mathbf{u} \in W_i$, ami ellentmondás.

• **(f)** Alkalmazzuk most is az e)-beli gondolatmenetet. A $\mathbf{v} + \lambda\mathbf{u}$ vektorok száma most $|T|$. Ha $|T| > k-1$, akkor ugyanúgy ellentmondásra jutunk, mint az előbb. Így valóban $k \ge |T| + 1$.

• **(g)** Legyen $\mathbf{b} \ne \mathbf{0}$ és $\mathbf{c} \ne \alpha\mathbf{b}$ (ilyen $\mathbf{b}$ és $\mathbf{c}$ vektorok biztosan találhatók, ha a V vektortérnek van nem triviális altere). Legyen W egy maximális (azaz tovább már nem bővíthető) olyan altér V-ben, amelynek a $\{\lambda\mathbf{b}+\mu\mathbf{c} \mid \lambda, \mu \in T\}$ halmazzal való metszete csak a nullvektorból áll. (Ilyen W létezik, véges elemszámú vektortér esetén ez nyilvánvaló, végtelen elemszám esetén pedig a szokásos halmazelméleti módszerekkel — pl. a Zorn-lemmával — igazolható.) Azt állítjuk, hogy ekkor az alábbi $k + 1$ darab valódi altér egyesítése kiadja a V vektorteret: $W' = \{\vartheta\mathbf{c} + \mathbf{w} \mid \vartheta \in T, \mathbf{w} \in W\}$, továbbá minden $\gamma \in T$-re $W_\gamma = \{\vartheta(\mathbf{b}+\gamma\mathbf{c})+\mathbf{w} \mid \vartheta \in T, \mathbf{w} \in W\}$. Könnyen igazolható, hogy ezek valóban alterek. Megmutatjuk, hogy ezek egyike sem egyezik meg V-vel. Pl. W_γ-nak nem lehet eleme $\mathbf{c}$. Ellenkező esetben ugyanis $\mathbf{c} = \vartheta(\mathbf{b} + \gamma\mathbf{c}) + \mathbf{w}$, ahonnan átrendezéssel $\mathbf{w} = -\vartheta\mathbf{b} + (1 - \vartheta\gamma)\mathbf{c}$ adódik. A W altérre szabott feltételünk szerint itt a jobb oldalon a nullvektor áll, ez viszont $\mathbf{b} \ne \mathbf{0}$ és $\mathbf{c} \ne \alpha\mathbf{b}$ miatt csak a $\vartheta = 1 - \vartheta\gamma = 0$ önmagának ellentmondó esetben valósulhatna meg. Hasonlóan igazolhatjuk, hogy $\mathbf{b} \notin W'$. Végül belátjuk, hogy tetszőleges $\mathbf{u} \in V$ vektor benne van a megadott $k + 1$ valódi altér egyesítésében. Legyen $U = \{\vartheta\mathbf{u}+\mathbf{w} \mid \vartheta \in T, \mathbf{w} \in W\}$. Ekkor U altér, és W maximalitása miatt van olyan

$\lambda\mathbf{b}+\mu\mathbf{c}\neq\mathbf{0}$ vektor, amely eleme U-nak: $\vartheta\mathbf{u}+\mathbf{w}=\lambda\mathbf{b}+\mu\mathbf{c}$. Itt a W-re adott feltétel szerint ϑ nem lehet 0, ezért $\mathbf{u}$ kifejezhető $\mathbf{u}=(\lambda/\vartheta)\mathbf{b}+(\mu/\vartheta)\mathbf{c}-(1/\vartheta)\mathbf{w}$ alakban. Innen kapjuk, hogy $\lambda=0$ esetén $\mathbf{u}\in W'$, egyébként pedig $\mathbf{u}\in W_{\mu/\lambda}$.

• *Megjegyzés*: érdemes végiggondolni, hogy az itt elmondott bizonyítás az útmutatásban jelzett utat valósítja meg. Magát a bizonyítást is a fentinél jóval kényelmesebben lehet(ne) leírni a dimenzió, továbbá a faktortér vagy a direkt összeg felhasználásával, de ezekre nem akartunk támaszkodni.

• **4.4.11** A feladat egyes részei sokféleképpen vizsgálhatók, pl. (a) igazsága nyilvánvaló a definícióból, (c)-re könnyű ellenpéldát találni. Az egységes tárgyalásmód érdekében azonban érdemes azt a $k\times m$-es mátrixot venni, amelynek az oszlopai az $\mathbf{u}_j$ vektorok. A vektorok függetlensége azt jelenti, hogy ennek a mátrixnak a rangja m. A mátrixrangot most determinánsrangként célszerű tekinteni. Mivel egy egész elemű mátrix determinánsa mindig egész szám, ezért mindegy, hogy a rangot $\mathbf{R}$ vagy $\mathbf{Q}$ felett tekintjük-e, tehát (a) és (b) igaz. A modulo p esetben a determináns p-vel való oszthatóságát kell vizsgálni. Egy nullától különböző egész lehet páros, ezért (c) hamis. Egy páratlan szám viszont biztosan nem nulla, tehát (d) igaz. Végül egy nullától különböző egész csak véges sok prímmel lehet osztható, tehát (e) is igaz. (Vö. a 3.4.8 és 4.6.16 feladatokkal.)

• **4.6.7(a)** Legyen $\mathbf{b}_1,\dots,\mathbf{b}_{100}$ egy bázis V-ben. Ekkor pl. a $\mathbf{v}_\gamma=\mathbf{b}_1+\gamma\mathbf{b}_2+{}$ $+\gamma^2\mathbf{b}_3+\ldots+\gamma^{99}\mathbf{b}_{100}$ ($\gamma\in\mathbf{R}$) végtelen sok vektor közül bármely 100 bázist alkot. Ehhez elég belátni, hogy bármely 100 ilyen vektor lineárisan független. Ez onnan adódik, hogy a megfelelő homogén lineáris egyenletrendszer determinánsa egy csupa különböző elemmel generált Vandermonde-determináns, tehát nem nulla.

• **(b)** Az F_2 test felett 101 ilyen vektor megadható: egy tetszőleges bázis és a báziselemek összege megfelelő. Megmutatjuk, hogy ennél több vektor már nem lehet. Vegyük bázisnak az első 100 vektort, $\mathbf{v}_1,\dots,\mathbf{v}_{100}$-at. A $\mathbf{v}_{101}$-et írjuk fel ezek lineáris kombinációjaként: $\mathbf{v}_{101}=\sum_{i=1}^{100}\alpha_i\mathbf{v}_i$. Ha itt valamelyik $\alpha_i=0$, akkor az ennek megfelelő $\mathbf{v}_i$ kivételével a többi 100 $\mathbf{v}_j$ vektor nyilván összefüggő, ami ellentmondás. Így minden $\alpha_i=1$, vagyis a $\mathbf{v}_{101}$ vektor egyértelműen meghatározott, tehát a rendszer tovább nem bővíthető.

Az F_{97} test felett is egy tetszőleges bázis és a báziselemek összege megfelelő 101 vektort alkot. Belátjuk, hogy itt sem lehet ennél több vektort megadni. Az F_2-nél látott gondolatmenethez hasonlóan a $\mathbf{v}_{101}=\sum_{i=1}^{100}\alpha_i\mathbf{v}_i$ vektor mindegyik α_i együtthatója most is nullától különböző. Az első 100 vektor helyett esetleg azok alkalmas skalárszorosát véve elérhető, hogy minden $\alpha_i=1$ legyen,

azaz $\mathbf{v}_{101} = \sum_{i=1}^{100} \mathbf{v}_i$. Tegyük fel, hogy létezne még egy $\mathbf{v}_{102} = \sum_{i=1}^{100} \beta_i \mathbf{v}_i$ vektor. A skatulyaelv alapján van olyan $i \neq j$, amelyre $\beta_i = \beta_j$, pl. $\beta_1 = \beta_2$. Ekkor $\mathbf{v}_{102} - \beta_1 \mathbf{v}_{101}$ előállítható $\mathbf{v}_3, \ldots, \mathbf{v}_{100}$ lineáris kombinációjaként, és így a $\mathbf{v}_3, \ldots, \mathbf{v}_{102}$ vektorok lineárisan összefüggők, ami ellentmondás.

Az F_{101} test felett már 102 ilyen tulajdonságú vektor is létezik: legyen $\mathbf{v}_1, \ldots, \mathbf{v}_{100}$ tetszőleges bázis, $\mathbf{v}_{101} = \sum_{i=1}^{100} \mathbf{v}_i$ és $\mathbf{v}_{102} = \sum_{i=1}^{100} i\mathbf{v}_i$. Könnyen látható, hogy ezek a vektorok valóban a kívánt tulajdonságúak. Megmutatjuk, hogy 103 ilyen vektor már nem adható meg. Az F_{97}-nél látott gondolatmenethez hasonlóan feltehető, hogy $\mathbf{v}_{101} = \sum_{i=1}^{100} \mathbf{v}_i$ és $\mathbf{v}_{102} = \sum_{i=1}^{100} \beta_i \mathbf{v}_i$, ahol a β_i-k egymástól és nullától különbözők. Ennélfogva a β_i-k az 1,2,...,100 számok egy permutációját alkotják. Tegyük fel, hogy létezne még egy $\mathbf{v}_{103} = \sum_{i=1}^{100} \gamma_i \mathbf{v}_i$ vektor. Ekkor szükségképpen a γ_i-k is az 1,2,...,100 számok egy permutációját alkotják. Emellett a $\gamma_i = \delta_i \beta_i$ előállításnál a δ_i-k egymástól (és nullától) különbözők kell hogy legyenek, ugyanis ha pl. $\delta_1 = \delta_2$, akkor $\mathbf{v}_{103} - \delta_1 \mathbf{v}_{102}$ előállítható $\mathbf{v}_3, \ldots, \mathbf{v}_{100}$ lineáris kombinációjaként, és így a $\mathbf{v}_3, \ldots, \mathbf{v}_{100}, \mathbf{v}_{102}, \mathbf{v}_{103}$ vektorok lineárisan összefüggők, ami ellentmondás. Szorozzuk össze a(z F_{101}-beli) $\gamma_i = \delta_i \beta_i$, $i = 1, 2, \ldots, 100$ egyenlőségeket. Modulo 101 kongruenciákkal számolva a Wilson-tétel alapján kapjuk, hogy

$$-1 \equiv 100! \equiv \prod_{i=1}^{100} \gamma_i \equiv \prod_{i=1}^{100} \delta_i \prod_{i=1}^{100} \beta_i \equiv (100!)^2 \equiv (-1)^2 = 1 \pmod{101},$$

ami ellentmondás.

• **4.6.16(c)** Jelölje egy 0–1 mátrixnak az F_2 feletti rangját s, a $\mathbf{Q}$ feletti rangját pedig t. Vegyünk s darab (F_2 felett) lineárisan független oszlopot, ezeknek $2^s - 1$ számú nem triviális lineáris kombinációja képezhető. Így a mátrixnak bármely $2^s - 1$-nél több oszlopa között vagy szerepel egy csupa nulla oszlop, vagy pedig előfordul két azonos oszlop, ezért $2^s - 1$-nél több oszlop $\mathbf{Q}$ felett sem lehet független. Ebből következik, hogy $t \leq 2^s - 1$. Megfordítva, megmutatjuk, hogy tetszőleges $(s \leq) t \leq 2^s - 1$ esetén létezik olyan $t \times t$-es 0–1 mátrix, amelynek az F_2 feletti rangja s, a $\mathbf{Q}$ feletti rangja pedig t. Innen kapjuk, hogy az 1000-es különbséget biztosító legkisebb s érték az $s = 10$, és ekkor a mátrix mérete $t = s + 1000 = 1010$.

A megfordítást elegendő a $t = 2^s - 1$ esetre igazolni. Ha ugyanis $s \leq t' < 2^s - 1$, akkor hagyjunk el a megfelelő $(2^s - 1) \times (2^s - 1)$ méretű A mátrixból $2^s - 1 - t'$ számú oszlopot úgy, hogy a megmaradók között szerepeljen s olyan oszlop, amelyek F_2 felett függetlenek. Ekkor a megmaradó t' számú oszlop $\mathbf{Q}$ felett továbbra is független, tehát ennek a $(2^s - 1) \times t'$ méretű B mátrixnak a $\mathbf{Q}$ feletti rangja t', az F_2 feletti rangja pedig s. Tartsunk most meg B-ből s olyan sort, amelyek F_2 felett függetlenek. Ekkor ezek $\mathbf{Q}$ felett is függetlenek,

tehát hozzávehetünk még $t' - s$ további sort B-ből, hogy a kapott t' sor $\mathbf{Q}$ felett független legyen. Az így adódó $t' \times t'$ méretű C mátrix megfelel; a $\mathbf{Q}$ feletti rangja t', az F_2 feletti rangja pedig s.

Legyen tehát $t = 2^s - 1$, és készítsünk egy olyan $t \times t$-es 0–1 mátrixot, amelynek az F_2 feletti rangja s, a $\mathbf{Q}$ feletti rangja pedig t. A mátrix első s oszlopába soronként rendre az $1, 2, \ldots, 2^s - 1$ számoknak a kettes számrendszerbeli számjegyei kerülnek, tehát az első sor első s eleme $(0, 0, \ldots, 0, 0, 1)$, a második soré $(0, 0, \ldots, 0, 1, 0)$, a harmadik soré $(0, 0, \ldots, 0, 1, 1)$ stb. A többi oszlop legyen ezután az első s oszlopnak az F_2 test felett képzett összes (további) nem triviális lineáris kombinációja (azaz ahol legalább két együttható nem nulla). Így egy $(2^s - 1) \times (2^s - 1)$ méretű 0–1 mátrixot kapunk. Megmutatjuk, hogy ennek az oszlopai a $\mathbf{Q}$ felett függetlenek, vagyis a $\mathbf{Q}$ feletti rang $2^s - 1$. Ebből a konstrukció és az elején látottak alapján az is következik, hogy az F_2 feletti rang s.

Az áttekinthetőség kedvéért egészítsük ki a mátrixunkat a tetején egy csupa nulla sorral (ez az oszlopok függetlenségi viszonyain nyilván nem változtat). Az s szerinti teljes indukcióval megmutatjuk, hogy az így kapott $2^s \times (2^s - 1)$ méretű A_s mátrix bármely oszlopában a 2^s darab elem fele 1, másik fele pedig 0. Ez $s = 1$-re nyilvánvaló. Legyen $s - 1$-re az első $s - 1$ oszlopvektor $\mathbf{a}_1, \ldots, \mathbf{a}_{s-1}$ (minden $\mathbf{a}_i$ vektornak 2^{s-1} komponense van). Ekkor s-re a konstrukció szerint a következőképpen kapjuk meg az első s oszlopot (ezek mindegyike 2^s komponensből áll):

$$\mathbf{b}_1 = \begin{pmatrix} \mathbf{0} \\ \mathbf{1} \end{pmatrix}, \mathbf{b}_2 = \begin{pmatrix} \mathbf{a}_1 \\ \mathbf{a}_1 \end{pmatrix}, \ldots, \mathbf{b}_s = \begin{pmatrix} \mathbf{a}_{s-1} \\ \mathbf{a}_{s-1} \end{pmatrix}.$$

Mivel az indukciós feltevés szerint az $\mathbf{a}_i$ vektorok komponenseinek pontosan a fele volt 1-es, ezért ez a tulajdonság öröklődik a $\mathbf{b}_j$ vektorokra is. Ezzel beláttuk, hogy s-re az első s oszlop rendelkezik a jelzett tulajdonsággal. A további oszlopokat az első s oszlop F_2 felett vett nem triviális lineáris kombinációjaként, azaz néhány $\mathbf{b}_j$ összegeként kapjuk. Ha az összeadandók között nem szerepel a $\mathbf{b}_1$, akkor az összegvektor „alsó és felső fele" ugyanúgy azonos, mint az összeadandóknál, tehát ugyanazt az indukciós következtetést alkalmazhatjuk, mint az első oszlopok esetében. Ha még a $\mathbf{b}_1$-et is hozzáadjuk egy ilyen vektorhoz, akkor az „alsó felében" az 1-esek és a 0-k helyet cserélnek, de mivel a számuk az indukciós feltevés szerint ugyanannyi volt, ezért most is készen vagyunk.

Szükségünk lesz még arra, hogy ($s > 1$ esetén) az A_s mátrix bármely két oszlopában az azonos helyeken szereplő 1-esek száma 2^{s-2}. Legyen $\mathbf{u}$ és $\mathbf{v}$ két tetszőleges oszlop, és legyen x azoknak a helyeknek a száma, ahol mindkettőben 1-es szerepel. Ekkor $\mathbf{u}$-nak és $\mathbf{v}$-nek is további $2^{s-1} - x$ olyan

komponense van, ahol az illető vektorban 1-es áll. Az F_2 felett képzett $\mathbf{u}+\mathbf{v}$ vektor a konstrukció alapján előfordul A_s oszlopai között és $\mathbf{u}+\mathbf{v}$-ben azokra a helyekre kerül 1-es, ahol $\mathbf{u}$-ban és $\mathbf{v}$-ben különböző értékek szerepeltek. Így $\mathbf{u}+\mathbf{v}$-ben az 1-esek száma $2(2^{s-1}-x)=2^{s-1}$. Innen $x=2^{s-2}$, ahogy állítottuk.

Az A_s mátrix $\mathbf{v}_1,\dots,\mathbf{v}_t$ oszlopainak a $\mathbf{Q}$ feletti lineáris függetlenségét a skalárszorzat (részletesen lásd a 7.1, 8.1, illetve 9.4 pontokban) segítségével igazoljuk. (Az $s=1$ esetben az állítás nyilvánvaló, tehát feltehetjük, hogy $s\geq 2$, bár az alábbi bizonyítás formálisan az $s=1$ esetre is helyes.) Legyen $\sum_{i=1}^{t}\alpha_i\mathbf{v}_i=\mathbf{0}$. Képezzük mindkét oldalnak egy tetszőleges $\mathbf{v}_j$ vektorral a skalárszorzatát. Két 0–1 vektor skalárszorzata a közös helyeken előforduló 1-esek száma. Az előző két bekezdésben igazoltak alapján így az $\alpha_j 2^{s-1}+$ $+\sum_{i\neq j}\alpha_i 2^{s-2}=0$, azaz $2^{s-2}(\alpha_j+\sum_{i=1}^{t}\alpha_i)=0$ egyenlőséghez jutunk. Mivel ez minden j-re teljesül, ezért nyilván minden α_i szükségképpen 0, amint állítottuk.

Megjegyezzük, hogy az A_s mátrix sor-, illetve oszlopcseréktől eltekintve a következőképpen is megadható: a sorokat indexezzük az $X=\{1,2,\dots,s\}$ halmaz részhalmazai, az oszlopokat pedig az X nem üres részhalmazai szerint, és legyen $\alpha_{Y,Z}=|Y\cap Z| \bmod 2$ (ahol $Y,Z\subseteq X$).

5. Lineáris leképezések

• **5.5.9** Írjuk fel, hogyan fogalmazható át az, hogy néhány $\mathcal{A}_{ij}$ lineáris kombinációja a $\mathcal{O}$ leképezés. A

$$\lambda_1\mathcal{A}_{i_1j_1}+\lambda_2\mathcal{A}_{i_2j_2}+\ldots+\lambda_m\mathcal{A}_{i_mj_m}=\mathcal{O}$$

egyenlőség azt jelenti, hogy tetszőleges $\alpha_{i_r},\alpha_{j_r}$ $(1\leq r\leq m)$ komplex számokra

$$\lambda_1\begin{pmatrix}\alpha_{i_1}\\ \alpha_{j_1}\end{pmatrix}+\lambda_2\begin{pmatrix}\alpha_{i_2}\\ \alpha_{j_2}\end{pmatrix}+\ldots+\lambda_m\begin{pmatrix}\alpha_{i_m}\\ \alpha_{j_m}\end{pmatrix}=\begin{pmatrix}0\\ 0\end{pmatrix},$$

azaz

$$\lambda_1\alpha_{i_1}+\lambda_2\alpha_{i_2}+\ldots+\lambda_m\alpha_{i_m}=0,\quad \lambda_1\alpha_{j_1}+\lambda_2\alpha_{j_2}+\ldots+\lambda_m\alpha_{j_m}=0$$

teljesül. Innen látszik, hogy ha pl. az i_1 index értéke az összes többi i_r index értékétől különbözik, akkor szükségképpen $\lambda_1=0$: helyettesítsük be ugyanis az $\alpha_{i_1}=1,\alpha_{i_2}=\ldots=\alpha_{i_m}=0$ számokat. Természetesen hasonló érvényes a j_r indexekre is.

• **(a)** Alkalmazzuk a fentieket most az $m=3$ esetre. Mivel az $\mathcal{A}_{ij}$ leképezések nyilván nem egymás skalárszorosai, ezért közülük bármelyik kettő független.

Emiatt ha három $\mathcal{A}_{ij}$-nek egy lineáris kombinációja a $\mathcal{O}$ leképezés, és kiderül, hogy ebben a kombinációban valamelyik λ_t együttható 0, akkor a másik két együttható is szükségképpen 0. A lineáris függetlenséghez így elég belátni, hogy bármely három (különböző) $(i_1, j_1), (i_2, j_2), (i_3, j_3)$ indexpár esetén vagy a három i indexérték, vagy a három j indexérték között van olyan, amely különbözik a másik kettőtől. Ha az i-k nem mind egyformák, akkor legalább az egyikük csak egyszer fordulhat elő. Ha egyformák, akkor pedig a j-k mind különbözők kell, hogy legyenek.

• **(b)** Pl. $\mathcal{A}_{11} + \mathcal{A}_{22} - \mathcal{A}_{12} - \mathcal{A}_{21} = \mathcal{O}$.

• **(c)** Pl. az alábbi hét (ij) indexpárhoz tartozó $\mathcal{A}_{ij}$ leképezések lineárisan függetlenek $\mathrm{Hom}\,(V_1\,,\,V_2)$-ben: $(11), (12), (13), (14), (24), (34), (44)$. Ugyanis az i-k között a 2, a 3 és a 4 csak egyszer fordul elő, így az ezeknek megfelelő leképezésekhez tartozó utolsó három együttható $\lambda_5 = \lambda_6 = \lambda_7 = 0$. Ugyanez a helyzet a j-knél az 1, 2, 3-mal, tehát az első három együttható is nulla. Ekkor azonban a maradék középső együttható, λ_4 is csak nulla lehet.

Bebizonyítjuk, hogy bármely nyolc darab $\mathcal{A}_{ij}$ leképezés már lineárisan összefüggő. Mivel a $\mathrm{Hom}\,(V_1\,,\,V_2)$ vektortér $4 \cdot 2 = 8$-dimenziós, így elég belátni, hogy az összes $\mathcal{A}_{ij}$ által generált altér nem tartalmazza $\mathrm{Hom}\,(V_1\,,\,V_2)$ minden elemét. Megmutatjuk, hogy pl. az $\mathcal{A}\begin{pmatrix}\alpha_1\\ \alpha_2\\ \alpha_3\\ \alpha_4\end{pmatrix} = \begin{pmatrix}\alpha_1\\ 0\end{pmatrix}$ leképezés nem áll elő $\mathcal{A} = \sum_{1\le i,j\le 4} \lambda_{ij}\mathcal{A}_{ij}$ alakban. Alkalmazzuk mindkét oldalt az egységvektorokra. Ha $\alpha_1 = 1, \alpha_2 = \alpha_3 = \alpha_4 = 0$, akkor a képvektorok két koordinátájában a $\lambda_{11}+\lambda_{12}+\lambda_{13}+\lambda_{14} = 1$ és a $\lambda_{11}+\lambda_{21}+\lambda_{31}+\lambda_{41} = 0$ egyenlőségeket kapjuk. Az $\alpha_2 = 1, \alpha_1 = \alpha_3 = \alpha_4 = 0$ esetben $\lambda_{21}+\lambda_{22}+\lambda_{23}+\lambda_{24} = = \lambda_{12} + \lambda_{22} + \lambda_{32} + \lambda_{42} = 0$ adódik, és a másik két egységvektorra hasonlóan $\sum_{j=1}^{4} \lambda_{3j} = \sum_{i=1}^{4} \lambda_{i3} = 0$, illetve $\sum_{j=1}^{4} \lambda_{4j} = \sum_{i=1}^{4} \lambda_{i4} = 0$ az eredmény. Az első koordinátákra kapott összes egyenlőséget összeadva $\sum_{1\le i,j\le 4} \lambda_{ij} = 1$, míg ugyanezt a második koordinátákra elvégezve $\sum_{1\le i,j\le 4} \lambda_{ij} = 0$ adódik, ami ellentmondás.

• Megjegyezzük, hogy a feladat kényelmesebben tárgyalható a lineáris leképezések mátrixának segítségével (lásd az 5.7 pontot). Az $\mathcal{A}_{ij}$ leképezésnek egy olyan 2×4-es (komplex elemű) mátrix felel meg, amelyben az első sor i-edik és a második sor j-edik eleme 1-es, a többi elem pedig 0. Ekkor az összes $\mathcal{A}_{ij}$ mátrixai által generált alteret azok a mátrixok alkotják, amelyekben a két sor elemeinek az összege megegyezik. Ennek alapján a feladat általánosítása is jól

kezelhető. Legyen $V_1 = T^n, V_2 = T^k$ és

$$\mathcal{A}_{i_1,i_2,\dots,i_k} \begin{pmatrix} \alpha_1 \\ \alpha_2 \\ \vdots \\ \alpha_n \end{pmatrix} = \begin{pmatrix} \alpha_{i_1} \\ \vdots \\ \alpha_{i_k} \end{pmatrix}, \qquad 1 \le i_j \le n, \quad j = 1, \dots, k.$$

Ekkor az így definiált n^k darab leképezésre az alábbiak igazak.

(a) Bármely három (különböző) leképezés lineárisan független Hom $(V_1\,,\, V_2)$-ben (feltéve hogy $nk \ge 3$).
(b) Megadható négy (különböző) leképezés, amely lineárisan összefüggő (kivéve, ha n és k valamelyike 1).
(c) A lineárisan független leképezések maximális száma $(n-1)k+1$.

• **5.6.24** Jelöljük rögzített u kvaternió esetén az $\alpha + \beta u$ alakú kvaterniók halmazát, ahol α, β valós, T_u-val. Az útmutatásban jelzett állítás szerint T_v a kvaternióalgebrának egy, a komplex számokkal izomorf részalgebrája. Legyen a w és a z kvaternió a v kvaterniónak egy-egy (feltételezett) n-edik gyöke. Mivel v nem valós szám, ezért nyilván w és z sem az. Ekkor a T_w és T_z részalgebra is 2-dimenziós, továbbá mindkettő tartalmazza a valós számokat és $(w^n = z^n =)v$-t, ezért T_w és T_z metszete is kétdimenziós. Ez csak úgy lehet, ha $T_w = T_z = T_v$. Ez azt jelenti, hogy a v kvaternió n-edik gyökeit T_v-ben kell keresnünk. Mivel T_v izomorf a komplex számokkal, ezért bármely nem nulla elemének, így a v-nek is pontosan n (különböző) n-edik gyöke van T_v-ben. Ennélfogva v-nek az összes kvaterniók körében is pontosan n (különböző) n-edik gyöke van.

6. Sajátérték, minimálpolinom

• **6.3.15** Jelölje egy tetszőleges r polinom esetén r^* azt a polinomot, amelyet úgy kapunk, hogy r-ben x helyére x^2-et helyettesítünk, azaz $r^*(x) = r(x^2)$. Nyilván $r(\mathcal{A}^2) = r^*(\mathcal{A})$. Többször fel fogjuk használni az innen adódó

$$r(\mathcal{A}^2) = \mathcal{O} \iff m_{\mathcal{A}} \mid r^* \tag{M.6.1}$$

összefüggést. Szükségünk lesz még az alábbi állításra:

Lemma: Ha $\lambda \neq 0$, akkor az r polinomnak a λ^2 pontosan ugyanannyiszoros gyöke, mint ahányszoros gyöke az r^* polinomnak a λ.

A lemma bizonyítása: Legyen r-ben j a λ^2 multiplicitása: $r = (x-\lambda^2)^j h$, ahol $h(\lambda^2) \neq 0$. Ekkor $r^* = (x^2-\lambda^2)^j h^* = (x-\lambda)^j (x+\lambda)^j h^*$, tehát r^*-ban a λ multiplicitása (pontosan) j, hiszen $-\lambda \neq \lambda$ és $h^*(\lambda) = h(\lambda^2) \neq 0$.

További előkészületként emeljük ki $m_{\mathcal{A}}$-ból a lehető legnagyobb x-hatványt, azaz írjuk fel $m_{\mathcal{A}}$-t a következő alakban:

$$m_{\mathcal{A}} = x^k g\,, \quad \text{ahol} \quad k \geq 0 \text{ és } g(0) \neq 0\,. \tag{M.6.2}$$

Rátérve a *szükségesség* igazolására, feltesszük, hogy az $\mathcal{A}$ és $\mathcal{A}^2$ transzformációk minimálpolinomja megegyezik, és megmutatjuk (i), (ii) és (iii) teljesülését.

(i) Ha $m_{\mathcal{A}}(\lambda) = 0$, akkor λ sajátértéke $\mathcal{A}$-nak. A két minimálpolinom egyezéséből a sajátértékek egyezése is adódik, tehát λ sajátértéke $\mathcal{A}^2$-nek is. Ezért λ egyik négyzetgyöke, λ_1 sajátértéke $\mathcal{A}$-nak (6.1.4c feladat), vagyis $m_{\mathcal{A}}(\lambda_1) = 0$. Ezt folytatva kapjuk, hogy $\lambda_2, \lambda_3, \ldots$ is gyöke $m_{\mathcal{A}}$-nak, ahol $\lambda_{i+1} = \sqrt{\lambda_i}$ egyik értéke.

Mivel $m_{\mathcal{A}}$ gyökeinek a száma véges, így van olyan $i > j$, hogy $\lambda_i = \lambda_j$. Ezt 2^i-ik hatványra emelve $\lambda = \lambda^{2^{i-j}}$, azaz $\lambda\bigl(1 - \lambda^{2^{i-j}-1}\bigr) = 0$ adódik. Ennélfogva λ valóban csak 0 vagy páratlan rendű egységgyök lehet.

(ii) Tegyük fel indirekt, hogy $x^2 \,|\, m_{\mathcal{A}}$, azaz (M.6.2)-ben $k \geq 2$. Megmutatjuk, hogy ekkor $\mathcal{A}^2$ gyöke lesz a $t = m_{\mathcal{A}}/x = x^{k-1}g$ polinomnak, ami ellentmond annak, hogy $m_{\mathcal{A}^2} = m_{\mathcal{A}}$.

Többször fel fogjuk használni (M.6.1)-et és (M.6.2)-t. A feltétel szerint $\mathcal{A}^2$ gyöke az $m_{\mathcal{A}}$-nak, továbbá

$$m_{\mathcal{A}}(\mathcal{A}^2) = \mathcal{O} \iff m_{\mathcal{A}} \mid m_{\mathcal{A}}^* \iff x^k g \mid x^{2k} g^*\,,$$

ahonnan $(g, x) = 1$ miatt $g \mid g^*$ következik. Mivel

$$t(\mathcal{A}^2) = \mathcal{O} \iff m_{\mathcal{A}} \mid t^* \iff x^k g \mid x^{2k-2} g^*\,,$$

és itt az utolsó oszthatóság $g \mid g^*$ és $k \leq 2k-2$ alapján teljesül, kapjuk, hogy $\mathcal{A}^2$ valóban gyöke a t-nek.

(iii) A(z esetleges) 0 gyökre az állítás nyilvánvaló. Legyen $\lambda \neq 0$, és tegyük fel, hogy $m_{\mathcal{A}}$-ban a λ multiplicitása k, a λ^2-é pedig j. Először azt igazoljuk, hogy $j \geq k$.

Egyrészt az $m_{\mathcal{A}}(\mathcal{A}^2) = \mathcal{O}$ feltétel miatt $m_{\mathcal{A}} \mid m_{\mathcal{A}}^*$, tehát a λ multiplicitása $m_{\mathcal{A}}^*$-ban legalább k. Másrészt a lemma alapján a λ multiplicitása $m_{\mathcal{A}}^*$-ban pontosan j. A kettő összevetéséből valóban $j \geq k$ adódik.

Tekintsük most a $\lambda, \lambda^2, \lambda^4, \lambda^8, \ldots$ sorozatot. Itt az elemek mindegyikének legalább akkora a multiplicitása $m_{\mathcal{A}}$-ban, mint az őt megelőzőnek. A már bizonyított (i) tulajdonság alapján azonban a sorozat (az elejétől kezdve) periodikus, ezért mindegyik multiplicitás szükségképpen egyenlő.

Az *elégségesség*hez azt kell megmutatnunk, hogy ha az (i), (ii) és (iii)

feltételek teljesülnek, akkor

$$\text{(a) } m_{\mathcal{A}}(\mathcal{A}^2)=\mathcal{O} \qquad \text{és} \qquad \text{(b) } s(\mathcal{A}^2)=\mathcal{O} \Longrightarrow m_{\mathcal{A}} \mid s\,.$$

Az (M.6.1) összefüggés alapján (a) és (b) ekvivalens

$$\text{(a1) } m_{\mathcal{A}} \mid m_{\mathcal{A}}^* \qquad \text{és} \qquad \text{(b1) } m_{\mathcal{A}} \mid s^* \Longrightarrow m_{\mathcal{A}} \mid s$$

fennállásával.

Először (a1)-et igazoljuk. A (iii) feltétel szerint $m_{\mathcal{A}}$ minden gyökének a négyzete is ugyanannyiszoros gyök. Megmutatjuk, hogy különböző gyökök négyzete is különböző. Ez azzal ekvivalens, hogy ha $\lambda \neq 0$ gyöke $m_{\mathcal{A}}$-nak, akkor $-\lambda$ nem lehet gyök. Az (i) feltétel szerint λ egy páratlan rendű egységgyök. Ekkor $-\lambda$ rendje a λ rendjének a kétszerese, tehát páros. Így ismét (i)-re hivatkozva $-\lambda$ nem lehet gyöke $m_{\mathcal{A}}$-nak.

A fentiek alapján, ha $m_{\mathcal{A}}$ gyöktényezős alakjában minden gyök helyett annak a négyzetét írjuk, akkor ugyanazt a polinomot kapjuk. Azaz

$$m_{\mathcal{A}}=\prod_{i=1}^{r}(x-\lambda_i)^{k_i}=\prod_{i=1}^{r}(x-\lambda_i^2)^{k_i}\,,$$

ahonnan

$$m_{\mathcal{A}}^*=\prod_{i=1}^{r}(x^2-\lambda_i^2)^{k_i}=\prod_{i=1}^{r}(x-\lambda_i)^{k_i}\prod_{i=1}^{r}(x+\lambda_i)^{k_i}=m_{\mathcal{A}}\prod_{i=1}^{r}(x+\lambda_i)^{k_i}\,,$$

tehát valóban $m_{\mathcal{A}} \mid m_{\mathcal{A}}^*$.

Rátérünk (b1) bizonyítására. Az $m_{\mathcal{A}} \mid s$ oszthatósághoz azt kell megmutatni, hogy $m_{\mathcal{A}}$ minden gyöke legalább akkora multiplicitással szerepel s-ben, mint $m_{\mathcal{A}}$-ban.

Ha a 0 gyöke $m_{\mathcal{A}}$-nak, akkor (ii) szerint csak egyszeres gyök, és így elég azt igazolni, hogy a 0 az s polinomnak is gyöke. Mivel $m_{\mathcal{A}}(0)=0$, ezért a 0 sajátértéke $\mathcal{A}$-nak, tehát sajátértéke $\mathcal{A}^2$-nek is. Az $s(\mathcal{A}^2)=\mathcal{O}$ feltételből következik, hogy az $\mathcal{A}^2$ sajátértékei szükségképpen gyökei s-nek, tehát valóban $s(0)=0$.

Tekintsük most $m_{\mathcal{A}}$-nak egy $\mu \neq 0$ gyökét, és legyen ennek a multiplicitása j. Ekkor az (i) és (iii) feltételből következik, hogy μ valamelyik négyzetgyöke is (pontosan) j-szeres gyöke $m_{\mathcal{A}}$-nak. Jelöljük μ-nek ezt a négyzetgyökét λ-val, azaz $\mu=\lambda^2$.

Legyen s-ben a $\mu=\lambda^2$ multiplicitása j'. Ekkor a lemma szerint s^*-ban a λ multiplicitása j'. Az $m_{\mathcal{A}} \mid s^*$ feltétel miatt — a λ multiplicitását összehasonlítva — $j \leq j'$ adódik. Ez azonban egyúttal azt is jelenti, hogy a μ multiplicitása s-ben legalább akkora, mint $m_{\mathcal{A}}$-ban, és éppen ezt kellett bizonyítani.

• **6.4.10(a)** Egy lineáris leképezés képtere altér, tehát $U = \operatorname{Im} f(\mathcal{A})$ altér. Belátjuk, hogy $\mathcal{A}$-invariáns. Legyen $\mathbf{u} \in U$, azaz valamilyen $\mathbf{x} \in V$-re $\mathbf{u} = f(\mathcal{A})\mathbf{x}$. Ekkor $\mathcal{A}\mathbf{u} = \mathcal{A}\big(f(\mathcal{A})\mathbf{x}\big) = \big(\mathcal{A}f(\mathcal{A})\big)\mathbf{x} = \big(f(\mathcal{A})\mathcal{A}\big)\mathbf{x} = f(\mathcal{A})(\mathcal{A}\mathbf{x})$, így $\mathcal{A}\mathbf{u} \in U$. (A 6.4.6 feladatra is hivatkozhattunk volna $\mathcal{B} = f(\mathcal{A})$-val.)

• **(b)** Először azt igazoljuk, hogy ha $(f\,,\, m_{\mathcal{A}}) = (g\,,\, m_{\mathcal{A}})$, akkor $\operatorname{Im} f(\mathcal{A}) = \operatorname{Im} g(\mathcal{A})$. Legyen $(f\,,\, m_{\mathcal{A}}) = d$; azt kell belátnunk, hogy $\operatorname{Im} f(\mathcal{A}) = \operatorname{Im} d(\mathcal{A})$. Az $f(\mathcal{A})\mathbf{x} = d(\mathcal{A})\big((f/d)(\mathcal{A})\mathbf{x}\big)$ egyenlőségből egyrészt azt kapjuk, hogy $\operatorname{Im} f(\mathcal{A}) \subseteq \operatorname{Im} d(\mathcal{A})$. Másrészt a $d = sf + tm_{\mathcal{A}}$ felírásból

$$d(\mathcal{A})\mathbf{z} = f(\mathcal{A})\big(s(\mathcal{A})\mathbf{z}\big) + t(\mathcal{A})\big(m_{\mathcal{A}}(\mathcal{A})\mathbf{z}\big) = f(\mathcal{A})\big(s(\mathcal{A})\mathbf{z}\big) + \mathbf{0},$$

tehát $\operatorname{Im} d(\mathcal{A}) \subseteq \operatorname{Im} f(\mathcal{A})$.

A megfordításhoz tegyük fel, hogy $\operatorname{Im} f(\mathcal{A}) = \operatorname{Im} g(\mathcal{A})$, és azt fogjuk igazolni, hogy $(f\,,\, m_{\mathcal{A}}) = (g\,,\, m_{\mathcal{A}})$. Az előzőek alapján elég megmutatnunk, hogy ha d_1 és d_2 az $m_{\mathcal{A}}$ minimálpolinom osztói és $\operatorname{Im} d_1(\mathcal{A}) = \operatorname{Im} d_2(\mathcal{A})$, akkor d_1 és d_2 egymástól csak konstans szorzóban különböznek. Tegyük fel tehát, hogy $\operatorname{Im} d_1(\mathcal{A}) = \operatorname{Im} d_2(\mathcal{A})$ és legyen $m_{\mathcal{A}} = h_1 d_1 = h_2 d_2$. Mivel $\mathcal{O} = m_{\mathcal{A}}(\mathcal{A}) = h_1(\mathcal{A})d_1(\mathcal{A})$, ezért $\operatorname{Im} d_1(\mathcal{A}) \subseteq \operatorname{Ker} h_1(\mathcal{A})$. Ugyanakkor $\operatorname{Im} d_1(\mathcal{A}) = \operatorname{Im} d_2(\mathcal{A})$, tehát $\operatorname{Im} d_2(\mathcal{A}) \subseteq \operatorname{Ker} h_1(\mathcal{A})$, és így $h_1(\mathcal{A})d_2(\mathcal{A}) = \mathcal{O}$. Emiatt $h_1 d_1 = m_{\mathcal{A}} \,|\, h_1 d_2$, vagyis $d_1 \,|\, d_2$. Ugyanígy kapjuk, hogy $d_2 \,|\, d_1$, tehát d_1 és d_2 valóban egymás konstansszorosai.

• **(c)** Legyenek d_i a minimálpolinom páronként nem-egységszeres osztói. Az előbb beláttuk, hogy ekkor az $\operatorname{Im} d_i(\mathcal{A})$ invariáns alterek mind különbözők.

• **(d)** Belátjuk, hogy $\mathcal{A}$-nak akkor és csak akkor nincs nem triviális invariáns altere, ha $m_{\mathcal{A}}$ irreducibilis (T felett) és $\deg m_{\mathcal{A}} = \dim V$. (Mint az eredményeknél említettük, ezek a feltételek ekvivalensek $k_{\mathcal{A}}$ irreducibilitásával.) Ha $m_{\mathcal{A}}$ reducibilis, akkor egy nem triviális $d \,|\, m_{\mathcal{A}}$ osztóhoz tartozó $\operatorname{Im} d(\mathcal{A})$ egy nem triviális invariáns alteret ad. Ha $\deg m_{\mathcal{A}} < \dim V$, akkor $\dim\langle \mathbf{u}, \mathcal{A}\rangle \le \deg m_{\mathcal{A}}$ miatt bármely $\mathbf{u} \neq \mathbf{0}$ esetén $\langle \mathbf{u}, \mathcal{A}\rangle$ nem triviális invariáns altér. A megfordításhoz tegyük fel, hogy $m_{\mathcal{A}}$ irreducibilis, $\deg m_{\mathcal{A}} = \dim V$, és legyen U az $\mathcal{A}$-nak egy invariáns altere. Azt kell megmutatnunk, hogy ha U tartalmaz egy $\mathbf{u} \neq \mathbf{0}$ vektort, akkor szükségképpen $U = V$. Az $\mathbf{u}$-t tartalmazó legszűkebb invariáns altér $\langle \mathbf{u}, \mathcal{A}\rangle \subseteq U$, tehát elég belátni, hogy $\langle \mathbf{u}, \mathcal{A}\rangle = V$. Ennek az igazolását a legkényelmesebben a 6.5 pontban bevezetett rendfogalom és annak néhány egyszerű tulajdonsága segítségével írhatjuk le (de hangsúlyozzuk, hogy enélkül csak a megfogalmazás lenne nehézkesebb). Mivel az $o_{\mathcal{A}}(\mathbf{u})$ rend osztója a minimálpolinomnak, így ($\mathbf{u} \neq \mathbf{0}$ miatt) csak maga a minimálpolinom (vagy annak konstansszorosa) lehet. Ennélfogva $\dim\langle \mathbf{u}, \mathcal{A}\rangle = \deg o_{\mathcal{A}}(\mathbf{u}) = \deg m_{\mathcal{A}} = \dim V$, és így (a véges dimenzió miatt) csak $\langle \mathbf{u}, \mathcal{A}\rangle = V$ lehetséges, amint állítottuk.

7. Bilineáris függvények

• **7.1.9(b)** A függvények helyett a megfelelő mátrixokkal okoskodunk. Legyen $[\mathbf{A}] = (\alpha_{ij})_{1\le i,j\le n}$, továbbá $\mathbf{A}_{ij}$ az a bilineáris függvény, amelynek a mátrixában az i-edik sor j-edik eleme α_{ij}, a többi elem pedig 0. Ekkor $\mathbf{A}_{ij}$ felírható $\mathbf{A}_{ij}(\mathbf{u},\mathbf{v}) = \Phi(\mathbf{u})\Psi(\mathbf{v})$ alakban, ahol Φ értéke a $\mathbf{b}_i$ helyen α_{ij} és a többi báziselemen 0, Ψ értéke pedig a $\mathbf{b}_j$ helyen 1 és a többi báziselemen 0. Mivel $\mathbf{A} = \sum_{1\le i,j\le n} \mathbf{A}_{ij}$, így $\mathbf{A}$ előáll a kívánt összegalakban, a tagok száma $r = n^2$.

Megmutatjuk, hogy r lehető legkisebb értéke az $\mathbf{A}$ mátrixának a rangja, $r([\mathbf{A}])$. Mivel egy $\Phi(\mathbf{u})\Psi(\mathbf{v})$ alakú (nem azonosan nulla) bilineáris függvény mátrixának a rangja 1, és mátrixok összegének a rangja legfeljebb a rangok összege, ezért $\mathbf{A}(\mathbf{u},\mathbf{v}) = \sum_{m=1}^{r} \Phi_m(\mathbf{u})\Psi_m(\mathbf{v})$ mátrixának a rangja legfeljebb r, azaz $r([\mathbf{A}]) \le r$.

Be kell még látni, hogy $\mathbf{A}$ valóban előáll $r([\mathbf{A}])$ tagú összegként ilyen alakban. Ez mátrixokra átfogalmazva azt jelenti, hogy egy r rangú A mátrix mindig felírható r darab ($n\times 1$-es mátrixnak tekintett) oszlopvektor és r darab ($1\times n$-es mátrixnak tekintett) sorvektor szorzatának, azaz r darab diádnak az összegeként. Legyen $A = (\alpha_{ij})_{1\le i,j\le n}$ és jelölje O_j, illetve S_i a mátrix j-edik oszlopából, illetve i-edik sorából álló ($n\times 1$-es, illetve $1\times n$-es) mátrixokat. Vegyünk egy tetszőleges $\alpha_{ij}\neq 0$ elemet és legyen $B = \big((1/\alpha_{ij})O_j\big)S_i$. Ekkor a B egy olyan diád, amelynek az i-edik sora és j-edik oszlopa azonos az A mátrix i-edik sorával és j-edik oszlopával, tehát az $A' = A - B$ mátrix i-edik sora és j-edik oszlopa csupa 0-ból áll. Megmutatjuk, hogy $r(A') = r(A)-1$, ezután az eljárást az A' mátrixra megismételve stb. (vagy r szerinti indukcióval) kapjuk a kívánt állítást. Vonjuk le az A mátrix oszlopaiból a j-edik oszlop megfelelő skalárszorosait, hogy az i-edik sorban a j-edik elemtől eltekintve minden elem 0 legyen, majd az (új) i-edik sor megfelelő skalárszorosait a többi sorból levonva érjük el, hogy a j-edik oszlop elemei is az i-edik helyen álló α_{ij}-től eltekintve mind 0-k legyenek. Az átalakítások során a rang nem változott, tehát az így kapott A_1 mátrixra $r(A_1) = r(A)$, továbbá A' és A_1 pontosan csak abban különböznek egymástól, hogy az i-edik sor j-edik eleme A'-ben 0, míg A_1-ben $\alpha_{ij}\neq 0$. Vegyünk A'-ben egy maximális méretű $h\times h$-as nem nulla D aldeterminánst. Ez nyilván nem tartalmazhatja a csupa nulla i-edik sort vagy j-edik oszlopot. Vegyük most A_1-ben azt a $(h+1)\times(h+1)$-es D_1 aldeterminánst, amelyet D-ből az (A_1-beli) i-edik sor és j-edik oszlop hozzávételével kapunk, ekkor nyilván $D_1 = \pm\alpha_{ij}D \neq 0$, tehát $r(A_1) \ge r(A') + 1$. Mivel A' és A_1 mindössze egyetlen elemben különböznek, ezért itt szükségképpen egyenlőség áll, tehát valóban $r(A) = r(A_1) = r(A') + 1$, ahogy állítottuk.

Megjegyezzük, hogy a bizonyításban nem használtuk ki, hogy négyzetes mátrixról van szó: bármilyen alakú mátrix előállítható diádok összegeként és

itt az összeadandók számának a lehető legkisebb értéke a mátrix rangja (a nullmátrixra ez úgy érvényes, ha az üres összeget a szokásos módon nullának vesszük).

• **7.2.9** A 7.2.3 Tétel második bizonyításából leolvasható, hogy a $\mathbf{v}$-re $\mathbf{A}$-ortogonális $\mathbf{w}$ vektorok W halmaza valóban altér és legalább $n-1$-dimenziós, azaz vagy $W = V$, vagy pedig $\dim W = n - 1$. Egy másik lehetőség, hogy a $[\mathbf{v}]^T[\mathbf{A}][\mathbf{w}] = 0$ homogén lineáris „egyenletrendszert" tekintjük, amelyben az ismeretlenek a $\mathbf{w}$ vektor koordinátái. Ez a rendszer egyetlen egyenletből áll, az ismeretlenek száma pedig n, tehát legalább $n - 1$ szabad paraméter van, azaz a megoldásokból egy legalább $n - 1$-dimenziós alteret kapunk.

Ha $\mathbf{A}(\mathbf{v}, \mathbf{v}) \neq 0$, akkor $\mathbf{v} \notin W$ miatt csak $\dim W = n - 1$ lehetséges, $\mathbf{v} = \mathbf{0}$ vagy $\mathbf{A} = \mathbf{0}$ esetén pedig triviálisan $W = V$. Ez azt jelenti, hogy $\dim W = n - 1$ és $\dim W = n$ egyaránt megvalósulhat.

Az alábbiakban részletesen megvizsgáljuk, hogy a $\mathbf{v} = \mathbf{0}$, illetve $\mathbf{A} = \mathbf{0}$ triviális eseteken kívül mikor lesz még $W = V$, azaz mikor lesz $\mathbf{v}$ minden vektorra $\mathbf{A}$-ortogonális. Ekkor $\mathbf{v}$-nek nyilván önmagára is $\mathbf{A}$-ortogonálisnak kell lennie, tehát a továbbiakban feltesszük, hogy $\mathbf{A}(\mathbf{v}, \mathbf{v}) = 0$ teljesül.

Nézzük először azt az esetet, amikor $\mathbf{A}(\mathbf{x}, \mathbf{x}) \geq 0$ minden $\mathbf{x}$-re vagy $\mathbf{A}(\mathbf{x}, \mathbf{x}) \leq 0$ minden $\mathbf{x}$-re (azaz a 7.3 pontban bevezetett terminológiával $\mathbf{A}$ pozitív vagy negatív szemidefinit). Megmutatjuk, hogy ekkor $W = V$. Tegyük fel például, hogy $\mathbf{A}(\mathbf{x}, \mathbf{x}) \geq 0$ minden $\mathbf{x}$-re, és vegyünk egy $\mathbf{A}$-ortogonális $\mathbf{c}_1, \ldots, \mathbf{c}_n$ bázist, ahol (valamilyen t-re) $\mathbf{A}(\mathbf{c}_i, \mathbf{c}_i) = 0$, ha $1 \leq i \leq t$, és $\mathbf{A}(\mathbf{c}_i, \mathbf{c}_i) > 0$, ha $t < i \leq n$. Ekkor könnyen láthatóan $\mathbf{A}(\mathbf{v}, \mathbf{v}) = 0 \iff$ $\iff \mathbf{v} \in \langle \mathbf{c}_1, \ldots, \mathbf{c}_t \rangle$, és ekkor $\mathbf{v}$ mindegyik $\mathbf{c}_j$-re $(1 \leq j \leq n)$, tehát a vektortér minden elemére is $\mathbf{A}$-ortogonális.

Tegyük most fel, hogy az $\mathbf{A}(\mathbf{x}, \mathbf{x})$ értékek között pozitív és negatív szám is előfordul (azaz $\mathbf{A}$ indefinit). Válasszunk egy $\mathbf{A}$-ortogonális $\mathbf{c}_1, \ldots, \mathbf{c}_n$ bázist, és legyenek $\mathbf{c}_1, \ldots, \mathbf{c}_t$ ebben azok a bázisvektorok, amelyekre $\mathbf{A}(\mathbf{c}_i, \mathbf{c}_i) = 0$ (most $t = 0$ is lehet). Ha $\mathbf{v} \in \langle \mathbf{c}_1, \ldots, \mathbf{c}_t \rangle$, akkor az előző bekezdésben látottakhoz hasonlóan $\mathbf{v}$ mindegyik $\mathbf{c}_j$-re $(1 \leq j \leq n)$, és így a vektortér minden elemére is $\mathbf{A}$-ortogonális, tehát $W = V$. Ha $\mathbf{v} \notin \langle \mathbf{c}_1, \ldots, \mathbf{c}_t \rangle$, akkor $\mathbf{v}$ nem lehet $\mathbf{c}_{t+1}, \ldots, \mathbf{c}_n$ mindegyikére $\mathbf{A}$-ortogonális, tehát ekkor $W \neq V$ (és így $\dim W = n - 1$).

• **7.2.10** Minden szimmetrikus bilineáris függvénynek van olyan diagonális mátrixa, ahol a főátló első néhány eleme 1, utána néhány -1, és végül néhány 0 következik. (A „néhány" itt azt is jelentheti, hogy esetleg egyetlen ilyen elem sincs, de azt is, hogy akár az összes elem ilyen.) A tehetetlenségi tétel szerint az ilyen típusú (különböző) mátrixok száma megegyezik a páronként nem ek-

vivalens szimmetrikus bilineáris függvények számával. Az ilyen mátrixokat az n pontból és 2 vonalból álló sorozatokkal jellemezhetjük: az első vonal elé, a két vonal közé, illetve a második vonal után rendre annyi pontot írunk, ahány 1, -1, illetve 0 van a mátrix főátlójában. Az ilyen sorozatok száma nyilván $\binom{n+2}{2}$.

• **7.3.13** Ha $\mathbf{A}$ nem indefinit, akkor a 7.2.9 feladat megoldásában látott gondolatmenettel igazolhatjuk, hogy bármely $\mathbf{v} \neq \mathbf{0}$ vektor kiegészíthető $\mathbf{A}$-ortogonális bázissá. Ha azonban $\mathbf{A}$ indefinit, akkor ez nem teljesül. Legyenek $\mathbf{c}_1, \mathbf{c}_2$ olyan $\mathbf{A}$-ortogonális vektorok, amelyekre $\mathbf{A}(\mathbf{c}_1, \mathbf{c}_1) = 1, \mathbf{A}(\mathbf{c}_2, \mathbf{c}_2) = -1$, ekkor pl. a $\mathbf{v} = \mathbf{c}_1 + \mathbf{c}_2 \neq \mathbf{0}$ vektor nem lehet eleme egy $\mathbf{A}$-ortogonális bázisnak. Ha ugyanis $\mathbf{v} = \mathbf{d}_1, \mathbf{d}_2, \ldots, \mathbf{d}_n$ mégis $\mathbf{A}$-ortogonális bázist alkotna, akkor $\mathbf{A}(\mathbf{v}, \mathbf{v}) = 0$ miatt $\mathbf{v}$ mindegyik $\mathbf{d}_i$-re, és így az egész V-re $\mathbf{A}$-ortogonális lenne, ami ellentmondás, hiszen pl. $\mathbf{A}(\mathbf{c}_1, \mathbf{v}) = \mathbf{A}(\mathbf{c}_1, \mathbf{c}_1) = 1$.

• **7.3.14(a)** Ha $\mathbf{A} = \mathbf{0}$, akkor $\operatorname{Ker} \tilde{\mathbf{A}} = V$. Ha $\mathbf{A}$ definit, akkor $\operatorname{Ker} \tilde{\mathbf{A}} = \mathbf{0}$. Ha $\mathbf{A}$ szemidefinit, és egy $\mathbf{A}$-ortogonális bázisban $\mathbf{c}_1, \ldots, \mathbf{c}_t$ azok a bázisvektorok, amelyekre $\tilde{\mathbf{A}}(\mathbf{c}_i) = 0$, akkor $\operatorname{Ker} \tilde{\mathbf{A}} = \langle \mathbf{c}_1, \ldots, \mathbf{c}_t \rangle$ (lásd pl. a 7.2.9 feladat megoldásánál). Végül megmutatjuk, hogy $\operatorname{Ker} \tilde{\mathbf{A}}$ nem altér, ha $\mathbf{A}$ indefinit. Legyen az $\mathbf{A}$-ortogonális $\mathbf{c}_1, \mathbf{c}_2$ vektorokra $\mathbf{A}(\mathbf{c}_1, \mathbf{c}_1) = 1, \mathbf{A}(\mathbf{c}_2, \mathbf{c}_2) = -1$. Ekkor a $\mathbf{v} = \mathbf{c}_1 + \mathbf{c}_2$ és $\mathbf{z} = \mathbf{c}_1 - \mathbf{c}_2$ vektorok elemei a magnak, azonban az összegük nem: $\mathbf{v} + \mathbf{z} = 2\mathbf{c}_1 \notin \operatorname{Ker} \tilde{\mathbf{A}}$.

• **(b)** A definit és szemidefinit esetekben a mag valódi altér, tehát nem tartalmazhatja az egész térnek egy bázisát. Ha $\mathbf{A} = \mathbf{0}$, akkor a mag az egész V, tehát bármely bázis megfelel. Végül megmutatjuk, hogy indefinit $\mathbf{A}$-ra is kiválasztható a magból a térnek egy bázisa. Legyen az $\mathbf{A}$ egy diagonális mátrixában a főátló első r eleme 1, a következő s eleme -1, a többi $t = n - r - s$ eleme pedig 0 (itt az indefinitség miatt $r \geq 1, s \geq 1$). Legyen az ennek megfelelő (egyik) $\mathbf{A}$-ortogonális bázis $\mathbf{m}_1, \ldots, \mathbf{m}_r, \mathbf{n}_1, \ldots, \mathbf{n}_s, \mathbf{o}_1, \ldots, \mathbf{o}_t$, ahol $\mathbf{A}(\mathbf{m}_i, \mathbf{m}_i) = 1, \mathbf{A}(\mathbf{n}_j, \mathbf{n}_j) = -1, \mathbf{A}(\mathbf{o}_k, \mathbf{o}_k) = 0$. Ekkor az $\mathbf{m}_i \pm \mathbf{n}_j$ és $\mathbf{o}_k$ vektorok valamennyien elemei a magnak, továbbá együttesen V-nek egy generátorrendszerét alkotják. Így közülük biztosan kiválasztható V-nek egy bázisa.

• **(c)** Ha a mag altér, akkor ez a maximális szám a mag dimenziója, azaz definit esetben 0, szemidefinit esetben a diagonális mátrix átlójában a nullák száma, $\mathbf{A} = \mathbf{0}$ esetén pedig n. Végül, ha $\mathbf{A}$ indefinit, akkor a (b) rész szerint a magból kiválasztható V-nek egy bázisa, tehát a keresett maximum n.

• **(d)** Ha a mag altér, akkor nyilván most is a mag dimenziója a válasz. Ha $\mathbf{A}$ indefinit, akkor megmutatjuk, hogy a keresett maximum a (b)-beli jelölésekkel

$n - \max(r, s)$. Legyen pl. $r \geq s$, ekkor az $\mathbf{m}_i + \mathbf{n}_i$, $1 \leq i \leq s$ és $\mathbf{o}_k$, $1 \leq k \leq t$ vektorok függetlenek és az általuk generált $s + t = n - r$ dimenziós altér része a magnak. Másrészt, ha U egy $n - r$-nél nagyobb dimenziós tetszőleges altér, akkor $\dim U + \dim\langle \mathbf{m}_1, \ldots, \mathbf{m}_r \rangle > (n - r) + r = n$, tehát a két altér metszete tartalmaz egy $\mathbf{z} \neq \mathbf{0}$ vektort. Azonban $\langle \mathbf{m}_1, \ldots, \mathbf{m}_r \rangle$ bármely $\mathbf{z} \neq \mathbf{0}$ elemére $\mathbf{A}(\mathbf{z}, \mathbf{z}) > 0$, tehát $\mathbf{z} \notin \operatorname{Ker} \tilde{\mathbf{A}}$ és így a $\mathbf{z}$-t tartalmazó U altér sem lehet része a magnak.

8. Euklideszi terek

• **8.2.17** Nyilván feltehetjük, hogy a vektorok egységnyi hosszúak.

• **(a)** Megmutatjuk, hogy ha a $\mathbf{v}_i$ vektorok közül bármelyik kettő 60 fokos szöget zár be, akkor szükségképpen lineárisan függetlenek, így a darabszámuk legfeljebb n. A feltételek szerint $\mathbf{v}_i \cdot \mathbf{v}_i = 1$ és $i \neq t$-re $\mathbf{v}_i \cdot \mathbf{v}_t = 1/2$. Tegyük fel, hogy $\sum_{i=1}^{k} \lambda_i \mathbf{v}_i = \mathbf{0}$, és vegyük mindkét oldalnak rendre a $\mathbf{v}_j$ $(j = 1, \ldots, k)$ vektorokkal a skalárszorzatát. A kapott egyenlőségeket 2-vel beszorozva a $\lambda_j + \sum_{i=1}^{k} \lambda_i = 0, \quad j = 1, \ldots, k$ egyenletrendszerhez jutunk. Az egyenletek összegét $k + 1$-gyel osztva $\sum_{i=1}^{k} \lambda_i = 0$, majd ezt visszahelyettesítve $\lambda_j = 0$ adódik, tehát az egyenletrendszernek csak triviális megoldása van. Így a $\mathbf{v}_i$ vektorok valóban függetlenek, amint állítottuk.

Most pedig teljes indukcióval belátjuk, hogy az n-dimenziós V euklideszi térben létezik n darab olyan $\mathbf{v}_i$ egységvektor, amelyek közül bármelyik kettő 60 fokos szöget zár be. Ha $n \leq 2$, akkor ez nyilvánvaló. Legyen most $n > 2$ és $\mathbf{e}_1, \ldots, \mathbf{e}_n$ egy ortonormált bázis V-ben. Az $n - 1$-dimenziós $\langle \mathbf{e}_1, \ldots, \mathbf{e}_{n-1} \rangle$ euklideszi térben az indukciós feltétel szerint léteznek megfelelő $\mathbf{v}_1, \ldots \mathbf{v}_{n-1}$ vektorok. Megmutatjuk, hogy ezekhez a $\mathbf{v}_n = \alpha \mathbf{e}_n + \beta(\mathbf{v}_1 + \ldots + \mathbf{v}_{n-1})$ vektort hozzávéve (alkalmas α, β esetén) a kívánt tulajdonságú vektorrendszerhez jutunk. Ehhez azt kell igazolni, hogy

(i) minden $j \leq n - 1$-re $\mathbf{v}_j \cdot \mathbf{v}_n = 1/2$ és (ii) $\mathbf{v}_n \cdot \mathbf{v}_n = 1$.

Jelöljük a $\mathbf{v}_1 + \ldots + \mathbf{v}_{n-1}$ összegvektort $\mathbf{s}$-sel. Az (i) egyenlőség $\mathbf{v}_j \cdot \mathbf{e}_n = 0$ miatt ekvivalens az $1/2 = \beta(\mathbf{v}_j \cdot \mathbf{s}) = n\beta/2$ feltétellel, ahonnan $\beta = 1/n$. A (ii) egyenlőség ezután átírható az $1 = \alpha^2 + \beta^2 ||\mathbf{s}||^2 = \alpha^2 + (n-1)/(2n)$ alakba. Innen $\alpha = \pm\sqrt{(n+1)/(2n)}$. (A fenti módszerrel a $\mathbf{v}_i$ vektorokat tulajdonképpen rekurzíve megkonstruáltuk, akár az explicit képletüket is felírhattuk volna. A fentieket megfelelően elemezve az is kiderül, hogy $\mathbf{v}_n$-re (lényegében) egyetlen választási lehetőség adódik, és ebből egy újabb bizonyítást nyerhetünk arra is, hogy n-nél több ilyen tulajdonságú vektor már nem adható meg.)

• **(b)** Mivel a síkon található három egységvektor, amelyek közül bármelyik kettő 120 fokos szöget zár be, ezért nyilván $\dim V \geq 2$ esetén is van három ilyen vektor. Megmutatjuk, hogy négy vektor viszont már nem adható meg. Legyen $\mathbf{a}, \mathbf{b}, \mathbf{c}$ három ilyen tulajdonságú vektor, ekkor

$$||\mathbf{a}+\mathbf{b}+\mathbf{c}||^2 = ||\mathbf{a}||^2 + ||\mathbf{b}||^2 + ||\mathbf{c}||^2 + 2\mathbf{a}\cdot\mathbf{b} + 2\mathbf{a}\cdot\mathbf{c} + 2\mathbf{b}\cdot\mathbf{c} = 3 - 3 = 0,$$

tehát szükségképpen $\mathbf{a}+\mathbf{b}+\mathbf{c} = \mathbf{0}$. Ha tehát lenne négy ilyen vektor, akkor közülük bármelyik három összege a nullvektor, és így mind a négy vektor maga is a nullvektor lenne, ami ellentmondás.

• *Megjegyzés*: A fenti megoldáshoz hasonlóan igazolható a feladat alábbi általánosítása:

(a) Tetszőleges hegyesszögre is igaz, hogy a keresett maximum éppen n.

(b) Tompaszög esetén az ilyen vektorok száma mindig egy, a dimenziótól független és csak az adott Φ szögtől függő korlát alatt marad: az elérhető maximum $\lfloor 1 - 1/\cos\Phi \rfloor$.

(A fennmaradó szögekre a válasz nyilvánvaló: 0 fokra végtelen sok vektor is megadható, 90 fokra a maximum n, 180 fokra pedig 2.)

• **8.4.14(a)** Az $\mathcal{A} = \lambda\mathcal{E}$ transzformációk nyilván megfelelnek. Megmutatjuk, hogy más ilyen tulajdonságú transzformáció nincs. Előrebocsátjuk, hogy bármely két független vektorhoz van olyan skalárszorzat, amely szerint ezek a vektorok merőlegesek: definiáljuk egy olyan bázissal a skalárszorzatot, amely a két adott vektort tartalmazza. Legyen $\mathcal{A} \neq \lambda\mathcal{E}$, ekkor tudjuk, hogy létezik olyan $\mathbf{e}$ vektor, hogy $\mathbf{e}$ és $\mathcal{A}\mathbf{e}$ nem egymás skalárszorosai, azaz $\mathbf{e}$ és $\mathcal{A}\mathbf{e}$ lineárisan független. Tegyük fel indirekt, hogy $\mathcal{A}^*$ nem függ a skalárszorzat választásától, ekkor bármely skalárszorzatra $0 \neq (\mathcal{A}\mathbf{e})\cdot(\mathcal{A}\mathbf{e}) = \mathbf{e}\cdot(\mathcal{A}^*\mathcal{A}\mathbf{e})$. Az $\mathbf{e}$ és $\mathcal{A}^*\mathcal{A}\mathbf{e}$ vektorok nem lehetnek függetlenek, hiszen akkor az előrebocsátott megjegyzés alapján alkalmas skalárszorzat szerint merőlegesek is lennének. Ennélfogva $\mathcal{A}^*\mathcal{A}\mathbf{e} = \beta\mathbf{e}$. Tekintsünk most egy olyan skalárszorzatot, amelyben a (független) $(1/\gamma)\mathbf{e}$ és $\mathcal{A}\mathbf{e}$ vektorok egy ortonormált bázis részét képezik, ekkor $1 = (\mathcal{A}\mathbf{e})\cdot(\mathcal{A}\mathbf{e}) = \mathbf{e}\cdot(\mathcal{A}^*\mathcal{A}\mathbf{e}) = \mathbf{e}\cdot(\beta\mathbf{e}) = \beta|\gamma|^2$, ami tetszőleges γ-ra nyilván nem lehetséges.

• **(b)** Először az elégségességet igazoljuk. Tegyük fel, hogy az S_1 és S_2 skalárszorzatokra $S_1 = \lambda S_2$ (megjegyezzük, hogy ekkor a λ szükségképpen pozitív valós szám), és legyen $\mathcal{A} \in \operatorname{Hom} V$ tetszőleges transzformáció. Jelölje $\mathcal{A}$-nak az S_1, illetve S_2 szerinti adjungáltját $\mathcal{A}_1$, illetve $\mathcal{A}_2$, belátjuk, hogy ezek mindig egyenlők. Bármely $\mathbf{u}, \mathbf{v} \in V$ vektorokra $S_2(\mathcal{A}\mathbf{u}, \mathbf{v}) = S_2(\mathbf{u}, \mathcal{A}_2\mathbf{v})$ és $S_1(\mathcal{A}\mathbf{u}, \mathbf{v}) = S_1(\mathbf{u}, \mathcal{A}_1\mathbf{v})$. A második egyenlőségbe az $S_1 = \lambda S_2$ feltételt beírva, majd λ-val egyszerűsítve kapjuk, hogy $S_2(\mathcal{A}\mathbf{u}, \mathbf{v}) = S_2(\mathbf{u}, \mathcal{A}_1\mathbf{v})$, és

így $S_2(\mathbf{u}, \mathcal{A}_2\mathbf{v}) = S_2(\mathbf{u}, \mathcal{A}_1\mathbf{v})$. Mivel ez minden $\mathbf{u}, \mathbf{v}$-re fennáll, ezért valóban $\mathcal{A}_1 = \mathcal{A}_2$.

Rátérve a szükségességre, tegyük fel, hogy bármely $\mathcal{A}$ transzformációnak az S_1 és S_2 skalárszorzat szerint képzett adjungáltja megegyezik. Megmutatjuk, hogy ekkor szükségképpen $S_1 = \lambda S_2$. Legyen az S_1 és S_2 skalárszorzatnak megfelelő egy-egy ortonormált bázis $\mathbf{e}_1, \ldots, \mathbf{e}_n$ és $\mathbf{f}_1, \ldots, \mathbf{f}_n$. A Gram–Schmidt-ortogonalizáció alapján feltehető, hogy $\langle \mathbf{e}_1, \ldots, \mathbf{e}_i \rangle = \langle \mathbf{f}_1, \ldots, \mathbf{f}_i \rangle$ minden $1 \leq i \leq n$-re.

Először belátjuk, hogy $\mathbf{f}_n = \lambda_n \mathbf{e}_n$ (alkalmas λ_n-re). Indirekt, ha $\mathbf{f}_n$ és $\mathbf{e}_n$ lineárisan független, akkor legyen $\mathcal{A}$ egy olyan lineáris transzformáció, amelyre $\mathcal{A}\mathbf{e}_n = \mathbf{e}_{n-1}$ és $\mathcal{A}\mathbf{f}_n = \mathbf{e}_n$. Ekkor S_1 szerint $0 = \mathbf{e}_{n-1} \cdot \mathbf{e}_n = (\mathcal{A}\mathbf{e}_n) \cdot \mathbf{e}_n = \mathbf{e}_n \cdot (\mathcal{A}^*\mathbf{e}_n)$, ezért $\mathcal{A}^*\mathbf{e}_n \in \langle \mathbf{e}_1, \ldots, \mathbf{e}_{n-1} \rangle = \langle \mathbf{f}_1, \ldots, \mathbf{f}_{n-1} \rangle$. Így S_2 szerint $\mathcal{A}^*\mathbf{e}_n \perp \mathbf{f}_n$, azaz $0 = \mathbf{f}_n \cdot (\mathcal{A}^*\mathbf{e}_n) = (\mathcal{A}\mathbf{f}_n) \cdot \mathbf{e}_n = \mathbf{e}_n \cdot \mathbf{e}_n$, ami ellentmondás. Tehát valóban $\mathbf{f}_n = \lambda_n \mathbf{e}_n$.

Az eljárást folytatva ugyanígy (vagy teljes indukcióval) minden i-re $\mathbf{f}_i = \lambda_i \mathbf{e}_i$ adódik. Most megmutatjuk, hogy minden $|\lambda_i|$ egyenlő. Legyen $\mathcal{A}$ egy olyan lineáris transzformáció, amelyre $\mathcal{A}\mathbf{f}_1 = \mathbf{f}_2$. Ekkor S_2 szerint $1 = \mathbf{f}_2 \cdot \mathbf{f}_2 = (\mathcal{A}\mathbf{f}_1) \cdot \mathbf{f}_2 = \mathbf{f}_1 \cdot (\mathcal{A}^*\mathbf{f}_2)$. Ha $\mathbf{v} = \mathcal{A}^*\mathbf{f}_2 = \sum_{i=1}^n \alpha_i \mathbf{f}_i$, akkor $\mathbf{f}_1 \cdot \mathbf{v} = \alpha_1$, tehát $\alpha_1 = 1$. Tekintsük most S_1 szerint ugyanezeket a skalárszorzatokat. Ekkor $\mathbf{f}_2 \cdot \mathbf{f}_2 = (\lambda_2 \mathbf{e}_2) \cdot (\lambda_2 \mathbf{e}_2) = |\lambda_2|^2$, míg a vele továbbra is egyenlő $\mathbf{f}_1 \cdot \mathbf{v} = (\lambda_1 \mathbf{e}_1) \cdot (\sum_{i=1}^n \alpha_i \lambda_i \mathbf{e}_i) = \overline{\lambda_1} \lambda_1 \alpha_1 = |\lambda_1|^2$, tehát $|\lambda_1| = |\lambda_2|$. Ugyanígy kapjuk, hogy minden $|\lambda_i|$ egyenlő.

Jelöljük λ-val a $|\lambda_i|^2$-ek közös értékét. Megmutatjuk, hogy ekkor $S_1 = \lambda S_2$. Vegyünk két tetszőleges vektort, $\mathbf{c}$-t és $\mathbf{d}$-t, és írjuk fel ezeket az $\mathbf{f}_i$-k, illetve $\mathbf{e}_i$-k lineáris kombinációjaként: $\mathbf{c} = \sum_{i=1}^n \gamma_i \mathbf{f}_i = \sum_{i=1}^n \gamma_i \lambda_i \mathbf{e}_i$, $\mathbf{d} = \sum_{i=1}^n \delta_i \mathbf{f}_i = \sum_{i=1}^n \delta_i \lambda_i \mathbf{e}_i$. Ekkor $\mathbf{c}$ és $\mathbf{d}$ skalárszorzata S_2 szerint véve $\rho_2 = \sum_{i=1}^n \overline{\gamma_i} \delta_i$, S_1 szerint véve pedig $\rho_1 = \sum_{i=1}^n |\lambda_i|^2 \overline{\gamma_i} \delta_i = \lambda \rho_2$, amint állítottuk.

9. Kombinatorikai alkalmazások

• **9.1.1(a)** 20 kérdés nyilván elég, kevesebb viszont nem, még akkor sem, ha Micimackó előre elhatározza, hogy mindig 0-t fog válaszolni. Ekkor ugyanis egy 20 ismeretlenes, 19 egyenletből álló homogén lineáris egyenletrendszert kapunk. Ennek a csupa nulla megoldáson kívül van nem triviális (racionális, és így egész számokból álló) megoldása is, tehát az x_i-k nem határozhatók meg egyértelműen.

• **(b)** Két kérdés elég: (i) $x_1 + x_2 + \ldots + x_{20}$, és ha erre a válasz N, akkor (ii) $x_1 + x_2(N+1) + x_3(N+1)^2 + \ldots + x_{20}(N+1)^{19}$. Egy kérdés nem elég:

legyen ez $c_1x_1 + c_2x_2 + \ldots + c_{20}x_{20}$, ahol pl. c_1 és c_2 mondjuk pozitív; ekkor $x_1 = 2c_2, x_2 = c_1, x_3 = \ldots = 1$ és $x_1 = c_2, x_2 = 2c_1, x_3 = \ldots = 1$ esetén ugyanazt a választ kapjuk.

• **(c)** Itt már egyetlen kérdés is elég. Tegyük fel először, hogy az x_i-k pozitívak. Ekkor megfelel $U = x_1 + (x_1 + x_2)^2 + \ldots + (x_1 + x_2 + \ldots + x_{20})^{20}$. Ugyanis $(x_1 + x_2 + \ldots + x_{20})^{20} < U < (1 + x_1 + x_2 + \ldots + x_{20})^{20}$, ahonnan U huszadik gyökének egész része $x_1 + \ldots + x_{20}$, ami ezzel ismertté vált és leválasztható. Az eljárást folytatva megkapjuk az $x_1 + \ldots + x_{19}$ stb. értékeket, és innen minden x_i meghatározható. Ha x_i negatív is lehet, akkor megfelel, ha az U-ra megadott fenti képletben x_i helyére $(3x_i + 1)^2$-t írunk.

• **9.1.2** *Első bizonyítás*:

(i) Először racionális számokra igazoljuk az állítást. Vegyük észre, hogy a számokat egy konstanssal beszorozva, vagy egy konstanst hozzájuk adva a feltételek nem változnak meg. Ezt felhasználva, pozitív egészekre a számok összege (vagy legnagyobbika) szerinti teljes indukcióval könnyen célhoz érünk. Ezután a racionális számok esetét beszorzással, majd eltolással a pozitív egészekre vezethetjük vissza.

(ii) Az általános esetre rátérve, tekintsük az adott 13 valós számot. Ezeknek a racionális számokkal képezett összes lineáris kombinációi egy legfeljebb 13-dimenziós vektorteret alkotnak a racionális számok felett a szokásos műveletekre. Vegyünk ebben egy bázist, és írjuk fel az eredetileg adott számainkat mint a báziselemek racionális együtthatós lineáris kombinációit. A feladat feltételei így azt jelentik, hogy ugyanezek a feltételek valamennyi komponensben teljesülnek. Mivel a báziselemek együtthatói már racionális számok, ezért az (i) rész alapján azt kapjuk, hogy a számaink valamennyi komponensben megegyeznek, azaz maguk is egyenlők.

• *Második bizonyítás*: Legyenek a számok $x_1, x_2, \ldots, x_{13}$. Alkalmas eltolás után feltehető, hogy $x_1 = 0$. A feladat feltétele azt jelenti, hogy az x_i-kből képezett bizonyos összegek megegyeznek. Ezeket felírva és átrendezve egy homogén lineáris egyenletrendszert kapunk, 13 egyenlettel és ($x_1 = 0$ miatt csak) 12 ismeretlennel. A feladathoz azt kell megmutatnunk, hogy az egyenletrendszernek csak triviális megoldása létezik.

Az első bizonyítás (i) része alapján ez racionális számokra igaz. Belátjuk, hogy a valós számok körében sem kaphatunk más megoldást. Mivel az egyenletrendszer megoldása (Gauss-féle kiküszöbölés) során mindvégig az együtthatókkal csak a négy alapműveletet végezzük, tehát ugyanahhoz az eredményhez jutunk, akár a racionális, akár a valós számok körében keressük a megoldásokat, hiszen a kiindulási együtthatók racionálisak voltak (± 1 és 0). (Vö. a 3.4.8, 4.4.11 és 4.6.16 feladatokkal.)

• *Harmadik bizonyítás*: A 3.4.8, illetve 4.4.11 feladatok alapján elég azt igazolni, hogy a második bizonyításban leírt egyenletrendszernek a modulo 2 testben csak a triviális megoldása létezik. (Ebből ugyanis az említett feladatok bármelyike szerint már következik, hogy a valós számok körében sincs más megoldás.) Modulo 2 viszont az igazolandó állítás csak annyit mond ki, hogy ha a megfelelő hatos összegek paritása megegyezik, akkor mind a 13 szám azonos paritású, ez pedig nyilvánvaló.

• *Negyedik bizonyítás*: A racionálisról a valósra történő átmenet eszköze most nem a(z elemi) lineáris algebra, hanem az elemi számelmélet lesz. Az adott valós számokat nagyon jól közelítjük majd racionálisokkal, és arra fogunk támaszkodni, hogy ezekre a közelítő törtekre már igaz az állítás.

Lemma: Tetszőleges $x_1, x_2, \ldots, x_m$ valós számokhoz és N pozitív egészhez léteznek olyan $a_1, a_2, \ldots, a_m$ egészek és $b \leq N^m$ természetes szám, amelyekre

$$\left| x_i - \frac{a_i}{b} \right| \leq \frac{1}{Nb} \qquad i = 1, 2, \ldots, m.$$

A lemma bizonyítása: Minden $1 \leq t \leq N^m + 1$ egész számra készítsük el a $\mathbf{v}_t = (\{tx_1\}, \ldots, \{tx_m\})$ vektorokat, ahol (*) $\{y\} = y - \lfloor y \rfloor$, tehát $\{y\}$ az y szám ún. törtrésze, azaz a hozzá balról legközelebbi egésztől mért távolsága. A skatulyaelv alapján lesz olyan $t \neq s$, hogy a $\mathbf{v}_t$ és $\mathbf{v}_s$ vektorok bármely komponensében az eltérés legfeljebb $1/N$. Beírva (*)-ot, így azt kapjuk, hogy valamilyen a_i egészekkel és $b = |s-t|$-vel $|bx_i - a_i| \leq 1/N$ teljesül minden i-re. Ez pedig éppen a lemma állítása.

A feladat bizonyításához alkalmazzuk a lemmát az adott x_i valós számokra és $N \geq 13$-ra. A feladat feltételeiben szereplő egyenlőségekben az x_i-k helyett a közelítő a_i/b-ket írva, a két oldal eltérése a lemma alapján legfeljebb $12/(Nb) < 1/b$, de mivel mindkét oldalon b nevezőjű törtek állnak, így a két oldal csak egyenlő lehet. Vagyis a közelítő törtekre is teljesülnek a feladat feltételei. Ekkor tudjuk, hogy a közelítő törtek szükségképpen valamennyien egyenlők. Ugyanezt tetszőlegesen nagy N-ekre elvégezve adódik, hogy a valós számok is mind meg kell hogy egyezzenek.

• **9.1.4(a)/(i)** Válasz: $\lceil \log_2 m \rceil$. Először megmutatjuk, hogy ennyi alkalmas összeadandó elég. Ha m nem kettőhatvány, akkor az i-edik összeadandó vektor j-edik koordinátája legyen $r_{ij}2^{i-1}$, ahol r_{ij} a j szám kettes számrendszerbeli felírásában hátulról az i-edik jegy ($1 \leq i \leq \lceil \log_2 m \rceil$, $1 \leq j \leq m$). Ekkor mindegyik vektorban csak kétféle koordináta-érték fordul elő (hiszen $r_{ij} = 0$ vagy 1). A vektorok összege valóban a kívánt vektor, ugyanis a j-edik koordináták összege éppen a j szám kettes számrendszer szerinti előállítása. Ha

az m kettőhatvány, akkor a megadott $\mathbf{z} = \begin{pmatrix} 1 \\ 2 \\ \vdots \\ m \end{pmatrix}$ vektor helyett a $\begin{pmatrix} 0 \\ 1 \\ \vdots \\ m-1 \end{pmatrix}$ vektorra készítsük el a fenti konstrukciót, majd valamelyik összeadandó vektor mindegyik komponenséhez adjunk hozzá 1-et.

Most belátjuk, hogy $\lceil \log_2 m \rceil$-nél kevesebb összeadandó nem elég. Ha összeadunk t darab unalmas vektort, akkor az összegvektor minden koordinátája egy olyan t-tagú összeg, ahol minden tag (legfeljebb) kétféle értéket vehet fel. Ennélfogva egy ilyen összeg legfeljebb 2^t-féle lehet, tehát az összegvektor koordinátái között legfeljebb ennyi különböző érték szerepel. A $\mathbf{z}$ vektorunknak mind az m koordinátája különböző, ezért ha t darab unalmas vektor összegeként előállítható, akkor szükségképpen $2^t \geq m$, azaz $t \geq \lceil \log_2 m \rceil$.

• **(a)/(ii)** Válasz: $m-1$. Először megmutatjuk, hogy ennyi alkalmas összeadandó elég:

$$\begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_3 \\ \beta_4 \\ \vdots \\ \beta_m \end{pmatrix} = \begin{pmatrix} \beta_1 \\ \beta_2 \\ \beta_1 \\ \beta_1 \\ \vdots \\ \beta_1 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ \beta_3 - \beta_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \begin{pmatrix} 0 \\ 0 \\ 0 \\ \beta_4 - \beta_1 \\ \vdots \\ 0 \end{pmatrix} + \ldots + \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ \vdots \\ \beta_m - \beta_1 \end{pmatrix}.$$

Most belátjuk, hogy $m-1$-nél kevesebb összeadandó nem elég. Ha egy vektor minden koordinátájához ugyanazt a számot hozzáadjuk, akkor nyilván mindkét vektor ugyanannyi unalmas vektor összegeként írható fel. Ezért elegendő olyan vektorok előállítását vizsgálni, amelyeknek az első koordinátája 0. Ezután hasonlóan igazolható, hogy az összeadandóként szereplő unalmas vektorokról is feltehetjük, hogy az első koordinátájuk 0. Tegyük fel, hogy minden $\mathbf{v} = \begin{pmatrix} 0 \\ \beta_2 \\ \beta_3 \\ \vdots \\ \beta_m \end{pmatrix}$ vektor előáll t darab olyan $\mathbf{u}_j$ unalmas vektor összegeként, amelyek első koordinátája 0. A j-edik összeadandó többi koordinátája ekkor 0 vagy valamilyen x_j valós szám. Az összegelőállítást koordinátánként felírva és az első koordinátára vonatkozó semmitmondó $0+0+\ldots+0=0$ azonosságot elhagyva, a többi $m-1$ koordinátára olyan t ismeretlenes, $m-1$ egyenletből álló egyenletrendszereket kapunk, amelyeknél (a „bal oldalon") minden együttható 0 vagy 1 aszerint, hogy az illető $\mathbf{u}_j$ unalmas vektor adott koordinátája

0 vagy x_j. (Az összes lehetséges együtthatóválasztásnak megfelelően az ilyen egyenletrendszerek száma $2^{t(m-1)}$, illetve $\binom{2^{m-1}+t-1}{t}$, ha az összeadandó vektorok sorrendje közömbös.) Ha minden $\mathbf{v}$ vektor előáll a kívánt módon, ez azt jelenti, hogy bármilyen $\beta_2, \beta_3, \ldots, \beta_m$ „jobb oldal" esetén legalább az egyik ilyen típusú egyenletrendszer megoldható. Ha $t < m-1$, azaz az ismeretlenek száma kisebb az egyenletek számánál, akkor egy ilyen egyenletrendszer nem lehet tetszőleges jobb oldal esetén megoldható, ezért azok a $\mathbf{v}' = \begin{pmatrix} \beta_2 \\ \beta_3 \\ \vdots \\ \beta_m \end{pmatrix}$ jobb oldalak, amelyekre megoldható, egy valódi alteret alkotnak $\mathbf{R}^{m-1}$-ben. Véges sok valódi altér egyesítése nem adhatja ki a vektorteret (4.2.12e feladat), így azok a $\mathbf{v}'$ jobb oldalak, amelyekre legalább az egyik ilyen egyenletrendszer megoldható, együttesen sem merítik ki $\mathbf{R}^{m-1}$-et, azaz van olyan vektor, amely nem áll elő t darab unalmas vektor összegeként.

• **(b)** Válasz: (i): $\lceil \log_k m \rceil$. (ii): $\lceil (m-1)/(k-1) \rceil$ (ha $m \geq k$). A bizonyítás az imént látott $k = 2$ eset mintájára történhet. Az (i) résznél k alapú számrendszert kell használni. A (ii) résznél az összeadandó unalmas vektorok mindegyikéhez nem 1, hanem $k-1$ ismeretlen tartozik, hiszen a 0-n kívül ennyiféle koordinátájuk lehet.

• **(c)/(i)** Válasz: $\lceil \log_k s \rceil$, ahol $s = \min(m, p)$. Ez a korábbi meggondolásokhoz hasonlóan adódik, azzal a kiegészítéssel, hogy az ismétlődő koordinátaértékek nyilván nem számítanak.

• **(c)/(ii)** A korábban látott gondolatmenet akkor alkalmazható, ha p elegendően nagy m-hez képest (4.2.12f feladat). Kis p esetén azonban nemcsak a módszerrel van baj, hanem a válasz is módosul: mivel $\lceil \log_k p \rceil$ unalmas vektor az (i)-beli konstrukció alapján mindenképpen elegendő, ezért $p \leq k^{(m-k)/(k-1)}$ esetén a keresett minimum biztosan kisebb lesz a valós számokra kapott $\lceil (m-1)/(k-1) \rceil$ értéknél.

• **9.1.5(a)** Válasz: 5. Először megmutatjuk, hogy 5 forduló elég. Számozzuk meg a gyerekeket 0-tól 31-ig, és írjuk fel a sorszámokat kettes számrendszerben. Megfelelő lesz, ha az egyes fordulókban aszerint képezzük a (16 fős) csapatokat, hogy az 1., 2., ..., 5. számjegy 0 vagy 1.

Most belátjuk, hogy kevesebb forduló nem elég. Feltehetjük, hogy minden fordulóban minden diák játszik (a pihenőket berakjuk akármelyik csapatba). Az első fordulóban valamelyik csapatban legalább 16-an vannak. Közülük a második fordulóban legalább 8-an ugyanabban a csapatban szerepelnek.

Ezek közül a harmadik fordulóban legalább 4-en csapattársak, a negyedik fordulóban pedig legalább ketten, ők tehát egyszer sem voltak ellenfelek.

• **(b)** Könnyen látható, hogy 31 forduló elegendő; egy lehetséges lebonyolítás a következő. Az első fordulóban az egyik csapat egyetlen diákból áll, a másik csapat a többi 31-ből. A második fordulóban a 31 diákból egy alkotja az egyik csapatot, a többi 30 a másikat stb.

Most megmutatjuk, hogy 30 vagy kevesebb fordulóval a feltételeket nem lehet teljesíteni. Készítsünk egy 32 szögpontú teljes gráfot. A csúcsokat feleltessük meg a diákoknak, az i-edik csúcs mellé írjunk egy később alkalmasan megválasztandó x_i valós számot, $i = 1, 2, 3, \ldots, 32$, az i-edik és a j-edik csúcsot összekötő élre pedig írjuk az $x_i x_j$ szorzatot.

Tegyük fel indirekt, hogy 30 vagy kevesebb fordulóban lebonyolítható a verseny. Azt, hogy az i-edik és a j-edik tanuló (valamikor) egymás ellenfele, az őket összekötő élen levő $x_i x_j$ szorzattal hozzuk kapcsolatba.

Tekintsük az összes élen levő szorzatok S összegét.

$$S = \sum_{1 \le i < j \le 32} x_i x_j = \frac{1}{2}\Big[(\sum_{m=1}^{32} x_m)^2 - \sum_{m=1}^{32} x_m^2\Big] \tag{M.9.1}$$

Számoljuk most meg, hogy egy-egy fordulóban a szembenálló csapatok „menynyivel járulnak hozzá" az S összeghez: legyen S_t a t-edik fordulóban az „ellenfél" diákokat összekötő élekre írt $x_i x_j$ szorzatok összege. Mivel a verseny során bármely két diák pontosan egyszer lesz egymás ellenfele, így

$$S = \sum_{t=1}^{r} S_t \quad , \tag{M.9.2}$$

ahol r a fordulók számát jelöli. Másrészt

$$S_t = (\sum_{k \in C_{1t}} x_k)(\sum_{l \in C_{2t}} x_l), \tag{M.9.3}$$

ahol C_{1t}, illetve C_{2t} jelöli a t-edik forduló két csapatát, ugyanis egy adott fordulóban az egyik csapat minden tagja a másik csapat minden tagjának ellenfele, tehát minden olyan $x_k x_l$ szorzatot össze kell adni, ahol k az első, l pedig a második csapatban szerepel.

Az (M.9.1), (M.9.2) és (M.9.3) képletek alapján az alábbi egyenlőséget kapjuk:

$$\frac{1}{2}\Big[(\sum_{m=1}^{32} x_m)^2 - \sum_{m=1}^{32} x_m^2\Big] = \sum_{t=1}^{r}\Big(\sum_{k \in C_{1t}} x_k\Big)\Big(\sum_{l \in C_{2t}} x_l\Big). \tag{M.9.4}$$

Az (M.9.4) egyenlőség egy azonosság: az $x_1, x_2, \ldots, x_{32}$ értékek tetszőleges megválasztása mellett fenn kell állnia. Válasszuk most meg ezeket úgy, hogy

$$\sum_{m=1}^{32} x_m = 0 \qquad \text{és} \qquad \sum_{k \in C_{1t}} x_k = 0, \quad t = 1, 2, \ldots, r \tag{M.9.5}$$

teljesüljön. Az (M.9.5) homogén egyenletrendszerben az ismeretlenek száma 32, az egyenleteké $r + 1$, ami az indirekt feltevés szerint legfeljebb 31. Így az egyenletrendszernek van nem triviális (valós) megoldása. Egy ilyen megoldást (M.9.4)-be behelyettesítve

$$\sum_{m=1}^{32} x_m^2 = 0$$

adódik, ami ellentmondás, hiszen valós számok négyzetösszege csak akkor lehet 0, ha mindegyikük 0 volt.

• *Megjegyzés*: Tulajdonképpen azt láttuk be, hogy ha egy n csúcsú teljes gráfot éldiszjunkt teljes páros gráfok uniójára bontunk, akkor minimálisan $n-1$ páros gráf szükséges ehhez. Ha azonban az élidegenség feltételét elejtjük, akkor ez a szám az (a) rész gondolatmenete szerint $\lceil \log_2 n \rceil$-re csökken.

• **9.2.16** *Első megoldás*: Az útmutatást követve, az olyan, n darab $+1$-ből és $n-1$ darab -1-ből álló sorozatok számát kell meghatároznunk, amelyekben az elejétől számítva akárhány tag összege pozitív. Ebből a szempontból nyilván rosszak a -1-gyel kezdődő sorozatok. A $+1$-gyel kezdődő rossz sorozatoknál keressük meg az első 0 részösszeget, és a sorozat addig terjedő elemeit szorozzuk meg -1-gyel. Ekkor egy -1-gyel kezdődő sorozatot kapunk. Megfordítva, bármely -1-gyel kezdődő sorozatnál keressük meg az első 0 részösszeget (ilyen biztosan van, hiszen a $+1$-ek száma nagyobb a -1-ek számánál), és a sorozat addig terjedő elemeit -1-gyel megszorozva egy $+1$-gyel kezdődő rossz sorozathoz jutunk. Ily módon tehát kölcsönösen egyértelmű megfeleltetést létesítettünk a $+1$-gyel kezdődő rossz sorozatok és a -1-gyel kezdődő („automatikusan" rossz) sorozatok között. Az összes rossz sorozatok száma ennélfogva a -1-gyel kezdődő sorozatok számának a duplája, azaz $2\binom{2n-2}{n-2}$. Ezt az összes sorozatok számából levonva megkapjuk a „jó" sorozatok számát: $\binom{2n-1}{n-1} - 2\binom{2n-2}{n-2} = \binom{2n-2}{n-1}/n$.

• *Második megoldás*: Az útmutatást követve, az $A(z) = \sum_{n=1}^{\infty} \alpha_n z^n$ hatványsorra az $A^2(z) = A(z) - z$ egyenletet kapjuk. Célunk az α_n együtthatók meghatározása. Az egyenletet $A(z)$-re megoldva $A(z) = (1 \pm \sqrt{1-4z})/2$. Itt az

$(1-4z)^{1/2}$ kifejezést binomális sorba fejtve $A(z) = (1 \pm \sum_{n=0}^{\infty} \binom{1/2}{n}(-4z)^n)/2$ adódik. Itt a $\sum$ előtt a negatív előjelet kell venni, ugyanis $A(z)$ hatványsorában pl. a konstans tag 0 (vagy mert minden további α_n együttható pozitív). A kétféle hatványsoralak összehasonlításából $\alpha_n = \binom{1/2}{n}4^n(-1)^{n+1}/2$, amiből némi technikai átalakítás után $\alpha_n = \binom{2n-2}{n-1}/n$ adódik.

• *Harmadik megoldás*: Legyen β_n az n szám lehetséges szorzatainak a száma, ha még a tényezők sorrendje is cserélődhet, ekkor $\beta_n = n!\alpha_n$. Megmutatjuk, hogy (*) $\beta_n = (4n-6)\beta_{n-1}$. Nézzünk az $a_1, a_2, \ldots, a_{n-1}$ számokból egy tetszőleges szorzatot. Ez $n-2$ szorzást jelent. Az a_n számot megszorozhatjuk az első szorzás bármelyik tényezőjével balról vagy jobbról, a második szorzás bármelyik tényezőjével balról vagy jobbról stb., végül a kész szorzattal balról vagy jobbról, ez tehát $4(n-2)+2 = 4n-6$ lehetőség az a_n beillesztésére. Ezzel a (*) rekurziót beláttuk. Ennek ismételt alkalmazásával kapjuk, hogy $\beta_n = 2^{n-1}(2n-3)!!$, ahonnan $\alpha_n = \binom{2n-2}{n-1}/n$.

• **9.3.2** Tegyük fel indirekt, hogy a kongruenciarendszernek csak triviális megoldása van. Ekkor az

$$F(\mathbf{x}) = \prod_{i=1}^{k}\bigl(1 - f_i^{p-1}(x_1, x_2, \ldots, x_t)\bigr) \equiv \prod_{j=1}^{t}(1 - x_j^{p-1}) = G(\mathbf{x}) \pmod{p}$$

kongruencia azonosságként teljesül, ugyanis ha mindegyik $x_i \equiv 0 \pmod{p}$, akkor mindkét oldal 1-gyel kongruens, minden más esetben pedig van olyan i, illetve j, hogy $f_i \not\equiv 0$, $x_j \not\equiv 0$, azaz a kis-Fermat-tétel alapján $f_i^{p-1} \equiv 1$, $x_j^{p-1} \equiv 1$, vagyis mindkét oldalon szerepel egy 0 tényező, és így mindkét oldal 0-val kongruens. A két oldalon álló (a modulo p test feletti) F és G polinomnak tehát minden helyettesítési értéke megegyezik.

Nevezzük egy H polinom redukált alakjának azt a H^* polinomot, amelyet H-ból úgy kapunk, hogy H-ban mindenhol x_i^p helyére x_i-t írunk, ameddig csak lehetséges. Nyilván H^* minden tagjában bármelyik x_i kitevője legfeljebb $p-1$, továbbá H és H^* minden helyettesítési értéke megegyezik. A változók száma szerinti teljes indukcióval könnyen megmutatható, hogy ha a H^* és K^* polinomok minden helyettesítési értéke megegyezik, akkor a H^* és K^* polinomok (formálisan is) egyenlők.

Láttuk, hogy az F és G polinomok minden helyettesítési értéke megegyezik, ezért ugyanez érvényes az F^* és G^* polinomokra is. Az előzőek szerint ekkor az F^* és G^* polinomok meg kell hogy egyezzenek. Ez azonban lehetetlen, ugyanis $G = G^*$ és a $\sum_{i=1}^{k} \deg f_i < t$ feltétel miatt $\deg G^* = t(p-1) > \deg F \geq \deg F^*$.

• **9.4.10** A keresett maximum értéke k. Többféleképpen is megadható k ilyen részhalmaz: Jelöljük a halmaz egyik elemét x_1-gyel, ekkor megfelelnek pl. az x_1-et tartalmazó egy- és kételemű részhalmazok, vagy itt az $\{x_1\}$ részhalmaz kicserélhető a komplementerére. Bizonyos k-kra további lehetőséget jelentenek az ún. (nem elfajuló) *véges projektív síkok* (lásd a Megjegyzést a megoldás végén). Arra, hogy k-nál több ilyen részhalmaz már nem adható meg, két bizonyítást mutatunk.

• *Első bizonyítás*: Az útmutatást követve belátjuk, hogy a $H_1, \ldots, H_n$ halmazoknak megfelelő $\mathbf{h}_1, \ldots, \mathbf{h}_n$ szokásos 0–1 vektorok lineárisan függetlenek a valós test felett. A $\delta_1\mathbf{h}_1 + \ldots + \delta_n\mathbf{h}_n = \mathbf{0}$ valós együtthatós lineáris kombinációnak önmagával való skalárszorzata átrendezés után a

$$(\sum_{j=1}^{n} \delta_j)^2 + \sum_{j=1}^{n} \delta_j^2(|H_j| - 1) = 0$$

összefüggést adja. Nemnegatív számok összege csak úgy lehet 0, ha minden összeadandó 0, továbbá a feltételek szerint legfeljebb egy kivétellel minden $|H_j| > 1$. Innen kapjuk, hogy valóban mindegyik $\delta_j = 0$.

• *Második bizonyítás*: Legyenek az X halmaz elemei az $x_1, x_2, \ldots, x_k$ „pontok". Egy $x \in X$ pont *fok*án az őt tartalmazó H_j részhalmazok számát értjük: $d(x) = \big|\{j \,|\, x \in H_j\}\big|$.

Megmutatjuk, hogy $x \notin H_j \Rightarrow d(x) \leq |H_j|$. Ha ugyanis $x \in H_t$ és $x \in H_i$ (ahol $t \neq i$), akkor $H_t \cap H_j \neq H_i \cap H_j$, ugyanis $H_t \cap H_i$-nek x az egyetlen közös eleme. Ezért az x-et tartalmazó H_t-k mindegyike más pontot metsz ki H_j-ből, vagyis valóban $d(x) \leq |H_j|$.

Ha indirekt feltesszük, hogy $k < n$, akkor bármely $x \notin H_j$-re a $d(x) \leq |H_j|$ egyenlőtlenségből

$$\frac{d(x)}{n - d(x)} < \frac{|H_j|}{k - |H_j|} \tag{M.9.6}$$

következik. Ezt az összes $x \notin H_j$ párra összegezve $\sum_{x \in X} d(x) < \sum_{j=1}^{n} |H_j|$ adódik, ami ellentmondás, hiszen itt a fokszám definíciója alapján nyilván egyenlőségnek kell állnia.

• *Megjegyzés*: Mindkét bizonyításból (egymástól eltérő) további információkat is leolvashatunk. Az első bizonyítás átvihető arra az esetre is, ha bármely két részhalmaznak ugyanannyi (pozitív számú, de nem feltétlenül egyetlen) közös eleme van (ezt a gondolatmenetet kell a 9.4.11 feladat megoldásában felhasználni). A második bizonyításból pedig kiderül, hogyan kapjuk meg az $n = k$ esetben a megfelelő halmazokat. Az (M.9.6)-beli bal oldali tört nevezője 0, ha x mind a k részhalmaznak közös eleme, ekkor az x-et tartalmazó egy- és kételemű részhalmazokról van szó (ez volt a megoldás elején

felsorolt első példa). Ettől a triviális esettől eltekintve a törtek értelmesek, és ugyanúgy ellentmondásra jutunk, kivéve ha minden $x \notin H_j$ párra $d(x) = |H_j|$ teljesül. A H_j halmazokat egyeneseknek (az x elemeket pedig továbbra is pontoknak) nevezve ez azt jelenti, hogy bármely két ponton egy egyenes megy át, és bármely két egyenesnek egy közös pontja van. Ezek pedig éppen a véges projektív síkok (a megoldás elején felsorolt második példa egy elfajuló projektív síkot jelent, amikor a pontok egy kivételével egy egyenesre esnek).

• **9.4.12** Megfelel, ha vesszük az összes legfeljebb m elemű részhalmazt, ezek száma $\sum_{i=0}^{m} \binom{k}{i}$. Belátjuk, hogy ez a maximum. Tekintsük a $H_1, \ldots, H_n$ halmazoknak megfelelő $\mathbf{h}_1, \ldots, \mathbf{h}_n$ szokásos 0–1 vektorokat, és legyen a $t \neq j$ párokhoz tartozó összes $|H_t \cap H_j|$ érték $\beta_1, \ldots, \beta_m$.

Vegyük észre, hogy a feltétel alapján bármely $t \neq j$-re a $\prod_{u=1}^{m}(\mathbf{h}_t \cdot \mathbf{h}_j - \beta_u)$ szorzat szükségképpen nulla. Definiáljuk ennek megfelelően a k-változós $f_1, \ldots, f_n$ valós együtthatós polinomokat a következőképpen: $f_j(\mathbf{x}) = \prod_{u=1}^{m}(\mathbf{x} \cdot \mathbf{h}_j - \beta_u)$. Ekkor $f_j(\mathbf{h}_t) = 0$, ha $t \neq j$, és így az f_j-k lineáris függetlenségét kényelmesen be tudnánk látni, ha $f_j(\mathbf{h}_j) \neq 0$ is teljesülne. Ez azonban sajnos nem feltétlenül igaz, ezért a konstrukciót egy kicsit finomítani kell.

A problematikus $f_j(\mathbf{h}_j) = 0$ feltétel azt jelenti, hogy $|H_j|$ megegyezik valamelyik β_u-val. Ezért ezt a(z esetleges) tényezőt hagyjuk ki, vagyis legyen g_j azoknak az $(\mathbf{x} \cdot \mathbf{h}_j - \beta_u)$ tényezőknek a szorzata, ahol $\beta_u \neq |H_j|$. Feltehetjük, hogy $|H_1| \leq |H_2| \leq \ldots \leq |H_n|$, ekkor nyilván

$$g_j(\mathbf{h}_t) \begin{cases} = 0, & \text{ha } t < j; \\ \neq 0, & \text{ha } t = j. \end{cases}$$

A g_j-k lineárisan függetlenek a valós test felett, mert a $\sum_{j=1}^{n} \lambda_j g_j = 0$ polinomegyenlőségbe $\mathbf{h}_1, \ldots, \mathbf{h}_n$-et ebben a sorrendben egymás után behelyettesítve rendre kapjuk, hogy $\lambda_1 = \ldots = \lambda_n = 0$.

Valamennyi g_j egy k-változós legfeljebb m-edfokú polinom, így a függetlenség miatt számuk legfeljebb annyi, mint ennek a térnek a dimenziója. Ez sajnos még mindig nem adja ki a kívánt becslést, azonban a következő észrevétellel ezen is segíteni tudunk. A polinomokba csak a $\mathbf{h}_j$ vektorokat kellett behelyettesíteni, és ezek minden koordinátája 0 vagy 1. Mivel $0^2 = 0$, $1^2 = 1$, ezért a helyettesítési értékek ugyanazok maradnak, ha a változók magasabb hatványait az első hatványra redukáljuk, azaz elég, ha minden változó csak az első hatványon szerepel.

Legyen ennek megfelelően ($j = 1, 2, \ldots, n$-re) G_j az a polinom, amelyet g_j-ből úgy kapunk, hogy minden egyes x_s változónál x_s^2 helyére x_s-et írunk,

amíg ez csak lehetséges. Ekkor az előbbiek szerint $G_j(\mathbf{h}_t) = g_j(\mathbf{h}_t)$ minden t, j-re. Ennélfogva a fenti gondolatmenetet a g_j-k helyett a G_j-kre alkalmazva kapjuk, hogy a G_j-k is függetlenek. Másrészt a G_j-k benne vannak az $1, x_1, \dots, x_k, x_1x_2, \dots, x_{k-1}x_k, x_1x_2x_3, \dots, x_1x_2 \cdot \dots \cdot x_m, \dots$ polinomok által generált altérben. A generátorelemek száma $\sum_{i=0}^{m} \binom{k}{i}$, tehát a dimenzió, és így (a lineáris függetlenség miatt) a G_j-k száma is legfeljebb ennyi.

• **9.4.18** Legyenek $S_1, \dots, S_b$, illetve $T_1, \dots, T_c$ a páros, illetve páratlan elemszámú részhalmazok ($b + c = n$). A feltétel szerint bármely két (különböző) részhalmaz metszete páros elemszámú. Ekkor az S_j, illetve T_i halmazoknak megfelelő $\mathbf{s}_j$, illetve $\mathbf{t}_i$ szokásos 0–1 vektorok páronként merőlegesek, sőt az $\mathbf{s}_j$-k önmagukra is merőlegesek (az F_2 testet használjuk). Legyen az $\mathbf{s}_j$-k, illetve a $\mathbf{t}_i$-k által generált altér U_s, illetve U_t, és ezek dimenziója s, illetve t. A Páratlanváros-tétel bizonyítása szerint a $\mathbf{t}_i$ vektorok függetlenek, ezért $t = c$, továbbá nyilván $b \le 2^s$, tehát $n = b + c \le t + 2^s$.

Megmutatjuk, hogy $U_s \cap U_t = \mathbf{0}$. Legyen $\mathbf{x} \in U_s \cap U_t$, azaz $\mathbf{x} = \sum_{j=1}^{b} \lambda_j \mathbf{s}_j = \sum_{i=1}^{c} \mu_i \mathbf{t}_i$. Vegyük mindkét oldalnak a skalárszorzatát $\mathbf{t}_m$-mel, ekkor $\mu_m = 0$ adódik. Mivel ez minden m-re igaz, ezért valóban $\mathbf{x} = \mathbf{0}$.

A feltételek szerint $\langle U_s, U_t \rangle \subseteq U_s^{\perp}$, így $s + t = \dim\langle U_s, U_t \rangle \le k - s$, azaz $s \le \lfloor (k-t)/2 \rfloor$. Innen

$$n \le t + 2^s \le t + 2^{\lfloor (k-t)/2 \rfloor} \le 2^{\lfloor k/2 \rfloor} + \begin{cases} 0, & \text{ha } k \text{ páros;} \\ 1, & \text{ha } k \text{ páratlan.} \end{cases}$$

Végül, a felső korlát megvalósulását páros k-ra a 9.4.2 Tétel bizonyításában látott „házaspáros” konstrukció biztosítja, páratlan k-ra pedig a hasonlóan adódó részhalmazok mellé hozzávehetjük pl. magát az egész X-et (azaz az összes lakost magában foglaló egyesületet).

• **9.5.5** I. Az útmutatást követve először azt igazoljuk, hogy ha $f(A) = J$, akkor A minden sajátvektora J-nek is sajátvektora. Ez azonnal adódik a sajátvektor definíciójából.

II. Tegyük most fel, hogy A minden sajátvektora J-nek is sajátvektora. Megmutatjuk, hogy ekkor G reguláris és összefüggő. Mivel A sajátvektorai kifeszítik a teret, ezért az A egyik sajátvektora a $\mathbf{j}$ kell hogy legyen. Ha az ehhez tartozó sajátérték d, akkor G minden csúcsa d-edfokú, tehát G reguláris.

Ha G nem lenne összefüggő, akkor jelöljük az egyik komponensét G_1-gyel, és legyen $\mathbf{u}$ az a vektor, amelynek az i-edik koordinátája $u_i = 1$, illetve 0 aszerint, hogy az i-edik csúcs benne van-e a G_1 komponensben vagy sem. Ekkor

$\mathbf{u}$ sajátvektora A-nak (ugyancsak d sajátértékkel), azonban nem sajátvektora J-nek. Ezzel beláttuk, hogy G valóban összefüggő is.

III. Végül tegyük fel, hogy G reguláris és összefüggő, ekkor meg kell adnunk olyan f polinomot, amelyre $f(A) = J$. A regularitás miatt $\mathbf{j}$ sajátvektora az A-nak d sajátértékkel. Legyen $\mathbf{j}, \mathbf{v}_2, \ldots, \mathbf{v}_n$ az A ortogonális sajátvektoraiból álló bázis és $d, \lambda_2, \ldots, \lambda_n$ a megfelelő sajátértékek. Ekkor $\mathbf{v}_i \in \langle \mathbf{j} \rangle^\perp$, és így $J\mathbf{v}_i = \mathbf{0}$ minden $2 \le i \le n$ esetén.

Megmutatjuk, hogy a d csak egyszeres sajátértéke az A-nak. Tekintsünk egy d-hez tartozó $\mathbf{x}$ sajátvektort és ebben a(z egyik) legnagyobb komponenst. Vizsgáljuk az ehhez tartozó csúcsot és annak a d darab szomszédját; az egyszerűbb jelölés kedvéért tegyük fel, hogy ezek éppen az első $d+1$ csúcs. Ekkor (amint a 9.5.2 feladatban láttuk) $d \cdot x_1 = x_2 + \ldots + x_{d+1} \le d \cdot x_1$, ahonnan kapjuk, hogy $x_1 = x_2 = \ldots = x_{d+1}$. Ugyanezt a gondolatmenetet most az x_1 helyett az $x_2, \ldots, x_{d+1}$-vel megismételve stb., a gráf összefüggőségét kihasználva adódik, hogy minden x_i egyenlő, tehát az $\mathbf{x}$ valóban csak a $\mathbf{j}$ skalárszorosa lehet.

Legyen f olyan (interpolációs) polinom, amelyre $f(d) = n$ és $f(\lambda_2) = \ldots = f(\lambda_n) = 0$ (itt felhasználjuk, hogy $d \ne \lambda_i$). Ekkor $f(A)\mathbf{j} = f(d)\mathbf{j} = n\mathbf{j}$ és $f(A)\mathbf{v}_i = f(\lambda_i)\mathbf{v}_i = \mathbf{0}$, tehát $f(A)$ a $\mathbf{j}, \mathbf{v}_2, \ldots, \mathbf{v}_n$ báziselemeket ugyanoda képezi, mint a J, ennélfogva valóban $f(A) = J$.

• **9.5.10** Az útmutatást követve először az (i) állítást igazoljuk. Legyen A nemnegatív elemű szimmetrikus mátrix, Λ a legnagyobb sajátértéke, $\mathbf{x} \ge \mathbf{0}$, $\mathbf{x} \ne \mathbf{0}$ és $A\mathbf{x} \ge \tau\mathbf{x}$. Legyen továbbá $\mathbf{b}_1, \ldots, \mathbf{b}_n$ ortonormált sajátbázis, $\lambda_1, \ldots, \lambda_n$ a megfelelő sajátértékek és $\mathbf{x} = \sum_{i=1}^n \xi_i \mathbf{b}_i$. Feltehetjük, hogy $\mathbf{x}$ normált, azaz $\mathbf{x}\cdot\mathbf{x} = \sum_{i=1}^n \xi_i^2 = 1$. Ekkor

$$\tau = \mathbf{x}\cdot(\tau\mathbf{x}) \le \mathbf{x}\cdot(A\mathbf{x}) = \sum_{i=1}^n \lambda_i \xi_i^2 \le \Lambda \sum_{i=1}^n \xi_i^2 = \Lambda\,.$$

Ezzel (i)-et beláttuk. Ennek felhasználásával (ii) a következőképpen igazolható. Legyen $\mathbf{z}$ az A' mátrixnak egy, a Λ' maximális sajátértékhez tartozó sajátvektora, $A'\mathbf{z} = \Lambda'\mathbf{z}$. Feltehetjük, hogy $\mathbf{z}$-nek pl. az első koordinátája pozitív. Hagyjuk meg $\mathbf{z}$ nemnegatív koordinátáit, és a(z esetleges) negatív koordináták helyére írjunk 0-t, az így kapott (nemnegatív) vektor legyen $\mathbf{x}$. Könnyen láthatóan $A\mathbf{x} \ge A'\mathbf{x} \ge \Lambda'\mathbf{x}$, és így (i) alapján valóban $\Lambda \ge \Lambda'$.

Rátérünk a(z eredeti) feladatnak a csúcsok száma szerinti teljes indukciós bizonyítására. Legyen $k = \Lambda + 1$, meg kell mutatnunk, hogy a gráf k színnel kiszínezhető. Ha csak egy csúcs van, akkor az egyetlen sajátérték a $\Lambda = 0$, tehát $k = \Lambda + 1 = 1$, és egy szín nyilván elég. Vegyünk most egy n csúcsú

G gráfot, és hagyjuk el a(z egyik) legkisebb fokszámú csúcsot a hozzá tartozó élekkel. Az elhagyott csúcs foka a 9.5.9 feladat szerint $\leq \Lambda = k-1$. A megmaradó G_1 gráfhoz vegyük hozzá az elhagyott csúcsot izolált pontként, az élek nélkül, az így kapott gráfot jelöljük G'-vel. Könnyen adódik, hogy a G_1 és G' gráfok maximális sajátértéke ugyanaz (sőt a 0 sajátértéktől, illetve annak multiplicitásától eltekintve valamennyi sajátérték azonos). A G' gráf maximális sajátértékét Λ'-vel jelölve a (ii) állítás alapján kapjuk, hogy $\Lambda' \leq \Lambda$, ezért az indukciós feltétel szerint G_1 kiszínezhető legfeljebb $\Lambda'+1 \leq \Lambda+1 = k$ színnel. Mivel az elhagyott csúcsnak legfeljebb $k-1$ szomszédja volt, ezért a k szín között biztosan van olyan, amelyet ezeknek a szomszédoknak a színezésére nem használtunk fel, tehát a G_1-nek ez a színezése kiterjeszthető G megfelelő színezésévé.

• **9.6.3** Tekintsük a p^2 elemű T_2 véges testet és ebben a p elemű T_1 résztestet. Mivel egy véges test multiplikatív csoportja ciklikus, így van T_2-nek olyan Δ eleme, amelynek a hatványai T_2 minden nem nulla elemét előállítják.

Vegyünk egy tetszőleges $\Theta \in T_2 \setminus T_1$ elemet, és legyenek T_1 elemei $\gamma_1, \ldots, \gamma_p$. Írjuk fel a $\Theta+\gamma_i$ elemeket $\Theta+\gamma_i = \Delta^{a_i}$ alakban, ezzel kijelöltünk p darab a_i egész számot 1 és p^2-1 között.

Megmutatjuk, hogy ezek eleget tesznek a feltételnek, azaz az $a_i + a_j$ összegek páronként különböző maradékot adnak modulo p^2-1.

Tegyük fel, hogy $a_i + a_j \equiv a_k + a_l \pmod{p^2-1}$. Ekkor az a_i-k definíciója alapján $(\Theta+\gamma_i)(\Theta+\gamma_j) - (\Theta+\gamma_k)(\Theta+\gamma_l) = 0$ adódik. A bal oldal Θ-nak legfeljebb elsőfokú polinomja T_1-beli együtthatókkal, hiszen Θ^2 kiesik. Elsőfokú azonban nem lehet, mert akkor $\Theta \in T_1$ következne, így — mivel a Θ gyöke — csak az azonosan nulla polinom lehet. Ekkor azonban pl. a polinomok gyöktényezős alakjának az egyértelműsége miatt $\{\gamma_i, \gamma_j\} = \{\gamma_k, \gamma_l\}$, és így ugyanez áll az a_i-kre is, ami éppen a bizonyítandó állítás volt.

• **9.6.4** Az útmutatást követve vegyünk egy g primitív gyököt modulo p, és legyen a_i az $x \equiv i \pmod{p-1}$, $x \equiv g^i \pmod{p}$ szimultán kongruenciarendszer megoldása modulo $p(p-1)$, $i = 1, 2, \ldots, p-1$. Nyilván elég azt megmutatnunk, hogy bármely c-re a $c \equiv a_i + a_j \pmod{p(p-1)}$ kongruencia legfeljebb egyetlen $\{i, j\}$-vel teljesülhet. Az a_i definíciója alapján ez a kongruencia a $c \equiv i+j \pmod{p-1}$, $c \equiv g^i + g^j \pmod{p}$ szimultán kongruenciarendszerrel ekvivalens. Itt az első kongruencia átírható a $g^c \equiv g^i g^j \pmod{p}$ alakba, vagyis a g^i és g^j számok összegét és szorzatát is ismerjük modulo p. A gyökök és együtthatók közötti összefüggés alapján a g^i és g^j maradékosztályok a $z^2 - cz + g^c \equiv 0 \pmod{p}$ másodfokú kongruencia egyértelműen meghatározott gyökei (p prím), és így i és j is egyértelmű.

• **9.6.7(c)** Legyen $Z=\sum_{i=1}^{s} a_i$ és tekintsük azt az η valószínűségi változót, amely a (különböző) a_i-kből képezett 2^s darab u_i összeg mindegyikét 2^{-s} valószínűséggel veszi fel (az u_i-k között szerepel a 0 és a Z is). A várható érték $E(\eta)=Z/2$, ugyanis az u_i-k összepárosíthatók úgy, hogy az egy párban levő u_i-k összege Z legyen. A szórás kiszámításához vezessük be a ξ_i, $i=1,2,\dots,s$ valószínűségi változókat: ξ_i az a_i, illetve 0 értéket 1/2-1/2 valószínűséggel veszi fel. Ekkor a ξ_i változók függetlenek és összegük éppen η, tehát a szórásnégyzetre

$$D^2(\eta)=\sum_{i=1}^{s} D^2(\xi_i)=\frac{1}{4}\sum_{i=1}^{s} a_i^2<\frac{sn^2}{4}$$

adódik. Alkalmazzuk most a Valószínűség$(|\eta-E(\eta)|\ge cD(\eta))\le c^{-2}$ *Csebisev-egyenlőtlenség*et az E-re és D-re kapott fenti értékekkel és $c=2$-vel. A számolást elvégezve azt kapjuk, hogy a 2^s darab (csupa különböző) u_i összeg legalább háromnegyed része a $Z/2$-re szimmetrikus $2n\sqrt{s}$ hosszúságú intervallumba esik. Ezért szükségképpen $3\cdot 2^s/4<2n\sqrt{s}$ [tehát a b)-beli hasonló becsléshez képest lényegében a jobb oldal változott s helyett $\sqrt{s}$-re]. A kapott egyenlőtlenséget egymás után kétszer logaritmálva

$$s<\log_2 n+(\log_2 s)/2+\log_2(8/3)\le 2\log_2 n\,, \qquad \text{(M.9.7)}$$

illetve $\log_2 s\le 1+\log_2\log_2 n$ adódik. Írjuk be ez utóbbit (M.9.7)-be $\log_2 s$ helyére, ekkor a feladat állításához jutunk.

• **9.6.9** Az útmutatást követve tekintsük azokat a számokat n-ig, amelyeket a d alapú számrendszerben felírva minden számjegy $<d/2$ és a számjegyek négyzetösszege egy adott q érték. Ha három ilyen szám számtani sorozatot alkot, akkor minden számjegyükre ugyanez áll fenn, mert a jegyekre adott korlátozás miatt két szám összeadása során sohasem képződik átvitel a következő helyiértékre. Így a középső szám valamennyi jegye a másik két szám megfelelő jegyeinek számtani közepe. Felírva, hogy mindhárom szám jegyeinek négyzetösszege q, egyszerű számolással adódik, hogy a számok szükségképpen egyenlők. (Más megfogalmazásban: ha a három számot a számjegyeikből alkotott vektoroknak tekintjük, akkor a harmadik vektor az első kettő összegének a fele, továbbá mindhárom vektor euklideszi normája egyenlő. Ez csak úgy lehet, ha maguk a vektorok is megegyeznek.)

Adott d a felírásban $u\approx(\log n)/(\log d)$ számjegy szerepel, és q-nak legfeljebb $ud^2/4$-féle értéke lehet. A halmazainkat minden lehetséges q-ra egyesítve az összes olyan számot megkapjuk, amelynek minden jegye $d/2$-nél kisebb. Ez összesen kb. $n/2^u$ szám. Ezért biztosan van olyan q, amelynek megfelelő halmaz elemszáma legalább $n/(2^{u-2}ud^2)$. Ez akkor veszi fel a maximumát ha $\log d\approx\sqrt{\log n}$, és ez a maximum éppen a tétel állításában előírt érték.

• **9.6.10** *Első megoldás*: Legyen h tetszőleges. Egy adott n-re az $1, 2, \ldots, n$ számokat 2^n-féleképpen színezhetjük ki két színnel. Számoljuk most meg azokat a színezéseket, amelyeknél előfordul h-tagú egyszínű számtani sorozat (h-ESZ). Ha egy h-ESZ kezdőtagja j, akkor a differenciája legfeljebb $\lfloor (n-j)/(h-1) \rfloor$, azaz az ilyen sorozatok száma legfeljebb

$$\frac{\sum_{j=1}^{n-h+1}(n-j)}{h-1} < \frac{n^2}{2h-2}.$$

Egy h-ESZ színe kétféle lehet, a többi szám színezése pedig 2^{n-h}-féle. Ennélfogva összesen legfeljebb $n^2 2^{n-h}/(h-1)$ színezésnél fordulhat elő h-ESZ (persze így számos rossz színezést többszörösen is megszámoltunk). Ezért, ha $n^2 2^{n-h}/(h-1) < 2^n$, azaz $n < 2^{h/2}\sqrt{h-1}$, akkor biztosan van olyan színezés, amelyben nem fordul elő h-ESZ.

• *Második megoldás*: Az útmutatást követve tekintsük a p prímmel a 2^p elemű T véges testet, legyen Δ a multiplikatív csoport generátoreleme és W egy $p-1$-dimenziós altér T-ben (mint F_2 feletti vektortérben). A színezés: k akkor piros, ha $\Delta^k \in W$. Megmutatjuk, hogy az $1, 2, \ldots, p(2^p-1)$ számokat ily módon kiszínezve nem fordul elő $p+1$-tagú egyszínű számtani sorozat.

Tegyük fel indirekt, hogy az $1 \le b < b+d < b+2d < \ldots < b+pd \le$ $\le p(2^p-1)$ számok mind azonos színűek. Legyen $\Theta = \Delta^b, \Psi = \Delta^d$. A feltétel szerint ekkor a $\Theta, \Theta\Psi, \ldots, \Theta\Psi^p$ „vektorok" vagy valamennyien a W altérbe esnek, vagy pedig egyikük sem esik W-be.

Ha a számtani sorozat piros, akkor tehát ezek a vektorok egy $p-1$-dimenziós altér elemei. Ezért közülük már az első p darab is lineárisan összefüggő, azaz alkalmas $\gamma_i \in F_2$ együtthatókkal $\sum_{i=0}^{p-1} \gamma_i(\Theta\Psi^i) = 0$ nem triviálisan teljesül. Az egyenlőséget Θ-val elosztva azt kapjuk, hogy Ψ gyöke egy p-nél alacsonyabb fokú F_2 feletti polinomnak. Mivel Ψ foka osztója T fokának, vagyis p-nek, ezért Ψ foka csak 1 lehet, azaz $\Psi \in F_2$. Ez azonban ellentmondás, hiszen nyilván $\Psi \neq 0$ és $d < 2^p - 1$ miatt $\Psi \neq 1$.

Ha a számtani sorozat kék, akkor a $\Theta\Psi - \Theta, \Theta\Psi^2 - \Theta\Psi, \ldots, \Theta\Psi^p - \Theta\Psi^{p-1}$ vektorokra kell megismételni az előző gondolatmenetet (csak Θ helyett most $\Theta(\Psi-1)$-gyel kell a megfelelő egyenlőséget elosztani).

• *További megoldások*: Közvetlen számolással igazolható, hogy az útmutatásoknál jelzett további három konstrukció is megfelel a feladat feltételeinek.

• *Megjegyzés*: Az egyes megoldások „hatékonyságát" összevetve a következőket állapíthatjuk meg. Az első megoldás semmilyen értelemben nem ad konstrukciót, a számtani sorozat tagszáma tetszőleges h lehet, és nagyjából az $n < 2^{h/2}\sqrt{h}$ korlátig alkalmazható. A második megoldás sem „igazi" konstrukció, továbbá itt a h speciálisan csak $p+1$ lehet (természetesen a prímek sűrű

elhelyezkedése alapján valamivel gyengébb eredmény a többi h-ra is nyerhető), az n-re kapott korlát viszont jobb, az előzőnek durván a négyzete. A további három megoldás „igazi" konstrukciót biztosít, ugyanakkor nagy h esetén kisebb n-ig lesz használható. A harmadik megoldás a következőképpen általánosítható: a 7 és a 17 helyett egy h, illetve $h/2$ körüli prímet prímet kell venni, és ekkor kb. $n = h^3/2$-ig jó a színezés. A negyedik megoldás nagy h-ra történő általánosításánál a $\sqrt{h}$ és $2\sqrt{h}$ prímekkel dolgozhatunk, és kb. $n = e^{\sqrt{h}}$-ig jó a színezés. Az ötödik megoldásnál az általános esetben $2h^3$ körüli korlát adódik n-re. Ebből látszik, hogy nagy h esetén az első két megoldás lényegesen nagyobb n-ekre biztosítja a megfelelő színezés létezését, mint a másik három konstrukció.

• **9.7.7(a)** Utalunk az útmutatásra és csak az ott „észrevételnek" nevezett állítás bizonyítását részletezzük. Legyenek tehát egy H háromszög szögei a racionális test felett lineárisan függetlenek. Azt kell igazolnunk, hogy H csak úgy bontható fel hasonló háromszögekre, ha azok H-hoz is hasonlók, továbbá ekkor H felbontásánál a kis háromszögek H szögeit nem vághatják el. Legyenek a kis háromszögek szögei $\alpha_1, \alpha_2, \alpha_3$, ekkor H szögei $\sum_{i=1}^{3} k_i\alpha_i$ alakúak nemnegatív egész k_i-kkel. Összeadva H szögeit $\pi = \sum_{i=1}^{3} m_i\alpha_i$ adódik. Ha itt pl. $m_1 = 0$, akkor H mindhárom szöge kifejezhető α_2 és α_3 lineáris kombinációjaként, ami ellentmond annak, hogy H szögei lineárisan függetlenek. Ha mindegyik $m_i \geq 1$, akkor $\pi = \sum_{i=1}^{3} \alpha_i$ miatt csak $m_i = 1$ lehetséges, vagyis H szögei is $\alpha_1, \alpha_2, \alpha_3$, tehát H valóban hasonló a kis háromszögekhez. Azt is kaptuk, hogy H felbontásánál a kis háromszögek H szögeit nem vághatják el.

• **(b)** Az útmutatásban jelzett állításokat igazoljuk. Legyen H olyan háromszög, amelyben mind a szögek, mind pedig az oldalak lineárisan függetlenek a racionális test felett. Tegyük fel, hogy n nem négyzetszám, azaz $\sqrt{n}$ irracionális, és H-t mégis fel lehet bontani n egybevágó K kis háromszögre.

Az (a) részben láttuk, hogy ekkor a szögek függetlensége miatt K szükségképpen hasonló H-hoz. Legyenek a K, illetve H háromszögek oldalai a_1, a_2, a_3, illetve A_1, A_2, A_3. Ekkor egyrészt $A_i = a_i\sqrt{n}$, másrészt $A_i = \sum_{j=1}^{3} k_{ij}a_j$, ahol a k_{ij}-k nemnegatív egészek. Ez azt jelenti, hogy a_1, a_2, a_3 egy nem triviális megoldása a

$$\begin{aligned}
(k_{11} - \sqrt{n})x_1 + \quad k_{12}x_2 \quad + \quad k_{13}x_3 \quad &= 0 \\
k_{21}x_1 \quad + (k_{22} - \sqrt{n})x_2 + \quad k_{23}x_3 \quad &= 0 \\
k_{31}x_1 \quad + \quad k_{32}x_2 \quad + (k_{33} - \sqrt{n})x_3 &= 0
\end{aligned}$$

homogén lineáris egyenletrendszernek. Ezért az

$$A=\begin{pmatrix} k_{11}-\sqrt{n} & k_{12} & k_{13} \\ k_{21} & k_{22}-\sqrt{n} & k_{23} \\ k_{31} & k_{32} & k_{33}-\sqrt{n} \end{pmatrix}$$

együtthatómátrix rangja $r(A)<3$. Továbbá $\sqrt{n}$ irracionalitása miatt az első két sor csak úgy lehet egymás skalárszorosa, ha $k_{13}=k_{23}=0$, ekkor viszont a harmadik sor és az első sor nem skalárszorosok, tehát $r(A)>1$. Emiatt $r(A)=2$, tehát az egyenletrendszer megoldásában egyetlen szabad paraméter van. Legyen ez pl. a_3 és válasszuk a_3 értékét 1-nek. Ekkor a_1 és a_2 is $c+d\sqrt{n}$ alakú lesz, ahol c és d alkalmas racionális számok. Így mindhárom a_i benne van az $\langle 1,\sqrt{n}\rangle$ kétdimenziós altérben, ami ellentmond annak, hogy az a_i oldalak lineárisan függetlenek voltak.

Meg kell még mutatnunk, hogy valóban létezik olyan háromszög, amelyben mind a szögek, mind pedig az oldalak lineárisan függetlenek. Az utóbbi feltétel a szinusztétel alapján ekvivalens azzal, hogy a szögek szinuszai függetlenek. Belátjuk, hogy ha egy háromszögben az egyik szög szinusza egy $0,\pm1/2,\pm1$-től különböző racionális szám és egy másik szög szinusza transzcendens, akkor mind a szögek, mind pedig a szinuszaik lineárisan függetlenek a racionális test felett.

Fel fogjuk használni, hogy ha $\sin\gamma$ algebrai, akkor tetszőleges s racionális számra $\sin(s\gamma)$ is algebrai. Valóban, mivel $\sin\gamma$ algebrai, ezért $\cos\gamma=$ $=\pm\sqrt{1-\sin^2\gamma}$ is az, ennélfogva $z=\cos\gamma+i\sin\gamma$ is algebrai. Mivel egy algebrai szám minden racionális kitevőjű hatványa is algebrai, tehát z^s és így annak képzetes része, azaz $\sin(s\gamma)$ is algebrai. Hasonlóan adódik, hogy ha $\sin\gamma_1$ és $\sin\gamma_2$ mindketten algebraiak, akkor $\sin(\gamma_1+\gamma_2)$ is algebrai. (Összefoglalva, azok a szögek, amelyek szinusza algebrai, alteret alkotnak a valós számoknak a racionális test feletti szokásos vektorterében.)

Ezen előkészületek után tekintsünk egy olyan háromszöget, amelyben $\sin\alpha_1=r$, $\sin\alpha_2=t$, ahol r egy $0,\pm1/2,\pm1$-től különböző racionális, t pedig tetszőleges transzcendens szám. Először a szögek függetlenségét igazoljuk. Indirekt tegyük fel, hogy az α_1,α_2 és $\alpha_3=\pi-(\alpha_1+\alpha_2)$ szögek egy nem triviális racionális együtthatós kombinációja nulla. Ezt átrendezve $r_0\pi+r_1\alpha_1=r_2\alpha_2$ adódik, ahol az r_i-k racionális számok és nem mindegyik nulla. Itt az előrebocsátott megjegyzés szerint a bal oldal szinusza algebrai, ugyanakkor a jobb oldalé $r_2\neq0$ esetén transzcendens. Így szükségképpen $r_2=0$. Ez azonban azt jelentené, hogy α_1/π racionális, ami a 9.7.2b feladat szerint lehetetlen. Ez az ellentmondás igazolja, hogy az α_i szögek valóban függetlenek.

Most rátérünk a szinuszok függetlenségének az igazolására. Indirekt tegyük fel, hogy $\sin\alpha_1,\sin\alpha_2$ és $\sin\alpha_3=\sin\alpha_1\cos\alpha_2+\cos\alpha_1\sin\alpha_2$ lineárisan

összefüggők. Mivel a feltétel szerint $\sin\alpha_2/\sin\alpha_1$ irracionális (sőt transzcendens), ezért $\sin\alpha_1\cos\alpha_2+\cos\alpha_1\sin\alpha_2 = r_1\sin\alpha_1+r_2\sin\alpha_2$ kell hogy fennálljon alkalmas r_i racionális számokkal. Ezt átrendezve $\sin\alpha_1(\cos\alpha_2-r_1) = \sin\alpha_2(-\cos\alpha_1+r_2)$ adódik. Emeljük mindkét oldalt négyzetre, írjunk $\sin^2\alpha_2$ helyére $1-\cos^2\alpha_2$-t, és rendezzünk $\cos\alpha_2$ hatványai szerint. Itt $\cos^2\alpha_2$ együtthatója $\sin^2\alpha_1+(r_2-\cos\alpha_1)^2\neq 0$. Így azt kaptuk, hogy $\cos\alpha_2$ gyöke egy olyan másodfokú egyenletnek, amelynek az együtthatói algebrai számok. A másodfokú egyenlet megoldóképletéből ekkor $\cos\alpha_2$-re is algebrai szám adódik, így $\sin\alpha_2$ is algebrai, ami ellentmond a feltételnek.

• **(c)** Ha $n=k^2$, akkor egy tetszőleges háromszög minden oldalát k egyenlő részre osztva nyilván megfelelő felbontást kapunk. Ha $n=k^2+m^2$ (ahol $k,m>0$), akkor vegyünk egy olyan derékszögű háromszöget, amelynek a befogói k és m, és húzzuk meg az átfogóhoz tartozó magasságot. Ekkor két, az eredetihez hasonló derékszögű háromszöget kapunk, amelyek átfogói k, illetve m. A kapott két háromszög oldalait k, illetve m egyenlő részre osztva fel tudjuk bontani őket k^2, illetve m^2 olyan, az eredetihez hasonló kis háromszögre, amelyek átfogója egységnyi, és így a kis háromszögek egybevágók. Ezzel az eredeti háromszöget valóban $n=k^2+m^2$ megfelelő kis háromszögre bontottuk. (Speciálisan, ha $k=m$, akkor egyenlő szárú derékszögű háromszöget kell venni.)

Ha $n=3k^2$, akkor a következő konstrukció lesz megfelelő. Húzzuk be egy S szabályos háromszög súlyvonalait, ezek S-et 6 darab egybevágó derékszögű háromszögre bontják, amelyek másik két szöge 30 és 60 fokos. Ugyanilyen az S „egyik felét” alkotó F háromszög is. Ezért F felbontható 3 darab egybevágó és hozzá hasonló háromszögre. Ezután a három háromszög mindegyikét a szokásos eljárással egyenként k^2 részre vágva F-et valóban $n=3k^2$ megfelelő kis háromszögre bontottuk.

10. Kódok

• **10.2.1** Először a kódoló függvényeket tekintjük. Egy (k,n) kód kódoló függvénye egy tetszőleges $\varphi: T^n\to T^k$ injektív leképezés. Legyen $T^n=\{\mathbf{v}_1,\dots,\mathbf{v}_{2^n}\}$. A $\mathbf{v}_1$-hez hozzárendelhető bármely $\mathbf{c}_1\in T^k$, a $\mathbf{v}_2$-höz bármely $\mathbf{c}_2\neq\mathbf{c}_1$ stb. Így a kódoló függvények száma $\Gamma=\prod_{i=1}^{2^n}(2^k-i+1)$.

A lineáris kódok kódoló függvényei $\mathcal{A}: T^n\to T^k$ injektív lineáris leképezések. Ezeket úgy jellemezhetjük, hogy egy $\mathbf{b}_1,\dots,\mathbf{b}_n\in T^n$ bázishoz $\mathbf{c}_1,\dots,\mathbf{c}_n\in T^k$ lineárisan független vektorokat rendelünk. Így $\mathbf{c}_1$ bármely

nem nulla vektor lehet T^k-ban, $\mathbf{c}_2$ bármely vektor, ami nincs a $\langle \mathbf{c}_1 \rangle$ altérben, és általában, $\mathbf{c}_j$ tetszőleges vektor, ami nincs a $\langle \mathbf{c}_1, \dots, \mathbf{c}_{j-1} \rangle$ altérben. Így a lineáris leképezések száma $\Lambda = \prod_{j=0}^{n-1} (2^k - 2^j)$.

Mivel Λ a Γ néhány tényezőjének a szorzata, ezért $\Lambda \mid \Gamma$, azaz (b) igaz.

Rátérve a kódokra, egy (k, n) kód a T^k tetszőleges 2^n elemű részhalmaza. Az összes kód száma tehát $\gamma = \binom{2^k}{2^n} = \prod_{i=1}^{2^n} \frac{2^k - i + 1}{i}$.

Egy (k, n) lineáris kód a T^k tetszőleges n-dimenziós altere. Egy ilyen alteret n lineárisan független $\mathbf{c}_1, \dots, \mathbf{c}_n \in F^k$ vektor generál. Az ilyen vektorrendszerek száma Λ (ahol a vektorok sorrendje is számít). Azonban ugyanazt a W alteret generálja bármely n lineárisan független W-beli vektor. A Λ meghatározási módszerét T^k helyett W-re alkalmazva, az ilyen rendszerek száma $\prod_{j=0}^{n-1} (2^n - 2^j)$. Azaz a liná ris kódok száma $\lambda = \prod_{j=0}^{n-1} \frac{2^k - 2^j}{2^n - 2^j}$.

Azt kaptuk, hogy λ-ban a számláló, illetve nevező a γ számlálójából, illetve nevezőjéből vett néhány tényező szorzata. Ebből azonban nem következik $\lambda \mid \gamma$. Például $n = 3$-ra

$$\frac{\gamma}{\lambda} = \frac{2^{k-4}(2^k - 3)(2^k - 5)(2^k - 6)(2^k - 7)}{3 \cdot 5}.$$

A számláló tényezői nem fedik le az összes lehetséges maradékot mod 5; egyikük sem osztható 5-tel, ha $2^k \equiv 4 \pmod 5$. Mivel $2^6 \equiv 4 \pmod 5$, így γ/λ nem egész szám, ha $(k, n) = (6, 3)$. Tehát (a) hamis.

• **10.4.3(a)** A 10.4.1 Tétel utáni példa mintájára vehető $m_1 = x^4 + x + 1$. A $\Theta = \Delta^3$ elemre $\Theta^5 = \Delta^{15} = 1$, ezért Θ gyöke az $f = x^4 + x^3 + x^2 + x + 1$ (körosztási) polinomnak. Ez könnyen láthatóan irreducibilis F_2 felett, így $m_3 = f$. A $\Psi = \Delta^5$ elemre $\Psi^3 = \Delta^{15} = 1$, ezért Ψ gyöke a $h = x^2 + x + 1$ irreducibilis polinomnak, ahonnan $m_5 = h$. Innen $s = 4 + 4 + 2 = 10$.

• **(b)** Mivel a 3 és az 5 is relatív prím a T^q test multiplikatív csoportjának az elemszámához, a $2^q - 1$-hez, ezért Δ^3 és Δ^5 is generátorelem ebben a csoportban. Ebből következik, hogy az F_2 testnek a Δ^3-nal, illetve a Δ^5-nel való bővítése kiadja az egész T^q testet (sőt az összeadásra tulajdonképpen nincs is szükség), ezért Δ^3 és Δ^5 minimálpolinomja is q-adfokú.

A 10.4.2 feladat szerint azt kell még belátnunk, hogy Δ, Δ^3 és Δ^5 közül semelyik kettőnek sem ugyanaz a minimálpolinomja. Ehhez először azt igazoljuk, hogy ha Δ^i generátorelem a T^q test multiplikatív csoportjában (azaz

i és 2^q-1 relatív prímek), akkor m_i összes gyökét a Δ-nak az $i\cdot 2^j$ kitevőjű hatványai adják, ahol $0\le j<q$. A 10.4.2 Tétel bizonyításánál láttuk, hogy Θ és Θ^2 minimálpolinomja ugyanaz. Ebből következik, hogy m_i-nek a megadott q darab Δ-hatvány valóban gyöke. Belátjuk még, hogy ezek mind különbözők, és így szükségképpen m_i-nek mind a q darab gyökét megkaptuk. A Δ két hatványa pontosan akkor egyenlő, ha a kitevők különbsége osztható $o(\Delta)=2^q-1$-gyel. Ha $0\le u<j<q$, akkor $i2^j-i2^u=i2^u(2^{j-u}-1)$-ben az első két tényező relatív prím a 2^q-1-hez, a harmadik tényező pedig kisebb 2^q-1-nél, így a szorzat nem lehet osztható 2^q-1-gyel. Ezzel megmutattuk, hogy a megadott Δ-hatványok mind különbözők, és így ezek adják az m_i polinom gyökeit.

Most belátjuk, hogy a Δ, Δ^3 és Δ^5 elemeknek páronként különböző a minimálpolinomja. Ha $m_1=m_3$ lenne, akkor Δ^3 szerepelne az m_1 gyökei között, azaz $3=2^j$ teljesülne, ami lehetetlen (itt a kitevőknél a modulo 2^q-1 kongruencia helyett azért lehetett az egyenlőséget nézni, mert mind a 3, mind pedig a 2^j kitevő 0 és 2^q-1 közé esett). Ugyanígy az $m_1=m_5$ feltételezés is ellentmondásra vezet. Végül tegyük fel, hogy $m_3=m_5$, azaz Δ^5 gyöke m_3-nak. Az m_3 gyökei Δ-nak az alábbi kitevőjű hatványai:

$$3,6,12,\dots,3\cdot 2^{q-2},3\cdot 2^{q-1}=2^q+2^{q-1}\equiv 2^{q-1}+1 \pmod{2^q-1}.$$

Azonban az 5 ezek közül (a 0 és 2^q-1 közötti értékek közül) egyikkel sem egyezhet meg (az utolsóval $q>3$ miatt nem), tehát ebben az esetben is ellentmondásra jutottunk.

• **10.4.5(a)** Tudjuk, hogy a 2^q elemű test összes részteste 2^v elemű, ahol $v\mid q$, és minden ilyen v-hez pontosan egy 2^v elemű T^v résztest tartozik. A T^v test G_v multiplikatív csoportja egy 2^v-1 elemű részcsoport a T^q test (ciklikus) multiplikatív csoportjában, így G_v-t a Δ-nak a $(2^q-1)/(2^v-1)$-edik hatványa generálja. Ez azt jelenti, hogy T^v nem nulla elemei azok a Δ^i hatványok, ahol $(2^q-1)/(2^v-1)\mid i$. Más szóval, valamely i-re Δ^i pontosan azokban a T^v résztestekben van benne, amelyekre $(2^q-1)/(2^v-1)\mid i$. Tudjuk, hogy $\deg m_i$ a Δ^i-t tartalmazó legszűkebb résztestnek a(z F_2 test feletti) dimenziója. A legszűkebb résztestet éppen a legkisebb megfelelő v érték szolgáltatja, tehát $\deg m_i$ valóban a legkisebb ilyen tulajdonságú v, amint állítottuk.

• **(b)** A 10.4.2 Tétel bizonyításánál láttuk, hogy Θ és Θ^2 minimálpolinomja ugyanaz. Ebből következik, hogy m_i-nek gyöke minden olyan Δ-hatvány, ahol a kitevő $i\cdot 2^j$ alakú. Nézzük meg, hány különböző ilyen hatvány keletkezik. Az első ismétlődés akkor következik be, amikor $i\cdot 2^v-i$ először osztható $o(\Delta)=2^q-1$-gyel, vagyis a legkisebb olyan v-re, amikor $(2^q-1)/(2^v-1)\mid i$. Az (a) részben láttuk, hogy ez a v éppen $\deg m_i$. Ez azt jelenti, hogy a

szóban forgó Δ-hatványok között éppen $\deg m_i$ darab különböző található, ezek valamennyien gyökei m_i-nek, vagyis valóban ezek adják m_i összes gyökét.

• **10.4.6** Először megmutatjuk, hogy minden $i \le 2t-1$-re $\deg m_i = q$. Ellenkező esetben a 10.4.5a feladat szerint lenne a q-nak olyan valódi v osztója, amelyre $(2^q-1)/(2^v-1) \mid i$. Ekkor $v \le q/2$, és így

$$i \ge (2^q-1)/(2^v-1) \ge (2^q-1)/(2^{q/2}-1) = 2^{q/2}+1,$$

ugyanakkor a feltétel szerint $i \le 2t-1 \le 2^{q/2}-1$, ami ellentmondás.

Most belátjuk, hogy $m_i \ne m_l$, ahol i és l különböző páratlan számok 1 és $2t-1$ között. Indirekt tegyük fel, hogy $m_i = m_l$. Ekkor Δ^l szerepel m_i gyökei között, azaz a 10.4.5b feladat szerint $l \equiv i \cdot 2^j \pmod{2^q-1}$ teljesül valamilyen $0 \le j < q$-ra. Ha $j \le q/2$, akkor $i \cdot 2^j \le (2^{q/2}-1)2^{q/2} < 2^q-1$, tehát a kongruencia helyett egyenlőségnek kellene teljesülnie, ami nyilván nem lehet. Ha $j > q/2$, akkor írjuk át a kongruenciát $i2^j - y2^q = l - y$ alakba. Itt a bal oldal osztható 2^j-vel, de ($j < q$ miatt) nem lehet nulla, ezért abszolút értéke legalább $2^j > 2^{q/2}$. A jobb oldal abszolút értéke azonban ennél kisebb, hiszen $0 < l \le 2t-1 < 2^{q/2}$, valamint ($j < q$ miatt) $0 \le y < i < 2^{q/2}$. Mindenképpen ellentmondásra jutottunk, tehát valóban $m_i \ne m_l$.

Ezzel igazoltuk, hogy $m_1, m_3, \ldots, m_{2t-1}$ páronként különböző q-adfokú polinomok, amiből a 10.4.2 feladat alapján következik, hogy $s = tq$.

• **10.4.9(a)** A továbbiakban $T_k[x]$-et az $R_k = T[x]/(x^k-1)$ faktorgyűrűvel azonosítjuk, azaz a legfeljebb $k-1$-edfokú polinomokat mint az x^k-1-gyel való osztási maradékokat tekintjük. Ennek az az előnye, hogy $T_k[x]$-en a szorzás is értelmes, tehát egy gyűrűt (sőt algebrát) kapunk.

Ennek alapján a ciklikus kód definíciója pontosan azt jelenti, hogy egy kódszó x-szerese is kódszó: $x(\gamma_0+\gamma_1x+\ldots+\gamma_{k-1}x^{k-1}) = \gamma_0x+\gamma_1x^2+\ldots+$ $+\gamma_{k-2}x^{k-1}+\gamma_{k-1}x^k = \gamma_{k-1}+\gamma_0x+\gamma_1x^2+\ldots+\gamma_{k-2}x^{k-1}$.

Felhasználva, hogy a kód lineáris, azaz kódszavak összege is kódszó, azonnal adódik, hogy a ciklikus kódok úgy is jellemezhetők, hogy egy kódszó bármely polinomszorosa is kódszó. Így egy kód pontosan akkor ciklikus, ha a kódszavak egy *ideál*t alkotnak R_k-ban.

Mivel $T[x]$-ben van maradékos osztás, ezért minden ideálja főideál, és így ugyanez érvényes R_k-ban is. Ez azt jelenti, hogy ciklikus kód esetén K egy alkalmas g polinom többszöröseiből áll. A 10.2.8c feladat alapján feltehető, hogy $g \mid x^k-1$ és K éppen a g polinom által generált polinomkód kódszavaiból áll.

Végül, a megfordításhoz azt igazoljuk, hogy egy ilyen polinomkód valóban ciklikus. Ez onnan adódik, hogy ha gf kódszó, akkor ennek a ciklikus per-

mutációja $x(gf) = g(xf)$ is kódszó. (Ha az xf polinom foka n, akkor helyette az $(x^k - 1)/g$ polinommal való osztási maradékát kell venni.)

• **10.4.10** A 10.3.9 feladat szerint olyan $m \times k$ méretű kvázi-paritásellenőrző mátrixot kell gyártani, amelynek bármelyik $d-1$ oszlopa független. Az első oszlop legyen egy tetszőleges nem nulla vektor. Tegyük fel, hogy az első j oszlopot már elkészítettük. Ekkor a $j+1$-ediket úgy kell megválasztani, hogy az ne legyen felírható az első j oszlop közül semelyik legfeljebb $d-2$-nek a lineáris kombinációjaként. Ezzel kizártuk a nullvektort, a j darab eddigi oszlopvektort, ezek $\binom{j}{2}$ darab páronkénti összegét, $\binom{j}{3}$ darab hármankénti összegét stb. Így összesen legfeljebb $\sum_{i=0}^{d-2}\binom{j}{i}$ vektort zártunk ki (lehet, hogy csak kevesebbet, mert ezek között az öszegek között — $i \geq d/2$ esetén — már előfordulhatnak egybeesők). Ha $\sum_{i=0}^{d-2}\binom{j}{i} < 2^m$, akkor biztosan nem zártuk ki T^m összes vektorát, tehát tudunk egy alkalmas $j+1$-edik oszlopot választani. A feltétel alapján ez még $j = k-1$-re is megvalósítható, tehát valóban egy megfelelő $m \times k$ méretű kvázi-paritásellenőrző mátrixhoz jutunk.

• **10.4.11(a)** A q szerinti teljes indukciót formálisan a (tulajdonképpen tiltott) $q = 1$ esettel érdemes kezdeni, amelyre az állítás nyilvánvaló. Tegyük fel, hogy q-ra igaz az állítás, azaz a nem nulla kódszavak súlyának a minimuma 2^{q-1}. Amikor q-ról $q+1$-re lépünk, akkor a generátormátrixnak kétszer annyi sora és eggyel több oszlopa lesz. Legyen $G(1,q) = (\,\mathbf{1} \quad \mathbf{a}_1 \quad \ldots \quad \mathbf{a}_q\,)$, ekkor $G(1,q+1) = \begin{pmatrix} \mathbf{1} & \mathbf{0} & \mathbf{a}_1 & \ldots & \mathbf{a}_q \\ \mathbf{1} & \mathbf{1} & \mathbf{a}_1 & \ldots & \mathbf{a}_q \end{pmatrix}$, azaz az új mátrixban az utolsó q oszlopnak és az első oszlopnak az alsó és felső fele egyaránt a régi mátrix megfelelő oszlopa, a második oszlop felső és alsó fele pedig csupa 0, illetve csupa 1. Ez azt jelenti, hogy az új kódszavakat részben a régiek megduplázásával kapjuk, részben pedig úgy, hogy egy régi kódszó után annak komplementerét írjuk. Az utóbbi módon gyártott vektorok súlya nyilván 2^q, a duplázottak súlya pedig a kétszerese az eredeti kódszavak súlyának, vagyis az indukciós feltevés szerint (a nem nulla kódszavakra) legalább $2 \cdot 2^{q-1} = 2^q$.

• **(b)** Jelöljük a kódszavak közötti minimális távolságot $d(m,q)$-val. A $d(m,q) = 2^{q-m}$ állítást (pl.) $q+m$ szerinti teljes indukcióval bizonyíthatjuk. Az $m = 1$ esetet már az (a) részben igazoltuk, tehát feltehetjük, hogy $q > m \geq 2$. A $G(m,q)$ mátrix oszlopait permutáljuk úgy, hogy a végére kerüljenek mindazok az oszlopok, amelyeknek a felső része csupa 0 (ez az eredeti számozás szerinti második oszlop, valamint annak valahány további oszloppal való szorzata). Ekkor — felhasználva az (a) rész meggondolásait is — az alábbi blokkokból álló mátrixot kapjuk: $\begin{pmatrix} G(m,q-1) & 0 \\ G(m,q-1) & G(m-1,q-1) \end{pmatrix}$.

Ez a 10.2.7 feladat III. konstrukciójának felel meg. Ezért

$$d(m,q) = \min\bigl(2d(m,q-1), d(m-1,q-1)\bigr),$$

és így az indukciós feltétel szerint

$$d(m,q) = \min\bigl(2\cdot 2^{q-1-m}, 2^{(q-1)-(m-1)}\bigr) = 2^{q-m}.$$

A. Algebrai alapfogalmak

• **A.3.14(b)** Jelölje T_n az összes primitív n-edik egységgyök összegét. Nyilván $T_1 = 1$. Belátjuk, hogy

I. $T_p = -1$ és $T_{p^k} = 0$, ha p prímszám és $k > 1$, valamint

II. $T_k T_m = T_{km}$, ha $(k,m) = 1$.

Ezekből azonnal következik, hogy $T_n = (-1)^r$, ha az n szám r különböző prím szorzata, és $T_n = 0$ a többi $n > 1$-re. Ez az ún. Möbius-függvény, amelynek szokásos jelölése $\mu(n)$, és fontos szerepet játszik a számelméletben. Az A.11.12b feladat megoldásában is előfordul.

I. Jelölje S_n az összes n-edik egységgyök összegét. Az A.3.12 feladat alapján minden $n > 1$-re $S_n = 0$. Ha $n = p$, akkor $z = 1$ kivételével minden p-edik egységgyök primitív, mivel $z^p = 1 \iff o(z) \mid p \iff o(z) = p$ or 1. Így $T_p = S_p - 1 = 0 - 1 = -1$.

Ha $n = p^k$, ahol $k > 1$, akkor

$$z^{p^k} = 1 \iff o(z) \mid p^k \iff o(z) = p^k \text{ vagy } o(z) \mid p^{k-1} \iff$$
$$\iff o(z) = p^k \text{ vagy } z^{p^{k-1}} = 1,$$

amiből $T_{p^k} = S_{p^k} - S_{p^{k-1}} = 0 - 0 = 0$ következik.

II. Belátjuk, hogy ha z és w primitív k-adik és m-edik egységgyökök, ahol $(k,m) = 1$, akkor zw primitív km-edik egységgyök. Más szóval, ha $o(z) = k$ és $o(w) = m$, akkor $o(zw) = km$. Az A.3.13(b) feladat szerint $o(zw) \mid km$. A fordított irányú oszthatóság belátásához legyen $o(wz) = t$, tehát $1 = (wz)^t$. Innen w-t úgy tudjuk kiküszöbölni, hogy ezt az egyenlőséget az m-edik hatványra emeljük: $1 = z^{tm}w^{tm} = z^{tm}$. Ebből következik, hogy $o(z) = k \mid tm$, ezért $(k,m) = 1$ miatt $k \mid t$. Az $m \mid t$ oszthatóság ugyanígy adódik. Így $km = [k,m] \mid t$, ahogy állítottuk.

Most megmutatjuk, hogy megfordítva, minden u primitív km-edik egységgyök egyértelműen felírható $u = zw$ alakban, ahol z és w primitív k-adik, illetve m-edik egységgyök. Az euklideszi algoritmusból következik, hogy

$(k,m)=1=rk+ms$ alkalmas r és s egészekkel. Nyilván $(r,m)=(s,k)=1$. Ekkor $u=u^{ms+kr}=u^{ms}u^{kr}$. Belátjuk, hogy $z=u^{ms}$ és $w=u^{kr}$ primitív k-adik, illetve m-edik egységgyökök. Az A.3.13(a) feladat alapján

$$o(z)=o(u^{ms})=\frac{o(u)}{(o(u),ms)}=\frac{km}{(km,ms)}=\frac{k}{(k,s)}=k,$$

és ugyanígy $o(w)=m$. Az egyértelműség igazolásához legyen $z_1w_1=z_2w_2$, ahol $o(z_j)=k$ és $o(w_j)=m$. Ekkor $v=z_1/z_2=w_2/w_1$-re $v^k=v^m=1$ teljesül. Tehát $o(v)\mid(k,m)=1$, azaz $v=1$, és így $z_1=z_2$ és $w_1=w_2$.

Legyen $z_1,z_2,\dots,z_a$, $w_1,w_2,\dots,w_b$ és $u_1,u_2,\dots,u_c$ rendre az összes primitív k-adik, m-edik és km-edik egységgyök. Beláttuk, hogy az u_h számok ugyanazok, mint a z_iw_j szorzatok. Ennek alapján

$$T_{km}=\sum_{h=1}^{c}u_h=\sum_{\substack{1\le i\le a\\1\le j\le b}}z_iw_j=\left(\sum_{i=1}^{a}z_i\right)\left(\sum_{j=1}^{b}w_j\right)=T_kT_m.$$

• **A.3.16** Legyen $U=\sum_{k=1}^{n}\cos(kx)$. Ha $x=2m\pi$, ahol m egész szám, akkor $\cos(kx)=1$, tehát $U=n$. A továbbiakban feltesszük, hogy $x\neq 2m\pi$.

Első megoldás: Legyen $z=\cos x+i\sin x$, ekkor U a $V=\sum_{k=1}^{n}z^k$ mértani sorösszeg valós része. Mivel $z\neq 1$, $V=z\dfrac{z^n-1}{z-1}$. A $\operatorname{Re}V$ szebb alakjához legyen $w=\cos(x/2)+i\sin(x/2)$, ekkor $z=w^2$. Helyettesítsük ezt be V-be, emeljünk ki w^n-et a számlálóból és w-t a nevezőből, és használjuk fel, hogy $1/w=\overline{w}$:

$$V=w^2\frac{w^{2n}-1}{w^2-1}=w^{2+n-1}\frac{w^n-(1/w)^n}{w-(1/w)}=w^{n+1}\frac{w^n-(\overline{w})^n}{w-\overline{w}}=$$
$$=w^{n+1}\frac{2i\sin(nx/2)}{2i\sin(x/2)}=\Big(\cos\big((n+1)x/2\big)+i\sin\big((n+1)x/2\big)\Big)\frac{\sin(nx/2)}{\sin(x/2)}.$$

Tehát $U=\operatorname{Re}V=\dfrac{\sin(nx/2)\cos((n+1)x/2)}{\sin(x/2)}$.

Második megoldás: A második útmutatást követve legyen $W=\sin(x/2)U$. Mivel $x\neq 2m\pi$, így $\sin(x/2)\neq 0$. Az útmutatásban megadott trigonometikus azonosság alapján $\sin(x/2)\cos(kx)=\dfrac{\sin\big((2k+1)x/2\big)-\sin\big((2k-1)x/2\big)}{2}$.

Ezeket az egyenlőségeket $k = 1, 2, \ldots, n$-re összegezve egy teleszkopikus összeg adódik, tehát

$$W = \frac{\sin\big((2n+1)x/2\big) - \sin(x/2)}{2} = \sin(nx/2)\cos\big((n+1)x/2\big)$$

(az utolsó lépésben még egyszer alkalmaztuk ugyanazt a trigonometrikus azonosságot).

• **A.7.7(f)** Az állítás a (c) rész alapján minden $1 \le i \le n-1$-re igaz. Továbbá az $a_0 + a_1x + a_2x^2 + \ldots + a_nx^n$ és $a_n + a_{n-1}x + \ldots + a_1x^{n-1} + a_0x^n$ polinomok gyökei éppen egymás reciprokai, ezért az $i = n$ és $i = 0$ esetek közül elég az egyikre szorítkozni.

Az $i = 0$ eset igazolásához tegyük fel indirekt, hogy véges sok kivételtől eltekintve bármilyen s egész szám esetén az $s + a_1x + a_2x^2 + \ldots + a_nx^n$ polinomnak van racionális gyöke, azaz alkalmas r racionális számmal a $-s$ felírható $-s = a_1r + a_2r^2 + \ldots + a_nr^n$ alakban. Egy ilyen r gyök (s-től függetlenül) csak k/a_n alakú racionális szám lehet. Ez azt jelenti, hogy a $g = a_1x + a_2x^2 + \ldots + a_nx^n$ polinomfüggvénybe a k/a_n alakú racionális számokat behelyettesítve véges sok kivételtől eltekintve minden egész számot meg kellene kapnunk.

Legyen M egy nagy szám és tekintsük az összes olyan $g(k/a_n)$ helyettesítési értéket, amelyre $|g(k/a_n)| < M$. Ha $|k/a_n| \ge \sqrt{2M/|a_n|}$, akkor — felhasználva, hogy minden elég nagy abszolút értékű x-re $|g(x)| > |a_nx^n/2| \ge$ $\ge |a_nx^2/2|$ — azt kapjuk, hogy $|g(k/a_n)| > M$, ami ellentmondás. Ennek megfelelően szükségképpen $|k/a_n| < \sqrt{2M/|a_n|}$.

Az ilyen k/a_n számok száma legfeljebb $2|a_n|\sqrt{2M/|a_n|} < 3|a_n|\sqrt{M}$. A feltétel szerint ugyanakkor az ezekből képzett $g(k/a_n)$ helyettesítési értékek között legfeljebb R darab kivételtől eltekintve a $-M$ és M közé eső összes egész számnak is szerepelnie kell. Ez azt jelenti, hogy $2M - 1 - R \le 3|a_n|\sqrt{M}$, ami elég nagy M esetén nyilván lehetetlen.

• **A.8.10(a)** Ha $|G| = 1$ vagy prímszám, akkor egy H részcsoportra Lagrange tétele szerint csak $|H| = 1$ vagy $|H| = |G|$ lehetséges, vagyis szükségképpen $H = e$ vagy $H = G$. Tehát ha $|G| = 1$ vagy prímszám, akkor G-nek csak triviális részcsoportjai vannak. Megmutatjuk, hogy más ilyen tulajdonságú csoport nincs. Tegyük fel, hogy G-nek az e-n és önmagán kívül nincs más részcsoportja. Ekkor bármely $g \ne e$-re szükségképpen $G = \langle g\rangle$. Ha $o(g) = \infty$, akkor $\langle g^2\rangle$, ha pedig $o(g)$ összetett szám és d az $o(g)$ egy nem triviális osztója, akkor $\langle g^d\rangle$ egy nem triviális részcsoportot alkot $\langle g\rangle$-ben, ami ellentmondás. Tehát $|G| = o(g)$ valóban csak 1 vagy prímszám lehet.

• **(b)** Egy véges csoportnak nyilván csak véges sok részcsoportja van. Megmutatjuk, hogy ennek a megfordítása is igaz, azaz bármely végtelen csoportban végtelen sok részcsoport található. Ha létezik olyan $g \in G$, amelyre $o(g) = \infty$, akkor a $\langle g^k \rangle$, $k = 1, 2, 3, \ldots$ részcsoportok mind különbözők. Ha G-ben minden elem véges rendű (de $|G| = \infty$), akkor legyen pl. $g_1 = e$, és ha már $g_1, \ldots, g_i$-t kiválasztottuk, akkor g_{i+1} legyen egy tetszőleges olyan elem, amely nincs benne a $\langle g_1 \rangle, \ldots, \langle g_i \rangle$ ciklikus részcsoportok egyesítésében. Az elemrendek végessége miatt a ciklikus részcsoportok végesek, ugyanakkor $|G| = \infty$, ezért ez az eljárás nem akad meg. Az így nyert $\langle g_i \rangle$, $i = 1, 2, 3, \ldots$ részcsoportok mind különbözők.

• **A.10.1** A feltételek szerint M egy n-dimenziós vektortér L felett, ezért bármely $n + 1$ eleme lineárisan összefüggő. Speciálisan, az $1, \Theta, \Theta^2, \ldots, \Theta^n$ elemek is lineárisan összefüggők, azaz léteznek olyan $\gamma_0, \gamma_1, \ldots \gamma_n \in L$ nem csupa nulla „skalárok", amelyekre $\sum_{i=0}^{n} \gamma_i \Theta^i = 0$. Ez azt jelenti, hogy Θ gyöke az $f = \sum_{i=0}^{n} \gamma_i x^i \in L[x]$ nem nulla polinomnak, tehát legfeljebb n-edfokú algebrai elem L felett.

A $\deg \Theta \mid n$ állítás bizonyításához tekintsük az $L \subseteq L(\Theta) \subseteq M$ testláncot. A fokszámtétel szerint $n = \deg(M : L) = \deg\big(M : L(\Theta)\big) \cdot \deg\big(L(\Theta) : L\big)$, és itt a második tényező éppen $\deg \Theta$.

• **A.10.16** Mivel $|z| = 1$, ezért $\overline{z} = 1/z$, és így $\operatorname{Re} z = (z + 1/z)/2 \in \mathbf{Q}(z)$. Ebből következik, hogy $\mathbf{Q}(\operatorname{Re} z) \subseteq \mathbf{Q}(z)$. Továbbá nyilván $\mathbf{Q}(\operatorname{Re} z) \subseteq \mathbf{R}$, tehát $\mathbf{Q}(\operatorname{Re} z) \subseteq \mathbf{Q}(z) \cap \mathbf{R}$.

A másik irányú tartalmazáshoz vegyünk $\mathbf{Q}(z)$-ből egy w valós elemet. Azt kell igazolni, hogy $w \in \mathbf{Q}(\operatorname{Re} z)$.

A gondolatmenet jobb megvilágítása érdekében először tegyük fel, hogy z algebrai szám. Ekkor w felírható $w = \sum_{i=0}^{n-1} \alpha_i z^i$ alakban, ahol $\alpha_i \in \mathbf{Q}$ és $n = \deg z$. Mivel w valós, ezért

$$2w = w + \overline{w} = \sum_{i=0}^{n-1} \alpha_i (z^i + \overline{z}^i) = \sum_{i=0}^{n-1} \alpha_i \Big(z^i + \frac{1}{z^i} \Big) .$$

Ha megmutatjuk, hogy $z^i + 1/z^i$ felírható $z + 1/z = 2\operatorname{Re} z$ racionális együtthatós polinomjaként, akkor az előzőek alapján ugyanez érvényes $2w$-re és így w-re is, tehát valóban $w \in \mathbf{Q}(2\operatorname{Re} z) = \mathbf{Q}(\operatorname{Re} z)$.

A jelzett állítást i szerinti teljes indukcióval bizonyítjuk. Az állítás $i = 1$-re triviális, $i = 2$-re $z^2 + 1/z^2 = (z + 1/z)^2 - 2$. Elfogadva $i - 1$-re és i-re, $z^{i+1} + 1/z^{i+1} = (z^i + 1/z^i)(z + 1/z) - (z^{i-1} + 1/z^{i-1})$ alapján kapjuk, hogy $i + 1$-re is igaz.

Ha z transzcendens, akkor is hasonló gondolatmenetet követünk. Legyen w valós és $w \in \mathbf{Q}(z)$, azaz $w = g(z)/h(z)$, ahol $g, h \in \mathbf{Q}[x]$. Mivel $w = \overline{w}$ és $\overline{z} = 1/z$, ezért $g(z)/h(z) = g(1/z)/h(1/z)$. A nevezőkkel átszorozva kapjuk, hogy $g(z)h(1/z) = g(1/z)h(z)$. Jelöljük ezt a közös értéket u-val, ekkor $2u = g(z)h(1/z)+g(1/z)h(z)$. Itt a szorzásokat elvégezve $2u = \sum_i \gamma_i(z^i+1/z^i)$ adódik, ahol $\gamma_i \in \mathbf{Q}$. Mint láttuk, ekkor $2u$ felírható $z + 1/z$ racionális együtthatós polinomjaként, tehát $u \in \mathbf{Q}(\mathrm{Re}\, z)$. Ugyanígy kapjuk, hogy $v = h(z)h(1/z) \in \mathbf{Q}(\mathrm{Re}\, z)$. Végül $w = u/v$, azaz w is eleme a $\mathbf{Q}(\mathrm{Re}\, z)$ bővítésnek.

• **A.10.17** Legyen $f = \Theta_0 + \Theta_1 x + \ldots + \Theta_n x^n$, ahol Θ_i algebrai, és legyen $f(\Psi) = 0$. Tekintsük az alábbi bővítésláncot:

$$M_0 = \mathbf{Q}, \quad M_{i+1} = M_i(\Theta_i), \text{ ha } i = 0, 1, \ldots, n \quad \text{és} \quad M_{n+2} = M_{n+1}(\Psi)\,.$$

Mindegyik „láncszem" véges fokú bővítés: bármely $0 \le i \le n$-re $\deg(M_{i+1} : M_i) \le \deg \Theta_i$ (itt azért nem áll feltétlenül egyenlőség, mert lehet, hogy a Θ_i-nek az M_i feletti foka kisebb, mint a $\mathbf{Q}$ feletti foka) és $\deg(M_{n+2} : M_{n+1}) \le n$. A fokszámtétel miatt ekkor az $M_{n+2} : \mathbf{Q}$ bővítés is véges fokú. Ebből következik, hogy M_{n+2} minden eleme algebrai szám, tehát speciálisan a Ψ is az.

• **A.11.8** Ha f osztója a $g_k = x^{p^k} - x$ polinomnak, akkor az A.11.7 feladat alapján f-nek van gyöke a p^k elemű M_k véges testben (sőt gyökténye zőkre bomlik M_k-ban). Egy ilyen gyöknek a foka éppen $\deg f$, és M_k minden elemének a foka osztója k-nak.

Megfordítva, tegyük fel, hogy $\deg f \mid k$. Jelöljük f fokát n-nel, ekkor az $F_p[x]/(f)$ faktorgyűrű egy p^n elemű véges test. Ez az M_n test az F_p-nek az f egyik Θ gyökével történő bővítése, $M_n = F_p(\Theta)$. Ekkor (pl. az A.11.7 feladat alapján) Θ gyöke a $g_n = x^{p^n} - x$ polinomnak. Mivel az f-nek és g_n-nek van közös gyöke és f irreducibilis, ezért szükségképpen $f \mid g_n$. Továbbá $n \mid k \Rightarrow p^n - 1 \mid p^k - 1 \Rightarrow g_n \mid g_k$. Innen kapjuk, hogy $f \mid g_k$ is teljesül.

• **A.11.12(a)** A p^k elemű test multiplikatív csoportjának a generátorelemei éppen a k-adfokú primitív polinomok gyökei. Két különböző primitív polinomnak az irreducibilitás miatt nem lehet közös gyöke, és ugyancsak az irreducibilitás miatt nincs többszörös gyök sem. Így minden primitív polinomnak k gyöke van, az összes primitív elemek száma $\varphi(p^k - 1)$, tehát a polinomok száma $\varphi(p^k - 1)/k$.

• **(b)** Jelöljük az F_p feletti k-adfokú irreducibilis (1 főegyütthatójú) polinomok számát I_k-val. Az útmutatást követve, az A.11.8 feladat szerint az $x^{p^k} - x$ polinom irreducibilis tényezőkre bontásában azok az irreducibilis polinomok szerepelnek, amelyeknek a foka osztója k-nak. Ezek mindegyike egyszer fordul elő $x^{p^k} - x$ felbontásában, mert $x^{p^k} - x$-nek nincs többszörös gyöke. A fokszámokat összehasonlítva $p^k = \sum_{d \mid k} dI_d$ adódik.

Innen I_k-t a *Möbius-féle megfordítási formula* segítségével fogjuk kifejezni. Ez az elnevezés a következő tételt takarja: ha $h(n)$ a pozitív egészeken értelmezett tetszőleges (komplex értékű) függvény és $H(n) = \sum_{d \mid n} h(d)$, akkor $h(n) = \sum_{d \mid n} \mu(d) H(n/d)$ (a $\mu(n)$ Möbius-függvény definícióját lásd az útmutatásnál). A $H(n)$-et a $h(n)$ osztókra vonatkozó *összegzési függvény*ének, $h(n)$-et pedig a $H(n)$ *megfordítási függvény*ének nevezzük. A formula bizonyítása a $\mu(n)$ következő tulajdonságán múlik: $S = \sum_{d \mid n} \mu(d) = 0$, ha $n > 1$ és $S = 1$, ha $n = 1$.

Visszatérve a $p^k = \sum_{d \mid k} dI_d$ összefüggésre, ez azt fejezi ki, hogy a $h(n) = nI_n$ számelméleti függvénynek az osztókra vonatkozó összegzési függvénye $H(n) = \sum_{d \mid n} dI_d = p^n$. Ekkor a Möbius-féle megfordítási formula alapján $h(n) = \sum_{d \mid n} \mu(d) H(n/d) = \sum_{d \mid n} \mu(d) p^{n/d}$, azaz $I_k = (1/k) \sum_{d \mid k} \mu(d) p^{k/d}$.

TÁRGYMUTÓ, JELÖLÉSEK

A könyvben szereplő fogalmak, elnevezések, valamint a leggyakrabban használt jelölések felsorolása következik (általában) az első előfordulási hely adataival. A fogalom, elnevezés után megadjuk a könyvben használt tipikus jelölését (ha van ilyen), majd annak a definíciónak, tételnek stb. a számát, ahol a fogalom, elnevezés, jelölés magyarázata megtalálható, végül zárójelben odaírjuk az oldalszámot is. A definíciószám, tételszám stb. után egy „−", illetve „+" jel szerepel, ha az adott fogalmat nem a jelzett definícióban, tételben stb., hanem (közvetlenül) azt megelőzően, illetve követően a szövegben (külön számozás nélkül) vezetjük be. Így pl. a transzcendens számnál DA.10.6+ arra utal, hogy a transzcendens szám értelmezése az A.10.6 definíció *után* (néhány sorral lejjebb) történik.

A jelölésekkel kapcsolatos legfontosabb információkat a 9. oldalon a „Technikai tudnivalók" c. rész is tartalmazza, de az alábbiakban ezeket is megismételjük.

A tárgymutatóban D1.1.2 jelenti az 1.1.2 Definíciót, és a D betű helyett T, L, B, F, E, M rendre a megfelelő számú tételre, lemmára, bizonyításra, feladatra, a feladathoz tartozó eredményre, illetve megoldásra utal. A 4.1 pontban szereplő 3. példát 4.1.P3-mal, a 6.6 pontot 6.6-tal, az A.7 pont 2. alpontját A.7/2-vel jelezzük.

A definíciók stb. számozásánál az első szám mindig a fejezetet, a második a fejezeten belül a pontot, a harmadik pedig a ponton belül a sorszámot jelöli. A definíciók és tételek sorszámozása egy ponton belül folyamatos, tehát pl. az 1.1.2 Definíció után az 1.1.3 Tétel következik. Az „A" fejezet „számjele" természetesen „A". Az illusztrációs példák (sima, egy számmal történő) számozása pontonként újrakezdődik.

Külön is kiemelünk néhány fontos jelölést, amelyek a könyvben leggyakrabban szereplő fogalmakat érintik. A vektorokat vastag latin kisbetűvel ($\mathbf{a}$), a skalárokat általában görög kisbetűvel (α), a mátrixokat dőlt latin nagybetűvel (A), a lineáris leképezéseket írott latin nagybetűvel ($\mathcal{A}$), a bilineáris függvényeket pedig vastag latin nagybetűvel ($\mathbf{A}$) jelöljük. Felhívjuk még a figyelmet arra, hogy a nulla nagyon sok mindent jelenthet (egész számot, gyűrű nullelemét, testbeli skalárt, vektort, vektorteret, alteret, mátrixot, lineáris leképezést, bilineáris függvényt stb.), és ezek közül többet ugyanúgy is jelölünk, azonban a szövegösszefüggésből mindig kiderül, hogy melyik jelentésről van szó.

A polinomokat f vagy $f(x)$, a fokszámukat „deg", a komplex számok valós

és képzetes részét „Re”, illetve „Im” jelöli, pl. $\deg(x^3+x)=3$, $\mathrm{Re}\,(4-i)=4$, $\mathrm{Im}\,(4-i)=-1$. Megkülönböztetjük a (valós) számok alsó és felső egész részét, és ezeket $\lfloor\ \rfloor$, illetve $\lceil\ \rceil$ jelöli, így pl. $\lfloor\pi\rfloor=3$, $\lceil\pi\rceil=4$. Az osztathatóságra, a legnagyobb közös osztóra és a legkisebb közös többszörösre (az egész számok és a polinomok esetén is) a szokásos jelöléseket használjuk, tehát pl. $x-1 \mid x^2-1$, $(9,15)=3$, $[9,15]=45$. A $[\ ]$ szögletes zárójel a legtöbbször egyszerűen zárójelet, néha legkisebb közös többszöröst, a 9.6 pontban pedig zárt intervallumot jelöl, továbbá $[\mathcal{A}]$, illetve $[\mathbf{A}]$ az $\mathcal{A}$ lineáris leképezés, illetve az $\mathbf{A}$ bilineáris függvény mátrixát jelenti.

Megemlítjük még, hogy a könyvben a definíciók, illetve a tételek megfogalmazásának a végén ♣ áll, a bizonyítások befejezését pedig ■ jelzi.