Fried Katalin

Korándi József

Török Judit

A modern algebra alapjai

Tartalomjegyzék

1. fejezet

Bevezető

Kedves Olvasó!

Ez a könyv egy háromkötetes elektronikus jegyzet harmadik kötete. A jegyzet a modern algebrához vezető rögös és hosszú út első és bátortalan lépéseit mutatja be tanárszakos hallgatóknak. Igyekeztünk azokra az alapvető ismeretekre szorítkozni, illetve részletesen kitérni, amelyek a tanítás során (akár burkoltan is) felmerülhetnek. Továbbá igyekeztünk az egyetemi szintű ismereteket összefűzni a korábban tanultakkal, hogy megkönnyítsük az új (fajta) gondolatmenetek feldolgozását.

Munkánkban sokan segítettek, külön köszönettel tartozunk Komjáth Péternek, a könyv korábbi verziójának lektorálásáért. Köszönetünk Hraskó Andrásnak, aki a javított, elektronikus kiadást nézte át. A könyv technikai feldolgozásában segítségünkre volt sok-sok hallgató, akiknek ezúton is köszönjük a munkájukat.

Az anyag három részre tagozódik:

Számelmélet Ez a rész az általános- és középiskolában tanult számelméleti ismereteket kívánja megalapozni, rendszerezni és kiegészíteni. Lényegében az oszthatóság fogalmától elindulva jutunk el a kongruenciákig és a számelméleti függvényekig. Utalás történik a mai modern számelméletnek – ha nem is a módszereire, de – néhány problémájára és eredményére. A feldolgozás során – tekintettel arra, hogy ez a rész kapcsolódik a legközvetlenebbül az általános iskolai anyaghoz – folyamatosan szem előtt tartottuk az iskolai alkalmazásokat, még ha nem is mindig tértünk ki rá.

„Klasszikus" algebra Ebben a részben megpróbáljuk összefoglalni azokat a (klasszikus) algebrai ismereteket, amelyek meggyőződésünk szerint az

algebrai alapműveltség részét képezik, és amelyekre a hallgatóknak egyéb tanulmányaik során is szükségük lehet. Így bevezetjük a komplex számokat, szólunk polinomokról és polinomegyenletekről, valamint még számos olyan dologról, amelyek neve egy ilyen bevezetésben valószínűleg inkább ijesztőek semmint lelkesítőek lennének, így most fel sem soroljuk ezeket. (A bátrabbak és a Szellemvasút kedvelői esetleg kukucskáljanak bele a tartalomjegyzékbe.) A feldolgozás során folyamatosan használni kezdjük az (absztrakt) algebra kifejezéseit, de ez már igazából a következő részhez tartozik. Íme:

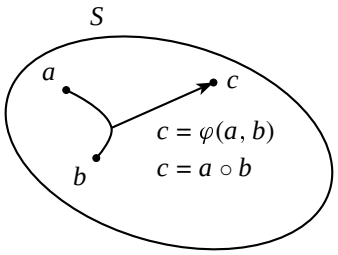
„Modern" algebra Manapság leginkább ezt szokás algebrának nevezni. Ebben a részben megismerked(het)ünk a mai matematika (és részben fizika, kémia stb.) egészét átható „absztrakt" gondolkodásmód alapfogalmaival, alapvető, illetve elemi tételeivel. Kiderül(het), hogy hol mindenütt fordulnak elő „algebrai" megfontolások az analízis témaköreiben, hogy miért nem geometriai, hanem algebrai probléma például a „kör négyszögesítése", de még akár az is megtudható, hogy mik azok a racionális számok.

2. fejezet

Algebrai műveletek

A következő fejezetekben elsősorban különféle algebrai struktúrákról lesz szó. Algebrai struktúrát úgy kaphatunk, ha egy nem üres halmazon egy vagy több ún. algebrai műveletet definiálunk.

2.1. Definíció. Az S nem üres halmazon értelmezett (kétváltozós) *algebrai művelet* egy olyan ($\varphi\colon S \times S \to S$) leképezés, amely az S halmaz két tetszőleges (nem feltétlenül különböző) eleméhez hozzárendeli az S halmaz egy elemét.



2.1. ábra.

Azt, hogy a leképezés az (a, b) elempárhoz a c elemet rendeli, vagyis

$$\varphi(a, b) = c,$$

úgy is jelölhetjük, hogy $a \circ b = c$, ahol „$\circ$” a műveletet jelöli.

Egy halmazon értelmezett kétváltozós algebrai művelet tehát egyrészt leképezés, vagyis a halmaz tetszőleges két (nem feltétlenül különböző) eleméhez hozzárendel egy eredményt – vagyis a halmaz bármelyik két elemén

elvégezhető a művelet –, másrészt a halmaznak zártnak kell lennie a műveletre nézve, vagyis tetszőleges két elem esetén a művelet eredményének is halmazbeli elemnek kell lennie.

Algebrai művelet például az egész (vagy páros egész vagy racionális vagy valós) számok halmazán az összeadás, a kivonás, a szorzás, a maximum-, illetve minimumképzés vagy például ha két számhoz hozzárendeljük a két szám négyzetösszegét.

Nem algebrai művelet az egész számok halmazán például az osztás (két egész szám hányadosa nem mindig egész szám) vagy a legnagyobb közös osztó képzése (a 0-nak és a 0-nak nincs értelmezve a legnagyobb közös osztója). Szintén nem algebrai művelet például a páratlan egészek halmazán az összeadás (a szorzás viszont igen), vagy a sík vektorainak halmazán a vektorok skaláris szorzása.

Megjegyzés. A kétváltozós műveletek értelmezéséhez hasonlóan értelmezhetünk egyváltozós, illetve kettőnél több változós algebrai műveleteket is. (Az egyváltozós műveleteket gyakrabban nevezzük függvényeknek.) Egyváltozós művelet például az egész számok halmazán az ellentettképzés vagy az abszolút érték képzése; háromváltozós pedig például az a művelet, amely tetszőleges három számhoz hozzárendeli a három szám maximumát.

2.2. ábra. A kétváltozós maximum művelet táblázata. A szürke oszlopban a művelet első operandusa, a szürke sorban a második szerepel.

2.2. Definíció. *Algebrai struktúrának* nevezzük az $(S, \circ, *, \ldots)$ legalább kéttagú rendszert, ahol S egy nem üres halmaz, a $\circ$, $*$, $\ldots$ pedig az S halmazon értelmezett algebrai műveletek.

Az algebrai struktúra tehát egy halmaz és egy vagy több rajta értelmezett algebrai művelet együttesét jelenti. Ahhoz, hogy egy $(H, \oplus, \otimes, \ldots)$ rendszerről eldöntsük, hogy algebrai struktúra-e, mindössze azt kell ellenőriznünk, hogy a $\oplus$, $\otimes$ stb. algebrai műveletek-e az S halmazon. Ennek megfelelően beszélhetünk például a páros egészek összeadási struktúrájáról, de nem beszélhetünk a páratlan egészek összeadási struktúrájáról.

Megjegyzés. Egy halmazon általában igen sokféle algebrai művelet értelmezhető. Ha például az $\{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$ tíz elemű halmazon szeretnénk egy kétváltozós algebrai műveletet értelmezni, akkor a halmaz elemeiből álló $10 \cdot 10 = 100$ elempár mindegyikéhez hozzá kell rendelnünk egy halmazbeli elemet. Miután a 100 elempár mindegyikénél teljesen szabadon

dönthetjük el, hogy a halmaz tíz eleme közül melyiket rendeljük hozzá az illető elempárhoz, ezt összesen 10^{100}-féleképpen tehetjük meg, tehát a fenti halmazon 10^{100}-féle algebrai művelet értelmezhető. Ezek közül bizonyosaknak van ismerős neve – szerepelni fog köztük például a maximumképzés vagy a legnagyobb közös osztó képzése –, többségüknek azonban nincs, de ettől még bármelyiket is választhatjuk vizsgálódásaink tárgyául.

Amikor egy $(S, \circ, *, \cdot, \ldots)$ algebrai struktúráról beszélünk, akkor a $\circ$, $*$, $\ldots$ műveletek nem az S halmazon értelmezett összes elképzelhető algebrai műveletet jelentik, hanem egy vagy több konkrétan megadott műveletet. Ennek megfelelően $(\mathbb{Z}, +)$ jelenti az egész számok összeadási struktúráját, $(\mathbb{Z}, \cdot)$ az egész számok szorzási struktúráját, $(\mathbb{Z}, +, \cdot)$ pedig az egész számok struktúráját az összeadásra és a szorzásra nézve. $(\mathbb{Z}, \circ)$ nem jelent semmit, amíg meg nem mondjuk, hogy pontosan milyen műveletet jelöltünk $\circ$-rel. Ha az egész számok összeadását, kivonását és szorzását már értelmeztük, akkor mondhatjuk például azt, hogy definiáljuk a $\circ$ műveletet a következőképpen:

$$\forall a, b \in \mathbb{Z}, \qquad a \circ b := a + b - ab,$$

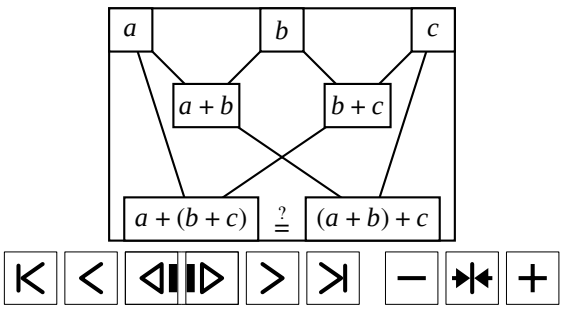
és ekkor már beszélhetünk a $(\mathbb{Z}, \circ)$ struktúráról.

Mint később látni fogjuk, az algebrai struktúrákat aszerint szokás csoportosítani, hogy a bennük szereplő művelet vagy műveletek milyen tulajdonságokkal rendelkeznek. A leggyakoribb szóbajövő szempontok (műveleti tulajdonságok) a következők:

2.3. Definíció. Az $(S, \circ, \ldots)$ struktúra $\circ$ művelete

kommutatív, ha $\forall a, b \in S$-re $a \circ b = b \circ a$;

asszociatív, ha $\forall a, b, c \in S$-re $(a \circ b) \circ c = a \circ (b \circ c)$; (2.3. ábra), azaz a zárójel elhagyható



2.3. ábra.

invertálható, ha $\forall a, b \in S$-hez léteznek olyan $x, y \in S$ elemek, amelyekre $a \circ x = b$ és $y \circ a = b$. (Az $a \circ x = b$ és $y \circ a = b$ egyenletek megoldhatók S-ben.)

Az $(S, \circ, *, \ldots)$ struktúra $*$ művelete *disztributív* a $\circ$ műveletére, ha $a, b, c \in S$-re a $a * (b \circ c) = (a * b) \circ (a * c)$ és $(a \circ b) * c = (a * c) \circ (b * c)$.

2.1. Megjegyzés. Amikor azt mondjuk, hogy minden $a, b \in S$, akkor természetesen akár ugyanaz az elem is lehet az a és a b, vagyis arra gondolunk – most és a továbbiakban is –, hogy minden, nem feltétlenül különböző $a, b \in S$ elemekre vonatkozik az megállapítás.

Ritkábban fogunk hivatkozni a következő műveleti tulajdonságokra:

Az $(S, \circ, \ldots)$ struktúra $\circ$ művelete *idempotens,* ha $\forall a \in S$-re $a \circ a = a$ és *kancellatív,* ha $\forall a, b \in S$-re az $a \circ x = b$ és $y \circ a = b$ egyenleteknek legfeljebb egy-egy megoldása van S-ben.

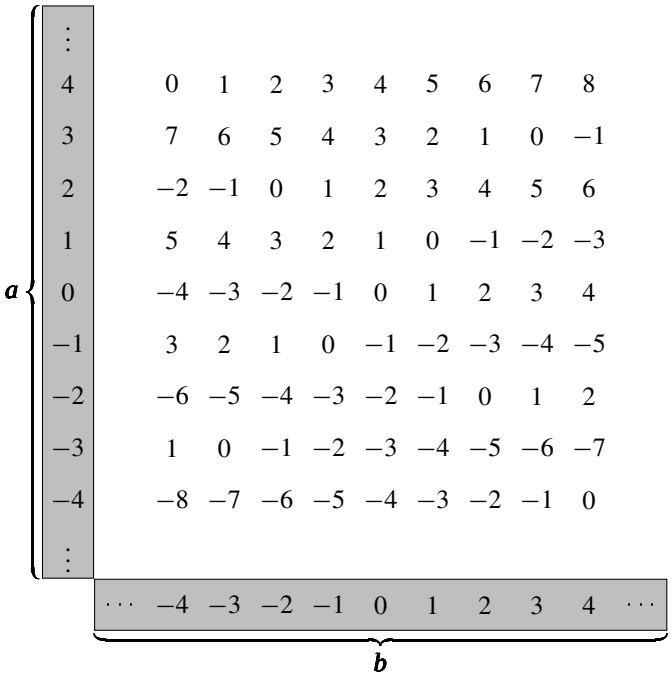
Az $(S, \circ, *, \ldots)$ struktúra művelete *abszorbtív* a $\circ$ műveletre nézve, ha $\forall a, b \in S$-re a $(a \circ b) = a$ (elnyelési tulajdonság).

Például az egész számok halmazán értelmezett műveletek közül könnyen ellenőrízhető, hogy:

1. Kommutatív, asszociatív és invertálható (nem idempotens de kancellatív) például az összeadás.
2. Kommutatív, asszociatív de nem invertálható (nem idempotens és nem kancellatív) például a szorzás.
3. Nem kommutatív, nem asszociatív de invertálható (nem idempotens de kancellatív) például a kivonás.
4. Kommutatív, nem asszociatív de invertálható (nem idempotens és nem kancellatív) például a következő művelet: $a \circ b := |a + b|$.
5. Nem kommutatív de asszociatív és invertálható (nem idempotens de kancellatív) például a következő művelet:

$$a \circ b := \begin{cases} a + b, & \text{ha } a \text{ páros} \\ a - b, & \text{ha } a \text{ páratlan.} \end{cases} \quad \text{(2.4. ábra)}$$

6. Kommutatív de nem asszociatív és nem invertálható (nem idempotens és nem kancellatív) például a következő művelet: $a \circ b := (a + b)^2$.
7. Nem kommutatív de asszociatív és nem invertálható (idempotens és nem kancellatív) például a következő művelet: $a \circ b := a$.



2.4. ábra.

8. Nem kommutatív, nem asszociatív és nem is invertálható (nem idempotens és nem kancellatív) például a következő művelet: $a \circ b := a^2 + b$.

A fenti példák közül a szorzás disztributív az összeadásra nézve (a 6. példában szereplő művelet pedig abszorbtív bármelyik műveletre nézve).

Algebrai struktúrák vizsgálata során azt is érdemes megnézni, hogy vannak-e az adott művelettel kapcsolatban speciálisan viselkedő elemek a halmazban:

2.4. Definíció. Az $(S, \circ)$ algebrai struktúra n elemét *neutrális elemnek* nevezzük, ha $\forall a \in S$-re $a \circ n = n \circ a = a$.

Egyműveletes struktúrákban szokás a neutrális elemet egységelemnek nevezni, több művelet esetén mindig meg kell mondanunk, hogy melyik művelet neutrális eleméről beszélünk. Ha a műveletek között szerepel összeadás vagy szorzás (avagy annak nevezett művelet), akkor az összeadás neutrális elemét általában (additív) zérusnak, a szorzás neutrális elemét pedig egységelemnek nevezzük.

Amennyiben az $(S, \circ)$ struktúra n' elemére teljesül, hogy $\forall a \in S$-re $n' \circ a = a$, akkor n'-t szokás bal oldali neutrális elemnek (bal oldali egységelemnek), ha pedig $\forall a \in S$-re $a \circ n' = a$, akkor jobb oldali neutrális elemnek (jobb oldali egységelemnek) nevezni.

Megjegyzés. Az „egység" és az „egységelem" nem azonos fogalmak. Az egységelem definiciója a fenti, míg az $(S, \circ)$ struktúra egy ε elemét akkor nevezzük egységnek, ha a struktúra minden elemének „osztója", vagyis ha $\forall a \in S$-hez létezik olyan $q \in S$, amelyre $\varepsilon \circ q = q \circ \varepsilon = a$. Az egységelem mindig egység is, fordítva viszont nem igaz, például $(\mathbb{Z}, \cdot)$-ban a -1 egység, de nem egységelem.

Például az egész számok halmazán:

1. Az összeadás neutrális eleme (additív zérus) a 0.
2. A szorzás neutrális eleme (egységelem) az 1.
3. Az $a \circ b := |a + b|$ műveletnek nincs neutrális eleme.
4. Az $a \circ b := \begin{cases} a + b, & \text{ha } a \text{ páros} \\ a - b, & \text{ha } a \text{ páratlan} \end{cases}$ művelet neutrális eleme a 0. (2.4. ábra)
5. Az $a \circ b := (a + b)^2$ műveletnek nincs neutrális eleme.
6. Az $a \circ b := a$ műveletnek nincs neutrális eleme, viszont bármelyik (egész) szám jobb oldali neutrális elem.
7. A kivonásnak nincs neutrális eleme, viszont a 0 jobb oldali neutrális elem.
8. Az $a \circ b := a^2 + b$ műveletnek nincs neutrális eleme, viszont a 0 bal oldali neutrális elem.

2.1. Tétel. *Egy $(S, \circ)$ struktúrában legfeljebb egy neutrális elem lehet.*

Bizonyítás. Tegyük fel, hogy az $(S, \circ)$ struktúrában n_1 is és n_2 is neutrális elem. Ekkor egyrészt $n_1 \circ n_2 = n_1$ (mert n_2 neutrális elem), másrészt $n_1 \circ n_2 = n_2$ (mert n_1 neutrális elem), így $n_1 = n_2$. □

Megjegyzés. A tétel bizonyítása során csak azt használtuk fel, hogy n_2 jobb oldali, n_1 pedig bal oldali neutrális elem. Ezek szerint az is igaz, hogy ha egy struktúrában van bal oldali neutrális elem is és jobb oldali neutrális elem is, akkor azok szükségképpen egybeesnek.

2.5. Definíció. Az $(S, \circ)$ struktúra z elemét *zéruselemnek* nevezzük, ha $\forall S$-re $a \circ z = z \circ a = z$.

A neutrális elemhez hasonlóan definiálhatunk bal, illetve jobb oldali zéruselemet is.

Megjegyzés. A „zérus” és a „zéruselem” nem azonos fogalmak, zérusnak általában az összeadás neutrális elemét nevezik.

a \ b	$\cdots$	-4	-3	-2	-1	0	1	2	3	4	$\cdots$
$\vdots$											
4		0	1	2	3	4	5	6	7	8	
3		1	0	1	2	3	4	5	6	7	
2		2	1	0	1	2	3	4	5	6	
1		3	2	1	0	1	2	3	4	5	
0		4	3	2	1	0	1	2	3	4	
-1		5	4	3	2	1	0	1	2	3	
-2		6	5	4	3	2	1	0	1	2	
-3		7	6	5	4	3	2	1	0	1	
-4		8	7	6	5	4	3	2	1	0	
$\vdots$											

2.5. ábra.

Fenti példáink közül:

1. $(\mathbb{Z}, +)$-ban nincs zéruselem.
2. $(\mathbb{Z}, \cdot)$-ban zéruselem a 0.
3. $(\mathbb{Z}, \circ)$-ben, ahol $a \circ b := |a + b|$, nincs zéruselem. (2.5. ábra)
4. $(\mathbb{Z}, \circ)$-ben, ahol $a \circ b := \begin{cases} a + b, & \text{ha } a \text{ páros} \\ a - b, & \text{ha } a \text{ páratlan} \end{cases}$, nincs zéruselem. (2.4. ábra)

5. $(\mathbb{Z}, \circ)$-ben, ahol $a \circ b := (a+b)^2$, nincs zéruselem.
6. $(\mathbb{Z}, \circ)$-ben, ahol $a \circ b := a$, nincs zéruselem, viszont minden (egész) szám bal oldali zéruselem.
7. $(\mathbb{Z}, -)$-ban nincs zéruselem.
8. $(\mathbb{Z}, \circ)$-ben, ahol $a \circ b := a^2 + b$, nincs zéruselem.

2.2. Tétel. *Egy $(S, \circ)$ struktúrában legfeljebb egy zéruselem lehet.*

Bizonyítás. Tegyük fel, hogy z_1 is és z_2 is zéruselem. Ekkor $z_1 \circ z_2 = z_1$ (mert z_2 zéruselem), ugyanakkor $z_1 \circ z_2 = z_2$ (mert z_1 zéruselem), így $z_1 = z_2$. □

Érdekes kérdés lehet, hogy ha a struktúrában van neutrális elem, akkor mely elemekhez létezik olyan elem, amellyel „összeművelve" a neutrális elemet kapjuk eredményül, azaz mely a elemek esetén van megoldása az $a \circ x = n$, illetve $y \circ a = n$ egyenletnek.

2.6. Definíció. Amennyiben az $(S, \circ)$ struktúra neutrális eleme n, és a struktúra a eleméhez létezik a struktúrának olyan a' eleme, amelyre $a \circ a' = a' \circ a = n$, akkor az a' elemet az a elem *inverzének* nevezzük. (Ha $a \circ a' = n$, akkor a' az a jobb oldali, ha pedig $a' \circ a = n$, akkor a' az a bal oldali inverze.)

Ha a struktúra művelete az összeadás, akkor az a elem inverzét szokás $(-a)$-val, egyébként pedig (a^{-1})-nel jelölni.

Például:

1. $(\mathbb{Z}, +)$-ban minden elemnek van inverze (az ellentettje).
2. $(\mathbb{Z}, \cdot)$-ban csak az 1-nek és a (-1)-nek van inverze (mindkettőnek önmaga).
3. $(\mathbb{Z}, \circ)$-ben, ahol $a \circ b := \begin{cases} a+b, & \text{ha } a \text{ páros} \\ a-b, & \text{ha } a \text{ páratlan} \end{cases}$, minden elemnek van inverze (a páros számoknak az ellentettjük, a páratlanoknak önmaguk). (2.4. ábra)

Érdemes észrevenni, hogy egy struktúra egységeleme (ha van) mindig önmaga inverze.

Azt is érdekes lehet megvizsgálni, hogy egy zéruselemes struktúrában vannak-e olyan – a zéruselemtől különböző – elemek, amelyeken elvégezve a műveletet a zéruselemet kapjuk.

2.7. Definíció. Az $(S, \circ)$ zéruselemes struktúrát *zérusosztómentesnek* (*nullosztómentesnek*) nevezzük, ha $\forall a, b \in S$-re $a \circ b = z$ akkor és csak akkor teljesül, ha $a = z$ vagy $b = z$ (ahol z a struktúra zéruseleme).

Példáink közül csak $(Z, \cdot)$-ban volt zéruselem, és mivel két egész szám szorzata akkor és csak akkor 0, ha legalább az egyik tényező 0, $(Z, \cdot)$ zérusosztómentes. Nem zérusosztómentes például a 2×2-es mátrixok szorzási struktúrája, mert például

$$\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

További példák:

1. Logikai műveletek A kételemű i, h halmazon összesen 16-féle (legfeljebb) kétváltozós algebrai műveletet értelmezhetünk, ezeket szokás kijelentéslogikai műveleteknek nevezni. Megvizsgálva közülük néhányat, például a következőket tapasztalhatjuk:

– Az „és” művelet ($\wedge$): kommutatív és asszociatív, de nem invertálható. (Továbbá idempotens és nem kancellatív.) Egységelem az i, zéruselem a h. Csak az egységelemnek van inverze. Az $(\{i, h\}, \wedge)$ struktúra zérusosztómentes.

		b: i	h
	$\wedge$		
a: i		i	h
a: h		h	h

– A „(megengedő) vagy” művelet ($\vee$): kommutatív, asszociatív, nem invertálható (idempotens és nem kancellatív). Egységelem a h, zéruselem az i. Csak az egységelemnek van inverze. Az $(\{i, h\}, \vee)$ struktúra zérusosztómentes.

		b: i	h
	$\vee$		
a: i		i	i
a: h		i	h

Az „és” művelet disztributív a „vagy” műveletre nézve, és a „vagy” művelet is disztributív az „és” műveletre nézve. (Az „és” művelet abszorbtív a „vagy” műveletre nézve, és a „vagy” művelet is abszorbtív az „és” műveletre nézve.)

– Implikáció ($a \to b$) nem kommutatív, nem asszociatív, nem invertálható (nem idempotens és nem kancellatív). Sem egységelem, sem zéruselem nincs (az i bal oldali egységelem, és egyben jobb oldali zéruselem).

		b: i	h
	$\to$		
a: i		i	h
a: h		h	i

– Ekvivalencia ($\Leftrightarrow$) kommutatív, asszociatív, invertálható (nem idempotens de kancellatív). Egységelem az i, zéruselem nincs. Mindkét elem önmaga inverze.

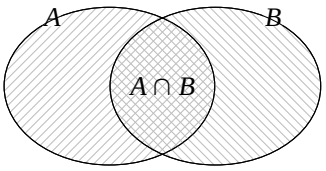
	$\Leftrightarrow$	b: i	h
a: i		i	h
a: h		h	i

2. Halmazműveletek Ahhoz, hogy egy halmazokból álló alaphalmaz algebrai struktúrát alkosson valamelyik ismerős halmazműveletre – például a metszet- vagy unióképzésre – nézve (vagyis ahhoz, hogy például a metszet- vagy unióképzés algebrai művelet legyen halmazok valamilyen halmazán), igen körültekintően kell eljárnunk az alaphalmaz megválasztásakor. Teljesülnie kell ugyanis annak, hogy az alaphalmaz tetszőleges két elemén elvégzett művelet eredményének is az alaphalmaz elemének kell lennie. Ezt például úgy garantálhatjuk, ha egy előre rögzített H halmaz $P(H)$ hatványhalmazát választjuk alaphalmaznak.

– A metszetképzés ($\cap$):

$$A \cap B := \{x \mid (x \in A) \wedge (x \in B)\}$$

kommutatív, asszociatív, nem invertálható (idempotens és nem kancellatív). Egységelem maga a H halmaz, zéruselem az üres halmaz. Az egységelemen kívül egyik elemnek sincs inverze. A $(P(H), \cap)$ struktúra nem zérusosztómentes (hiszen két diszjunkt halmaz metszete akkor is üres, ha egyik halmaz sem az üres halmaz).

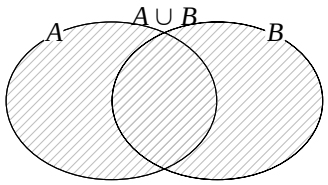


2.6. ábra.

– Unióképzés ($\cup$):

$$A \cup B := \{x \mid (x \in A) \vee (x \in B)\}$$

kommutatív, asszociatív, nem invertálható (idempotens és nem kancellatív). Egységelem az üres halmaz, zéruselem a H halmaz. Az egységelemen kívül egyik elemnek sincs inverze. A $(P(H), \cup)$ struktúra nem zérusosztómentes (hiszen tetszőleges A elemét például a (H-ra vonatkozó) komplementerével egyesítve a H halmazt kapjuk). A metszet- és unióképzés kölcsönösen disztributívak (és abszorbtívak) egymásra nézve.

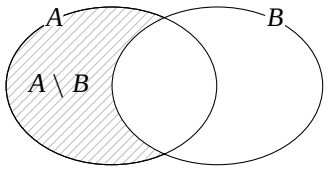


2.7. ábra.

– Különbség ($\setminus$):

$$A \setminus B := \{x \mid (x \in A) \wedge (x \notin B)\}$$

nem kommutatív, nem asszociatív, nem invertálható (nem idempotens de kancellatív). Sem egységelem, sem zéruselem nincs.

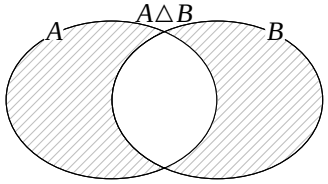


2.8. ábra.

– Szimmetrikus differencia ($\triangle$):

$$\begin{aligned} A \triangle B &:= (A \setminus B) \cup (B \setminus A) \\ &= \Big\{x \mid \big((x \in A) \wedge (x \notin B)\big) \vee \big((x \notin A) \wedge (x \in B)\big)\Big\} \end{aligned}$$

kommutatív, asszociatív, invertálható (nem idempotens de kancellatív). Egységelem az üres halmaz, zéruselem nincs. Minden elemnek van inverze (saját maga). A metszetképzés disztributív, de nem abszorbtív a szimmetrikus differenciára nézve.



2.9. ábra.

3. Leképezések szorzása (függvénykompozíció, összetett függvény) Általában egy $\varphi(x)\colon H \to K$ és egy $\psi(x)\colon K \to L$ leképezés szorzatán a $\psi \cdot \varphi\colon H \to L$, $(\psi \cdot \varphi)(x) = \psi\big(\varphi(x)\big)$ leképezést értjük. Ahhoz, hogy leképezések egy halmaza algebrai struktúrát alkosson erre a műveletre nézve, arra van szükség, hogy a szóbanforgó leképezések bármelyikének az értelmezési tartománya tartalmazza bármelyiknek az értékkészletét. Az alaphalmaznak emiatt egy előre rögzített H halmazt önmagára vivő leképezésekből, vagy ezek egy alkalmasan megválasztott részhalmazából kell állnia.

– Az összes $\mathbb{R} \to \mathbb{R}$ (valós függvények) leképezések halmazán a függvénykompozíció nem kommutatív de asszociatív, és nem invertálható (nem idempotens és nem kancellatív). Egységelem az $x \mapsto x$ függvény, zéruselem nincs. Inverze a bijektív leképezéseknek (és csak azoknak) van.

– Az $\mathbb{R} \to \mathbb{R}$ lineáris függvények ($x \mapsto ax + b$, ahol $a \neq 0$ és $a, b \in \mathbb{R}$) halmazán a függvénykompozíció nem kommutatív, de asszociatív és invertálható (nem idempotens de kancellatív). Egységelem az $x \mapsto x$ függvény, zéruselem nincs. Minden elemnek van inverze:

$$(x \mapsto ax + b)^{-1} = \left(x \mapsto \frac{1}{a}x - \frac{b}{a}\right)$$

– A kételemű $\{0, 1\}$ halmazt a következő négy leképezés viszi önmagára:

$$\varphi_1\colon \begin{cases} 0 \to 0 \\ 1 \to 0 \end{cases} ; \varphi_2\colon \begin{cases} 0 \to 0 \\ 1 \to 1 \end{cases} ; \varphi_3\colon \begin{cases} 0 \to 1 \\ 1 \to 0 \end{cases} ; \varphi_4\colon \begin{cases} 0 \to 1 \\ 1 \to 1 \end{cases}$$

E leképezések halmazán a leképezések szorzásának művelettáblázata:

		$\overbrace{\qquad\qquad}^{\varphi_b}$			
$\varphi_a \cdot \varphi_b$		φ_1	φ_2	φ_3	φ_4
φ_a	φ_1	φ_1	φ_1	φ_1	φ_1
	φ_2	φ_1	φ_2	φ_3	φ_4
	φ_3	φ_4	φ_3	φ_2	φ_1
	φ_4	φ_4	φ_4	φ_4	φ_4

Ez a művelet nem kommutatív de asszociatív, nem invertálható (nem idempotens és nem kancellatív). Egységelem a φ_2, zéruselem nincs (φ_1 bal oldali, φ_4 pedig jobb oldali zéruselem).

Inverze φ_2-nek és φ_3-nak van (mindkettőnek önmaga).

– A $\{0, 1\}$ halmazt önmagára vivő bijektív leképezések halmazán (vagyis a fenti halmaz $\{\varphi_2, \varphi_3\}$ részhalmazán a leképezések szorzása kommutatív, asszociatív és invertálható) (nem idempotens de kancellatív).

– Geometriai transzformációk

Egy tetszőleges ponthalmazt (például a síkot) önmagára vivő leképezéseket szokás geometriai transzformációknak nevezni. A leképezések szorzása ilyenkor a transzformációk egymás utáni alkalmazását jelenti. például a síkot önmagára vivő összes transzformációk halmazán a transzformációk szorzása nem kommutatív de asszociatív, nem invertálható (nem idempotens és nem kancellatív); egységelem a helyben hagyás (identikus leképezés), zéruselem nincs; inverze a bijektív leképezéseknek (és csak azoknak) van.

Egy ponthalmazt önmagára vivő transzformációk közül a távolságtartó leképezéseket egybevágósági transzformációknak nevezik. Egy tetszőleges ponthalmazt önmagára vivő egybevágósági transzformációk halmazán a leképezések szorzása általában nem kommutatív, de mindig asszociatív és invertálható (általában nem idempotens de mindig kancellatív). Egységelem a helyben hagyás, zéruselem általában nincs.

– Homogén lineáris leképezések

Egy T test feletti vektorteret önmagára vivő leképezések közül a homogén lineáris leképezések (transzformációk) önmagukban is algebrai struktúrát alkotnak a leképezések szorzására nézve. Például a valós test feletti (tetszőleges) n-dimenziós vektortér homogén lineáris transzformációinak halmazán a leképezések szorzása nem kommutatív de asszociatív, nem invertálható (nem idempotens de kancellatív); egységelem az identikus leképezés, zéruselem az a leképezés, amely minden vektorhoz a 0-vektort rendeli. A struktúra nem zérusosztómentes. (Minden lényeges tulajdonsága megegyezik a valós feletti $n \times n$-es mátrixok szorzási struktúrájának tulajdonságaival.)

4. Vektorok szorzása A tér vektorainak halmazán szokás úgynevezett skaláris szorzást, illetve vektoriális szorzást definiálni.

2.8. Definíció. A vektorok *skaláris szorzása* ($\mathbf{a} \cdot \mathbf{b} = |\mathbf{a}| \cdot |\mathbf{b}| \cdot \cos(\mathbf{a}, \mathbf{b})$) nem algebrai művelet, hiszen két vektor skaláris szorzata nem eleme az alaphalmaznak (nem vektor, hanem szám).

2.9. Definíció. Két vektor *vektoriális szorzatát* a következőképpen értelmezzük: $\mathbf{a} \times \mathbf{b} = \mathbf{c}$, ahol $|\mathbf{c}| = |\mathbf{a}| \cdot |\mathbf{b}| \cdot \sin(\mathbf{a}, \mathbf{b})$ és $\mathbf{c}$ merőleges $\mathbf{a}$-ra is és $\mathbf{b}$-re is, továbbá az $\mathbf{a}$, $\mathbf{b}$, $\mathbf{c}$ vektorok (ebben a sorrendben) jobbrendszert alkotnak.

A vektoriális szorzás

– nem kommutatív ($\forall \mathbf{a}, \mathbf{b}$-re $\mathbf{a} \times \mathbf{b} = -\mathbf{b} \times \mathbf{a}$),

– nem is asszociatív ($\forall \mathbf{a}$, $\mathbf{b}$-re $(\mathbf{a} \times \mathbf{a}) \times \mathbf{b} = \mathbf{0} \times b = \mathbf{0}$, míg ha $\mathbf{a}$, $\mathbf{b} \neq \mathbf{0}$ és $\mathbf{a}$ nem párhuzamos $\mathbf{b}$-vel, akkor $\mathbf{a} \times (\mathbf{a} \times \mathbf{b}) \neq 0$),

– nem invertálható (ha $\mathbf{b}$ nem merőleges $\mathbf{a}$-ra, akkor sem az $\mathbf{a} \times \mathbf{x} = \mathbf{b}$, sem az $\mathbf{y} \times \mathbf{a} = \mathbf{b}$ egyenletnek nincs megoldása).

(Nem idempotens (hiszen $\forall \mathbf{a}$-ra $\mathbf{a} \times \mathbf{a} = \mathbf{0}$), és nem is kancellatív (az $\mathbf{a} \times \mathbf{x} = \mathbf{0}$, és az $\mathbf{y} \times \mathbf{a} = \mathbf{0}$ egyenletnek minden olyan vektor megoldása, amely párhuzamos $\mathbf{a}$-val).)

– Egységelem nincs, zéruselem a $\mathbf{0}$ vektor.

Érdemes még megjegyezni, hogy a vektoriális szorzás disztributív a vektorok összeadására.

Feladatok

1. Adja meg a $\{0, 1\}$ kételemű halmazon értelmezhető összes kétváltozós műveletet! Határozza meg, hogy ezek közül melyek asszociatívak!

2. Legyen $\circ$ olyan művelet, hogy $a \circ b = a \cdot b + a + b$ (a „$\cdot$” és a „$+$” a valós számok halmazán szokásos műveleteket jelöli).

   Művelet-e a $\circ$ a nemnegatív egész számok halmazán?

   Művelet-e a $\circ$ az egész számok halmazán?

   Művelet-e a $\circ$ a valós számok halmazán?

   Határozza meg, hogy a megismert műveleti tulajdonságok közül melyekkel rendelkezik a $\circ$!

3. Keressünk olyan műveletet a $\mathbb{Z}$ halmazon, amely

   (a) Kommutatív, de nem asszociatív;
   (b) Asszociatív, de nem kommutatív;
   (c) Asszociatív és kommutatív;
   (d) Nem asszociatív és nem is kommutatív.

4. Határozza meg, hogy elvégezhetők-e az alábbi műveletek az adott halmazokon, vagyis hogy zártak-e a halmazok az adott műveletekre! Ha igen, határozzuk meg, milyen műveleti tulajdonságokkal rendelkeznek!

   (a) $\mathbb{N}$, $+$ (b) $\mathbb{N}$, $-$ (c) $\mathbb{N}$, $\cdot$ (d) $\mathbb{N}$, $/$

   (e) $\mathbb{Z}$, $+$ (f) $\mathbb{Z}$, $-$ (g) $\mathbb{Z}$, $\cdot$ (h) $\mathbb{Z}$, $/$

   (i) $\mathbb{Z}_4$, $+$ (j) $\mathbb{Z}_4$, $-$ (k) $\mathbb{Z}_4$, $\cdot$ (l) $\mathbb{Z}_4$, $/$

5. (a) Írja fel a négyzetet önmagába vivő egybevágósági transzformációkat!

(b) Határozza meg a transzformációpárok szorzatát!

(c) Keressen köztük két olyan transzformációt (u_1, u_2), amelyekre $u_1 u_2 = u_2 u_1$.

(d) Kommutatív-e a négyzet transzformációinak halmazán a transzformációszorzás?

6. Igazolja, hogy tetszőleges A és B halmazokra $(A \triangle B) \triangle A = B$ és $(B \triangle A) \triangle B = A$!

   Igazolja, hogy az $A_1 \triangle A_2 \triangle \cdots \triangle A_n$ (bármely zárójelezés mellett elvégzett) művelet eredménye azon elemek halmaza, amelyek az A_1, A_2, …, A_n halmazok közül páratlan sokban szerepelnek!

7. Legyen H a sík pontjainak halmaza, és jelöljük az origót O-val. Legyen A az origó körüli síkbeli forgatások halmaza. Értelmezzük az A halmazon a forgatásszorzat műveletet: két forgatáshoz hozzárendeli a szorzatukat (egymás után végzett forgatást).

   Zárt-e az A halmaz a forgatásszorzatra nézve?

   Milyen műveleti tulajdonságai vannak a forgatásszorzatnak?

8. Az S sík O pontjára illeszkedő egynesek az alaphalmaz, az ezekre vonatkozó tükrözés egy művelet. Értelmezzük a tükrözések halmazán a szorzás műveletet az alábbiak szerint. Értelmezzük tükrözések halmazán a tükrözésszorzat műveletet, amely definíció szerint két tengelyes tükrözéshez hozzárendeli a szorzatukat (egymás után végzett tükrözést).

   Zárt-e a B halmaz a tükrözésszorzatra nézve?

   Milyen műveleti tulajdonságai vannak a tükrözésszorzásnak?

3. fejezet

Félcsoportok

A következő néhány fejezetben (2–6.) egyműveletes algebrai struktúrákról lesz szó. Amikor általában beszélünk egy egyműveletes $(S, \circ)$ algebrai struktúráról, akkor a műveletet – bármi is legyen az – szokás szorzásnak nevezni, és a művelethez kapcsolódó jelölések is általában a szorzásnál megszokott jelölésrendszert követik. Például a művelet jele gyakran a „$\cdot$” jel (és $a \cdot b$ helyett gyakran csak ab-t írunk), az a elem inverzét a^{-1}, az a elemen ismételten (n-szer) elvégzett művelet eredményét a^n jelöli, a neutrális elemet (ha van) egységelemnek nevezik, satöbbi.

Mi a továbbiakban – az esetleges félreértések elkerülése végett – általában „$\circ$”-rel jelöljük a műveletet, de elő fog fordulni, hogy a *két elemen elvégzett művelet eredménye* helyett a két elem *szorzatáról* beszélünk, és egyéb jelöléseink (például inverz) is általában a szorzásnál megszokottak lesznek.

Olyankor persze, amikor konkrét, ismert és nem szorzás nevű műveletről van szó (például összeadás, legnagyobb közös osztó képzése, satöbbi), az illető művelet nevét, jelét, és (ha vannak ilyenek, akkor) a hozzá igazodó egyéb jelöléseket használjuk (ha például összeadás a művelet, akkor az a elem (additív) inverzét $-a$-val jelöljük).

3.1. Definíció. Az $(S, \circ)$ algebrai struktúra *félcsoport,* ha a $\circ$ művelet asszociatív.

Ahhoz tehát, hogy eldönthessük, hogy egy halmaz egy műveletre nézve félcsoport-e, először is meg kell győződnünk arról, hogy a művelet értelmes-e a halmazon és a halmaz zárt-e a műveletre nézve (a halmaz bármelyik két elemén elvégezhető a művelet, és az eredmény is minden esetben benne van a halmazban), majd ellenőriznünk kell, hogy a művelet asszociatív-e. Ha a művelet nemcsak asszociatív, hanem kommutatív is, akkor szokás *kommutatív félcsoportról* beszélni.

Például:

1. A természetes számok halmaza a legnagyobb közös osztó képzésére nem félcsoport, mert a $(0, 0)$ nincs értelmezve. (Könnyen belátható, hogy ha a legnagyobb közös osztó definícióját kiegészítenénk azzal, hogy $(0, 0) = 0$ – vagyis ha a legnagyobb közös osztó művelet helyett a kitüntetett közös osztót tekintjük –, akkor az így módosított műveletre nézve már félcsoportot alkotnának a természetes számok.) A pozitív egészek halmazán már értelmes művelet a legnagyobb közös osztó képzése, hiszen tetszőleges két pozitív egész számnak egyértelműen létezik legnagyobb közös osztója, és az minden esetben pozitív egész. Mivel tetszőleges a, b, c pozitív egészekre $(a, (b, c)) = ((a, b), c)$, vagyis a művelet asszociatív, a pozitív egészek félcsoportot (és mivel $(a, b) = (b, a)$, kommutatív félcsoportot) alkotnak a legnagyobb közös osztó képzésére. (Hasonlóan gondolható meg, hogy a nem 0 egész számok halmaza is kommutatív félcsoport a legnagyobb közös osztó képzésére.)

2. A természetes (egész, racionális, valós, komplex) számok egyaránt kommutatív félcsoportot alkotnak az összeadásra is és a szorzásra is.

3. A természetes számok nem alkotnak félcsoportot a kivonásra nézve, mert például $2 - 5$ nem természetes szám. Az egész (racionális, satöbbi) számok halmazán már értelmes művelet a kivonás, de félcsoportról most sem beszélhetünk, mert nem asszociatív. $(a - b) - c$ általában nem egyenlő $a - (b - c)$-vel.

4. Az egész számok tetszőleges részhalmaza kommutatív félcsoportot alkot akár a maximum- (3.1. ábra) akár a minimumképzésre.

a \ b	2	3	4	5	6	7	8	9	10
10	10	10	10	10	10	10	10	10	10
9	9	9	9	9	9	9	9	9	10
8	8	8	8	8	8	8	8	9	10
7	7	7	7	7	7	7	8	9	10
6	6	6	6	6	6	7	8	9	10
5	5	5	5	5	6	7	8	9	10
4	4	4	4	5	6	7	8	9	10
3	3	3	4	5	6	7	8	9	10
2	2	3	4	5	6	7	8	9	10

3.1. ábra. A $\max(a, b)$ művelet táblázata

5. Értelmezzük a pozitív egészek halmazán a $\circ$ műveletet úgy, hogy $a \circ b$ jelentse azt a pozitív egész számot, melyet úgy kapunk, hogy az a szám „mögé írjuk" a b számot, például $152 \circ 98 = 15\,298$. Könnyen meggondolható, hogy $(\mathbb{N}^+, \circ)$ félcsoport (amely nyilvánvalóan nem kommutatív). Hasonlóan értelmezhetjük egy tetszőleges halmaz elemeiből alkotott összes véges sorozat halmazán az „egymás mögé írás" műveletét, minden esetben félcsoportot fogunk kapni. (Ha például „szó"-nak nevezünk egy tetszőleges véges betűsorozatot, akkor a „szavak" halmaza félcsoportot alkot az „egymás mögé írás" műveletre nézve.)

6. Egy tetszőleges halmaz hatványhalmaza (összes részhalmazainak halmaza) kommutatív félcsoportot alkot akár a metszet, akár az unió műveletére nézve.

7. Egy tetszőleges halmazt önmagára vivő leképezések halmaza félcsoportot alkot a leképezések szorzására (függvények kompozíciójára).

Az, hogy egy művelet asszociatív, azt jelenti, hogy tetszőleges három elem esetén a három elemen elvégzett művelet eredménye független a zárójelezéstől (l. 2.3. ábra és animáció az asszociativitásra), így a zárójelek akár el is hagyhatók. Az is igaz azonban, hogy ha asszociatív a művelet, akkor hosszabb műveletláncok elvégzése esetén is független az eredmény a zárójelezéstől. Ha tehát $(S, \circ)$ félcsoport, akkor például tetszőleges $a, b, c, d \in S$ esetén:

$$\begin{aligned}\Big(\big((a \circ b) \circ c\big) \circ d\Big) &= \big(a \circ (b \circ c)\big) \circ d = \\ &= (a \circ b) \circ (c \circ d) = \\ &= a \circ \big(b \circ (c \circ d)\big) = \\ &= a \circ \big((b \circ c) \circ d\big).\end{aligned}$$

A fenti egyenlőségek az asszociativitás definíciójából könnyen bizonyíthatóak, mi most tetszőleges n (≥ 3, pozitív egész) darab elem esetére fogjuk bizonyítani a következő állítást.

3.1. Tétel. *Az $(S, \circ)$ félcsoportban véges sok elemen végrehajtott művelet eredménye független a zárójelek elhelyezkedésétől.*

Bizonyítás. Egy vagy két elem esetén semmitmondó az állítás, $n \geq 3$ darab elem esetén teljes indukcióval fogjuk bizonyítani. Három elem esetén az asszociativitás miatt nyilvánvalóan igaz az állítás. Legyen $n > 3$, és tegyük

fel, hogy minden n-nél kisebb darabszámra már igaz az állítás. Jelöljük A-val az n elemen a rögzített

$$\Big(\big((\ldots(a_1 \circ a_2) \circ \ldots) \circ a_{n-1}\big) \circ a_n\Big)$$

zárójelezéssel nyert eredményt, B-vel pedig egy tetszőleges zárójelezéssel nyert eredményt. Azt szeretnénk bizonyítani, hogy $A = B$. Könnyen meggondolható, hogy B mindig felírható $B = C \circ D$ alakban, ahol D már n-nél kevesebb elemet tartalmaz, így indukciós feltevésünk szerint átzárójelezhető $D = E \circ a_n$ alakúra. Ekkor $B = C \circ D = C \circ (E \circ a_n)$. Az asszociativitás miatt viszont $C \circ (E \circ a_n) = (C \circ E) \circ a_n$, ahol $C \circ E$ is n-nél kevesebb elemet tartalmaz, így az indukciós feltevés ismételt kihasználásával átzárójelezhető

$$C \circ E = \Big(\big((\cdots(a_1 \circ a_2) \circ a_3) \circ \ldots\big) \circ a_{n-1}\Big)$$

alakúra, így $B = (C \circ E) \circ a_n = A$, amit bizonyítani akartunk. □

Megjegyzés. Könnyen meggondolható, hogy ha a művelet kommutatív is, akkor véges sok elemen elvégzett művelet eredménye az elemek sorrendjétől sem függ.

Megjegyzés. Ha a $\circ$ művelet asszociatív, akkor az a elemen n-szer ($n \in \mathbf{N}^+$) elvégzett ismételt művelet eredménye független a zárójelezéstől. Ez jogosít fel minket a következő jelölésre:

$$\underbrace{a \circ a \circ a \circ a \circ \ldots \circ a}_{n} = a^n$$

Szintén az asszociativitás következménye, hogy a következő azonosságok teljesülnek:

$$a^k \circ a^n = a^{k+n}, \qquad \text{illetve} \qquad (a^k)^n = a^{kn}$$

Ha a $\circ$ művelet nemcsak asszociatív, hanem kommutatív is, akkor a következő azonosság is igaz:

$$(a \circ b)^n = a^n \circ b^n$$

Egy $(S, \circ)$ félcsoportban nem feltétlenül van egységelem (vagyis olyan $e \in$ $\in S$, melyre tetszőleges $a \in S$ esetén $a \circ e = e \circ a = a$) (ahogyan a maximum művelet esetében sem volt, a műveleti táblát a 3.1. ábrán láthatjuk), de ha mégis van, akkor *egységelemes félcsoportról* beszélünk. Fenti példáink közül

1. $(\mathbf{N}^+, \text{lnko})$-ban nincs egységelem.Igaz ugyan, hogy tetszőleges a-hoz találhatók olyan x számok, amelyekre $(a, x) = a$, de olyan x szám, amely egyszerre lenne megfelelő minden a-hoz, nincs. Más lenne a helyzet, ha a legkisebb közös többszörös képzését választottuk volna a műveletnek, ekkor $[a, 1] = a$ miatt az 1 egységelem.

2. $(\mathbb{N}, +)$-ban a 0, $(\mathbf{N}, \cdot)$-ban az 1 egységelem.

3. $(\mathbf{Z}, -)$ nem volt félcsoport. Ettől még lehetne benne egységelem, de nincs. Igaz ugyan, hogy minden a-ra $a - 0 = a$, de $0 - a \neq a$. (A 0 jobb oldali egységelem, de nem bal oldali egységelem.)

4. $(\mathbf{N}^+, \text{egymás mögé írás})$-ban nyilvánvalóan nincs egységelem. (Ha azonban megengednénk a 0 darab karakterből álló, úgynevezett üres sorozatot, akkor ez egységelem lenne.)

5. $(P(H), \cap)$-ban egységelem a H halmaz, hiszen tetszőleges $A \subseteq H$ esetén $A \cap H = A$. $(P(H), \cup)$-ban egységelem az üres halmaz, hiszen teszőleges $A \subseteq H$ esetén $A \cup \emptyset = A$.

6. Az *egy halmazt önmagára vivő leképezések* félcsoportjában egységelem az identikus leképezés.

7. A maximum, illetve minimumképzés esetén attól függ az egységelem létezése, hogy van-e az alaphalmaznak legkisebb, illetve legnagyobb eleme. Maximumképzés esetén a legkisebb, minimumképzés esetén a legnagyobb elem az egységelem (ha van).

Egy félcsoport elemeinek nem feltétlenül van inverzük. (Ahol például nincs egységelem, ott nincs is értelme inverzekről beszélni). Belátható azonban, hogy félcsoportban – ha van is – egy elemnek *legfeljebb egy* inverze lehet.

3.2. Tétel. *Az $(S, \circ)$ félcsoportban bármely elemnek legfeljebb egy inverze van.*

Bizonyítás. Tegyük fel, hogy az a elemnek a' is és a'' is inverze, vagyis

$$a \circ a' = a' \circ a = e \qquad \text{és} \qquad a \circ a'' = a'' \circ a = e.$$

Ekkor az asszociativitás miatt

$$(a'' \circ a) \circ a' = a'' \circ (a \circ a').$$

Mivel $a'' \circ a = a \circ a' = e$ ebből $e \circ a' = a'' \circ e$, vagyis $a' = a''$. □

Megjegyzés. Ugyanígy látható be, hogy ha egy félcsoportban egy elemnek van bal inverze is és jobb inverze is, akkor egyetlen bal inverze és egyetlen jobb inverze van, melyek megegyeznek. Az viszont lehetséges, hogy egy elemnek több bal inverze is van de csak akkor, ha jobb inverze nincs, és viszont.

Meg fogjuk mutatni, hogy ha egy egységelemes félcsoportban minden elemnek van inverze, akkor a művelet invertálható, és megfordítva, ha egy félcsoportban invertálható a művelet, akkor a félcsoportnak van egységeleme, és minden elemnek van inverze.

3.3. Tétel. *Ha az $(S, \circ)$ algebrai struktúrában a $\circ$ művelet asszociatív, akkor a következő két állítás ekvivalens:*

1. *$\exists e \in S$, amelyre tetszőleges $a \in S$ esetén $a \circ e = e \circ a = a$ (van egységelem), és $\forall a \in S$-hez $\exists a^{-1}$, amelyre $a \circ a^{-1} = a^{-1} \circ a = e$ (minden elemnek van inverze).*
2. *Tetszőleges $a, b \in S$ esetén van megoldása az $a \circ x = b$ és $y \circ a = b$ egyenleteknek (a $\circ$ művelet invertálható).*

Bizonyítás. Az első állításból következik a második, mert mint arról behelyettesítéssel könnyen meggyőződhetünk $x = a^{-1} \circ b$ megoldása az egyik, $y = b \circ a^{-1}$ pedig a másik egyenletnek. Most megmutatjuk, hogy a második állításból következik az első. Az $a \circ x = b$ és $y \circ a = b$ egyenletnek tetszőleges a és b esetén van megoldása, így akkor is, ha $b = a$. Jelöljük az $a \circ x = a$ megoldását e_j-vel, az $y \circ a = a$ megoldását pedig e_b-vel. Meg fogjuk mutatni, hogy a félcsoport tetszőleges c elemére teljesül, hogy $c \circ e_j = e_b \circ c = c$, majd pedig hogy $e_j = e_b$, amiből következik, hogy $e_j = e_b = e$ egységelem.

Legyen az $y \circ a = c$ egyenlet megoldása y_0 és az $a \circ x = c$ egyenlet megoldása x_0. Ekkor

$$c \circ e_j = (y_o \circ a) \circ e_j = y_o \circ (a \circ e_j) = y_0 \circ a = c,$$

és

$$e_b \circ c = e_b \circ (a \circ x_o) = (e_b \circ a) \circ x_o = a \circ x_o = c,$$

vagyis e_j jobb oldali, e_b pedig bal oldali egységelem a félcsoportban. Ha viszont tetszőleges c esetén teljesül, hogy $c \circ e_j = c$, akkor $c = e_b$ esetén is, így $e_b \circ e_j = e_b$. Ugyanígy, ha tetszőleges c esetén $e_b \circ c = c$, akkor $c = e_j$ esetén is, így $e_b \circ e_j = e_j$. Vagyis $e_b \circ e_j$ e_b-vel is és e_j-vel is egyenlő, ami csak úgy lehet, ha $e_b = e_j$. Tehát ha $e_b = e_j = e$, akkor tetszőleges c-re $c \circ e = e \circ c = c$, vagyis e egységelem. Jelöljük most egy tetszőleges a elem esetén a'-vel az $a \circ x = e$, a''-vel pedig az $y \circ a = e$ egyenlet megoldását. Ekkor $a \circ a' = a'' \circ a = e$, amiből az előző tétel bizonyítása szerint következik, hogy $a' = a''$, vagyis az $a^{-1} = a' = a''$ elem az a elem inverze, tehát minden elemnek van inverze. □

3.4. Tétel. *Ha egy $(S, \circ)$ egységelemes félcsoportban az a elemnek is és a b elemnek is van inverze (a-nak a', b-nek b'), akkor az $a \circ b$ elemnek is van inverze, és ez $(a \circ b)' = b' \circ a'$.*

Bizonyítás. Az asszociativitás miatt

$$(a \circ b) \circ (b' \circ a') = \big(a \circ (b \circ b')\big) \circ a'.$$

Ebből kihasználva, hogy $b \circ b' = e$, $a \circ e = a$ és $a \circ a' = e$, a következő adódik:

$$\big(a \circ (b \circ b')\big) \circ a' = (a \circ e) \circ a' = a \circ a' = e,$$

vagyis $(a \circ b) \circ (b' \circ a') = e$, tehát a $b' \circ a'$ elem jobbinverze $a \circ b$-nek.

Hasonlóan látható be, hogy balinverz is:

$$(b' \circ a') \circ (a \circ b) = b' \circ ((a' \circ a) \circ b) = b' \circ (e \circ b) = b' \circ b = e.$$

Ebből már következik a tétel állítása. □

3.5. Tétel. *Ha egy $(S, \circ)$ félcsoportban a c elemnek van inverze (c'), továbbá $a \circ c = b \circ c$ vagy $c \circ a = c \circ b$, akkor $a = b$.*

Bizonyítás. Ha $a \circ c = b \circ c$, akkor $(a \circ c) \circ c' = (b \circ c) \circ c'$. Felhasználva az asszociativitást,

$$(a \circ c) \circ c' = a \circ (c \circ c') = a \qquad \text{és} \qquad (b \circ c) \circ c' = b \circ (c \circ c') = b.$$

Ezek szerint $a = b$. Hasonlóan látható be az is, hogy ha $c \circ a = c \circ b$, akkor $a = b$. □

Megjegyzés. Ha egy $(S, \circ)$ struktúrában – annak ellenére, hogy nem minden elemnek létezik inverze – teljesül, hogy $\forall a, b, c \in S$ elemekre $a \circ c = b \circ c$, illetve $c \circ a = c \circ b$ esetén teljesül $a = b$, akkor azt mondjuk, hogy ebben a struktúrában érvényes az **egyszerűsítési szabály**. Ilyen struktúra például a természetes számok az összeadásra. (Az, hogy itt teljesül az egyszerűsítési szabály levezethető például a Peano-axiómákból: ha két rákövetkező egyenlő, akkor a két szám is egyenlő, és visszafelé lépkedve a számokon eljutunk az $a = b$-hez.)

Részfélcsoport

Ha egy $(S, \circ)$ félcsoportban elemek valamilyen nem üres halmaza zárt a műveletre nézve, akkor ez a halmaz az adott műveletre önmagában is félcsoportot alkot. Az ilyen tulajdonságú halmazokat szokás az eredeti félcsoport részfélcsoportjainak nevezni. Az $(S, \circ)$ félcsoport $(S_1, \circ)$ részcsoportját így jelöljük: $S \geq S_1$ vagy $S_1 \leq S$.

3.2. Definíció. Ha az $(S, \circ)$ félcsoportban $S^* \subseteq S$ és $(S^*, \circ)$ önmagában is félcsoport, akkor azt mondjuk, hogy $(S^*, \circ)$ *részfélcsoportja* az $(S, \circ)$ félcsoportnak.

3.6. Tétel. *Legyen S^* (nem üres) részhalmaza S-nek, és $(S, \circ)$ félcsoport. $(S^*, \circ)$ akkor és csak akkor részfélcsoportja $(S, \circ)$-nek, ha tetszőleges $a, b \in S^*$ esetén $a \circ b$ is eleme S^*-nak.*

Bizonyítás. Ha $(S^*, \circ)$ részfélcsoportja $(S, \circ)$-nek, akkor önmagában is félcsoport, aminek szükséges feltétele, hogy az S^* halmaz zárt legyen a $\circ$ műveletre nézve, ami éppen azt jelenti, hogy tetszőleges $a, b \in S^*$ esetén $a \circ b$ is eleme S^*-nak. Ha tetszőleges $a, b \in S^*$ esetén $a \circ b$ is eleme S^*-nak, akkor az S^* halmaz zárt a $\circ$ műveletre. Ahhoz, hogy félcsoport legyen az kell még, hogy a $\circ$ művelet asszociatív legyen. Abból azonban, hogy $(S, \circ)$ félcsoport, tudjuk, hogy a $\circ$ művelet asszociatív, így mivel $S^* \subseteq S$, $(S^*, \circ)$ részfélcsoportja $(S, \circ)$-nek. □

Tetszőleges $(S, \circ)$ félcsoport triviálisan részfélcsoportja önmagának. Ha van a félcsoportban egységelem, akkor ez az elem önmagában $e \circ e = e$ miatt szintén triviálisan egy egyelemű részfélcsoportot alkot. Az ettől a kétféle (triviális) részfélcsoporttól különböző részfélcsoportokat szokás *valódi részfélcsoportnak* nevezni. A triviális részfélcsoportot ennek megfelelően szokás nem valódinak is nevezni.

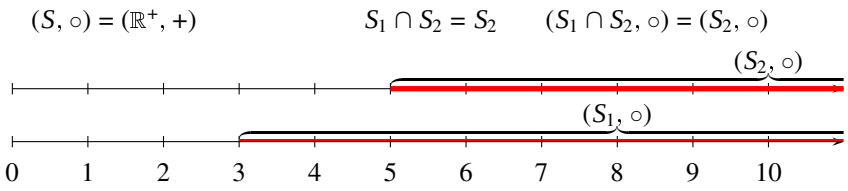
Valódi részfélcsoportja például a természetes számok összeadási félcsoportjának a páros természetes számok halmaza (mert két páros természetes szám összege is páros természetes szám), vagy egy tetszőleges n természetes szám nem negatív többszöröseinek a halmaza az összeadásra nézve. Szintén valódi részfélcsoport például a 100-nál nagyobb egészek halmaza (mert két 100-nál nagyobb egész összege is 100-nál nagyobb egész).

Néha arra vagyunk kíváncsiak, hogy egy adott félcsoportnak melyik az a legszűkebb részfélcsoportja, amely néhány előre rögzített elemet tartalmaz. Legszűkebben azt értjük, hogy neki már nincs olyan saját magától különböző részfélcsoportja, amely a megadott elemeket tartalmazná. Azt, hogy ez egyértelmű, a következő tétel garantálja.

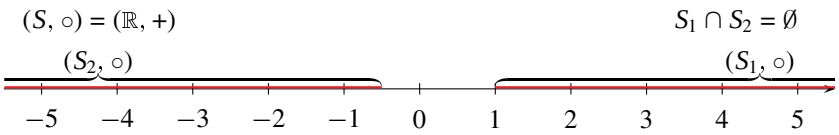
3.7. Tétel. *Egy félcsoport akárhány részfélcsoportjának metszete vagy üres, vagy szintén részfélcsoport.*

Például:
Bizonyítás. Legyen $(S_1, \circ)$ is és $(S_2, \circ)$ is részfélcsoportja $(S, \circ)$-nek. Elég azt megmutatni, hogy tetszőleges $a, b \in S_1 \cap S_2$ esetén $a \circ b \in S_1 \cap S_2$.

Ha $a, b \in S_1 \cap S_2$, akkor a is és b is eleme S_1-nek is és S_2-nek is. Mivel $(S_1, \circ)$ félcsoport, az igaz lesz, hogy $a \circ b \in S_1$, és mivel $(S_2, \circ)$ is félcsoport,



3.2. ábra.



3.3. ábra.

$a \circ b \in S_2$. Ha viszont S_1-nek is és S_2-nek is eleme, akkor a metszetüknek is. Kettőnél több részfélcsoport esetén ugyanígy gondolható meg, hogy ha a is és b is eleme a részfélcsoportok metszetének, akkor $a \circ b$ is eleme a metszetnek. □

Most már biztosak lehetünk abban, hogy ha megadjuk egy félcsoport valahány elemét, akkor mindig lesz a félcsoportnak egy legszűkebb részfélcsoportja, amely a megadott elemeket tartalmazza, hiszen az eredeti teljes félcsoport mindig tartalmazza az adott elemeket, ha pedig több olyan részfélcsoport is van amely tartalmazza az adott elemeket, akkor az összes ilyennek a metszete lesz a legszűkebb.

3.3. Definíció. Az $(S, \circ)$ félcsoportnak azt a legszűkebb $(S^*, \circ)$ részfélcsoportját, amelyre teljesül, hogy $a, b, c, \ldots \in S^*$, az $a, b, c \ldots$ *elemek által generált részfélcsoportjának* nevezzük.

Például: $(\mathbb{N}, +)$-ban a 0 az egyelemű, csak a 0-t tartalmazó részfélcsoportot generálja, az 1 a pozitív egészek összeadási félcsoportját, a 2 a páros pozitív egészeket,egy tetszőleges n pozitív egész szám pedig az n pozitív többszörseit.

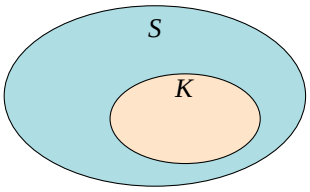
Két rögzített elem, a és b esetén, azoknak a számoknak a halmazát kapjuk, amelyek előállnak $ax + by$ alakban, ahol x és y természetes számok, de nem mindkettő 0.

Ha például $a = 3$ és $b = 5$, akkor az általuk generált részfélcsoportnak eleme lesz a 3, az 5, a $3 + 3 = 6$, a $3 + 5 = 8$, a $3 + 3 + 3 = 9$, az $5 + 5 = 10$, továbbá a $8 + 3 = 11$, a $9 + 3 = 12$, a $10 + 3 = 13$, és így tovább, 3-asával növelve a már megkapott elemeket, az összes 13-nál nagyobb egészt megkapjuk. Vagyis a 3 és az 5 által generált részfélcsoportnak a 3, az 5 és a

6 mellett minden 8-nál nem kisebb egész szám eleme lesz. (Általában is igaz, hogy ha $(a, b) = 1$, akkor minden $(a-1)(b-1)$-nél nem kisebb egész előáll $ax + by$ alakban, ahol x és y természetes számok, de nem mindkettő 0.)

Komplexusok

3.4. Definíció. Az $(S, \circ)$ félcsoportban az S halmaz egy tetszőleges nem üres részhalmazát *komplexusnak* nevezzük. Komplexusok között értelmezzük a következő *komplexusszorzás* nevű műveletet.



3.4. ábra.

3.5. Definíció. Legyen K_1 és K_2 az $(S, \circ)$ félcsoport két komplexusa.

$$K_1 \circ K_2 := \{a \circ b \mid a \in K_1 \text{ és } b \in K_2\}.$$

Két komplexus szorzata tehát egy olyan halmaz, mely az S halmaz elemeiből készített összes olyan kéttényezős „szorzat”-ot tartalmazza, ahol a „szorzat” első tényezője K_1-ból, a második K_2-ból való.

Megjegyzés. A *komplexusszorzás* művelet nevében a *szorzás* nem a szorzás nevű műveletet jelenti, hanem azt a műveletet, amelyre nézve az S halmaz félcsoportot alkot. Ha ennek a műveletnek van saját neve, akkor a *szorzás* szót helyettesíthetjük ezzel a névvel, például $(\mathbb{N}, +)$ komplexusain végzett komplexusszorzás esetén szokás a komplexusok összeadásáról beszélni.

Például:

1. Legyen az $(\mathbb{N}, +)$ félcsoportban $K_1 = \{0, 1\}$ és $K_2 = \{10, 100\}$.
   Ekkor $K_1 + K_2 = \{10, 11, 100, 101\}$.

2. Legyen $S = \{0, 1, 2, 3, 4\}$, a művelet a modulo 5 összeadás. (S erre a műveletre zárt, a művelet asszociatív, tehát $(S, +_{\bmod 5})$ félcsoport.) Ha $K_1 = \{1, 2\}$ és $K_2 = \{3, 4\}$, akkor $K_1 + K_2 = \{1+3, 1+4, 2+3, 2+4\} = \{4, 0, 1\}$. De:

   Legyen $S = \{1, 2, 3, 4\}$, a művelet a modulo 5 szorzás. (S erre a műveletre zárt, a művelet asszociatív, tehát $(S, \cdot_{\bmod 5})$ félcsoport.) Ha $K_1 = \{1, 2\}$ és $K_2 = \{3, 4\}$, akkor $K_1 \cdot K_2 = \{1 \cdot 3, 1 \cdot 4, 2 \cdot 3, 2 \cdot \cdot 4\} = \{3, 4, 1\}$.

Két komplexus szorzata nyilvánvalóan szintén komplexus, vagyis szintén részhalmaza az S halmaznak, hiszen minden $a \in K_1$-re és $b \in K_2$-re a is és b is eleme S-nek, és mivel S zárt arra a műveletre, amire nézve félcsoport, $a \cdot b$ is eleme S-nek. Ez egyben azt is jelenti, hogy egy $(S, \circ)$ félcsoport összes komplexusainak halmaza zárt a komplexusszorzásra nézve.

3.8. Tétel. *A komplexusszorzás asszociatív.*

Bizonyítás. Az állítás azon múlik, hogy az eredeti félcsoportban asszociatív a művelet. Legyen ugyanis K_1, K_2 és K_3 az $(S, \circ)$ félcsoport három tetszőleges komplexusa. Azt szeretnénk belátni, hogy $(K_1 \circ K_2) \circ K_3 = K_1 \circ (K_2 \circ K_3)$.

$$(K_1 \circ K_2) \circ K_3 = \{(a \circ b) \circ c \mid a \in K_1, b \in K_2, c \in K_3\}$$
$$K_1 \circ (K_2 \circ K_3) = \{a \circ (b \circ c) \mid a \in K_1, b \in K_2, c \in K_3\}$$

Mivel tetszőleges $a, b, c \in S$ esetén $(a \circ b) \circ c = a \circ (b \circ c)$, a két halmaz egyenlő. □

Tételünk miatt egy tetszőleges $(S, \circ)$ félcsoport esetén S összes komplexusainak halmaza félcsoportot alkot a komplexusszorzásra.

Például: legyen $S = \{0, 1\}$, a művelet pedig a szokásos szorzás. Könnyen meggyőződhetünk arról, hogy $(S, \cdot)$ félcsoport (csak azt kell ellenőriznünk, hogy a művelet nem vezet ki). Ekkor S összes komplexusainak halmaza: $\{\{0\}, \{1\}, \{0, 1\}\}$, a komplexusszorzás művelettáblázata pedig a következő:

$\cdot$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0\}$	$\{0\}$	$\{0\}$	$\{0\}$
$\{1\}$	$\{0\}$	$\{1\}$	$\{0,1\}$
$\{0,1\}$	$\{0\}$	$\{0,1\}$	$\{0,1\}$

Feladatok

1. Az $S = \{\mathrm{i}, \mathrm{h}\}$ logikai értékek halmaza mely logikai műveletekkel alkot félcsoportot?

2. Félcsoportot alkot-e a $\{10, 12, 14, \ldots\}$ végtelen halmaz a szokásos összeadásra, illetve a szokásos szorzásra nézve? Állapítsuk meg, hogy milyen tulajdonságokkal rendelkeznek ezek a műveletek!

3. Fécsoportot alkot-e az $\{0, 1, 2, 3\}$ halmaz a 4 maradékai szerint végzett összeadásra, illetve szorzásra nézve? (Vagyis ha valamely művelet eredménye nem esik a halmazba, akkor ahelyett annak 4 szerinti maradékát vesszük.) Állapítsa meg, hogy milyen tulajdonságokkal rendelkeznek ezek a műveletek!

4. Félcsoportot alkot-e az egész számok fölötti polinomok halmaza a polinomösszeadás műveletére?

5. Félcsoportot alkot-e a sík vektorainak halmaza a szokásos vektorösszeadás műveletére?

6. Félcsoportot alkot-e a sík vektorainak halmaza a szokásos skalárszorzás műveletére?

7. Igazolja, hogy a 2×2-es valós mátrixok halmaza a mátrixösszeadásra félcsoportot alkot!

8. Igazolja, hogy az $S = \{2k \mid k \in \mathbb{N}\}$ halmaz a szokásos összeadásra nézve félcsoportot alkot! Tekintsük ennek két komplexusát: $K_1 = \{2, 4, 6\}$ és $K_2 = \{10, 20, 30\}$. Határozza meg a $K_1 + K_2$ komplexusszorzatot!

9. Igazolja, hogy a 2×2-es reguláris (invertálható) valós mátrixok halmaza a mátrixszorzásra nézve félcsoportot alkot!

   (a) Részfélcsoportotját alkotják-e az 1 determinánsú mátrixok?

   (b) Részfélcsoportotját alkotják a -1 determinánsú mátrixok?

   (c) Mi az általuk generált félcsoport?

   (d) Mi az 1, illetve a -1 determinánsú mátrixok részhalmazának komplexusszorzata?

10. Az $S = \{a, b, c\}$ halmazon értelmezzük úgy a $\circ$ műveletet, hogy tetszőleges $x, y \in S$ elemekre $x \circ y = y$. Félcsoport-e $(S, \circ)$?

4. fejezet

Csoportok

Mint láttuk, a félcsoportokban nem feltétlenül van egységelem, és még ha van is, akkor sincs feltétlenül inverze az elemeknek. Azokat a speciális félcsoportokat, amelyekben van egységelem és minden elemnek van inverze, csoportoknak nevezik. A 3.3. Tétel szerint ezt a definíciót a következőképpen is megfogalmazhatjuk:

4.1. Definíció. A $(G, \circ)$ algebrai struktúra *csoport,* ha a $\circ$ művelet asszociatív és invertálható.

Ha a művelet még kommutatív is, akkor szokás kommutatív csoportról vagy más néven *Abel-csoportról* beszélni.

Például:

1. $(\mathbb{Z}, +)$ kommutatív csoport.
2. $(\mathbb{Z}, \cdot)$ nem csoport, mert a szorzás nem invertálható (csak a ± 1-nek van multiplikatív inverze).
3. $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$ kommutatív csoportok.
4. $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$ egyike sem csoport, mert a szorzás nem invertálható (az $a \cdot x = b$ egyenletnek nincs megoldása, ha $a = 0$ és $b \neq 0$). Könnyen meggondolható azonban, hogy $(\mathbb{Q}^+, \cdot)$, $(\mathbb{R}^+, \cdot)$, $(\mathbb{C}\setminus\{0\}, \cdot)$ és $(\mathbb{Q}\setminus\{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$ mindegyike kommutatív csoport.
5. Tetszőleges test feletti polinomok az összeadásra nézve kommutatív csoportot alkotnak, a szorzásra nézve nem alkotnak csoportot.
6. Az $n \times n$-es mátrixok halmaza az összeadásra nézve kommutatív csoport, a szorzásra nézve nem csoport.

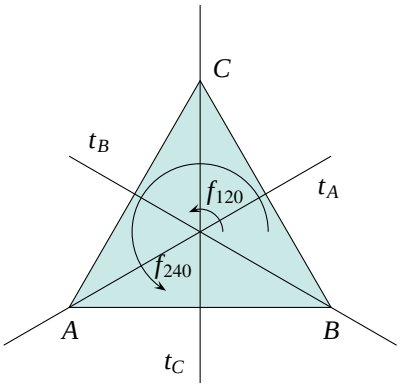
7. Szimmetriacsoportok

Egy tetszőleges geometriai alakzatot önmagára vivő egybevágósági transzformációk csoportot alkotnak a leképezések szorzására (transzformációk egymásutánja) nézve. (Egybevágóságok egymásutánja is egybevágóság; a leképezések szorzása asszociatív; egységelem az identikus leképezés (helyben hagyás, ami szintén egybevágóság); az egybevágósági transzformációk bijektív leképezések, így mindegyiknek van inverze, és az szintén olyan bijektív leképezés, amely az alakzatot önmagára viszi.) Ezt a csoportot nevezik az illető alakzat *szimmetriacsoportjának*.

Például a (nem négyzet) téglalap szimmetriacsoportjának négy eleme van: e (helyben hagyás), f_{180} (180 fokos forgatás, más néven középpontos tükrözés), t_1 és t_2 (az oldalfelező merőlegesekre vonatkozó tengelyes tükrözés), művelettáblázata pedig a következő:

$\cdot$	e	f_{180}	t_1	t_2
e	e	f_{180}	t_1	t_2
f_{180}	f_{180}	e	t_2	t_1
t_1	t_1	t_2	e	f_{180}
t_2	t_2	t_1	f_{180}	e

A szabályos sokszögek szimmetriacsoportját szokás *diédercsoportnak* is nevezni, ahol D_n-nel jelöljük a szabályos n-szög diédercsoportját (csak az $n > 2$ esettel foglalkozunk). Egy szabályos n-szög D_n szimmetriacsoportjának (ahol $n \geq 3$) mindig $2n$ eleme van (n darab tengelyes tükrözés és – beleértve a 0 fokos forgatást, azaz a helyben hagyást – n darab forgatás), és sohasem kommutatív csoport.



4.1. ábra. D_3 – a harmadrendű diédercsoport

8. **Mod m maradékosztályok**

Egy tetszőleges m modulus esetén kommutatív csoportot alkotnak a mod m maradékosztályok az összeadásra nézve. (A maradékosztályok összeadása asszociatív és kommutatív; egységelem a 0 maradékosztálya; az a elem maradékosztályának additív inverze a $-a$ elem maradékosztálya.) Szokásos jelölése ennek a csoportnak: $(\mathbb{Z}_m, +)$.

Az is könnyen meggondolható, hogy a mod m redukált maradékosztályok kommutatív csoportot alkotnak a szorzásra nézve. (Redukált maradékosztályok szorzata is redukált maradékosztály; a maradékosztályok szorzása asszociatív és kommutatív, egységelem az 1 maradékosztálya, az a elem maradékosztályának inverze – az Euler-Fermat tétel következtében – az $a^{\varphi(m)-1}$ maradékosztálya.)

$\dots$	-16	-11	-6	-1	4	9	14	19	24	$\dots$
$\dots$	-17	-12	-7	-2	3	8	13	18	23	$\dots$
$\dots$	-18	-13	-8	-3	2	7	12	17	22	$\dots$
$\dots$	-19	-14	-9	-4	1	6	11	16	21	$\dots$
$\dots$	-20	-15	-10	-5	0	5	10	15	20	$\dots$

4.2. ábra. A modulo 5 maradékosztályok – és lehetséges reprezentánsaik

Például az $m = 5$ esetben a mod 5 maradékosztályok összeadásának és a redukált maradékosztályok szorzásának művelettáblázata:

$+$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$
$\bar{2}$	$\bar{2}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$
$\bar{3}$	$\bar{3}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{0}$	$\bar{1}$	$\bar{2}$	$\bar{3}$

$\cdot$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{1}$	$\bar{1}$	$\bar{2}$	$\bar{3}$	$\bar{4}$
$\bar{2}$	$\bar{2}$	$\bar{4}$	$\bar{1}$	$\bar{3}$
$\bar{3}$	$\bar{3}$	$\bar{1}$	$\bar{4}$	$\bar{2}$
$\bar{4}$	$\bar{4}$	$\bar{3}$	$\bar{2}$	$\bar{1}$

9. **Permutációcsoportok**

Egy H halmazt önmagára vivő bijektív leképezéseket *permutációknak* nevezzük. Ha a H halmaznak n darab eleme van, akkor $n!$ darab különböző bijektív leképezés viszi önmagára, vagyis n elem permutációinak száma $n!$. Ha például $H = \{1, 2, 3\}$, akkor a hat bijektív leképezés:

1. $1 \to 1$, $2 \to 2$, $3 \to 3$
2. $1 \to 1$, $2 \to 3$, $3 \to 2$
3. $1 \to 2$, $2 \to 1$, $3 \to 3$
4. $1 \to 2$, $2 \to 3$, $3 \to 1$
5. $1 \to 3$, $2 \to 1$, $3 \to 2$
6. $1 \to 3$, $2 \to 2$, $3 \to 1$

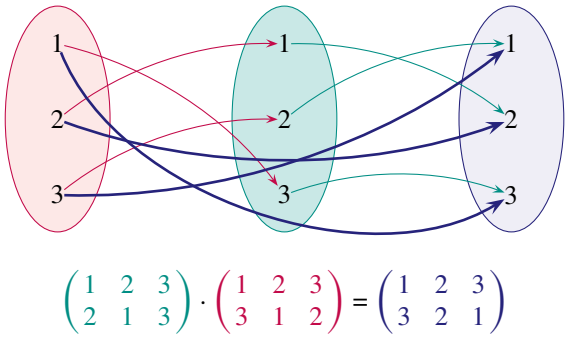
Szokásos jelöléssel:

$$\begin{pmatrix}1&2&3\\1&2&3\end{pmatrix},\begin{pmatrix}1&2&3\\1&3&2\end{pmatrix},\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix},\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix},\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix}.$$

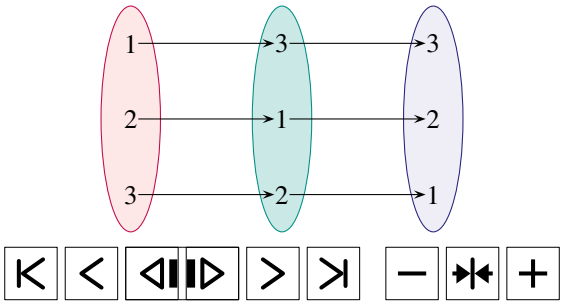
Egy n elemű halmaz összes permutációi csoportot alkotnak a leképezések szorzására nézve, ugyanis bijektív leképezések szorzata is bijektív; a leképezések szorzása asszociatív; egységelem az identikus leképezés, ami szintén bijektív; a bijektív leképezések invertálhatóak, és inverzük is bijektív.

Például: (Vigyázzunk! A permutációk – mivel maguk is leképezések – szorzásakor először, azaz balról a külső hozzárendelést írjuk le, utána, tehát jobbról a belsőt. Gondoljunk az $(f\cdot g)(x)=f(g(x))$ írásmódra!)

$$\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}\cdot\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}=\begin{pmatrix}1&2&3\\3&2&1\end{pmatrix},$$
$$\begin{pmatrix}1&2&3\\2&3&1\end{pmatrix}^{-1}=\begin{pmatrix}1&2&3\\3&1&2\end{pmatrix}.$$



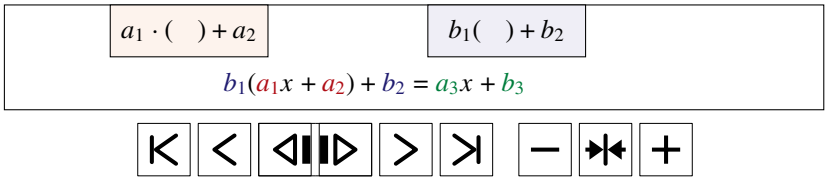
4.3. ábra.



4.4. ábra.

Az n elem összes permutációinak csoportját n-ed rendű *szimmetrikus csoportnak* nevezik, és S_n-nel jelölik. Az $n = 2$ esetet kivéve S_n sosem kommutatív. S_n-nek azokat a részhalmazait, amelyek önmagukban is csoportot alkotnak a leképezések szorzására, szokás *permutációcsoportoknak* nevezni. Jelölése: P_n.

10. Tekintsük a valós számokon értelmezett (nem konstans) lineáris függvények halmazát. Ez a halmaz (nem kommutatív) csoportot alkot a függvények összetételére nézve. (Lináris függvények kompozíciója is lineáris függvény; a leképezések szorzása asszociatív; egységelem az $x \mapsto x$ függvény, a lináris függvények bijektívek, így invertálhatóak, és inverzük is lineáris.)



4.5. ábra.

11. Értelmezzük az egész számok halmazán a következő műveletet:

$$a \circ b := \begin{cases} a + b, & \text{ha } a \text{ páros} \\ a - b, & \text{ha } a \text{ páratlan} \end{cases} \quad \text{(2.4. ábra)}$$

Könnyen belátható, hogy ez a $\circ$ művelet asszociatív; egységelem a 0; minden páros szám inverze az ellentettje, minden páratlan szám inverze önmaga. Vagyis $(\mathbb{Z}, \circ)$ csoport, amely például $2 \circ 3 = 5$ de $3 \circ 2 = 1$ miatt nem kommutatív.

4.2. Definíció. Egy $(G, \circ)$ *csoport rendjén* a G halmaz $|G|$ számosságát értjük. Ha G véges halmaz, akkor véges (rendű), ha G végtelen halmaz, akkor végtelen (rendű) csoportról beszélünk.

Fenti példáink közül az 1., 3., 4., 5., 6., 10. és 11. csoportok végtelen rendűek. Egy geometriai alakzat szimmetriacsoportjának rendje megegyezik azoknak a különböző egybevágósági transzformációknak a számával, amelyek az alakzatot önmagára viszik. Ez a rend lehet végtelen is (például kör vagy egyenes esetén), véges is (például a téglalap esetén 4). A szabályos n-szög diédercsoportjának rendje $|D_n| = 2n$. A mod m maradékosztályok összeadási csoportjának rendje m, a mod m redukált maradékosztályok szorzási csoportjának rendje $\varphi(m)$. Az S_n szimmetrikus csoport rendje $n!$.

Részcsoport

4.3. Definíció. A $(G, \circ)$ csoport *részcsoportjának* nevezzük a $(G^*, \circ)$ struktúrát, ha $G^* \subseteq G$ és $(G^*, \circ)$ maga is csoport. Jelölése: $G^* \leq G$ vagy $G \geq G^*$.

Például:

1. $(\mathbb{Z}, +)$-nak részcsoportja a páros számok halmaza (vagy egy tetszőleges egész összes többszöröseinek halmaza) az összeadásra nézve.
2. $(\mathbb{Q}^+, \cdot)$-nak részcsoportja például a 2^k alakú racionális számok halmaza, ahol k egész szám.
3. A test feletti polinomok összeadási csoportjának részcsoportja például a legfeljebb másodfokú polinomok halmaza.
4. Az $n \times n$-es mátrixok összeadási csoportjában részcsoportot alkotnak azok a mátrixox, amelyekben például az első sor első eleme 0.
5. Egy szabályos n-szög szimmetriacsoportjában például részcsoportot alkotnak a forgatások (beleértve a 0 fokos forgatást).
6. $(\mathbb{Z}_6, +)$-ban részcsoportot alkotnak például a páros maradékosztályok.
7. S_3-ban részcsoportot alkot például a következő három permutáció:
$$\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$$
8. A valós számokon értelmezett lineáris függvények függvénykompozíciós csoportjában részcsoportot alkotnak például azok az $x \mapsto ax + b$ alakú függvények, ahol a és b racionális ($a \neq 0$).
9. A csoportokra írt 11. példa $(\mathbb{Z}, \circ)$ csoportjában részcsoportot alkotnak a páros számok, vagy egy tetszőleges páros szám összes többszörösei. Szintén részcsoport például a $\{0, 3\}$ halmaz.

Ahhoz, hogy egy csoport egy részhalmázáról eldöntsük, hogy részcsoporte, elegendő azt ellenőriznünk, hogy benne van-e az egységelem, és hogy zárt-e a műveletre és az inverzképzésre nézve.

4.1. Tétel. *Legyen G^* nem üres részhalmaza G-nek, és $(G, \circ)$ csoport. Ekkor $(G^*, \circ)$ akkor és csak akkor részcsoportja $(G, \circ)$-nek, ha $\forall a, b \in G^*$-ra $a \circ b^{-1}$ is eleme G^*-nak.*

Bizonyítás.

1. Ha $(G^*, \circ)$ részcsoportja $(G, \circ)$-nek, akkor önmagában is csoport, így G^* tetszőleges b elemének b^{-1} inverze is benne van G^*-ban, és tetszőleges két elemén elvégzett művelet eredménye – vagyis $a \circ b^{-1}$ is – eleme G^*-nak.

2. Mivel $(G, \circ)$ csoport, a $\circ$ művelet asszociatív és invertálható, csak azt kell igazolnunk, hogy G^* zárt a műveletre és az inverzképzésre. Ha $\forall a, b \in$ $\in G^*$-ra $a \circ b^{-1}$ is eleme G^*-nak, akkor tetszőleges $a \in G^*$-ra $a \circ a^{-1} = e$, vagyis az egységelem is, továbbá $e \circ a^{-1} = a^{-1}$, vagyis egy tetszőleges elem inverze is eleme G^*-nak, így a művelet invertálható. Ez azt jelenti, hogy $\forall a, b \in G^*$-ra a, b^{-1} is eleme G^*-nak, így $a \circ (b^{-1})^{-1} = a \circ b$ is, vagyis G^* zárt a műveletre. □

Megjegyzés. A bizonyítás második felét visszafelé gondolkodva is elvégezhetjük.

Azt szeretnénk bizonyítani, hogy tetszőleges $a, b \in G^*$ elemekre $a \circ b$ is benne van G^*-ban.

Mivel mi csak $g_1 \circ g_2^{-1}$ típusú elemre tudunk következtetni, azt kell belátnunk, hogy $a \circ (b^{-1})^{-1} \in G^*$, vagyis hogy b^{-1} is benne van G^*-ban.

Az a feladat, hogy bebizonyítsuk, hogy ha $b \in G^*$, akkor $b^{-1} \in G^*$. Vagyis b^{-1}-t $g_1 \circ g_2^{-1}$ alakban kell felírnunk. Ezt így lehet: $b^{-1} = e \circ b^{-1}$.

Most már csak azt kellene látnunk, hogy e is benne van G^*-ban. Eszerint e-t $g_1 \circ g_2^{-1}$ alakban kell felírnunk: $g_1 \circ g_1^{-1}$, ahol $g_1 \in G^*$. Mivel G^* nem üreshalmaz, biztosan van eleme, legyen ez a g_1.

Vagyis beláttuk, hogy tetszőleges $a, b \in G^*$ elemekre b^{-1}, e is benne van G^*-ban, így $a \circ \left[\left(a \circ a^{-1}\right) \circ b^{-1}\right] = a \circ b$ is.

A komplexusszorzás segítségével a következőképpen is megfogalmazhatjuk annak szükséges és elégséges feltételét, hogy egy részhalmaz részcsoport legyen:

4.4. Definíció. Legyen $K \subseteq G$ a $(G, \circ)$ csoport egy komplexusa. A K *komplexus inverzén* a $K^{-1} := \{k^{-1} \mid k \in G\}$ komplexust értjük.

4.2. Tétel. *A $(G, \circ)$ csoport egy K komplexusa akkor és csak akkor részcsoport, ha $K \circ K^{-1} \subseteq K$.*

Bizonyítás. A tétel az előző tétel átfogalmazása, az, hogy $K \circ K^{-1} \subseteq K$, éppen azt jelenti, hogy $a, b \in K$-ra $a \circ b^{-1}$ is eleme K-nak. □

4.3. Tétel. *Egy csoport valahány részcsoportjának metszete is részcsoport.*

Bizonyítás. Legyen $(G_1, \circ)$ és $(G_2, \circ)$ a $(G, \circ)$ csoport két részcsoportja. Azt, hogy $(G_1 \cap G_2, \circ)$ félcsoport, már a 3.7. Tételben bizonyítottuk. Azt kell még megmutatnunk, hogy a metszet zárt az inverzképzésre. Mivel $(G_1, \circ)$ is és $(G_2, \circ)$ is részcsoport, mindkettő, ezért metszetük is tartalmazza $(G, \circ)$ egységelemét. Ugyanígy, a közös rész elemeinek inverze benne van G_1-ben is és G_2-ben is, így azok metszetében is. Vagyis a művelet a metszeten is invertálható. (Kettőnél több részcsoport esetén ugyanígy gondolható meg, hogy azok metszete is részcsoport.) □

4.5. Definíció. A $(G, \circ)$ csoport egy eleme vagy egy komplexusa által *generált részcsoportján* a legszűkebb olyan részcsoportját értjük, amely tartalmazza az illető elemet, illetve komplexust.

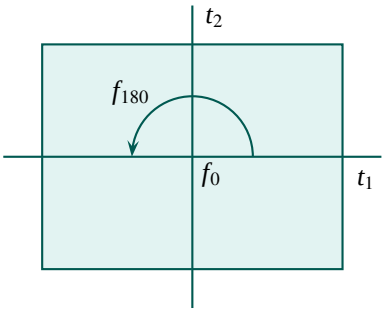
Megjegyzés. Olyan részcsoport, amely az adott komplexust tartalmazza, mindig létezik, ha más nem, akkor a teljes csoport. Ha több ilyen is létezik, akkor nyilvánvalóan az összes ilyen metszete lesz a legszűkebb, így egy komplexus által generált részcsoport mindig egyértelmű. (Az elemet felfoghatjuk egyelemű komplexusnak.)

4.6. Definíció. Az olyan részcsoportokat, amelyeket egyetlen elem generál, *ciklikus részcsoportnak* nevezzük. Ha a csoportnak van olyan eleme, amely a teljes csoportot generálja, akkor a csoportot *ciklikus csoportnak* nevezzük.

Például:

1. $(\mathbb{Z}, +)$-ban az a szám által generált ciklikus részcsoport az a szám összes többszöröseinek halmaza lesz. Általában az $\{a, b, c, \ldots\}$ komplexus által generált részcsoport az $a, b, c, \ldots$ elemek legnagyobb közös osztójának összes többszöröseiből álló halmaz lesz, amely szintén felfogható egyetlen elem – a legnagyobb közös osztó – által generált részcsoportnak, így szintén ciklikus.

2. A nem négyzet téglalap szimmetriacsoportjában e a csak önmagát tartalmazó egyelemű részcsoportot generálja; f_{180} az $\{e, f_{180}\}$ kételemű részcsoportot generálja, t_1, illetve t_2 pedig az $\{e, t_1\}$, illetve $\{e, t_2\}$ kételemű részcsoportot generálja. Ha egy komplexus tartalmazza mindkét tengelyes tükrözést, vagy az egyik tengelyes tükrözést és a 180°-os forgatást, akkor az általa generált részcsoport maga a teljes csoport lesz.



4.6. ábra.

3. $(\mathbb{Z}_6, +)$-ban

a 0 maradékosztálya	a $\{\overline{0}\}$ részcsoportot,
az 1 maradékosztálya	a teljes csoportot,
a 2 maradékosztálya	a $\{\overline{0}, \overline{2}, \overline{4}\}$ részcsoportot,
a 3 maradékosztálya	a $\{\overline{0}, \overline{3}\}$ részcsoportot,
a 4 maradékosztálya	a $\{\overline{0}, \overline{2}, \overline{4}\}$ részcsoportot,
az 5 maradékosztálya	a teljes csoportot generálja.

4. A csoportokra említett 11. példa $(\mathbb{Z}, \circ)$ csoportjában a 0 a csak őt tartalmazó egyelemű részcsoportot generálja, tetszőleges páros szám az ő összes többszöröseiből álló részcsoportot, tetszőleges k páratlan szám pedig a $\{0, k\}$ kételemű részcsoportot generálja.

Általában ha egy csoportban az a elem által generált részcsoportra vagyunk kíváncsiak, akkor ennek a részcsoportnak tartalmaznia kell az a elemet, a művelet zártsága miatt az $a \circ a = a^2$ elemet, emiatt és a művelet zártsága miatt az $a^2 \circ a = a^3$ elemet is és így tovább, az összes a^n alakú elemet (n pozitív egész). Tartalmaznia kell továbbá az egységelemet, és az összes elem inverzét, vagyis az összes a^{-k} alakú elemet, ahol k egész szám.

Véges csoportban (ahol az alaphalmaznak véges sok eleme van) az a elem pozitív egész kitevős hatványai csak véges sokféle értéket vehetnek fel (hiszen a művelet zártsága miatt minden hatvány benne van a csoportban, de a csoportnak csak véges sok eleme van), és megfigyelhetjük, hogy ezek között szerepel az egységelem is, és minden felvett érték inverze is.

Például: S_3-ban az $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ permutáció hatványai:

$$a^2 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix},$$

$$a^3 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = e$$

Látható, hogy innen kezdve nem kapunk újabb elemeket, $a^3 = e$ miatt $a^4 = a$, így $a^5 = a^2$, $a^6 = a^3 = e$ stb. Azt is észrevehetjük, hogy az a elem inverze éppen az a^2 elem (és viszont), így az a elem által generált részcsoport a fenti három elemből áll.

4.4. Tétel. *Véges csoportban tetszőleges elemnek van olyan pozitív egész kitevős hatványa, amely egyenlő az egységelemmel.*

Bizonyítás. Legyen $(G, \circ)$ egy véges csoport, a pedig egy tetszőleges eleme G-nek. Tekintsük az a, a^2, a^3, a^4, ... elemeket. Mivel a művelet zártsága miatt mindegyikük eleme a csoportnak, aminek viszont csak véges sok eleme van, előbb-utóbb eljutunk egy olyan hatványig, ami már szerepelt. Tegyük fel, hogy a, a^2, a^3, ..., a^{k-1} mind különbözőek, a^k az első olyan, amely megegyezik valamelyik korábbival, mondjuk a^l-nel ($l < k$). Ha viszont $a^k = a^l$, akkor az egyenlőség mindkét oldalát l-szer megszorozva a inverzével azt kapjuk, hogy $a^{k-l} = e$, ahol $l < k$ miatt $0 < k - l < k$. Vagyis van olyan pozitív egész n, amelyre $a^n = e$. □

Megjegyzés. Azt is könnyű belátni, hogy amennyiben a^k az első olyan hatványa a-nak, amely megegyezik valamelyik korábbival, akkor a bizonyítás jelöléseit használva $l = 1$ és $n = k - 1$, vagyis az első megismétlődő elem maga az a lesz, és a megismétlődését közvetlenül megelőző elem az egységelem. Ez azon múlik, hogy ha $a^n = e$, akkor $a^{n+1} = a$, de a már biztosan szerepelt a felsorolásban, így ha n kisebb lenne $k - 1$-nél, akkor már a^k előtt lett volna ismétlődés.

4.7. Definíció. Legyen a egy csoport eleme. Azt a legkisebb pozitív egész n kitevőt, amelyre $a^n = e$, az a *elem rendjének* nevezzük, és $o(a)$-val (ordó = rend) jelöljük. Amennyiben nincs ilyen kitevő, azt mondjuk, hogy az elem rendje végtelen.

A 4.4. Tétel szerint véges csoportban minden elem rendje véges.

4.5. Tétel. *Véges csoportban egy tetszőleges a elem összes pozitív egész kitevős hatványainak halmaza a csoportbeli műveletre nézve részcsoportot alkot.*

Bizonyítás. Az a elem hatványainak halmaza nyilván zárt a műveletre nézve, hiszen a két hatványának „szorzata” (a „szorzat” most a csoportbeli művelet eredményét jelenti) is a hatványa. Azt kell megmutatnunk, hogy az inverzképzésre is zárt.

Véges csoportban minden elem rendje véges, így van olyan (pozitív egész) n, amelyre $a^n = e$, vagyis a hatványai között szerepel az egységelem.

Ugyanakkor, mivel $a \circ a^{n-1} = a^n = e$, az a elem inverze $a^{-1} = a^{n-1}$, ami szintén szerepel a hatványai között. Mivel a tetszőleges hatványának inverze megegyezik a inverzének megfelelő hatványával, a összes hatványának inverze is a hatványa lesz. □

Megjegyzés. Ha egy csoportban az a elem rendje véges, mondjuk n, akkor $a^n = e$ miatt a minden hatványa meg fog egyezni az

$$e, a, a^2, a^3, \ldots, a^{n-1}$$

elemek valamelyikével. Mivel ezek az elemek mind különbözőek (mert különben az a rendje kisebb lenne n-nél), az a elem egy éppen $o(a) = n$ elemből álló részcsoportot generál, vagyis véges csoportban minden elem rendje megegyezik az általa generált részcsoport rendjével.

Ciklikus (rész)csoportokkal kapcsolatban számos további észrevételt tehetünk, könnyen beláthatók például a következő állítások:

- Ciklikus csoportok mindig kommutatívak.
- Ha van a csoportban olyan elem, melynek rendje megegyezik a csoport rendjével, akkor a csoport ciklikus.
- Ha egy csoportnak nincs valódi (triviálistól különböző) részcsoportja, akkor az prímszám rendű ciklikus csoport.

Csoportok izomorfiája

Gyakran tapasztalhatjuk – például amikor egy adott számhoz keresünk olyan csoportokat, amelyeknek az adott szám a rendje –, hogy látszólag teljesen különböző csoportok nagyon hasonlóan viselkednek, azonos szerkezetűek.

Vizsgáljunk meg például néhány másodrendű (kételemű) csoportot:

- A paralelogramma szimmetriacsoportjának elemei f_0 (helyben hagyás) és f_{180} (180 fokos forgatás, más néven középpontos tükrözés), a művelettáblázata a következő:

$\cdot$	f_0	f_{180}
f_0	f_0	f_{180}
f_{180}	f_{180}	f_0

- $(\mathbb{Z}_2, +)$ elemei a $\bar{0}$ és az $\bar{1}$ maradékosztályok, művelettáblázata a következő:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

– $(\mathbb{Z}_3 \setminus \bar{0}, \cdot)$ elemei az $\bar{1}$ és $\bar{2}$ maradékosztályok, művelettáblázata a következő:

$\cdot$	$\bar{1}$	$\bar{2}$
$\bar{1}$	$\bar{1}$	$\bar{2}$
$\bar{2}$	$\bar{2}$	$\bar{1}$

– Az S_2 szimmetrikus csoport elemei: $\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$ és $\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$, a művelettáblázat a következő:

$\cdot$	$\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$
$\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$
$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ 2 & 1\end{pmatrix}$	$\begin{pmatrix}1 & 2\\ 1 & 2\end{pmatrix}$

Látható, hogy a fenti csoportok bizonyos értelemben teljesen egyformák, a két elem közül az egyik (e) egységelem, a másik (a) pedig egy másodrendű elem, művelettáblázata pedig mindegyiknek a következő alakú:

$\circ$	e	a
e	e	a
a	a	e

Könnyen belátható az is, hogy egy tetszőleges kételemű csoport egységelemét e-vel, a másik elemét pedig a-val jelölve mindig ilyen alakú lesz a művelettáblázat, hiszen abból, hogy e egységelem (aminek egy csoportban lennie kell), következik, hogy $e \circ e = e$ és $e \circ a = a \circ e = a$; az inverz egyértelműségéből pedig következik, hogy a művelettáblázat semelyik sorában vagy oszlopában nem szerepelhet ugyanaz az elem kétszer, így $a \circ a$ csak e lehet. Vagyis minden kételemű csoport egyforma.

Vizsgáljuk meg most a háromelemű csoportokat. Egyik elemük az egységelem, a másik kettőt jelöljük a-val, illetve b-vel. A művelettáblázatának egységelemhez tartozó sorát és oszlopát csak így tölthetjük ki:

$\circ$	e	a	b
e	e	a	b
a	a		
b	b		

Ezekután $a \circ a$ már a nem lehet (mert $a \circ e = a \circ a$-ból következne $e = a$, de mi feltettük, hogy e, a és b három különböző elem), így a második sor második eleme vagy e, vagy b:

$\circ$	e	a	b
e	e	a	b
a	a	e	
b	b		

$\circ$	e	a	b
e	e	a	b
a	a	b	
b	b		

Figyelembe véve, hogy a művelettáblázat egy sorában vagy oszlopában sem szerepelhet ugyanaz az elem kétszer, az első táblázatot nem tudjuk jól folytatni, (tehát $a \circ a$ nem lehet e), a másodikból pedig a következőt kapjuk:

$\circ$	e	a	b
e	e	a	b
a	a	b	e
b	b	e	a

,

vagyis háromelemű csoport is csak egyféle lehet.

Könnyen ellenőrízhető, hogy ha például a következő háromelemű csoportok elemeinek az alábbi módon feleltetjük meg az e, a, b elnevezéseket, akkor művelettáblázatuk a fenti alakot ölti:

- A szabályos háromszög szimmetriacsoportjából a forgatások részcsoportjában $e = f_0$, $a = f_{120}$, $b = f_{240}$.
- $(\mathbb{Z}_3, +)$-ban $e = \overline{0}$, $a = \overline{1}$, $b = \overline{2}$.
- S_3-nak az $a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, elem által generált részcsoportjában

$$e = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \qquad a = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \qquad b = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Észrevehető az is hogy $a^2 = b$ és $a^3 = e$, így az összes háromelemű csoport ciklikus. (Hasonlóan, $b^2 = a$ és $b^3 = e$, így akár az a, akár a b elem generálja.)

Azt, hogy általában mikor tekinthető két csoport „egyformának”, tükrözi a következő definíció:

4.8. Definíció. Azt mondjuk, hogy a $(G_1, \circ)$ és a $(G_2, *)$ csoportok *izomorfak*, ha létezik olyan $f\colon G_1 \to G_2$ bijektív leképezés, amelyre tetszőleges $a, b \in G_1$ elemek esetén $f(a \circ b) = f(a) * f(b)$. (Vagyis a két csoport között létezik kölcsönösen egyértelmű, művelettartó leképezés.) Jelölése: $(G_1, \circ) \cong (G_2, *)$ vagy $(G_1, \circ) \simeq (G_2, *)$.

Fenti példáink alapján elmondhatjuk, hogy az összes másodrendű csoport izomorf egymással, és az összes harmadrendű csoport is izomorf egymással. Az is könnyen belátható, hogy az összes n-ed rendű ciklikus csoport izomorf egymással.

Azt is mondhatjuk, hogy az egymással izomorf csoportok csak abban különböznek egymástól, hogy az elemek és a művelet neve más az egyik csoportban, mint a másikban, az elemek és a művelet minden lényeges tulajdonsága ugyanaz – például az egyik csoport elemeinek rendje megegyezik a másik csoportban nekik megfelelő elemek rendjével, egy elem inverzének a képe megegyezik az elem képének inverzével, ha egy csoport kommutatív, akkor a vele izomorf csoport is az, ha az egyik ciklikus (amit egy g elem generál), akkor a másik is ciklikus lesz (amit a g képe generál) stb.

Például:

A negyedrendű csoportok közül $(\mathbb{Z}_4, +)$ izomorf $(\mathbb{Z}_5 \setminus \{\overline{0}\}, \cdot)$-ral:

$(\mathbb{Z}_4,+)$

$+$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{0}$
$\overline{2}$	$\overline{2}$	$\overline{3}$	$\overline{0}$	$\overline{1}$
$\overline{3}$	$\overline{3}$	$\overline{0}$	$\overline{1}$	$\overline{2}$

$\overline{0} \mapsto \overline{1}$
$\overline{1} \mapsto \overline{2}$
$\overline{2} \mapsto \overline{4}$
$\overline{3} \mapsto \overline{3}$

$(\mathbb{Z}_5\setminus\{\overline{0}\},\cdot)$

$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{3}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{3}$	$\overline{1}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{1}$	$\overline{2}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{2}$	$\overline{4}$

,

viszont ezek nem izomorfak például a téglalap szimmetriacsoportjával, hiszen abban az egységelemen kívül minden elem másodrendű (vagyis saját magának az inverze), így nem lehet ciklikus, míg a fenti csoportokban 2-2 negyedrendű elem is van, így ciklikusak.

A hatodrendű csoportok közül például a D_3 (a szabályos háromszög szimmetriacsoportja) izomorf az S_3 szimmetrikus csoporttal, de nem izomorf a $(\mathbb{Z}_6, +)$ maradékosztály csoporttal.

A permutációcsoportok érdekes tulajdonságára utal a következő tétel:

4.6. Tétel. (Cayley-tétel) *Tetszőleges (véges) n-ed rendű $(G, \circ)$ csoporthoz létezik S_n-nek olyan részcsoportja, amely izomorf a $(G, \circ)$ csoporttal.*

Bizonyítás. Jelöljük a csoport elemeit g_1, g_2, g_3, …, g_n-nel, és rendeljük hozzá a g_i elemhez a következő permutációt:

$$\begin{pmatrix} g_1 & g_2 & g_3 & \dots & g_n \\ g_i \circ g_1 & g_i \circ g_2 & g_i \circ g_3 & \dots & g_i \circ g_n \end{pmatrix},$$

amelyet röviden így jelölhetünk: $\begin{pmatrix} x \\ g_i \circ x \end{pmatrix}$.

Ez valóban permutáció lesz, hiszen ha a csoport minden elemét rendre „megszorozzuk” g_i-vel, akkor különböző elemeket „megszorozva” (az inverz egyértelműsége miatt) különböző eredményeket kapunk; az összes elemet „megszorozva” n különböző eredményt kapunk, amelyek a művelet zártsága miatt mind elemei a csoportnak, aminek viszont éppen n eleme van, vagyis minden eleme pontosan egyszer áll elő eredményként. (Más szavakkal: az $x \mapsto g_i \circ x$ leképezés bijektív.) Valójában azt a permutációt rendeltük hozzá a g_i elemhez, amely a csoport művelettáblázatában a „fejlécet” a g_i sorába viszi.

Azt fogjuk megmutatni, hogy hasonlóan hozzárendelve a G csoport minden eleméhez a G halmaz egy permutációját, a

$$g_i \mapsto \begin{pmatrix} x \\ g_i \circ x \end{pmatrix}$$

hozzárendelés művelettartó, vagyis a $g_a \circ g_b$ elemhez rendelt

$$\begin{pmatrix} x \\ (g_a \circ g_b) \circ x \end{pmatrix}$$

permutáció megegyezik a g_a elemhez rendelt

$$\begin{pmatrix} x \\ g_a \circ x \end{pmatrix}$$

permutációnak és a g_b elemhez rendelt

$$\begin{pmatrix} x \\ g_b \circ x \end{pmatrix}$$

permutációnak a szorzatával. Ez könnyen ellenőrizhető, a

$$\begin{pmatrix} x \\ g_b \circ x \end{pmatrix}$$

permutáció a csoport elemeit a g_b-szeresükbe viszi, a képekre alkalmazva a

$$\begin{pmatrix} x \\ g_a \circ x \end{pmatrix}$$

permutációt, azok a g_a-szorosukba kerülnek, így a két leképezés egymásutánja minden elemet a $g_a \circ g_b$-szeresébe visz. Vagyis:

$$\begin{pmatrix} x \\ g_a \circ x \end{pmatrix} \cdot \begin{pmatrix} x \\ g_b \circ x \end{pmatrix} = \begin{pmatrix} x \\ g_a \circ (g_b \circ x) \end{pmatrix} = \begin{pmatrix} x \\ (g_a \circ g_b) \circ x \end{pmatrix}.$$

Mivel a csoport különböző elemeihez nyilvánvalóan különböző permutációkat rendeltünk (csoport művelettáblázatának nem lehet két egyforma sora), ezzel sikerült bijektív, művelettartó leképezést létesítenünk a $(G, \circ)$ csoport elemei és a G halmazhoz tartozó P_n permutációcsoport egy részhalmaza között, ami azt jelenti, hogy a hozzárendelésben szereplő permutációk P_n-nek egy részcsoportját alkotják. Vagyis van olyan részcsoportja P_n-nek, amely izomorf G-vel. □

Például: $(\mathbb{Z}_5 \setminus \{\overline{0}\}, \cdot)$ esetén a következő permutációkat rendeljük az elemekhez:

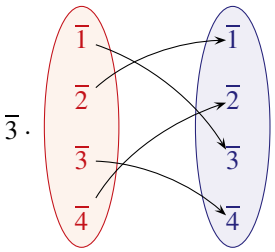
$\cdot$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

$$\overline{1} \mapsto \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{1} & \overline{2} & \overline{3} & \overline{4} \end{pmatrix}$$

$$\overline{2} \mapsto \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{2} & \overline{4} & \overline{1} & \overline{3} \end{pmatrix}$$

$$\overline{3} \mapsto \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{3} & \overline{1} & \overline{4} & \overline{2} \end{pmatrix}$$

$$\overline{4} \mapsto \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{4} & \overline{3} & \overline{2} & \overline{1} \end{pmatrix}$$



$$\overline{3} \mapsto \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{3}\cdot\overline{1} & \overline{3}\cdot\overline{2} & \overline{3}\cdot\overline{3} & \overline{3}\cdot\overline{4} \end{pmatrix} =$$

$$= \begin{pmatrix} \overline{1} & \overline{2} & \overline{3} & \overline{4} \\ \overline{3} & \overline{1} & \overline{4} & \overline{2} \end{pmatrix}$$

4.7. ábra.

Megjegyzés. Az S_n szimmetrikus csoport viselkedése teljesen független attól, hogy mik annak az n elemű halmaznak az elemei, amelynek az önmagára vivő bijektív leképezéseiről beszélünk. Amikor például az $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$ permutációról beszélünk, akkor ezt úgy képzeljük, hogy van egy háromelemű halmazunk, amelynek az elemeit sorba raktuk, vagyis az „első”, „második”,

illetve „harmadik” névvel láttuk el őket. Ez a permutáció azt a bijektív leképezést jelenti, amely az első elemet a harmadikba, a másodikat az elsőbe, a harmadikat pedig a másodikba viszi, függetlenül attól, hogy valójában mik voltak ezek az elemek. Ebben a jelölésben az elemeket a sorbarakás során kapott indexeikkel helyettesítjük. Amikor azonban valamilyen szempontból fontos, hogy mik voltak az alaphalmaz elemei, akkor a permutáció megadásakor magukat az elemeket és a képeiket írjuk fel. Ezt tettük a fenti példában. Úgy is elképzelhetjük, hogy minden n elemű halmaznak megvan a maga szimmetrikus csoportja, de ezek mind izomorfak.

Feladatok

1. Az $S = \{a, b, c\}$ halmazon értelmezzük a $\circ$ műveletet a következők szerint: tetszőleges $x, y \in S$ elemekre $x \circ y = x$. Mely csoporttulajdonságok teljesülnek $\circ$-re? Melyek nem?

2. Csoportot alkot-e az egész számok halmaza a $*$ műveletre, amelyet úgy értelmezünk, hogy $a * b = ab + a + b$.

3. Csoport-e? Ha nem, azt is mondja meg, miért nem!

   (a) $(\mathbb{N}, +)$ (b) $(\mathbb{N}, -)$ (c) $(\mathbb{N}, \cdot)$ (d) $(\mathbb{N}, /)$

   (e) $(\mathbb{Z}, +)$ (f) $(\mathbb{Z}, -)$ (g) $(\mathbb{Z}, \cdot)$ (h) $(\mathbb{Z}, /)$

   (i) $(\mathbb{Q}, +)$ (j) $(\mathbb{Q}, -)$ (k) $(\mathbb{Q} \setminus \{0\}, \cdot)$ (l) $(\mathbb{Q}, /)$

   (m) $(\mathbb{Z}_4, +_{\text{ mod } 4})$ (n) $(\mathbb{Z}_4, \cdot_{\text{ mod } 4})$

   (o) $(\mathbb{R}, +)$ (p) $(\mathbb{R} \setminus \{0\}, \cdot)$

   (q) $(\mathbb{C} \setminus \{0\}, \cdot)$ (r) $(\{z \mid z \in \mathbb{C}, |z| = 1\}, \cdot)$

   (s) $(\{z \mid z \in \mathbb{C}, z^p = 1, p \text{ prímszám}\}, \cdot)$

4. Csoport-e? Ha nem, azt is mondja meg, miért nem! (Ahol nem jelöltük másként, ott a $+$ és a $\cdot$ a szokásos műveleteket jelenti.)

   (a) $(\{0\}, \cdot)$ (b) $(\{0\}, +)$ (c) $(\{1\}, \cdot)$ (d) $(\{1\}, +)$

   (e) $(\{-1, 1\}, \cdot)$ (f) $(\{0, 1\}, +_{\text{ mod } 2})$

   (g) $(\{0, 1\}, \cdot_{\text{ mod } 2})$ (h) $(\{5k \mid k \in \mathbb{Z}\}, \cdot)$

   (i) $(\{\mathbb{Z}[x]\}, +)$ (egész együtthatós polinomok a polinomösszeadásra)

5. Igazolja, hogy ha egy *véges* félcsoportban érvényes a bal és jobb oldali egyszerűsítési szabály is (tetszőleges a, b, c félcsoportbeli elemekre $a \circ c = b \circ c$-ből és $c \circ a = c \circ b$-ből is következik, hogy $a = b$), akkor ez csoport!

   Miért nem igaz az állítás végtelen félcsoportban?

   Mondjon olyan végtelen (egységelemes) félcsoportot, ahol bár igaz mindkét oldali egyszerűsítési szabály, mégsem csoport.

6. Egy tetszőleges csoportban melyik egyenlet oldható meg az alábbiak közül (x jelöli az ismeretlent, minden más betű a csoport elemét jelöli)?

   (a) $ax = b$ (b) $xa = b$ (c) $ax = ab$

   (d) $a^2bx = b$ (e) $axb = c$ (f) $ax = xb$

7. Csoportot alkotnak-e az (a) egész, (b) racionális, (c) komplex együtthatós polinomok az összeadásra nézve?

8. Csoportot alkotnak-e a legfeljebb n-edfokú (a) egész, (b) racionális, (c) komplex együtthatós polinomok az összeadásra nézve?

9. Csoportot alkotnak-e a 2×2-es valós reguláris (invertálható) valós mátrixok a mátrixszorzásra nézve?

10. Csoportot alkotnak-e a síkvektorok a vektorösszeadásra nézve?

11. Csoportot alkotnak-e a síkvektorok a skaláris szorzásra nézve?

12. Csoportot alkotnak-e a térvektorok a vektoriális szorzásra nézve?

13. Csoportot alkotnak-e a térvektorok a skaláris szorzásra nézve?

14. Igazolja, hogy a szabályos hatszög egybevágósági transzformációi a transzformációszorzásra (D_6) csoportot alkotnak! Határozza meg, hogy az S_6 mely részcsoportjával izomorf D_6!

15. Igazolja, hogy a $\{5^n \mid n \in \mathbb{Z}\}$ halmaz a szokásos szorzásra nézve csoport!

    Kommutatív-e ez a csoport?

    Igaz-e, hogy izomorf a $(\mathbb{Z}, +)$ csoporttal!

16. Igazolja, hogy bármely két n elemű ciklikus csoport izomorf!

17. Igaz-e, hogy $(\{-1, 1\}, \cdot)$ és $(\{0, 1\}, +_{\bmod 2})$ izomorf csoportok?

18. Igaz-e, hogy bármely négyelemű csoport ciklikus? Igaz-e, hogy minden négyelemű csoport kommutatív? Igaz-e, hogy minden négyelemű csoport izomorf egymással? (Használhatja a www.cs.elte.hu/~kfried/algebra3/groups2-8.jar csoportkészítő programot. A piros betű az invertálhatóság, a narancssárga színezés az asszociativitás sérülésére utaló hibát jelez.)

19. Igazolja, hogy D_3 és S_3 izomorfak egymással! Van-e más k is, amelyre D_k és S_k izomorf csoportok?

20. Adja meg D_8 (a szabályos 8-szög szimmetriacsoportja) összes ciklikus részcsoportját!

21. A következőkben megadjuk egy csoport műveleti táblázatát – hiányosan. Fejezze be a kitöltést!

$*$	a	b	c	d	e	f	g	h
a			e		a	g		d
b			a		b			
c					c			
d		g	f		d			
e	a	b	c	d	e	f	g	h
f			g		f			
g			h	e	g			
h					h	e		b

(Használhatja a www.cs.elte.hu/~kfried/algebra3/groups2-8.jar csoportkészítő programot. A piros betű az invertálhatóság, a narancssárga színezés az asszociativitás sérülésére utaló hibát jelez.)

Határozza meg a kapott csoport részcsoportjait!

Hány eleme lehet egy 8 elemű csoport részcsoportjainak?

Van-e más 8 elemű csoport?

22. Igazolja, hogy egy G csoport tetszőleges a, b elemeire

    (a) a rendje egyenlő a $b^{-1}ab$ elem rendjével,

    (b) ab rendje egyenlő ba rendjével.

23. Igazolja, hogy ha egy n elemű csoportban van n-edrendű elem, akkor a csoport ciklikus!

24. Igazolja, hogy ha egy csoportban van $n_1 \cdot n_2$ rendű elem, akkor van n_1 rendű elem is.

25. Igazolja, hogy minden prímszám elemű csoport ciklikus. Van-e nem prímszám elemű ciklikus csoport?

26. Igazolja, hogy ha $G \subseteq \mathbb{R}$ halmaz a valós számok összeadására nézve csoportot alkot, akkor a $H = \{2^g \mid g \in G\}$ halmaz a szorzásra nézve csoportot alkot, és $(G, +) \equiv (H, \cdot)$!

    Igazolja, hogy ha $G \subseteq \mathbb{R}^+$ halmaz a valós számok szorzására nézve csoportot alkot, akkor a $H = \{\log_2 \mid g \in G\}$ halmaz az összeadásra nézve csoportot alkot, és $(G, +) \equiv (H, \cdot)$!

27. Igazolja, hogy a legfeljebb n-edfokú, valós együtthatós polinomok összeadásra vett csoportja izomorf az $(n + 1)$-dimenziós valós vektorok összeadásra vett csoportjával!

5. fejezet

Mellékosztályok, normálosztó

5.1. Definíció. Legyen a $(G, \circ)$ csoportnak $(H, \circ)$ egy részcsoportja. Egy tetszőleges $g \in G$ esetén a $(G, \circ)$ csoport g elemmel képzett H szerinti bal oldali *mellékosztályának* nevezzük a $g \circ h$ alakú elemek halmazát, ahol $h \in$ $\in H$. Jelölése: $g \circ H$. Hasonlóan, a g elemmel képzett H szerinti jobb oldali mellékosztály:

$$H \circ g = \{h \circ g \mid h \in H\}.$$

Megjegyzés. A $g \circ H$ mellékosztályt úgy is elképzelhetjük, mint az egyelemű $\{g\}$ halmaz és a H halmaz $\{g\} \circ H$ komplexusszorzatát. (Hasonlóan: $H \circ g = H \circ \{g\}$.)

Például:

1. $(\mathbb{Z}_6, +)$ részcsoportjai: $(A, +)$, ahol $A = \{\overline{0}\}$; $(B, +)$, ahol $B = \{\overline{0}, \overline{3}\}$; $(C, +)$, ahol $C = \{\overline{0}, \overline{2}, \overline{4}\}$; továbbá maga a teljes $(\mathbb{Z}_6, +)$ csoport, ahol

$$\mathbb{Z}_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}.$$

Az A szerinti

bal oldali mellékosztályok:	jobb oldali mellékosztályok:
$\overline{0} + A = \{\overline{0}\} = A$	$A + \overline{0} = \{\overline{0}\} = A$
$\overline{1} + A = \{\overline{1}\}$	$A + \overline{1} = \{\overline{1}\}$
$\overline{2} + A = \{\overline{2}\}$	$A + \overline{2} = \{\overline{2}\}$
$\overline{3} + A = \{\overline{3}\}$	$A + \overline{3} = \{\overline{3}\}$
$\overline{4} + A = \{\overline{4}\}$	$A + \overline{4} = \{\overline{4}\}$
$\overline{5} + A = \{\overline{5}\}$	$A + \overline{5} = \{\overline{5}\}$

A B szerinti

bal oldali mellékosztályok:	jobb oldali mellékosztályok:
$\bar{0}+B=\{\bar{0},\bar{3}\}=B$	$B+\bar{0}=\{\bar{0},\bar{3}\}=B$
$\bar{1}+B=\{\bar{1},\bar{4}\}$	$B+\bar{1}=\{\bar{1},\bar{4}\}$
$\bar{2}+B=\{\bar{2},\bar{5}\}$	$B+\bar{2}=\{\bar{2},\bar{5}\}$
$\bar{3}+B=\{\bar{3},\bar{0}\}=\bar{0}+B$	$B+\bar{3}=\{\bar{3},\bar{0}\}=B+\bar{0}$
$\bar{4}+B=\{\bar{4},\bar{1}\}=\bar{1}+B$	$B+\bar{4}=\{\bar{4},\bar{1}\}=B+\bar{1}$
$\bar{5}+B=\{\bar{5},\bar{2}\}=\bar{2}+B$	$B+\bar{5}=\{\bar{5},\bar{2}\}=B+\bar{2}$

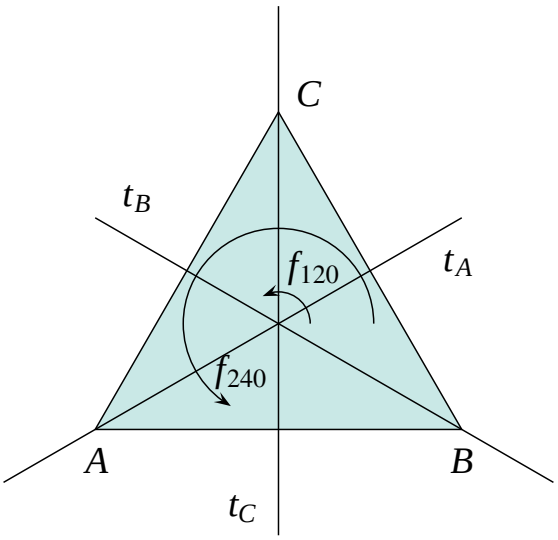
A C szerinti

bal oldali mellékosztályok:	jobb oldali mellékosztályok:
$\bar{0}+C=\{\bar{0},\bar{2},\bar{4}\}=C$	$C+\bar{0}=\{\bar{0},\bar{2},\bar{4}\}=C$
$\bar{1}+C=\{\bar{1},\bar{3},\bar{5}\}$	$C+\bar{1}=\{\bar{1},\bar{3},\bar{5}\}$
$\bar{2}+C=\bar{4}+C=C$	$C+\bar{2}=C+\bar{4}=C$
$\bar{3}+C=\bar{5}+C=\bar{1}+C$	$C+\bar{3}=C+\bar{5}=C+\bar{1}$

A teljes $\mathbb{Z}_6$ szerinti tetszőleges elemmel képzett, akár bal, akár jobb oldali mellékosztályok megegyeznek magával a teljes $\mathbb{Z}_6$-tal.

Ha a csoport nem kommutatív, akkor általában nem egyezik meg az ugyanavval az elemmel képzett bal, illetve jobb oldali mellékosztály. Erre példa a következő:

2. D_3-ban (a szabályos háromszög szimmetriacsoportjában) az elemek: f_0 (identikus leképezés), f_{120}, f_{240} (forgatások), továbbá t_A, t_B, t_C (az egyes csúcsokon átmenő tengelyekre vonatkozó tükrözések), a művelet pedig a leképezések szorzása (transzformációk egymásutánja).



5.1. ábra.

D_3 részcsoportjai:

$$H_1 = \{f_0\},$$
$$H_2 = \{f_0, f_{120}, f_{240}\},$$
$$H_3 = \{f_0, t_A\},$$
$$H_4 = \{f_0, t_B\},$$
$$H_5 = \{f_0, t_C\}$$
és maga a teljes $D_3 = \{f_0, f_{120}, f_{240}, t_A, t_B, t_C\}$ csoport.

A H_1 szerinti mellékosztályok: tetszőleges g elem esetén

$$g \cdot H_1 = \{g\} = H_1 \cdot g.$$

	f_0	f_{120}	f_{240}	t_A	t_B	t_C
f_0	f_0	f_{120}	f_{240}	t_A	t_B	t_C
f_{120}	f_{120}	f_{240}	f_0	t_C	t_A	t_B
f_{240}	f_{240}	f_0	f_{120}	t_B	t_C	t_A
t_A	t_A	t_B	t_C	f_0	f_{120}	f_{240}
t_B	t_B	t_C	t_A	f_{240}	f_0	f_{120}
t_C	t_C	t_A	t_B	f_{120}	f_{240}	f_0

5.1. táblázat.

A H_2 szerinti mellékosztályok:

$$f_0 \cdot H_2 = f_{120} \cdot H_2 = f_{240} \cdot H_2 = \{f_0, f_{120}, f_{240}\} = H_2 = H_2 \cdot f_0 = \\ = H_2 \cdot f_{120} = H_2 \cdot f_{240},$$
$$t_A \cdot H_2 = t_B \cdot H_2 = t_C \cdot H_2 = \{t_A, t_B, t_C\} = H_2 \cdot t_A = \\ = H_2 \cdot t_B = H_2 \cdot t_C.$$

A H_3 szerinti

bal oldali mellékosztályok:	jobb oldali mellékosztályok:
$f_0 \cdot H_3 = \{f_0, t_A\} = H_3$	$H_3 \cdot f_0 = \{f_0, t_A\} = H_3$
$f_{120} \cdot H_3 = \{f_{120}, t_C\}$	$H_3 \cdot f_{120} = \{f_{120}, t_B\}$
$f_{240} \cdot H_3 = \{f_{240}, t_B\}$	$H_3 \cdot f_{240} = \{f_{240}, t_C\}$
$t_A \cdot H_3 = \{t_A, f_0\} = H_3$	$H_3 \cdot t_A = \{t_A, f_0\} = H_3$
$t_B \cdot H_3 = \{t_B, f_{240}\} = f_{240} \cdot H_3$	$H_3 \cdot t_B = \{t_B, f_{120}\} = H_3 \cdot f_{120}$
$t_C \cdot H_3 = \{t_C, f_{120}\} = f_{120} \cdot H_3$	$H_3 \cdot t_C = \{t_C, f_{240}\} = H_3 \cdot f_{240}.$

A H_4 szerinti

bal oldali mellékosztályok:	jobb oldali mellékosztályok:
$f_0 \cdot H_4 = t_B \cdot H_4 = \{f_0, t_B\} = H_4$	$H_4 \cdot f_0 = H_4 \cdot t_B = \{f_0, t_B\} = H_4$
$f_{120} \cdot H_4 = t_A \cdot H_4 = \{f_{120}, t_A\}$	$H_4 \cdot f_{120} = H_4 \cdot t_C = \{f_{120}, t_C\}$
$f_{240} \cdot H_4 = t_C \cdot H_4 = \{f_{240}, t_C\}$	$H_4 \cdot f_{240} = H_4 \cdot t_A = \{f_{240}, t_A\}$

A H_5 szerinti

bal oldali mellékosztályok:	jobb oldali mellékosztályok:
$f_0 \cdot H_5 = t_C \cdot H_5 = \{f_0, t_C\} = H_5$	$H_5 \cdot f_0 = H_5 \cdot t_C = \{f_0, t_C\} = H_5$
$f_{120} \cdot H_5 = t_B \cdot H_5 = \{f_{120}, t_B\}$	$H_5 \cdot f_{120} = H_5 \cdot t_A = \{f_{120}, t_A\}$
$f_{240} \cdot H_5 = t_A \cdot H_5 = \{f_{240}, t_A\}$	$H_5 \cdot f_{240} = H_5 \cdot t_B = \{f_{240}, t_B\}$

A teljes D_3 szerinti tetszőleges elemmel készített akár bal, akár jobb oldali mellékosztályok megegyeznek magával D_3-mal.

Vizsgáljunk meg egy olyan csoportot is, amelynek végtelen a rendje:

3. $(\mathbb{Z}, +)$-ban például részcsoportot alkotnak a hárommal osztható számok:
$$H = \{3k \mid k \in \mathbb{Z}\}.$$

A H szerinti mellékosztályok:

$$\begin{aligned}
0 + H &= H = H + 0 \\
1 + H &= \{1 + 3k \mid k \in \mathbb{Z}\} = H + 1 \\
2 + H &= \{2 + 3k \mid k \in \mathbb{Z}\} = H + 2 \\
3 + H &= \{3 + 3k \mid k \in \mathbb{Z}\} = \{3k \mid k \in \mathbb{Z}\} = H \\
4 + H &= \{4 + 3k \mid k \in \mathbb{Z}\} = \{1 + 3k \mid k \in \mathbb{Z}\} = 1 + H \\
&\vdots
\end{aligned}$$

...	−10	−7	−4	−1	2	5	8	11	14	...
...	−11	−8	−5	−2	1	4	7	10	13	...
...	−12	−9	−6	−3	0	3	6	9	12	...

5.2. ábra. A modulo 3 maradékosztályok, a H szerinti mellékosztályok

Példáinkból leszűrhetünk néhány általánosabb észrevételt egy tetszőleges $(G, \circ)$ csoport $(H, \circ)$ részcsoportja szerinti mellékosztályaival kapcsolatban:

5.1. Állítás. *Tetszőleges $h \in H$ elem esetén a $h \circ H$, illetve $H \circ h$ mellékosztály megegyezik H-val.*

Bizonyítás. Egyrészt mivel H részcsoport, tetszőleges két elemének, így h-nak és egy tetszőleges elemének „szorzata” is benne van H-ban. Másrészt az inverz egyértelműsége miatt ha különböző elemeit „szorozzuk” h-val, akkor az eredmények is különbözőek lesznek. Az is igaz, hogy H egy tetszőleges h^* eleme előáll h és egy H-beli elem szorzataként, ugyanis H részcsoport, így h^{-1}, valamint $h^{-1} \circ h^*$ is eleme H-nak, és $h^* = h \circ (h^{-1} \circ h^*)$. Vagyis a $h_i \to h \circ h_i$ a H halmazt bijektíven képezi le önmagára. □

5.2. Állítás. *Tetszőleges $g \in G$ elem esetén a $g \circ H$, illetve $H \circ g$ mellékosztály számossága megegyezik a H számosságával.*

Bizonyítás. Az előzőekhez hasonlóan könnyen belátható, hogy a $h_i \to g \circ h_i$ bijektíven képezi le H-t $g \circ H$-ra. □

5.3. Állítás. *Tetszőleges $g \in G$ elem esetén a $g \circ H$, illetve $H \circ g$ mellékosztálynak eleme lesz a g elem.*

Bizonyítás. Mivel H részcsoport, benne van a csoport e egységeleme, így a $g \circ H$ mellékosztálynak eleme lesz a $g \circ e = g$, a $H \circ g$ mellékosztálynak pedig az $e \circ g = g$ elem. □

5.4. Állítás. *Tetszőleges $a, b \in G$ esetén az $a \circ H$ és $b \circ H$ mellékosztályok vagy egybeesnek, vagy diszjunktak, és hasonlóan, a $H \circ a$ és $H \circ b$ mellékosztályok is vagy azonosak, vagy diszjunktak.*

Bizonyítás. Tegyük fel, hogy az $a \circ H$ mellékosztály egy $a \circ h_1$ eleme egyben a $b \circ H$ mellékosztálynak is eleme. Ez azt jelenti, hogy ez az elem felírható $b \circ h_2$ alakban is, ahol $h_2 \in H$, vagyis

$$a \circ h_1 = b \circ h_2.$$

Ekkor mindkét oldalt jobbról „szorozva” h_1 inverzével, azt kapjuk, hogy

$$a = (b \circ h_2) \circ h_1^{-1}.$$

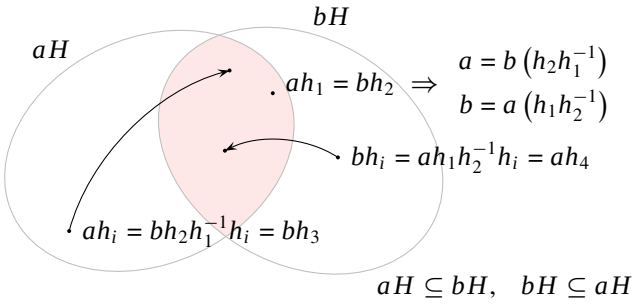
Ezt felhasználva az $a \circ H$ mellékosztály tetszőleges $a \circ h_i$ elemét

$$a \circ h_i = \left((b \circ h_2) \circ h_1^{-1}\right) \circ h_i = b \circ (h_2 \circ h_1^{-1} \circ h_i)$$

alakban írhatjuk fel. Mivel $h_1, h_2, h_i \in H$ és H részcsoport, h_1^{-1} és

$$h_k = h_2 \circ h_1^{-1} \circ h_i$$

is eleme H-nak, vagyis az $a \circ H$ mellékosztály minden eleme előáll $b \circ h_k$ alakban, így az $a \circ H$ mellékosztály minden eleme eleme a $b \circ H$ mellékosztálynak is. Tehát $a \circ H \subseteq b \circ H$. Hasonlóan bizonyítható, hogy $b \circ H \subseteq a \circ H$, amiből következik, hogy $a \circ H = b \circ H$. A jobb oldali mellékosztályokra is ugyanígy igazolható az állítás. □



5.3. ábra. Ha két mellékosztály nem diszjunkt, akkor azonosak

A fenti állítások alapján kimondhatjuk a következő tételeket:

5.1. Tétel. *A $(G, \circ)$ csoport $(H, \circ)$ részcsoportja szerinti összes – mondjuk bal oldali – mellékosztály megadja G-nek egy osztályozását. (Hasonló állítás teljesül a jobb oldali mellékosztályokra is.)*

Bizonyítás. Azt kell megmutatnunk, hogy a H szerinti (bal oldali) mellékosztályok olyan halmazrendszert alkotnak, amelynek uniója éppen a G halmaz, és amelyben a halmazok páronként diszjunktak és egyikük sem üres.

Az, hogy a mellékosztályok uniója a G, vagyis G minden eleme benne van valamelyik mellékosztályban, a 3. állításból; az pedig, hogy két különböző maradékosztály nem tartalmazhat közös elemet, a 4. állításból következik. Az, hogy egyik mellékosztály sem üres, akár a 2., akár a 3. állításból következik. □

5.2. Tétel. (Lagrange-tétel) *Legyen $(G, \circ)$ egy véges csoport, amelynek $(H, \circ)$ egy tetszőleges részcsoportja. Ekkor $|H| \mid |G|$ (vagyis véges csoport tetszőleges részcsoportjának rendje osztója a csoport rendjének).*

Bizonyítás. A 5.1. Tételből tudjuk, hogy a H szerinti (mondjuk bal oldali) mellékosztályok elkészítésekor közös részt nem tartalmazó részhalmazokra osztjuk fel a G halmazt. A 2. állítás szerint a létrejövő osztályok mindegyikének megegyezik a számossága $|H|$-val, így számosságuk egymáséval is megegyezik, ami véges halmazok esetén azt jelenti, hogy ugyanannyi elemük van. Vagyis a csoport elemeit egyenlő létszámú osztályokba soroltuk be. Ha a létrejövő különböző mellékosztályok száma k, és minden osztályban $|H|$ darab elem van, akkor, mivel minden elem pontosan egy osztályban szerepel, $k \cdot |H| = |G|$, ahol k egész szám, vagyis $|H| \mid |G|$. □

Megjegyzés. A 5.1. és 5.2. Tétel bizonyításának lényegi része az 1–4. állítások indoklásában rejlik.

Megjegyzés. Tetszőleges G véges csoportban, ha a H részcsoport szerinti jobb oldali mellékosztályokat készítjük el, akkor – mivel ezek számossága is megegyezik H-éval – a csoport elemeit ugyanolyan létszámú osztályokba soroljuk be, mint a bal oldali mellékosztályok esetén. Emiatt – mivel a jobb oldali mellékosztályok uniója is G – ugyanannyi különböző jobb oldali mellékosztályt kapunk, mint bal oldalit. Az tehát, hogy a H szerinti osztályozás során hány mellékosztály lesz, független attól, hogy jobb vagy bal oldali mellékosztályokról beszélünk. (Bár a fentiek során kihasználtuk, hogy véges csoportról van szó, meggondolható, hogy ha H egy végtelen csoport részcsoportja, akkor is igaz, hogy H szerint osztályozva a csoport elemeit, ugyanannyi bal oldali mellékosztályt kapunk, mint jobb oldalit.)

A H szerinti különböző bal oldali – vagy különböző jobb oldali – mellékosztályok darabszámát szokás a H *részcsoport G-re vonatkozó indexének* nevezni, és $|G : H|$-val jelölni. Ennek segítségével így is felírható a Lagrange-tétel:

$$|G| = |H| \cdot |G : H|.$$

Következmény. A 4.5. Tételt követően megjegyeztük, hogy egy elem rendje megegyezik az általa generált (ciklikus) részcsoport rendjével. Véges csoport esetén ez a rend egy pozitív egész szám, és a Lagrange-tétel miatt osztója a csoport rendjének, így véges csoportban egy tetszőleges elem rendje is osztója a csoport rendjének. Ennek alapján megállapíthatjuk például hogy minden prímrendű csoport ciklikus, így tetszőleges p prím esetén a p-edrendű csoportok izomorfak.

Normálosztó

Mint azt korábban láttuk, egy nem kommutatív csoportban az $a \circ H$ bal oldali mellékosztály néha megegyezik a $H \circ a$ jobb oldali mellékosztállyal, néha nem. Az, hogy a két halmaz egybeesik vagy nem, függ attól is, hogy a csoport melyik elemével képezzük a mellékosztályokat, attól is, hogy mely részcsoport szerinti mellékosztályokról beszélünk. Ha például $a \in H$, akkor $a \circ H = H \circ a (= H)$. Ha H triviális részcsoportja G-nek, akkor tetszőleges elem esetén egybeesik az illető elemmel képzett H szerinti bal oldali mellékosztály a jobb oldalival.

5.2. Definíció. A $(G, \circ)$ csoport egy $(H, \circ)$ részcsoportját *normálosztónak* (vagy *normális részcsoportnak*) nevezzük, ha tetszőleges $g \in G$ esetén $g \circ H = H \circ g$. Jelölése: $H \lhd G$.

Például:

1. Kommutatív csoportnak minden részcsoportja normálosztó.

2. Tetszőleges csoportban a triviális részcsoportok normálosztók.

   Bizonyítás. Ha ugyanis $H = \{e\}$, ahol $\{e\}$ a csoport egységeleme, akkor $\forall g$-re
   $$g \circ H = \{g\} = H \circ g;$$
   ha pedig $H = G$, akkor
   $$g \circ H = G = H \circ g. \square$$

3. Tetszőleges véges csoportban egy 2 rendű részcsoport normálosztó.

   Bizonyítás. Ha ugyanis H rendje fele a csoport rendjének, akkor két különböző – mondjuk bal oldali – mellékosztályt kapunk ($|G : H| = 2$), amelyek egyike maga a H, a másik pedig a H-ból kimaradó elemek halmaza. Ha egy $h \in H$ elemmel képezzük akár a bal, akár a jobb oldali mellékosztályt, akkor magát a H halmazt kapjuk, ha pedig egy H-n kívüli elemmel, akkor H-nak a G-re vonatkozó komplementerét, ami szintén független attól, hogy bal vagy jobb oldali mellékosztályról van-e szó. $\square$

4. A $(\mathbb{Z}, \circ)$ csoportban, ahol $a \circ b = a + b$, ha a páros és $a \circ b = a - b$, ha a páratlan, például a 10-zel osztható számok halmaza normálosztó.

   Bizonyítás. Azt, hogy egy páros szám többszörösei részcsoportot alkotnak, már láttuk. Legyen $N = \{10k \mid k \in \mathbb{Z}\}$. Ha most a páros szám, akkor mivel a $10k$ alakú számok mindig párosak, tetszőleges k-ra
   $$a \circ 10k = a + 10k = 10k + a = 10k \circ a,$$
   vagyis $a \circ N = N \circ a$. Ha a páratlan, akkor
   $$a \circ 10k = a - 10k,$$
   míg
   $$10k \circ a = 10k + a.$$
   Mivel az $a - 10k$ alakú számok halmaza egybeesik a $10k + a$ alakú számok halmazával, $a \circ N$ most is egyenlő $N \circ a$-val. Ugyanebben a csoportban a kételemű részcsoportok – például $H = \{0, 3\}$ – nem normálosztók. (Például $2 \circ H = \{2, 5\}$, míg $H \circ 2 = \{2, 1\}$). $\square$

5. D_4-ben (a négyzet szimmetriacsoportja) az $N = \{f_0, f_{180}\}$ normálosztó.

   Bizonyítás. Könnyen meggyőződhetünk arról, hogy a transzformációk egymásutánjára is és az inverzképzésre is zárt a halmaz, vagyis

N részcsoport. Mivel D_4-ben a forgatások kommutatív részcsoportot alkotnak (ami szintén normálosztó, hiszen rendje fele a csoport rendjének), és N részcsoportja az összes forgatás részcsoportjának, így ha g egy forgatás, akkor $g \cdot N = N \cdot g$. Ha g egy tükrözés, akkor könnyen ellenőrizhető, hogy $g \cdot N = \{g, t\} = N \cdot g$, ahol t a g tengelyére merőleges tengelyre vonatkozó tükrözés. □

6. Könnyen ellenőrizhető, hogy ugyanebben a csoportban a $H = \{f_0, t\}$ részcsoport, ahol t az egyik tükrözés, nem normálosztó.

Megjegyzés. Ha egy normáloszó szerint készítjük el a mellékosztályokat, akkor a normálosztó definíciója szerint mindegy, hogy bal vagy jobb oldali mellékosztályokról van szó, így beszélhetünk a g elemmel képzett N normálosztó szerinti mellékosztályról anélkül, hogy megmondanánk, hogy az bal vagy jobb oldali mellékosztály.

5.3. Tétel. *Egy csoport két normálosztójának metszete is és komplexusszorzata is normálosztó.*

Bizonyítás. Legyen N_1 és N_2 a $(G, \circ)$ csoport két normálosztója. Azt, hogy $N_1 \cap N_2$ részcsoport, már a 2.3. tételből tudjuk (a normálosztók részcsoportok, és részcsoportok metszete is részcsoport). Legyen g egy tetszőleges eleme a csoportnak. Könnyen meggondolható, hogy a $g \circ (N_1 \cap N_2)$ mellékosztály részhalmaza lesz a $(g \circ N_1) \cap (g \circ N_2)$ halmaznak és viszont, így a kölcsönös tartalmazás miatt

$$g \circ (N_1 \cap N_2) = (g \circ N_1) \cap (g \circ N_2).$$

Mivel N_1 és N_2 normálosztó,

$$g \circ N_1 = N_1 \circ g \quad \text{és} \quad g \circ N_2 = N_2 \circ g,$$

így

$$g \circ (N_1 \cap N_2) = (g \circ N_1) \cap (g \circ N_2) = (N_1 \circ g) \cap (N_2 \circ g) = (N_1 \cap N_2) \circ g.$$

Vagyis a két normálosztó metszete is normálosztó.

Ahhoz, hogy $N_1 \circ N_2$ részcsoportja G-nek, a 3.2. Tétel értelmében elegendő azt belátni, hogy $(N_1 \circ N_2) \circ (N_1 \circ N_2)^{-1} \subseteq N_1 \circ N_2$. Ehhez egyrészt azt fogjuk felhasználni, hogy $N_1 \circ N_2 = N_2 \circ N_1$ (hiszen N_2 normálosztó, így N_1 tetszőleges n elemére $n \circ N_2 = N_2 \circ n$); másrészt, hogy

$$(N_1 \circ N_2)^{-1} (N_2)^{-1} \circ (N_1)^{-1} \subseteq N_2 \circ N_1$$

(hiszen N_2 is és N_1 is részcsoport). Ezek alapján:

$$(N_1 \circ N_2) \circ (N_1 \circ N_2)^{-1} = (N_1 \circ N_2) \circ (N_2^{-1} \circ N_1^{-1}) =$$
$$= N_1 \circ (N_2 \circ N_2^{-1}) \circ N_1^{-1} \subseteq (N_1 \circ N_2) \circ N_1^{-1} = (N_2 \circ N_1) \circ N_1^{-1} =$$
$$= N_2 \circ (N_1 \circ N_1^{-1}) \subseteq N_2 \circ N_1 = N_1 \circ N_2.$$

Be kell még látnunk, hogy $N_1 \circ N_2$ normálosztó, vagyis tetszőleges g elem esetén

$$g \circ (N_1 \circ N_2) = (N_1 \circ N_2) \circ g.$$

Felhasználva, hogy N_1 és N_2 normálosztók:

$$g \circ (N_1 \circ N_2) = (g \circ N_1) \circ N_2 = (N_1 \circ g) \circ N_2 =$$
$$= N_1 \circ (g \circ N_2) = N_1 \circ (N_2 \circ g) = (N_1 \circ N_2) \circ g. \square$$

Megjegyzés. A bizonyítás első felében a részcsoport tulajdonság a nyilvánvaló, a második részben a normálosztó tulajdonság.

Megjegyzés. A $(G, \circ)$ csoport egy N normálosztójára ugyan teljesül, hogy tetszőleges $g \in G$ elemre $g \circ N = N \circ g$, mindazonáltal nem szükségszerű, hogy minden $n \in N$ elemre fennálljon, hogy $g \circ n = n \circ g$. Sőt!

Vizsgáljuk a D_6 csoport műveleti táblázatát!

$\cdot$	f_0	f_{60}	f_{120}	f_{180}	f_{240}	f_{300}	t_1	t_2	t_3	t_4	t_5	t_6
f_0	f_0	f_{60}	f_{120}	f_{180}	f_{240}	f_{300}	t_1	t_2	t_3	t_4	t_5	t_6
f_{60}	f_{60}	f_{120}	f_{180}	f_{240}	f_{300}	f_0	t_6	t_1	t_2	t_3	t_4	t_5
f_{120}	f_{120}	f_{180}	f_{240}	f_{300}	f_0	f_{60}	t_5	t_6	t_1	t_2	t_3	t_4
f_{180}	f_{180}	f_{240}	f_{300}	f_0	f_{60}	f_{120}	t_4	t_5	t_6	t_1	t_2	t_3
f_{240}	f_{240}	f_{300}	f_0	f_{60}	f_{120}	f_{180}	t_3	t_4	t_5	t_6	t_1	t_2
f_{300}	f_{300}	f_0	f_{60}	f_{120}	f_{180}	f_{240}	t_2	t_3	t_4	t_5	t_6	t_1
t_1	t_1	t_2	t_3	t_4	t_5	t_6	f_0	f_{60}	f_{120}	f_{180}	f_{240}	f_{300}
t_2	t_2	t_3	t_4	t_5	t_6	t_1	f_{300}	f_0	f_{60}	f_{120}	f_{180}	f_{240}
t_3	t_3	t_4	t_5	t_6	t_1	t_2	f_{240}	f_{300}	f_0	f_{60}	f_{120}	f_{180}
t_4	t_4	t_5	t_6	t_1	t_2	t_3	f_{180}	f_{240}	f_{300}	f_0	f_{60}	f_{120}
t_5	t_5	t_6	t_1	t_2	t_3	t_4	f_{120}	f_{180}	f_{240}	f_{300}	f_0	f_{60}
t_6	t_6	t_1	t_2	t_3	t_4	t_5	f_{60}	f_{120}	f_{180}	f_{240}	f_{300}	f_0

A szomszédos tengelyek az elsőtől a hatodikig az egymással 30°-os szöget zárnak be egymással. $H = \{f_0, f_{120}, f_{240}\}$ részcsoport. Normálosztó is, mert a forgatások részcsoportja eleve kommutatív – a táblázatban feltüntetett tükörtengely indexelés mellett pedig – a tengelyek indexének paritása megmarad, akár jobbról, akár balról szorozzuk meg vele H-t:

$$Ht_1 = \{t_1, t_5, t_3\}, \quad t_1H = \{t_1, t_3, t_5\}; \quad Ht_2 = \{t_2, t_6, t_4\}, \quad t_2H = \{t_2, t_4, t_6\};$$
$$Ht_3 = \{t_3, t_1, t_5\}, \quad t_3H = \{t_3, t_5, t_1\}; \quad Ht_4 = \{t_4, t_2, t_6\}, \quad t_4H = \{t_4, t_6, t_2\};$$
$$Ht_5 = \{t_5, t_3, t_1\}, \quad t_5H = \{t_5, t_1, t_3\}; \quad Ht_6 = \{t_6, t_4, t_2\}, \quad t_6H = \{t_6, t_2, t_4\}.$$

Az is látszik viszont, hogy például $f_{120}t_1 \neq t_1 f_{120}$.

Feladatok

1. Hány elemű részcsoportja lehet egy (a) 6, (b) 5 elemű csoportnak? (Használhatja a www.cs.elte.hu/~kfried/algebra3/groups2-8.jar csoportkészítő programot.) Melyek lehetnek normálosztók? Egy konkrét példán adja meg a mellékosztályokat!

2. Határozza meg a (a) $(\mathbb{Z}_6, +_{\text{ mod } 6})$ (b) $(\mathbb{Z}_5, +_{\text{ mod } 5})$ csoport részcsoportjait, normálosztóit!

3. Határozza meg a $(\mathbb{Z}_6, +_{\text{ mod } 6})$ csoport részcsoportjait, normálosztóit!

4. Legyen p tetszőleges pozitív prímszám. Értelmezzük a $\{1, p, p^2, p^3, p^4, p^5\}$ halmazon a $\circ$ műveletet úgy, hogy $p^k \circ p^m = p^r$, ahol $r \equiv k + m \pmod 6$, $0 \leq r < 6$. Igazolja, hogy csoportot kapunk!

   Van-e normálosztó ebben a csoportban?

   Ciklikus-e ez a csoport? Kommutatív-e a csoport?

5. Ellenőrizze, hogy $(\mathbb{Z}, +)$ csoport!

   Igazolja, hogy a $H = \{8k \mid k \in \mathbb{Z}\}$ részhalmaz részcsoportot alkot.

   Készítse el a H szerinti mellékosztályokat! Mit kapunk?

6. Határozza meg $(\mathbb{Z}_6, +_{\text{ mod } 6})$ részcsoportjait! Melyek normálosztók ezek közül?

7. Igazolja, hogy a 2×2-es valós reguláris (invertálható) mátrixok a mátrixszorzásra nézve csoportot alkotnak. Igazolja, hogy az 1 determinánsú mátrixok halmaza részcsoport ebben a struktúrában!

8. Melyek lesznek a $(\mathbb{R}, +)$ csoport $\mathbb{Z}$ részcsoport szerinti mellékosztályai?

9. Igazolja, hogy a valós számok $[0, 1)$ intervallumába eső részhalmaza a mod 1 összeadás szerint csoportot alkot. (r_1 és r_2 összegét értelmezzük $r_1 + r_2$ törtrészeként, azaz $\{r_1 + r_2\}$-nek.)

10. A sík vektorai a vektorösszeadásra nézve csoportot alkotnak. Ennek részcsoportja az $y = x$ egyenessel egyirányú vektorok halmaza. Mik lesznek eszerint a részcsoport szerinti mellékosztályok?

11. Igazolja, hogy a komplex egységvektorok (az 1 abszolút értékű komplex számok) a komplex számok szorzására nézve csoportot alkotnak. Keressen részcsoportot ebben a csoportban!

12. Határozza meg $(\mathbb{Z}_8, +_{\text{ mod } 8})$ elemeinek rendjét!

    Hány eleme lehet egy részcsoportjának?

    Határozza meg a részcsoportokat!

    Adja meg a részcsoportok indexét!

    Melyek normálosztók a részcsoportok közül?

13. A $(G, \circ)$ csoport centrumának nevezzük a csoport azon c elemeinek halmazát, amelyekre teljesül, hogy tetszőleges $g \in G$ elemre $g \circ c = c \circ g$.

    (a) Igazolja, hogy egy csoport centruma részcsoport.

    (b) Igazolja, hogy egy csoport centruma normálosztó.

14. Igazolja, hogy egy ciklikus csoport minden részcsoportja normálosztó!

15. Tekintsük $\mathbb{R}[x]$ összeadásra vett csoportjának a legfeljebb n-edfokú valós együtthatós polinomok H részcsoportját.

    Adja meg a H szerinti mellékosztályokat!

16. (a) A $(\mathbb{Z}, +)$ csoportnak részcsoportja, sőt normálosztója a $H_3 = \{3k \mid k \in \mathbb{Z}\}$ és $H_4 = \{4k \mid k \in \mathbb{Z}\}$ is. (Lássa be!)
    Határozza meg $H_3 \cap H_4$-t és $H_3 + H_4$-et. Ellenőrizze, hogy mindkettő normálosztó!

    (b) A $(\mathbb{Z}, +)$ csoportnak részcsoportja, sőt normálosztója a $H_9 = \{9k \mid k \in \mathbb{Z}\}$ és $H_{12} = \{12k \mid k \in \mathbb{Z}\}$ is. (Ezt is lássa be!)
    Határozza meg $H_9 \cap H_{12}$-t és $H_9 + H_{12}$-t. Ellenőrizze, hogy mindkettő normálosztó!

6. fejezet

Csoport kompatibilis osztályozása

Legyen a $(G, \circ)$ csoport $(N, \circ)$ részcsoportja normálosztó, és készítsük el az N szerinti mellékosztályokat: N, $a \circ N = N \circ a$, $b \circ N = N \circ b$, ...

Ha megvizsgáljuk két tetszőleges mellékosztály komplexus-szorzatát, a következőt tapasztaljuk:

$$\begin{aligned}(a \circ N) \circ (b \circ N) &= a \circ (N \circ b) \circ N = \\ &= a \circ (b \circ N) \circ N = \\ &= (a \circ b) \circ (N \circ N) = \\ &= (a \circ b) \circ N,\end{aligned}$$

vagyis az a és b elemmel képzett mellékosztályok „szorzata" megegyezik az $a \circ b$ elemmel képzett mellékosztállyal.

Felhasználtuk, hogy

- N normálosztó, így $b \circ N = N \circ b$.
- Asszociatív struktúrában a komplexusszorzás is asszociatív (az a és b elemeket tekinthetjük egyelemű komplexusoknak).
- $N \circ N = N$, ami azért igaz, mert N részcsoport, így tetszőleges $n_i \in N$ elem esetén az $n_i \circ N$ mellékosztály egybeesik N-nel, és $N \circ N$ éppen az összes $n_i \in N$ elemmel képzett mellékosztály uniója.

Az, hogy tetszőleges a és b elemek esetén

$$(a \circ N) \circ (b \circ N) = (a \circ b) \circ N$$

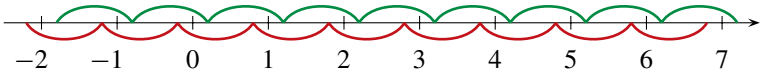
egyrészt azt jelenti, hogy az N szerinti mellékosztályok halmaza zárt a komplexusszorzásra nézve, másrészt, hogy ha az $a \circ N$ mellékosztály egy tetszőleges elemét „megszorozzuk” a $b \circ N$ mellékosztály tetszőleges elemével, akkor függetlenül attól, hogy melyik elemet választottuk az egyik, illetve a másik maradékosztályból, az eredmények mindig ugyanabban – az $(a \circ b) \circ N$ – mellékosztályban lesznek, vagyis a művelet eredménye ebben az értelemben független a reprezentáns elemek megválasztásától. Az ilyen típusú osztályozást kompatibilis osztályozásnak nevezik:

6.1. Definíció. Ha egy $(S, \circ)$ algebrai struktúra elemeit úgy soroljuk be (ekvivalencia) osztályokba, hogy tetszőleges A és B osztályok esetén tetszőleges a_1, $a_2 \in A$ és b_1, $b_2 \in B$-re az $a_1 \circ b_1$ elem ugyanabban az osztályban van, mint az $a_2 \circ b_2$ elem, akkor az osztályozást *kompatibilisnek,* az osztályokat pedig *maradékosztályoknak* nevezzük.

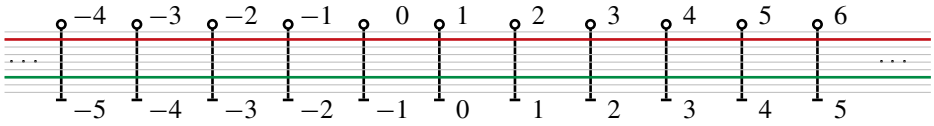
Megjegyzés. Az ilyen osztályozást nevezhetnénk művelettartó osztályozásnak is. Többműveletes struktúrákban természetesen minden műveletre teljesülnie kell a művelettartásnak – ezt majd később látni fogjuk.

Például: Ha $(\mathbb{R}, +)$ elemeit úgy soroljuk osztályokba, hogy azok a valós számok kerüljenek egy osztályba, amelyeknek a törtrésze ugyanannyi, akkor kompatibilis osztályozást kapunk, hiszen ha $\{a_1\} = \{a_2\}$ és $\{b_1\} = \{b_2\}$, akkor

$$\{a_1 + b_1\} = \big\{\{a_1\} + \{b_1\}\big\} = \big\{\{a_2\} + \{b_2\}\big\} = \{a_2 + b_2\}.$$



6.1. ábra.



6.2. ábra. A számegyenest 1 hosszú intervallumokra osztva a törtrész szerinti osztályok így képzelhetők el. Continuum sok osztály keletkezik.

Ha viszont az egészrészük szerint soroljuk osztályokba $(\mathbb{R}, +)$ elemeit, akkor nem kapunk kompatibilis osztályozást, mert például

$$[3{,}3] = [3{,}5] \quad \text{és} \quad [1{,}1] = [1{,}8];$$

de

$$[3{,}3 + 1{,}1] = 4 \neq [3{,}5 + 1{,}8] = 5.$$

A fentiek szerint ha egy csoportban elkészítjük a valamelyik normálosztó szerinti mellékosztályokat, akkor az így kapott osztályozás kompatibilis.

Ha például a $(\mathbb{Z}, +)$ csoportot a 3-mal osztható számok N részcsoportja szerint osztályozzuk, akkor három mellékosztályt kapunk: a 3-mal osztva 0, a 3-mal osztva 1, valamint a 3-mal osztva 2 maradékot adó számok halmazát. Vagyis éppen a (mod 3) maradékosztályokat, amelyekre valóban teljesül: az, hogy két szám összege 3-mal osztva milyen maradékot ad (melyik osztályban van), nem függ maguktól a számoktól, csak attól, hogy azok milyen maradékot adtak 3-mal osztva (melyik osztályban voltak). Hasonlóan, ha $(\mathbb{Z}, +)$-t az m szám többszöröseiből álló részcsoportja szerint osztályozzuk, akkor a mod m maradékosztályokat kapjuk.

Vizsgáljuk meg, hogy $(\mathbb{Z}, +)$-nak még milyen kompatibilis osztályozásai lehetségesek:

osztályok:	A	B	C	D	$\ldots$
elemek:	0				
	1				

1. Az 1 vagy ugyanabba az osztályba kerül, mint a 0, vagy egy másikba:

(a)

osztályok:	A	B	C	D	$\ldots$
elemek:	0				
	1				

(b)

osztályok:	A	B	C	$\ldots$
elemek:	0	1		

Az, hogy az osztályozás kompatibilis, azt jelenti, hogy ha például találunk két (nem feltétlenül különböző) A-beli elemet, amelyek összege is A-beli, akkor A két tetszőleges elemének az összege is A-ban kell, hogy legyen. Ezek szerint az 1.(a) esetben, mivel $0 + 0 = 0 \in A$ és $1 \in A$, az $1 + 1 = 2$-nek is A-ban kell lennie. Ekkor viszont az $1 + 2 = 3$-nak és a $2 + 2 = 4$-nek is, emiatt az $1 + 4 = 5$-nek is, és így tovább: ha az $1 \in A$, akkor az A minden eleménél eggyel nagyobb számnak is benne kell lennie A-ban, vagyis ebben az esetben az összes pozitív egész szám A-ba kerül. Könnyen meggondolható, hogy a negatív egészek sem kerülhetnek máshová, hiszen ha például a -1 valamelyik másik, mondjuk a B, osztályban lenne, akkor mivel $0 \in A$, $-1 \in$ $\in B$ és $0 + (-1) = -1 \in B$, a kompatibilis osztályozás miatt egy tetszőleges A-beli és egy tetszőleges B-beli elem összegének, például $1 + (-1) = 0$-nak is

B-belinek kell lennie. Ez viszont ellentmond annak, hogy a 0 az A osztályban van. Vagyis a -1 is csak az A osztályban lehet, és hasonlóképp látható be, hogy az összes egész szám az A osztályban lesz.

Vagyis ha az 1 ugyanabba az osztályba kerül, mint a 0, akkor csak egy osztályunk van, maga az egész számok halmaza.

Vizsgáljuk meg most azt az esetet, amikor az 1 nem a 0 osztályában van:

2. Ekkor a 2 vagy a 0 osztályában vagy az 1 osztályában vagy egy harmadik (C) osztályban van:

(a)

A	B	C	...
0	1		
2			

(b)

A	B	C	...
0	1		
	2		

(c)

A	B	C	...
0	1	2	

Először is a 2.(b) eset lehetetlen, mert akárhol is van a -1, hiába van 1 és 2 ugyanabban az osztályban, $0 = 1 + (-1)$ és $1 = 2 + (-1)$ különböző osztályba esnek.

A 2.(a) esetben, mivel $0 + 0 = 0 \in A$, és a 2 egy osztályban van a 0-val, a $2 + 2 = 4$-nek is ide kell kerülnie, emiatt a $2 + 4 = 6$-nak is és így tovább, az A tetszőleges eleménél 2-vel nagyobb számnak is, vagyis az összes pozitív páros számnak A-ban kell lennie. Hasonlóan, $0 + 1 = 1 \in B$ miatt a $2 + 1 = 3$-nak és így tovább, az összes pozitív páratlan számnak B-ben kell lennie. A -1-nek is a B osztályban kell lennie, mert ha 2-t adunk hozzá, akkor B-belit kapunk, így ha a 2-vel egy osztályban levő 0-t adjuk hozzá, akkor is B-belit kell kapnunk. Hasonlóan, a -2 csak az A osztályban lehet, mert ha 2-t adunk hozzá, akkor A-belit kapunk, így ha a 2-vel egy osztályban levő 0-t adjuk hozzá, akkor is A-belit kell kapnunk, és így tovább, az összes páratlan számnak B-be, az összes páros számnak A-ba kell kerülnie.

Vagyis ha a 0 és az 1 nincs egy osztályban és a 2 ugyanabban az osztályban van, mint a 0, akkor éppen a mod 2 maradékosztályokat kapjuk.

3. A 2.(c) esetben vizsgáljuk meg, hogy hova kerülhet a 3.

A 3 nem eshet egy osztályba 1-gyel, mert akkor (bárhova kerül is a -1) $(-1) + 3 = 2$ és $(-1) + 1 = 0$ egy osztályba esne, márpedig ez nem teljesül.

A 3 nem eshet egy osztályba 2-vel sem, mert akkor viszont $(-1) + 3 = 2$ és $(-1) + 2 = 1$ esne egy osztályba, márpedig ez sem teljesül.

Két lehetőség maradt: vagy a 0 osztályában van, vagy egy negyedik (D) osztályban:

Az első esetben a 2.(a) esetnél látottakhoz hasonló módon gondolható végig, hogy az összes 3-mal osztható szám A-ba, az összes $3k + 1$ alakú B-

be, az összes $3k+2$ alakú C-be kerül, vagyis a mod 3 maradékosztályokat kapjuk.

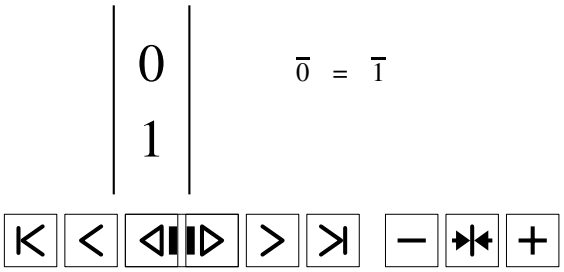
A másik esetben könnyen belátható, hogy a 4 nem kerülhet sem B-be, sem C-be, sem D-be.

Ha az A-ba kerül, akkor a mod 4 maradékosztályokat kapjuk, ha egy ötödik osztályba, akkor az 5 megint csak vagy a 0-val egy osztályba, vagy egy hatodik osztályba kerülhet és így tovább.

Ezek alapján megfogalmazhatjuk a következő sejtést:

6.1. Tétel. *Az egész számok összeadási csoportjának tetszőleges, triviálistól különböző kompatibilis osztályozásához létezik olyan $m(>1)$, hogy az osztályozás éppen a* mod m *maradékosztályokat hozza létre. (Triviális az osztályozás, ha vagy az összes elem egy osztályban van, vagy minden elem külön-külön egy-egy egyelemű osztály.)*

Bizonyítás. Először vizsgáljuk azt az esetet, amikor 0 és 1 egy osztályba esik. Ekkor tetszőleges k egész számra k és $k+1$ ugyanabba az osztályba esik, hiszen az egy osztályhoz tartozó 0-hoz és 1-hez hozzáadva a k-t (bárhová esik is k), az eredmény – vagyis k és $k+1$ – ugyanabban az osztályban lesz. Ebből az következik, hogy minden egész szám ugyanabba az osztályba esik, mint a 0.

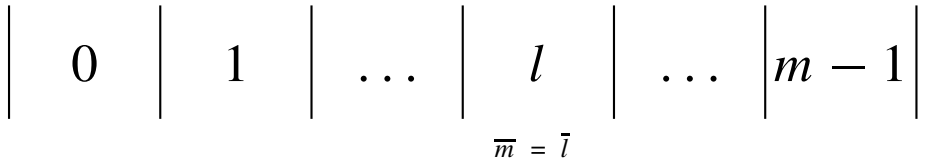


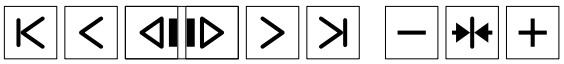
6.3. ábra.

Most tegyük fel, hogy egy kompatibilis osztályozás során a 0 és az 1 nem kerül egy osztályba. Legyen m a legkisebb olyan természetes szám, amelyre a $0, 1, 2, \ldots, m-1$ számok mindegyike különböző osztályban van, de m egy osztályba kerül egy nála kisebb nemnegatív egésszel, például l-lel, ahol $0 \leq \leq l < m$. (Később majd vizsgáljuk, hogy mi történik, ha nincs ilyen osztály.)

Ekkor mivel m és l egy osztályba esnek, $m+(-l) = m-l$ és $l+(-l) = 0$ is ugyanabba az osztályba kerülnek. Eszerint $m-l$ a 0 osztályába esik. A

$0 \leq l < m$ feltétel miatt azonban $m \geq m - l > 0$ – ezek közül a számok közül $1, 2, \ldots, m-1$ nem esik a 0 osztályába, vagyis ez csak úgy eshet a 0 osztályába, ha $m - l = m$, $l = 0$, és m a 0-val egy osztályban van.





6.4. ábra.

Ebből viszont levezethetjük, hogy tetszőleges k egész számra k és $k+m$ ugyanabban az osztályban van: $\overline{k+0} = \overline{k+m}$, azaz $\overline{k} = \overline{k+m}$. Innen már következik, hogy tetszőleges két olyan egész szám, amelyek különbsége m-nek egész számú többszöröse, ugyanabban az osztályban van.

Ezek szerint minden szám az m-mel való osztási maradékának megfelelő osztályba kerül, vagyis a keletkező osztályok $m \geq 2$ esetén éppen a mod m maradékosztályok, ha pedig $m = 1$, akkor az egyik triviális – minden szám a 0 osztályában van – osztályozást kapjuk, ahogyan azt korábban már láttuk.

Az imént feltételeztük, hogy van olyan m pozitív egész szám, amely az osztályozás során egy nála kisebb nemnegatív szám osztályába kerül. Ha viszont nincs ilyen m szám, akkor ez azt jelenti, hogy az összes természetes szám egy-egy külön osztályt képvisel. Mivel ilyenkor 0 és 1 különböző osztályba esnek, így tetszőleges k egész számra k és $k+1$ is más-más osztályba esik. (Ellenkező esetben $k+(-k)$ és $k+1+(-k)$, azaz 0 és 1 is egy osztályba esne.)

Vagyis ebben az esetben a másik triviális – minden szám külön osztály – osztályozást kapjuk.

Tehát $(\mathbb{Z}, +)$ egy osztályozása csak úgy lehet kompatibilis, ha

– vagy minden szám ugyanabba az osztályba kerül;

– vagy minden egyes szám külön-külön osztályba kerül;

– vagy van olyan $m \geq 2$ pozitív egész szám, amelyre az osztályok éppen a mod m maradékosztályok. □

Megjegyzés. A fejezet elején láttuk, hogy ha egy tetszőleges csoportot egy normálosztója szerint osztályozunk (elkészítjük a mellékosztályokat), akkor az így kapott osztályozás kompatibilis. $(\mathbb{Z}, +)$-nak (mivel kommutatív) minden részcsoportja normálosztó. Ez azt jelenti, hogy bármelyik részcsoportja szerint osztályozzuk, a fenti esetek valamelyikét kapjuk. (Ha a részcsoport, ami szerint osztályozunk a teljes csoport, akkor az első esetet; ha az az egyelemű $\{0\}$ halmaz, akkor a másodikat; ha pedig egy $|m| \geq 2$ szám többszöröseinek halmaza, akkor a harmadikat.) Vagyis $(\mathbb{Z}, +)$-ban a kompatibilis osztályozás, a valamely részcsoport szerinti mellékosztályok elkészítése, és valamilyen modulusra a mod m maradékosztályok elkészítése ugyanazt jelenti.

Az egész számokon szerzett tapasztalataink általánosan is igazak. Ezt fogalmazzuk meg a következő tételben.

6.2. Tétel. *Egy G csoport kompatibilis osztályozásai éppen a normálosztói szerintiek.*

(Vagyis ha egy csoportot egy tetszőleges normálosztója szerint osztályozunk, akkor az osztályozás kompatibilis, és viszont, ha egy kompatibilis osztályozást adunk meg egy csoportban, akkor a csoportnak mindig van olyan normálosztója, ami szerinti mellékosztályok éppen az adott osztályozást hozzák létre.)

Bizonyítás. Az állítás első felét már a fejezet elején bizonyítottuk, azt kell még belátnunk, hogy ha egy osztályozás kompatibilis, akkor van olyan normálosztó, ami szerint ugyanezt az osztályozást kapjuk.

Tegyük fel, hogy egy kompatibilis osztályozás során az E, A, B, C, D, ... osztályokat kaptuk, ahol E a csoport e egységelemének az osztálya.

Azt fogjuk megmutatni, hogy E részcsoport, normálosztó, és E szerint osztályozva a csoportot, éppen a fenti osztályozást kapjuk.

1. (a) Az egységelem benne van E-ben (éppen az e-t tartalmazó osztályt neveztük E-nek).

Vegyük észre, hogy mivel az osztályozás kompatibilis, így ha egy X osztály x elemét „megszorozzuk" (például balról) egy E osztályba eső egyik elemmel – konkrétan e-vel –, akkor ismét X-beli elemet kapunk. Így bármely X-beli elemet megszorozva bármely E-belivel, X-beli elemet kapunk. (Eszerint $E \circ X \subseteq X$ és $X \circ E \subseteq X$.)

1. (b) Ebből ($X = E$ választással) azonnal következik, hogy E zárt a $\circ$ műveletre.

1. (c) Mivel G csoport, a $\circ$ művelet asszociatív, így persze E-ben is az.

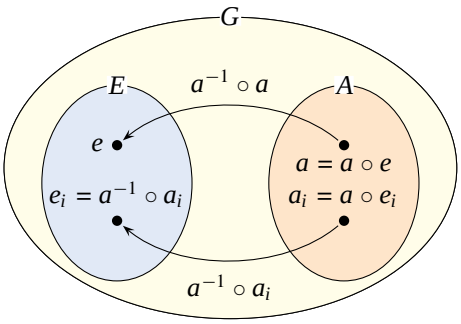
1. (d) Belátjuk, hogy minden $e_i \in E$ elem inverze is E-ben van – vagyis végső soron E valóban részcsoport.

Ha ugyanis e_i inverze az X osztályban van, akkor $e_i \circ e_i^{-1} = e$, azaz E-beli és X-beli szorzata E-ben van, tehát $e \circ e_i^{-1} = e_i^{-1}$ is E-ben van. (Ez a korábbi észrevételből is adódik, mert E-beli és X-beli csak úgy lehet X-beli is és E-beli is, ha $X = E$.)

2. Belátjuk, hogy E normálosztó, azaz ha például a az A osztály egy tetszőleges eleme, akkor $a \circ E = A$, vagyis minden osztály megegyezik valamelyik elemével képzett E szerinti (mondjuk bal oldali) mellékosztállyal.

A korábbi *észrevétel* alapján tudjuk, hogy az E-beli és az A-beli elemek „szorzata" A-ba esik, de azt nem tudjuk, hogy minden A-beli a_i elem előáll-e $a \circ e_i$ alakban, ahol $e_i \in E$.

Mivel a és a_i egyaránt A-ba esik, így ha mindkettőt „megszorozzuk" az a^{-1} elemmel, akkor az eredmények is ugyanabba az osztályba fognak esni – hiszen az osztályozás kompatibilis. Márpedig $a^{-1} \circ a = e \in E$, vagyis $a^{-1} \circ a_i \in E$. Eszerint találtunk olyan E-beli elemet ($e_i = a^{-1} \circ a_i$), amelyet a-val (balról) „megszorozva" a_i-t kapjuk: $a \circ (a^{-1} \circ a_i) = (a \circ a^{-1}) \circ a_i = a_i$.



6.5. ábra.

Ezek szerint $A = a \circ E$. Hasonlóan bizonyítható, hogy $E \circ a$ is megegyezik A-val.

A fenti állításban az A osztályt választottuk, de választhattuk volna bármelyik másikat. Vagyis mindegyik mellékosztályra igaz, hogy ő valamely (sőt, bármely) elemével képezett bal, illetve jobb oldali mellékosztálya az E-nek.

Ebből következik, hogy $\forall g \in G$-re $g \circ E = E \circ g$, vagyis az E részcsoport valóban normálosztó. Az E szerinti osztályok pedig az imént látottak alapján éppen az adott kompatibilis osztályozás szerinti osztályok. □

Megjegyzés. Ha például a valós számokat a törtrészük szerint osztályozzuk, akkor mint már láttuk, $(\mathbb{R}, +)$ egy kompatibilis osztályozását kapjuk. Tételünk szerint ekkor lennie kell egy olyan normálosztónak, ami szerint elkészítve a mellékosztályokat, ugyanezt az osztályozást kapjuk. Példánkban ez a normálosztó a 0 osztálya (azoknak a valós számoknak az osztálya, amelyek törtrésze 0), vagyis a $(\mathbb{Z}, +)$ részcsoport.

Tételünk szerint egy csoport kompatibilis osztályozása, illetve valamelyik normálosztója szerinti mellékosztályok elkészítése ugyanazt jelenti, így a jövőben ha maradékosztályokról beszélünk, akkor azt képzelhetjük úgy is, hogy egy normálosztó szerinti mellékosztályokról van szó, és úgy is, hogy egy kompatibilis osztályozás során létrejövő maradékosztályokról. A $(G, \circ)$ csoport N normálosztója szerinti maradékosztályok halmazát (tehát azt a halmazt, amelynek az N szerinti mellékosztályok az elemei) szokás G/N-nel jelölni.

A fejezet elején láttuk, hogy tetszőleges $(G, \circ)$ csoport maradékosztályainak halmaza zárt a komplexusszorzásra nézve (67. oldal), és mivel csoportban a művelet asszociatív, a komplexusszorzás is asszociatív, így ha N egy normálosztója a csoportnak, akkor a $(G/N, \circ)$ struktúra félcsoport. Ennél azonban több is igaz:

6.3. Tétel. *A $(G, \circ)$ csoport egy tetszőleges N normálosztója szerinti maradékosztályok halmaza csoportot alkot a komplexusszorzásra. (Vagyis $(G/N, \circ)$ csoport.)*

Bizonyítás. Azt, hogy $(G/N, \circ)$ félcsoport, az imént láttuk. Keressük meg, mi lehet az egységelem. A fejezet elején (66. oldal) azt is láttuk, hogy $N \circ N = N$, így tetszőleges $g \in G$-re:

$$(g \circ N) \circ N = g \circ (N \circ N) = g \circ N$$

és

$$N \circ (g \circ N) = (N \circ g) \circ N = (g \circ N) \circ N = g \circ (N \circ N) = g \circ N,$$

vagyis az N maradékosztály egységelem a $(G/N, \circ)$ félcsoportban.

A $g \circ N$ komplexus inverze: $(g \circ N)^{-1} = N^{-1} \circ g^{-1}$. De mivel N részcsoport, $N^{-1} = N$, így $(g \circ N)^{-1} = N \circ g^{-1}$ ($= g^{-1} \circ N$, mert N normálosztó), vagyis a g elemmel képzett maradékosztály inverze megegyezik a g elem inverzével képzett maradékosztállyal. Tehát G/N az inverzképzésre is zárt, így $(G/N, \circ)$ csoport. □

6.2. Definíció. A $(G/N, \circ)$ csoportot a $(G, \circ)$ csoport N normálosztójához tartozó *faktorcsoportjának* nevezik.

Például:

1. $(\mathbb{Z}, +)$-t az m szám többszöröseiből álló részcsoportja szerint osztályozva a mod m maradékosztályok összeadási csoportját kapjuk. Vagyis ha $N = \{km \mid k \in \mathbb{Z}\}$, akkor a faktorcsoport: $(\mathbb{Z}/N, +) = (\mathbb{Z}_m, +)$.

2. $(\mathbb{Z}_6, +)$-t (a 5.1. Definíciót [mellékosztályok] követő példák jelöléseit használva) a triviális $A = \{\bar{0}\}$ normálosztó szerint osztályozva hat (egyelemű) osztályt kapunk, a $(\mathbb{Z}_6/A, +)$ faktorcsoport izomorf lesz az eredeti csoporttal. Ha a $B = \{\bar{0}, \bar{3}\}$ normálosztó szerint osztályozunk, akkor három osztályt kapunk. A $(\mathbb{Z}_6/B, +)$ faktorcsoport művelettáblázata és az egyes elemek inverze a következő:

$+$	$\{\bar{0},\bar{3}\}$	$\{\bar{1},\bar{4}\}$	$\{\bar{2},\bar{5}\}$
$\{\bar{0},\bar{3}\}$	$\{\bar{0},\bar{3}\}$	$\{\bar{1},\bar{4}\}$	$\{\bar{2},\bar{5}\}$
$\{\bar{1},\bar{4}\}$	$\{\bar{1},\bar{4}\}$	$\{\bar{2},\bar{5}\}$	$\{\bar{0},\bar{3}\}$
$\{\bar{2},\bar{5}\}$	$\{\bar{2},\bar{5}\}$	$\{\bar{0},\bar{3}\}$	$\{\bar{1},\bar{4}\}$

egységelem:	$\{\bar{0},\bar{3}\}$
$-\{\bar{0},\bar{3}\}$	$= \{\bar{0},\bar{3}\}$
$-\{\bar{1},\bar{4}\}$	$= \{\bar{2},\bar{5}\}$
$-\{\bar{2},\bar{5}\}$	$= \{\bar{1},\bar{4}\}$

Ha a $C = \{\bar{0}, \bar{2}, \bar{4}\}$ normálosztó szerint osztályozunk, akkor két osztályt kapunk, amelyekre:

$+$	$\{\bar{0},\bar{2},\bar{4}\}$	$\{\bar{1},\bar{3},\bar{5}\}$
$\{\bar{0},\bar{2},\bar{4}\}$	$\{\bar{0},\bar{2},\bar{4}\}$	$\{\bar{1},\bar{3},\bar{5}\}$
$\{\bar{1},\bar{3},\bar{5}\}$	$\{\bar{1},\bar{3},\bar{5}\}$	$\{\bar{0},\bar{2},\bar{4}\}$

egységelem:	$\{\bar{0},\bar{2},\bar{4}\}$
$-\{\bar{0},\bar{2},\bar{4}\}$	$= \{\bar{0},\bar{2},\bar{4}\}$
$-\{\bar{1},\bar{3},\bar{5}\}$	$= \{\bar{1},\bar{3},\bar{5}\}$

Ha a teljes $\mathbb{Z}_6$ – mint triviális normálosztó – szerint osztályozunk, akkor a faktorcsoportnak egyetlen eleme lesz, maga a $\mathbb{Z}_6 = \{\bar{0}, \bar{1}, \bar{2}, \bar{3}, \bar{4}, \bar{5}\}$ halmaz, amelynek saját magával vett komplexusszorzata saját maga.

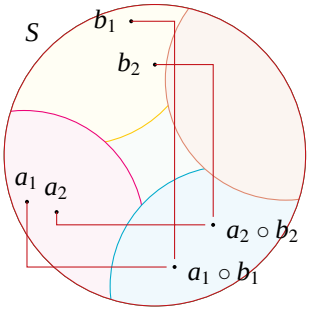
3. A szabályos háromszög D_3 szimmetriacsoportjának csak egy valódi (nem triviális) normálosztója van: a forgatások részcsoportja. (A forgatások részcsoportjának rendje 3 – az elemszáma fele a csoport elemszámának –, ezért biztosan normálosztó.) E részcsoport szerint osztályozva két osztályt kapunk: a forgatások $F = \{f_0, f_{120}, f_{240}\}$, valamint a tükrözések $T = t_A, t_B, t_C$ halmazát. Könnyen ellenőrízhető, hogy

$$F \cdot F = F, \qquad F \cdot T = T \cdot F = T, \qquad T \cdot T = F;$$

Ez a kételemű struktúra tehát egy kételemű csoport, ahol az egységelem F, és $T^{-1} = T$.

Általában is szokás egy algebrai struktúra faktorstruktúrájáról beszélni:

6.3. Definíció. Tekintsük az $(S, \circ)$ algebrai struktúra egy (σ ekvivalencia reláció szerinti) kompatibilis osztályozását, és jelöljük S/σ-val az osztályok halmazát. (Az S/σ halmazt szokás az S halmaz σ ekvivalencia relációhoz tartozó faktorhalmazának nevezni.) Ekkor az osztályok között az $\overline{a} * \overline{b} := \overline{a \circ b}$ műveletet definiálva (vagyis az a elem osztálya és a b elem osztálya „szorzatának" az $a \circ b$ elem osztályát tekintve) az $(S/\sigma, *)$ algebrai struktúrát *az* $(S, \circ)$ *struktúra* (σ szerinti) *faktorstruktúrájának* nevezzük.



6.6. ábra. A faktorstruktúrában $\overline{a} * \overline{b} = \overline{a \circ b}$

Megjegyzés. A fenti elnevezéshez azért volt jogunk, mert S/σ zárt a fent definiált $*$ műveletre, hiszen az, hogy az osztályozás kompatibilis, éppen azt jelenti, hogy az a elem osztályának egy tetszőleges elemét „megszorozva" ($a \circ$ művelet szerint) a b elem osztályának tetszőleges elemével, az eredménynek az $a \circ b$ osztályában kell lennie, vagyis az osztályokon végzett művelet eredménye független a reprezentáns elemektől.

Érdemes észrevenni, hogy csoportok esetén az így definiált művelet éppen a komplexusszorzás, hiszen ott az N normálosztó szerinti maradékosztályokra az a elem $a \circ N$ maradékosztályának és a b elem $b \circ N$ maradékosztályának a komplexusszorzata éppen az $a \circ b$ elemhez tartozó $(a \circ b) \circ N$ maradékosztály. Általában csak annyi igaz, hogy az $\overline{a}$ osztály és a $\overline{b}$ osztály $a \circ b$ komplexusszorzata részhalmaza lesz az $a \circ b$ elem osztályának, azaz $\overline{a} * \overline{b}$-nek.

Ha például a 10-nél nagyobb egészek összeadási félcsoportját osztályozzuk úgy, hogy azok a számok kerülnek egy osztályba, amelyek ugyanarra a számjegyre végződnek (ugyanazt a maradékot adják 10-zel osztva), akkor könnyen belátható, hogy az osztályozás kompatibilis (az, hogy két szám összege mire végződik, csak a két szám utolsó jegyétől függ). Ha most szemügyre vesszük például a 11 és a 12 osztályát, akkor ezek $\overline{11} * \overline{12} = \overline{11 + 12} = \overline{23} = \overline{13}$ szorzatában benne lesz a 13 (mivel a 13 – végződése szerint – ugyanabban az osztályban van, mint a 23), míg a két osztály komplexusszorzatában nem lesz benne (mivel a 11 és a 12 osztályuk legkisebb elemei, így

osztályuk komplexusszorzatának legkisebb eleme a 23). Ez azt jelenti, hogy egy struktúra maradékosztályainak halmaza a komplexusszorzásra nem feltétlenül zárt, míg a fent definiált $*$ műveletre igen.

Homomorfizmusok

Egy H halmaz osztályozását úgy is elképzelhetjük, hogy definiálunk egy

$$\varphi\colon H \to K$$

leképezést (ahol K tetszőleges halmaz), és egy osztályba soroljuk H azon elemeit, amelyeknek ugyanaz a képük.

Ha például minden egész számhoz hozzárendeljük négyzetének utolsó számjegyét, akkor ezzel az egész számokat hat osztályba soroltuk be, ahol az egyik osztályban lesz az összes 0-ra végződő egész szám, egy másikban az összes olyan szám, amely 10-zel osztva 1-et vagy 9-et ad maradékul stb.

Ha minden egész számhoz hozzárendeljük a 3-mal való osztási maradékát, akkor három osztályt – a mod 3 maradékosztályokat – kapunk.

Ha minden valós együtthatós polinomhoz hozzárendeljük a fokszámát, akkor az azonos fokszámú polinomok kerülnek egy osztályba, minden természetes számnak megfelel egy osztály.

Csoportok – és általában algebrai struktúrák – leképezései közül különleges szerepet játszanak azok, amelyek művelettartóak a következő értelemben:

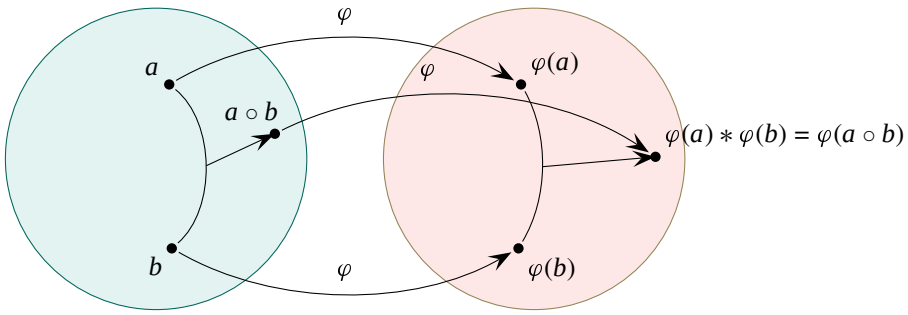
6.4. Definíció. Az $(S, \circ)$ algebrai struktúrát az $(S', *)$ algebrai struktúrára vivő $\varphi\colon S \to S'$ leképezést *homomorfizmusnak* (vagy homomorf leképezésnek) nevezzük, ha tetszőleges $a, b \in S$ esetén $\varphi(a \circ b) = \varphi(a) * \varphi(b)$. (Vagyis bármely két elem „szorzatának” a képe megegyezik a képelemek „csillagszorzatával”.)

Ha például minden egész számhoz a hármas maradékát rendeljük, akkor ez a leképezés homomorf módon viszi a $(\mathbb{Z}, +)$ csoportot a $(\mathbb{Z}_3, +)$ csoportba, és a $(\mathbb{Z}, \cdot)$ félcsoportot a $(\mathbb{Z}_3, \cdot)$ félcsoportba.

Ha minden valós számhoz hozzárendeljük a törtrészét, akkor $(\mathbb{R}, +)$-t homomorf módon képeztük le a $(\{x \mid 0 \le x < 1\}, *)$ csoportra, ahol $a * b = \{a + b\}$.

Ha a valós együtthatós polinomokhoz hozzárendeljük a fokszámukat, akkor ezzel homomorf módon képezzük le az $(\mathbb{R}[x]\backslash\{0\}, \cdot)$ félcsoportot az $(\mathbb{N}, +)$ félcsoportra – mivel tetszőleges két polinom esetén

$$\big(f(x)g(x)\big)^\circ = f(x)^\circ + g(x)^\circ.$$



6.7. ábra. Homomorfizmus: művelettartó leképezés

Készítsük most el az S halmaz egy osztályozását úgy, hogy azokat az elemeket soroljuk egy osztályba, amelyeknek ugyanaz az S'-beli elem a képe egy $\varphi\colon (S,\circ) \to (S',*)$ leképezés szerint. Ahhoz, hogy ez a φ leképezés kompatibilis osztályozást hozzon létre az S halmazon, az kell, hogy tetszőleges $a_1, a_2, b_1, b_2 \in S$ elemekre, ha

$\varphi(a_1) = \varphi(a_2)$ (vagyis a_1 és a_2 egy osztályban van) és

$\varphi(b_1) = \varphi(b_2)$ (b_1 és b_2 egy osztályban van), akkor

$\varphi(a_1 \circ b_1) = \varphi(a_2 \circ b_2)$ teljesüljön.

Amennyiben a φ leképezés homomorfizmus, akkor ez nyilvánvalóan teljesül:

6.4. Tétel. *Ha a $\varphi(S,\circ) \to (S',*)$ leképezés homomorfizmus, akkor egy osztályba sorolva S-nek azokat az elemeit, amelyeknek ugyanaz az S'-beli elem a képe, az így kapott osztályozás kompatibilis.*

tetel

Bizonyítás. Ha a leképezés homomorf, akkor $\forall a_1, a_2, b_1, b_2 \in S$-re $\varphi(a_1 \circ b_1) = \varphi(a_1) * \varphi(b_1)$ és $\varphi(a_2 \circ b_2) = \varphi(a_2) * \varphi(b_2)$. Ha $\varphi(a_1) = \varphi(a_2)$ és $\varphi(b_1) = \varphi(b_2)$, akkor ebből következik, hogy $\varphi(a_1 \circ b_1) = \varphi(a_2 \circ b_2)$, vagyis az osztályozás kompatibilis. □

Az is igaz, hogy ha megadjuk a $(G,\circ)$ csoport egy kompatibilis osztályozását, akkor van olyan homomorfizmus, amely ugyanezt az osztályozást hozza létre. Ha ugyanis a kompatibilis osztályozás során az N normálosztó szerinti maradékosztályokat kapjuk, akkor a csoportot a $(G/N,\circ)$ faktorcsoportba vivő $g \to g \circ N$ leképezés homomorf lesz. Általában:

6.5. Tétel. *Ha egy $(S,\circ)$ algebrai struktúrán létrehozunk egy σ kompatibilis osztályozást, majd minden elemhez hozzárendeljük azt az osztályt, amelyik*

az illető elem osztálya, akkor az így definiált $\varphi\colon (S,\circ)\to(S/\sigma,*)$ $(s\to\overline{s})$ *leképezés homomorf.*

Bizonyítás. Ahhoz, hogy a leképezés homomorf legyen, az kell (szükséges), hogy tetszőleges $a,b\in S$-re $\varphi(a\circ b)=\varphi(a)*\varphi(b)$ teljesüljön. Mivel a leképezés szerint az $a\circ b$ elem képe az $\overline{a\circ b}$ osztály, az a képe az $\overline{a}$, a b képe a $\overline{b}$ osztály, és a faktorstruktúrában két osztály szorzatát éppen úgy definiáltuk, hogy $\overline{a}*\overline{b}=:\overline{a\circ b}$, az állítás nyilvánvalóan teljesül. Vagyis egy struktúra tetszőleges faktorstruktúrája homomorf képe a struktúrának. □

Következmény. Egy $(G,\circ)$ csoport tetszőleges $(G/N,\circ)$ faktorcsoportja homomorf képe a csoportnak (a $g\to g\circ N$ leképezés szerint). Az is igaz, hogy egy csoport tetszőleges homomorf képe szintén csoport lesz, méghozzá egy olyan csoport, amely izomorf az eredeti csoport valamelyik faktorcsoportjával.

6.6. Tétel. *Ha a* $(G',*)$ *struktúra homomorf képe a* $(G,\circ)$ *csoportnak, akkor* $(G',*)$ *izomorf a* $(G,\circ)$ *csoport egy* $(G/N,\circ)$ *faktorcsoportjával.*

Bizonyítás. Ha egy osztályba soroljuk G azon elemeit, amelyeknek ugyanaz a G'-beli elem a képe, akkor az 6.4. Tétel szerint G-nek egy kompatibilis osztályozását kapjuk. Legyen N az a normálosztója G-nek, ami szerint ugyanezt az osztályozást kapjuk (ilyen normálosztó a 6.2. Tétel szerint biztosan van). Azt szeretnénk megmutatni, hogy az ehhez az N-hez tartozó $(G/N,\circ)$ faktorcsoport izomorf a $(G',*)$ struktúrával. Ehhez egy olyan bijektív $\varphi\colon (G/N,\circ)\to(G',*)$ leképezést kell megadnunk, amelyre tetszőleges $a,b\in G$ esetén az $a\circ N$, $b\circ N$ maradékosztályokra $\varphi\big((a\circ N)\circ(b\circ N)\big)=\varphi(a\circ N)*\varphi(b\circ N)$ teljesül. Megmutatjuk, hogy a $\varphi\colon g\circ N\to g'$ leképezés – ahol $g'\in G'$ a $g\in G$ elem képe az eredeti $(G,\circ)\to(G',*)$ homomorf leképezés szerint – ilyen.

A φ leképezés nyilvánvalóan bijektív, hiszen a $g\circ N$ maradékosztály éppen azokat az elemeit tartalmazza G-nek, amelyeket a homomorf leképezés ugyanabba a $g'\in G'$ elembe vitt. Így G' minden eleméhez pontosan egy olyan maradékosztály tartozik, amelynek elemeit a homomorf leképezés az illető G'-beli elembe vitte.

Mivel

$$(a\circ N)\circ(b\circ N)=(a\circ b)\circ N,$$

így

$$\varphi\big((a\circ N)\circ(b\circ N)\big)=\varphi\big((a\circ b)\circ N\big)=(a\circ b)'.$$

Felhasználva, hogy $\varphi(a\circ N)=a'$ és $\varphi(b\circ N)=b'$, a művelettartáshoz azt kell megmutatnunk, hogy $(a\circ b)'=a'*b'$. Ez pedig azért igaz, mert az eredeti $(G,\circ)\to(G',*)$ leképezés homomorf volt. □

A tétel állítását a következő példával szemléltethetjük:

Adjuk meg $(\mathbb{Z}, +)$-nak egy homomorf leképezését!

Minden homomorf leképezés létrehoz egy kompatibilis osztályozást.

Tudjuk, hogy $(\mathbb{Z}, +)$ minden (triviálistól különböző) kompatibilis osztályozása olyan, hogy azok a számok kerülnek egy osztályba, amelyek valamilyen m számmal osztva ugyanazt a maradékot adják (6.1. Tétel).

Emiatt ez a homomorf leképezés csak olyan lehet, hogy van egy olyan m szám, amelyre igaz, hogy a leképezés ugyanazt rendeli az összes olyan egészhez, amelyek ugyanazt a maradékot adják m-mel osztva.

Rendeljük mondjuk a 3-mal osztható számok mindegyikéhez a „pricc" szót, a $3k+1$ alakú számok mindegyikéhez a „pracc", a $3k+2$ alakú számokhoz pedig a „prucc" szót.

Ezzel az egész számok halmazát leképeztük a $H = \{\text{pricc}, \text{pracc}, \text{prucc}\}$ halmazra.

Ahhoz, hogy egy $(\mathbb{Z}, +) \to (H, *)$ leképezés homomorf legyen, az is kell, hogy tetszőleges a, b egészekre $(a+b)' = a' * b'$ teljesüljön (ahol a' az a képe, b' a b képe, $(a+b)'$ pedig az $a+b$ képe). Ez azt jelenti, hogy például pricc$*$pracc csak pracc lehet, hiszen $0 \to$ pricc, $1 \to$ pracc és $0+1 = 1 \to$ pracc. Könnyen meggondolható, hogy $(H, *)$ művelettáblázata csak a következő lehet:

$*$	pricc	pracc	prucc
pricc	pricc	pracc	prucc
pracc	pracc	prucc	pricc
pracc	prucc	pricc	pracc

Látható, hogy a H halmaz az így definiált művelettel, izomorf a $(\mathbb{Z}_3, +)$ csoporttal, ami éppen az a faktorcsoportja $(\mathbb{Z}, +)$-nak, amelyet a homomorf leképezés szerinti kompatibilis osztályozás létrehozott.

Feladatok

1. Készítse el az $(\mathbb{Z}, +)$ csoport $(\{5k \mid k \in \mathbb{Z}\}, +)$ részcsoportja szerinti faktorcsoportját! Hány elemű a kapott faktorcsoport?
2. Legyen $(G, +) = \left(\left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \;\middle|\; a, b, c, d \in \mathbb{Z} \right\}, + \right)$

   Legyen továbbá $H = \left\{ \begin{pmatrix} 2k & 2l \\ 2m & 2n \end{pmatrix} \;\middle|\; k, l, m, n \in \mathbb{Z} \right\}$ a G-nek egy részhalmaza.

Igazolja, hogy $(H,+)$ részcsoport! Igazolja, hogy normálosztó is!

Határozza meg G-nek H szerinti faktorcsoportját!

3. Legyen $(G,\cdot)=\left(\left\{\begin{pmatrix}a & b\\ c & d\end{pmatrix}\;\middle|\; a,b,c,d\in\mathbb{Q}, ad-bc\neq 0\right\},\cdot\right)$ (A reguláris mátrixok a mátrixszorzásra.)

   Legyen továbbá $H=\left\{\begin{pmatrix}k & l\\ m & n\end{pmatrix}\;\middle|\; kn-lm=1\right\}$ a G-nek egy részhalmaza.

   Igazolja, hogy $(H,\cdot)$ részcsoport! Igazolja, hogy normálosztó is!

   Határozza meg G-nek H szerinti faktorcsoportját!

   Adjon meg olyan csoportot, amely izomorf G/H-val!

4. Igazolja, hogy a $G=\{a+b\sqrt{5}\mid a,b\in\mathbb{Z}\}$ alakú számok az összeadásra nézve csoportot alkotnak!

   Igazolja, hogy ennek részcsoportja a $H=\{2u+2v\sqrt{5}\mid u,v\in\mathbb{Z}\}$ alakú számok halmaza (ugyanerre az összeadásra)! Írja fel a mellékosztályokat! Mik a létrejövő osztályok?

   Adja meg azt a homomorfizmust, amely ezt az osztályozást hozza létre!

5. Legyen $G=\left\{\begin{bmatrix}a\\ b\end{bmatrix}\mid a,b,\in\mathbb{Z}\right\}$ a sík egészek feletti vektorai, a művelet a vektorösszeadás. Tekintsük az $\varphi\colon \begin{bmatrix}a\\ b\end{bmatrix}\mapsto a-b$ leképezést.

   Igazoljuk, hogy φ homomorfizmus.

   Melyik részcsoport szerinti faktorizációt adtuk meg ezzel?

   Mik lesznek a mellékosztályok? (Vö. 9.1. ábra.)

6. Legyen $G=\left\{\begin{bmatrix}a\\ b\end{bmatrix}\mid a,b\in\mathbb{Z}, b\neq\{0\}\right\}$ (vektorok halmaza); a műveletet definiáljuk így:

$$\begin{bmatrix}a_1\\ b_1\end{bmatrix}\circ\begin{bmatrix}a_2\\ b_2\end{bmatrix}=\begin{bmatrix}a_1a_2\\ b_1b_2\end{bmatrix}$$

   Igazolja, hogy $(G,\circ)$ csoport.

   Tekintsük az $\psi\colon \begin{bmatrix}a\\ b\end{bmatrix}\mapsto\frac{a}{b}$ leképezést. Igazolja, hogy ψ homomorfizmus.

   Melyik részcsoport szerinti faktorizációt adtuk meg ezzel?

   Mik lesznek a mellékosztályok? (Vö. 11.1. ábra.)

7. Igazolja, hogy bármely két n elemű ciklikus csoport izomorf!

   Írjon fel egy 6 elemű ciklikus csoportot! Határozza meg az összes részcsoportját, azok összes mellékosztályát, illetve adja meg mindegyikhez az őt definiáló homomorfizmust!

8. Igazolja, hogy izomorfia erejéig csak kétféle lehet egy 4 elemű csoport! (Használhatja a `www.cs.elte.hu/~kfried/algebra3/groups2-8.jar` csoportkészítő programot. A piros betű az invertálhatóság, a narancssárga színezés az asszociativitás sérülésére utaló hibát jelez.)

   Mindkét típusú 4 elemű csoportban adja meg a részcsoportokat, normálosztókat, mellékosztályaikat, illetve az őket megadó homomorfizmusokat!

9. Tekintsük $\mathbb{R}[x]$ összeadásra vett csoportjának a legfeljebb n-edfokú valós együtthatós polinomok H részcsoportját.

   Adja meg a H szerinti mellékosztályokat meghatározó homomorfizmust!

7. fejezet

Permutációcsoportok

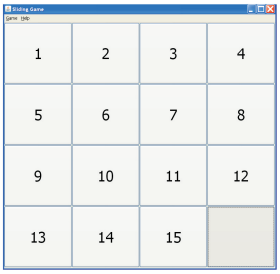
Már a 4. fejezetben, a csoportokra látott példák között megismerkedtünk a permutációcsoportokkal. Különleges fontosságukat mutatja a Cayley-tétel (4.6.), miszerint minden véges, n-edrendű csoport izomorf az S_n szimmetrikus csoport valamelyik részcsoportjával. Matematikatörténeti szerepük is jelentős, annak bizonyítása, hogy a negyedfokúnál magasabb fokú egyenletekhez nem adható meg általános megoldóképlet, a permutációcsoportok tulajdonságain alapul (bár ennek bemutatása meghaladja könyvünk kereteit).

Sorbarakások és bijektív leképezések közötti kapcsolat

Általában az $a_1, a_2, a_3, \dots a_n$ elemek egy permutációján egy sorbarakásukat értjük. Egy n elemű halmaz összes permutációnak száma annyi, ahányféleképpen sorbarakhatók az elemei, vagyis $n!$. Ebben az értelemben az a_1, a_2, a_3 elemek permutációi a következő sorrendeket jelentik:

$$a_1, a_2, a_3$$
$$a_1, a_3, a_2$$
$$a_2, a_1, a_3$$
$$a_2, a_3, a_1$$
$$a_3, a_1, a_2$$
$$a_3, a_2, a_1$$

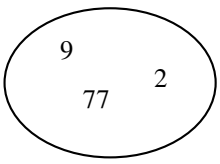
www.cs.elte.hu/~kfried/algebra3/PERMUT.EXE Program: n elem sorrendjei ($1 < n < 9$).

Egy-egy sorrend tekinthető egy permutációnak. 

függetlenül attól, hogy a_1, a_2, illetve a_3 miféle három különböző dolgot jelöl. (Ha például $a_1 = 9$, $a_2 = 77$ és $a_3 = 2$, akkor a fenti hat permutáció rendre a következő sorbarakásokat jelenti: $9, 77, 2$; $9, 2, 77$; $77, 9, 2$; $77, 2, 9$; $2, 9, 77$; $2, 77, 9$.)

Ha most azt vizsgáljuk, hogy melyek azok a bijektív leképezések, amelyek a $H = a_1, a_2, a_3$ (vagy a $9, 77, 2$) halmazt önmagára képezik le, akkor a fenti sorbarakások mindegyikének megfelel pontosan egy bijektív leképezés, mégpedig az, amelyik az adott sorbarakás első tagját rendeli a_1-hez, a másodikat a_2-höz, a harmadikat a_3-hoz. Vagyis ha megadjuk a halmaz elemeinek egy kitüntetett sorrendjét, – és amikor a halmaz elemeit valahogy felsoroltuk, akkor ezzel éppen egy kitüntetett sorrendet adtunk meg, ennek alapján neveztük az „első” elemet a_1-nek, a „másodikat” a_2-nek, a „harmadikat” a_3-nak –, akkor ehhez a sorrendhez képest minden sorbarakásnak megfelel egy bijektív leképezés és viszont. Ez adott lehetőséget arra, hogy a permutációkat bijektív leképezésekként definiáljuk.

Vegyük észre, hogy csak véges halmazok bijekciót tekintettük. Végtelen halmazok önmagára való bijekciót általában nem szokás permutációnak nevezni.

$H =$ 

Kitüntetett sorrend: 9, 77, 2

Soroljuk fel az összes bijekciót az összes különböző sorbarakás alapján, amelyek (mint korábban láttuk):

$9, 77, 2$; $9, 2, 77$; $77, 9, 2$; $77, 2, 9$; $2, 9, 77$; $2, 77, 9$

Leképezések:

$$\begin{pmatrix} 9 & 77 & 2 \\ 9 & 77 & 2 \end{pmatrix} \quad \begin{pmatrix} 9 & 77 & 2 \\ 9 & 2 & 77 \end{pmatrix} \quad \begin{pmatrix} 9 & 77 & 2 \\ 77 & 9 & 2 \end{pmatrix}$$
$$\begin{pmatrix} 9 & 77 & 2 \\ 77 & 2 & 9 \end{pmatrix} \quad \begin{pmatrix} 9 & 77 & 2 \\ 2 & 9 & 77 \end{pmatrix} \quad \begin{pmatrix} 9 & 77 & 2 \\ 2 & 77 & 9 \end{pmatrix}$$

A továbbiakban az $a_1, a_2, a_3, \ldots, a_n$ elemeket (bármit is jelentsenek) általában – az egyszerűbb írásmód kedvéért – $1, 2, 3, \ldots, n$-nel fogjuk jelölni. Amikor az n elem permutációiról beszélünk, akkor ez egyrészt jelenti az $1, 2, 3, \ldots, n$-nel jelölt n elem lehetséges sorrendjeit, másrészt azokat a

$$\varphi = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \varphi(1) & \varphi(2) & \varphi(3) & \ldots & \varphi(n) \end{pmatrix}$$

bijektív leképezéseket, amelyek a kitüntett $1, 2, 3, \ldots, n$ sorrendben felsorolt elemekhez rendelik hozzá ugyanezen elemek $\varphi(1)$, $\varphi(2)$, $\varphi(3)$, …, $\varphi(n)$ sorrendjét. Így például az 1, 2, 3 elemek 2, 3, 1 sorrendjének az

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$$

bijektív leképezés felel meg.

Érdemes észrevenni, hogy ugyanazt a permutációt leképezésként többféleképpen (éppen $n!$-féleképpen) is leírhatjuk. A fenti $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$ permutáció pontosan ugyanazt jelenti, mint például a $\begin{pmatrix} 3 & 2 & 1 \\ 1 & 3 & 2 \end{pmatrix}$ leképezés, hiszen mind a három elem képe ugyanaz az egyik leképezés szerint, mint a másik szerint. A permutációk leképezéses írásmódjánál nem lényeges az, hogy a „felső sorban" milyen sorrendben soroljuk fel az elemeket, csak az, hogy minden elem alá a képét írjuk. Az $1, 2, 3, \ldots, n$ sorrendet nem az tünteti ki, hogy a „felső sorban" ilyen sorrendben írjuk az elemeket (ezt csak a könnyebb áttekinthetőség miatt szoktuk így írni, de nem kötelező), hanem az, hogy a halmaz elemeinek volt eredetileg egy sorrendje, ami szerint neveztük az elsőt 1-nek, a másodikat 2-nek stb., vagyis maguk a számok tükröznek egy eredeti kitüntetett sorbarakást.

Inverzió, permutációk paritása

Amennyiben megállapodtunk az n elem egy kitüntetett sorrendjében (alapelrendezésben), akkor beszélhetünk arról, hogy ehhez a kitüntett sorrendhez képest két elem *inverziót* alkot, vagy inverzióban áll. Ez azt jelenti, hogy

az éppen vizsgált permutációban az illető két elem egymáshoz képest nem a kitüntetett permutációban tapasztalt sorrendben követi egymást.

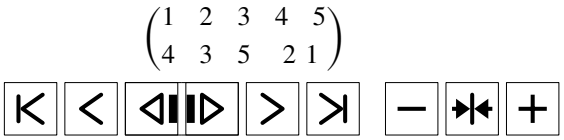
Ha például a 9, 77, 2 elemeknek ezt (a felsorolásuk szerinti) sorrendjét tüntetjük ki, akkor a 2, 77, 9 sorrendjükben inverzióban áll a 9 a 2-vel, a 9 a 77-tel és a 2 a 77-tel, vagyis ebben a permutációban az inverziók száma 3. Ha a 2, 9, 77 sorrendet tüntetjük ki, akkor ugyanebben a 2, 77, 9 sorrendben csak a 9 és a 77 alkot inverziót, vagyis az inverziók száma 1. Önmagában tehát nincs értelme arról beszélni, hogy (sorbarakásként felfogva) egy permutációban mely elemek állnak inverzióban, vagy hány inverzió van, csak egy előre megadott sorrendhez képest.

Ha pusztán annyit kérdezek, hogy (leképezésként felfogva) a $\begin{pmatrix} 9 & 77 & 2 \\ 9 & 2 & 77 \end{pmatrix}$ permutációban mely elemek állnak inverzióban, ez éppen olyan értelmetlen kérdés, hiszen nem ismerjük a kitüntetett alapelrendezést. Ha ez a 9, 77, 2 sorrend volt, akkor a $\begin{pmatrix} 9 & 77 & 2 \\ 9 & 2 & 77 \end{pmatrix}$ leképezés a 9, 2, 77 sorrendnek felel meg, amelyben 1 az inverziók száma (a 2 inverzióban áll a 77-tel). Ha az alapelrendezés a 2, 9, 77 volt, akkor mivel $\begin{pmatrix} 9 & 77 & 2 \\ 9 & 2 & 77 \end{pmatrix} = \begin{pmatrix} 2 & 9 & 77 \\ 77 & 9 & 2 \end{pmatrix}$, ugyanez a leképezés a 77, 9, 2 sorrendnek felel meg, amelyben 3 inverzió van.

Ahhoz tehát, hogy egy adott permutáció esetén (akár sorbarakásként, akár leképezésként képzeljük el) inverziókról beszéljünk, szükség van egy alapelrendezésre. Akkor, amikor egy n elemű halmaz elemeit 1, 2, 3, ... n-nel jelöljük, ezzel kitüntetjük az elemek egy sorrendjét. Célszerű ezt a névadást éppen az alapelrendezésnek megfelelően megtenni, vagyis a halmaz elemeit épp abban a felsorolásban megadni, amit alapelrendezésnek szeretnénk tekinteni az inverziók vizsgálatakor. Ennek alapján ha például a $\begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix}$ permutációról beszélünk, akkor feltételezhetjük, hogy a névadás éppen az alapelrendezésnek megfelelően történt, vagyis hogy a kitüntetett sorrend az 1, 2, 3. Ekkor a $\begin{pmatrix} 3 & 1 & 2 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ permutációnak az 1, 3, 2 sorrend felel meg, amelyben a 2 és a 3 alkotja az egyetlen inverziót. (Amennyiben valaki mégsem az $1, 2, \ldots, n$ sorrendhez képest szeretné vizsgálni az inverziókat, akkor ezt megteheti, feltéve, hogy megad egy másik kitüntetett sorrendet. Ha például a 2, 1, 3 sorrendet tünteti ki, akkor a fenti permutációnak a 3, 1, 2 sorrend fog megfelelni, melyben a 2, 1, 3 kitüntetett sorrendhez képest az inverziók száma 3 (mindegyik mindegyikkel).)

Egy permutációt *párosnak* nevezünk, ha benne (az alapelrendezéshez képest) páros sok elempár alkot inverziót. *Páratlannak,* ha az inverziók száma páratlan.

Például az 1, 2, 3, 4, 5 alapsorrendhez képest az $\begin{pmatrix}1&2&3&4&5\\4&3&5&2&1\end{pmatrix}$ permutációban az inverziók száma 8 (1–2, 1–5, 1–3, 1–4, 2–5, 2–3, 2–4, 3–4), így páros.



7.1. ábra. Az inverziók leszámlálása

Belátható, hogy ha egy permutációban két elemet felcserélünk, akkor a permutáció paritása megváltozik. (Ha két szomszédos elemet cserélünk fel, akkor ha eredetileg nem álltak inverzióban, akkor a csere után inverziót alkotnak, a többi elemhez viszonyított helyzetük pedig nem változik, így az inverziók száma 1-gyel nő; ha pedig eredetileg inverzióban álltak, akkor ez a cserével megszűnik, így az inverziók száma 1-gyel csökken. Mindenképpen 1-gyel változik, így biztos, hogy a paritás változik. Nem szomszédos elemek cseréje estén meggondolható, hogy ha az n-edik és az $n+k$-adik elemet akarjuk felcserélni, akkor ez megoldható $2k-1$ – tehát páratlan sok – lépésben úgy, hogy minden lépésben a szóbanforgó elemek valamelyikét egy szomszédjával cseréljük fel. Az inverziók száma ilyenkor is páratlan számmal változik, ami megváltoztatja paritását.)

Érdemes meggondolnunk, hogy mit jelent két elem cseréje, ha a permutációt leképezésként képzeljük el.

Például:

A kitüntetett sorrend (alapelrendezés): 1, 2, 3, 4, 5.

Tekintsük a 4, 3, 5, 2, 1 sorrendet, és cseréljük ki a 4-et és a 2-t. A 2, 3, 5, 4, 1 sorrendet kapjuk.

A 4, 3, 5, 2, 1 permutáció leképezésként felírva: $\begin{pmatrix}1&2&3&4&5\\4&3&5&2&1\end{pmatrix}$.

A 2, 3, 5, 4, 1 permutáció leképezésként felírva: $\begin{pmatrix}1&2&3&4&5\\2&3&5&4&1\end{pmatrix}$.

Vegyük észre, hogy

$$\begin{pmatrix}1&2&3&4&5\\4&3&5&2&1\end{pmatrix}\cdot\begin{pmatrix}1&2&3&4&5\\4&2&3&1&5\end{pmatrix}=\begin{pmatrix}1&2&3&4&5\\2&3&5&4&1\end{pmatrix},$$

vagyis az első és a negyedik elem felcserélésével keletkező permutációt megkaptuk úgy is, hogy az eredeti permutációt megszoroztuk jobbról azzal a

leképezéssel, amely az 1-et a 4-be, a 4-et az 1-be viszi, a többi elemet helyben hagyja. Ez a permutáció ugyanis úgy hat az eredetire, hogy annak felső sorában felcseréli az 1-et a 4-gyel:

$$\begin{pmatrix} 4 & 2 & 3 & 1 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix},$$

hiszen az általa létrehozott képekre kell alkalmaznunk az eredeti permutációnak megfelelő leképezést. Általában is igaz az, hogy ha n elem valamelyik permutációjában felcseréljük az a-adik és a b-edik elemet, akkor az eredményt úgy is megkaphatjuk, hogy a szóbanforgó permutációt (mint leképezést) megszorozzuk jobbról az $\begin{pmatrix} 1 & 2 & \dots & a & \dots & b & \dots & n \\ 1 & 2 & \dots & b & \dots & a & \dots & n \end{pmatrix}$ permutációval (amelynek éppen az a sorrend felel meg, amit az alapelrendezésből kapunk a szóbanforgó két elem felcserélésével).

Azt is észrevehetjük, hogy

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 3 & 2 & 5 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 5 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 5 & 4 & 1 \end{pmatrix},$$

vagyis ugyanezt az eredményt úgy is megkaphatjuk, hogy az eredeti permutációt megszorozzuk balról azzal a leképezéssel, amely az alapelrendezéshez képest a 2-est a 4-esbe, a 4-est a 2-esbe viszi, a többieket változatlanul hagyja. Most ugyanis az eredeti permutációt hajtjuk végre először, majd a kapott képek között a 2-est és a 4-est felcseréljük. Általában ez most is egy

$$\begin{pmatrix} 1 & 2 & \dots & a & \dots & b & \dots & n \\ 1 & 2 & \dots & b & \dots & a & \dots & n \end{pmatrix}$$

alakú permutációval való szorzást jelent, de most balról, és míg az előbb az adott permutációban az a-adik és a b-edik elemet (első és negyedik) akartuk felcserélni, most az a számot a b számmal (2 és 4). Ez az alapelrendezésben tetszőleges a és b esetén egybeesik (ott éppen a az az a-dik és b a b-edik szám), általában azonban nem.

Permutációk paritását vizsgálva megfigyelhetjük, hogy n elem összes permutációi között ugyanannyi a páros, mint a páratlan (vagyis akár a páros, akár a páratlan permutációk száma $n!/2$).

Például négy elem esetén (1, 2, 3, 4 alapelrendezést feltételezve):

Párosak:		Páratlanok:	
	1, 2, 3, 4 (0 inverzió)		2, 1, 3, 4 (1 inverzió)
	1, 3, 4, 2 (2 inverzió)		3, 1, 4, 2 (3 inverzió)
	1, 4, 2, 3 (2 inverzió)		4, 1, 2, 3 (3 inverzió)
	2, 1, 4, 3 (2 inverzió)		1, 2, 4, 3 (1 inverzió)
	2, 3, 1, 4 (2 inverzió)		3, 2, 1, 4 (3 inverzió)
	2, 4, 3, 1 (4 inverzió)		4, 2, 3, 1 (5 inverzió)
	3, 1, 2, 4 (2 inverzió)		1, 3, 2, 4 (1 inverzió)
	3, 2, 4, 1 (4 inverzió)		2, 3, 4, 1 (3 inverzió)
	3, 4, 1, 2 (4 inverzió)		4, 3, 1, 2 (5 inverzió)
	4, 1, 3, 2 (4 inverzió)		1, 4, 3, 2 (3 inverzió)
	4, 2, 1, 3 (4 inverzió)		2, 4, 1, 3 (3 inverzió)
	4, 3, 2, 1 (6 inverzió)		3, 4, 2, 1 (5 inverzió)

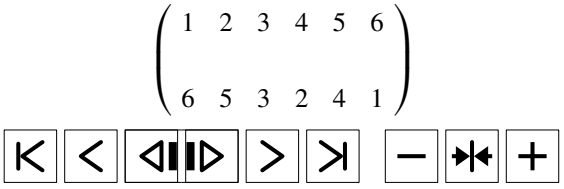
(Általában is igaz, hogy ha felsoroljuk az összes páros permutációt, akkor megkaphatjuk az összes páratlant úgy, hogy a párosakban az első két elemet felcseréljük. Két elem cseréje mindig megváltoztatja a paritást, így ezáltal a párosokból páratlanokat fogunk kapni. Másrészt, ha volna olyan páratlan, amit így nem kaptunk meg, akkor abban felcserélve az első két elemet, olyan páros permutációt kellene kapnunk, ami nem szerepelt a felsorolásban. Márpedig az összeset felsoroltuk, így ez nem lehetséges. Tehát mindig ugyanannyi a páros permutációk száma, mint a páratlanoké, vagyis az összes permutációk fele páros, fele páratlan.)

Ciklusok, transzpozíciók

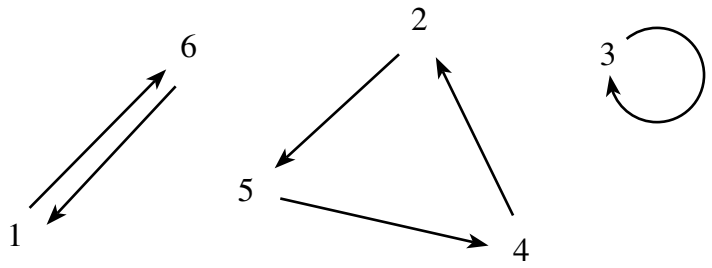
Mint azt a 4. fejezet elején láttuk, ha egy n elemű halmazt önmagára vivő bijektív leképezéseknek tekintjük a permutációkat, akkor a halmaz összes permutációi között a leképezések szorzása értelmes művelet, amelyre nézve az összes permutáció P_n halmaza csoportot alkot. A továbbiakban az n elemű halmaz elemeit $1, 2, 3, \ldots, n$-nel fogjuk jelölni, és ezt a sorrendjüket fogjuk egyben alapelrendezésnek is tekinteni. Elvileg a permutációknak ez a definíciója kiterjeszthető végtelen halmazokra is – egy végtelen alaphalmaz esetén is csoportot alkotnak a halmazt önmagára vivő bijektív leképezések a leképezések szorzására (a valós számokon értelmezett lineáris függvények például egy ilyen csoportnak alkotják részcsoportját) – de mi a továbbiakban csak véges permutációcsoportok vizsgálatára szorítkozunk.

A permutációkat irányított gráfokkal is ábrázolhatjuk úgy, hogy a H halmaz elemeit tekintjük a gráf csúcsainak, és minden csúcsot összekötünk a képével, az ős felől a kép felé irányítva az összekötő élt. Például az $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix}$ permutációt szemlélteti a 7.2. animáció és a 7.3. ábra.

Megfigyelhetjük, hogy minden elemből pontosan egy nyíl indul ki, és mindegyikbe pontosan egy fut be, és hogy az ábra diszjunkt körökből tevődik össze, a permutáció egyértelműen jellemezhető az $(1,6)$, $(2,4,5)$, (3) körökkel.



7.2. ábra. A ciklusok meghatározása



7.3. ábra.

Tapasztalataink általánosíthatóak:

Mindig igaz, hogy mivel leképezésről van szó, minden elemnek pontosan egy képe van, így minden pontból egy nyílnak kell kiindulna, és mivel a leképezés bijektív, képelemként is minden elem pontosan egyszer fordul elő, így minden pontba pontosan egy nyílnak kell befutnia. Ha most egy kiválasztott pontból elindulunk a belőle kiinduló nyilat követve, akkor a képéből megint tovább tudunk menni egy nyíl mentén, és így tovább, véges sok elemről lévén szó, előbb-utóbb visszaérünk a kiindulási pontba, bezárva ezzel egy kört. Lehet, hogy mindjárt az első lépésben; ha a kiindulási pont olyan elemnek felelt meg, amelynek képe önmaga, akkor egy olyan (triviális) kört kapunk, amely csak egy pontot tartalmaz. Az is lehet, hogy csak akkor, amikor már minden elemet útbaejtettünk; az összes elem egyetlen körre fűződik fel. (Ilyen például az $\begin{pmatrix}1&2&3&4&5&6\\6&5&1&2&3&4\end{pmatrix}$ permutáció.) Ha visszaértünk a kiindulópontba, akkor választunk egy olyan elemet, amit még nem érintettünk utunk során, és az abból kiinduló nyíl mentén elindulva, majd a képéből – majd annak képéből, és így tovább –, kiinduló nyíl mentén folytatva, előbb-utóbb újabb kör fog bezáródni. Ezt ismételjük, ameddig még van kimaradó elem, míg

végül az összes elemet tartalmazni fogja valamelyik kör. Azt, hogy a körök diszjunktak lesznek, az garantálja, hogy minden pontból egy nyíl indul ki és egy fut be, így utunk során csak egyszer haladhattunk át rajta.

Vannak oylan permutációk, amelyek gráfja – a triviális egyelemű köröket (azaz a hurokéleket) nem számítva – mindössze egyetlen kört tartalmaz. (Olyan is van, nevezetesen az identikus leképezés, amelyik egyet sem.) Az ilyen permutációkat – függetlenül attól, hogy hány pontból áll a kör – szokás ciklikus permutációknak, vagy ciklusoknak nevezni. Ilyen például az $\begin{pmatrix}1&2&3&4&5&6\\6&2&3&4&5&1\end{pmatrix}$ vagy az $\begin{pmatrix}1&2&3&4&5&6\\1&5&3&2&4&6\end{pmatrix}$ permutáció. (Érdemes észrevenni, hogy a fenti példában szereplő $\begin{pmatrix}1&2&3&4&5&6\\6&5&3&2&4&1\end{pmatrix}$ permutáció épp e kettő szorzata.)

7.1. Definíció. Az

$$\begin{pmatrix}i_1&i_2&\dots&i_{k-1}&i_k&i_{k+1}&\dots&i_n\\i_2&i_3&\dots&i_k&i_1&i_{k+1}&\dots&i_n\end{pmatrix}$$

alakú permutációt *ciklikus permutációnak* vagy (k-tagú) *ciklusnak* nevezzük, és $(i_1, i_2, \dots, i_k)$-val jelöljük.

Például:

$$\begin{pmatrix}1&2&3&4&5&6\\6&2&3&4&5&1\end{pmatrix}=\begin{pmatrix}1&6&2&3&4&5\\6&1&2&3&4&5\end{pmatrix}=(1,6)$$

$$\begin{pmatrix}1&2&3&4&5&6\\1&5&3&2&4&6\end{pmatrix}=\begin{pmatrix}2&5&4&1&3&6\\5&4&2&1&3&6\end{pmatrix}=(2,5,4)$$

A kéttagú ciklusokat szokás *transzpozícióknak* nevezni.

7.1. Tétel. *Minden permutáció – a tényezők sorrendjétől eltekintve – egyértelműen írható fel páronként diszjunkt ciklusok szorzataként.*

Bizonyítás. A tétel indoklását már az irányított gráfokkal való ábrázolás kapcsán láttuk, a

$$\varphi=\begin{pmatrix}1&2&3&\dots&n\\\varphi(1)&\varphi(2)&\varphi(3)&\dots&\varphi(n)\end{pmatrix}$$

permutáció esetén az 1-ből indulva az

$$1, \varphi(1), \varphi(\varphi(1)), \varphi(\varphi(\varphi(1)))\dots$$

sorozatban előbb-utóbb újra elő fog fordulni az 1 (mert véges sok elemünk van, és a bijektivitás miatt az ismétlődés előtt minden elem legfeljebb egyszer fordulhat elő), és ezzel lezárul egy ciklus. Válasszunk ekkor egy új, az előbbi ciklusban nem szereplő a elemet. Az előbbiekhez hasonlóan, az $a, \varphi(a), \varphi(\varphi(a)) \dots$ sorozatot folytassuk addig, amíg az a meg nem ismétlődik, előállítva ezzel a következő ciklust. Mivel minden elemnek pontosan egy képe és pontosan egy őse van, ebben a ciklusban nem szerepelhet olyan elem, amelyik már az előzőben is szerepelt, tehát s két ciklus diszjunkt lesz. Ezt az eljárást folytatjuk addig, míg ki nem merítettük a halmaz összes elemét. Az egyértelműség ugyancsak a bijektivitásból következik. □

Például:

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix} = (1,6) \cdot (2,5,4) \cdot (3)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1) \cdot (2) \cdot (3) \cdot (4) \cdot (5) \cdot (6)$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 2 & 1 & 3 \end{pmatrix} = (1,6,3,4,2,5)$$

Próbálja ki az 1–9 számok egy permutációját diszjunk ciklusokra bontó `www.cs.elte.hu/~kfried/algebra3/permcikl.exe` programot.

Megjegyzés. Az egytagú ciklusokat nem mindig szokás kiírni, így például az

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 3 & 2 & 4 & 1 \end{pmatrix} = (1,6) \cdot (2,5,4),$$

az identikus leképezés esetén pedig az

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 3 & 4 & 5 & 6 \end{pmatrix} = (1)$$

alak is elfogadható.

7.2. Tétel. *Minden permutáció felírható transzpozíciók szorzataként.*

Bizonyítás. Könnyen ellenőrizhető, hogy tetszőleges $(i_1, i_2, i_3, \dots, i_k)$ ciklus esetén $(i_1, i_2, i_3, \dots, i_k) = (i_1, i_2) \cdot (i_2, i_3) \cdot \dots \cdot (i_{k-1}, i_k)$, így minden ciklus felírható transzpozíciók szorzataként. Az előző tételből viszont tudjuk, hogy minden permutáció felírható ciklusok szorzataként. □

Megjegyzés. Például a $(2,5,4)$ ciklus a helyben maradó elemeket kihagyva a felírásból a $\begin{pmatrix} 2 & 5 & 4 \\ 5 & 4 & 2 \end{pmatrix}$ permutációt, a $(2,5)$ transzpozíció a $\begin{pmatrix} 2 & 5 & 4 \\ 5 & 2 & 4 \end{pmatrix}$

permutációt, az $(5,4)$ transzpozíció a $\begin{pmatrix} 2 & 5 & 4 \\ 2 & 4 & 5 \end{pmatrix}$ jelenti. Azt, hogy $(2,5,4) = (2,5)\cdot(5,4)$, úgy is elképzelhetjük, hogy az érintett elemek $2,5,4$ sorrendjéből úgy is megkaphatjuk az $5,4,2$ sorrendet, hogy először felcseréljük (az $(5,4)$ transzpozíciónak megfelelően) az 5-öt a 4-gyel, majd az így kapott $2,4,5$ sorozatban felcseréljük (a $(2,5)$ trnaszpozíciónak megfelelően) a 2-t az 5-tel.

Egyébként a tétel állításánál több is igaz, ezt a 7.4. Tételben fogjuk látni.

Érdemes észrevenni, hogy általában az, hogy egy permutációt balról megszorzunk egy (a,b) transzpozícióval, azt eredményezi, hogy az adott permutáció képelemeinek sorrendjéhez képest az eredmény képelemei között az a és a b kicserélődik:

$$(a,b)\cdot\begin{pmatrix} 1 & 2 & \dots & x & \dots & y & \dots & n \\ \varphi(1) & \varphi(2) & \dots & \varphi(x)=a & \dots & \varphi(y)=b & \dots & \varphi(n) \end{pmatrix} =$$

$$= \begin{pmatrix} 1 & 2 & \dots & x & \dots & y & \dots & n \\ \varphi(1) & \varphi(2) & \dots & b & \dots & a & \dots & \varphi(n) \end{pmatrix}.$$

Tételünk szemléletes tartalma az, hogy az $1,2,3,\dots n$ elemek tetszőleges sorrendje előállítható megfelelő számú lépésben úgy, hogy egy lépés során mindig két elemet cserélünk ki. (Lásd például a 7.1. ábrán látható animációt.)

Ebből a szemléletes tartalomból az is világos, hogy amikor transzpozíciók szorzataként állítunk elő egy permutációt, akkor ez az előállítás egyáltalán nem egyértelmű, sőt, mindig végtelen sokféleképpen tehető meg, hiszen például a 2-t és az 5-öt úgy is kicserélhetem egymással, hogy először az 5-öt kicserélem egy tetszőleges elemmel, azután a 2-vel, majd a 2-t azzal az elemmel, amelyikkel az első lépésben az 5-öt cseréltem ki. Általában: $(a,b) = (a,x)\cdot$ $\cdot\,(a,b)\cdot(x,b)$ (és e három transzpozíció bármelyike szintén felírható három transzpozíció szorzataként és így tovább).

Így az sem egyértelmű, hogy egy permutáció transzpozíciók segítségével felírt alakjában hány transzpozíció szorzata fog szerepelni. Azt azonban elmondhatjuk, hogy a páros permutációk mindig páros sok transzpozíció, a páratlan permutációk pedig mindig páratlan sok transzpozíció szorzataként fognak előállni. A transzpozíciók ugyanis éppen két elem cseréjét jelentik, és azt már korábban láttuk, hogy két elem cseréje megváltoztatja egy permutáció paritását. Páros sok változatás, azaz páros sok transzpozíció összeszorzása megtartja a paritást, páratlan sok megváltoztatja.

Úgy képzelhetjük el a dolgot, hogy az identikus leképezésnek megfelelő permutációt szorozzuk meg különféle transzpozíciókkal egészen addig, míg a vizsgálni kívánt permutációhoz nem jutunk. A vizsgált permutáció egyrészt éppen e transzpozíciók szorzata lesz, másrészt ezek a transzpozíciók annyi-

szor változtatták meg az identikus leképezés paritását, ahányan voltak. Az identikus leképezés pedig nyilván páros.

7.3. Tétel. *A P_n permutációcsoportban a páros permutációk részcsoportot alkotnak, és ez a részcsoport normálosztó.*

Bizonyítás. Azt, hogy két páros permutáció szorzata is páros, belátjuk például úgy, hogy ha mindkettőt felírjuk transzpozíciók szorzataként, akkor külön-külön mindkettőjük páros sok tényező szorzata lesz, szorzatuk megkapható e páros + páros = páros sok tényező szorzataként. A páros permutációk részhalmaza tehát zárt a permutációszorzásra.

A permutációcsoport egységeleme, az identikus leképezés szintén páros, így az egységelem is benne van a halmazban.

Belátjuk, hogy páros permutációk inverze páros. Ezt meggondolhatjuk például úgy, hogy mivel minden transzpozíció önmagának az inverze, egy permutáció inverze előállítható úgy, hogy a benne szereplő transzpozíciókat fordított sorrendben szorozzuk össze.

Tehát a páros permutációk halmaza részcsoport. Az, hogy normálosztó is, azon múlik, hogy a páros permutációk részcsoportjának a rendje éppen a fele a csoport rendjének (ugyanis mint már láttuk, a páros és páratlan permutációk száma megegyezik), és azt már tudjuk (lásd a normálosztókra a 5.2. Definíciót követően írt példákat), hogy az ilyen tulajdonságú részcsoportok mindig normálosztók. □

7.4. Tétel. *Bármely permutáció felbontható $(1, i)$ alakú transzpozíciók szorzataként. A felbontás – természetesen – itt sem egyértelmű, a tényezők számának paritása azonban igen.*

Bizonyítás. Először vizsgáljuk azt az esetet, amikor a permutáció ciklus, mégpedig olyan ciklus, amelyben nincsenek helyben maradó elemek: $(a_i, a_{i+1}, \ldots, a_n, 1, 2, \ldots, a_{i-1})$.

Az 1 elemet rendre felcserélgetve az a_n, a_{n-1}, …, a_i, a_{i-1}, …, 3, 2 elemekkel, a ciklus „1-gyel jobbra lép”, vagyis az $(a_{i-1}, a_i, \ldots, a_{n-1}, 1, 2, \ldots, ai + 1)$ ciklust kapjuk. Ezt még a_{i-1}-szer végrehajtva az identikus permutációt kapjuk.

Ha a ciklusban szerepel az 1-es, akkor függetlenül attól, hogy milyen elemek ciklusáról van szó, elvégezhetjük ugyanezt az eljárást. A végeredmény az adott részhalmaz identikus permutációja lesz.

Most vizsgáljuk azt, amikor a permutáció több diszjunkt ciklus szorzataként áll elő:

$$\pi = (a_{i_1}, a_{i_1+1}, \ldots, a_{i_1-1})(a_{i_2}, a_{i_2+1}, \ldots, a_{i_2-1}) \ldots (a_{i_k}, a_{i_k+1}, \ldots, a_{i_k-1})$$

Vegyük előre azt a tényezőt, amelyben benne van az 1. (Ezt megtehetjük, mert a felbontás a tényezők sorrendjétől függetlenül egyértelmű.) Ezt a tényezőt ezután felírjuk $(1, i)$ alakú transzpozíciók szorzataként úgy, ahogyan azt az előző lépésben is láttuk.

Ha a következő ciklusban a legkisebb elem az a_{i_2+j}, akkor végezzük el az $(1, a_{i_2+j})$ transzpozíciót, majd rendezzük a második ciklust az elsőben végzett eljáráshoz hasonlóan, végül végezzük el ismét a $(1, a_{i_2+j})$ transzpozíciót.

Ezt az eljárást ismételjük addig, amíg minden cikluson végig nem érünk.

Ezzel tehát a ciklusokat $(1, i)$ alakú transzpozíciók segítségével az identikus permutációba vittük.

Az ebben a modellben elvégzett transzpozíciók számát meg tudjuk mondani $(a_{i_1} \cdot (i_1 - 1) + 1 + a_{i_2} \cdot (i_2 - 1) + 1 + \ldots + 1 + a_{i_k} \cdot (i_k - 1) + 1)$, de ez lényegtelen. A transzpozíciók számának paritása viszont egyértelmű, ahogyan ezt már korábban láttuk (7. oldal). □

Megjegyzés. Természetesen az előző tételre adott bizonyítás messze nem a legegyszerűbb. Egy jól felépített konstrukció szemléletesebb, követhetőbb is. Egy ilyet mutatunk most. (Ebben általában a lépésszám is nyilván jóval kevesebb lesz.)

Bizonyítás. Az eljárás a következő lesz. A legnagyobbtól kezdve (n) a legkisebbig (1) sorban a helyükre visszük az elemeket.

Tegyük fel, hogy a k-nál nagyobb elemek a helyükön vannak, a k-t akarjuk a helyére vinni; az 1-est az l-hez rendeljük, és a k-hoz az m-et (lásd a kiinduló permutációt alább).

Először cseréljük fel az 1-est az m-mel, majd az 1-est a k-val, tehát a

$$\begin{pmatrix} 1 & 2 & \ldots & a_k & \ldots & l & \ldots & k & k+1 & \ldots & n \\ a_1 & a_2 & \ldots & k & \ldots & 1 & \ldots & m & k+1 & \ldots & n \end{pmatrix}$$

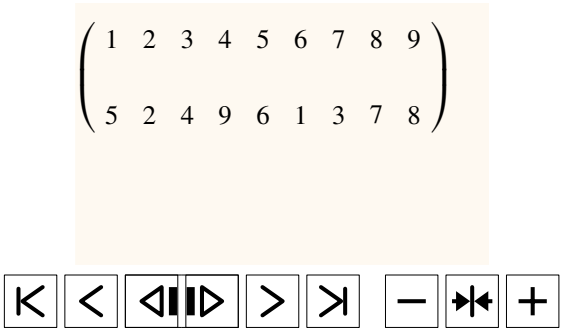
permutációból kiindulva a

$$(1,k) \cdot (1,m) \cdot \begin{pmatrix} 1 & 2 & \ldots & a_k & \ldots & l & \ldots & k & k+1 & \ldots & n \\ a_1 & a_2 & \ldots & k & \ldots & 1 & \ldots & m & k+1 & \ldots & n \end{pmatrix} = \begin{pmatrix} 1 & 2 & \ldots & a_k & \ldots & l & \ldots & k & k+1 & \ldots & n \\ a_1 & a_2 & \ldots & 1 & \ldots & m & \ldots & k & k+1 & \ldots & n \end{pmatrix}$$

permutációt kapjuk.

Ezzel a módszerrel egyesével a helyére visszük az egyes elemeket – mindegyiket legfeljebb 2 lépésben (végül az 1 automatikusan a helyére kerül) –, így legfeljebb $(n-1) * 2$ cserét, azaz transzpozíciót végeztünk. □

Az eljárást egy konkrét animáción is bemutatjuk (7.4. ábra).



7.4. ábra.

Feladatok

1. Határozza meg a következő permutációk inverzióinak számát, a permutációk paritását!

   (a) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 5 & 4 & 3 \end{pmatrix}$ (b) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 6 & 1 & 5 & 3 & 4 \end{pmatrix}$

   (c) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 5 & 4 & 3 & 2 & 1 \end{pmatrix}$ (d) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 6 & 1 & 2 & 3 & 4 & 5 \end{pmatrix}$

2. (a) Bontsa diszjunkt ciklusok szorzatára az előző feladat permutációit!

   (b) Írja fel őket transzpozíciók szorzataként!

   (c) Írja fel mindegyiket $(1, i)$ típusú transzpozíciók szorzataként!

   (d) Állapítsa meg a permutációk (mint csoportelemek) rendjét!

3. Végezze el a következő műveleteket!

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}^2, \qquad \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 3 & 2 & 1 \end{pmatrix}^3$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 5 & 2 & 4 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 4 & 3 & 5 & 1 \end{pmatrix}$$

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 4 & 5 & 2 & 3 \end{pmatrix}^2 \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}^3$$

4. Tekintse D_3 műveleti táblázatát (4.1. táblázat). Helyettesítse az egyes transzformációkat az 1, 2, 3, 4, 5, illetve 6 számokkal.

   Írja fel a kapott permutációkat.

   Határozza meg a permutációk paritását! Mit vesz észre?

5. Az ismert 15-ös játékban (tili-toli) 15 számozott négyzet mozog egy 4×4 helyet tartalmazó táblán. Az a feladat, hogy a számokat – összekeverés után – rendezzük vissza a kiinduló helyzetbe. A játék kipróbálása:

   www.cs.elte.hu/~kfried/algebra3/Sliding_Puzzle_1.0bn1.jar

   Legyen a kitüntett sorrend az 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15 és az üres hely.

   (a) Igazolja, hogy ha keverés után az üres hely továbbra is a jobb alsó helyen van, akkor a számok permutációja páros!

   (b) Igazolja, hogy ha a keverés után az üres hely az 1. vagy a 3. sorban van, akkor a számok permutációja páratlan.

6. (a) Határozza meg a $\pi_1 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$ és a $\pi_2 = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 1 & 3 & 2 & 4 & 5 \end{pmatrix}$ permutációkhoz a $\pi_1 \cdot \pi_2$ és a $\pi_2 \cdot \pi_1$ szorzatot is!

   (b) Határozza meg ennek a két permutációnak mint csoportelemnek a rendjét!

   (c) Keressen olyan σ_1, σ_2 permutációkat, amelyekre $\sigma_1 \cdot \sigma_2 = \sigma_2 \cdot \sigma_1$!

7. Igazolja, hogy páros ciklus rendje páratlan, páratlan ciklus rendje páros!

8. Igazolja, hogy páratlan permutáció rendje páros!

9. Igazolja, hogy D_3 izomorf P_3-mal!

10. Jelöljük a szabályos háromszög három csúcsát 1, 2, 3-mal. Írjuk fel az egyes transzformációkat aszerint, hogy azok az 1-hez, a 2-höz, illetve 3-hoz rendre mit rendelnek. Mit tapasztalunk?

11. Hány egymással nem izomorf 6-elemű csoportot tud felírni? (Használhatja a `www.cs.elte.hu/~kfried/algebra3/groups2-8.jar` csoportkészítő programot. A piros betű az invertálhatóság, a narancssárga színezés az asszociativitás sérülésére utaló hibát jelez.)

12. Van olyan titkosírás, amelynek során az ábécé betűit adott sorrendben összekeverjük, és a szöveg minden egyes betűjét az eredeti az ábécében elfoglalt sorszámához rendelt új sorszám szerinti betűvel helyettesítjük. Ha például az *a* betűt az *e*-be, az *z* betűt a *k*-ba viszi a keverés, akkor az *az* szóból *ek* lesz. (A szóközök a helyükön maradnak.)

    (a) Hogyan lehet kódolni egy szöveget, ha ismerjük a szöveget és a kevert ábécét?

    (b) Hogyan lehet dekódolni (visszaalakítani egy kódolt szöveget), ha ismert a kódolás és a kódolt szöveg?

    (c) Valaki úgy szeretné összetettebbé tenni a kódolást, hogy többször is elvégzi ezt a fajta kódolási eljárást. Mit szól az ötlethez?

13. Egy kódolási eljárás során a titkosítandó szöveget (szóközökkel együtt) 3 karakter hosszú részekre bontjuk (ha nem osztható 3-mal a betűk száma, akkor az utolsó néhány karaktert változatlanul leírjuk, vagy tetszőlegesen keverhetjük). A kapott 3 hosszú jelsorozatokat egy véletlenszerű permutáció szerint összekeverjük. (Választhatjuk egyszerűbb esetben azt, hogy minden részjelsorozatot ugyanazzal a keveréssel keverjük össze.)

    Dekódolja az ezzel az eljárással kódolt szöveget:

    Z EGMÉESME PRUMCTÁKÓIS ZZORTAA.

    A megoldás itt olvasható: 202

    (A jelsorozatok hosszát 3 helyett más értéknek is választhatjuk.)

8. fejezet

Gyűrűk

8.1. Definíció. Az $(R, \circ, *)$ algebrai struktúra *gyűrű*, ha

- $(R, \circ)$ kommutatív csoport,
- $(R, *)$ félcsoport
- a $*$ művelet disztibutív a $\circ$ műveletre nézve.

Ha a $*$ művelet kommutatív, akkor kommutatív gyűrűről, ha pedig a $*$ műveletnek van neutrális eleme, akkor egységelemes gyűrűről szokás beszélni. (A $\circ$ művelet neutrális elemét általában zérusnak nevezik.)

Például:

1. $(\mathbb{Z}, +, \cdot)$ egységelemes, kommutatív gyűrű.
2. A páros számok, illetve egy tetszőleges k egész szám többszörösei is a szokásos összeadással és szorzással kommutatív gyűrűt alkotnak.
3. A 0 szám önmagában az összeadásra és szorzásra szintén gyűrűt alkot, az olyan gyűrűt, amelynek csak egyetlen eleme van, szokás *null-gyűrűnek* nevezni.
4. Tetszőleges $m \geq 2$ egész szám esetén a $\bmod\ m$ maradékosztályok kommutatív, egységelemes gyűrűt alkotnak a maradékosztályok összeadására és szorzására nézve.
5. Az $a + bi$ alakú komlpex számok, ahol a és b egész (*Gauss-egészek*) a komplex számok szokásos összeadására és szorzására nézve, kommutatív, egységelemes gyűrűt alkotnak.

6. Az $a + b\sqrt{2}$ alakú valós számok, ahol a és b egész, a szokásos összeadásra és szorzásra nézve kommutatív, egységelemes gyűrűt alkotnak. Hasonlóan, az $a+b\sqrt{n}$ alakú számok halmaza, ahol a és b egész, tetszőleges rögzített n egész szám esetén a szokásos összeadásra és szorzásra kommutatív, egységelemes gyűrűt alkotnak. (Ha n négyzetszám, akkor éppen az egész számok gyűrűjét kapjuk.)

7. Egy tetszőleges test vagy gyűrű feletti polinomok gyűrűt alkotnak a polinomok összeadására és szorzására nézve. A testek feletti polinomgyűrűk mindig kommutatívak és egységelemesek.

8. Egy tetszőleges T test feletti $n \times n$-es mátrixok egységelemes gyűrűt alkotnak a mátrixok összeadására és szorzására nézve

9. Egy test feletti vektorteret önmagára vivő homogén lineáris leképezések (lineáris transzformációk) egységelemes gyűrűt alkotnak a $(\varphi+\psi)\mathbf{v} := \varphi(\mathbf{v}) + \psi(\mathbf{v})$ összeadásra és a leképezések szorzására.

10. Az egész számok halmazán definiáljuk a következő két műveletet: $a \circ b := a + b - 1$ és $a * b := a + b - ab$. Ekkor a $(\mathbb{Z}, \circ, *)$ struktúra kommutatív, egységelemes gyűrű.

11. Ha egy tetszőleges $(G, \circ)$ kommutatív csoportban úgy értelmezzük a $*$ műveletet, hogy bármelyik két elemre $a * b$ a csoport neutrális eleme (zérus) legyen, akkor $(G, \circ, *)$ kommutatív gyűrű lesz. Az ilyen típusú gyűrűket *zérógyűrűnek* nevezik.

Megjegyzés. A természetes számok halmaza az összeadásra és a szorzásra nézve nem alkot gyűrűt, mert az összeadás nem invertálható. Ezt a típusú struktúrát félgyűrűnek nevezzük, és később még ejtünk róla szót. Az egész számok az összadásra és szorzásra nézve kommutatív gyűrűt alkot.

Ebben a tananyagban korábban nem vizsgáltunk kétműveletes struktúrákat. (Tudjuk, hogy a test is kétműveletes, de egyelőre még nem vizsgáltuk.)

A két művelet tulajdonságait külön-külön írtuk fel: $(R, \circ)$ kommutatív csoport, $(R, *)$ félcsoport. A két művelet közötti kapcsolatot a $*$ művelet $\circ$ műveletre vett disztributivitás tulajdonsága jelenti. Felmerül a kérdés, hogy például az $(R, \circ)$ csoportból kiindulva nem jelent-e ez valami megkötést a $*$ műveletre nézve.

A $\circ$ művelet speciális eleme az egységeleme, vagy neutrális eleme (a zérus, jelölje n) – milyen összefüggéseket állapíthatunk meg minden gyűrűben?

Minden elemnek létezik $\circ$ szerinti inverze – milyen kapcsolatban áll ez a $*$ művelettel?

Nem lehet-e, hogy $*$ invertálhatósága is következik már a műveleti tulajdonságokból?

Mi lesz például egy tetszőleges $a*n$ szorzás eredménye? Milyen feltételekkel lehet $a*b=n$? (Vannak-e zérusosztók R-ben?) Tetszőleges elem előáll-e valamely elemek $*$ művelet szerinti eredményeként?

Ezekre a kérdésekre többnyire egyszerű a válasz, mert nem teljesülnek tetszőleges gyűrűben: ehhez elég csak egy ellenpéldát adnunk.

Például a gyűrűkre adott 2. példában a 6 nem áll elő két szám szorzataként, illetve jól láthatóan nem invertálható a szorzás.

De vannak olyan tulajdonságok, amelyeket érdemes megfigyelni, például:

8.1. Tétel. *Egy $(R,\circ,*)$ gyűrűben $\forall a,b,c\in R$ esetén érvényesek az alábbiak:*

1. $a*n=n*a=n$,
2. $(-a)*b=a*(-b)=-(a*b)$, *illetve* $(-a)*(-b)=a*b$,
3. $a*(b\circ(-c))=(a*b)\circ(-(a*c))$, *illetve* $(a\circ(-b))*c=(a*c)\circ(-(b*c))$,

ahol n a $\circ$ művelet egységeleme (neutrális eleme), vagyis a zérus, $-x$ pedig az x szám $\circ$ szerinti inverzét jelöli.

Bizonyítás. A bizonyításhoz mindenekelőtt többször a disztributivitást használjuk, valamint a $\circ$ és $*$ asszociativitását, $\circ$ invertálhatóságát.

1. Tudjuk, hogy $n=n\circ n$, tehát $a*n=a*(n\circ n)=(a*n)\circ(a*n)$, amiből a $\circ$ művelet invertálhatóságából következik, hogy $n=a*n$. Hasonlóan, $n*a=(n\circ n)*a=n*a\circ n*a$, amiből következik, hogy $n=n*a$.

2. Tudjuk, hogy $(a*b)\circ(-(a*b))=n$, és asszociatív struktúrában az inverz egyértelmű (3.2. Tétel). Mivel pedig

$$(a*b)\circ(-a)*b=(a\circ(-a))*b=n*b=n$$

az 1. állítás szerint, így $(-a)*b$ is inverze $a*b$-nek, tehát $(-a)*b=-(a*b)$.

Hasonlóan: $(a*b)\circ(a*(-b))=a*(b\circ(-b))=a*0$.

Ezek szerint pedig $(-a)*(-b)=-(-(a*b))$, egy elem inverzének inverze pedig önmaga, vagyis az állítás valóban igaz.

3. Ezek az állítások a disztributivitás és a 2. állítás alapján azonnal adódnak. □

8.1. Megjegyzés. Ezeket az összefüggéseket az $(\mathbb{Z}, +, \cdot)$ gyűrűben felírva azt kapjuk, hogy tetszőleges a, b egész számok esetén

$$a \cdot 0 = 0 \cdot a = 0,$$
$$(-a) \cdot b = a \cdot (-b) = -(a \cdot b), \qquad \text{illetve } (-a) \cdot (-b) = a \cdot b, \text{ valamint}$$
$$a \cdot (b + (-c)) = (a \cdot b) + (-(a \cdot c)), \quad \text{illetve } (a + (-b)) \cdot c = (a \cdot c) + (-(b \cdot c))$$

(vagy másképp $a \cdot (b - c) = (a \cdot b) - (a \cdot c)$ és $(a - b) \cdot c = (a \cdot c) - (b \cdot c)$).

Bármilyen magától értetődőnek is gondoljuk ezeket az összefüggéseket – mint azt az előző tételben láttuk – nem azok. Az összeadás asszociativitása, invertálhatósága (következményeként az ellentett egyértelműsége), valamint a szorzás összeadásra vett disztributivitása mind szerepet játszik a bizonyításunkban. Ezekkel az azonosságokkal ugyan már az általános iskolában megismerkedtünk, de nyilván nem adtunk rá bizonyítást. Ennek alapjául absztrakt algebrai ismereteink szolgálnak.

Érdekes kérdés, hogy nem vezethető-e le más hasonló speciális tulajdonság, amely minden gyűrűben teljesül.

Például: Lehet-e két nem zérus gyűrűbeli elem $*$ művelet szerinti eredménye n (vagyis vannak-e zérusosztópárok)?

Előfordulhat-e, hogy az $(R, \circ)$ struktúrának mindig van $*$ szerinti egységeleme is (vagy más speciális tulajdonsága)? Esetleg teljesül a kommutativitás?

Ezek azonban túl speciális tulajdonságok, és a gyűrű definíciójából nem vezethetők le. De érdemes megkülönböztetni azokat a gyűrűket, amelyek rendelkeznek ezekkel.

8.2. Definíció. A kommutatív és zérusosztómentes gyűrűket *integritási tartományoknak* nevezzük.

Megjegyzés. Vannak olyanok, akik azt is megkövetelik egy integritási tartománytól, hogy legyen egységeleme, vagyis az egységelemes, kommutatív és zérusosztómentes gyűrűket nevezik integritási tartományoknak.

Ahhoz, hogy a gyűrűk típusainak vizsgálatát leegyszerűsítsük, csak olyanokat akarunk megkülönböztetni, amelyek algebrailag is különböznek. Vagyis azonosnak tekintjük az ugyanolyan szerkezetűeket, azokat, amelyek között van művelettartó megfeleltetés – izomorfak, ahogyan korábban neveztük.

Gyűrűk (és általában azonos típusú algebrai struktúrák) izomorfiáját hasonlóan értelmezzük, mint csoportokét:

8.3. Definíció. Az $(R, +, \cdot)$ gyűrű izomorf az $(R', \circ, *)$ gyűrűvel, ha létezik olyan $\varphi\colon R \to R'$ bijektív leképezés, amelyre $\forall a, b \in R$ esetén $\varphi(a + b) = \varphi(a) \circ \varphi(b)$ és $\varphi(a \cdot b) = \varphi(a) * \varphi(b)$.

Például:

1. A $(\mathbb{Z}, +, \cdot)$ gyűrű izomorf a $(\mathbb{Z}, \circ, *)$ gyűrűvel, ha $a \circ b = a + b - 1$ és $a*b = a+b-ab$, ekkor ugyanis a $\varphi\colon n \to 1-n$ hozzárendelés rendelkezik a definíció szerinti tulajdonságokkal: bijektív és művelettartó.

2. Egy T test feletti n-dimenziós vektorteret önmagára vivő lineáris transzformációk gyűrűje izomorf a T test feletti $n \times n$-es mátrixok gyűrűjével. (Rögzítve a vektortér egy bázisát, minden leképezéshez egyértelműen hozzárendelhető a leképezés mátrixa, és a leképezések összegének, illetve szorzatának mátrixa a hozzájuk tartozó mátrixok összege, illetve szorzata.)

3. A Gauss-egészek gyűrűje izomorf az a $\mathbb{Z}$ feletti $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ alakú mátrixok gyűrűjével; a két gyűrű között a művelettartó bijekció a $\varphi\colon a+bi \to \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.

Ezekután vizsgáljuk meg, hogy a korábban látott gyűrűk közül melyek milyen speciális tulajdonsággal rendelkeznek.

Fenti példáink közül keressük meg, melyik integritási tartomány:

1. $(\mathbb{Z}, +, \cdot)$ egységelemes integritási tartomány.

2. Egy k egész szám többszöröseinek gyűrűje mindig integritási tartomány, viszont $|k| \geq 2$ esetén nincs egységeleme.

3. A null-gyűrű integritási tartomány (hiszen csak egyetlen eleme van, a 0).

4. Ha m összetett szám, akkor $(\mathbb{Z}_m, +, \cdot)$ nem zérusosztómentes, így nem integritási tartomány. (Például mod 10 esetén $\bar{2} \neq \bar{0}$ és $\bar{5} \neq \bar{0}$ de $\bar{2} \cdot \bar{5} = \bar{0}$.)

   Ha m prím, akkor $(\mathbb{Z}_m, +, \cdot)$ egységelemes integritási tartomány (sőt, mint azt később látni fogjuk, test).

5. A Gauss-egészek gyűrűje egységelemes integritási tartomány.

6. Az $a + b\sqrt{n}$ (a, b egész) alakú számok halmaza gyűrű tetszőleges n esetén egységelemes integritási tartomány (n négyzetszám esetén ez maga az egész számok gyűrűje, n negatív egész szám esetén a komplex számok egy részgyűrűgyjét kapjuk, $n = -1$-re pedig az úgy nevezett Gauss egészeket).

7. Tetszőleges test feletti polinomgyűrű egységelemes integritási tartomány. Egy R gyűrű feletti polinomgyűrű akkor és csak akkor integritási tartomány, ha R is az.

8. A T test feletti $n \times n$-es mátrixok gyűrűje nem integritási tartomány, mert a mátrixszorzás nem kommutatív (tudván, hogy T-ben van zéruselem és tőle különböző egységelem is):
   például $\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix} = \begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix}$, míg $\begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}\begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}$.
   Nem is zérusosztómentes:
   például $\begin{pmatrix}1 & 0\\ 0 & 0\end{pmatrix}\begin{pmatrix}0 & 1\\ 0 & 0\end{pmatrix} = \begin{pmatrix}0 & 0\\ 0 & 0\end{pmatrix}$.

9. A lineáris transzformációk gyűrűje egy T test feletti n-dimenziós vektortér esetén izomorf a T test feletti $n \times n$-es mátrixok gyűrűjével (a művelettartó bijekció során a transzformációkhoz hozzárendeljük egy rögzített bázisban a mátrixukat); nem is kommutatív, nem is zérusosztómentes, így nem is integritási tartomány. (Azért nem kommutatív és nem zérusosztómentes, mert a mátrixok szorzásra vett gyűrűje – amellyel izomorf – sem kommutatív és zérusosztómentes.)

10. A $(\mathbb{Z}, \circ, *)$ gyűrű (ahol $a \circ b = a + b - 1$ és $a * b = a + b - ab$) egységelemes integritási tartomány (belátható, hogy izomorf az egész számok gyűrűjével).

11. A zérógyűrűk (a null-gyűrű kivételével) nyilvánvalóan nem zérusosztómentesek, így nem integritási tartományok.

Láttuk korábban, hogy minden gyűrűben a $\circ$ művelet neutrális eleme (8.1. Tétel, 1. állítás), azaz az additív zérus, mindig egybeesik a szorzás zéruselemével.

Megjegyzés. A továbbiakban általában egy $(R, \circ, *)$ gyűrű esetén – a szokásoknak megfelelően – a $\circ$ műveletet (bármi is legyen) összeadásnak fogjuk nevezni, és $+$-szal jelöljük, a $*$ műveletet (bármi is legyen) szorzásnak fogjuk nevezni, és $\cdot$-sal (szorzással) jelöljük. (A szokásoknak megfelelően a szorzás jelét – amennyiben ez nem okozhat félreértést – többnyire elhagyjuk.) Az összeadás neutrális elemét (és egyben a szorzás zéruselemét) 0-val, az a elem

additív inverzét $-a$-val, az $a + (-b)$ elemet $a - b$-vel, a szorzás neutrális elemét 1-gyel jelöljük.

Abban is érdemes megállapodnunk, hogy ha egy műveletsorban több kijelölt művelet szerepel, és ezek elvégzésének sorrendjéről nem rendelkeztünk megfelelően elhelyezett zárójelekkel, akkor a műveletek közül először mindig a szorzásokat kell elvégezni. Tulajdonképpen ez nem lenne annyira fontos, mert például $a \cdot b + c + d$ esetében előbb is elvégezhetjük a $c + d$ összeadást, mint az $a \cdot b$ szorzást, de rendkívül komplikált lenne az a megfogalmazás, hogy azok a műveleti sorrendek a helyesek, amelyek tetszőlegesen választott operandusok esetén ugyanazt az eredményt adják, mintha a szorzásokat végeztük volna el először. Akkor fogalmaznánk kellően körültekintően, ha egy adott műveletsorban megkülönböztetnénk a szorzás tényezőit és az összeadás tagjait, és azt mondanánk: egyetlen tényezőt sem lehet tagként kezelni, csak magát a szorzatot, amelyben a tényező szerepel. Így a korábbi műveletben a és b tényezők, $a \cdot b$ szorzat, valamint c és d tagok. Ebben az értelmezésben az a lényeg, hogy tényezőt taggal nem adhatunk – vagy ha kivonás is szerepel – nem vonhatunk össze. Például az $a \cdot (b + c)$ műveletsorban a tényező, b és c tagok, míg $b + c$ tényező. Itt tehát csak b-t és c-t adhatjuk össze (ezek tagok), a-t és b-t nem (mert a tényező). Vagy $a + b \cdot c$-ben a tag, $b \cdot c$ is tag, míg b és c tényezők. Összeadni pedig csak a-t és bc-t szabad.

Ezekkel a jelölésekkel a 8.1. Tétel állításai a következőképpen írhatók:

Egy $(R, +, \cdot)$ gyűrűben $\forall a, b, c \in R$ esetén érvényesek az alábbiak:

1. $a \cdot 0 = 0 \cdot a = 0$ *(vagy* $a0 = 0a = 0$*),*
2. $(-a)b = a(-b) = -(ab)$*, illetve* $(-a)(-b) = ab$*,*
3. $a(b - c) = ab - ac$*, illetve* $(a - b)c = ac - bc$*,*

A továbbiakban azt fogjuk vizsgálni, hogy a csoportok körében tett megfigyeléseink milyen feltételek mellett lehetnek érvényesek gyűrűk körében.

8.4. Definíció. Az $(R_1, \circ, *)$ algebrai struktúra *részgyűrűje* az $(R, \circ, *)$ gyűrűnek, ha $R_1 \subseteq R$ és $(R_1, +, *)$ maga is gyűrű. Az $(R, \circ, *)$ gyűrű $(R_1, \circ, *)$ részgyűrűjét így jelöljük: $R \geq R_1$ vagy $R_1 \leq R$.

Például:

1. $(\mathbb{Z}, +, \cdot)$-nak részgyűrűje a páros számok gyűrűje, illetve egy tetszőleges egész szám összes többszöröseiből álló gyűrű.

2. A páros számok gyűrűjének részgyűrűje például a 4-gyel osztható számok gyűrűje, egy k egész szám többszöröseinek gyűrűjében részgyűrű a k egy tetszőleges többszörösének összes többszöröseiből álló gyűrű. (Általában egy gyűrű részgyűrűjének részgyűrűje az eredeti gyűrűnek is részgyűrűje.)

3. Egy null-gyűrűnek egyetlen részgyűrűje saját maga.

4. A $(\mathbb{Z}_{10}, +_{\bmod\ 10}, \cdot_{\bmod\ 10})$ maradékosztálygyűrűben például részgyűrűt alkotnak a páros maradékosztályok. Általában egy $(\mathbb{Z}_m, +_{\bmod\ m}, \cdot_{\bmod\ m})$ maradékosztálygyűrűben részgyűrűt alkotnak egy tetszőleges szám összes többszörösei által reprezentált maradékosztályok.

5. A Gauss-egészek gyűrűjének részgyűrűje az egész számok gyűrűje, továbbá részgyűrűt alkotnak például az $a+2bi$ vagy – tetszőleges k egész esetén – az $a + kbi$ alakú Gauss-egészek.

6. Az $a + b\sqrt{2}$ (a, b egész) alakú számok gyűrűjében részgyűrűt alkotnak azok az $a+b\sqrt{2}$ alakú elemek, amelyekben az a páros, a b pedig például 5-tel osztható, vagyis az $2u + 5v\sqrt{2}$ alakú számok, ahol $u, v \in \mathbb{Z}$.

7. Egy tetszőleges test (vagy gyűrű) feletti polinomgyűrűben részgyűrűt alkotnak például azok a polinomok, amelyekben a konstans tag 0.

8. Egy tetszőleges test (vagy gyűrű) feletti $n \times n$-es mátrixok gyűrűjében részgyűrűt alkotnak például azok a mátrixok, amelyekben az első sor minden eleme 0.

9. A síkot önmagára vivő homogén lineáris leképezések (lineáris transzformációk) gyűrűjében részgyűrűt alkotnak például az origó középpontú középpontos hasonlóságok. (A valós test feletti 2×2-es mátrixok gyűrűjében a középpontos hasonlóságoknak az $\begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ alakú mátrixok részgyűrűje felel meg. Egyszerűbb látni, hogy ezek a 2×2-es valós elemű mátrixok körében részgyűrűt alkotnak a mátrixösszeadás és mátrixszorzás művelettel.)

10. A $(\mathbb{Z}, \circ, *)$ gyűrűben, ahol $a \circ b = a + b - 1$ és $a * b = a + b - ab$ részgyűrűt alkotnak például a páratlan vagy a $3k + 1$ alakú egészek. (Ezt a gyűrűt a $(\mathbb{Z}, +, \cdot)$ gyűrű izomorf képeként kaptuk meg, ahol a művelettartó bijekció a $\varphi\colon n \mapsto n-1$ volt. Az új $\mathbb{Z}$ halmazban a $3k+1$ alakó elemek az eredeti $\mathbb{Z}$ halmazban a $3k$ alakú elemek felelnek meg. Azok ott a korábbaikban látottak szerint részgyűrűt alkottak.)

11. Egy $(R, \circ, *)$ zérógyűrűben $(R, \circ)$ tetszőleges részcsoportja részgyűrű lesz.

12. Tetszőleges gyűrűnek részgyűrűje maga a teljes gyűrű, illetve az egyelemű, csak a 0-t tartalmazó null-gyűrű. Ezeket *triviális részgyűrűknek* nevezzük (míg az ezektől különbözőeket – ha vannak – *valódi részgyűrűknek*). Ennek megfelelően a triviális részgyűrűt szokás nem valódi részgyűrűnek is nevezni.

Ahhoz, hogy egy $(R,+,\cdot)$ gyűrű egy R_1 komplexusáról eldöntsük, hogy részgyűrű-e, elegendő azt ellenőriznünk, hogy $(R_1,+)$ részcsoportja-e $(R,+)$-nak, illetve $(R_1,\cdot)$ részfélcsoportja-e $(R,\cdot)$-nak (hiszen ha $(R,+,\cdot)$ gyűrű, akkor a szorzás biztosan disztributív az összeadásra nézve). Ezt tükrözi a következő tétel:

8.2. Tétel. *Ha $R_1 \subseteq R$, akkor $(R_1,+,\cdot)$ akkor és csak akkor részgyűrűje az $(R,+,\cdot)$ gyűrűnek, ha $\forall a,b \in R_1$-re $a-b \in R_1$ és $ab \in R_1$.*

Bizonyítás. A tétel a részcsoportokra, illetve részfélcsoportokra vonatkozó 4.1. Tétel, illetve a 3.6. Tétel következménye. □

8.3. Tétel. *Az $(R,+,\cdot)$ gyűrű tetszőleges részgyűrűinek metszete is részgyűrű.*

Bizonyítás. A tétel a részcsoportok, illetve részfélcsoportok metszetére vonatkozó 4.3. Tétel, illetve 3.7. Tétel következménye. □

Ezen tétel alapján – a félcsoportoknál, illetve csoportoknál látottakhoz hasonló módon – most is beszélhetünk egy elem, illetve komplexus által generált részgyűrűről:

8.5. Definíció. Az $(R,+,\cdot)$ gyűrű egy *eleme vagy komplexusa által generált részgyűrűjén* a legszűkebb olyan részgyűrűjét értjük, amely tartalmazza az illető elemet, illetve komplexust.

Például:

1. $(\mathbb{Z},+,\cdot)$-ban egy tetszőleges k egész szám a k összes többszöröseiből álló részgyűrűt generálja.
2. Egy tetszőleges k egész szám többszöröseinek gyűrűjében tetszőleges l elem az l összes többszöröseinek részgyűrűjét generálja.
3. Egy null-gyűrűnek egyetlen részgyűrűje van: saját maga, amelyet a null-gyűrű egyetlen eleme (a 0) generál.
4. $(\mathbb{Z}_m,+_{\bmod m},\cdot_{\bmod m})$-ban egy tetszőleges $\overline{a}$ maradékosztály által generált részgyűrű elemei az $\overline{a}$, $\overline{2a}$, $\overline{3a}$, …, $\overline{\frac{m}{(m,a)}a}$ maradékosztályok.

5. A Gauss-egészek gyűrűjében az 1 az egész számok gyűrűjét, a 2 a páros egészekét, az i a teljes gyűrűt generálja. Az $1+i$ az olyan $k+ni$ alakú elemek részgyűrűjét generálja, amelyekben a k és n paritása megegyezik. ($1+i$ együtthatóinak paritása megegyezik. Azt könnyű belátni, hogy ha a_1+b_1i és a_2+b_2i olyan számok, amelyekre a_1+b_1 és a_2+b_2 is páros egész számok – vagyis megegyezik a paritásuk –, akkor ezek összegében, különbségében és szorzatában is a valós és a képzetes rész összege páros egész szám lesz. De vajon minden ilyen $a+bi$ előáll $(1+i)$-ből alkalmas műveletekkel? $(1+i)^2 = 2i$ és $2i - 2i(1+i) = 2$. Legyen $a = 2a_1 + r_a$, $b = 2b_1 + r_b$, ahol $r_a + r_b = 0$ vagy 2, de egyik sem negatív, tehát $r_a = r_b = 0$ vagy $r_a = r_b = 1$. $2a_1$, $2b_1i$, $1+i$ pedig egyaránt előállítható $1+i$-vel.)

6. Az $a+b\sqrt{2}$ (a, b egész) alakú számok gyűrűjében az 1 az egész számok gyűrűjét, az $1+\sqrt{2}$ a teljes gyűrűt, a $\sqrt{2}$ pedig az olyan $k+n\sqrt{2}$ alakú számok gyűrűjét generálja, ahol k páros, n tetszőleges egész.

7. Egy tetszőleges test (vagy gyűrű) feletti polinomgyűrűben például az $f(x) = x$ polinom a konstans tagot nem tartalmazó egész együtthatós polinomok részgyűrűjét generálja.

8. A síkot önmagára vivő lineáris transzformációk gyűrűjében például az origó körüli 180°-os forgatás azoknak az origó középpontú középpontos nagyításoknak a részgyűrűjét generálja, amelyek arányszáma egész szám.

9. A $(\mathbb{Z}, \circ, *)$ gyűrűben, ahol $a \circ b = a + b - 1$ és $a * b = a + b - ab$, a 0 a teljes gyűrűt, az 1 – mint zéruselem – az egyelemű, triviális null-gyűrűt, a 2 a teljes gyűrűt, a 3 a páratlan számok részgyűrűjét, a 4 a $3k+1$ alakú számok részgyűrűjét, egy tetszőleges n szám az $(n-1)k+1$ alakú számok részgyűrűjét generálja. (Ezeket az $(\mathbb{Z}, +, \circ)$ gyűrűbe képező $m \mapsto m+1$ izomorfizmus segítségével láthatjuk be.)

Gyűrűk kompatibilis osztályozásai

A csoportoknál láttuk, hogy egy csoport kompatibilis osztályozásait a csoport speciális tulajdonságú részcsoportjai – a normálosztók – szerinti osztályozások adták.

Egy $(R, +, \cdot)$ gyűrű tetszőleges $(R_1, +, \cdot)$ részgyűrűje esetén az $(R, +)$ csoportnak mindig normálosztója lesz az $(R_1, +)$ részcsoport, hiszen $(R, +)$ kommutatív csoport.

Így az $(R, +, \cdot)$ egy tetszőleges részgyűrűje kompatibilis osztályozást generál az $(R, +)$ csoporton.

De vajon szükségszerűen kompatibilis lesz-e az osztályozás a szorzásra is?

Két elem szorzatának osztálya csak az osztályaiktól függ-e, azaz független lesz-e az elemek választásától?

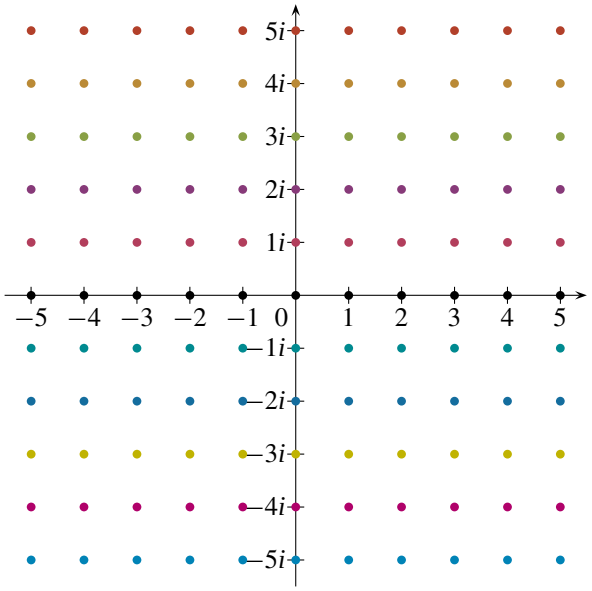
Nézzük meg most néhány példán, hogy az $(R,+)$ csoport $(R_1,+)$ részcsoport szerinti osztályozása milyen $(R_1,+,\cdot)$ részgyűrű esetén adja meg az $(R,+,\cdot)$ gyűrűnek is egy kompatibilis osztályozását (vagyis teljesül-e, hogy két elem szorzatának osztálya csak az osztályaiktól és nem az elemek megválasztásától függ), illetve milyen részgyűrűknél nem lesz kompatibilis az osztályozás!

1. $(\mathbb{Z},+,\cdot)$-ban egy tetszőleges k egész szám összes többszörösei részgyűrűt alkotnak. Ha elkészítjük a $(\mathbb{Z},+)$ csoport e részcsoport szerinti mellékosztályait, akkor a mod k maradékosztályokat kapjuk. Mivel az, hogy két szám szorzata milyen maradékot ad k-val osztva (melyik maradékosztályban lesz) nem függ attól, hogy mi volt a két szám, csak attól, hogy milyen maradékot adtak k-val osztva (mely maradékosztályokban voltak), ez az osztályozás a szorzásra nézve is kompatibilis. Vagyis a k többszöröseinek részgyűrűje szerint osztályozva az egész számok gyűrűjét, kompatibilis osztályozást kapunk.

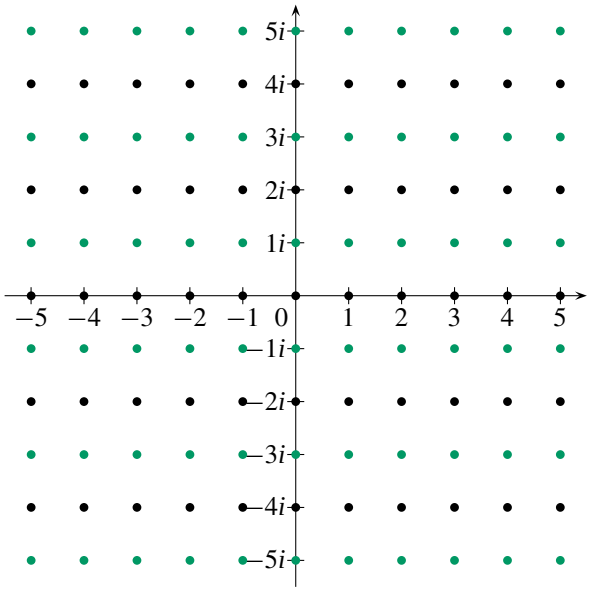
2. A Gauss-egészek gyűrűjének részgyűrűje az egész számok gyűrűje. Ha a Gauss-egészek összeadási csoportját az egész számok összeadási csoportja – mint normálosztó – szerint osztályozzuk, akkor a következő mellékosztályokat kapjuk: $\mathbb{Z}$, $\mathbb{Z}+i$, $\mathbb{Z}-i$, $\mathbb{Z}+2i$, $\mathbb{Z}-2i$, $\ldots$, $\mathbb{Z}+ki$, $\ldots$ (k egész). Ez az osztályozás a szorzásra nézve nem kompatibilis, mert például i, i, $1+i$ a $\mathbb{Z}+i$ osztály eleme, de a szorzataik különböző osztályokba esnek: $i\cdot i=-1\in\mathbb{Z}+0\cdot i$, $i(1+i)=i-1\in\mathbb{Z}+i$ (8.1. ábra).

   Hasonló a helyzet akkor is, ha az osztályozás alapjául az $a+2bi$ alakú Gauss-egészek részgyűrűjét választjuk. Ekkor két osztályt kapunk, az egyikben az $a+2bi$ alakú, a másikban az $a+(2b+1)i$ alakú Gauss-egészek lesznek. Ez az osztályozás nem kompatibilis, hiszen például a 2 is és az $1+2i$ is az $a+2bi$ alakú elemek osztályában van, de az i-szeresük két különböző osztályban van (8.2. ábra).

   Ha viszont a $2k+2ni$ alakú Gauss-egészek részgyűrűje szerint osztályozunk, akkor kompatibilis lesz az osztályozás. Négy osztályt kapunk, az egyikben lesznek azok az $a+bi$ Gauss-egészek, amelyekben a is és b is páros; egy másikban azok, amelyekben a páros, b páratlan; egy harmadikban azok, amelyekben a páratlan, b páros; a negyedikben pedig azok, amelyekben a is és b is páratlan. Az, hogy egy $(a+bi)(c+di)=(ac-bd)+(ad+bc)i$ szorzat melyik osztályban lesz,



8.1. ábra. A fekete pontok a részgyűrű elemei, az azonos mellékosztályokhoz tartozó pontokat ugyanolyan színnel színeztük. A szorzásra nézve nem kompatibilis az osztályozás.



8.2. ábra. A fekete pontok a részgyűrű elemei, az azonos mellékosztályokhoz tartozó pontokat ugyanolyan színnel színeztük. A szorzásra nézve nem kompatibilis az osztályozás.

csak attól függ, hogy a, b, c és d paritása milyen (melyik osztályban van $a+bi$, illetve $c+di$) (8.3. ábra).

3. Láttuk, hogy a Gauss-egészek gyűrűjében az $1+i$ elem által generált részgyűrű az olyan $a+bi$ alakú számok, amelyekre $a+b$ páros (108. oldal). Két osztályt kapunk: azt, amelyekben az együtthatók összege páros (ez a részgyűrű), illetve azt, amelyben páratlan (8.4. ábra).

   Ez a részgyűrű kompatibilis osztályozást ad a szorzásra nézve is, mert ha $c+di$-ben $c+d$ páros, akkor a generált részgyűrűn belül lesz minden szorzat, ha pedig páratlan, akkor $ac+bd+bc+ad=(a+b)(c+d)$ is páros. Vagyis akár a részgyűrűn belül, akár a részgyűrűn kívül van az elem, amivel szorzunk, a részgyűrűn belül lesz a szorzat. Két részgyűrűn kívül eső elemre pedig az együtthatók összege páratlan, így azok szorzatában is páratlan lesz az együtthatók összege.

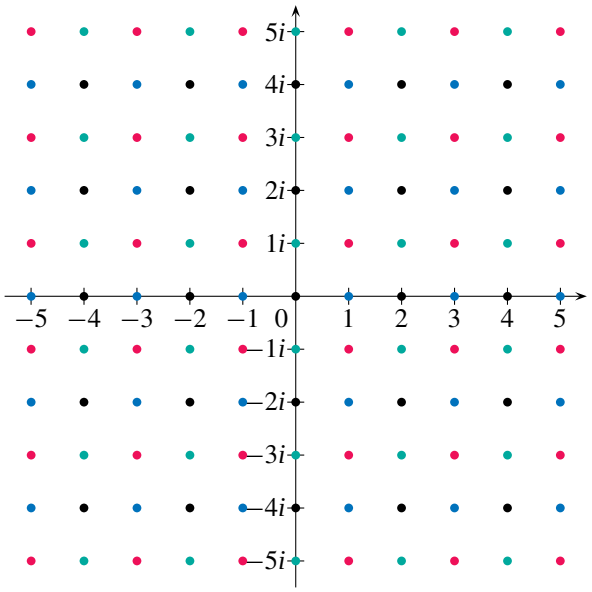
4. Az $a+b\sqrt{2}$ alakú számok (a, b egész) gyűrűjében a $2k+5n\sqrt{2}$ alakú elemek részgyűrűt alkotnak. Eszerint a részgyűrű – mint az összeadási csoport normálosztója – szerint osztályozva az $a+b\sqrt{2}$ elemeket, tíz osztályt kapunk annak megfelelően, hogy a páros-e vagy páratlan, illetve hogy b milyen maradékot ad 5-tel osztva. Ez az osztályozás nem lesz kompatibilis, mert például a $\sqrt{2}$ és a $2+\sqrt{2}$ egy osztályban van, de a $\sqrt{2}$-szeresük (a 2 és a $2+2\sqrt{2}$) két különböző osztályban van (a $\sqrt{2}$ együtthatója a 2 esetében 0, a $2+2\sqrt{2}$ esetében 2 maradékot ad 5-tel osztva).

   Ha viszont a $2k+n\sqrt{2}$ alakú számok részgyűrűje szerint osztályozunk, akkor kompatibilis lesz az osztályozás. Két osztályt kapunk, az egyikben lesznek azok az $a+b\sqrt{2}$ elemek, amelyekben az a páros, a másikban azok, amelyekben az a páratlan. Az, hogy két elem $(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+bc)\sqrt{2}$ szorzata melyik osztályban lesz, csak attól függ, hogy az illető két elem mely osztályokból való (vagyis a, illetve c paritásától).

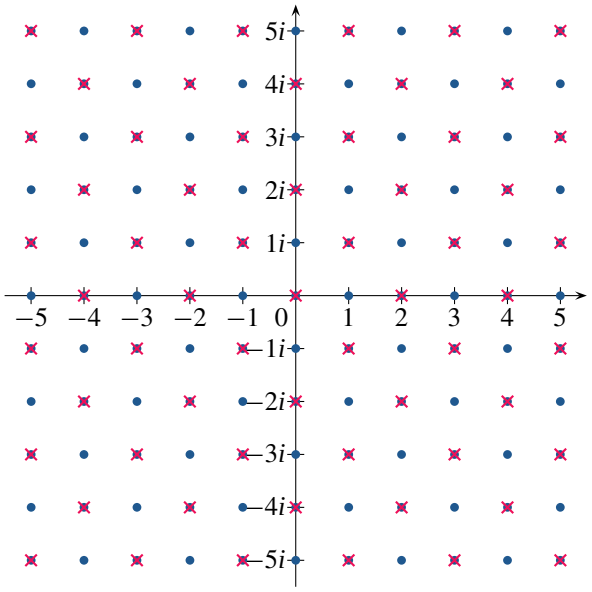
Látható, hogy ha egy $(R,+,\cdot)$ gyűrűt egy részgyűrűje – mint az összeadási csoport normálosztója – szerint osztályozunk, akkor nem minden esetben lesz az osztályozás a szorzásra nézve is kompatibilis, csak speciális részgyűrűk esetén. Ahhoz, hogy az osztályozás kompatibilis legyen, az kell, hogy akárhogy választunk is ki két azonos osztálybeli elemet, egy tetszőleges harmadik elemmel megszorozva őket, a szorzatoknak ugyanabban az osztályban kell lenniük.

Tegyük fel, hogy az R_1 részgyűrű szerinti osztályozás az R-nek egy kompatibilis osztályozását adja (a szorzás szerint is).

Ha az osztályozás kompatibilis, akkor tetszőleges $r\in R$ elemre $0\in R_1$ és $r\cdot 0=0\cdot r=0\in R_1$ miatt $r\cdot r_1\in R_1$ ($r_1\in R_1$). (Ez nagyon erős, de csak



8.3. ábra. A fekete pontok a részgyűrű elemei, az azonos mellékosztályokhoz tartozó pontokat ugyanolyan színnel színeztük. A szorzásra nézve is kompatibilis az osztályozás.



8.4. ábra. A kék pontok a Gauss-egészeket, a piros keresztek a részgyűrű elemeit jelölik – ez az osztályozás a szorzásra nézve is kompatibilis

szükséges feltétel! Azaz ha egy R_1 szerinti osztályozás kompatibilis, akkor tetszőleges $r \in R$ esetén $r * R_1 \subseteq R_1$.)

Mint később látni fogjuk, ez a feltétel elégséges is ahhoz, hogy az osztályozás kompatibilis legyen.

Ahogyan a részcsoportok között a normálosztót, úgy a gyűrűknél is az ilyen – nagyon erős feltételnek – eleget tevő részgyűrűket nevükben is megkülönböztetjük a közönséges részgyűrűktől:

8.6. Definíció. Az $(R, +, \cdot)$ gyűrű egy I részgyűrűjét *ideálnak* nevezzük, ha tetszőleges $r \in R$ esetén $rI \subseteq I$ és $Ir \subseteq I$.

Például:

1. Az egész számok $(\mathbb{Z}, +, \cdot)$ gyűrűjének minden részgyűrűje ideál.
2. Az egész számok egy tetszőleges részgyűrűjének is minden részgyűrűje ideál.
3. Maga a teljes gyűrű mint triviális részgyűrű minden gyűrűben – így egy null-gyűrűben is – ideál.
4. Tetszőleges m modulus esetén a $(\mathbb{Z}_m, +_{\bmod\ m}, \cdot_{\bmod\ m})$ maradékosztály-gyűrű minden részgyűrűje ideál.
5. A Gauss-egészek gyűrűjében – mint már láttuk – például az egész számok részgyűrűje, vagy az $a + 2bi$ alakú elemek részgyűrűje nem ideál, míg a $2k + 2ni$ alakú elemek részgyűrűje ideál.
6. Az $a + b\sqrt{2}$ alakú számok (a, b egész) gyűrűjében – mint már láttuk – például a $2k + 5n\sqrt{2}$ alakú elemek részgyűrűje nem ideál, míg a $2k + n\sqrt{2}$ alakú elemek részgyűrűje ideál.
7. Egy tetszőleges test feletti polinomok gyűrűjében például a konstans polinomok olyan részgyűrűt alkotnak, amely nem ideál. Ideál viszont például az egész együtthatós polinomok gyűrűjében azoknak a polinomoknak a részgyűrűje, amelyeknek minden együtthatója páros szám, vagy egy tetszőleges test (vagy gyűrű) feletti polinomgyűrűben azoknak a polinomoknak a részgyűrűje, amelyekben a konstans tag 0.
8. Egy tetszőleges test (vagy gyűrű) feletti 2×2-es mátrixok gyűrűjében sem az $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ alakú mátrixok részgyűrűje, sem az $\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix}$ alakú mátrixok részgyűrűje nem ideál, mert az első esetben egy $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ alakú

mátrixot jobbról megszorozva az $\begin{pmatrix}1 & 1\\ 0 & 0\end{pmatrix}$ mátrixszal (a gyűrű egy elemével) az $\begin{pmatrix}a & a\\ 0 & 0\end{pmatrix}$ mátrixot kapjuk, amely nem eleme az $\begin{pmatrix}a & 0\\ 0 & 0\end{pmatrix}$ alakú mátrixok részgyűrűjének. Hasonló a helyzet a második esetben is, ha egy $\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$ alakú mátrixot megszorzunk balról például az $\begin{pmatrix}1 & 0\\ 1 & 0\end{pmatrix}$ mátrixszal, ekkor ugyanis az $\begin{pmatrix}a & b\\ a & b\end{pmatrix}$ mátrixot kapjuk, ami nem eleme az $\begin{pmatrix}a & b\\ 0 & 0\end{pmatrix}$ alakú mátrixok részgyűrűjének. Belátható, hogy egy tetszőleges test feletti $n \times n$-es ($n \geq 2$) mátrixgyűrűnek soha nincs valódi ideálja (csak maga a teljes gyűrű vagy a gyűrű 0 elemét tartalmazó null-gyűrű)

9. Hasonló a helyzet egy T test feletti vektorteret önmagára vivő lineáris transzformációk gyűrűjében is: egyetlen valódi részcsoport sem lesz ideál.

10. A $(\mathbb{Z}, \circ, *)$ gyűrű (ahol $a \circ b = a + b - 1$ és $a * b = a + b - ab$) minden részgyűrűje ideál.

11. Egy tetszőleges zérógyűrű minden részgyűrűje ideál.

8.4. Tétel. *Egy tetszőleges gyűrű akárhány ideáljának metszete is, összege is ideál.*

Bizonyítás. Az, hogy ideálok metszete részgyűrű, következik abból, hogy az ideálok részgyűrűk, és részgyűrűk metszete is részgyűrű (8.3. Tétel). Ha I_1 és I_2 ideál, akkor a gyűrű tetszőleges r elemére $rI_1 \subseteq I_1$ és $rI_2 \subseteq I_2$, így $r(I_1 \cap I_2)$ részhalmaza lesz I_1-nek is és I_2-nek is, vagyis $I_1 \cap I_2$-nek is. Az, hogy $(I_1 \cap I_2)r$ is részhalmaza $I_1 \cap I_2$-nek, ugyanígy gondolható meg.

Az, hogy ideálok összege az összeadásra nézve csoport lesz, a normálosztók komplexusszorzatára vonatkozó 5.3. Tétel következménye (az ideálok ugyanis az $(\mathbb{R}, +)$ csoportban normálosztók, a csoportművelet az összeadás, így komplexusszorzatuk most az összegüket jelenti).

Az, hogy az ideálok összege a szorzásra is zárt (így részgyűrű) abból következik, hogy a gyűrű egy tetszőleges r elemével megszorozva $I_1 + I_2$ egy $r_1 + r_2$ alakú elemét, ahol $r_1 \in I_1$, $r_2 \in I_2$, $r(r_1 + r_2) = rr_1 + rr_2$ is eleme lesz $I_1 + I_2$-nek, hiszen I_1 és I_2 ideál, így $rr_1 \in I_1$ és $rr_2 \in I_2$. Ugyanígy gondolható meg, hogy $(I_1 + I_2)r$ is részhalmaza $I_1 + I_2$-nek. Ezek szerint részgyűrű (hiszen ha r eleme $I_1 + I_2$-nek, akkor a fentiek éppen a szorzásra való zártságot jelentik), sőt ideál.

(Kettőnél több ideál metszete, illetve összege esetén ugyanígy bizonyítható az állítás.) □

8.5. Tétel. *Egy $(\mathbb{R}, +, \cdot)$ gyűrű kompatibilis osztályozásai éppen a valamelyik ideálja szerinti osztályozások.*

Bizonyítás. Az, hogy egy ideál szerinti osztályozás kompatibilis az összeadásra nézve, következik abból, hogy az $(\mathbb{R}, +)$ csoport kompatibilis osztályozásai éppen a valamelyik normálosztója szerintiek (6.2. Tétel). Legyenek az I ideál szerinti mellékosztályok: I, $a + I$, $b + I$, ... Azt kell megmutatnunk, hogy például $a + I$ két tetszőleges a_1, a_2 elemére és $b + I$ két tetszőleges, b_1, b_2 elemére teljesül, hogy a_1b_1 ugyanabban az osztályban van, mint a_2b_2. Legyen $a_1 = a + i_1$, $a_2 = a + i_2$, $b_1 = b + j_1$, $b_2 = b + j_2$, ahol $i_1, i_2, j_1, j_2 \in I$. Ekkor $a_1b_1 = (a + i_1)(b + j_1) = ab + aj_1 + i_1b + i_1j_1$ és $a_2b_2 = (a + i_2)(b + j_2) = ab + aj_2 + i_2b + i_2j_2$.

Mivel I ideál, az aj_1, i_1b, i_1j_1, aj_2, i_2b, i_2j_2 elemek mindegyike eleme I-nek (hiszen mindegyik szorzatban valamelyik tényező I-beli elem), így a_1b_1 is és a_2b_2 is eleme $ab + I$-nek.

Az, hogy csak a valamely ideál szerinti osztályozások kompatibilisek, egyrészt annak a következménye, hogy $(R, +)$ kompatibilis osztályozását csak valamelyik normálosztója szerint kaphatjuk. Másrészt, ha ez a normálosztó I, akkor az I, $a + I$, $b + I$, ... osztályozás – mint már az ideál definícióját megelőző példákon láttuk – csak úgy lehet kompatibilis a szorzásra nézve is, ha I egy tetszőleges elemét a gyűrű egy r elemével szorozva ugyanabban az osztályban (I-ben) lesz az eredmény, mint amikor r-et a 0 ($\in I$)-val szorozzuk, vagyis csak ha I ideál. □

Könnyen meggondolható, hogy egy gyűrű kompatibilis osztályozása esetén a maradékosztályok maguk is gyűrűt alkotnak a maradékosztályok összeadására, illetve szorzására nézve. Az így kapott gyűrűt az eredeti gyűrű – az osztályozást létrehozó ideálja szerinti – *faktorgyűrűjének* nevezzük.

A csoportoknál látottakhoz hasonlóan látható be a gyűrűkre vonatkozó homomorfizmustétel:

8.6. Tétel. *Egy gyűrű homomorf képe mindig izomorf a gyűrű egy faktorgyűrűjével.*

Főideálgyűrűk

8.7. Definíció. Az $(\mathbb{R}, +, \cdot)$ gyűrű egy $H \subseteq \mathbb{R}$ részhalmazát tartalmazó legszűkebb ideálját a H *halmaz által generált ideálnak,* az egy elem által generált ideált *főideálnak* nevezzük.

Ideálokra írt példáink közül:

1. $(\mathbb{Z}, +, \cdot)$ minden ideálja főideál, a k szám összes többszöröséből álló ideált generálja a k szám. A teljes gyűrűt az 1 generálja.

2. Az egész számok tetszőleges részgyűrűjének is minden ideálja főideál.

3. Egy null-gyűrűnek egyetlen ideálja van, saját maga, amit generál a 0 elem, így ez az ideál főideál.

4. $(\mathbb{Z}_m, +_{\bmod\ m}, \cdot_{\bmod\ m})$ minden ideálja főideál.

5. A Gauss-egészek körében a $2k + 2ni$ alakú elemekből álló ideált a $2i$ generálja, így főideál. Bizonyítható, hogy a Gauss egészek gyűrűjének minden ideálja főideál.

6. Az $a+b\sqrt{2}$ alakú számok (a, b egész) gyűrűjében is bizonyítható, hogy minden ideál főideál. Például a $2k+n\sqrt{2}$ alakú elemekből álló ideált a $\sqrt{2}$ generálja.

7. Egy test feletti polinomgyűrűben minden ideál főideál. Például azoknak a polinomoknak az ideálját, amelyekben a konstans tag 0, az $f(x) = x$ polinom generálja.

Megjegyzés. Egy elem által generált részgyűrű nem feltétlenül esik egybe az elem által generált ideállal. A Gauss-egészek gyűrűjében például a $2i$ által generált részgyűrű a $4a + 2bi$ alakú, míg a $2i$ által generált ideál a $2k + 2ni$ alakú elemekből áll.

Gondoljuk ezt végig! $2i$ összeadás szerinti többszörösei (az általa generált additív csoport) a $2bi$ alakú számok. $2i$ önmagával vett szorzata -4 – ez is eleme a generált részgyűrűnek. A -4 által generált additív részcsoport a $4a$ alakú elemek. Ilyenek és az előző típusúak összegeként állnak elő a $4a + 2bi$ alakúak. Ezek pedig már gyűrűt alkotnak, hiszen az összeadásra nyilván zártak, a szorzásra pedig: $(4a_1+2b_1i)(4a_2+2b_2i) = 4(4a_1a_2-b_1b_2)+2(4a_1b_2+4a_2b_1)i$, vagyis zárt.

Nem alkotnak azonban ideált, hiszen egy $4a + 2bi$ alakú számot i-vel szorozva $-2b + 4ai$ alakú számot kapunk – ez nincs benne a részgyűrűben. Ahhoz, hogy ideált kapjunk, további elemeket kell hozzávennünk a részgyűrűhöz.

$2i \cdot i = -2$ miatt bele kell vennünk a $2a$ alakú számokat. Emiatt a $2a+2bi$ alakúak is benne lesznek. Azt tudjuk, hogy ez részgyűrű, és – ahogyan azt már korábban láttuk – ideál is (113. oldal).

8.8. Definíció. Ha egy $(R, +, \cdot)$ gyűrűnek minden ideálja főideál, akkor R-et *főideál-gyűrűnek* nevezzük.

A főideálgyűrűk jelentőségét az adja, hogy azokban az integritástartományokban, amelyek egyben főideálgyűrűk is, az egész számokéhoz hasonló számelmélet alakítható ki.

Tetszőleges kommutatív gyűrűben az egészekéhez hasonlóan definiálhatjuk az oszthatóság fogalmát ($a \mid b$, ha $\exists c \in R$, amelyre $ac = (ca =)b$); az egységeket (ε egység, ha $\forall a \in R$-re $\varepsilon \mid a$); kitüntetett közös osztót (a és b kitüntetett közös osztója d, ha $d \mid a$ és $d \mid b$, és ha $c \mid a$ és $c \mid b$, akkor $c \mid d$); felbonthatatlan ($q \not= \varepsilon$ felbonthatatlan, ha $q = ab$-ből következik, hogy a vagy b egység), illetve prímelemet ($p \not= 0$, ε prím, ha $p \mid ab$-ből következik, hogy $p \mid a$ vagy $p \mid b$).

Könnyen meggondolható, hogy egy kommutatív gyűrűben akkor és csak akkor léteznek egységek, ha egységelemes.

Az is belátható, hogy két elem kitüntetett közös osztója egységfaktor erejéig egyértelműen van meghatározva, ha egyáltalán létezik. Azt, hogy bármelyik két elemnek létezik kitüntetett közös osztója, az egész számok és a test feletti polinomok gyűrűjének esetében az euklideszi algoritmus segítségével bizonyítottuk, euklideszi algoritmus azonban nem minden gyűrűben van, csak azokban, amelyekben az abszolútérték-függvény helyett definiálható egy megfelelő, ún. normafüggvény, amellyel az abszolútértéket helyettesítve, a maradékos osztás tétele teljesül. (A polinomok esetében ez a norma a polinom fokszáma volt.)

8.9. Definíció. Az $(E, +, \cdot)$ integritási tartományt *euklideszi gyűrűnek* nevezzük, ha nullától különböző elemein értelmezhető egy olyan f függvény (euklideszi norma), amelyre

- ha $a \in E$ és $a \not= 0$, akkor $f(a)$ nemnegatív egész,
- ha $a, b \in E$ és $ab \not= 0$, akkor ha $a \mid b$, akkor $f(a) \leq f(b)$; valamint
- ha $a, b \in E$ és $b \not= 0$, akkor $\exists q, r \in E$, amelyekre $a = bq + r$, ahol $r = 0$ vagy $f(r) < f(b)$.

Példáink közül az egész számok, illetve a test feletti polinomok gyűrűjén kívül például a Gauss-egészek is, és az $a + b\sqrt{2}$ alakú számok (a, b egész) gyűrűje is euklideszi gyűrű. Belátható, hogy az első esetben az $f(a + bi) = |a + bi|^2 = a^2 + b^2$, a másik esetben pedig az $f\left(a + b\sqrt{2}\right) = a^2 - 2b^2$ norma kielégíti a fenti követelményeket.

Nem euklideszi gyűrű viszont például az egész együtthatós polinomok gyűrűje, vagy az $a + b\sqrt{-5}$ (a, b egész) alakú komplex számok gyűrűje.

Az egész számoknál látottakhoz hasonlóan minden euklideszi gyűrűben egybeesnek a felbonthatatlanok és a prímek, továbbá minden euklideszi gyűrűben teljesül a számelmélet alaptételének megfelelő egyértelmű prímfaktorizációs tétel, azaz egy euklideszi gyűrű minden 0-tól és egységektől különböző eleme sorrendtől és egységtényezőktől eltekintve egyértelműen előállítható véges sok felbonthatatlan tényező szorzataként.

Igaz továbbá, hogy minden euklideszi gyűrű főideálgyűrű.

A számelmélet alaptételének megfelelője azonban nem csak euklideszi gyűrűkben teljesülhet. Belátható, hogy ha egy integritástartomány főideálgyűrű, akkor bármely két elemnek van kitüntetett közös osztója, amely előáll $(a, b) = ax + by$ alakban, és érvényes az egyértelmű prímfaktorizáció.

Azokat az integritástartományokat, melyekben érvényes a számelmélet alaptételének megfelelője, *Gauss-féle gyűrűknek* nevezik. A fentiek szerint minden olyan integritástartomány, amely főideálgyűrű, Gauss-féle (így minden euklideszi gyűrű is), de nem minden Gauss-féle gyűrű főideálgyűrű. Fenti példáink közül az egész együtthatós polinomok gyűrűje Gauss-féle, de nem főideálgyűrű; az $a+b\sqrt{-5}$ (a, b egész számok) alakú komplex számok gyűrűje nem Gauss-féle gyűrű.

Feladatok

1. Melyek alkotnak gyűrűt az alábbiak közül?

   (a) $(\mathbb{N}, +, \cdot)$

   (b) $(\mathbb{Z}, +, \cdot)$

   (c) $(\mathbb{Q}, +, \cdot)$

   (d) $(\mathbb{R}, +, \cdot)$

   (e) $(\{a + b\sqrt{3}, a, b \in \mathbb{Z}\}, +, \cdot)$

   (f) $(\{a + b\sqrt[3]{3}, a, b \in \mathbb{Z}\}, +, \cdot)$

   (g) $(\{a + b\sqrt[4]{4}, a, b \in \mathbb{Z}\}, +, \cdot)$

   (h) $(\{a + b\sqrt[3]{3} + c\sqrt[3]{9}, a, b \in \mathbb{Z}\}, +, \cdot)$

   (i) $(\{\mathbb{Z}_{10}\}, +_{\text{ mod } 10}, \cdot_{\text{ mod } 10})$

   (j) $(\{\mathbb{Z}_{11}\}, +_{\text{ mod } 11}, \cdot_{\text{ mod } 11})$

   (k) $\left(\left\{\begin{pmatrix} a & b \\ b & -a \end{pmatrix}, a, b \in \mathbb{Z}\right\}, +, \cdot\right)$

(l) A legfeljebb 10-edfokú egész együtthatós polinomok az összeadásra és a szorzásra.

(m) Az egész együtthatós polinomok az összeadásra és a szorzásra.

(n) A véges tizedestörtek az összeadásra és a szorzásra.

(o) A 2×2-es egész együtthatós mátrixok a mátrixösszeadásra és a mátrixszorzásra.

2. Határozza meg, hogy az előző példában adott gyűrűk közül melyek egységelemesek!

3. Határozza meg a fenti gyűrűkben a nullosztókat!

4. Egy H halmaz részhalmazainak halmaza P.

   (a) Gyűrű-e P az unió és a metszet műveletekkel?

   (b) Gyűrű-e P a szimmetrikus differencia és a metszet műveletekkel?

   Melyik gyűrűt kapjuk, ha H üreshalmaz?

5. Értelmezzük az egész számok halmazán a $\circ$ és $*$ műveleteket a következőképpen: $a \circ b = a + b + 1$, $a * b = ab + a + b$.

   Igazolja, hogy $(\mathbb{Z}, \circ, *)$ gyűrű!

   Igazolja, hogy $(\mathbb{Z}, \circ, *)$ izomorf az egész számok összeadással és szorzással alkotott gyűrűjével!

6. Igazolja, hogy az egész számokból alkotott $\begin{pmatrix} a & b \\ a & b \end{pmatrix}$ alakú mátrixok a mátrixösszeadásra és mátrixszorzásra nézve gyűrűt alkotnak!

   (a) Létezik-e nullosztó a gyűrűben?

   (b) Létezik-e a szorzásnak egységeleme?

   (c) Létezik-e a szorzás szerinti egyik oldali egységelem? Mennyi?

7. Igazolja, hogy ha egy (legalább kételemű) gyűrűben van két jobb oldali egységelem, akkor nem létezhet bal oldali egységelem!

8. Legyen $G = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \mid a, b, \in \mathbb{N}, b \neq 0 \right\}$ a sík természetes számok feletti vektorainak részhalmaza. Tekintsünk két vektort, $\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}$-et és $\begin{bmatrix} a_2 \\ b_2 \end{bmatrix}$-t egyenlőnek, ha $a_1 + b_2 = a_2 + b_1$.

   Az összeadást a következőképpen értelmezzük:

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \oplus \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 + a_2 \\ b_1 + b_2 \end{bmatrix}$$

Igazolja, hogy $(G, \oplus)$ csoport!

Definiáljuk a szorzást a következőképpen:

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \odot \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 b_1 + a_2 b_2 \\ a_1 b_2 + a_2 b_1 \end{bmatrix}.$$

Igazolja, hogy $(G, \oplus, \odot)$ gyűrű!

9. Igazolja, hogy $(\mathbb{Q}, +, \cdot)$ gyűrű, $(\mathbb{Z}, +, \cdot)$ ennek részgyűrűje, de nem ideálja! (Fogalmazza meg azt a tulajdonságot, amely nem teljesül!)

10. Igazolja, hogy $(\mathbb{R}, +, \cdot)$ gyűrű, $(\mathbb{Q}, +, \cdot)$ ennek részgyűrűje, de nem ideálja! (Fogalmazza meg azt a tulajdonságot, amely nem teljesül!)

9. fejezet

Félgyűrű beágyazása integritástartományba (Az egész számok felépítése)

Az egész számokat szemléletesen úgy kaphatjuk meg a természetes számokból (amint azt az I. kötet bevezetőjében is leírtuk néhány mondatban), hogy kiegészítjük őket a számok „ellentettjével", vagyis tetszőleges természetes számhoz elképzeljük (és persze el is készítjük) azt a számot, amelyet hozzáadva 0-t kapunk.

Az, hogy ez algebrailag korrekt, vagyis hogy a legszűkebb olyan kétműveletes struktúrát kapjuk, amely tartalmazza a természetes számokat, és invertálható az összeadás (gyűrű), csak hosszas algebrai levezetés árán tudjuk megmutatni.

Ebben a fejezetben ennek az egyszerűen átlátható struktúrabővítésnek a részleteit írjuk le. Az lebeg mindvégig a szemünk előtt, hogy két természetes szám különbsége nem mindig természetes szám. Mindeközben azt sem felejtjük el, hogy egy különbséget végtelen sokféleképpen elő lehet állítani, például 5 és 2 különbsége ugyanannyi, mint 6 és 3, 7 és 4 stb. különbsége, így a 8 és 15, 9 és 16, 10 és 17 különbségekről is azt fogjuk feltételezni, hogy megegyeznek.

Nemcsak a természetes számokból készíthetjük el az egész számokat, hanem bármely félgyűrűből kiindulva az absztakt algebra módszereit precízen használva készíthetünk olyan legszűkebb gyűrűt, amely tartalmazza az eredeti félgyűrűt. Ebben a fejezetben ezt az eljárást mutatjuk be; a természetes számok félgyűrűjéből kiindulva „elkészítjük" az egész számokat.

9.1. Definíció. Az $(F, +, \cdot)$ struktúra *félgyűrű,* ha $(F, +)$ kommutatív félcsoport, $(F, \cdot)$ félcsoport, és a művelet (mindkét oldalról) disztributív a $+$ műveletre nézve. Ha a szorzás is kommutatív, akkor kommutatív félgyűrűről beszélünk.

Jó példa kommutatív félgyűrűre a természetes számok (vagy a pozitív egészek) halmaza a szokásos összeadásra és szorzásra nézve. A következőkben megmutatjuk, hogy a természetes számok halmazából kiindulva miként konstruálható meg a legszűkebb olyan integritástartomány, amely a természetes számok félgyűrűjével izomorf félgyűrűt tartalmaz, azaz hogyan konstruálható meg az egész számok gyűrűje.

Először is tekintsük a természetes számokból álló számpárok $\mathbb{N} \times \mathbb{N}$ halmazát. Ezen a halmazon a következőképp definiálhatjuk az összeadást és a szorzást:

$$(a, b) + (c, d) := (a + c, b + d)$$
$$(a, b) \cdot (c, d) := (ac + bd, bc + ad)$$

Könnyen ellenőrizhető, hogy a számpárok halmaza erre a két műveletre nézve maga is kommutatív félgyűrűt alkot, azaz

– az összeadás kommutatív és asszociatív;

$$(a, b) + (c, d) = (a + c, b + d) = (c + a, d + b) = (c, d) + (a, b)$$

és

$$(a, b) + \big((c, d) + (e, f)\big) = (a + c + e, b + d + f) = \\ = \big((a, b) + (c, d)\big) + (e, f)$$

– a szorzás kommutatív és asszociatív;

$$(a, b)(c, d) = (ac + bd, bc + ad) = (ca + db, da + cb) = (c, d)(a, b)$$

és

$$(a, b)\big((c, d)(e, f)\big) = (ace + adf + bde + bcf, bce + bdf + ade + acf) = \\ = \big((a, b)(c, d)\big)(e, f)$$

(Felhasználtuk, hogy a természetes számok összeadása is és szorzása is kommutatív és asszociatív.)

– a szorzás disztibutív az összeadásra nézve.

$$(a, b) \cdot \big((c, d) + (e, f)\big) = (ac + ae + bd + bf, bc + be + ad + af) = \\ = \big((a, b) \cdot (c, d)\big) + \big((a, b) \cdot (e, f)\big)$$

(Mivel a természetes számok szorzása kommutatív, elég csak az egyik oldalról vizsgálni a disztributivitást. Nem kommutatív félgyűrűk esetén hasonlóan igazolható, hogy a szorzás a másik oldalról is disztributív az összeadásra nézve.)

A továbbiakban tekintsük ekvivalensnek az (a_1, b_1) és az (a_2, b_2) számpárokat, ha $a_1 + b_2 = a_2 + b_1$. Ez éppen azt jelenti, hogy az egy osztályba sorolt rendezett párok mindegyikében az első tag ugyanannyival nagyobb (vagy kisebb) a másodiknál.

Könnyen belátható, hogy a számpárok halmazán az így definiált reláció valóban ekvivalenciareláció, vagyis

– reflexív, azaz $(a, b) \sim (a, b)$ (mert $a + b = a + b$);

– szimmetrikus, azaz ha $(a, b) \sim (c, d)$, akkor $(c, d) \sim (a, b)$ (mert ha $a + d = b + c$, akkor $c + b = d + a$);

– tranzitív, azaz ha $(a, b) \sim (c, d)$ és $(c, d) \sim (e, f)$, akkor $(a, b) \sim (e, f)$ (mert ha $a + d = b + c$ és $c + f = d + e$, akkor

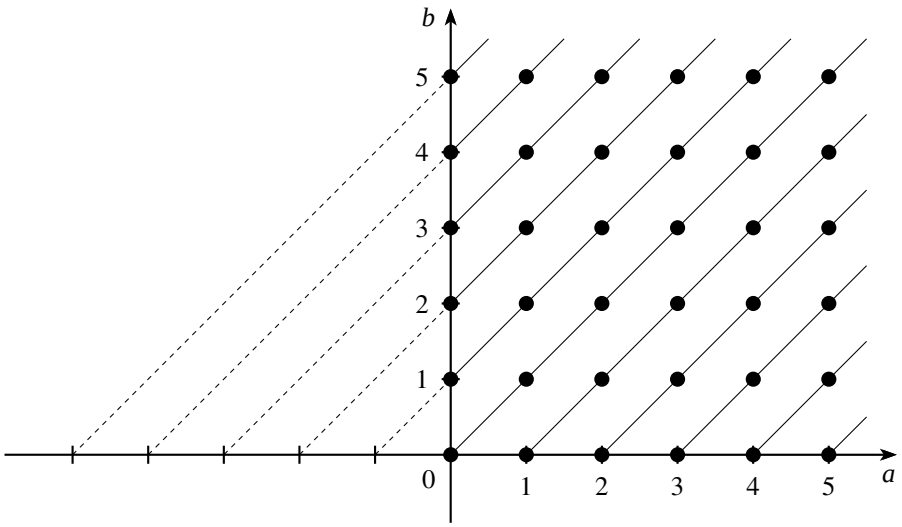
$$a + d + c + f = b + c + d + e,$$

amiből már következik, hogy $a + f = b + e$. Felhasználtuk, hogy a természetes számok körében $n+k = m+k$-ből következik, hogy $n = m$).

Ha most egy osztályba soroljuk az egymással ekvivalens elemeket, megkapjuk $\mathbb{N} \times \mathbb{N}$ egy osztályozását:

$$\left|\begin{array}{c|c|c|c|c|c|c|c}
(0,0) & (1,0) & (0,1) & (2,0) & \dots & (a,b) & \dots & \\
(1,1) & (2,1) & (1,2) & (3,1) & \dots & (a+1,b+1) & \dots & \\
(2,2) & (3,2) & (2,3) & (4,2) & \dots & (a+2,b+2) & \dots & \dots \\
\vdots & \vdots & \vdots & \vdots & \dots & \vdots & \vdots & \\
(n,n) & (n+1,n) & (n,n+1) & (n+2,n) & \dots & (a+n,b+n) & \dots & \\
\vdots & & & & & & &
\end{array}\right|$$

Ezt az osztályozást szemlélteti az alábbi ábra, amelyen az (a, b) számpárnak megfeleltettük az (a, b) koordinátájú rácspontot. Az ábráról leolvasható, hogy éppen azok az elemek lesznek egy osztályban, amelyek egy – az $y = x$ egyenessel párhuzamos – egyenesen helyezkednek el. Az osztályokat szemléltető egyeneseknek az x tengellyel való metszéspontja mutatja, hogy a későbbiekben melyik osztálynak melyik egész szám fog megfelelni.



9.1. ábra.

Ez az osztályozás kompatibilis lesz a fent definiált két műveletre, vagyis ha (a_1, b_1) egy osztályban van (a_2, b_2)-vel (azaz $a_1 + b_2 = a_2 + b_1$) és (c_1, d_1) egy osztályban van (c_2, d_2)-vel (azaz $c_1+d_2 = c_2+d_1$), akkor $(a_1, b_1)+(c_1, d_1)$ egy osztályban lesz $(a_2, b_2) + (c_2, d_2)$-vel, és $(a_1, b_1) \cdot (c_1, d_1)$ egy osztályban lesz $(a_2, b_2) \cdot (c_2, d_2)$-vel.

Ezt a következőképpen láthatjuk be:

$$(a_1, b_1) + (c_1, d_1) = (a_1 + c_1, b_1 + d_1)$$
$$(a_2, b_2) + (c_2, d_2) = (a_2 + c_2, b_2 + d_2)$$

Mivel $a_1+b_2 = a_2+b_1$ és $c_1+d_2 = c_2+d_1$, $a_1+c_1+b_2+d_2 = a_2+c_2+b_1+d_1$, ami éppen azt jelenti, hogy (a_1+c_1, b_1+d_1) egy osztályban van (a_2+c_2, b_2+d_2)-vel.

A szorzásra:

$$(a_1, b_1) \cdot (c_1, d_1) = (a_1c_1 + b_1d_1, b_1c_1 + a_1d_1)$$
$$(a_2, b_2) \cdot (c_2, d_2) = (a_2c_2 + b_2d_2, b_2c_2 + a_2d_2)$$

Ha $a_1 + b_2 = a_2 + b_1$ és $c_1 + d_2 = c_2 + d_1$, akkor

$(a_1 + b_2)c_1 = (a_2 + b_1)c_1$, azaz $a_1c_1 + b_2c_1 = a_2c_1 + b_1c_1$;

$(a_1 + b_2)d_1 = (a_2 + b_1)d_1$, azaz $a_2d_1 + b_1d_1 = a_1d_1 + b_2d_1$;

$b_2(c_1 + d_2) = b_2(c_2 + d_1)$, azaz $b_2c_2 + b_2d_1 = b_2c_1 + b_2d_2$;

$a_2(c_1 + d_2) = a_2(c_2 + d_1)$ azaz $a_2c_1 + a_2d_2 = a_2c_2 + a_2d_1$.

Összeadva a négy egyenlőséget és rendezve a tagokat:

$$a_1c_1 + b_1d_1 + b_2c_2 + a_2d_2 + (b_2c_1 + a_2d_1 + b_2d_1 + a_2c_1) =$$
$$= a_2c_2 + b_2d_2 + b_1c_1 + a_1d_1 + (b_2c_1 + a_2d_1 + b_2d_1 + a_2c_1),$$

amiből már következik, hogy

$$a_1c_1 + b_1d_1 + b_2c_2 + a_2d_2 = a_2c_2 + b_2d_2 + b_1c_1 + a_1d_1,$$

vagyis hogy $(a_1c_1+b_1d_1, b_1c_1+a_1d_1)$ és $(a_2c_2+b_2d_2, b_2c_2+a_2d_2)$ ugyanabban az osztályban vannak.

(Most is kihasználtuk, hogy a természetes számok körében $n+k = m+k$-ból következik, hogy $n = m$.)

Mivel az osztályozás kompatibilis, ezért jogunk van az osztályok közötti műveleteket a következőképpen értelmezni:

$$\overline{(a,b)} \oplus \overline{(c,d)} := \overline{(a,b)+(c,d)} \qquad \text{és} \qquad \overline{(a,b)} \otimes \overline{(c,d)} := \overline{(a,b)\cdot(c,d)}.$$

Belátható, hogy ezekre a műveletekre nézve az osztályok gyűrűt, sőt egységelemes integritástartományt alkotnak.

Az, hogy az osztályok összeadása és szorzása kommutatív és asszociatív, továbbá a szorzás disztributív az összeadásra nézve, következik abból, hogy az osztályokon végzett művelet eredménye független attól, hogy mely elemeikkel reprezentáljuk az osztályokat, és a természetes számokból álló számpárok félgyűrűjében teljesültek ezek a tulajdonságok.

Azt kell még megmutatnunk, hogy az összeadás invertálható, van a szorzásnak egységeleme, és hogy a kapott gyűrű zérusosztómentes.

Könnyen ellenőrízhető, hogy az összeadás neutrális eleme a $\overline{(0,0)}$ osztály, az $\overline{(a,b)}$ osztály additív inverze pedig a $\overline{(b,a)}$ osztály (hiszen $(a,b)+(b,a) = (a+b, a+b) \in \overline{(0,0)}$).

A szorzás egységeleme az $\overline{(1,0)}$ osztály (hiszen $(a,b)(1,0) = (a,b)$).

A zérusosztómentességhez arra van szükségünk, hogy ha sem (a,b), sem (c,d) nem eleme a $\overline{(0,0)}$ osztálynak, akkor $(a,b)(c,d) = (ac+bd, bc+ad)$ se lehessen eleme a $\overline{(0,0)}$ osztálynak, vagyis $ac+bd = bc+ad$ csak úgy legyen lehetséges, ha $a = b$ vagy $c = d$. Az, hogy ez a természetes számok körében teljesül, a következőképp látható be:

Tegyük fel, hogy $a \neq b$, mondjuk $a > b$, így $\exists p \in \mathbb{N}^+$, amelyre $a = b+p$. Ekkor $(b+p)c + bd = bc + (b+p)d$. Ebből már következik, hogy $pc = pd$, azaz $c = d$. Tehát a kapott gyűrű zérusosztómentes.

Most megmutatjuk, hogy a kapott gyűrű tartalmaz a természetes számokéval izomorf részfélgyűrűt.

Tekintsük az $(n,0)$ alakú számpárok által reprezentálható osztályokat. A $\varphi\colon \overline{(n,0)} \to n$ leképezés izomorf módon képezi le ezeket az osztályokat a természetes számok részgyűrűjére, ugyanis φ nyilvánvalóan bijektív, továbbá $\varphi\big(\overline{(a,0)}\big) = a$, $\varphi\big(\overline{(b,0)}\big) = b$.

$$\varphi\big(\overline{(a,0)}\oplus\overline{(b,0)}\big) = \varphi\big(\overline{(a+b,0)}\big) = a+b \text{ és } \varphi\big(\overline{(a,0)}\otimes\overline{(b,0)}\big) = \varphi\big(\overline{(ab,0)}\big) = ab.$$

Vagyis a gyűrű tartalmaz a természetes számokéval izomorf részfélgyűrűt. Ez azt is jelenti, hogy ha a gyűrűben kicseréljük az $\overline{(n,0)}$ alakú elemeket a nekik megfelelő természetes számokra, akkor a gyűrűbeli műveletek értelmezését módosíthatjuk úgy, hogy természetes számok között a náluk szokásos módon végezzük el az összeadást és a szorzást, minden más esetben pedig úgy, ahogy eddig tettük a gyűrűben. (Vagyis például $\overline{(a,b)} \oplus n = \overline{(a+n,b)}$.) Ekkor a gyűrű már magát a természetes számok félgyűrűjét fogja tartalmazni.

Érdemes észrevenni, hogy a gyűrű minden eleme előáll egy természetes szám, és egy természetes szám additív inverzének összegeként: $\overline{(a,b)} = \overline{(a,0)} \oplus \overline{(0,b)} = a \oplus \overline{(0,b)}$, ahol $\overline{(0,b)}$ a b természetes szám additív inverze.

Ha most $\overline{(0,b)}$ helyett $-b$-t, $\oplus$ helyett $+$-t és $\otimes$ helyett $\cdot$-t írunk, akkor felhasználva, hogy $\overline{(a,b)} = a + (-b)$, az egész számok $(\mathbb{Z}, +, \cdot)$ gyűrűjét kapjuk.

Ezekután az egész számok halmazán a következőképpen értelmezhetjük a kivonás nevű műveletet: $a - b := a + (-b)$.

Gondoljuk meg, hogy a fentiek során mennyiben használtuk ki a természetes számok speciális tulajdonságait, vagyis hogy milyen más félgyűrűkre alkalmazható a fenti eljárás.

Tetszőleges félgyűrű esetén elkészíthetjük a félgyűrű elemeiből álló elempárokat, és a fentiekhez hasonlóan definiálhatjuk az elempárok összegét, illetve szorzatát. (Az elempárok szorzása csak kommutatív félgyűrű esetén lesz kommutatív.)

Akkor, amikor osztályokba soroltuk az elempárokat, kihasználtuk, hogy az $(a,b) \sim (c,d) \Leftrightarrow a + d = b + c$ reláció a természetes számpárok halmazán ekvivalenciareláció, vagyis reflexív, szimmetrikus és tranzitív. A tranzitivitás bizonyításához szükségünk volt a természetes számoknak arra a tulajdonságára, hogy $n+k = m+k$-ból következik, hogy $n = m$. Az olyan félgyűrűket, amelyekben teljesül, hogy $n + k = m + k$-ból következik $n = m$, *reguláris félgyűrűknek* nevezik. (Azt, hogy a természetes számok félgyűrűje reguláris, kihasználtuk akkor is, amikor megmutattuk, hogy az osztályozás kompatibilis.)

Tetszőleges reguláris félgyűrű a fentiekkel teljesen analóg módon ágyazható be gyűrűbe. Ahhoz, hogy a kapott gyűrű kommutatív legyen, az kell, hogy a félgyűrűben is kommutatív legyen a szorzás.

Ahhoz, hogy a kapott gyűrű zérusosztómentes legyen, az kell, hogy a félgyűrű tetszőleges a, b, c, d elemeire $a \cdot c + b \cdot d = b \cdot c + a \cdot d$ csak úgy legyen lehetséges, ha $a = b$ vagy $c = d$.

Ahhoz, hogy a kapott gyűrű egységelemes legyen, elégséges, ha a félgyűrűben van egységelem, de nem szükséges (ha például a 10-nél nagyobb pozitív egészek – egységelem nélküli – félgyűrűjéhez konstruáltunk volna őt tartalmazó gyűrűt a fenti módon, ugyancsak az egész számok egységelemes gyűrűjét kaptuk volna).

Feladatok

1. Írja fel, hogy a fejezetben olvasott felépítésben milyen elemekkel ekvivalensek: $(3, 5)$, $(5, 3)$, $(2, 10)$! Melyik egész számoknak feleltethetők meg?

2. Írja fel, hogy a fejezetben olvasott felépítésben milyen elemekkel ekvivalens a $(3, 7) + (7, 3)$ összeg. Ez az osztály melyik egész számnak feleltethető meg?

3. Írja fel, hogy a fejezetben olvasott felépítésben milyen elemekkel ekvivalens a $(8, 1) \cdot (2, 10)$ szorzat. Ez az osztály melyik egész számnak feleltethető meg?

4. Az egész számok fenti bevezetése helyett tekintsük a következőt:

   Készítsük el a természetes számokon a rendezett párokat azzal a megkötéssel, hogy két számpár, (a_1, b_1) és (a_2, b_2) egyenlő, ha $a_1 + b_2 = a_2 + b_1$.

   (a) Igazolja, hogy $(a_1, b_1) = (a_1 - b_1, 0)$, ha $a_1 \geq b_1$ és $(a_1, b_1) = (0, b_1 - a_1)$, ha $b_1 > a_1$.

   Definiáljuk az összeadást $(\oplus)$ a következőképpen:

   $$(a_1, b_1) \oplus (a_2, b_2) = (a_1 + a_2, b_1 + b_2).$$

   (b) Igazolja, hogy az összeadás kommutatív, asszociatív és invertálható!

   Definiáljuk a szorzást $(\odot)$ a következőképpen:

   $$(a_1, b_1) \odot (a_2, b_2) = (a_1 a_2 + b_1 b_2, a_1 b_2 + a_2 b_1).$$

   (c) Igazolja, hogy ez a szorzás kommutatív, asszociatív és disztributív az összeadásra nézve! (Vagyis hogy $(\mathbb{N} \times \mathbb{N}, \oplus, \odot)$ gyűrű.)

(d) Igazolja, hogy az $(a, 0)$ alakú elemek részgyűrűje ennek a gyűrűnek!

(e) Van-e a szorzásnak egységeleme?

(f) Vannak-e a nullosztók a gyűrűben?

10. fejezet

Testek

10.1. Definíció. A $(T, \circ, *)$ algebrai struktúra, ahol a T halmaz legalább kételemű *test,* ha:

- $(T, \circ)$ kommutatív csoport,
- $(T \setminus \{0\}, *)$ kommutatív csoport, továbbá
- a $*$ művelet disztributív a $\circ$ műveletre nézve.

Testekben a $\circ$ műveletet általában összeadásnak, a $*$ műveletet általában szorzásnak nevezzük. Az, hogy $(T, +, \cdot)$ test, azt jelenti, hogy olyan legalább kételemű kommutatív, egységelemes gyűrű, amelyben a 0-tól különböző elemeknek a szorzásra vonatkozóan is van inverzük, vagy részletesebben kiírva: $(T, +, \cdot)$ test, ha:

- T legalább kételemű halmaz;
- az összeadás kommutatív, asszociatív, invertálható;
- a szorzás a $T \setminus \{0\}$ halmazon kommutatív, asszociatív, invertálható;
- a szorzás disztributív az összeadásra nézve.

Megjegyzés. A szorzás egyébként a teljes T halmazon kommutatív és asszociatív – bár nem ezt követeljük meg –, de az invertálhatóság nem igaz az egész T-n. Sőt! T biztosan gyűrű, így teljesül rá a 8.1. Megjegyzés: egy gyűrű 0 elemével szorozva egy tetszőleges elemét, 0-t kapunk. Emiatt képtelenség olyan a elemet találnunk, amelyre $a \cdot 0 = 1$ lenne. Eszerint egy testben az additív egységelemnek, azaz a 0-nak nincs multiplikatív inverze.

Megjegyzés. A szorzás kommutatívitását nem mindenki követeli meg. Ennek megfelelően vannak, akik megkülönböztetnek kommutatív, illetve nem kommutatív testeket. A nem kommutatív testeket (vagyis az olyan algebrai struktúrákat, amelyek csak abban különböznek a testektől, hogy a szorzás nem kommutatív) szokás *ferde testeknek* nevezni.

10.1. Tétel. *Minden test zérusosztómentes.*

Bizonyítás. Az állítás annak a következménye, hogy a nem 0 elemeken invertálható a szorzás. Tegyük fel ugyanis, hogy a nem egyenlő 0-val, és a test valamelyik b elemére $ab = 0$. Ha $a \neq 0$, akkor van inverze, ami szintén nem 0. Megszorozva az egyenlőség mindkét oldalát a inverzével: $a^{-1}ab = a^{-1} \cdot 0$, amiből azt kapjuk, hogy $b = 0$. Vagyis ha egy nem 0 elemet megszorzunk egy másik elemmel, akkor csak úgy kaphatunk 0-t, ha a másik elem 0. □

Példák testre:

1. a racionális számok $(\mathbb{Q}, +, \cdot)$ teste;
2. a valós számok $(\mathbb{R}, +, \cdot)$ teste;
3. a komplex számok $(\mathbb{C}, +, \cdot)$ teste;
4. a mod p (p prím) maradékosztályok $(\mathbb{Z}_p, +_{\bmod p}, \cdot_{\bmod p})$ teste;
5. testet alkotnak az $a + bi$, illetve általában az $a + b\sqrt{k}$ alakú komplex számok halmaza, ahol a és b racionális, k egész szám (ha k történetesen négyzetszám, akkor – elég semmitmondó módon – éppen a racionális számok halmazát kapjuk) a szokásos összeadásra és szorzásra.

10.2. Definíció. $(T', +, \cdot)$ *részteste* a $(T, +, \cdot)$ testnek, ha T részhalmaza T' és maga is test. A $(K, +, \cdot)$ test $(L, +, \cdot)$ résztestét így jelöljük: $K \geq L$ vagy $L \leq K$.

Például:

1. A racionális testnek nincs valódi (saját magától különböző) részteste. Egy résztestnek ugyanis tartalmaznia kell a 0-t (az összeadás neutrális elemét) és az 1-et (a szorzás egységelemét). (Most belátjuk, hogy a 0 és az 1 által generált legszűkebb test a racionális számok teste.)

   Ahhoz, hogy egy a 0-t és az 1-et tartalmazó halmaz zárt legyen az összeadásra nézve, tartalmaznia kell minden pozitív egész számot. Ahhoz, hogy az összeadás invertálható legyen, a negatív egész számokat

is tartalmaznia kell. Ahhoz, hogy a szorzás invertálható legyen, tartalmaznia kell az összes nem 0 egész szám multiplikatív inverzét (azaz reciprokát), vagyis az összes $\frac{1}{n}$ $(0 \neq n \in \mathbb{Z})$ alakú racionális számot; végül tartalmaznia kell tetszőleges két elemének a szorzatát, vagyis az összes $k \cdot \frac{1}{n} = \frac{k}{n}$ $(k, n \in \mathbb{Z},\ n \neq 0)$ alakú számot, végső soron tehát az összes racionális számot.

2. A valós testnek részteste a racionális test vagy például az $a + b\sqrt{2}$ (a, b racionális) alakú számok teste.

3. A komplex testnek részteste a valós test (és így annak összes részteste), vagy például az $a + bi$ (a, b racionális) alakú számok teste.

4. $(\mathbb{Z}_p, +, \cdot)$-nek semmilyen p esetén nincs valódi részteste. Egy résztestének ugyanis tartalmaznia kellene a szorzás egységelemét, vagyis az $\bar{1}$ maradékosztályt. Ahhoz, hogy a résztest zárt legyen az összeadásra, tartalmaznia kell az $\bar{1} + \bar{1} = \bar{2}$, az $\bar{1} + \bar{2} = \bar{3}$ stb. $\bar{1} + \overline{p-1} = \bar{0}$ maradékosztályok mindegyikét.

Korábban megszoktuk, hogy egy algebrai struktúrának két típusú triviális részstruktúrája lehet: önmaga és egy „minimális” részstruktúra. Ez a testek esetében a $\{0, 1\}$ halmazt jelentené, ez azonban általában nem test. (Kivéve a kételemű testet, a $(\mathbb{Z}, +_{\bmod 2}, \cdot_{\bmod 2})$, amely azonban csak önmagának részteste, és rajta kívül más részteste nincs is.)

10.3. Definíció. Egy test *prímtest,* ha nincs valódi részteste.

Mint már láttuk, a racionális test és a $(\mathbb{Z}, +_{\bmod p}, \cdot_{\bmod p})$ (mod p maradékosztály-testek, p prímszám) prímtestek. A következő tétel azt mondja ki, hogy ezektől lényegesen különböző prímtestek nincsenek:

10.2. Tétel. *Minden prímtest izomorf a racionális testtel, vagy valamelyik* mod p *maradékosztály-testtel.*

Bizonyítás. Legyen $(P, +, \cdot)$ egy prímtest, amelynek egységeleme e, és tekintsük a $\ldots, -2e, -e, 0, e, 2e, 3e, \ldots, ke, \ldots$ elemeket. Két esetet különböztetünk meg:

(a) nincs olyan 0-tól különböző k egész szám, amelyre $ke = 0$

(b) van ilyen k.

Az (a) eseteben a fenti elemek mind különbözőek. Mivel a $(P,+,\cdot)$ test nem 0 elemein a szorzás invertálható, az összes $(ae)(be)^{-1}$ $(b \neq 0)$ alakú elem benne van P-ben. Az ilyen alakú elemek egyben résztestét is alkotják $(P,+,\cdot)$-nak, mégpedig olyan résztestét, amelyet a $\varphi\colon (ae)(be)^{-1} \mapsto \frac{a}{b}$ leképezés – mint az könnyen ellenőrizhető – izomorf módon képez le a racionális testre.

Másfelől, ha $(P,+,\cdot)$ prímtest, akkor ez a résztest nem lehet valódi, csak maga a teljes $(P,+,\cdot)$ test, így $(P,+,\cdot)$ izomorf a racionális testtel. (Ez éppen az a konstrukció, amelyet 10.2. Definíciót követő példában tárgyaltunk.)

A (b) esetben legyen m a legkisebb pozitív egész, amelyre $me = 0$. Ekkor m csak prímszám lehet, hiszen $m = ab$ esetén $me = (ab)e = (ae)(be)$ csak úgy lehetne 0, ha már ae vagy be is 0 lett volna, de valódi felbontás esetén a is és b is kisebb, mint m. Ekkor az $ne \mapsto \overline{n}$ leképezés izomorf módon képezi le az $e, 2e, 3e, \ldots, (m-1)e, me = 0$ elemeket a mod m (m prím) maradékosztály-testre, így ezek az elemek maguk is testet alkotnak, amely részteste a $(P,+,\cdot)$ testnek.

Mivel $(P,+,\cdot)$ prímtest, ez nem lehet valódi résztest, csak maga a teljes $(P,+,\cdot)$ test, vagyis maga $(P,+,\cdot)$ izomorf a mod m (m prím) maradékosztály-testtel. □

Megjegyzés. Az, hogy egy $(P,+,\cdot)$ prímtest a $(\mathbb{Q},+,\cdot)$, illetve a $(\mathbb{Z}_p,+,\cdot)$ maradekosztály-testek melyikével lesz izomorf, nyilván csak P számosságától függ. Ha $|P|$ végtelen, akkor a racionális testtel, ha $|P| = n$ ($n \geq 2$, és mint láttuk, csak prím lehet), akkor a $(\mathbb{Z}_n,+,\cdot)$ testtel. Ebből az is következik, hogy ha egy prímtest számossága végtelen, akkor csak megszámlálhatóan végtelen lehet; ha pedig véges, akkor csak prímszám lehet.

Feladatok

1. Igazolja, hogy a 10.1. Definícióban az a feltétel, hogy T legalább kételemű, elhagyható.

2. Melyik test az alábbiak közül?

   (a) Az egész számok az összeadásra és a szorzásra.

   (b) A racionális számok halmaza az összeadásra és a szorzásra.

   (c) A véges tizedestörtek halmaza az összeadásra és a szorzásra.

   (d) Az $a + bc$ alakú számok, ahol $a, b \in \mathbb{Q}$, $c^2 \in \mathbb{Z}^+$ az összeadásra és a szorzásra.

   (e) Az $a + b\sqrt[3]{2}$ alakú számok, ahol $a, b \in \mathbb{Q}$ az összeadásra és a szorzásra.

(f) A 2×2-es valós reguláris (azaz invertálható) mátrixok a mátrixösszeadásra és a mátrixszorzásra.

(g) A valós együtthatós polinomok a polinomösszeadásra és polinomszorzásra.

3. Keresse meg az összes – izomorfia erejéig különböző – kételemű testet! Hány – izomorfia erejéig különböző – háromelemű test létezik?

4. Legyen p egy adott prímszám, például 7. Hány – izomorfia erejéig különböző – p-elemű test létezik? Hány részteste van ezeknek?

5. Készítsen 4-elemű testet!

11. fejezet

Integritástartomány beágyazása testbe, hányadostest (A racionális számok felépítése)

A 9. fejezetben láttuk, hogy egy reguláris félgyűrűhöz (például a természetes számok félgyűrűjéhez) hogyan konstruálható olyan gyűrű, illetve közülük bizonyosakhoz olyan integritástartomány, amely tartalmaz a félgyűrűvel izomorf részt, azaz, hogy miként építhetők fel a természetes számokból kiindulva az egész számok. Az egész számok halmazán már invertálható az összeadás, de a szorzás nem. A következőkben azzal a kérdéssel foglalkozunk, hogy miképpen tehető invertálhatóvá a 0-tól különböző elemek szorzása is, vagyis hogy miként építhetők fel az egész számokból kiindulva a racionális számok. Általánosabban megfogalmazva a kérdést, egy I integritástartományhoz szeretnénk megtalálni a legszűkebb olyan testet, amely tartalmaz I-vel izomorf részt.

Tekintsük ehhez először az integritástartomány elemeiből (egész számokból) álló $(a, b) \in I \times I \setminus \{0\}$ párok halmazát (ahol $b \neq 0$). Ezen a halmazon a kovetkezőkeppen értelmezhetünk egy összeadás és egy szorzás nevű műveletet:

$(a, b) + (c, d) := (ad + bc, bd)$, például $(1, 4) + (2, 6) = (14, 24)$

$(a, b) \cdot (c, d) := (ac, bd)$, például $(1, 4) \cdot (2, 6) = (14, 24)$.

Könnyen ellenőrízhető, hogy a párok így definiált összeadása esetén

– Az összeadás kommutatív és asszociatív, neutrális eleme a $(0,1)$ (viszont nem invertálható)

$$(a,b)+(c,d)=(ad+bc,bd)=(cb+da,db)=(c,d)+(a,b) \quad \text{és}$$
$$(a,b)+\big((c,d)+(e,f)\big)=(adf+bcf+bde,bdf)=\big((a,b)+(c,d)\big)+(e,f)$$
$$(a,b)+(0,1)=(a\cdot 1+b\cdot 0,b\cdot 1)=(a,b).$$

– A szorzás kommutatív és asszociatív, egységeleme az $(1,1)$ (viszont nem invertálható és nem disztributív az összeadásra nézve)

$$(a,b)\cdot(c,d)=(ac,bd)=(ca,db)=(c,d)\cdot(a,b)$$
$$(a,b)\cdot\big((c,d)\cdot(e,f)\big)=(ace,bdf)=\big((a,b)\cdot(c,d)\big)\cdot(e,f)$$
$$(a,b)\cdot(1,1)=(a\cdot 1,b\cdot 1)=(a,b).$$

Érdemes észrevenni, hogy ha egy (a,b) számpárral ekvivalensnek tekintenénk azokat az (a',b') számparokat, amelyekre $ab'=a'b$ (vagyis például a $(0,1)$ párral ekvivalensnek tekintenénk az összes $(0,n)$ alakú, az $(1,1)$ párral az összes (n,n) alakú számpárt), akkor már – ekvivalencia erejéig – invertálható lenne az összeadás is és a szorzás is, továbbá a szorzás disztributív lenne az összeadásra nézve, ugyanis:

$$\begin{aligned}
(a,b)+(-a,b)&=(ab-ba,b^2)=(0,b^2)\sim(0,1)\\
(a,b)\cdot(b,a)&=(ab,ba)\sim(1,1)\\
(a,b)\cdot\big((c,d)+(e,f)\big)&=(acf+ade,bdf), \qquad \text{míg}\\
(a,b)(c,d)+(a,b)(e,f)&=(acbf+bdae,bdbf), \qquad \text{ahol}\\
(acf+ade,bdf)&\sim(acbf+bdae,bdbf).
\end{aligned}$$

Az $(a,b)\sim(a',b')$ akkor és csak akkor, ha $ab'=a'b$ reláció ekvivalenciareláció, hiszen

– reflexív, azaz $(a,b)\sim(a,b)$, mert $ab=ab$;

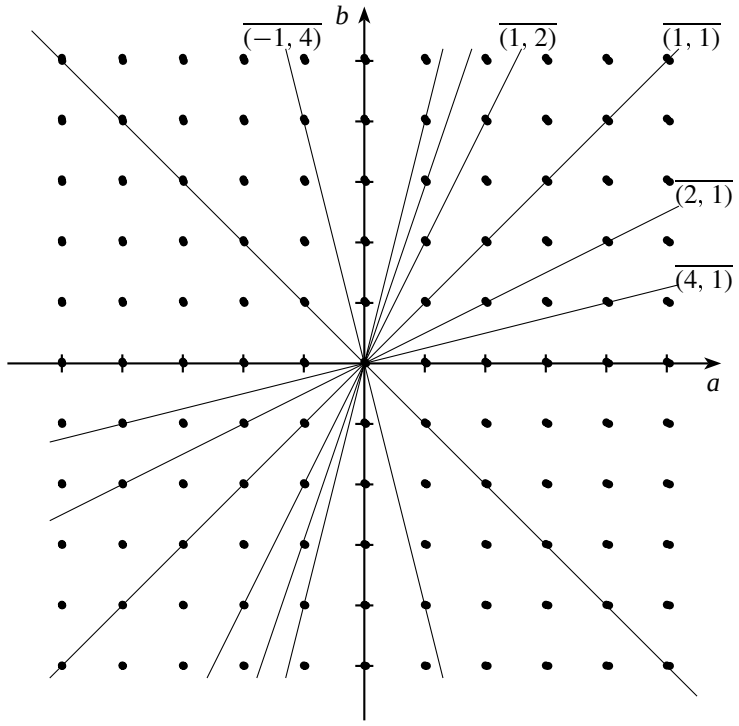
– szimmetrikus, azaz ha $(a,b)\sim(a',b')$, akkor $(a',b')\sim(a,b)$, mert ha $ab'=a'b$, akkor $a'b=ab'$; végül

– tranzitív, azaz ha $(a,b)\sim(a',b')$ és $(a',b')\sim(a'',b'')$, akkor $(a,b)\sim$ $\sim(a'',b'')$, mert ha $ab'=a'b$ és $a'b''=a''b'$, akkor $ab'a'b''=a'ba''b'$, amiből az egész számok halmazán (illetve minden integritástartományban – a kommutativitás és a zérusosztómentesség miatt) következik, hogy $ab''=a''b$.

Ha most egy-egy osztályba gyűjtjük az egymással ekvivalens elemeket, akkor megkapjuk a párok halmazának egy osztályozását:

$$\begin{array}{c|c|c|c|c|c|c|c|c}
 & (-1,1) & (0,1) & (1,1) & (1,2) & (2,1) & \dots & (a,b) & \\
 & (1,-1) & (0,-1) & (-1,-1) & (-1,-2) & (-2,-1) & \dots & (-a,-b) & \\
 & (-2,2) & (0,2) & (2,2) & (2,4) & (4,2) & \dots & (2a,2b) & \\
\dots & (2,-2) & (0,-2) & (-2,-2) & (-2,-4) & (-4,-2) & \dots & (-2a,-2b) & \dots \\
 & (-3,3) & (0,3) & (3,3) & (3,6) & (6,3) & \dots & (3a,3b) & \\
 & \vdots & \vdots & \vdots & \vdots & \vdots & \dots & \vdots & \\
 & (-n,n) & (0,n) & (n,n) & (n,2n) & (2n,n) & \dots & (an,bn) & \\
 & \vdots & & & & & & &
\end{array}$$

Az alábbi ábráról leolvasható, hogy ha az (a,b) számpárnak megfeleltetjük az (a,b) koordinátájú rácspontot, akkor két elem akkor és csak akkor lesz egy osztályban, ha összekötő egyenesük átmegy az origón. Az osztályoknak majdan megfelelő racionális számokat az illető osztályt szemléltető egyenesnek az $y=1$ egyenessel való metszéspontjának abszcisszája mutatja.



11.1. ábra.

Belátjuk, hogy az osztályozás kompatibilis, vagyis hogy ha (a_1,b_1) egy osztályban van (a_2,b_2)-vel, és (c_1,d_1) egy osztályban van (c_2,d_2)-vel, akkor $(a_1,b_1)+(c_1,d_1)$ egy osztályban lesz $(a_2,b_2)+(c_2,d_2)$-vel, és $(a_1,b_1)\cdot(c_1,d_1)$

is egy osztályban lesz $(a_2, b_2) \cdot (c_2, d_2)$-vel:

$$(a_1, b_1) + (c_1, d_1) = (a_1d_1 + b_1c_1, b_1d_1) \qquad \text{és}$$
$$(a_2, b_2) + (c_2, d_2) = (a_2d_2 + b_2c_2, b_2d_2).$$

Ha $a_1b_2 = a_2b_1$ és $c_1d_2 = c_2d_1$, akkor $a_1b_2d_1d_2 = a_2b_1d_1d_2$ és $c_1d_2b_1b_2 = c_2d_1b_1b_2$, amiből $a_1b_2d_1d_2 + c_1d_2b_1b_2 = a_2b_1d_1d_2 + c_2d_1b_1b_2$, ami éppen azt jelenti, hogy $(a_1d_1 + b_1c_1, b_1d_1)$ egy osztályban van $(a_2d_2 + b_2c_2, b_2d_2)$-vel.

$$(a_1, b_1) \cdot (c_1, d_1) = (a_1c_1, b_1d_1) \qquad \text{és}$$
$$(a_2, b_2) \cdot (c_2, d_2) = (a_2c_2, b_2d_2).$$

Ha $a_1b_2 = a_2b_1$ és $c_1d_2 = c_2d_1$, akkor $a_1b_2c_1d_2 = a_2b_1c_2d_1$, ami épp azt jelenti, hogy (a_1c_1, b_1d_1) egy osztályban van (a_2c_2, b_2d_2)-vel. Ezek után a következőképp értelmezhetjük az osztályok összeadását és szorzását:

$$\overline{(a,b)} \oplus \overline{(c,d)} := \overline{(a,b) + (c,d)}$$
$$\overline{(a,b)} \otimes \overline{(c,d)} := \overline{(a,b) \cdot (c,d)}.$$

Megmutatjuk, hogy az osztályok az így definiált összeadásra és szorzásra nézve testet alkotnak: Az, hogy az összeadás is és a szorzás is kommutatív és asszociatív, az összeadás neutrális eleme a $\overline{(0,1)}$, a szorzás egységeleme pedig az $\overline{(1,1)}$ osztály, következik abból, hogy az osztályozás kompatibilis volt. Meg kell még mutatnunk, hogy az összeadás invertálható, a nem nulla elemek halmazán (a $\overline{(0,1)}$ osztálytól különböző osztályok halmazán) a szorzás is invertálható, továbbá hogy a szorzás disztributív az összeadásra nézve.

Az $\overline{(a,b)}$ osztály additív inverze a $\overline{(-a,b)}$ osztály, hiszen

$$\overline{(a,b)} \oplus \overline{(-a,b)} = \overline{(a,b) + (-a,b)} = \overline{\big(ab + b(-a), b \cdot b\big)} = \overline{(0, b \cdot b)} = \overline{(0,1)}.$$

Az $\overline{(a,b)}$ osztály multiplikatív inverze a $\overline{(b,a)}$ osztály, hiszen

$$\overline{(a,b)} \otimes \overline{(b,a)} = \overline{(a,b) \cdot (b,a)} = \overline{(ab,ab)} = \overline{(1,1)}.$$

A disztibutivitást a következőképp láthatjuk be:

$$\begin{aligned}\overline{(a,b)} \otimes (\overline{(c,d)} \oplus \overline{(e,f)}) &= \overline{(a,b) \cdot ((c,d) + (e,f))} = \overline{(acf + ade, bdf)} = \\ &= \overline{(acbf + bdae, bdbf)} = \overline{(a,b) \cdot (c,d) + (a,b)(e,f)} = \\ &= \big(\overline{(a,b)} \otimes \overline{(c,d)}\big) \oplus \big(\overline{(a,b)} \otimes \overline{(e,f)}\big).\end{aligned}$$

Most megmutatjuk, hogy az így kapott test tartalmaz az egész számok gyűrűjével izomorf részt:

A $\varphi\colon \overline{(k,1)} \to k$ leképezés izomorf módon képezi le a $\overline{(k,1)}$ alakú osztályok részhalmazát az egész számok halmazára, hiszen nyilvánvalóan bijektív, és míg $\varphi\big(\overline{(a,1)}\big) = a$ és $\varphi\big(\overline{(b,1)}\big) = b$,

$$\varphi\big(\overline{(a,1)}\big) \oplus \overline{(b,1)} = \varphi\big(\overline{(a,1)+(b,1)}\big) = \varphi\big(\overline{(a+b,1)}\big) = a+b \qquad \text{és}$$
$$\varphi\big(\overline{(a,1)} \otimes \overline{(b,1)}\big) = \varphi\big(\overline{(a,1)\cdot(b,1)}\big) = \varphi\big(\overline{(ab,1)}\big) = ab.$$

Ha most a $\overline{(k,1)}$ alakú osztályokat kicseréljük a nekik megfelelő egész számokra, és az egész számok között az ott szokásos módon, egyébként pedig az osztályokon definiált módon végezzük el a műveleteket, akkor az így módosított test már valódi részként fogja tartalmazni az egész számok gyűrűjét.

11.1. Megjegyzés. Érdemes még észrevenni, hogy minden osztály felírható

$$\overline{(a,b)} = \overline{(a,1)} \otimes \overline{(1,b)} = \overline{(a,1)} \otimes \big(\overline{(b,1)}\big)^{-1}$$

alakban, így az $\overline{(a,b)}$ osztály helyett írhatunk $a \cdot b^{-1}$-et, vagy a szokásoknak megfelelően $\dfrac{a}{b}$-t. Így a racionális számok $(\mathbb{Q}, +, \cdot)$ testéhez jutunk. A fenti eljárás segítségével tetszőleges integritástartományhoz megkonstruálható az őt (vele izomorf részt) tartalmazó legszűkebb test, amit a szóbanforgó integritástartomány hányadostestének neveznek. A Gauss-egészek gyűrűjének hányadosteste például az olyan $a+bi$ alakú komplex számok teste lesz, ahol a és b racionális szám (Gauss-racionálisok); egy T test feletti polinomgyűrű hányadosteste pedig az $\dfrac{f(x)}{g(x)}$ alakú elemekből álló racionális függvénytest, ahol $f(x),\ g(x) \in T[x]$ és $g(x) \neq 0$.

Feladatok

1. A fejezetben megadott felépítésben melyik ekvivalenciaosztályba tartoznak, illetve milyen racionális számnak felelnek meg: $(4,2)$, $(1,3)$, $(3,1)$, $(-2,5)$, $(1,2)+(3,2)$, $(2,3)\cdot(3,4)$?

2. Legyen $T = \left\{ \begin{bmatrix} a \\ b \end{bmatrix} \mid a, b, \in \mathbb{Z}, b \neq 0 \right\}$ a sík egészek feletti vektorainak részhalmaza. Tekintsünk két vektort, $\begin{bmatrix} a_1 \\ b_1 \end{bmatrix}$-et és $\begin{bmatrix} a_2 \\ b_2 \end{bmatrix}$-t egyenlőnek, ha $a_1 b_2 = a_2 b_1$.

   Az összeadást a következőképpen értelmezzük:

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \oplus \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 b_2 + a_2 b_1 \\ b_1 b_2 \end{bmatrix}.$$

Írjon fel néhány, ezzel egyenlő elemet!

A szorzást a következőképpen adjuk meg:

$$\begin{bmatrix} a_1 \\ b_1 \end{bmatrix} \odot \begin{bmatrix} a_2 \\ b_2 \end{bmatrix} = \begin{bmatrix} a_1 a_2 \\ b_1 b_2 \end{bmatrix}.$$

Írjon fel néhány, ezzel egyenlő elemet!

Igazolja, hogy $(T, \oplus, \odot)$ test!

12. fejezet

Testbővítések

12.1. Definíció. A $(T', +, \cdot)$ testet a $(T, +, \cdot)$ test *bővítésének* nevezzük, ha T részteste T'-nek.

A valós számok teste például bővítése a racionális számok testének, a komplex számok teste pedig bővítése a valós testnek is és a racionális testnek is. Gyakran van szükségünk arra, hogy megkeressük vagy megkonstuáljuk egy adott T test bizonyos feltételeknek eleget tevő bővítését. Ez bizonyos esetekben azt jelenti, hogy T egy már ismert bővítésének kell megkeresnünk azt a résztestét, amely szintén bővítése T-nek, és amely eleget tesz a feltételeknek; más esetekben egy új testet kell létrehoznunk: T-ből kiindulva egy olyan testet kell konstruálnunk, amely tartalmazza T-t, és amely eleget tesz a feltételeknek. Ha például a racionális testnek keressük azt a legszűkebb bővítését, amelyben már van olyan elem, amelynek négyzete 2, akkor ez más feladatot jelent, ha ismerjük a valós számok testét, mint akkor, ha nem ismerjük. Az első esetben mindössze meg kell keresnünk a valós számoknak azt a legszűkebb résztestét, amely tartalmazza a racionális testet is és a $\sqrt{2}$-t is, míg a második esetben – pusztán a racionális számokra támaszkodva – meg kell konstruálnunk a keresett testet.

Azt a legszűkebb testet, amely tartalmaz egy adott T testet is és az előre rögzített a, b, c, ... elemeket is, a T test a, b, c, ... elemekkel való bővítésének nevezzük, és $T(a, b, c, \ldots)$-vel jelöljük. Ezt a testet nyilván úgy is megkaphatjuk, hogy először megkeressük a legszűkebb, T-t és a-t tartalmazó $T_1 = T(a)$ testet, majd az így kapott testet és a b-t tartalmazó legszűkebb $T_2 = T_1(b)$ testet, majd T_2 testet és a c-t tartalmazó legszűkebb $T_3 = T_2(c)$ testet stb.

12.2. Definíció. A T test egyetlen elemmel való $T(\alpha)$ bővítését *egyszerű testbővítésnek* nevezzük.

Megjegyzés. Ezt nem úgy kell elképzelni, hogy vesszük a $T \cup \alpha$ halmazt a két eredeti művelettel, mert az (megmutatható, hogy soha) nem lesz test. Inkább úgy kell rá gondolni, hogy a T testhez az α elem mellett addig-addig veszünk hozzá további számokat, amíg még szükséges; hogy végül testet kapjuk, de közben olyat nem veszünk hozzá, amit nem muszáj.

A továbbiakban csak egyszerű testbővítésekkel foglalkozunk.

Az egyszerű testbővítések két fajtáját különböztetjük meg aszerint, hogy van-e olyan T test feletti polinom, amelynek α gyöke, vagy nincs.

12.3. Definíció.

1. Azt mondjuk, hogy α *algebrai elem* a T test felett, ha létezik olyan (nem azonosan zérus) $f(x) \in T[x]$, amelyre $f(\alpha) = 0$.
2. Azt mondjuk, hogy α *transzcendens elem* a T test felett, ha nincs olyan (nem azonosan zérus) $f(x) \in T[x]$, amelyre $f(\alpha) = 0$.
3. A racionális test feletti algebrai elemeket szokás *algebrai számoknak,* a racionális test felett transzcendens elemeket pedig szokás *transzcendens számoknak* nevezni.

Például:

1. Az 5 algebrai elem a $\mathbb{Q}$ felett, mert eleme neki.
2. A $\sqrt{2}$ algebrai elem $\mathbb{Q}$ felett, azaz algebrai szám, mert gyöke a racionális együtthatós $f(x) = x^2 - 2$ polinomnak.

   Hasonlóan a $\sqrt{3}$, mert az meg gyöke az $x^2 - 3$ racionális együtthatós polinomnak.
3. A $\sqrt{2}$ algebrai elem, sőt, algebrai szám a valósok felett is, mert eleme annak. (Gyöke a racionális együtthatós $f(x) = x^2 - 2$ polinomnak.)
4. A π algebrai elem a valós számtest felett, mert eleme. Sőt, tetszőleges test esetén a test bármelyik eleme algebrai elem a test felett.
5. Az i komplex szám algebrai elem a valós test felett, mert gyöke a valós (racionális, sőt egész) együtthatós $f(x) = x^2 + 1$ polinomnak. Az i algebrai szám.
6. Bármelyik komplex szám algebrai elem a valós test felett, mert z gyöke például az $x^2 - (z + \overline{z})x + z\overline{z}$ valós együtthatós polinomnak.
7. Sem a π, sem az e nem algebrai a racionálisok felett, mert nincs olyan racionális együtthatós polinom, amelynek gyöke lenne. (Nem bizonyítjuk.) A π és az e transzcendens számok.

Egyszerű testbővítés

Egyszerű testbővítés algebrai elemmel (egyszerű algebrai bővítés)

Először azzal az esettel foglalkozunk, amikor egy T felett algebrai α elemmel szeretnénk bővíteni a T testet.

Például:

1. Ha azt a legszűkebb testet keressük, amelynek részteste a valós számok teste és amely tartalmazza az $f(x) = x^2 + 1$ polinom (valamelyik) gyökét, akkor a következőképpen járhatunk el:

   Ha egy test tartalmazza az összes valós számot és az i-t (vagy a $-i$-t), akkor a szorzás zártsága miatt tartalmaznia kell az összes bi alakú számot, ahol $b \in \mathbb{R}$. Tartalmaznia kell továbbá az összes $a + bi$ alakú számot (a, b valós) is az összeadás zártsága miatt, vagyis az összes komplex számot. A komplex számokról már tudjuk, hogy testet alkotnak, a fenti megfontolások miatt ez a legszűkebb $\mathbb{R}$-et és i-t tartalmazó test, tehát $\mathbb{R}(i) = \mathbb{C}$.

Ebben a gondolatmenetben felhasználtuk, hogy már ismertük a komplex számtestet, és tudtuk, hogy az $f(x) = x^2 + 1$ polinom (egyik) gyöke i. Ha még nem ismertük volna a komplex számokat, akkor a következőképp gondolkodhattunk volna:

A komplex számok felépítése

Keressük azt a legszűkebb testet, amely tartalmazza a valós számtestet, és amelyben már van az $f(x) = x^2 + 1$ polinomnak gyöke. Legyen α a keresett testnek egy olyan eleme, amelyre $\alpha^2 = -1$. Jelöljük a test összeadás nevű műveletét a $\oplus$, a szorzás nevű műveletét a $\otimes$ jellel, megjegyezve, hogy amikor valós számok között végezzük a műveletet, akkor ezek jelentsék a valós számok szokásos összeadását és szorzását. Ha a keresett testnek α is és a valós számok is elemei, akkor benne kell lennie az összes $a \oplus (b \otimes \alpha)$ alakú elemnek is, ahol a, b valós. A testekben érvényes műveleti tulajdonságok miatt két ilyen alakú elem összegére, illetve szorzatára a következőknek kell teljesülnie:

$$\begin{aligned}
&\big(a \oplus (b \otimes \alpha)\big) \oplus \big(c \oplus (d \otimes \alpha)\big) = (a \oplus c) \oplus \big((b \oplus d) \otimes \alpha\big) = \\
&\qquad = (a + c) \oplus \big((b + d) \otimes \alpha\big) \\
&\big(a \oplus (b \otimes \alpha)\big) \otimes \big(c \oplus (d \otimes \alpha)\big) = \\
&\qquad = (a \otimes c) \oplus (b \otimes d \otimes \alpha^2) \oplus \big((b \otimes c) \oplus (a \otimes d \otimes \alpha)\big)
\end{aligned}$$

Felhasználva, hogy $\alpha^2 = -1$:

$$\big(a \oplus (b \otimes \alpha)\big) \otimes \big(c \oplus (d \otimes \alpha)\big) = (ac - bd) \oplus \big((bc + ad) \otimes \alpha\big)$$

Könnyen belátható, hogy az $a \oplus (b \otimes \alpha)$ alakú elemek testet alkotnak, éppen ezt a testet szokás a komplex számok testének nevezni. Érdemes még észrevenni, hogy ha $\oplus$ helyett $+$-t, $\otimes$ helyett $\cdot$-t (vagy semmit sem) α helyett pedig i-t írunk, akkor a szokásos $a + bi$ jelöléshez jutunk.

Lényegében ugyanezt az utat követjük akkor is, amikor valós számpárokból építjük fel a komplex testet úgy, hogy megmutatjuk, hogy a valós számpárok testet alkotnak a következő két műveletre nézve:

$$(a, b) \oplus (c, d) = (a + c, b + d)$$
$$(a, b) \otimes (c, d) = (ac - bd, bc + ad);$$

majd megmutatjuk, hogy ez a test tartalmaz a valós testtel az $(a, 0) \to$ $\to a$ leképezés szerint izomorf résztestet. Ezekután észrevéve, hogy $(a, b) = (a, 0) \oplus \big((b, 0) \otimes (0, 1)\big)$; az $(a, 0)$ párt kicserélve az a, a $(b, 0)$ párt a b valós számra, $\oplus$ helyett $+$-t, $\otimes$ helyett $\cdot$-t, a $(0, 1)$ pár helyett pedig i-t írva kapjuk a komplex számok $a + b \cdot i$ kanonikus alakját.

2. Keressük a legszűkebb testet, amely tartalmazza a racionális testet és az $x^2 - 2$ polinom (valamelyik) gyökét.

   Ha a keresett test tartalmazza az összes racionális számot is és a $\sqrt{2}$-t (vagy a $-\sqrt{2}$-t) is, akkor – a műveletek zártsága miatt – tartalmaznia kell az összes $b\sqrt{2}$ alakú számot. Ezek mind különböző számok lesznek, mert ha $b_1\sqrt{2} = b_2\sqrt{2}$, akkor $(b_1 - b_2)\sqrt{2} = 0$, ami – mivel $\sqrt{2}$ irracionális – csak úgy lehet, ha $b_1 = b_2$. Nem alkotnak azonban testet. A $b\sqrt{2}$ alakúak racionális számokkal vett összege nem lehet ilyen alakú: az $a_1 + b_1\sqrt{2} = b_2\sqrt{2}$ egyenlőségből $a_1 = (b_2 - b_1)\sqrt{2}$ következnék, ez azonban csak úgy lehetséges, ha $a_1 = 0$ és $b_1 = b_2$. Eszerint az összes $a+b\sqrt{2}$ alakú számot hozzá kell vennünk. Ezek mind különböző számok lesznek, mert ha $a_1 + b_1\sqrt{2} = a_2 + b_2\sqrt{2}$, akkor $(b_1 - b_2)\sqrt{2} = a_2 - a_1$, ami – mivel $\sqrt{2}$ irracionális – csak úgy lehet, ha $b_1 - b_2$ és $a_2 - a_1$ is nulla. Vagyis megkaptuk az összes $a + b\sqrt{2}$ alakú számot, ahol a és b racionális. Belátjuk, hogy ez már test.

   Mivel

   $$(a + b\sqrt{2}) + (c + d\sqrt{2}) = (a + c) + (b + d)\sqrt{2} \qquad \text{és}$$
   $$(a + b\sqrt{2}) \cdot (c + d\sqrt{2}) = (ac + 2bd) + (bc + ad)\sqrt{2},$$

   vagyis zárt az összeadásra és a szorzásra (két ilyen alakú szám összege is szorzata is ilyen alakú).

Létezik zéruselem és egységelem: $0 = 0+0\cdot\sqrt{2}$ és $1 = 1+0\cdot\sqrt{2}$ (vagyis a neutrális elemek is ilyen alakúak).

Léteznek a szükséges inverzek: $-(a+b\sqrt{2}) = -a-b\sqrt{2}$, valamint ha $a \neq 0, b \neq 0$ (mivel $a, b \in \mathbb{Q}$, $a+b\sqrt{2} = 0$ akkor és csak akkor teljesül, ha $a = 0$ és $b = 0$), akkor

$$(a+b\sqrt{2})^{-1} = \frac{1}{a+b\sqrt{2}} = \underbrace{\frac{a}{a^2-2b^2}}_{\text{racionális}} + \underbrace{\frac{-b}{a^2-2b^2}}_{\text{racionális}}\sqrt{2}$$

Itt azt is felhasználtuk, hogy $a-b\sqrt{2}$ nem lehet nulla. Ez nyilvánvalóan igaz, mert $a = b\sqrt{2}$ csak úgy teljesülhetne, ha $a = b = 0$ lenne, amit kizártunk.

Azt kaptuk, hogy $a+b\sqrt{2}$ elem additív, illetve multiplikatív inverze egyaránt ilyen alakú.

Az $a+b\sqrt{2}$ alakú valós számok testet alkotnak, mégpedig éppen a valós test kívánt tulajdonságú résztestét.

Gondolatmenetünk során felhasználtuk, hogy ismerjük a valós testet, és tudtuk, hogy az x^2-2 polinom (egyik) gyöke a $\sqrt{2}$. Ha pusztán a racionális testből kiindulva szeretnénk megkonstruálni a kívánt tulajdonságú testet, akkor ehhez először készítsük el a racionális számokból álló számpárokat, majd értelmezzük a számpárok halmazán az összeadást és a szorzást a következőképpen:

$(a,b) \oplus (c,d) := (a+c, b+d)$, illetve

$(a,b) \otimes (c,d) := (ac+2bd, bc+ad)$.

Könnyen belátható, hogy az így definiált összeadás kommutatív és asszociatív, neutrális eleme a $(0,0)$, az (a,b) additív inverze pedig a $(-a,-b)$; továbbá, hogy a szorzás is kommutatív és asszociatív, disztributív az összeadásra, egységeleme az $(1,0)$, az $(a,b) \neq (0,0)$ (ilyenkor $a^2-2b^2 \neq 0$) multiplikatív inverze pedig az $\left(\frac{a}{a^2-2b^2}, \frac{-b}{a^2-2b^2}\right)$. Vagyis a racionális számpárok a fent definiált összeadásra és szorzásra nézve testet alkotnak.

A $\varphi\colon (a,0) \to a$ leképezés izomorf módon képezi le e test $(a,0)$ alakú elemekből álló részhalmazát a racionális számok testére (hiszen míg $\varphi(a,0) = a$ és $\varphi(b,0) = b$; addig $\varphi\big((a,0) \oplus (b,0)\big) = \varphi(a+b,0)$ és $\varphi\big((a,0) \otimes (b,0)\big) = \varphi(ab,0)$), így a számpárok teste tartalmaz a racionálissal izomorf résztestet. Ha most az $(a,0)$ alakú párokat kicseréljük a nekik megfelelő racionális számokra, és valahányszor a racionális számok között végzünk műveleteket, akkor a $\oplus$ helyett $+$-t, a $\otimes$ helyett pedig $\cdot$-t (vagy semmit sem) írunk, akkor a számpárok így módosított teste már magát

a racionális testet fogja tartalmazni. Mivel tetszőleges (a, b) pár felírható $(a, b) = (a, 0) \oplus (b, 0) \otimes (0, 1)$ alakban, azt is megtehetjük, hogy a $(0, 1)$ párt α-val jelöljük, és a továbbiakban mindenhol $+$-t és $\cdot$-t írunk az összeadás, illetve a szorzás jeleként. Ekkor az (a, b) pár $a + b\alpha$ alakba írható, ahol α éppen az $x^2 - 2$ polinom (egyik) gyökét jelöli, hiszen $(0, 1) \otimes (0, 1) = (2, 0)$.

A fenti eljáráshoz hasonlóan végezhetjük el a racionális test bővítését egy tetszőleges – a racionális test felett irreducibilis – $f(x) = x^2 + qx + r$ másodfokú polinom gyökével (q és r racionális számok). (Ha a polinom nem volna irreducibilis, akkor gyökei racionálisak lennének, így a keresett test maga a racionális test volna.)

Jelöljük α-val az $x^2 + qx + r$ polinomnak azt a gyökét, amellyel bővíteni szeretnénk a racionális testet. A keresett testnek nyilván eleme lesz az összes $a + b\alpha$ alakú komplex szám, ahol a és b racionális. Az $a + b\alpha$ alakú elemek halmaza zárt az összeadásra is és a szorzásra is, hiszen $(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$ és $(a + b\alpha) \cdot (c + d\alpha) = ac + bd\alpha^2 + ad\alpha + bc\alpha$, amiből felhasználva, hogy $\alpha^2 = -q\alpha - r$ (hiszen α gyöke az $x^2 + qx + r$ polinomnak) azt kapjuk, hogy $(a + b\alpha) \cdot (c + d\alpha) = (ac - bdr) + (ad + bc - bdq)\alpha$, vagyis (mivel a, b, c, d, q és r racionális) két ilyen alakú elem szorzata is ilyen alakú. Könnyen ellenőrízhető, hogy az ilyen alakú elemek integritástartományt alkotnak, viszont nehezebb megmutatni, hogy a szorzás a nem 0 elemek halmazán invertálható. Belátható, hogy ha $a + b\alpha \neq 0$, akkor

$$(a + b\alpha)^{-1} = \underbrace{\frac{a - bp}{a^2 - abq - rb^2}}_{\text{racionális}} - \underbrace{\frac{b}{a^2 - abq - rb^2}}_{\text{racionális}} \alpha,$$

vagyis a 0-tól különböző elemek multiplikatív inverzei is ilyen alakúak, tehát az $a + b\alpha$ alakú elemek testet alkotnak, amely nyilván a legszűkebb olyan test, amely tartalmazza a racionális testet is és az $x^2 + qx + r$ polinom α gyökét. (Ugyanezt a testet kaptuk volna, ha a $\sqrt{q^2 - 4r}$ komplex számok valamelyikével bővítettük volna a racionális testet.)

Ha a racionális számpárok segítségével szerettük volna megkonstruálni a kívánt testet, akkor a számpárok halmazán a következőképpen definiáltuk volna az összeadást és a szorzást:

$$(a, b) \oplus (c, d) := (a + c, b + d)$$
$$(a, b) \otimes (c, d) := (ac - bdr, ad + bc - bdq);$$

majd megmutattuk volna, hogy a racionális számpárok testet alkotnak e két műveletre nézve. Ezután észrevettük volna, hogy e test tartalmaz az $(a, 0) \to a$ leképezés szerint a racionális testtel izomorf résztestet, majd felhasználva, hogy $(a, b) = (a, 0) \oplus (b, 0) \otimes (0, 1)$, és az $(a, 0)$ alakú elemek helyére a nekik megfelelő racionális számot, a $\oplus$ helyett $+$-t, a $\otimes$ helyett $\cdot$-t

(vagy semmit sem), a $(0,1)$ pár helyett pedig α-t írva kaptuk volna meg az $a+b\alpha$ alakú elemek testét.

Hasonlóan járhatunk el akkor is, ha az

$$f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$$

racionális együtthatós, a racionális test felett irreducibilis polinom valamelyik gyökével szeretnénk bővíteni a racionális testet. Nyilvánvaló, hogy – α-val jelölve a polinomnak azt a gyökét, amellyel bővítünk – az összes

$$r_0+r_1\alpha+r_2\alpha^2+\ldots+r_{n-1}\alpha^{n-1}$$

alakú elemnek, ahol r_0, r_1, r_2, …, r_{n-1} racionális számok, a műveletek zártsága miatt benne kell lennie a keresett testben. Felhasználva, hogy

$$\alpha^n=-a_{n-1}\alpha^{n-1}-\ldots-a_1\alpha-a_0$$

(hiszen α gyöke az $f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ polinomnak), könnyen belátható, hogy az ilyen alakú elemek halmaza zárt az összeadásra és a szorzásra, sőt integritástartományt alkot.

Azt, hogy egy $r_0+r_1\alpha+r_2\alpha^2+\ldots+r_{n-1}\alpha^{n-1}\neq 0$ elemnek van (ilyen alakú) multiplikatív inverze, a következőképpen láthatjuk be:

Tekintsük a $g(x)=r_0+r_1x+r_2x^2+\ldots+r_{n-1}x^{n-1}$ polinomot.

Mivel $f(x)$ irreducibilis volt a racionális test felett, és $g(x)$ fokszáma kisebb, mint $f(x)$ fokszáma, nincs olyan racionális együtthatós, legalább elsőfokú polinom, amely mindkettőnek osztója lenne, vagyis $\big(g(x),f(x)\big)=1$. A racionális együtthatós (illetve egy tetszőleges test feletti) polinomok gyűrűje euklideszi gyűrű, így teljesül, hogy két polinom legnagyobb (kitüntetett) közös osztója előáll a két polinom lineáris kombinációjaként, vagyis létezik olyan $h(x)$ és $u(x)$ racionális együtthatós polinom, amelyre $1=g(x)h(x)+f(x)u(x)$.

Ekkor a polinomok α helyen felvett helyettesítési értékére $1=g(\alpha)h(\alpha)+f(\alpha)u(\alpha)$-nak kell teljesülnie. Felhasználva, hogy $f(\alpha)=0$, azt kapjuk, hogy $g(\alpha)h(\alpha)=1$, vagyis a $g(\alpha)=r_0+r_1\alpha+r_2\alpha^2+\ldots+r_{n-1}\alpha^{n-1}$ elem multiplikatív inverze az $1=g(x)h(x)+f(x)u(x)$ előállításban szereplő $h(x)$ polinom α helyen felvett helyettesítési értéke, ami $\alpha^n=-a_{n-1}\alpha^{n-1}-\ldots-a_1\alpha-a_0$ miatt szintén felírható a kívánt alakban. Tehát az $r_0+r_1\alpha+r_2\alpha^2+\ldots+r_{n-1}\alpha^{n-1}$ alakú elemek testet alkotnak, és ez a test nyilván a legszűkebb olyan test, amely tartalmazza a racionális testet is és az $f(x)=x^n+a_{n-1}x^{n-1}+\ldots+a_1x+a_0$ polinom α gyökét is. (Megtehettük volna azt is, hogy a számpárokon alapuló konstrukcióhoz hasonlóan a racionális számokból álló szám n-eseken definiálunk egy megfelelő összeadást és szorzást, és az így kapott testbe ágyazzuk be a racionális testet.)

Gondolatmenetünk során sehol nem használtuk ki, hogy éppen a racionális testet bővítettük egy algebrai számmal, egy tetszőleges test bővítése egy, a test feletti algebrai elemmel ugyanígy történik.

Legyen T egy tetszőleges test, és α algebrai elem a T test felett. Ekkor van olyan T feletti polinom, amelynek α gyöke. Az ilyen tulajdonságú polinomok közül keressük meg a legkisebb fokszámúakat, és azok közül is azt, amelyiknek a főegyütthatója 1. Ezt a polinomot α már egyértelműen meghatározza, hiszen ha két ilyen tulajdonságú polinomnak is gyöke lenne α, akkor a két polinom különbségének is, ami viszont ha mindkét polinom főegyütthatója 1, akkor kisebb fokszámú lenne, mint a két minimális fokszámú polinom, ami ellentmondás.

12.4. Definíció. Legyen α algebrai elem a T test felett. Azok közül a T feletti polinomok közül, amelyeknek α gyöke, α *definiáló polinomjának* vagy *minimálpolinomjának* nevezzük a minimális fokszámú, 1 főegyütthatójú polinomot.

12.1. Tétel. *Ha α algebrai elem a T test felett, akkor az α definiáló polinomja irreducibilis T felett.*

Bizonyítás. Legyen $f(x) \in T[x]$ az α definiáló polinomja. Ha $f(x)$ nem lenne irreducibilis, akkor volnának olyan $g(x)$ és $h(x) \in T[x]$, legalább elsőfokú polinomok, amelyekre $f(x) = g(x)h(x)$.

Ekkor azonban $f(\alpha) = 0 = g(\alpha)h(\alpha)$ miatt α gyöke lenne $g(x)$ és $h(x)$ valamelyikének, ami ellentmondana annak, hogy $f(x)$ minimális fokszámú azok között a polinomok között, amelyeknek α gyöke. □

Tapasztalataink alapján kimondhatjuk a következő tételt:

12.2. Tétel. *Ha α algebrai elem a T test felett, és definiáló polinomja n-edfokú, akkor a $T(\alpha)$ test – azaz a legszűkebb olyan test, amely T-t is és α-t is tartalmazza – minden eleme felírható $a_0 + a_1\alpha + a_2\alpha^2 + \ldots + a_{n-1}\alpha^{n-1}$ alakban, ahol $a_0, a_1, \ldots, a_{n-1} \in T$.*

12.5. Definíció. A T test α algebrai elemmel történő egyszerű bővítése esetén a *testbővítés fokának* nevezzük az α definiáló polinomának a fokszámát.

Például:

1. A komplex számok teste másodfokú bővítése a valós számok testének.
2. Az $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ alakú számok teste, ahol a, b, c racionális, harmadfokú bővítése a racionális számok testének.

A T testet és az α – T felett algebrai – elemet tartalmazó legszűkebb testhez a következőképp is eljuthatunk:

Legyen az α definiáló polinomja $f(x)$, és tekintsük a $T[x]$ polinomgyűrűben mindazokat a polinomokat, amelyek többszörösei $f(x)$-nek. Ezek éppen azok a polinomok lesznek, amelyeknek α gyöke, hiszen egyrészt ha α gyöke $f(x)$-nek, akkor nyilván gyöke $f(x)$ minden többszörösének is; másrészt ha $h(x)$ egy olyan polinom, amelynek α gyöke, akkor $h(x)$-et maradékosan osztva $f(x)$-szel azt kapjuk, hogy létezik olyan $q(x)$ és $r(x)$ polinom, amelyekre $h(x) = f(x)q(x) + r(x)$, ahol $r(x)$ fokszáma kisebb $f(x)$ fokszámánál. Ez azonban csak úgy lehetséges, ha $r(x) = 0$ – vagyis ha $h(x)$ többszöröse $f(x)$-nek –, mert ellenkező esetben abból, hogy

$$\underbrace{h(\alpha)}_{=0} = \underbrace{f(\alpha)}_{=0} q(\alpha) + r(\alpha),$$

az következne, hogy α gyöke $r(x)$-nek, ami ellentmondana $f(x)$ minimális fokszámú tulajdonságának.

Jelöljük a polinomgyűrű $f(x)$ többszöröseiből álló részhalmazát I_f-fel. Könnyen belátható, hogy I_f részgyűrű, sőt ideál $T[x]$-ben.

Ha most elkészítjük az I_f szerinti maradékosztályokat, akkor megkapjuk $T[x]$ egy faktorgyűrűjét (és mivel I_f-ben éppen azok a polinomok vannak, amelyeknek α gyöke, az osztályozás során azok a polinomok fognak egy osztályba kerülni, amelyeknek az α helyen felvett helyettesítési értékük egyenlő).

Belátható, hogy ezt a faktorgyűrűt a $\overline{g(x)} \to g(\alpha)$ leképezés izomorf módon képezi le $T(\alpha)$-ra, ami azt jelenti, hogy a keresett $T(\alpha)$ testhez úgy is eljuthatunk, hogy a $T[x]$ polinomgyűrűt faktorizáljuk az α definiáló polinomjának többszöröseiből álló ideálja szerint, azaz:

12.3. Tétel. *Ha α algebrai elem a T test felett, és α definiáló polinomja $f(x)$, akkor a $T(\alpha)$ test izomorf a $T[x]/\big(f(x)\big)$ maradékosztálygyűrűvel (ahol $\big(f(x)\big)$ az $f(x)$ által generált ideál).*

Algebrai bővítésekkel kapcsolatban további kérdések is felvethetők. Kereshetjük például azt a legszűkebb testet, amelyben egy T feletti $f(x)$ polinomnak már minden gyöke benne van, vagyis azt a legszűkebb testet, amely felett $f(x)$ már lineáris polinomok szorzatára esik szét. Bizonyítható, hogy tetszőleges T test esetén, tetszőleges T feletti polinomhoz izomorfia erejéig egyértelműen létezik ilyen test. Ezt a testet az $f(x)$ polinomhoz tartozó *felbontási testnek* nevezzük.

Az algebra alaptételéből tudjuk, hogy a komplex test felett már minden legalább elsőfokú komplex együtthatós polinom felbontható elsőfokú polinomok szorzatára. Általában is kereshetjük azt a legszűkebb testet, amely az

összes T feletti polinom összes gyökét tartalmazza. Az ilyen tulajdonságú testet a T test *algebrai lezártjának* nevezzük. Bizonyítható, hogy tetszőleges T testnek – izomorfia erejéig – egyértelműen létezik algebrai lezártja. A valós test algebrai lezártja a komplex test, a komplex test algebrai lezártja pedig önmaga. Megmutatható, hogy az algebrai számok testet alkotnak, így a racionális test algebrai lezártja az algebrai számok teste. Az is belátható, hogy algebrai együtthatós polinomok gyökei is algebrai számok (vagyis algebrai bővítések egymásutánja is algebrai), így az algebrai számok teste is önmagának az algebrai lezártja.

Az algebrai lezártnak van más (nyilván a fentivel ekvivalens) definíciója, nevezetesen: algebrai lezártnak szokás azt a kiinduló testet tartalmazó legszűkebb testet nevezni, amelynek minden polinomja megoldható a testen belül. Nem bizonyítjuk a két deifníció ekvivalenciáját.

Ha egy testet addig bővítgetünk, amíg eljutunk egy olyan testhez, amelyet már nem lehet további algebrai elemével bővíteni (azaz minden polinomjának minden gyökét tartalmazza), akkor ezt a *test lezártjának* nevezzük. Ismerünk olyan testet, amelyben minden polinomnak minden gyöke a test eleme, azaz az irreducibilis polinomok éppen az elsőfokúak: ez a komplex számtest. A racionális test lezártja a komplex számtest. A valós számtesté is. A komplex számtest lezártja önmaga, ezt *algebrailag zárt testnek* nevezzük.

Egyszerű testbővítés transzcendens elemmel

Ha például a valós testnek azt a legszűkebb résztestét keressük, amely tartalmazza a racionális testet is és a π-t is, akkor a szorzás zártsága miatt π minden hatványának benne kell lennie a keresett testben. Az összeadás és a szorzás zártsága miatt ekkor a π hatványainak összes – racionális együtthatós – lineáris kombinációjának is benne kell lennie a keresett testben. Ahhoz, hogy a 0-tól különböző elemek halmazán a szorzás invertálható legyen, minden lineáris kombináció multiplikatív inverzének, és így az összes

$$\frac{a_n\pi^n + a_{n-1}\pi^{n-1} + \cdots + a_1\pi + a_0}{b_k\pi^k + b_{k-1}\pi^{k-1} + \cdots + b_1\pi + b_0}$$

alakú elemnek ($a_i, b_j \in \mathbb{Q}$, $b_k \neq 0$, $n, k \in \mathbb{N}$) benne kell lennie a keresett testben. Könnyen ellenőrízhető, hogy az ilyen alakú elemek már testet alkotnak, amely izomorf a racionális együtthatós polinomok gyűrűjéhez tartozó hányadostesttel.

Gondolatmenetünk során sem a racionális test, sem a π speciális tulajdonságait nem használtuk ki, így kimondhatjuk a következő tételt:

12.4. Tétel. *Legyen α transzcendens elem a T test felett. Ekkor a $T(\alpha)$ test izomorf a T feletti polinomgyűrű hányadostestével. (V. ö. 11.1. Megjegyzés.)*

Néhány mellékes megjegyzés a valós számokról

Mint már láttuk, az ismerős testek közül a komplex számok teste egyszerű algebrai bővítése a valós testnek, az algebrai számok teste pedig egyszerű algebrai bővítések egymásutánjával (végtelen sokkal) kapható meg a racionális testből, ezzel szemben a valós test nem kapható meg algebrai bővítésekkel a racionális testből.

A valós számok felépítése a racionális számokból az analízis eszközeinek felhasználásával történik. Mint tudjuk, a racionális számok testére nem teljesül a Cantor-axióma (azaz nem minden egymásba ágyazott, zárt, racionális intervallumsorozatnak van közös racionális pontja), amit úgy is fogalmazhatunk, hogy vannak olyan végtelen, racionális számokból álló konvergens számsorozatok, amelyek határértéke nem racionális szám. A kérdés az, hogy miként lehetne olyan testet konstruálni, amely már tartalmazza minden konvergens sorozatának a határértékét, és amely tartalmaz egy, a racionális testtel izomorf résztestet. A konstrukció lényege az, hogy a valós számokat a racionális számokból álló konvergens sorozatok határértékeiként képzeljük el. Ez részletesebben (de még mindig vázlatosan) körülbelül a következőképp történhet:

1. Értelmezzük a racionális számok halmazán a számsorozatok konvergenciájának fogalmát. Ezt most nem célszerű a szokásos módon – a határérték fogalmának felhasználásával – megtenni, hiszen akkor csak azokat a racionális sorozatokat tekinthetnénk konvergensnek, amelyek határértéke racionális, hanem a Cauchy-féle konvergenciakritérium segítségével tesszük meg (azaz (a_n) konvergens, ha $\forall \varepsilon > 0$ $(\varepsilon \in \mathbb{Q})$ számhoz létezik olyan n_0 küszöbindex, amelyre $\forall k, m \geq n_0$ esetén teljesül, hogy $|a_k - a_m| < \varepsilon$). Egy sorozat konvergenciájából következik, hogy Cauchy-konvergens is, de fordítva nem. Éppen ezt akarjuk kihasználni: azok a racionális számsorozatok, amelyek a valósban konvergensek, nem konvergensek a racionálisban, azonban Cauchy-konvergensek. Ezen sorozatok határártékeit hozzávéve a raiconális számokhoz, megkapjuk a valósokat.

2. Induljunk ki a Cauchy-konvergens racionális számsorozatok A halmazából.

3. Definiáljuk két sorozat összegét és szorzatát a szokásos módon: ha $(a_n) \in A$ és $(b_n) \in A$, akkor legyen $(a+b)_n := a_n + b_n$, illetve $(a \cdot b)_n := a_n \cdot b_n$. Belátható, hogy az így értelmezett $(A, +, \cdot)$ egységelemes kommutatív gyűrű, amelynek zéruseleme a konstans 0, egységeleme pedig a konstans 1 sorozat.

4. Az A halmazon tekintsünk ekvivalensnek két sorozatot, ha a különbségük nullsorozat. Ekkor nyilvánvalóan pontosan azok a sorozatok kerülnek egy osztályba, amelyenek létezik (valósban értelmezett) határértéke, és az ugyanannyi.

5. Belátjuk, hogy az így kapott osztályozás kompatibilis (meggondolható, hogy az $(A, +, \cdot)$ gyűrűnek a nullasorozatok halmaza részgyűrűje, sőt ideálja, és eszerint az ideál szerint osztályozva a gyűrűt ugyanezt az osztályozást kapnánk), így a kapott osztályok az osztályműveletekre nézve szintén egységelemes kommutatív gyűrűt alkotnak, majd belátjuk, hogy ez a (faktor)gyűrű test.

6. Megmutatjuk, hogy ez a test tartalmaz a racionális testtel izomorf résztestet (azoknak az osztályoknak, amelyekben az osztályt alkotó sorozatok (közös) határértéke racionális szám, megfeleltetjük ezt a határértéket), majd végrehajtjuk a beágyazást (a racionális testtel izomorf részt kicseréljük magára a racionális testre). Az így kapott test lesz a valós számok teste (melyről az is belátható, hogy már „teljes" test abban az értelemben, hogy minden (Cauchy-értelemben) konvergens sorozatának határértékét is tartalmazza).

Testbővítés vektorterekkel

Eddig a testbővítést úgy végeztük, hogy kerestük azt a legszűkebb testet, amely tartalmazta a kiinduló testet és azt az elemet is, amellyel bővíteni akartunk.

Most egy kicsit más szemszögből is ránézünk erre a konstrukcióra, egy más módon is megvizsgáljuk testbővítést. A teljesség kedvéért – hogy a fejezet önmagában is teljes legyen – esetleg megismétlünk néhány olyan dolgot, amelyet már korábban is elmondtunk.

Először ismételjünk át néhány fogalmat.

Test: $(T, +, \cdot)$ test, ha T zárt az összeadásra, az összeadás kommutatív, asszociatív és invertálható; T zárt a szorzásra, a szorzás a $T \setminus \{0\}$ halmazon kommutatív, asszociatív, invertálható, valamint a szorzás disztributív az összeadásra nézve.

Vektortér: Ha $(T, +, \cdot)$ test és $(V, \oplus)$ csoport, továbbá létezik olyan *külső szorzat* T és V között, hogy ha $1 \in T$ a T multiplikatív egysége, és $\forall t_1, t_2 \in \in T$, $\mathbf{v}_1, \mathbf{v_2} \in V$ elemre teljesülnek a következő tulajdonságok:

1. Létezik a $t\mathbf{v}$ szorzat, és az eleme V-nek;
2. $(t_1 + t_2)\mathbf{v}_1 = t_1\mathbf{v}_1 + t_2\mathbf{v}_1$
3. $t_1(\mathbf{v}_1 + \mathbf{v}_2) = t_1\mathbf{v}_1 + t_1\mathbf{v}_2$
4. $t_1(t_2\mathbf{v}_1) = (t_1t_2)\mathbf{v}_1$
5. $1\mathbf{v}_1 = \mathbf{v}_1$

Bázisnak nevezünk egy olyan vektorrendszert, amely lineárisan független (vagyis csak a triviális lineáris kombinációja állítja elő a $\mathbf{0}$ vektort) és generátorrendszert (azaz a vaktortér minden elemét előállítja valamely lineáris kombinációja).

Mint ismeretes, egy vektortér minden bázisának ugyanannyi eleme van.

A vektorrendszer lineáris függetlenségének három ekvivalens megfogalmazása:

– Nincs olyan vektora a vektorrendszernek, amely előállna a többi lineáris kombinációjaként.

– Csak a triviális lineáris kombinációja állítja elő a $\mathbf{0}$ vektort.

– Ha egy, a vektorrendszerhez nem tartozó vektor előáll a vektorrendszer lineáris kombinációjaként, akkor az az előállítás egyértelmű.

Ennek megfelelően a lineáris összefüggőség három ekvivalens megfogalmazása:

– Van olyan vektora a vektorrendszernek, amely előáll a többi lineáris kombinációjaként.

– Nem csak a triviális lineáris kombinációja állítja elő a $\mathbf{0}$ vektort.

– Ha egy, a vektorrendszerhez nem tartozó vektor előáll a vektorrendszer lineáris kombinációjaként, akkor az az előállítás nem egyértelmű.

Még egy fontos tulajdoinságra emlékeztetünk:

A vektortér dimenziója a vektortér bázisának elemszáma, és bár több bázisa is lehet egy vektortérnek, ez a szám független attól, hogy melyik bázist választjuk ki.

Ezután egy érdekes észrevételre (12.1. Állítás) alapozva egy egészen más testbővítési modellt mutatunk be.

12.1. Állítás. *Ha a $(T_0, +, \cdot)$ testnek bővítése a $(T_1, +, \cdot)$ test, akkor T_1 a T_1-beli összeadással és a T_0-beli szorzással mint skalárral való szorzással vektorteret alkot T_0 felett.*

Bizonyítás. Idézzük fel a vektortér-axiómákat, és közben vizsgáljuk meg, hogy teljesülnek-e. $\forall \lambda, \mu \in T_0 \subset T_1$, $\forall \mathbf{a}, \mathbf{b} \in T_1$ esetén:

$(T_0, +, \cdot)$ test, $(T_1, +)$ csoport. Ez nyilván teljesül.

1. $\lambda\mathbf{a} \in T_1$. Ez is nyilvánvaló, hiszen mindkét tényező T_1-ben van, T_1 pedig zárt a szorzásra.

2. $(\lambda+\mu)\mathbf{a} = \lambda\mathbf{a}+\mu\mathbf{a}$. Ez is teljesül, mert $\lambda, \mu, \mathbf{a}$ mindegyike T_1-ben van, ott pedig érvényes a szorzás összeadásra vonatkozó disztributivitása.

3. $\lambda(\mathbf{a}+\mathbf{b}) = \lambda\mathbf{a}+\lambda\mathbf{b}$. Ez is teljesül, mert $\lambda, \mathbf{a}, \mathbf{b}$ mindegyike T_1-ben van, ott pedig érvényes a szorzás összeadásra vonatkozó disztributivitása.

4. $\lambda(\mu\mathbf{a}) = (\lambda\mu)\mathbf{a}$. Ez is teljesül, mert $\lambda, \mu, \mathbf{a}$ mindegyike T_1-ben van, ott pedig érvényes a szorzás asszociativitása.

5. $1 \in T_0$ mellett $1 \cdot \mathbf{a} = \mathbf{a}$. Ez is teljesül, mert az 1 a T_1-ben is multiplikatív egységelem. □

Például:

1. A komplex számtest vektorteret alkot a valós számtest fölött ($\mathbb{R} \subset \mathbb{C}$). Vajon hány dimenziós ez a vektortér?

   Nyilván azt kell kiderítenünk, hogy egy komplex számot hány valós számmal írhatunk le egyértelműen. Mivel minden komplex szám egyértelműen írható fel egy valós számpárként, a komplex számok számteste kétdimenziós a valós számtest felett: $a + bi$, pontosabban $a \cdot 1 + b \cdot i$, ahol $a, b \in \mathbb{R}$, $1, i \in \mathbb{C}$.

2. A valós számtest vektortér a racionális számtest fölött, mert $\mathbb{Q} \subset \mathbb{R}$. Vajon mennyi a dimenziója?

   Az a kérdés, hogy hány racionális számmal írható le egyértelműen egy-egy valós szám.

   Mivel a racionális számok száma megszámlálhatóan végtelen, így megszámlálható (véges vagy végtelen) vektorrendszerrel csak megszámlálható sok vektort tudunk felírni. Márpedig a valós számok száma nem megszámlálható, így a bázis elemszám sem megszámlálható.

   Eszerint az is elképzelhetetlen, hogy a racionális számokat egyenként bővítve eljuthatunk a valós számokhoz. (Nemcsak azért, mert végtelen sok elemmel kellene bővíteni – ezt még el tudjuk képzelni –, hanem azért sem, mert nem lehet sorbarendezni a számokat, amelyekkel bővítenünk kell.)

3. A $(\mathbb{Q}, +, \cdot)$ testnek bővítése az $a + bi$ alakú számok, ahol $a, b \in \mathbb{Q}$, i pedig az imaginárius egység. A bővebb test dimenziója (csakúgy, mint az első példában) 2.

4. A $(\mathbb{Q}, +, \cdot)$ testnek bővítése az $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ alakú számok, ahol $a, b, c \in \mathbb{Q}$. A dimenzió ezúttal 3, hiszen minden szám az 1, $\sqrt[3]{2}$, $\sqrt[3]{4}$ számok racionális lineáris kombinációja.

5. A $(\mathbb{Q}, +, \cdot)$ testnek bővítése az $a + b\sqrt{4}$ alakú számok, ahol $a, b \in \mathbb{Q}$. Mivel azonban $\sqrt{4}$ maga is eleme $\mathbb{Q}$-nak, a dimenzió 1. (Ez nem valódi bővítés.)

A 12.2. és a 12.3. Definíció segítségével idézzük fel, hogy mit jelent az egyszerű testbővítés, az algebrai, illetve a transzcendens elem, vamaint az algebrai, illetve transzcendens szám.

Ezúttal is csak az egyszerű testbővítéssel foglalkozunk.

Egyszerű testbővítés

Egyszerű testbővítés algebrai elemmel

12.6. Definíció. T_1 vektortér T_0 feletti dimenzióját a *testbővítés fokának* nevezzük.

Megjegyzés. Korábban a testbővítés fokának a definiáló polinom fokszámát neveztük. Ez nem ugyanaz a definíció. E perctől kezdve az a legfontosabb, hogy bebizonyítsunk, hogy ez a definíció ugyanazt eredményezi, mint a korábbi.

Példák:

1. A valós számok testbővítésével kapjuk a komplex számokat, a bővítés foka 2, mert a komplex számok mint vektortér kétdimenziós a valós fölött. Mivel minden valós számot $a + bi$ alakban írhatunk, ezért a testbővítés foka 2. Mivel $\sqrt{-1}$ definiáló polinomja másodfokú, látjuk, hogy ebben a konkrét esetben a testbővítés fokára adott két definíció ugyanazt eredményezi.

2. A valósok dimenziója végtelen a racionális fölött, a testbővítés foka tehát végtelen.

3. A racionális számok $\mathbb{Q}$ halmazát a $\sqrt{5}$-tel bővítve a $\mathbb{Q}(\sqrt{5})$ testet kapjuk. Ez a legszűkebb olyan test, amely tartalmazza $\mathbb{Q}$-t és $\sqrt{5}$-öt is. Ennek a testnek az elemei $a + b\sqrt{5}$ alakúak, azaz két, a bővebb testből vett elem (az 1 és a $\sqrt{5}$) racionális lineáris kombinációjaként írhatók fel. A bővítés foka a vektortér dimenziója: 2. Egyébként más bázisvektorokat is választhattunk volna, például $\sqrt{5}$ helyett $1/\sqrt{5}$-öt. Ekkor az $a + b\sqrt{5} = a + 5b \cdot (1/\sqrt{5})$ felírást kapjuk.

4. Ha a racionális számokat a $\sqrt[3]{2}$-vel bővítjük, akkor a testbővítéssel kapott testben minden számot $a + b\sqrt[3]{2} + c\sqrt[3]{4}$ alakban írhatunk ($a, b, c \in \in \mathbb{Q}$), ezért a testbővítés foka 3. Mivel $\sqrt[3]{3}$ definiáló polinomja harmadfokú, látjuk, hogy ebben a konkrét esetben is ugyanazt eredményezi a testbővítés fokára adott két definíció.

   Megjegyezzük, hogy $\sqrt[3]{2}$ valóban a fenti testet generálja:

   Mivel bármely két eleme különböző, $a_1+b_1\sqrt[3]{2}+c_1\sqrt[3]{4} = a_2+b_2\sqrt[3]{2}+\sqrt[3]{4}$-ből $(a_1 - a_2) + (b_1 - b_2)\sqrt[3]{2} + (c_1 - c_2)\sqrt[3]{2}^2 = 0$ lenne, vagyis $\sqrt[3]{2}$

gyöke lenne egy másodfokú racionális egyenletnek, ami nem igaz. (A másodfokú racionális együtthatós polinomok gyökei nem $\sqrt[3]{2}$ alakúak.)

Valóban testet kapunk, ezt könnyen ellenőrizhetjük.

Benne van $\mathbb{Q}$ és $\sqrt[3]{2}$ is.

Láttuk, hogy a valós számtest ugyan bővítése a racionális számtestnek, a dimenziója (mint vektortér) viszont nem megszámlálhatóan végtelen. Ezért egészen biztosak lehetünk benne, hogy a racionális számokat nem elegendő a négyzetgyökeikkel (sőt, köbgyökeikkel, negyedik, ötödik stb gyökeikkel) bővíteni ahhoz, hogy megkapjuk az összes valós számot.

A racionális együtthatós polinomok gyökeinek száma még mindig „csak" megszámlálhatóan végtelen. Megszámlálhatóan végtelen sok elemmel való bővítés után még mindig „csak" megszámlálhatóan végtelen testet kapunk. (Egyébként érthető is, hogy nem minden valós szám gyöke valamely racionális együtthatós polinomnak, hiszen vannak transzcendens számok. Másrész viszont most éppen azt bizonyítottuk, hogy az algebrai számok száma megszámlálhatóan végtelen, tehát biztos, hogy vannak transzcendens számok.)

Legyen tehát T egy test, $\alpha \notin T$ egy algebrai elem T felett. Legyen f olyan T-beli együtthatós polinom, amelynek gyöke α.

A következőkben megkonstruáljuk a $T(\alpha)$ testet.

12.2. Állítás. *Létezik olyan legalacsonyabb fokú, 1 főegyütthatójú polinom, amelynek α gyöke, és ez a polinom egyértelmű.*

Bizonyítás. Mivel α algebrai elem, létezik olyan f polinom, amelynek α gyöke. (Ennek a polinomnak a fokszáma nagyobb 1-nél, mert α nem eleme T-nek.) Az összes olyan polinom közül, amelynek α gyöke létezik legalacsonyabb fokszámú, és ez a fokszám tehát legalább 2.

Most belátjuk, hogy az 1 főegyütthatójú polinomok között csak egy olyan minimális fokszámú van, amelynek gyöke az α.

Ha α gyöke két legalacsonyabb fokú polinomnak, akkor ezeket a főegyütthatójukkal végigosztva két főpolinomot kapunk, amelyeknek gyöke α. Mivel mindkettőnek gyöke α, így a különbségüknek is gyöke. Ennek a polinomnak a fokszáma viszont kisebb lesz, mint az eredeti polinomok fokszáma. Ez – a fokszám minimalitása miatt – csak úgy lehet, ha az eredmény az azonosan 0 polinom, vagyis a két főpolinom egyenlő, a két kiinduló polinom egymásnak asszociáltja, azaz a számszorosa. Eszerint minden minimális fokszámú polinom, amelynek gyöke α, ugyanannak a főpolinomnak az asszociáltja (számszorosa). □

12.7. Definíció. Azt a minimális fokszámú főpolinomot, amelynek α gyöke, *α definiáló polinomjának* nevezzük.

Az előző állítás szerint ez a polinom egyértelmű, tehát a definíció korrekt. Ezúttal is fontos megállapítanunk a következőt:

12.3. Állítás. *Minden definiáló polinom irreducibilis.*

Bizonyítás. Ha α definiáló polinomja (f) felbontható lenne két alacsonyabb, de nyilván nem nulladfokú polinom szorzatára, $f = g \cdot h$, akkor $0 = f(\alpha) = g(\alpha) \cdot h(\alpha)$ teljesül, amiből az következik, hogy $g(\alpha)$ vagy $h(\alpha)$ egyenlő nullával, mert $g(\alpha)$ és $h(\alpha)$ eleme a $K(\alpha)$ testnek, amely (mint minden test) nullosztómentes. A két polinom egyikének tehát biztosan gyöke α, tehát van olyan polinom, amely alacsonyabb fokú, mint f és mégis gyöke α. Ez azonban ellentmond annak, hogy f minimális fokszámú volt. □

Megjegyzés. Két különböző elem definiáló polinomja megegyezhet, például $(1 - i)$ és $(1 + i)$ definiáló polinomja a valós felett (és a racionális, sőt a nem test egészek felett is) $x^2 - 2x + 2$.

12.5. Tétel. *Legyen $(T, +, \cdot)$ test, az α elemmel való egyszerű algebrai bővítése pedig a $(T_1, +, \cdot)$ test. Ekkor a testbővítés foka (T_1 dimenziója T fölött) egyenlő az algebrai elem definiáló polinomjának fokszámával.*

Megjegyzés. Ezzel a tétellel lerójuk egy adósságunkat: biztosítjuk, hogy a testbővítés fokára korábban adott korábbi (12.5.) és az ebben a részben adott 12.6. Definíciók ekvivalensek.

Bizonyítás. Bővítsük a T testet az α elemmel, és legyen az α elem definiáló polinomja

$$f(x) = a_0 + a_1 x + a_2 x^2 + \cdots + a_{d-1} x^{d-1} + x^d, \qquad \text{amelyre tehát}$$
$$f(\alpha) = a_0 + a_1 \alpha + a_2 \alpha^2 + \cdots + a_{d-1} \alpha^{d-1} + \alpha^d = 0$$

(az együtthatók T-beliek). Mivel $T_1 \geq T$, így T_1 vektortér a T felett. Szeretnénk megállapítani a dimenzióját.

Belátjuk, hogy az

$$1, \alpha, \alpha^2, \ldots, \alpha^{d-1} \tag{12.1}$$

vektorrendszer bázis T_1-ben.

(Ezzel be is bizonyítjuk a tételt, mert akkor ez egy d-elemű bázis, tehát a vektortér dimenziója d, és a polinom fokszáma is d.)

A bázis három ismert és ekvivalens definíciója közül azt fogjuk használni, hogy egy vektorrendszer bázis, ha minden vektortérbeli elemet pontosan egyféleképpen állít elő a lineáris kombinációival.

1. Belátjuk, hogy ha egy vektor (T_1-beli elem) felírható a (12.1)-ben adott vektorrendszer (T-beli elemekkel vett) lineáris kombinációjaként, akkor az csakis egyértelmű lehet. Tegyük fel ugyanis, hogy valamely elem (z) kétféleképpen is előáll a bázis elemeinek lineáris kombinációjaként, azaz:

   $$z = k_0 + k_1\alpha + k_2\alpha^2 + \cdots + k_{d-1}\alpha^{d-1} = l_0 + l_1\alpha + l_2\alpha^2 + \cdots + l_{d-1}\alpha^{d-1},$$

   vagyis

   $$(k_0 - l_0) + (k_1 - l_1)\alpha + (k_2 - l_2)\alpha^2 + \cdots + (k_{d-1} - l_{d-1})\alpha^{d-1} = 0.$$

   Ez α-nak egy d-nél alacsonyabb fokú polinomja, ami – mivel a definiáló polinom minimális fokszámú – csak úgy lehetséges, ha ez az azonosan 0 polinom, vagyis a két eredeti polinom egyenlő volt, z két felírása egy és ugyanaz.

2. Most pedig bebizonyítjuk, hogy minden T_1-beli elem előáll

   $$k_0 + k_1\alpha + k_2\alpha^2 + \cdots + k_{d-1}\alpha^{d-1}$$

   alakban.

   (a) Először tetszőleges polinomra bebizonyítjuk, hogy az α helyen felvett helyettesítési értéke felírható α-nak egy legfeljebb $(d-1)$-edfokú polinomjaként. Legyen ezért g egy tetszőleges polinom. Ha g fokszáma kisebb, mint d, akkor készen vagyunk. Ellenkező esetben osszuk g-t maradékosan α definiálópolinomjával, f-fel: $g = fq + r$, ahol r fokszáma legfeljebb annyi, mint f-é, vagyis $d-1$. Mivel

   $$g(\alpha) = f(\alpha) \cdot g(\alpha) + r(\alpha) = 0 \cdot g(\alpha) + r(\alpha) = r(\alpha),$$

   így azt kaptuk, hogy tetszőleges g polinomra $g(\alpha)$ egyenlő α-nak egy legfeljebb $(d-1)$-edfokú polinomjával.

   Ez végsősoron azt is jelenti, hogy α tetszőleges polinomja felírható a (12.1) vektorrendszer T-beli lineáris kombinációjaként.

   (b) Belátjuk, hogy az α-nak legfeljebb $(d-1)$-edfokú T-beli együtthatós polinomjaként felírt elemek (jelöljük T'-vel) testet alkotnak.

   Hogy világosan értsük: ennek a halmaznak az elemei a legfeljebb $(d-1)$-edfokú polinomok α-ban felvett helyettesítési értékei.

A helyettesítési értékeken a műveleteket így értelmeztük: ha z_1, illetve z_2 valamely p_1, illetve p_2 polinom α-ban vett helyettesítési értéke, akkor $z_1 + z_1 := (p_1 + p_2)(\alpha)$ és $z_1 \cdot z_1 := (p_1 \cdot p_2)(\alpha)$.

A polinomokra a műveleti tulajdonságok ($T[x]$ polinomgyűrű részhalmazáról lévén szó) biztosan teljesülni fognak, ezeket tehát nem fogjuk ellenőrizni. Az α-ban vett helyettesítési értékekre hasonlóan teljesülnek a műveleti tulajdonságok.

A zártságot és az invertálhatóságot be kell még bizonyítanunk.

Az nyilvánvaló, hogy két legfeljebb $(d-1)$-edfokú T-beli együtthatós polinom összege is ilyen tulajdonságú, vagyis két T'-beli elem összege is T'-beli. A szorzatokra hasonló teljesül az (a) pontban látottak miatt. (Vagyis ha két polinom szorzásakor a fokszám nagyobbá válna, mint $d-1$, akkor van olyan polinom, amelynek a fokszáma kisebb d-nél, és a helyettesítési értékeik α-ban egyenlők.) Eszerint T' zárt a két műveletre.

Az additív inverzeik is nyilván T'-beliek.

Az már kevésbé nyilvánvaló, hogy egy T'-beli elem multiplikatív inverze is T'-höz tartozik. Legyen $g(\alpha) \in T'$, azaz g az α-nak egy legfeljebb $(d-1)$-edfokú polinomja. Bebizonyítjuk, hogy $\frac{1}{g}(\alpha) = \frac{1}{g(\alpha)} \in T'$. Mivel f – az α definiáló polinomja – irreducibilis, így minden polinomhoz, nevezetesen g-hez is relatív prím (csak konstans polinom lehet a közös osztójuk): $(f, g) = 1$. Ekkor (az euklideszi algoritmus következményeként) léteznek olyan u és v polinomok, amelyekre

$$fu + gv = 1.$$

Helyettesítsünk α-t a polinomokba:

$$1 = f(\alpha) \cdot u(\alpha) + g(\alpha) \cdot v(\alpha) = 0 \cdot u(\alpha) + g(\alpha) \cdot v(\alpha) = \\ = g(\alpha) \cdot v(\alpha).$$

Ebből pedig már következik, hogy $\frac{1}{g(\alpha)} = v(\alpha)$. Ha v fokszáma túl nagy lenne (nagyobb, mint $d-1$), akkor $v(\alpha)$-hoz mint az α egy polinomja az (a) pont szerint található egy legfeljebb $(d-1)$-edfokú polinom, amely egyenlő vele. Így biztos, hogy $\frac{1}{g(\alpha)} \in T'$.

Összefoglalva: T' zárt az összeadásra, a szorzásra, az additív és a multiplikatív inverz képzésére, teljesülnek rá a kirótt műveleti tulajdonságok, vagyis T' test.

(c) Végül azt látjuk be, hogy T_1 minden eleme α-nak egy legfeljebb $(d-1)$-edfokú T-beli együtthatós polinomja.

Nyilvánvaló, hogy $T_1 \leq T'$, mert T' olyan test, amely tartalmazza T minden elemét és α-t is.

Mivel T' az α-nak legfeljebb $(d-1)$-edfokú polinomjait tartalmazza, csak ilyenek lehetnek T_1-ben is.

Ebből következik, hogy T_1-nek minden eleme felírható α-nak egy legfeljebb $(d-1)$-edfokú polinomjaként, az (a) pont szerint viszont minden ilyen felírható az (12.1) vektorrendszer T-beli elemekkel vett lineáris kombinációjaként

Ezzel bebizonyítottuk a tétel állítását is. □

Megjegyzés. Végső soron T_1 nem más, mint a $T[x]$ polinomgyűrűnek f által generált ideál szerinti faktorgyűrűje, amely történetesen test.

Megjegyzés. A tétel bizonyításában az okozza a nehézséget, hogy egyszerre kell gondolnunk a T-feletti polinomgyűrűre – abban a polinomgyűrűk számelméletére –, az α-nak T-beli együtthatós polinomjaira, ezek helyettesítési értékeire (T_1 elemei), illetve az α egyes hatványainak T-beli együtthatókkal vett lineáris kombinációira.

Először is fontos látni, hogy a bővített testben a műveleteket miként értelmeztük: ha z_1, illetve z_2 az α-nak valamely p_1, illetve p_2 polinomja, akkor egyrészt $p_1(\alpha) = z_1$, $p_2(\alpha) = z_2$, másrészt

$$\underbrace{z_1 + z_1}_{\in T_1} := \underbrace{(p_1 + p_2)}_{T[x]}(\alpha) = p_1(\alpha) + p_2(\alpha) \qquad \text{és}$$

$$\underbrace{z_1 \cdot z_1}_{\in T_1} := \underbrace{(p_1 \cdot p_2)}_{T[x]}(\alpha) = p_1(\alpha) \cdot p_2(\alpha).$$

Ezek között – mint a definíció esetében is – gyakran váltunk, és a váltás nem nyilvánvaló. (Maguk a struktúrák a hozzájuk tartozó műveletekkel izomorfak.)

Az α egy T feletti lineáris kombinációját úgy tekintjük, mint egy T feletti polinom α helyen vett helyettesítési értékét, majd áttérünk a polinomok számelméletére.

Például felhasználtuk, hogy egy olyan polinom foka, amelynek gyöke az α kisebb, mint az α definiáló polinomjáé, akkor az csak az azonosan 0 polinom lehet. Egy d-nél kisebb fokú polinom maga nem szükségszerűen a nullpolinom. De ha gyöke az α, akkor már igen. Azok a polinomok, amelyeknek gyöke az α, az f polinom többszörösei. Eszerint vagy legalább annyi a fokszámuk, mint f-é, vagy az azonosan nulla polinomról van szó.

Annak bizonyításakor például, hogy $\dfrac{1}{g(\alpha)} \in T'$ azért kell átváltani a polinomok számelméletére, mert keresnünk kellett egy olyan elemet T'-ben $(v(\alpha))$, amellyel megszorozva az 1 polinomot kapjuk. Kiindultunk α egy polinomjából, és bár a polinomnak a reciproka nem polinom, de van olyan polinom, amelynek a helyettesítési értéke α-ban az eredeti polinom α-ban vett helyettesítési értékének a reciproka.

Próbáljuk ki, hogy ez mit jelentene például a $\sqrt[3]{2}$-vel való bővítés esetén a $\sqrt[3]{2}+\sqrt[3]{4}$ elemre. (Magyarul keressük meg, hogy a reciproka hogyan írható fel $a+b\sqrt[3]{2}+c\sqrt[3]{4}$ alakban.)

A $\sqrt[3]{2}$ definiáló polinomja x^3-2. A polinom, amelynek a reciprokpolinomját keressük, az x^2+x.

Írjuk fel az euklideszi algoritmust:

$$\begin{aligned} x^3-2 &= x(x^2+x)+(-x^2-2) = x(x^2+x)-1(x^2+x)+x-2 = \\ &= (x-1)(x^2+x)+x-2 \\ x^2+x &= x(x-2)+3x = x(x-2)+3(x-2)+6 = \\ &= (x+3)(x-2)+6 \end{aligned}$$

A maradék 6, azaz konstans, vagyis végetért az algoritmus. A legnagyobb közös osztó az 1 konstans polinom. Ezért kifejezzük a 6-ot, majd az utolsó lépésben osztjuk 6-tal. Átrendezzük a kapott egyenlőségeket:

$$6 = (x^2+x)-(x+3)(x-2).$$

A $(x-2)$-t helyettesítsük az első maradékos osztásból kapható kifejezéssel:

$$\begin{aligned} 6 &= (x^2+x)-(x+3)\left[(x^3-2)-(x-1)(x^2+x)\right] = \\ &= (x^2+x)-(x+3)(x^3-2)+(x+3)(x-1)(x^2+x) = \\ &= (x^2+x)-(x+3)(x^3-2)+(x^2+2x-3)(x^2+x) = \\ &= (x^2+x)(x^2+2x-2)-(x+3)(x^3-2) \end{aligned}$$

Ebből

$$1 = -\frac{1}{6}(x^3-2)(x+3)+\frac{1}{6}(x^2+x)(x^2+2x-2)$$

Az első tag $\alpha=\sqrt[3]{2}$-ben felvett helyettesítési értéke 0. Eszerint

$$1 = \frac{1}{6}\left(\sqrt[3]{4}+\sqrt[3]{2}\right)\left(\sqrt[3]{4}+2\sqrt[3]{2}-2\right).$$

Ebből adódik, hogy

$$\frac{1}{\sqrt[3]{4}+\sqrt[3]{2}} = \frac{1}{6}\sqrt[3]{4}+\frac{1}{3}\sqrt[3]{2}-\frac{1}{3}.$$

Ellenőrizzük beszorzással!

$$\left(\sqrt[3]{4}+\sqrt[3]{2}\right)\left[\frac{1}{6}\sqrt[3]{4}+\frac{1}{3}\sqrt[3]{2}-\frac{1}{3}\right]=$$
$$\frac{1}{6}\sqrt[3]{16}+\frac{1}{6}\sqrt[3]{8}+\frac{1}{3}\sqrt[3]{8}+\underbrace{\frac{1}{3}\sqrt[3]{4}-\frac{1}{3}\sqrt[3]{4}}_{0}-\frac{1}{3}\sqrt[3]{2}=$$
$$\frac{1}{3}\sqrt[3]{2}+\frac{1}{3}+\frac{2}{3}-\frac{1}{3}\sqrt[3]{2}=1.$$

Persze a konkrét történt másképpen is lehet „gyökteleníteni”.

Egyszerű testbővítés transzcendens elemmel

Bővítsük a T testet az α transzcendens elemmel. A reménybeli testet jelöljük T_1-gyel.

1. Azt jelenti a transzcendensség, hogy semmilyen T feletti polinomnak nem gyöke az α. Az összes T feletti p polinom ($p \in T[x]$) esetén a $p(\alpha)$ helyettesítési értékek különböznek egymástól (ellenkező esetben, azaz $p_1(\alpha)=p_2(\alpha)$ esetén a két polinom különbségének $(p_1-p_2)(\alpha)=0$ miatt gyöke lenne α, ami ellentmondana α transzcendensségének). Ezeket az elemeket tehát mind hozzá kell vennünk a T testhez, ha az α-val való testbővítést akarjuk megkapni. Jelöljük a hozzávett elemek halmazát T'-vel.

2. Belátjuk, hogy az így kapott $T\cup T'$ halmaz gyűrűt alkot, ami nem test.

Két elem összegének (szorzatának) értelmezése nyilvánvaló, ha mindkettő T-beli. A polinomok helyettesítési értékeivel értelmezhető, ha mindkettő T'-beli, illetve egy $t+p(\alpha)$ úgy értelmezhető, hogy $(p+t)(\alpha)$, valamint $tp(\alpha)$ úgy értelmezhető, hogy $(tp)(\alpha)$.

Eszerint $T\cup T'$ zárt az összeadásra és a szorzásra. A műveleti tulajdonságok nyilván teljesülnek.

A T-beli elemek additív inverzei T-beliek, a T'-beliek inverzei T'-beliek. A $t+p(\alpha)$ additív inverze $-t-p(\alpha)$ pedig $T\cup T'$-beli, vagyis az összeadás invertálható.

A multiplikatív inverzek azonban nem ilyen alakúak, hiszen $\dfrac{1}{p(\alpha)}=q(\alpha)$ esetén $q(\alpha)p(\alpha)-1=0$ miatt α gyöke lenne a $pq-1$ polinomnak.

3. $T\cup T'$ integritási tartomány. A multiplikatív egységelem az 1. Nullosztómentes, mert ha $[t_1+p_1(\alpha)][t_2+p_2(\alpha)]=0$, akkor $(p_2-p_1)(\alpha)=t_2-t_1$ miatt (α transzcendens) $p_2=p_1$ és $t_2=t_1$.

4. Az integritási tartományt a 11. fejezetben látott módon beágyazhatjuk egy testbe, azaz elkészíthetünk hozzá egy olyan testet, amely izomorf módon tartalmazza az eredeti integritási tartományt, és létezik multiplikatív inverz (a zérustól különböző elemekre).

Megjegyzés. Itt persze nincs másról szó – mint ahogyan a 11. fejezetben –, minthogy hozzávesszük a lehetséges hányadosokat a gyűrűhöz. Persze lesznek olyan hányadosok, amelyeket többféleképpen is megkaphatunk, ezeket ekvivalensnek tekintjük.

Az egyszerű algebrai bővítés következményei

12.6. Tétel. *Ha a $T_1 \leq T_2$ testbővítés foka n, a $T_2 \leq T_3$ testbővítés foka l, akkor T_1-nek bővítése T_3, és a $T_1 \leq T_3$ testbővítés foka $n \cdot l$.*

Bizonyítás. $T_1 \leq T_3$ nyilvánvaló, mert T_1 részteste T_3-nak. Azt kell bebizonyítanunk, hogy

$$\dim(T_3, T_1) = \dim(T_3, T_2) \cdot \dim(T_2, T_1).$$

Vegyünk fel ehhez egy bázist a (T_2, T_1) vektortérben: $e_1, \ldots, e_n$; egyet pedig a (T_3, T_2)-ben: $f_1, \ldots, f_l$. Ekkor egy tetszőleges T_3-beli $\mathbf{v}$ elem így írható:

$$\mathbf{v} = b_1 \cdot f_1 + \cdots + b_l \cdot f_l.$$

Ezek a b_i együtthatók T_2-beliek, nekünk pedig T_1-beliek kellenek, írjuk fel tehát a T_2-beli együtthatókat T_2-beli báziselemek T_1-beli lineáris kombinációjaként:

$$\begin{aligned} b_1 &= a_{11}e_1 + a_{21}e_2 + \cdots + a_{n1}e_n \\ &\vdots \\ b_l &= a_{1l}e_1 + a_{2l}e_2 + \cdots + a_{nl}e_n \end{aligned}$$

Ezekkel $\mathbf{v}$ így írható:

$$\begin{aligned} \mathbf{v} &= a_{11}e_1f_1 + a_{21}e_2f_1 + \ldots + a_{n1}e_nf_1 + \\ &= a_{12}e_1f_2 + a_{22}a_2f_2 + \ldots + a_{n2}e_nf_2 + \\ &\quad\vdots \\ &= a_{1l}e_1f_l + a_{2l}e_2f_l + \ldots + a_{nl}e_nf_l \end{aligned}$$

Az a_{ij} elemek T_1-beli együtthatók (számuk $n \cdot k$), az e_if_j elemek pedig T_3-beli vektorrendszert alkotnak. Nyilvánvalóan generátorrendszer, hiszen minden

$\mathbf{v} \in T_3$ előáll a fenti alakban. Azt kell már csak bizonyítani, hogy bázis. Ezt úgy látjuk be, hogy megmutatjuk, hogy a $\mathbf{0} \in T_3$ elemet csak a triviális lineáris kombinációjuk állítja elő. Legyen ugyanis

$$\mathbf{0} = a_{11}e_1f_1 + a_{12}e_1f_2 + \cdots + a_{1l}e_1f_l + \cdots + \cdots + \cdots + a_{n1}e_nf_1 + \cdots + a_{nl}e_nf_l,$$

ekkor – mivel f_j vektorrendszer T_2-ben – minden j-re az f_j együtthatója 0. Eszerint minden j-re

$$a_{1j}e_1 + a_{2j}e_2 + \cdots + a_{nj}e_n = 0.$$

Mivel azonban az e_i elemek bázist alkotnak T_2-ben, ez csak úgy lehet, ha minden a_{ij} együttható is nulla. Végső soron azt kaptuk, hogy minden i-re, j-re $a_{ij} = 0$. □

Következmény. Ha a $T_1 \leq T_2 \leq T_3 \leq \ldots$ testbővítési láncban csak másodfokú bővítéseket végzünk, akkor T_1-ből nézve minden test bővítésének foka 2-hatvány.

Következmény. A $T_1 \leq T_2 \leq T_3 \leq \ldots$ testbővítési láncban csak másodfokú bővítéseket végzünk. Ha $z \in T_1$ definiáló polinomjának fokszáma nem 2-hatvány, akkor $z \notin T_i$ semelyik i-re. (Hiszen annak definiáló polinomja nem 2-hatvány.)

Bizonyítás. Tegyük fel ugyanis, hogy z már eleme T_i-nek, de még nem eleme T_{i-1}-nek. Ekkor például $T_i = T_{i-1}(\alpha)$, α definiáló polinomja másodfokú.

Ha valamely z-re $z \notin T_{i-1}$, de $z \in T_i$, akkor $z = a_0 + a_1\alpha$ alakú (a_0, $a_1 \in T_{i-1}$), amiből $\alpha = \dfrac{1}{a_1}z - \dfrac{a_0}{a_1}$.

Minekután α definiáló polinomja $b_0 + b_1x + b_2x^2$, amelyre tehát $b_0 + b_1\alpha + b_2\alpha^2 = 0$; ha most α helyébe az imént kapott $\dfrac{1}{a_1}z - \dfrac{a_0}{a_1}$ kifejezést helyettesítjük, akkor azt kapjuk, hogy z egy másodfokú polinom gyöke. z definiáló polinomja tehát csak 2 lehet T_{i-1} felett.

Indukciós lépésekkel igazolható, hogy ekkor z-nek a T_1 feletti definiáló polinomja csak 2-hatvány lehet. □

Következmény. Ha egy elem definiáló polinomja harmadfokú, akkor csupa másodfokú bővítéseket végezve nem kaphatunk olyan testet, amely ezt az elemet tartalmazza.

Következmény. A racionális számokat tetszőleges másodfokú bővítésekkel bővítve sohasem kaphatunk olyan testet, amelynek eleme lenne a $\sqrt[3]{2}$. (Hiszen annak definiáló polinomja, $x^3 - 2$ harmadfokú.)

Feladatok

1. Írjuk fel a következő elemek racionális feletti minimálpolinomját!
   $\sqrt{2}$, $\sqrt{3}$, $\sqrt{4}$, $\sqrt{5}$, $\sqrt[3]{2}$, $\sqrt[3]{4}$, $\sqrt[3]{8}$
2. Keressük meg a kételemű testben az irreducibilis másodfokú polinomokat!
3. Keressük meg a háromelemű testben az irreducibilis másodfokú polinomokat!
4. Milyen testet kapunk, ha a háromelemű $(\{0,1,2\}, +_{\text{ mod } 3}, \cdot_{\text{ mod } 3})$ testet bővítjük $\sqrt{2}$-vel?

   Hány eleme lesz ennek a testnek?
5. Hányadfokú bővítése az a legszűkebb test a racionális számtestnek, amelynek eleme $\sqrt{2}+\sqrt{3}$?
6. Hányadfokú bővítése az a legszűkebb test a racionális számtestnek, amelynek eleme $\sqrt[3]{3-\sqrt{7}}$?
7. Határozza meg a $\mathbb{Q}(\sqrt{5})$ testben a $\sqrt{5}+1$ elem multiplikatív inverzét!
8. Eleme-e a $\sqrt[3]{25}$ a $\mathbb{Q}(\sqrt[3]{5})$ testnek? És a $\sqrt{5}$?
9. Határozza meg a $\mathbb{Q}(\sqrt[3]{5})$ testben a $\sqrt[3]{25}+\sqrt[3]{5}+1$ elem multiplikatív inverzét!

13. fejezet

A geometriai szerkeszthetőség algebrai elmélete

A testbővítések elméletének segítségével számos – korábban hosszú ideig megoldatlan – problémára sikerült megtalálni a választ. Az egyik ilyen kérdéskör a körzővel és vonalzóval történő, úgynevezett euklideszi szerkesztésekkel kapcsolatos. Az euklideszi síkon történő euklideszi szerkesztéshez egy (tetszőlegesen hosszú) egyélű, egyenes vonalzót és egy (tetszőleges távolságra kinyitható) körzőt használhatunk.

Megjegyzés. Természetesen az egyélű vonalzó egy idealizált vonalzó. Azért van szükség erre a kikötésre, hogy nehogy azt gondoljuk, hogy ha két például van két párhuzamos oldalpárja, akkor jogunkban áll úgy párhuzamost rajzolni, hogy mindkét él mentén húzunk egy vonalat. Nem mintha nem tudnánk csapán euklideszi eszközökkel párhuzamosokat rajzolni, de a két párhuzamos egyenes távolsága már nem minden körülmények között megszerkeszthető.

Arra sem szamáthatunk, hogy derékszögű vonalzó két, egymásra merőleges éle segítségével rajzolunk derékszöget – nem mintha nem tudnánk csupán euklideszi eszközökkel derékszöget rajzolni.

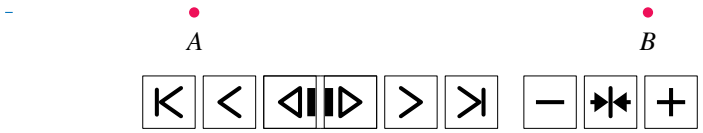
A két eszközre tett kikötés mindössze azt jelenti, hogy segítségükkel egyenest és kört tudunk rajzolni.

Fontos, hogy a szerkesztés sem csak úgy a vakvilágba történik, hanem a kiinduló vagy a már megszerkesztett pontokhoz, alakzatokhoz kapcsolódik.

Ennek megfelelően a következőkben rögzítjük, hogy melyek a szerkesztés megengedett eszközei.

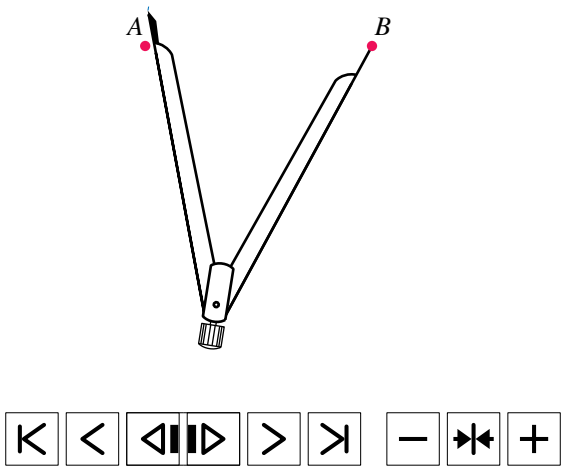
A vonalzó és a körző segítségével a következő hat műveletet hajthatjuk végre:

1. Két adott ponton át a vonalzóval egyenest húzhatunk.



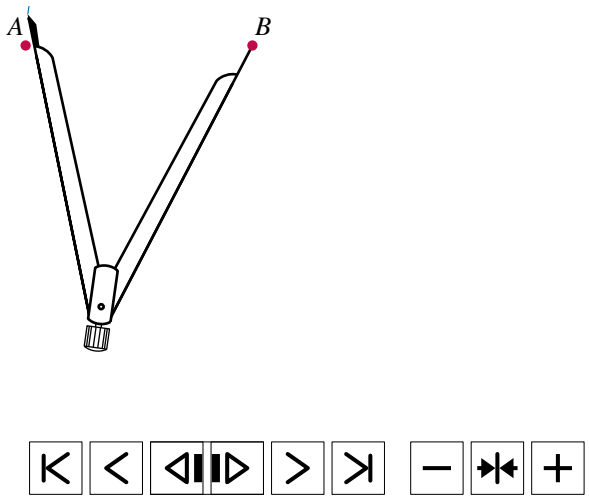
13.1. ábra. Két adott ponton át a vonalzóval egyenest húzhatunk.

2. Két pont távolságát körzőnyílásba vehetjük.



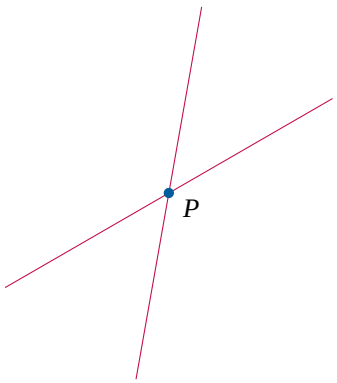
13.2. ábra. Két pont távolságát körzőnyílásba vehetjük.

3. Adott pont körül adott szakasszal – mint sugárral – kört rajzolhatunk.



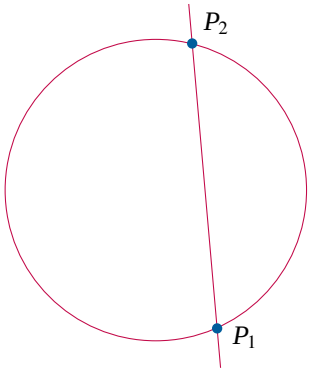
13.3. ábra. Adott pont körül adott szakasszal – mint sugárral – kört rajzolhatunk.

4. Két adott vagy már megszerkesztett egyenes metszéspontját megszerkesztettnek tekinthetjük.



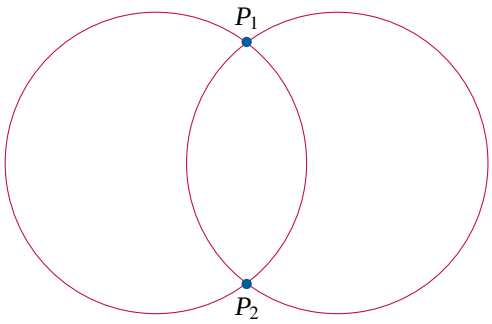
13.4. ábra. Két adott vagy már megszerkesztett egyenes metszéspontját megszerkesztettnek tekinthetjük.

5. Ha egy adott egyenes és egy adott kör két pontban metszi egymást, akkor metszéspontjaikat megszerkesztetteknek tekinthetjük.



13.5. ábra. Ha egy adott egyenes és egy adott kör két pontban metszi egymást, akkor metszéspontjaikat megszerkesztetteknek tekinthetjük.

6. Ha két adott kör két pontban metszi egymást, akkor metszéspontjaikat megszerkesztetteknek tekinthetjük.

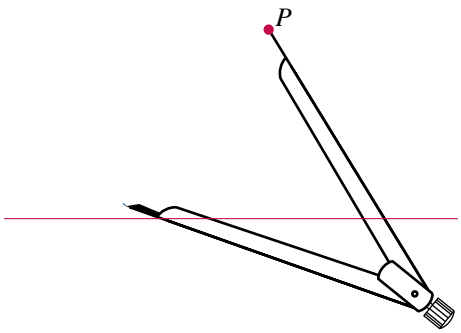


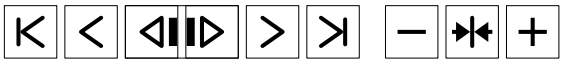
13.6. ábra. Ha két adott kör két pontban metszi egymást, akkor metszéspontjaikat megszerkesztetteknek tekinthetjük.

13.1. Definíció. *Euklideszi szerkesztésnek* nevezzük a fenti hat lépés **véges sokszori** alkalmazását. (A már megszerkesztett pontokat, egyeneseket, köröket a továbbiakban adottnak tekintjük.)

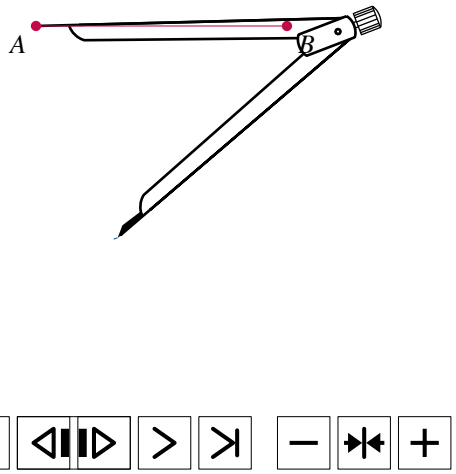
Megjegyzés. Definíciónk nem engedi meg például derékszögű vonalzó használatát, vagy azt, hogy tetszőlegesen vegyünk fel – akár egy adott egyenesen vagy körön – pontokat.

Nyilvánvalóan szerkeszthető viszont például egy adott pontból egy adott egyenesre bocsátott merőleges, adott egyenessel egy rá nem illeszkedő, adott ponton átmenő párhuzamos egyenes, egy adott szakasz felező merőlegese stb. Ezek közül az egyszerű szerkesztések közül néhányat szemléltetünk (13.7–13.9. animációk).

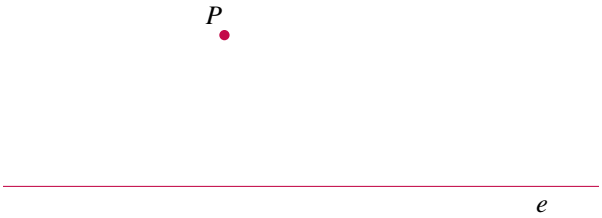




13.7. ábra. Egyenesre bocsátott merőleges külső pontból



13.8. ábra. Szakaszfelező merőleges szerkesztése



13.9. ábra. Párhuzamos szerkesztése külső pontból

Megjegyzés. A szerkesztési lépések véges sokszori alkalmazását nagyon fontos kikötni. Ugyan rendkívül természetesnek tűnik – hiszen valamikor véget kell érjen a szerkesztés, márpedig ez csak akkor sikerülhet, ha csak véges sok lépés van –, de a matematikában nem egyszer előfordul, hogy rekurzív módon konstruáljuk meg egy feladat megoldását. Arról szó sincs, hogy ilyenkor a valóságban is megkonstruálható a megoldás. Gondoljunk annak bizonyítására, hogy ha egy korlátos zárt intervallumon folytonos függvény az intervallum bal végpontjában nemnegatív, a jobb végpontjában nempozitív értéket vesz fel, akkor valahol az intervallumban felveszi a 0 értéket. (A rekurzív bizonyítás során az intervallumot megfelezzük, és megállapítjuk, hogy a keletkezett részintervallumok melyike tesz eleget az eredeti feltételeknek. Végül egy egymásba skatulyázott – végtelen – zárt intervallumsorozat közös pontjaként határozzuk meg a keresett pontot.)

Azért éppen ezt a példát hoztuk fel, mert – mint azt majd látni fogjuk – nem szerkeszthető meg tetszőleges szög harmadrésze, azonban egy hasonló jellegű szerkesztési lépéssorozattal végtelen sok lépésben megkaphatnánk egy tetszőleges szög harmadrészét: megfelezzük az adott szöget, és meghatározzuk, hogy a szög harmada melyik félszögbe esik. (Itt valójában az 1/3

tört kettes számrendszerbeli, úgynevezett bináris törtfelírását használjuk. Az 1/3 végtelen szakaszos kettedes tört.) Ez az eljárást nem ér véget véges sok lépésben.

A továbbiakban csak olyan szerkesztési feladatokkal foglalkozunk, amelyekben legalább két pont adott.

Ahhoz, hogy a szerkesztéseket algebrailag jellemezhessük, szerkesztési feladatunk kiindulási adatai közül válasszunk ki két adott pontot, és illesszünk rájuk derékszögű koordináta-rendszert úgy, hogy a két adott pont közül az egyik legyen a koordináta-rendszer $(0,0)$, a másik az $(1,0)$ pontja.

Ezen a síkon keressük azokat a pontokat, amelyek szerkesztéssel megkaphatók ebből a két pontból kiindulva. Vigyázzunk! Attól, hogy egy egyenes geometriai értelemben meg van szerkesztve, koránt sem tekinthetjük megszerkesztettnek minden egyes pontját, hiszen olyan szerkesztési lépés nincs, hogy válasszuk ki egy egyenes egy tetszőleges pontját. Új pontot csak úgy tudunk megszerkeszteni, ha az két, már megszerkesztett alakzat metszéspontja.

Valamilyen módon meg kell határoznunk, hogy milyen adatokkal határozhatjuk meg a sík pontjait, illetve milyen kritériumai vannak **egy pont** szerkeszthetőségének.

A továbbiakban a pontokat koordinátáikkal fogjuk jellemezni, és arra vagyunk kíváncsiak, hogy a megszerkeszthető pontok koordinátáinak milyen algebrai tulajdonságaik vannak. Nyilván a valós számkörön belül fogunk maradni.

A két adott pont koordinátája a $(0,0)$ és a $(0,1)$, ezekből a pontokból indulunk ki, ezek a kiindulási adatok.

13.2. Definíció. Abból a feltételezésből indulunk ki, hogy adott egy egység hozzúságú szakasz. Ezt a koordináta-rendszer $(0,0)$ és $(1,0)$ pontjával adjuk meg. *Megszerkeszthetőnek* nevezünk a egy számot, ha a kiindulási adatokból euklideszi eszközökkel megszerkeszthető – például az x tengelyen egy $|a|$ hosszúságú szakasz, vagyis az $(|a|,0)$ pont.

13.1. Állítás. *Ha az a hosszúságú szakasz megszerkeszthető, akkor az ellentettje is megszerkeszthető.*

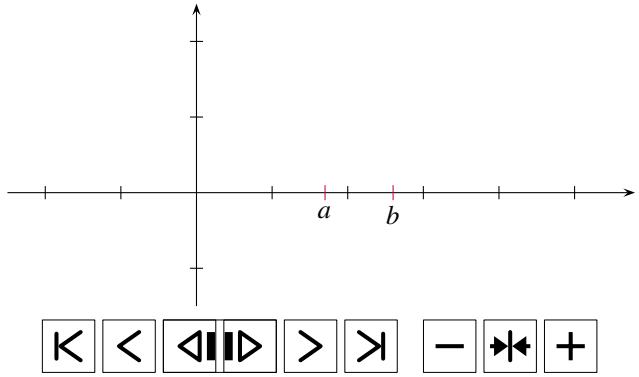
Bizonyítás. Ha a szerkeszthető, azaz az $(|a|,0)$ pont megszerkeszthető, akkor ezzel a $(-a)$-nak meglfelelő $(|a|,0)$ pontot is megadtuk. □

13.2. Állítás. *A szerkeszthető adatok (mint a valós számok egy részhalmaza) zártak a testműveletekre. Minekután a valós számhalmaz részét képezik, így testet alkotnak. Lásd a 13.10–13.13. animációkat.*

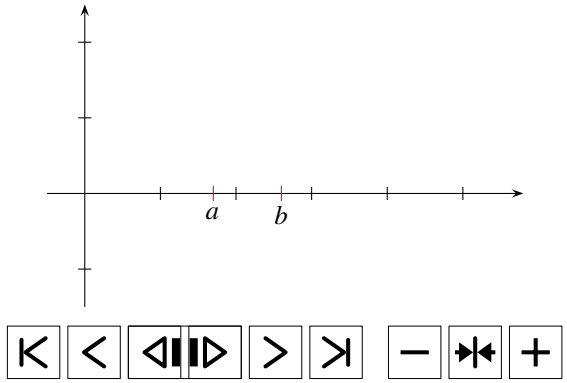
Bizonyítás. Tekintettel arra, hogy ha adott két távolság (például a felvett koordináta-rendszer x tengelyén), akkor azok összegét, különbségét, szorzatát és hányadosát (hasonlósággal) is meg tudjuk szerkeszteni (ugyanezen a tengelyen) – lásd a 13.10–13.13. animációkat –, a megszerkeszthető távolságok adatainak halmaza az összeadásra és a szorzásra nézve zárt.

A hosszúságok hányadosa az osztandó és az osztó reciprokának szorzata – így a szorzás mellett csak a reciprok szerkesztését illusztráltuk.

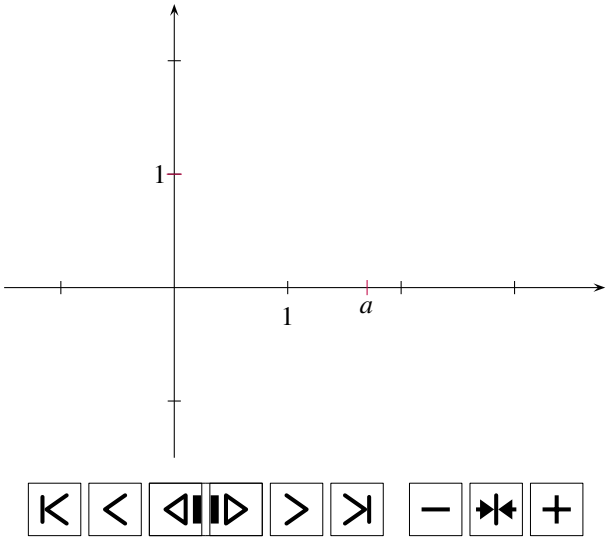
A műveletek a valós számok részhalmazaként megőrzi a műveleti tulajdonságokat. Eszerint a szerkeszthető hosszúságok halmaza testet alkot, a valós számok részteste. □



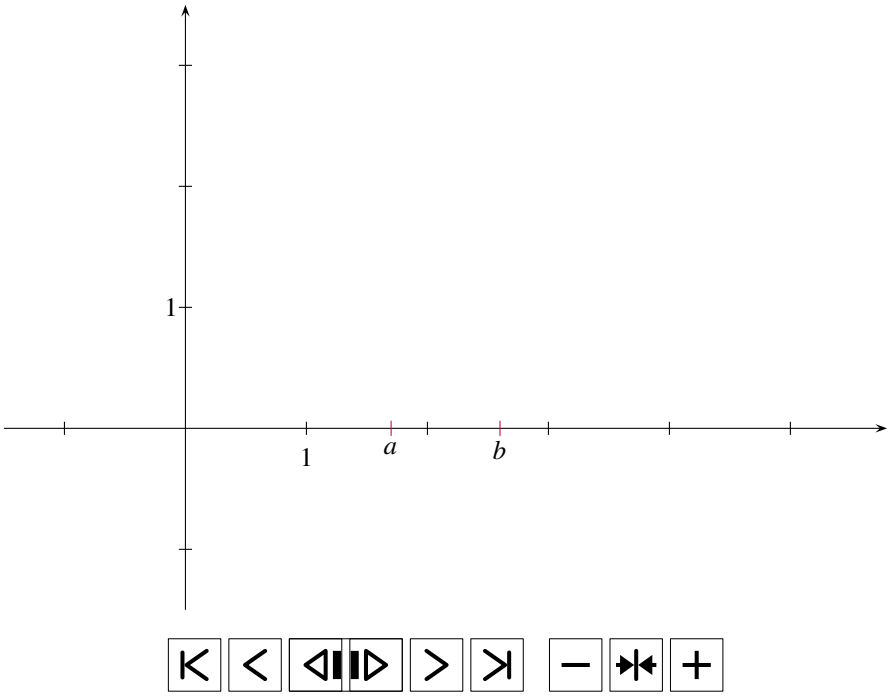
13.10. ábra. Szakaszok összegének szerkesztése



13.11. ábra. Szakaszok különbségének szerkesztése



13.12. ábra. Szakasz reciprokának szerkesztése



13.13. ábra. Szakaszok szorzatának szerkesztése

A számegyenes pontjai megfelelnek a valós számhalmaznak.

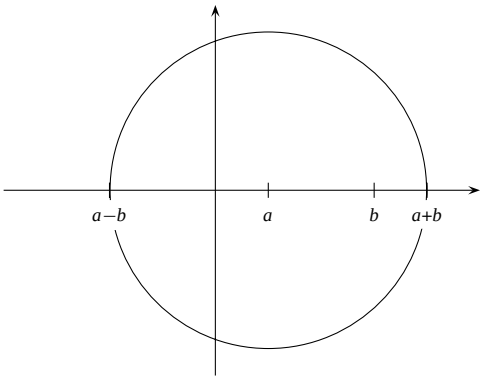
Keressük meg tehát ezekután a valós számtestnek azt a legszűkebb résztestét, amely a két kiindulási adatunkat tartalmazza.

13.3. Definíció. A *kiindulási adatok teste* (T_0) az a legszűkebb test, amely tartalmazza a két kiindulási pontnak megfelelő számot.

Ha – ahogyan a példánkban – eredetileg két pont volt adva és ez a két pont lett a koordináta-rendszer $(0,0)$, illetve $(1,0)$ pontja, akkor most a valós test legszűkebb olyan résztestét keressük, amely tartalmazza a 0-t és az 1-et. (Ebben az esetben T_0 éppen a racionális test, ezt korábban már láttuk.)

Meggondolható, hogy az, hogy egy adott szerkesztési feladatban mi lesz a kiindulási adatok teste, nem függ attól, hogy az adott pontok közül melyiket választjuk a koordináta-rendszer $(0,0)$, illetve $(1,0)$ pontjának. Ez azt is jelenti, hogy az egység hosszúságot tetszőlegesen felvehetjük, a kiindulási adatok teste két pont esetén mindenképpen a racionális számhalmaz.

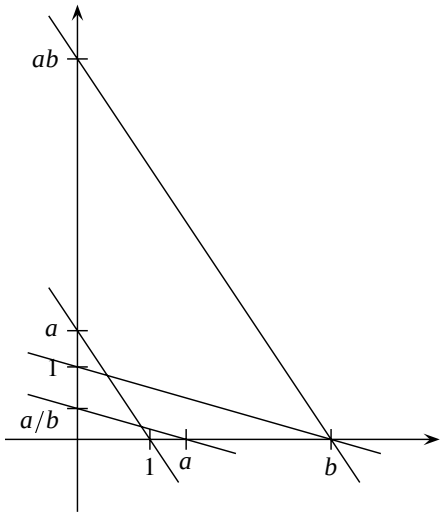
13.3. Állítás. *A kiindulási adatok testének, esetünkben a racionális számtestnek tetszőleges eleme szerkeszthető. Ehhez elég azt megmutatnunk, hogy ha a és $b \in T_0$, akkor $a-b$ is, $a+b$ is, ab is és $\frac{a}{b}$ $(b \neq 0)$ is szerkeszthető.*



13.14. ábra.

Bizonyítás. Mivel tetszőleges – már megszerkesztett – hosszúságok összegét, különbségét, szorzatát és hányadosát meg tudjuk szerkeszteni, ezért az egység hosszúságból kiindulva tetszőleges egész szám szerkeszthető, illetve ilyenek hányadosa is szerkeszthető. (13.14 és 13.15. ábrák.)

A jobb áttekinthetőség érdekében nem foglalkoztunk azzal, hogy a keletkezett műveleti eredmény feltétlenül az x tengelyen jelenjen meg. □



13.15. ábra.

Beláttuk, hogy a szerkeszthető hosszúságok testet alkotnak (13.2. Állítás). Beláttuk továbbá, hogy a racionális számtest minden eleme szerkeszthető (13.3 Állítás).

Vizsgáljuk most meg, hogy szerkesztési lépéseink milyen további adatok szerkesztését teszik lehetővé. Induljunk ki abból, hogy a T_0 (kezdetben a racionális számok) test minden eleme szerkeszthető. Végezzünk el egy olyan szerkesztési lépést, amelynek során új pont keletkezik: két egyenes; egy kör és egy egyenes; vagy két kör metszéspontja.

Ne feledjük, hogy egyelőre csak a T_0 elemei vannak megszerkesztve, és ebből kiindulva végzünk el – most csak egyetlen szerkesztési lépést.

13.1. Megjegyzés. Vezessük be ideiglenesen a következő kifejezéseket: Nevezzük T_0 pontjait már megszerkesztetteknek. Nevezzük már megszerkesztettnek azokat az egyeneseket, amelyekre illeszkedik két T_0-beli pont. Nevezzünk már megszerkesztettnek egy kört, ha a középpontja (mint pont) már megszerkesztett, illetve a sugara (mint hosszúság) is már megszerkesztett.

13.4. Állítás. *Bármely két már megszerkesztett egyenes metszéspontja már megszerkesztett.*

Bizonyítás. Ha a két egyenes már megszerkesztett, akkor van olyan már megszerkesztett pontpár, amelyre illeszkednek. A két egyenes egyenlete egy-egy T_0-beli együtthatós lineáris egyenlet. A metszéspontjuk a két lineáris egyenletből álló lineáris egyenletrendszer megoldása, amely – amennyiben létezik – szintén benne van T_0-ban, tehát egy már megszerkesztett pont. □

13.5. Állítás. *Egy már megszerkesztett egyenes és egy már megszerkesztett kör metszéspontjai vagy már megszerkesztettek, vagy koordinátái T_0 egy eleme négyzetgyökével történő másodfokú bővítésében vannak.*

Bizonyítás. Ha az e egyenes már megszerkesztett, akkor van olyan már megszerkesztett pontpár, (x_1, y_1), illetve (x_2, y_2), amelyre illeszkedik. Ekkor az egyenlete

$$(y - y_1)(x_2 - x_1) - (x - x_1)(y_2 - y_1) = 0$$

alakú, amelynek együtthatói már megszerkesztett adatok.

A már megszerkesztett K kör egyenlete pedig legyen az

$$(x - u)^2 + (y - v)^2 - r^2 = 0.$$

Mivel K már megszerkesztett, azért a középpontja koordinátái, illetve a sugár már megszerkesztett adatok.

Az e egyenletéből kifejezve például y-t és K egyenletébe helyettesítve másodfokú egyenletet kapunk x-re. A másodfokú egyenlet megoldóképletével felírhatjuk a megoldásokat az x-re. (Ha vannak!) Lehet, hogy ezek a metszéspontok már megszerkesztettek, azaz T_0-ban vannak. Azt is tudjuk azonban, hogy ha létezik is megoldása a másodfokú egyenletnek (a valósban), nem feltétlenül van T_0-ban. A diszkrimináns négyzetgyökével bővített T_1 testben (amelyet tehát egy egyszerű másofokú bővítéssel kapunk) azonban már benne lesznek. Az y az x-nek „racionális" kifejezése, tehát biztosan benne lesz T_1-ben. □

13.6. Állítás. *Két már megszerkesztett kör metszéspontjai vagy már megszerkesztettek, vagy T_0 egy eleme négyzetgyökével történő másodfokú bővítésében vannak.*

Bizonyítás. Legyen K_1 egyenlete $(x - u_1)^2 + (y - v_1)^2 - r_1^2 = 0$, K_2 egyenlete pedig $(x - u_2)^2 + (y - v_2)^2 - r_2^2 = 0$. Az egyik egyenletből kivonva a másikat lineáris összefüggést kapunk x-re és y-ra. Ehhez hozzávesszük valamelyik kör egyenltetét. Így a feladat megoldását visszavezettük az előző állítás bizonyítására. □

Mindez azt jelenti, hogy ha a kiindulási adatok teste T_0, akkor bármelyik megengedett szerkesztési lépést hajtjuk is végre, az újonnan megszerkesztett pont koordinátái vagy elemei T_0-nak, vagy T_0 valamelyik eleme négyzetgyökének „racionális" kifejezése. (Vagyis T_0-beli elemmel szorozzunk, ahhoz T_0-beli elemet adunk hozzá. A négyzetgyök persze akár benne is lehet T_0-ban.)

Ha most megkeressük a legszűkebb olyan T_1 testet, amely már nemcsak kiindulási adatainkat, hanem az újonnan megszerkesztett pont adatait is

tartalmazza, akkor ez a test vagy maga T_0 lesz, vagy T_0-nak egy T_0-beli pozitív szám négyzetgyökével való bővítése: $T_1 = T_0(\sqrt{\alpha})$, ahol $\alpha > 0$ és $\alpha \in T_0$.

Egyelőre csak azt tudjuk, hogy az eddig megszerkesztett pontok adatai $T_1 = T_0[\alpha]$ elemei, azt azonban nem tudjuk, hogy minden T_1-beli pont szerkeszthető-e.

13.7. Állítás. *Ha a T_0 testből valamely szerkesztési lépéssel olyan pontot kapunk, amelynek valamelyik koordinátája α_0-nak T_0-beli együtthatós lineáris kifejezése, $a + b\alpha_0$, akkor $T_1 = T_0[\alpha]$ minden eleme szerkeszthető. (Ne feledjük: α_0 egy T_0-beli elem négyzetgyöke.)*

Bizonyítás. Ha $a + b\sqrt{\alpha_0}$ szerkeszthető, akkor α_0 is.

A korábban látott módon tetszőleges b esetén $b\alpha_0$ is szerkeszthető, valamint $a + b\alpha_0$ is.

Az $a + b\alpha_0$ alakú elemek additív inverze (ellentettje) is nyilván szerkeszthető. A multiplikatív inverzre pedig

$$\frac{a - b\alpha_0}{a - b\alpha_0} \cdot \frac{1}{a + b\alpha_0} = \frac{a - b\alpha_0}{a^2 - b^2\alpha_0^2} = \frac{a}{a^2 - b^2\alpha_0^2} - \frac{b}{a^2 - b^2\alpha_0^2}\alpha_0$$

teljesül. Mivel α_0 együtthatói T_0-beliek, ez is egy $a + b\alpha_0$ alakú szám, azaz szerkeszthető. □

Eddig sehol nem használtuk fel, hogy T_0 a racionális számtest (a racionális kifejezés csak arra utalt, hogy összeadás/kivonás, szorzás/osztás szerepel benne), ezért az eljárást tovább folytathatjuk:

Ha egy szerkesztés menete során minden egyes lépés után megkeressük a legszűkebb olyan testet, amely a kiindulási adataink mellett tartalmazza az összes addig megszerkesztett pont koordinátáit (adatait), akkor egymást tartalmazó testek olyan $T_0 \subseteq T_1 \subseteq T_2 \subseteq \ldots \subseteq T_k$ láncolatához jutunk, ahol $T_{i+1} = T_i(\sqrt{\alpha_i})$, $\alpha_i > 0$ és $\alpha_i \in T_i$. Ebben a láncban tehát minden test vagy egybeesik az előzővel, vagy annak valós (pozitív szám négyzetgyökével való) másodfokú bővítése.

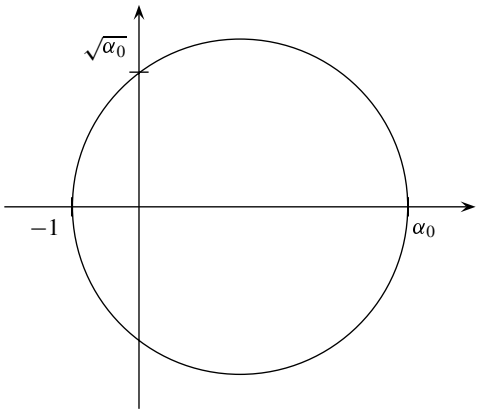
13.8. Állítás. *Az elmondottak alapján egy adat csak akkor szerkeszthető, ha benne van egy olyan T_k testben, amely a kiindulási adatok testéből megkapható véges sok egymás utáni valós másodfokú bővítéssel.*

13.9. Állítás. *Az állítás megfordítása is igaz, vagyis a fenti tulajdonságú T_k test minden eleme szerkeszthető.*

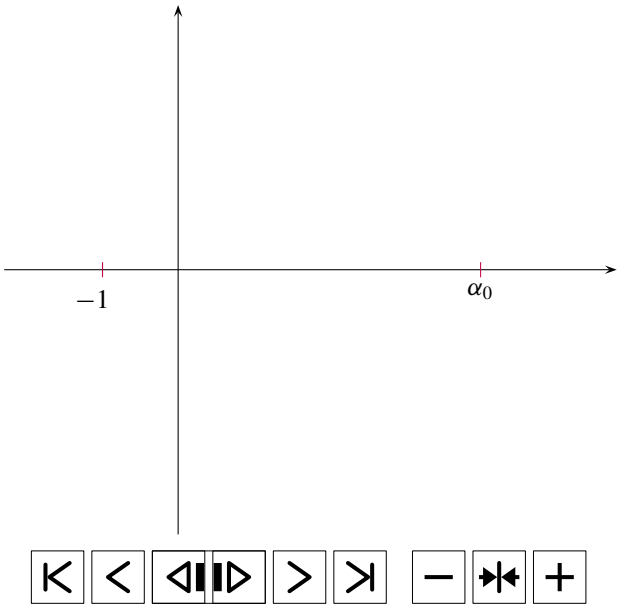
Azt, hogy T_0 minden eleme szerkeszthető, már láttuk. Azt kell csak bebizonyítanunk, hogy T_0 egy tetszőleges pozitív elemének a négyzetgyöke is szerkeszthető.

Bizonyítás. Legyen az a pozitív szám, amelynek a négyzetgyökét meg akarjuk szerkeszteni az a. A derékszögű háromszögben a magasságtétel szerint az átfogóhoz tartozó magasságvonal olyan részekre osztja az átfogót, amelyek szorzata a magasság háromszögbe eső szakaszának négyzetével egyenlő. Ha tehát c jelöli az átfogót, c_1 és c_2 az átfogóhoz tartozó magasságvonallal kettéosztott átfogó szeleteit, m_c pedig a magasságvonal hosszát, akkor $c_1c_2 = m_c^2$.

Ha most egy derékszögű háromszögben az átfogó két szeletének hosszúsága a és 1, akkor a magasságvonal hossza $\sqrt{a}$ (13.16. ábra). □



13.16. ábra. $\sqrt{\alpha_0}$ szerkesztése, ha az valós



13.17. ábra. $\sqrt{\alpha_0}$ egy lehetséges szerkesztése

Ez azt jelenti, hogy a T_1 testnek is minden eleme szerkeszthető. Mivel T_1 a T_0 $\sqrt{\alpha_0}$ elemmel való bővítése, a T_1 test minden eleme $a + b\sqrt{\alpha_0}$ alakú, ahol $\alpha_0 > 0$ és $a, b, \alpha_0 \in T_0$. Azt viszont már láttuk, hogy ha a, b és $\sqrt{\alpha_0}$ szerkeszthető, akkor $a + b\sqrt{\alpha_0}$ is szerkeszthető.

Hasonlóan, $T_2, T_3, \ldots, T_k$ testek mindegyikének minden eleme szerkeszthető.

Ezek alapján megfogalmazhatjuk a szerkeszthetőség szükséges és elégséges feltételét:

13.1. Tétel. *Euklideszi értelemben egy adat akkor és csak akkor szerkeszthető a kiindulási adatokból, ha eleme egy olyan T_k testnek, amely megkapható a kiindulási adatok testéből véges sok valós másodfokú bővítéssel.*

Tételünket úgy is fogalmazhatjuk, hogy egy α valós szám akkor és csak akkor szerkeszthető, ha eleme egy olyan T_k testnek, amelyre $T_0 \subseteq T_1 \subseteq T_2 \subseteq \subseteq \ldots \subseteq T_k$, ahol T_0 a kiindulási adatokat tartalmazó legszűkebb test, és $T_{i+1} = T_i(\sqrt{\alpha_i})$, $\alpha_i > 0$ és $\alpha_i \in T_i$.

Abból, hogy algebrai bővítések egymásutánja is algebrai, következik, hogy egy fenti tulajdonságú T_k test minden eleme algebrai elem a T_0 test felett. Így olyan elemek, amelyek T_0 felett transzcendensek, biztosan nem szerkeszthetők. Abból azonban, hogy egy elem algebrai a T_0 test felett, még

nem következik, hogy szerkeszthető, hiszen nem biztos, hogy az őt tartalmazó test megkapható másodfokú bővítések egymásutánjával T_0-ból.

Erre nézve a következő tétel fogalmazható meg:

13.2. Tétel. *Legyen az α valós szám algebrai elem a T_0 test felett. Ekkor α akkor és csak akkor szerkeszthető, ha definiáló polinomjának fokszáma kettő hatványa.*

Az világos, hogy ha egy valós szám szerkeszthető, akkor a racionális test felett a definiáló polinomjának a fokszáma kettő hatványa. (Hiszen másodfokú bővítésekkel megkapható.)

A másik irányban a definíció nem nyilvánvaló, és most nem is bizonyítjuk.

Könnyen igazolható viszont a következő speciális eset:

13.3. Tétel. *Legyen T_0 a kiindulási adatok teste, és legyen az*

$$f(x) = x^3 + c_2x^2 + c_1x + c_0$$

(1 főegyütthatós harmadfokú) polinom – ahol $c_2, c_1, c_0 \in T_0$ – irreducibilis a T_0 test felett. Ekkor $f(x)$ egyetlen gyöke sem szerkeszthető a kiindulási adatokból.

Bizonyítás. Tegyük fel, hogy $f(x)$ a T_1, T_2, …, T_{k-1} testek felett is irreducibilis, viszont van z_1 gyöke T_k-ban, vagyis z_1 szerkeszthető a kiindulási adatokból. Ekkor $z_1 = a + b\sqrt{\alpha}$, ahol $a, b, \alpha \in T_{k-1}$. Mivel z_1 gyöke f-nek:

$$\begin{aligned}
0 = f(z_1) &= z_1^3 + c_2z_1^2 + c_1z_1 + c_0 = \\
&= \left(a + b\sqrt{\alpha}\right)^3 + c_2\left(a + b\sqrt{\alpha}\right)^2 + c_1\left(a + b\sqrt{\alpha}\right) + c_0 = \\
&= a^3 + 3a^2b\sqrt{\alpha} + 3ab^2\alpha + b^3\alpha\sqrt{\alpha} + \\
&\qquad + c_2a^2 + 2c_2ab\sqrt{\alpha} + c_2b^2\alpha + c_1a + c_1b\sqrt{\alpha} + c_0 = \\
&= \sqrt{\alpha}\left(3a^2b + b^3\alpha + 2c_2ab + c_1b\right) + (a^3 + 3ab^2\alpha + c_2a^2 + c_2b^2\alpha + c_1a + c_0).
\end{aligned}$$

Vagyis $0 = u\sqrt{\alpha} + v$, azaz $u\sqrt{\alpha} = -v$, ahol $u, v, \alpha \in T_{k-1}$. Mivel azonban $\sqrt{\alpha} \notin T_{k-1}$, ez csak úgy lehet, ha $u = v = 0$.

Tekintsük most z_1-nek a T_{k-1} testbeli konjungáltját, azaz $a - b\sqrt{\alpha}$-t.

$$\begin{aligned}
0 = f(\overline{z_1}) &= \\
&= -\sqrt{\alpha}\left(3a^2b + b^3\alpha + 2c_2ab + c_1b\right) + (a^3 + 3ab^2\alpha + c_2a^2 + c_2b^2\alpha + c_1a + c_0),
\end{aligned}$$

Tehát $\overline{z_1}$ is gyöke f-nek, és benne van T_k-ban, de nincs benne T_{k-1}-ben.

Jelölje most f harmadik gyökét z_3. Ekkor a gyökök és együtthatók közti összefüggésekből $z_1 + z_2 + z_3 = -c_2$. Mivel

$$z_1 + z_2 = a + b\sqrt{\alpha} + a - b\sqrt{\alpha} = 2a,$$

ebből $z_3 = -c_2 - 2a- \in T_{k-1}$, vagyis az $f(x)$ polinomnak mégiscsak van olyan gyöke, amely eleme T_{k-1}-nek. Ez ellentmond annak, hogy $f(x)$ irreducibilis T_{k-1} felett. Végső soron tehát az $f(x)$ polinom egyik gyöke sem szerkeszthető. □

Következmény. Speciálisan, ha kiindulási adataink a 0 és az 1, (így a kiindulási adatok teste a racionális test), akkor tételünk szerint egyetlen olyan harmadfokú polinom gyökei sem szerkeszthetőek, amely irreducibilis $\mathbb{Q}$ felett.

Néhány nevezetes szerkeszthetőségi probléma

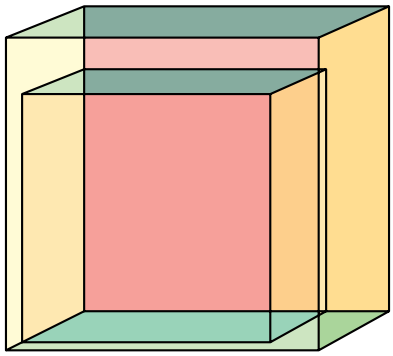
1. „A kör négyszögesítése”

   Szerkesztendő olyan négyzet, amelynek kerülete megegyezik egy (középpontjával és kerületének egy pontjával) adott kör kerületével. Válasszuk a kör középpontját koordináta-rendszer origójának, sugarát pedig egységnyinek (vagyis a kör kerületének adott pontja legyen az $(1, 0)$ pont). Ekkor a kiindulási adatok teste a racionális számtest, a szerkesztendő távolság pedig (a négyzet oldala) $\frac{2\pi}{4} = \frac{\pi}{2}$. Mivel a π transzcendens szám, sem ő, sem a fele nem szerkeszthető.

   Hasonló feladat adott kör területével egyenlő területű négyzet szerkesztése. Ez egy $\sqrt{\pi}$ oldalú négyzet szerkesztését kívánja, ami szintén lehetetlen (hiszen ha $\sqrt{\pi}$ szerkeszthető lenne, akkor a π is).

2. Déloszi probléma (kockakettőzés)

   Egy legenda szerint, amikor Délosz szigetén pestisjárvány tört ki, a délosziak (hogy megtudják, mi vethet véget a járványnak) a delphoi jósdához fordultak. Azt a választ kapták kérdésükre, hogy a járványnak akkor lesz vége, ha Apolló templomának kocka alakú oltárkövét kicserélik egy kétszer akkora (térfogatú) kockára. A feladat olyan kocka élének a megszerkesztése, amelynek térfogata kétszerese egy adott kocka térfogatának. Ha az adott kocka élét egységnyinek tekintjük, akkor a kiindulási adatok teste a racionális test, a megszerkesztendő távolság pedig a $\sqrt[3]{2}$. A $\sqrt[3]{2}$ definiáló polinomja az $x^3 - 2$, ami a racionális test felett irreducibilis harmadfokú polinom, így a 13.3. Tétel szerint egyetlen gyöke sem – így a $\sqrt[3]{2}$ sem szerkeszthető.



13.18. ábra. Déloszi kockakettőzés

3. Trisectio anguli (szögharmadolás)

   A feladat olyan szerkesztési eljárás megadása, amelynek segítségével egy tetszőlegesen adott – vagy a kiindulási adatokból szerkeszthető – szög harmadrésze megszerkeszthető.

   Meg fogjuk mutatni, hogy ha a kiindulási adatok teste a racionális test, akkor van olyan szög – pl. a 60°-os szög –, amely a kiindulási adatokból szerkeszthető, de a harmada – azaz a 20°-os szög – euklideszi eszközökkel nem szerkeszthető.

   Ebből már következik, hogy egyrészt nem minden szöghöz létezik olyan – esetleg szögről szögre változó – eljárás, amellyel az illető szög harmada megszerkeszthető, másrészt nyilván olyan univerzális eljárás sincs, amelynek segítségével minden szög harmada (ugyanúgy) megszerkeszthető.

   A racionális testből kiindulva a 60°-os szög nyilvánvalóan szerkeszthető.

   A 20°-os szög szerkesztése ekvivalens a $\cos 20°$ szerkesztésével. Felhasználva, hogy $\cos 3\alpha = 4\cos^3\alpha - 3\cos\alpha$, a szerkesztendő $x = \cos 20°$ távolságra azt kapjuk, hogy ki kell elégítenie az

$$\frac{1}{2} = 4x^3 - 3x$$

   egyenletet, vagyis gyöke a racionális test feletti

$$f(x) = 8x^3 - 6x - 1$$

   polinomnak. Ez a polinom viszont irreducibilis a racionális test felett (hiszen ha nem volna irreducibilis, akkor volna racionális gyöke, ami viszont a Rolle-tétel következtében csak a ± 1, $\pm\frac{1}{2}$, $\pm\frac{1}{4}$, $\pm\frac{1}{8}$ számok

valamelyike lehetne, viszont – mint arról behelyettesítéssel könnyen meggyőződhetünk – ezek egyike sem gyök), így egyik gyöke sem – ezért a $\cos 20^\circ$ sem – szerkeszthető.

Eredményünk nem jelenti azt, hogy semmilyen kiindulási adatokból nem szerkeszthető meg a 60°-os szög harmada, ha például kiindulási adataink tartalmaznak egy 40°-os szöget, akkor ezekből az adatokból a 60° is és a 20° is nyilván szerkeszthető (de ekkor a kiindulási adatok teste nem a racionális test).

Azt is érdemes megjegyezni, hogy a racionális test felett – szögfelezések és szögmásolások segítségével – számos szög harmada szerkeszthető. Nyilvánvalóan szerkeszthető például a 180° vagy a 90° harmada, sőt az összes $k\dfrac{180^\circ}{2^n}$ (k és n tetszőleges pozitív egészek) szög harmada. A szögharmadolás problémája nyilvánvalóan ekvivalens azzal a kérdéssel, hogy egy adott kiindulási test esetén egyáltalán mely szögek szerkeszthetők és melyek nem.

4. Szabályos sokszögek szerkesztése

A feladat egy adott kör kerületének n egyenlő részre osztása, vagyis a $\dfrac{360^\circ}{n}$ szög – vagy az ezzel ekvivalens $\cos\dfrac{2\pi}{n}$ távolság – szerkesztése.

A szabályos háromszög és a négyzet nyilvánvalóan szerkeszthető. Azt is tudjuk, hogy a szabályos ötszög is szerkeszthető. Ha valamilyen n-re szerkeszthető a szabályos n-szög, akkor a szabályos $2n$-szög is szerkeszthető (szögfelezéssel), így a szabályos 6-, 8- és 10-szög is (továbbá tetszőleges pozitív egész k-ra a szabályos 2^k, $3\cdot 2^k$ és $5\cdot 2^k$ szög is) szerkeszthető.

Megmutatjuk, hogy a szabályos hétszög nem szerkeszthető. Válasszuk az adott kör sugarát egységnyinek, így most is tekinthetjük a racionális testet a kiindulási adatok testének.

Feladatunk az $x = \cos\dfrac{2\pi}{7}$ távolság megszerkesztése.

Jelöljük ε-nal a $\cos\dfrac{2\pi}{7} + i\sin\dfrac{2\pi}{7}$ komplex hetedik egységgyököt. Ekkor egyrészt

$$\left(\varepsilon + \frac{1}{\varepsilon}\right) = 2\cos\frac{2\pi}{7} = 2x,$$

másrészt tudjuk, hogy

$$1 + \varepsilon + \varepsilon^2 + \varepsilon^3 + \varepsilon^4 + \varepsilon^5 + \varepsilon^6 = 0,$$

így

$$\left(\varepsilon^3 + \frac{1}{\varepsilon^3}\right) + \left(\varepsilon^2 + \frac{1}{\varepsilon^2}\right) + \left(\varepsilon + \frac{1}{\varepsilon}\right) + 1 = 0$$

Felhasználva, hogy

$$\left(\varepsilon^3+\frac{1}{\varepsilon^3}\right)=\left(\varepsilon+\frac{1}{\varepsilon}\right)^3-3\left(\varepsilon+\frac{1}{\varepsilon}\right)$$

és

$$\left(\varepsilon^2+\frac{1}{\varepsilon^2}\right)=\left(\varepsilon^2+\frac{1}{\varepsilon^2}\right)-2,$$

azt kapjuk, hogy

$$(2x)^3-3(2x)+(2x)^2-2+2x+1=0,$$

vagyis a szerkesztendő x távolság gyöke az

$$f(x)=8x^3+4x^2-4x-1$$

polinomnak. Ez viszont a racionális test felett irreducibilis harmadfokú polinom, így egyetlen gyöke sem szerkeszthető.

Nem szerkeszthető a szabályos kilencszög sem, hiszen ha szerkeszthető lenne, akkor a szabályos 18-szög is szerkeszthető lenne, a szabályos 18-szög szerkesztése viszont éppen a 20°-os szög szerkesztését jelentené, amiről már láttuk, hogy a racionális test felett lehetetlen.

Belátható, hogy ha a szabályos n_1-szög is és a szabályos n_2-szög is szerkeszthető ahol $(n_1,n_2)=1$, akkor szerkeszthető a szabályos n_1n_2-szög is. Ha ugyanis $(n_1,n_2)=1$, akkor az $n_1x-n_2y=1$ diofantoszi egyenletnek létezik pozitív egész megoldása, vagyis vannak olyan x_0 és y_0 pozitív egész számok, amelyekre

$$n_1x_0-n_2y_0=1,$$

és így

$$x_0\frac{2\pi}{n_2}-y_0\frac{2\pi}{n_1}=\frac{2\pi}{n_1n_2}.$$

Ez viszont azt jelenti, hogy az azonos körbe írt és közös csúccsal rendelkező szabályos n_1-szög és szabályos n_2-szög csúcspontjai közül kiválasztható egy-egy úgy, hogy a kiválasztott pontok által meghatározott középponti szög éppen a szabályos n_1n_2-szög oldalához tartozó középponti szög legyen. Ezek szerint elegendő olyan n-ekre vizsgálni a szabályos n-szög szerkeszthetőségének kérdését, melyek prímhatványok.

Azt már tudjuk, hogy ha $n=2^k$, akkor tetszőleges $k>1$ (egész) esetén szerkeszthető a szabályos n-szög. Bizonyítható, hogy $n=p^k$ esetén, ahol p páratlan prím, akkor és csak akkor szerkeszthető a szabályos n-szög, ha $k=1$, p pedig egy Fermat-prím ($2^{2^t}+1$ alakú).

Összefoglalva a fentieket, a következőket állapíthatjuk meg:

13.4. Tétel. *A szabályos n-szög (euklideszi értelemben) akkor és csak akkor szerkeszthető, ha $n = 2^k p_1 p_2 \dots p_r$, ahol p_1, p_2, …, p_r különböző Fermat-prímek és $k, r \geq 0$, egész.*

A fenti tételt az akkor 19 éves Gauss bizonyította 1796-ban, tisztázva ezzel egy kétezer éve megoldatlan problémát. Egyben eljárást is adott a szabályos 17-szög szerkesztésére, ennek emlékét őrzi a szülővárosában, Braunschweigben felállított Gauss-emlékmű talapzatába vésett szabályos 17-szög. A pillanatnyilag ismert öt Fermat-prím (3, 5, 17, 257, 65 537) mindegyikéhez sikerült azóta konkrét szerkesztési eljárást találni.

A szabályos 17-szög szerkesztéséről olvashatunk Frenkel Péter cikkében [5].

A fenti eredmények mindegyike szigorúan az euklideszi szerkesztésekre vonatkozik. Más eredményeket kaphatunk akkor, ha más eszközöket vagy más szerkesztési lépéseket engedünk meg. Létezik például olyan eszköz, amely kifejezetten szögek harmadolására született.

Külön kérdéskör foglalkozik az úgynevezett korlátozott szerkesztésekkel, amelynek egy érdekes kérdése például az, hogy minden olyan pont, amely euklideszi értelemben megszerkeszthető, akkor is megszerkeszthető-e, ha csak körzőt vagy csak vonalzót használhatunk. A tény az, hogy a síkban minden olyan pont, amely körzővel és vonalzóval megszerkeszthető, megszerkeszthető csak körző segítségével (Mascheroni-féle szerkesztés). Az azonban nem igaz, hogy csak vonalzóval megszerkeszthető lenne minden euklideszi eszközökkel szerkeszthető pont. Ha viszont adott két (egymástól egység távolságra lévő) párhuzamos egyenes, akkor már igen.

További érdekességként megemlítünk egy szerkesztéssel kapcsolatos eredményt, illetve néhány hozzá kapcsolódó tényt.

13.10. Állítás. *A legkisebb szerkeszthető, fokokban kifejezhető egész szám mértékű szög a $3°$.*

Bizonyítás. A szabályos 5-szög szerkeszthető, amelynek van $144°$-os szöge. A 8-adrésze ($18°$) tehát szerkeszthető. A $60°$-os szög negyedrésze ($15°$) szintén szerkeszthető. Ezért a $18° - 15° = 3°$-os szög is szerkeszthető.

Ha ennél kisebb egész szög is szerkeszthető lenne (1 vagy 2), akkor szerkeszthető lenne a $20°$-os szög is, ám ez nem igaz. □

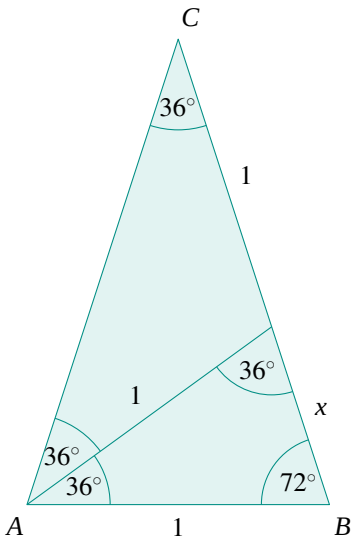
Megjegyzés. Jellemzően szögek összege és különbsége szerkeszthető, természetes számszorosaik is szerkeszthetők, illetve a szerkeszthető szöveg fele is szerkeszthető.

A 72°-os szög szerkesztése Képzeljünk el egy olyan egyenlő szárú háromszöget, amelynek alapja 1 hosszúságú, a szárszöge 36°, az alapon nyugvó szögei 72°-osak. Ha az alapon nyugvó egyik szögből megrajzoljuk a szögfelezőt, akkor ez az egyenes két olyan háromszögre bontja az eredeti háromszöget, amelyek közül az egyik hasonló az eredetihez (13.19. ábra).

Ezekre felírható egy hasonlósági arány: $1 : x = (1 + x) : 1$. Ebből $x^2 + x - 1 = 0$, amelynek (pozitív) gyöke:

$$\frac{-1 + \sqrt{1+4}}{2} = \frac{\sqrt{5} - 1}{2}.$$

Ezt a szakaszt – az egység hosszúságú szakaszból kiindulva – euklideszi eszközökkel meg tudjuk szerkeszteni. Vagyis a háromszög szerkeszthető, így tudunk 36°-os szöget szerkeszteni.



13.19. ábra. 36°–72°–72° szögű háromszög

Érdekesség, hogy a geometriában egy szerkesztési problémát a legritkább esetben szokás algebrai útra terelni – habár mindig eredményre vezet. A szabályos tízszög (illetve ötszög) szerkesztése éppen ilyen: egyszerűbb kiszámítani a keresett oldal hosszát és azt megszerkeszteni az algebrai összefüggések ismeretében, mint olyan geometriai mértani helyeket keresni, amelyek metszéspontjaként megkapjuk a tízszög (ötszög) egy még nem ismert csúcspontját (mint ahogyan azt a szabályos hatszög esetében oly egyszerűen megtehetjük).

Feladatok

1. Szerkesszen euklideszi módon $\sqrt{1000}$ hosszúságú szakaszt (az egysényi hosszú szakaszból kiindulva).

2. Szerkeszthető-e euklideszi értelemben egy tetszőleges szög $\frac{1}{5}$ része?

3. Szerkesszen szabályos ötszöget! Szerkessze meg csak körző használatával! (Az oldalak szakaszát nyilván nem tudjuk megszerkeszteni csak körzővel, ebben az esetben csak az öt csúcspontot tudjuk kijelölni.)

4. Adott egy 133°-os szög. Szerkeszthető-e ebből a 3°-os szög?

5. Igazolja, hogy ha adott egy 19°-os szög, akkor abból megszerkeszthető az 1°-os szög!

   Szerkeszthető-e (euklideszi értelemben) az 1°-os szög, ha csak egy egységnyi szakasz a kiindulási adat?

   Mekkora a legkisebb egész számmal kifejezhető fok, amely szerkeszthető?

6. Adott egy egyenlő szárú háromszög egyik szára (egy szakasz), valamint a vele szemben fekvő szög szögfelező egyenese (a szakaszt metsző egyenes). Megszerkeszthető-e ebből a háromszög? Miért?

7. Oldja meg a következő feladatot!

Irodalomjegyzék

[1] Bálintné Szendrei Mária, Czédli Gábor, Szendrei Ágnes: *Absztrakt algebrai feladatok,* Tankönyvkiadó, Budapest, 1985.

[2] Fried Ervin: *Algebra II., Algebra struktúrák,* Nemzeti Tankönyvkiadó, 2002.

[3] Korándi József, Török Judit, *Absztrakt algebra,* Számelmélet és algebra sorozat, 3. kötet. NLV Nyomda, Budapest, 1996

[4] Varga Árpád: *Absztrakt algebrai feladatgyűjtemény* (kézirat, 6., változatlan utánnyomás), Tanárképző Főiskolák sorozat, Tankönyvkiadó, Budapest, 1983.

[5] http://www.tankonyvtar.hu/hu/tartalom/tkt/uj-matematikai-mozaik-uj/ar12.html

Egyéb ajánlott irodalom

Israel Kleiner: From Numbers to Rings: The Early History of Ring, *Theory Elemente der Mathematik,* Volume 53, Number 1 (1998), 18–35,

J. Dieudonné: The historical developement of algebraic geometry, *The American Mathematical Monthly,* Vol. 79, No. 8 (Oct., 1972), pp. 827–866

Montágh Balázs: *Salakmotor-versenyek és véges síkok, Új matematikai mozaik,* Typotex, http://www.tankonyvtar.hu/hu/tartalom/tkt/uj-matematikai-mozaik-uj/ar01.html

Gyapjas Ferenc: *Csoportelmélet,* Tankönyvkiadó, Budapest, 1974, Középiskolai szakköri füzetek, ISBN-szám: 963-17-0530-7

B. L. Van Der Waerden: *A History of Algebra: From Al-Khwarizmi to Emmy Noether,* Springer, 1990 http://books.google.hu/books?id=1YnuAAAAMAAJ&q=Luca&redir_esc=y

14. fejezet

TESZTEK

Az alábbi tesztkérdések mindegyikében egyetlen helyes választ kell megjelölni.

1. Algebrai műveletek

1. Az alábbiak közül melyik alkot algebrai struktúrát?

   (a) A természetes számok az osztásra nézve.

   (b) A prímszámok a szorzásra nézve.

   (c) A természetes számok a rákövetkezés műveletére. ($n \in \mathbb{N}$ elemhez a rákövetkező természetes számot rendeljük.)

   (d) A valós számok.

2. Az alábbiak közül melyik alkot algebrai struktúrát?

   (a) Az egész számok az osztásra nézve.

   (b) Az 5-nél nem nagyobb természetes számok az összeadásra nézve.

   (c) A természetes számok a rákövetkezés műveletére. ($n \in \mathbb{N}$ elemhez a rákövetkező természetes számot rendeljük.)

   (d) A 2×3-as invertálható mátrixok a mátrixösszeadásra nézve.

3. Az alábbiak közül melyik alkot algebrai struktúrát?

   (a) A természetes számok a kivonásra nézve.

   (b) Az 5-nél nagyobb természetes számok az összeadásra nézve.

   (c) Az egész együtthatós polinomok a polinomosztásra nézve.

(d) A 2×3-as mátrixok a mátrixszorzásra nézve.

4. Az alábbiak közül melyik művelet a természetes számok halmazán?

   (a) Összeadás.
   (b) Additív inverzképzés.
   (c) Kivonás.
   (d) Osztás.

5. Az alábbiak közül melyik egyváltozós művelet az egész számok halmazán?

   (a) Összeadás.
   (b) Additív inverzképzés.
   (c) Kivonás.
   (d) Osztás.

6. Melyik nem alkot algebrai struktúrát az alábbiak közül?

   (a) A természetes számok az összeadásra nézve.
   (b) A természetes számok a rákövetkezésre nézve. ($n \in \mathbb{N}$ elemhez a rákövetkező természetes számot rendeljük.)
   (c) A természetes számok a szorzásra nézve.
   (d) A természetes számok az osztásra nézve.

7. Az $(S, \circ)$ algebrai struktúrában melyik műveleti tulajdonságból következik, hogy: $\forall a, b, c \in S$: $(a \circ b) \circ c = c \circ (a \circ b)$? (Figyelmesen nézze meg a felírt összefüggést!)

   (a) $\circ$ asszociativitása.
   (b) $\circ$ kommutativitása.
   (c) $\circ$ invertálhatósága.
   (d) $\circ$ disztributivitása.

8. Az $(S, \circ, *)$ algebrai struktúrában melyik művelet melyik tulajdonságából következik, hogy $\forall a, b, c \in S$: $(a \circ b) \circ (c * d) = a \circ (b \circ (c * d))$?

   (a) $*$ asszociativitása.
   (b) $\circ$ asszociativitása.
   (c) $\circ$ disztributivitása $*$-ra.
   (d) $*$-nak $\circ$-re vonatkozó disztributivitása.

9. Az $(S, \circ, *)$ algebrai struktúrában melyik műveleti tulajdonságból következik, hogy: $\forall a, b, c \in S$: $(a * b) \circ c = (a \circ c) * (b \circ c)$?

   (a) $\circ$ asszociativitása.

   (b) $*$ asszociativitása.

   (c) $*$ disztributivitása $\circ$-re.

   (d) $\circ$ disztributivitása $*$-ra.

2. Félcsoportok

1. Melyik félcsoport a következők közül?

   (a) $(\{0, 1, 2, 3, 4, 5\}, \circ)$, ahol $\circ$ a valós számokon értelmezett szorzás.

   (b) $(\mathbb{R}^+, \circ)$, ahol $a \circ b = a^b$.

   (c) $(\mathbb{N}, \circ)$, ahol a $\circ$ az egymás után írást jelenti, pl. $47 \circ 16 = 4716$.

   (d) $(\mathbb{R}, *)$, ahol $*$ az additív inverz (ellentett).

2. Melyik félcsoport a következők közül?

   (a) $(\mathbb{N}, \circ)$, ahol $a \circ b = a + b - 1$.

   (b) $(\mathbb{N}, \circ)$, ahol $a \circ b = ab + 1$.

   (c) $(\mathbb{N}, \circ)$, ahol $a \circ b = a + b + 1$.

   (d) $(\mathbb{N}, \circ)$, ahol $a \circ b = ab - 1$.

3. Melyik nem félcsoport a következők közül?

   (a) $(\mathbb{Q}, \cdot)$.

   (b) $(\mathbb{Z}^-, \cdot)$.

   (c) $(\mathbb{R}^+, \cdot)$.

   (d) $(\mathbb{Z}^-, +)$.

4. Melyik nem félcsoport és milyen okból a következők közül?

   (a) $(\mathbb{Z}^-, \cdot)$, mert nem asszociatív.

   (b) $(\mathbb{Z}, -)$, mert nem zárt.

   (c) $(\mathbb{R}, -)$, mert nem asszociatív.

   (d) $(\mathbb{R}^-, \cdot)$, mert nem asszociatív.

5. Melyik tulajdonság szükséges ahhoz, hogy $(S, \circ)$ félcsoport legyen?

   (a) $\circ$ kommutatív.

   (b) $\circ$ asszociatív.

(c) $\circ$ invertálható.

(d) $\circ$ disztributív.

6. Melyik tulajdonság nem szükséges ahhoz, hogy $(S, \circ)$ félcsoport legyen?

(a) S nem üres.

(b) S zárt a $\circ$ műveletre.

(c) $\circ$ kommutatív.

(d) $\circ$ asszociatív.

7. Melyik egységelemes félcsoport?

(a) $(\mathbb{N}, \cdot)$.

(b) $(\mathbb{Z}^-, \cdot)$.

(c) $(\mathbb{R}^+, +)$.

(d) $(\mathbb{R}^-, +)$.

8. Melyik félcsoportban nincs egységelem?

(a) $(\mathbb{Z}^+, +)$.

(b) $(\mathbb{R}^+, \cdot)$.

(c) $(\mathbb{R}, +)$.

(d) $(\mathbb{Z}^+, \cdot)$.

9. Melyik félcsoportban nincs egységelem, és ennek mi az oka?

(a) Az 5-nél nagyobb természetes számok összeadásra vett félcsoportjában, mert a művelet nem kommutatív.

(b) A pozitív egész számok szorzásra vett félcsoportjában, mert nincs benne a 0.

(c) A negatív egész számok összeadásra vett félcsoportjában, mert nincs benne a 0.

(d) A valós együtthatós polinomok szorzásra vett félcsoportja, mert a polinomok körében nincs inverz.

10. Mi az egységelem a $(\mathbb{Z}, \circ)$ félcsoportban, ahol $a \circ b = -ab + a + b$?

(a) -1.

(b) 1.

(c) 0.

(d) Nincs.

3. Csoportok

1. Melyik alkot csoportot az alábbi struktúrák közül?

   (a) $(\mathbb{N}, +)$
   (b) $(\mathbb{Z}, +)$
   (c) $(\mathbb{N}, \cdot)$
   (d) $(\mathbb{Z}, \cdot)$

2. Melyik nem csoport az alábbiak közül?

   (a) $(\mathbb{R}, +)$
   (b) $(\mathbb{Q}, +)$
   (c) $(\mathbb{Z}, +)$
   (d) $(\mathbb{N}, +)$

3. Melyik nem csoport, és miért nem az?

   (a) $(\mathbb{Z}, +)$, mert a művelet nem asszociatív.
   (b) $(\mathbb{Z}, \cdot)$, mert a művelet nem invertálható.
   (c) $(\mathbb{Z}, +)$, mert a művelet nem invertálható.
   (d) $(\mathbb{Z}, \cdot)$, mert a művelet nem asszociatív.

4. Keresse ki azt a struktúrát, amelyik csoport, de nem ciklikus?

   (a) $(\mathbb{N}, +)$
   (b) $(\mathbb{Z}, +)$
   (c) $(\mathbb{R}, +)$
   (d) $(\mathbb{Z}_5, +_{\text{mod } 5})$

5. Az $(S, \circ)$ csoportban a művelet melyik tulajdonságát nem követlejük meg?

   (a) Asszociativitás.
   (b) Zártság.
   (c) Invertálhatóság.
   (d) Kommutativitás.

6. Melyik elemnek nem 6 a rendje a $(\mathbb{Z}_{18}, +_{\text{mod } 18})$ csoportban?

   (a) 3.
   (b) 6.
   (c) 9.

(d) 15.

7. Hány részcsoportja van a $(\mathbb{Z}_8, +_{\text{ mod } 8})$ csoportnak?

   (a) 1.
   (b) 2.
   (c) 4.
   (d) 8.

4. Mellékosztályok, normálosztó

1. Hány mellékosztálya van a $(\mathbb{Z}_8, +_{\text{ mod } 8})$ csoportnak egy kételemű részcsoportja szerint?

   (a) 1.
   (b) 2.
   (c) 4.
   (d) 8.

2. Melyik normálosztó D_3-ban (a halmaz elemeit a szokásos módon f_0, f_{120}, f_{240}, t_A, t_B, t_C jelöli)?

   (a) $\{t_A, t_B, t_C\}$.
   (b) $\{f_0, f_{120}, f_{240}\}$.
   (c) $\{f_0, t_A\}$.
   (d) $\{f_0, t_B\}$.

3. Egy 24 elemű csoportot egy 6 elemű részcsoportja szerint faktorizálnuk. Hány eleme lesz a faktorcsoportnak?

   (a) 24.
   (b) 6.
   (c) 4.
   (d) 8.

4. Melyik állítás nem igaz az alábbiak közül?

   (a) Egy ciklikus csoportban minden részcsoport normálosztó.
   (b) Minden csoportban minden 2 indexű részcsoport normálosztó.
   (c) Minden csoportban minden kételemű részcsoport normálosztó.
   (d) Egy csoport centruma mindig normálosztó. (A $(G, \circ)$ csoport centruma azon h elemei halmaza, amelyekre minden csoportbeli g elemre $h \circ g = g \circ h$.)

5. Csoport kompatibilis osztályozása

1. A valós számok összeadásra vett csoportjában az egészek részcsoportot alkotnak ezzel faktorizálva a kapott struktúra melyik alábbival lesz izomorf?

   (a) $(\mathbb{Z}, +)$.

   (b) $(\mathbb{Z}, \circ)$, ahol $a \circ b = \{a\} + \{b\}$.

   (c) $([0, 1), \circ)$, ahol $a \circ b = \{a + b\}$.

   (d) $([0, 1), \circ)$, ahol $a \circ b = \{a\} + \{b\}$.

2. Melyik állítás nem feltétlenül igaz az alábbiak közül?

   (a) Egy G csoport kompatibilis osztályozásakor az egységelemet tartalmazó osztály normálosztó.

   (b) Egy G csoport normálosztója szerinti osztályozás kompatibilis.

   (c) Egy G csoportot homomorf módon leképezve egy H csoportba a kapott képelemek halmaza normálosztó G-ben.

   (d) Egy G csoportot homomorf módon leképezve egy H csoportba a kapott képelemek ősképei a csoport kompatibilis osztályozását adják.

3. $(\mathbb{Z}, +)$ melyik osztályozása kompatibilis?

   (a) Azokat az elemeket soroljuk egy osztályba, amelyek abszolút értéke ugyanarra a számjegyre végződik.

   (b) Azokat az elemeket soroljuk egy osztályba, amelyek ugyanazzal a számjeggyel kezdődnek.

   (c) Azokat az elemeket soroljuk egy osztályba, amelyekben ugyanannyi az 1-es számjegyek száma.

   (d) A számokhoz hozzáadjuk az abszolút értékeik 10-szeresét, majd azokat a számokat soroljuk egy osztályba, amelyekhez az így képzett összeg ugyanarra a számjegyre végződik.

4. Az alábbi csoportpárok közül melyek nem izomorfak?

   (a) S_3 és D_3.

   (b) $(\{\text{igaz}, \text{hamis}\}, \vee)$ és $(\{0, 1\}, \min)$.

   (c) $(\mathbb{R}^+, \cdot)$ és $(\mathbb{R}, +)$.

   (d) $(\mathbb{Q}^+, \cdot)$ és $(\mathbb{Q}, +)$.

6. Permutációcsoportok

1. Mennyi a $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 1 & 5 & 2 & 4 \end{pmatrix}$ permutáció rendje?

   (a) 1
   (b) 3
   (c) 5
   (d) 7

2. Hány diszjunkt ciklusra bomlik a $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 7 & 5 & 6 & 3 & 4 & 1 \end{pmatrix}$ permutáció?

   (a) 1
   (b) 3
   (c) 5
   (d) 7

3. Melyik állítás igaz az alábbiak közül? (Figyelmesen olvassa el az állításokat!)

   (a) Páros permutációk szorzata páros.
   (b) Páratlan permutációk szorzata páratlan.
   (c) Páros permutációk összege páros.
   (d) Páratlan permutációk összege páratlan.

4. Melyik állítás nem helyes?

   (a) Minden véges csoporthoz van vele izomorf permutációcsoport.
   (b) Minden permutációval van vele izomorf véges csoport.
   (c) Minden véges csoport izomorf egy permutációcsoport valamely részcsoportjával.
   (d) Minden permutációcsoport izomorf egy csoporttal.

7. Gyűrűk

1. Melyik nem gyűrű az alábbi struktúrák közül?

   (a) $(\mathbb{Z}, +, \cdot)$.
   (b) A 3×2-es valós elemű mátrixok a mátrixösszeadásra és a mátrixszorzásra.

(c) A valós együtthatós polinomok a polinomösszeadásra és polinomszorzásra.

(d) A teljes valós halmazon folytonos függvények a függvényösszeadásra és függvényszorzásra.

2. Az alábbiak közül melyik gyűrű nem izomorf az egész számok gyűrűjével?

(a) Az $\begin{pmatrix} a & 0 \\ a & 0 \end{pmatrix}$ alakú mátrixok a mátrixösszeadással és a mátrixszorzással.

(b) Az $\begin{pmatrix} a & a \\ 0 & 0 \end{pmatrix}$ alakú mátrixok a mátrixösszeadással és a mátrixszorzással.

(c) Az $\begin{pmatrix} a & a \\ a & a \end{pmatrix}$ alakú mátrixok a mátrixösszeadással és a mátrixszorzással.

(d) Az $\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix}$ alakú mátrixok a mátrixösszeadással és a mátrixszorzással.

3. Melyik igaz az alábbiak közül mindegyik $(R, +, \cdot)$ gyűrűre?

(a) Az összeadás nem feltétlenül kommutatív.

(b) Az összeadás nem lehet invertálható.

(c) A szorzás nem lehet invertálható.

(d) A szorzás nem feltétlenül kommutatív.

9. Testek

1. Melyik igaz az alábbiak közül minden $(T, +, \cdot)$ testre?

(a) Az összeadás nem feltétlenül kommutatív.

(b) Az összeadás nem szükségképpen invertálható.

(c) Van olyan eleme, amelynek nincs multiplikatív inverze.

(d) A szorzás nem lehet kommutatív.

2. Melyik nem test az alábbiak közül?

(a) $(\mathbb{Q}, +, \cdot)$.

(b) $(\mathbb{Z}, +, \cdot)$.

(c) $(\mathbb{R}, +, \cdot)$.

(d) $(\mathbb{C}, +, \cdot)$.

3. Melyik nem test az alábbiak közül?

   (a) $(\mathbb{Q}, +, \cdot)$.
   (b) $(\mathbb{C}, +, \cdot)$
   (c) $(\mathbb{Z}_5, +_{\text{ mod } 5}, \cdot_{\text{ mod } 5})$.
   (d) $(\mathbb{Z}_9, +_{\text{ mod } 9}, \cdot_{\text{ mod } 9})$.

4. Melyik nem prímtest az alábbiak közül?

   (a) $(\mathbb{Q}, +, \cdot)$.
   (b) $(\{0, 1\}, \circ, *)$, ahol 0 az összeadás, 1 a szorzás egységeleme.
   (c) $(\mathbb{Z}_5, +_{\text{ mod } 5}, \cdot_{\text{ mod } 5})$.
   (d) A 3×3-as reguláris (nem 0 determinánsú) mátrixok a mátrix-összeadásra és -szorzásra.

11. Testbővítések

1. Melyik testet kaphatjuk meg a $(\mathbb{Z}_3, +_{\text{ mod } 3}, \cdot_{\text{ mod } 3})$ test bővítéseként?

   (a) $(\mathbb{Z}, +, \cdot)$.
   (b) $(\mathbb{Z}_5, +_{\text{ mod } 5}, \cdot_{\text{ mod } 5})$.
   (c) $(\mathbb{Q}, +, \cdot)$.
   (d) A fentiek egyikét sem.

2. Melyik test fölött algebrai elem az $i \cdot \pi$?

   (a) $(\mathbb{Q}, +, \cdot)$.
   (b) $(\mathbb{Z}_{11}, +_{\text{ mod } 11}, \cdot_{\text{ mod } 11})$.
   (c) $(\mathbb{R}, +, \cdot)$.

3. Melyik algebrai szám?

   (a) $\frac{\pi}{\pi^2}$
   (b) $\frac{\pi^2}{\pi}$
   (c) $\frac{\pi^2}{2\pi}$
   (d) $\frac{\pi/2}{\pi}$

4. Hányadfokú testbővítése $\mathbb{Q}$-nak a $\sqrt{2} + \sqrt{7}$-tel való bővítése?

   (a) 1

(b) 2

(c) 3

(d) 4

5. Ha $A = \mathbb{Q}(\sqrt{2})$, $B = \mathbb{Q}(\sqrt{3})$, $C = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, akkor az alábbi állítások közül melyik igaz?

   (a) $C = A \cap B$

   (b) $C \subset A$

   (c) $A \subset C$

   (d) $A = C \setminus B$

12. A geometriai szerkeszthetőség algebrai elmélete

1. Egy szakasz ismeretében hányadrésze szerkeszthető meg Euklideszi eszközökkel?

   (a) A π-ed része.

   (b) Az e-ed része.

   (c) A $\sqrt{2}$-ed része.

   (d) Az i-ed része.

2. Egy szög ismeretében annak hányadrésze szerkeszthető meg Euklideszi eszközökkel?

   (a) A hatoda.

   (b) A hetede.

   (c) A nyolcada.

   (d) A tizede.

Megoldások

EZ MÉGSEM PERMUTÁCIÓK SZORZATA.

A tesztek megoldása:

1. fejezet: 1. (c) 2. (c) 3. (b) 4. (a) 5. (b) 6. (d) 7. (a) 8. (b) 9. (d)

2. fejezet: 1. (c) 2. (c) 3. (b) 4. (c) 5. (b) 6. (c) 7. (a) 8. (a) 9. (c) 10. (c)

3. fejezet: 1. (b) 2. (d) 3. (b) 4. (c) 5. (d) 6. (b) 7. (c)

4. fejezet: 1. (c) 2. (b) 3. (c) 4. (c) (Felezni mindig lehet $\mathbb{Q}$-ban, gyököt vonni nem minden esetben a $\mathbb{Q}^+$-ban.)

5. fejezet: 1. (c) 2. (c) 3. (d) 4. (d)

6. fejezet: 1. (c) 2. (b) 3. (a) 4. (b)

7. fejezet: 1. (b) 2. (c) 3. (d)

9. fejezet: 1. (c) 2. (b) 3. (d) 4. (d)

11. fejezet: 1. (d) 2. (c) 3. (d) 4. (d) 5. (c)

12. fejezet: 1. (c) 2. (c)

Tárgymutató

Az alábbi videón egy feladat látható, amelyet K. Hofstetter, A Simple Compass-Only Construction of the Regular Pentagon, Forum Geometricorum Volume 8 (2008) 147–148. cikke alapján készítettünk el.

http://www.cs.elte.hu/ kfried/algebra3/feladat.avi