PÉLDÁK ÉS MEGOLDÁSOK A

BEVEZETÉS A MATEMATIKÁBA

TÁRGY II. FÉLÉVÉHEZ

I. KÖTET

BURCSI PÉTER: GRÁFOK
LÁNG CSABÁNÉ: CSOPORTOK
GERMÁN LÁSZLÓ: GYŰRŰK ÉS TESTEK

ELTE Budapest 2006-03-16
IK Digitális Könyvtár
1. kiadás

Felsőoktatási tankönyv

Lektorálták:
Burcsi Péter: Csoportok
Láng Csabáné: Gráfok, Gyűrűk és testek

Szerkesztette: Láng Csabáné

Tartalomjegyzék

1. Bevezetés

Elsősorban az ELTE Informatikai Kar programtervező informatikus, programtervező matematikus, programozó és informatika tanár szakos hallgatói számára készült ez a példatár, amely részletesen kidolgozott példákat tartalmaz.

A 2. fejezetben a példákat soroltuk fel, a 3. fejezetben pedig ezek a példák megoldással együtt szerepelnek.

A példák részben más könyvekből, példatárakból, mások által összeállított feladatsorokból származnak. Azok a források, amelyekről tudomásunk van, szerepelnek az *Ajánlott irodalom* fejezetben. A feladatok más része pedig ebben a példatárban jelenik meg először.

A könyvben található hibákra, hiányosságokra vonatkozó észrevételeket köszönettel fogadjuk.

Budapest, 2006. március

Láng Csabáné

szerkesztő

zslang@compalg.inf.elte.hu

ELTE Informatikai Kar Komputer Algebra Tanszék

1117 Budapest, Pázmány Péter sétány I/C.

2. Példák

2.1. Gráfok

2.1.1. Alapfogalmak

2.1-1. Van-e olyan 7 pontú egyszerű gráf, melyben a csúcsok foka rendre

a. 4, 4, 4, 3, 3, 3, 3;

b. 6, 3, 3, 2, 2, 2, 0;

c. 5, 5, 5, 4, 4, 2, 2;

d. 5, 5, 5, 2, 2, 2, 1;

e. amelyben minden pont foka különböző?

2.1-2. Legyen $n \in \mathbb{N}$, és $G = (V, E)$ egyszerű gráf, melynek legfeljebb $2n + 1$ csúcsa van. Lássuk be, hogy ha minden $v \in V$ esetén $d(v) \geq n$, akkor G összefüggő. Igaz marad-e az állítás akkor is, ha csak azt tesszük fel, hogy minden csúcsra $d(v) \geq n - 1$?

2.1-3. Legyen G egy véges egyszerű gráf, $\overline{G}$ a komplementere. Lássuk be, hogy G vagy $\overline{G}$ összefüggő.

2.1-4. Igazoljuk, hogy ha egy véges egyszerű gráfban minden csúcs foka leg-

alább k (ahol $k \geq 2$), akkor van a gráfban olyan kör, amely legalább $k+1$ pontot tartalmaz.

2.1-5. Adjuk meg az összes 4, illetve 5 csúcsú egyszerű gráfot, amelyek izomorfak a komplementerükkel.

2.1-6. Hat versenyző körmérkőzést játszik. Bizonyítandó, hogy bármely időpontban van három olyan versenyző, akik már mind játszottak egymással, vagy három olyan, akik közül semelyik kettő nem játszott még.

2.1-7. Jelöljük egy véges fagráf elsőfokú pontjainak számát f_1-gyel, a 2-nél nagyobb fokú pontjainak számát pedig c-vel. Bizonyítsuk be, hogy ha a pontok száma legalább 2, akkor $f_1 \geq c+2$.

2.1-8. Igazoljuk, hogy egy összefüggő véges gráfban bármely két leghosszabb útnak van közös pontja.

2.1-9. Igazoljuk, hogy véges fában az összes leghosszabb út egy ponton megy át.

2.1-10. Legyen n egynél nagyobb pozitív egész.

a. Legfeljebb hány szeparáló él van egy n pontú gráfban? Adjuk meg az olyan gráfokat, amelyekben pontosan ennyi szeparáló él van.

b. Legfeljebb hány szeparáló csúcs van egy n pontú gráfban? Adjuk meg az olyan gráfokat, amelyekben pontosan ennyi szeparáló csúcs van.

2.1.2. Euler-gráf

2.1-11. Van-e olyan Euler-gráf, melynek páros számú pontja és páratlan számú éle van?

2.1-12. Igazoljuk, hogy ha egy hurokélt nem tartalmazó véges gráf minden pontjának foka 4, akkor élei megszínezhetők piros és kék színekkel úgy, hogy minden szögponthoz két piros és két kék él illeszkedjen.

2.1-13. Legyen a G véges összefüggő gráfban $2k$ darab páratlan fokú pont. Igazoljuk, hogy a gráf élhalmaza előáll k darab éldiszjunkt vonal élhalmazának egyesítéseként.

2.1.3. Hamilton-út, Hamilton-kör

2.1-14. Mutassuk meg, hogy egy körmérkőzéses pingpongverseny résztvevői sorba állíthatók úgy, hogy mindenki legyőzte a közvetlenül mögötte állót. (Azt nem követeljük meg, hogy az összes mögötte állót le kellett volna győznie.)

2.1-15. Legyen k pozitív egész. Igazoljuk a következőket:

- Ha egy véges összefüggő gráfban van k olyan csúcs, melyek elhagyásával

a gráf több mint k komponensre esik szét, akkor a gráfban nem találhatunk Hamilton-kört.

• Ha egy véges összefüggő gráfban van k olyan csúcs, melyek elhagyásával a gráf több mint $k+1$ komponensre esik szét, akkor a gráfban nincs Hamilton-út.

2.1-16. Bizonyítsuk be, hogy ha egy véges összefüggő gráf K köréből egy élt eltörölve a gráf egy leghosszabb útját kapjuk, akkor K Hamilton-köre a gráfnak.

2.1-17. Legyen $n \geq 3$ pozitív egész, és G egy n pontú egyszerű összefüggő gráf. Igazoljuk, hogy ha G minden csúcsának foka legalább $\frac{n}{2}$, akkor G-nek van Hamilton-köre.

2.1.4. Síkbeli gráfok

2.1-18.

a. Bizonyítsuk be, hogy ha egy G gráf pontszáma legalább 11, akkor vagy G, vagy G komplementere nem síkgráf.

b. Adjunk meg 8 pontú síkgráfot úgy, hogy komplementere is síkgráf legyen.

2.1-19. Hány éle van egy n pontú összefüggő síkgráfnak, ha minden tartománya (a külső is)

a. háromszög,

b. négyszög?

2.1-20. Hány éle lehet legfeljebb egy síkba rajzolható, n pontú egyszerű páros gráfnak?

2.2. Csoportok

2.2.1. Félcsoport, csoport

2.2-1. Vizsgáljuk meg az alábbi példákban, hogy a művelet vajon művelete az adott halmazon, s ha igen, akkor a halmaz a művelettel félcsoport-e, csoport-e.

a. $(\mathbb{Z}, \circ)$, ha $a \circ b = (a+b)/2 \quad (a, b \in \mathbb{Z})$;

b. $(\mathbb{Q}, \circ)$, ha $a \circ b = (a+b)/2 \quad (a, b \in \mathbb{Q})$;

c. $(A, \circ)$, ha A a $[0,1]$ intervallumon értelmezett valós függvények halmaza és $(f \circ g)(x) = \max(f(x), g(x))$;

d. $(\mathbb{R}$, osztás);

e. $(\mathbb{R} \setminus \{0\}$, osztás);

2.2-2. Lássuk be, hogy a 8-adik komplex egységgyökök a szorzással csoportot alkotnak.

2.2-3. Legyen n rögzített pozitív egész szám. Lássuk be, hogy az n-edik egységgyökök halmaza a szorzásra nézve csoportot alkot.

2.2-4. Lássuk be, hogy az összes n-edik egységgyök halmaza (n befutja a pozitív egész számokat) a szorzásra nézve csoportot alkot.

2.2-5.

a. Vizsgáljuk meg, hogy a modulo 5 maradékosztályok a maradékosztályok szorzására csoportot alkotnak-e.

b. Állapítsuk meg, hogy a modulo 5 maradékosztályok halmazából elhagyva a 0 által reprezentált maradékosztályt, a maradékosztályok szorzására csoportot kapunk-e?

2.2-6. a. Vizsgáljuk meg, hogy a modulo 8 maradékosztályok a maradékosztályok szorzására csoportot alkotnak-e.

b. Állapítsuk meg, hogy a modulo 8 maradékosztályok halmazából elhagyva a 0 által reprezentált maradékosztályt, a maradékosztályok szorzására csoportot kapunk-e?

c. Állapítsuk meg, hogy a modulo 8 vett redukált maradékosztályok a maradékosztályok szorzására csoportot alkotnak-e?

2.2-7.

a. Vizsgáljuk meg, hogy a modulo m vett maradékosztályok a szorzásra nézve csoportot alkotnak-e.

b. Vizsgáljuk meg, hogy a modulo m vett redukált maradékosztályok a szorzásra nézve csoportot alkotnak-e.

2.2-8. Csoportot alkotnak-e a következő konstrukciók?

a. A modulo 35 maradékosztályok közül az

$$A = \{0, 5, 10, 15, 20, 25, 30\}$$

által reprezentáltak a maradékosztály összeadásra;

b. A modulo 35 maradékosztályok közül

$$A = \{0, 5, 10, 15, 20, 25, 30\}$$

által reprezentáltak a maradékosztály szorzásra;

c. A modulo 35 maradékosztályok közül az

$$A \setminus \{0\}$$

által reprezentáltak a maradékosztály szorzásra;

d. A modulo 25 maradékosztályok közül a

$$B = \{5, 10, 15, 20\}$$

által reprezentáltak a maradékosztály szorzásra.

2.2-9. Az alábbi struktúrák közül válassza ki a félcsoportokat, illetve csoportokat:

a. A természetes számok halmaza az összeadásra nézve.

b. A páros számok halmaza az összeadásra nézve.

c. A páratlan számok halmaza a szorzásra nézve.

d. Az egész számok halmaza az összeadásra nézve.

e. Az egész számok halmaza a szorzásra nézve.

f. A nemnegatív racionális számok halmaza a szorzásra nézve.

g. A pozitív racionális számok halmaza a szorzásra nézve.

h. A nullától különböző valós számok halmaza a szorzásra nézve.

i. A sík vektorainak halmaza az összeadásra nézve.

j. A komplex számok halmaza az összeadásra nézve.

k. A valós elemű n-ed rendű mátrixok halmaza a szorzásra nézve. (n rögzített természetes szám.)

l. A valós elemű n-ed rendű nem szinguláris, (n rangú) mátrixok halmaza a szorzásra nézve.

2.2-10. Legyen $(G, \cdot)$ csoport, $u \in G$ rögzített elem. Definiáljunk G-n egy új $\circ$ műveletet $a \circ b := a \cdot u \cdot b$ segítségével. Csoport lesz-e $(G, \circ)$?

2.2-11. Lássuk be, hogy ha egy csoport minden elemének inverze önmaga, akkor a csoport kommutatív.

2.2-12. Bizonyítsuk be, hogy ha a $(G, \cdot)$ csoport minden a, b elempárjára $(a \cdot b)^2 = a^2 \cdot b^2$, akkor a csoport kommutatív.

2.2.2. Csoport rendje, elem rendje, részcsoport, generátum, Lagrange-tétel

2.2-13.

a. A 8-adik komplex egységgyökök szorzással alkotott csoportjában határozzuk meg a csoport rendjét és az egyes elemek rendjét.

b. Ebben a csoportban határozzuk meg az egyes elemek generátumát.

c. Ciklikus-e ez a csoport?

2.2-14. Vizsgáljuk meg, hogy a következő algebrai struktúrák csoportot alkotnake? Ha igen, adjuk meg a csoport rendjét. A csoportok közül melyek ciklikusak?

a. Az m-mel osztható (m pozitív egész) egész számok az összeadásra nézve.

b. Az egész számok halmaza az $a \circ b = a + b + 1$ műveletre nézve.

Diédercsoport

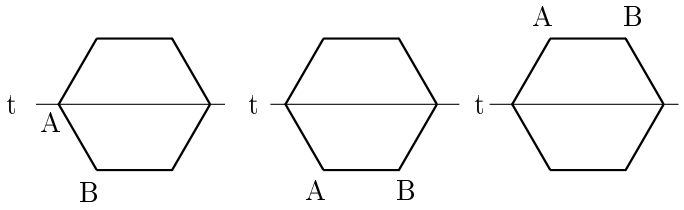
A D_n *diédercsoport* a síknak egy szabályos n oldalú sokszögét önmagába vivő egybevágósági transzformációkból áll, művelet a transzformációk egymás utáni végrehajtása. Ha φ a $\frac{2\pi}{n}$-nel való forgatást, τ pedig egy szimmetriatengelyre való tükrözést jelöl, akkor D_n elemei:

$$\{e, \varphi, \varphi^2, \ldots, \varphi^{n-1}, \tau, \tau \cdot \varphi, \tau \cdot \varphi^2 \ldots, \tau \cdot \varphi^{n-1}\}$$

A számolás szabályai:

$$\varphi^n = \tau^2 = e \quad \varphi \cdot \tau = \tau \cdot \varphi^{n-1}$$

Belátható, hogy D_n a fenti művelettel csoportot alkot.



2. ábra. Szabályos hatszög elforgatása a középpontja körül $\frac{\pi}{6} = 60°$-kal, majd tükrözés a t tükörtengelyre

Az $n = 2$ esetben a *Klein-féle* csoportot kapjuk. Ez az egyetlen kommutatív diédercsoport. $D_2 = \{e, a, b, c\}$, az egységelem kivételével mindegyik elem másodrendű, és bármelyik két elem szorzata a harmadik elem.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

2.2-15. Adott egy sík és abban egy szabályos háromszög. Tekintsük azon síkbeli egybevágósági transzformációk G halmazát, amelyek a szabályos háromszöget önmagába viszik át. A G halmazon értelmezzük a műveletet a transzformációk egymás utáni végrehajtásával (függvénykompozícióként). (Két háromszöget akkor tekintünk azonosnak, ha a megfelelő csúcsok ugyanott vannak.)

a. Bizonyítsuk be, hogy G csoportot alkot.

b. Határozzuk meg a G csoport rendjét.

c. Jelölje φ a szabályos háromszög középpontja körüli pozitív irányú $\frac{2\pi}{3} = 120°$-os elforgatást, τ pedig egy (a síkban rögzített) magasságvonalra vonatkozó tükrözést. Írjuk fel ezek segítségével G összes elemét, határozzuk meg az egyes elemek rendjét, inverzét, valamint a $\{\varphi\}$, a $\{\tau\}$, illetve a $\{\varphi, \tau\}$ halmazok által generált részcsoportokat.

d. Kommutatív-e ez a csoport?

e. Ciklikus-e ez a csoport?

2.2-16. Tekintsük a 15. példában szereplő síkbeli, szabályos háromszöget önmagába vivő egybevágósági transzformációk G csoportját. Határozzuk meg a részcsoportok rendjét.

2.2-17. Írjuk fel a D_4 diédercsoport elemeit, és a számolás szabályait.

2.2-18. Bizonyítsuk be, hogy $(G, \cdot)$ csoportban a és a^{-1} rendje egyenlő.

2.2-19. Bizonyítsuk be, hogy $(G, \cdot)$ csoportban az a és $b^{-1} \cdot a \cdot b$ elemek rendje egyenlő.

2.2-20. Legyen $(G, \cdot)$ véges, páros rendű csoport. Bizonyítsuk be, hogy G-nek van olyan az egységelemtől különböző eleme, amelynek az inverze önmaga.

2.2-21. Bizonyítsuk be, hogy ha $(G, \cdot)$ véges csoport, akkor minden $a \in G$-re

$$a^{|G|} = e,$$

ahol e a csoport egységeleme.

2.2-22. Egy multiplikatív csoport c elemére $c^{100} = e$ és $c^{1999} = e$. Határozzuk

meg c-t.

2.2-23. Bizonyítsuk be, hogy ha egy $(G, \cdot)$ csoportnak van az egységelemtől különböző véges rendű eleme, akkor van prímrendű eleme is.

2.2.3. Mellékosztályok, invariáns részcsoportok

2.2-24. Tekintsük a 15. példában szereplő síkbeli, szabályos háromszöget önmagába vivő egybevágósági transzformációk G csoportját.

a. Jelölje H a τ által generált részcsoportot. Határozzuk meg G-nek a H szerinti bal, illetve jobb oldali mellékosztályait. Invariáns részcsoportja-e H a G csoportnak?

b. Jelölje K a φ által generált részcsoportot. Határozzuk meg G-nek a K szerinti bal, illetve jobb oldali mellékosztályait. Invariáns részcsoportja-e K a G csoportnak?

2.2.4. Homomorfizmus, izomorfizmus

2.2-25. A komplex számok $\mathbb{C}$ halmazában a $*$ és $\circ$ műveleteket az alábbi módon értelmezzük:

$$a * b = a + b + 1, \qquad a \circ b = a + b + i.$$

a. Igazoljuk, hogy a $(\mathbb{C}, *)$ és a $(\mathbb{C}, \circ)$ struktúrák csoportok.

b. Igazoljuk, hogy az $\varphi : a \mapsto ai$ leképezés izomorfizmust létesít a $(\mathbb{C}, *)$ és a $(\mathbb{C}, \circ)$ csoportok között.

2.2-26. Az alábbi struktúrák közül melyek izomorfak?

a. a valós számok az összeadásra;

b. a pozitív valós számok a szorzásra;

c. a nem nulla valós számok a szorzásra;

d. az $\left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \middle| \, c \in \mathbb{R} \right\}$ mátrixok a mátrixszorzásra;

e. az $\left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| \, a \neq 0, a \in \mathbb{R} \right\}$ mátrixok a mátrixszorzásra;

f. a racionális számok az összeadásra $(\mathbb{Q}, +)$.

2.2-27. Az alábbi csoportok közül melyek izomorfok?

a. a modulo 15 redukált maradékosztályok a szorzásra;

b. a modulo 24 redukált maradékosztályok a szorzásra;

c. a nyolcadik komplex egységgyökök a szorzásra;

d. a négyzet szimmetriacsoportja (a D_4 diédercsoport) a transzformációk egymás utáni végrehajtására, mint műveletre.

2.3. Gyűrűk

2.3.1. Gyűrű, test, integritási tartomány, nullosztó

2.3-1. Vizsgáljuk meg, hogy gyűrűt alkotnak-e a az alábbi kétműveletes struktúrák:

a. egész számok az összeadásra és a szorzásra nézve;

b. a páros számok az összeadásra és szorzásra nézve;

c. $\left\{a + b\sqrt{2} \,|\, a, b \in \mathbb{Z}\right\}$ az összeadásra és szorzásra nézve;

d. $\{a + bi \,|\, a, b \in \mathbb{Z}\}$ az összeadásra és szorzásra nézve (Gauss-egészek);

e. $(\mathbb{Z}_m, +, \cdot)$, a modulo m tekintett maradékosztályok a maradékosztály összeadásra és szorzásra nézve.

2.3-2. Teljesüljenek az $(R, +, \cdot)$ struktúrában a következő tulajdonságok:

a. $(R, +)$ csoport,

b. $(R, \cdot)$ egységelemes félcsoport,

c. a szorzás az összeadásra nézve disztributív.

Bizonyítsuk be, hogy $(R, +, \cdot)$ gyűrű.

2.3-3. Bizonyítsuk be, hogy ha az $(R, +, \cdot)$ egységelemes gyűrű minden elemének van multiplikatív inverze, akkor a gyűrűnek csak egyetlen eleme van.

2.3-4. Testet alkotnak-e a $\mod 2m$ maradékosztályok közül a párosak, $\left\{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{2m-2}\right\}$, a maradékosztályok közötti összeadásra és szorzásra nézve, ha

a. $2m = 10$,

b. $2m = 20$.

2.3-5. Bizonyítsuk be, hogy ha $(T, +, \cdot)$ véges, legalább két elemet tartalmazó integritási tartomány, akkor test.

2.3-6. Határozzuk meg a modulo 12 maradékosztályok gyűrűjében a nullosz-

tókat.
2.3-7. Legyen $(R, +, \cdot)$ egységelemes gyűrű, jelölje a nullelemet 0, az egységelemet e. Bizonyítsuk be, hogy ha az $a \in R$ elemre fennáll az $a^n = 0$ valamilyen $n \in \mathbb{N}$-re (a nilpotens), akkor az $e - a$ elemnek van inverze.
2.3-8. Bizonyítsuk be, hogy ha egy $(R, +, \cdot)$ egységelemes gyűrű a elemének van bal oldali multiplikatív inverze, akkor az a elem nem lehet a gyűrű bal oldali nullosztója.

2.3.2. Karakterisztika

2.3-9. Mutassuk meg, hogy ha egy R gyűrű minden a elemére $a^2 = a$ teljesül, akkor R kommutatív és karakterisztikája 2.

2.3.3. Oszthatóság, osztó, egység, felbonthatatlan, prím

2.3-10.

a. Tekintsük a $\mathbb{Z}_{10}$ maradékosztály-gyűrűt. Írjuk fel ebben minden elem (minden maradékosztály) osztóit.

b. Mik az egységek, és mik a nullosztók?

c. Legyen $\overline{a}$ a $\mathbb{Z}_m$ maradékosztály-gyűrű egy maradékosztálya. Adjunk szükséges és elégséges feltételt arra, hogy mikor osztható minden maradékosztály $\overline{a}$-val - vagyis hogy az $\overline{a}$ maradékosztály mikor egység.

Megjegyzés. $\mathbb{Z}_{10}$ nem nullosztómentes, nem integritási tartomány, de alkalmazható az oszthatóság definíciója.
2.3-11.

a. Felbonthatatlan-e $\mathbb{Z}_{10}$-ben $\overline{5}$?

b. Prím-e $\mathbb{Z}_{10}$-ben $\overline{5}$?

Megjegyzés A 3.3.3. példához hasonlóan itt is kiterjesztjük a prím és felbonthatatlan definícióját tetszőleges egységelemes gyűrűre.
2.3-12. Lássuk be, hogy testben minden, a nullelemtől különböző elem egység.

2.3.4. Euklideszi gyűrű

2.3-13. Lássuk be, hogy ha integritási tartományban létezik prím, akkor van egységelem.
2.3-14. Legyen $L := \left\{a + bi\sqrt{5} \,|\, a, b \in \mathbb{Z}\right\}$ a szokásos műveletekkel.

a. Bizonyítsuk be, hogy az L egészek körében $1+i\sqrt{5}$, $1-i\sqrt{5}$, 2, 3 felbonthatatlan elemek, de nem prímelemek.

b. Bizonyítsuk be, hogy az $(L,+,\cdot)$ gyűrű nem euklideszi gyűrű.

2.3.5. Részgyűrű, ideál, faktorgyűrű

2.3-15. Melyek $(\mathbb{Z}_4,+,\cdot)$ részgyűrűi? Van-e köztük ideál?
2.3-16. Legyen R véges gyűrű, I ideál R-ben, és $R \neq I$. Bizonyítsuk be, hogy I minden nullelemtől különböző eleme nullosztó R-ben.
2.3-17. Határozzuk meg $(T,+,\cdot)$ ideáljait, ha T tetszőleges test. (Lássuk be, hogy testben nincs nem triviális ideál.)
2.3-18.

a. Lássuk be, hogy a páros számok halmaza (P) az egész számok gyűrűjének részgyűrűjét, sőt ideálját alkotja.

b. Határozzuk meg a $\mathbb{Z}/P$ maradékosztály-gyűrűt.
2.3-19. Legyen $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z} \right\}$, és $I = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in 2\mathbb{Z} \right\}$

a. Mutassuk meg, hogy I ideál R-ben.

b. Hány elemű az R/I faktorgyűrű?
2.3-20. Jelöljük N-nel az R kommutatív gyűrűben a nullosztók és a 0 által alkotott halmazt.

a. Lehet-e, hogy N nem részgyűrű?

b. Lehet-e, hogy N részgyűrű, de nem ideál?

c. Bizonyítsuk be, hogy ha N ideál, akkor R/N nullosztómentes.

2.3.6. Homomorfizmus, izomorfizmus

2.3-21. Legyen $M = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a,b \in \mathbb{Z} \right\}$. Bizonyítsuk be, hogy az $(M,+,\cdot)$ struktúra izomorf az $E = \left(\left\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\right\},+,\cdot\right)$ gyűrűvel.
2.3-22. Izomorfak-e a következő gyűrűk?

$$G = \left(\left\{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\right\},+,\cdot\right) \quad \text{és} \quad K = \left(\left\{a+b\sqrt{3} \mid a,b \in \mathbb{Z}\right\},+,\cdot\right)$$

3. Példák és megoldások

3.1. Gráfok

3.1.1. Alapfogalmak

3.1-1. Van-e olyan 7 pontú egyszerű gráf, melyben a csúcsok foka rendre

a. 4, 4, 4, 3, 3, 3, 3;

b. 6, 3, 3, 2, 2, 2, 0;

c. 5, 5, 5, 4, 4, 2, 2;

d. 5, 5, 5, 2, 2, 2, 1;

e. amelyben minden pont foka különböző?

Útmutatás. Próbáljunk olyan gráfot felrajzolni, melyben a csúcsok fokai a megadott sorozatot alkotják. Ha több kísérlet után sem találunk ilyet, megpróbálhatjuk belátni, hogy nem is létezik.

a. Ha nem találtunk, akkor érdemes még egy kicsit próbálkozni...

b. Melyek a hatodfokú csúcs szomszédai? És a nulladfokúé (az izolált csúcsé)?

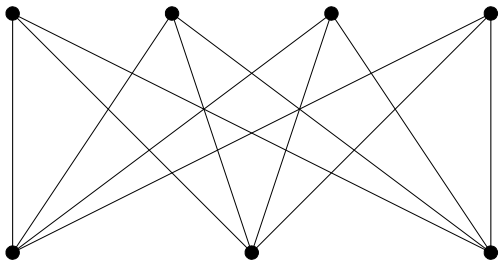
c. Használjuk a csúcsok fokainak összege és a gráf éleinek száma közötti összefüggést!

d. Egyszerű gráfról lévén szó, a három ötödfokú csúcs között csak három él haladhat. Legalább hány élnek kellene haladnia így az ötödfokú csúcsok és a maradék között?

e. Mi a lehető legnagyobb fok egy hétcsúcsú egyszerű gráfban? És a lehető legkisebb? ■

Megoldás. Csak az első esetben létezik a feltételeknek megfelelő gráf, mutatunk is egy ilyent. A többi négy esetben belátjuk, hogy nem létezik.

a. Egy lehetséges példa:



b. A hatodfokú csúcsot minden más csúccsal össze kellene kötni, márpedig van egy csúcs (a 0 fokú), amelyik izolált, vagyis nincs szomszédja. Ezért 6 és 0 egyszerre nem szerepelhet a sorozatban.

c. Minden véges gráfban igaz a következő: a fokok összege a gráf élszámának kétszerese, vagyis páros szám. Jelen esetben viszont 27 ez az összeg, ami páratlan, ezért ilyen gráf sem létezik.

d. A három darab ötödfokú csúcs között legfeljebb 3 él fut. Ezért a többi csúcsba is vezet ezekből legalább $15 - 2 \cdot 3 = 9$ él. De a többi csúcs fokainak összege csak 7, vagyis nem elég az ötödfokú csúcsok szabad „vegyértékeinek" lekötéséhez.

e. A lehetséges legnagyobb fok 6, a legkisebb 0. Ha minden csúcs foka különböző, akkor 0-tól 6-ig az összes egész szám szerepel is, márpedig láttuk (b. pont), hogy 0 és 6 együtt nem fordulhat elő. (Nemcsak 7 csúcs esetén, hanem általánosan is igaz, hogy legalább 2 csúcsú véges egyszerű gráf csúcsainak fokai nem lehetnek mind különbözők. A bizonyítás gond nélkül átvihető

az általános esetre.)

Megjegyzés. Ha nem kötjük ki, hogy a gráf egyszerű legyen, akkor párhuzamos és hurokélek segítségével minden olyan fokszámsorozat előállítható, melyben a fokok összege páros. ■

3.1-2. Legyen $n \in \mathbb{N}$, és $G = (V, E)$ egyszerű gráf, melynek legfeljebb $2n+1$ csúcsa van. Lássuk be, hogy ha minden $v \in V$ esetén $d(v) \geq n$, akkor G összefüggő. Igaz marad-e az állítás akkor is, ha csak azt tesszük fel, hogy minden csúcsra $d(v) \geq n-1$?

Útmutatás. Okoskodjunk indirekt módon: ha a gráf nem összefüggő, akkor legalább két komponense van. Adjunk felső becslést a kisebbnek a méretére. Jussunk ellentmondásra annak felhasználásával, hogy élek csak a komponenseken belül haladnak. A feladat második felében próbáljunk meg ellenpéldát találni. ■

Megoldás. Ha nem összefüggő a gráf, akkor van legalább két komponense. Mivel a csúcsok száma legfeljebb $2n+1$, van egy olyan komponens, amelyik legfeljebb n csúcsot tartalmaz. Ebben a komponensben minden csúcsból csak a komponensen belülre vezet él, vagyis összesen legfeljebb $n-1$ lehet a fokszáma. Ez ellentmond annak a feltételnek, mely szerint minden csúcs legalább n-edfokú. Ezzel beláttuk a feladat első felét.

A második kérdésben viszont csak $n-1$-et írunk elő, és ekkor van olyan gráf, mely nem összefüggő: egy két komponensből álló gráf, melynek mindkét komponense n pontú teljes gráf (az egyik lehet $n+1$ pontú is). ■

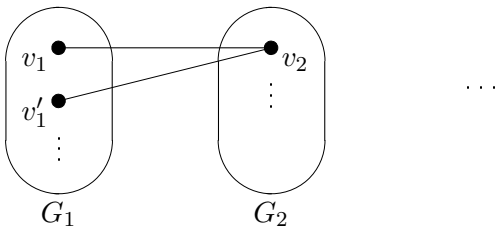
3.1-3. Legyen G egy véges egyszerű gráf, $\overline{G}$ a komplementere. Lássuk be, hogy G vagy $\overline{G}$ összefüggő.

Útmutatás. Tegyük fel, hogy G nem összefüggő. Mit mondhatunk két olyan pontról $\overline{G}$-ben, amelyek különböző komponensben vannak G-ben? ■

Megoldás. Ha G összefüggő, akkor nincs mit bizonyítanunk. Ha nem összefüggő, akkor az összefüggő komponensei legyenek

$$G_1 = (V_1, E_1),\ G_2 = (V_2, E_2),\ \ldots$$

Ha a gráf két csúcsa: v_1 és v_2 G-ben különböző komponensben voltak, akkor köztük G-ben nem megy él. De ekkor a komplementer definíciója szerint $\overline{G}$-ben össze vannak kötve éllel. Ha pedig v_1 és v_1' egy komponensben vannak G-ben, akkor bármely más komponensbeli csúcs (ilyen létezik, hiszen G nem összefüggő), pl. v_2 össze van kötve mindkettővel. Vagyis v_1, v_2, v_1' a köztük futó élekkel együtt egy 2 hosszúságú út. Ezzel beláttuk, hogy bármely két csúcs között megy egy legfeljebb 2 hosszú út $\overline{G}$-ben.



■

3.1-4. Igazoljuk, hogy ha egy véges egyszerű gráfban minden csúcs foka legalább k (ahol $k \geq 2$), akkor van a gráfban olyan kör, amely legalább $k+1$ pontot tartalmaz.

Útmutatás. Induljunk el az egyik csúcsból az egyik élen. Az új csúcsból menjünk tovább még nem érintett élen még nem érintett csúcsba, amíg tehetjük. Mikor akadunk el? Mik az utoljára érintett csúcs szomszédai? ■

Megoldás. Induljunk el az egyik csúcsból az egyik élen. Az új csúcsból menjünk tovább még nem érintett élen még nem érintett csúcsba, amíg tehetjük (a gráf véges, tehát előbb-utóbb elakadunk). Az így érintett csúcsok legyenek:

$$v_1, v_2, \ldots, v_s$$

Ha nem tudunk továbbmenni, akkor v_s minden szomszédja az előző $s-1$ csúcs valamelyike. Legyen ezek közül a legkisebb indexű v_t. A $v_t, v_{t+1}, \ldots, v_s, v_t$ pontsorozat kört alkot, hiszen a benne szereplő csúcsok v_t kivételével különbözőek, és az egymás után következő tagok szomszédosak a gráfban. A feladat feltételei szerint v_s legalább k-adfokú, ezért ez a kör legalább $k+1$ pontból áll, mert v_s és az összes szomszédja is szerepel benne.

Megjegyzés. A feladatot a leghosszabb út módszerével is megoldhatjuk. Leghosszabb úton maximális számú élt tartalmazó utat értünk. Véges gráfban mindenképpen van ilyen, de általában nem egyértelmű. Legyenek egy leghosszabb út csúcsai $v_1, v_2, \ldots, v_s$. Az út végpontja, v_s csak az úton előforduló többi csúccsal lehet összekötve (különben nem ez lenne a leghosszabb út). A továbbiakban a bizonyítás megegyezik az előbb mutatottal (ott is megeshet, de nem biztos, hogy egy leghosszabb utat találunk).

A feladat állítását a $k = 2$ speciális esetben érdemes külön is megfogalmazni. Eszerint, ha egy véges egyszerű gráf minden csúcsa legalább másodfokú, akkor van benne kör. (Azt nem kell mondani, hogy legalább három hosszú kör, hiszen egyszerű gráfban minden kör ilyen.) ■

3.1-5. Adjuk meg az összes 4, illetve 5 csúcsú egyszerű gráfot, amelyek izomorfak a komplementerükkel.

Útmutatás. Legyen G egy n pontú gráf, mely izomorf a komplementerével. A gráf egyik csúcsának fokát jelöljük d-vel. Ekkor ennek a csúcsnak a komplementerbeli fokszáma mennyi? Mi következik ebből a csúcsok fokszámsorozatára, ha tudjuk, hogy a gráf és komplementere izomorfak? ■

Megoldás. Legyen G egy n pontú véges gráf, $\overline{G}$ a komplementere, mely izomorf vele. Egy G-ben d-edfokú csúcs a komplementerben $n - d - 1$ fokú. Ha pedig a két gráf izomorf, akkor fokszámsorozatuk megegyezik. Így ha G csúcsainak a fokai sorrendben

$$d_1 \leq d_2 \leq \ldots \leq d_n,$$

akkor $\overline{G}$ csúcsainak fokai:

$$n - d_n - 1 \leq n - d_{n-1} - 1 \leq \ldots \leq n - d_1 - 1,$$

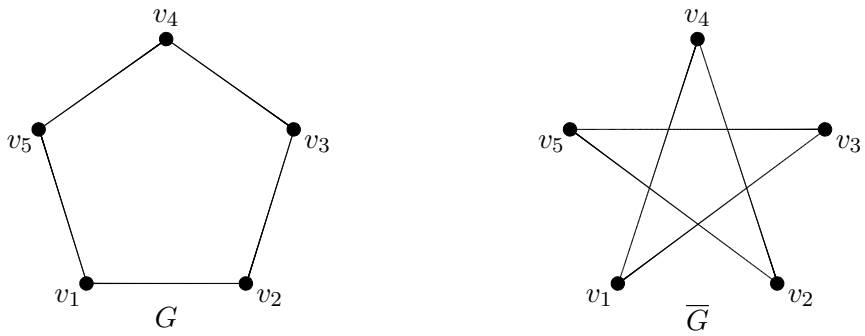
és ez a két sorozat ugyanaz. Vagyis $d_i + d_{n+1-i} = n - 1$. Tudjuk, hogy izolált és $n - 1$ fokú csúcs egyszerre nem fordulhat elő semmilyen egyszerű gráfban, ezért itt egyik sem lehetséges (mert az a másikkal együtt járna a fokszámokra kapott képlet alapján), tehát $d_i \geq 1$ és $d_i \leq n - 2$. Keressünk olyan nemcsökkenő sorozatot, mely teljesíti ezeket a feltételeket, és aztán vizsgáljuk meg, létezik-e gráf ezzel a fokszámsorozattal, majd végül azt, hogy izomorf-e a komplementerével.

Először az $n = 4$ esetet vesszük sorra. Itt vagy 1, vagy 2 a csúcsok foka, és minden elsőfokúhoz tartozik egy másodfokú. Az egyetlen lehetséges fokszámsorozat: $1, 1, 2, 2$. Egyszerű gráfban ez csak úgy fordulhat elő, ha az elsőfokú csúcsok nincsenek egymással összekötve, és ekkor a négy csúcs egy 3 hosszúságú utat alkot, aminek a komplementere is egy három hosszúságú út. Ez $n = 4$ esetén az egyetlen megoldás. Az alábbi ábrán a gráfot és a komplementerét láthatjuk.

Egy lehetséges izomorf leképezés a csúcsokon: $v_1 \mapsto v_2$, $v_2 \mapsto v_4$, $v_3 \mapsto v_1$, $v_4 \mapsto v_3$.

Áttérve az $n = 5$ esetre, itt a fokok 1 és 3 között vannak, és még azt tudjuk, hogy 1-esből és 3-asból ugyanannyi van. Három lehetséges fokszámsorozat adódik:

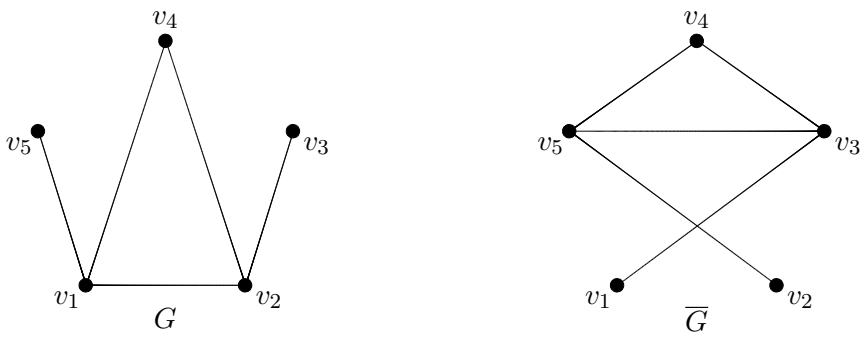
a. 2, 2, 2, 2, 2. Az egyetlen egyszerű gráf ezzel a fokszámsorozattal egy öt hosszúságú kör. Ennek a komplementere tehát önmaga:



Egy lehetséges izomorf leképezés a csúcsokon: $v_1 \mapsto v_1$, $v_2 \mapsto v_3$, $v_3 \mapsto v_5$, $v_4 \mapsto v_2$, $v_5 \mapsto v_4$.

b. 1, 2, 2, 2, 3. Ebben az esetben G elsőfokú pontja $\overline{G}$ harmadfokú pontja, és fordítva. Az izomorfizmus miatt ez a két pont vagy mindkét gráfban szomszédos, vagy egyikben sem. De a komplementer tulajdonsága miatt ez lehetetlen.

c. 1, 1, 2, 3, 3. Első- és harmadfokú csúcsok között összesen négy él megy a két gráfban. Mivel ezek a csúcsok a komplementerben is harmad- és elsőfokúak, az izomorfiából következik, hogy két-két él jut G-be és $\overline{G}$-be, mégpedig úgy, hogy nincs közös végpontjuk sem G-ben, sem $\overline{G}$-ben. Ez azt jelenti, hogy az elsőfokú csúcsok egy-egy harmadfokúhoz csatlakoznak. A maradék élek pedig egy háromszöget alkotnak. Ez a gráf valóban izomorf a komplementerével:



Egy lehetséges izomorf leképezés a csúcsokon: $v_1 \mapsto v_5$, $v_2 \mapsto v_3$, $v_3 \mapsto v_1$, $v_4 \mapsto v_4$, $v_5 \mapsto v_2$.

■

3.1-6. Hat versenyző körmérkőzést játszik. Bizonyítandó, hogy bármely időpontban van három olyan versenyző, akik már mind játszottak egymással, vagy három olyan, akik közül semelyik kettő nem játszott még.

Útmutatás. Fogalmazzuk át a feladatot a gráfelmélet nyelvére! Azt kell bizonyítani, hogy minden hatpontú egyszerű gráfban vagy a komplementerében van háromszög. Ennek belátásához válasszunk egy tetszőleges csúcsot, és G ill. $\overline{G}$ közül azt vizsgáljuk, amelyikben nagyobb a foka. ■

Megoldás. Valójában azt kell igazolni, hogy minden hatpontú egyszerű gráfban vagy a komplementerében van háromszög. Legyen v a gráf egy pontja.

Ennek G-beli és $\overline{G}$-beli foka összeadva 5. Ezért valamelyik fok legalább 3. Feltehetjük például, hogy G-ben van v-nek 3 szomszédja. Ha ezek közül bármelyik kettő össze van kötve, akkor v-vel együtt háromszöget alkotnak, ha pedig nincs, akkor ez a három szomszédja v-nek a komplementerben alkot háromszöget.

Megjegyzés. Ha csak öt pontja van a gráfnak, nem feltétlenül igaz az állítás, az ellenpélda az ötszög, mely önmaga komplementere.

A feladatot gyakran a következő ekvivalens formában fogalmazzák meg: Színezzük ki egy hatpontú teljes gráf éleit valahogyan két színnel. Igazoljuk, hogy minden színezésnél keletkezik egyszínű háromszög. A kérdés ebben a formában könnyen általánosítható több színre. Igaz például, hogy egy 17 pontú teljes gráf éleit *három* színnel megjelölve mindenképpen kapunk egyszínű háromszöget. További általánosítást jelenthet a háromszög helyett n-szög vagy tetszőleges gráf megkövetelése. A témakörbe tartozó kérdések spektruma igen széles, és Ramsey-féle problémáknak hívják őket. ■

3.1-7. Jelöljük egy véges fagráf elsőfokú pontjainak számát f_1-gyel, a 2-nél nagyobb fokú pontjainak számát pedig c-vel. Bizonyítsuk be, hogy ha a pontok száma legalább 2, akkor $f_1 \geq c + 2$.

Útmutatás. Többféleképpen is célhoz érhetünk. Első megoldásként használhatjuk a csúcsok foka és az élek száma közötti összefüggést és azt, hogy n pontú fa éleinek száma $n - 1$.

Másrészről használhatjuk azt az állítást, mely szerint ha egy véges gráfban minden pont legalább másodfokú, akkor van a gráfban kör. Átfogalmazva: véges körmentes gráfban (=véges erdőben) van olyan csúcs, melynek foka legfeljebb egy. Ha még összefüggő is az erdő (fa), akkor van elsőfokú csúcs. Ezt az elsőfokú csúcsot elhagyva teljes indukciót alkalmazhatunk. ■

Megoldás. *Első megoldás.* Jelöljük a k-adfokú csúcsok számát f_k-val, a legnagyobb fokot d-vel, a gráf csúcsainak számát n-nel. A gráf csúcsainak összfokszáma az élek számának kétszerese, ez fagráfban $2(n-1)$. Az összfokszámot

számoljuk ki úgy, hogy a csúcsokat fokszám szerint csoportosítjuk:

$$\sum_{i=1}^{d}(f_i \cdot i) = f_1 + 2f_2 + \ldots + df_d = 2(n-1).$$

Másrészt összesen n csúcs van:

$$\sum_{i=1}^{d} f_i = f_1 + f_2 + \ldots + f_d = n.$$

Utóbbi egyenlet kétszereséből az elsőt kivonva:

$$\sum_{i=1}^{d}(2-i)f_i = f_1 - f_3 - 2f_4 - \ldots - (d-2)f_d = 2$$

A negatív előjelű tagokat a másik oldalra rendezve:

$$f_1 = 2 + f_3 + 2f_4 + \ldots \geq 2 + f_3 + f_4 + \ldots = c + 2,$$

hiszen így definiáltuk c-t.

Második megoldás. A gráf csúcsainak n száma szerinti teljes indukcióval bizonyítunk. Ha $n = 2$, akkor igaz az állítás ($2 \geq 2$). Legyen most $n > 2$, és tegyük fel, hogy minden $n-1$ pontú fában igaz az állítás. Használjuk fel, hogy minden véges fának van elsőfokú pontja. Egy ilyen pontot elhagyva egy $n-1$ pontú G' fát kapunk, melyre igaz az állítás: $f_1' \geq c' + 2$. Ha visszavesszük az elhagyott csúcsot, akkor ha

• a szomszéd G'-ben elsőfokú, akkor $f_1 = f_1'$ és $c = c'$, tehát igaz maradt az állítás,

• a szomszéd G'-ben másodfokú volt, akkor $f_1 = f_1' + 1$ és $c = c' + 1$, az egyenlőtlenség mindkét oldalát 1-gyel növeltük,

• a szomszéd G'-ben legalább harmadfokú, akkor $f_1 = f_1' + 1$ és $c = c'$, tehát az egyenlőtlenség „még inkább" igaz lett.

Mindhárom esetben működik az indukció, az állítást beláttuk.

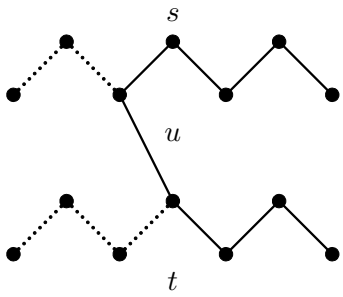
Megjegyzés. Mindkét bizonyításból kiolvasható, hogy az egyenlőtlenség akkor és csak akkor éles ($f_1 = c + 2$), ha a gráfnak nincs 3-nál magasabb fokú csúcsa. ■

3.1-8. Igazoljuk, hogy egy összefüggő véges gráfban bármely két leghosszabb útnak van közös pontja.

Útmutatás. Indirekt módon okoskodjunk: tegyük fel, hogy van két olyan leghosszabb út, amelyeknek a ponthalmaza diszjunkt, és jussunk ellentmondásra annak felhasználásával, hogy a gráf összefüggő. ■

Megoldás. Tegyük fel, hogy van két leghosszabb út (s és t), melyeknek nincs közös pontja. Legyen a hosszuk m. A két út tetszőleges két pontja között vezet út, tekintsük egy ilyen útnak s és t közé eső olyan darabját (u), aminek egyik végpontja az s-en, másik a t-n van, és (esetleges) belső pontjai egyiken sincsenek rajta. Ennek hossza legalább 1. Készítsünk egy újabb utat felhasználva s és t hosszabbik (legalább félútnyi) részét, középen kiegészítve u-val, így legalább $\lceil \frac{m}{2} \rceil + \lceil \frac{m}{2} \rceil + 1$ hosszú utat kapnánk, ami hosszabb s-nél és t-nél is. Így ellentmondásra jutottunk, tehát az indirekt feltevés helytelen.

Az ábrán az indirekt feltevésből következő lehetetlen állapotokat tekinthetjük meg. Itt $m = 6$. A folytonos vonallal rajzolt út hosszabb lenne, mint a feltételezett leghosszabb utak.



■

3.1-9. Igazoljuk, hogy véges fában az összes leghosszabb út egy ponton megy át.

Útmutatás. Válasszunk ki egy leghosszabb utat tetszés szerint, és próbáljuk meg belátni, hogy van olyan csúcsa, mely minden más leghosszabb úton is rajta van. ■

Megoldás. Legyen s_1 egy leghosszabb út, és $v_1, v_2, \ldots, v_m$ a pontsorozata. Legyen $w = v_{\lfloor \frac{m}{2} \rfloor}$, vagyis az út középső csúcsa (a két középső csúcs közül az egyik, ha m páros). Be fogjuk látni, hogy a fa minden leghosszabb útja tartalmazza w-t. Ehhez használjuk fel, hogy bármely két útnak van közös pontja. Most indirekt módon tegyük fel, hogy van egy másik leghosszabb út (s_2), melynek csúcsai $u_1, u_2, \ldots, u_m$, és ezek között nem szerepel w. Legyen k a legkisebb olyan index, amire u_k eleme s_1-nek, és l a legnagyobb ilyen. Mivel egy fában bármely két csúcs között pontosan egy út halad, ezért u_k és u_l között minden csúcs szerepel mindkét leghosszabb úton. Indirekt feltevésünk szerint ez a közös szakasz nem tartalmazza w-t. Emiatt két lehetőség van:

- u_l az s_1-nek w-nél kisebb indexű tagja, mondjuk $u_l = v_j$, ahol $j < \lfloor \frac{m}{2} \rfloor$. Ekkor a két út hosszabbik felét u_l-nél összefűzve egy m-nél több csúcsból álló utat kapnánk, ami ellentmondás. Ennek az útnak a pontjai u_1, u_2, $\ldots$, $u_l(= v_j)$, v_{j+1}, $\ldots$, v_m, ha $l > \lfloor \frac{m}{2} \rfloor$, különben pedig u_m, u_{m-1}, $\ldots$, $u_l(= v_j)$, v_{j+1}, $\ldots$, v_m.

- $u_k = v_j$, ahol $j > \lfloor \frac{m}{2} \rfloor$. Ekkor is több mint m pontos utat kapnánk, ha a két út hosszabbik felét kötjük össze. A csúcsok halmaza u_1, u_2, $\ldots$, $u_k(= v_j)$, v_{j-1}, $\ldots$, v_1, ha $k > \lfloor \frac{m}{2} \rfloor$, és u_m, u_{m-1}, $\ldots$, $u_k(= v_j)$, v_{j-1}, $\ldots$, v_1 különben.

Mindkét esetben ellentmondásra vezet az indirekt feltevés, beláttuk tehát, hogy w az összes leghosszabb útban szerepel.

Megjegyzés. A megoldásból az is látszik, hogy ha a leghosszabb utak hossza páratlan (m páros), akkor nemcsak egy, hanem két olyan szomszédos csúcs is van, mely minden leghosszabb útban szerepel, természetesen a köztük futó éllel együtt. ■

3.1-10. Legyen n egynél nagyobb pozitív egész.

a. Legfeljebb hány szeparáló él van egy n pontú gráfban? Adjuk meg az olyan gráfokat, amelyekben pontosan ennyi szeparáló él van.

b. Legfeljebb hány szeparáló csúcs van egy n pontú gráfban? Adjuk meg az olyan gráfokat, amelyekben pontosan ennyi szeparáló csúcs van.

Útmutatás. Egy él (csúcs) szeparáló, ha elhagyásával olyan gráfot kapunk, melyben van két, eredetileg úttal összekötött csúcs, melyek külön komponensbe esnek.

a. Tehát a szeparáló éleket egymás után elhagyva a gráfból, a komponensek száma minden lépésben nő. Hány lépésben folytathatjuk ekkor az élek törlését, ha a kiinduló állapotban legalább egy komponensünk, a végén pedig legfeljebb n komponensük van? Keressünk olyan gráfot, melyben minden él szeparál.

b. A csúcsoknál úgy tudunk felső becslést adni, ha megfigyeljük, hogy egy leghosszabb út két végpontja sosem szeparáló csúcs. ■

Megoldás.

a. Egy szeparáló él elhagyásával nő a komponensek száma. Ezért ha sorra hagyjuk el egy gráf szeparáló éleit, még ha összefüggő gráfból indultunk is, legkésőbb $n-1$ lépés után véget ér a procedúra, és már csak különálló pontjaink lehetnek. Ezért legfeljebb $n-1$ szeparáló él van. Van is olyan gráf, amelyben van pontosan ennyi, mégpedig egy n-pontú fa (olyan gráf kell, ami összefüggő és $n-1$ élű). Ebben minden él szeparáló, hiszen két pont között csak egy út megy, és az élek száma pontosan $n-1$.

b. Egy leghosszabb út két végpontja nem lehet szeparáló, hiszen minden szomszédja az úton van. Egy n pontú gráfban (kivéve az egy élt sem tartalmazó triviális esetet) viszont mindig van legalább egy leghosszabb út, két nem szeparáló végponttal. Ezért legfeljebb $n-2$ szeparáló csúcs van. Ez az érték egy n pontú úttal el is érhető.

■

3.1.2. Euler-gráf

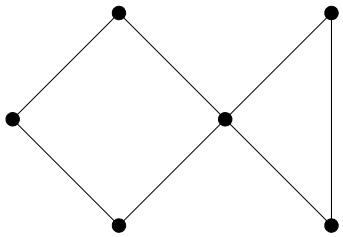
3.1-11. Van-e olyan Euler-gráf, melynek páros számú pontja és páratlan számú éle van?

Útmutatás. Ahhoz, hogy egy véges gráf Euler-gráf legyen, két dolog szükséges:

- a gráfnak összefüggőnek kell lennie,
- minden csúcsának a foka legyen páros.

Próbálkozzunk, már viszonylag kis számú csúcs esetén található ilyen gráf. ■

Megoldás. Van ilyen gráf, pl. a következő, mely egy négyszöget és egy háromszöget tartalmaz az egyik csúcsuknál összenőve (6 csúcs, 7 él).



Ha nem akarunk egyszerű gráfot, akkor a következő gráf is jó: két csúcs párhuzamos élekkel összekötve, és az egyik körül még egy hurokél (2 csúcs, 3 él). ■

3.1-12. Igazoljuk, hogy ha egy hurokélt nem tartalmazó véges gráf minden pontjának foka 4, akkor élei megszínezhetők piros és kék színekkel úgy, hogy minden szögponthoz két piros és két kék él illeszkedjen.

Útmutatás. Próbáljuk meg először azt az esetet belátni, amikor a gráf összefüggő. Ekkor a gráf Euler-gráf, vagyis van benne olyan zárt vonal, mely az összes élt pontosan egyszer tartalmazza. Hogyan tudnánk ennek a vonalnak a segítségével egy olyan színezési eljárást megadni, ami garantálja, hogy minden csúcsra két-két piros és kék él illeszkedjen? Ha megvan az eljárás, még marad egy kis bizonyítanivaló (segítség: miért nem másodfokú csúcsok szerepelnek a példában?). Végül a nem összefüggő esetre való áttérés triviális. ■

Megoldás. Tegyük fel először, hogy a gráf összefüggő. Ekkor van benne Euler-vonal, hiszen minden csúcsának páros a fokszáma. Induljunk el egy tetszőleges v csúcsból, és járjuk körbe az Euler-vonalat úgy, hogy az érintett éleket felváltva pirosra és kékre színezzük. Végül visszaérkezünk v-be. Minden v-től különböző csúcson kétszer haladtunk át, beérkezéskor és távozáskor egy-egy élt pirosra és kékre színezve, ezeknél a csúcsoknál jól színeztünk. Egyedül v lehet kérdéses. Itt is áthaladtunk egyszer menet közben, tehát csak az kell, hogy az Euler-vonal legelső és legutolsó éle ellentétes színű legyen. Ehhez pontosan az kell, hogy az Euler-vonalnak páros sok éle legyen, de mivel a vonal a gráf összes élét tartalmazza, ezért a gráf élszámának paritása érdekel minket.

Az élszám a csúcsok összfokszámának fele, de mivel minden fok 4, ezért az összfokszám osztható 4-gyel, vagyis a fele, az élek száma páros. Ezzel beláttuk az összefüggő gráf esetét.

Ha a gráf több komponensből áll, akkor minden komponense egy Euler-gráf. A fenti színezést komponensenként kell elvégeznünk.

Megjegyzés. Ha csak azt kötjük ki, hogy minden fok legyen páros, és azt várjuk el, hogy minden csúcsban az élek fele-fele arányban legyenek kiszínezve, akkor még azt is meg kell követelnünk, hogy komponensenként páros sok él legyen a gráfban. Például egy ötszög – bár minden pontja másodfokú, és van Euler-vonala – nem színezhető ki ilyen módon. ■

3.1-13. Legyen a G véges összefüggő gráfban $2k$ darab páratlan fokú pont. Igazoljuk, hogy a gráf élhalmaza előáll k darab éldiszjunkt vonal élhalmazának egyesítéseként.

Útmutatás. Használjuk a *zárt* Euler-vonal létezését leíró állítást. Milyen trükkel tudjuk elérni, hogy az a tétel itt is alkalmazható legyen? ■

Megoldás. Állítsuk k darab párba a páratlan fokú csúcsokat, és az egy párban levők közé húzzunk be egy élt (ez esetleg párhuzamos él lesz, ha már eredetileg is össze voltak kötve). Ekkor minden fok páros, vagyis egy Euler-gráfot kapunk. Ebben a gráfban van tehát egy zárt Euler vonal, ami persze a plusz-éleket is tartalmazza. Ha most töröljük a k darab élt, akkor a vonal k darab éldiszjunkt nyílt vonalra esik szét. (Egy zárt vonal k élének törlésével *legfeljebb* k részre esik, de most pontosan k darab keletkezik, mert az elhagyott élek közül semelyik kettő nem szomszédos.) Ezt az előállítást kerestük.

Megjegyzés. Nem működik a következő indukciós gondolatmenet: induljunk el egy páratlan fokú csúcsból, és haladjunk mindig még fel nem használt éleken. Csak akkor akadunk el, ha egy csúcsban már minden élt felhasználtunk, és ez csak egy páratlan fokú csúcsban fordulhat elő, hiszen áthaladáskor kettő él „fogy el". Találtunk tehát egy nyílt vonalat. Hagyjuk el ennek az éleit, így egy olyan gráfot kapunk, melyben kettővel kevesebb a páratlan fokú csúcs. Alkalmazhatjuk tehát az indukciót. Ám ez nem igaz minden esetben! A prob-

léma ott van, hogy a kapott gráf nem biztos, hogy összefüggő marad! ■

3.1.3. Hamilton-út, Hamilton-kör

3.1-14. Mutassuk meg, hogy egy körmérkőzéses pingpongverseny résztvevői sorba állíthatók úgy, hogy mindenki legyőzte a közvetlenül mögötte állót. (Azt nem követeljük meg, hogy az összes mögötte állót le kellett volna győznie.)

Útmutatás. Egy pingpongmeccs végeredménye nem lehet döntetlen, tehát a feladatot átfogalmazhatjuk a gráfok nyelvére. A játékosok legyenek egy irányított gráf csúcsai, és a győztes csúcsból mutasson nyíl a vesztes felé. Bármely két csúcs között van pontosan egy irányított él. A következőt kell igazolni: Bárhogy készítünk egy teljes gráfból irányított gráfot, mindig lesz az utóbbiban irányított Hamilton-út. Ezt pedig beláthatjuk a csúcsok száma szerinti indukcióval. ■

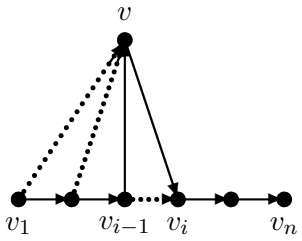
Megoldás. A körmérkőzésből készítsünk irányított gráfot. A játékosok legyenek az irányított gráf csúcsai, és a győztes csúcsból mutasson nyíl a vesztes felé. Bármely két csúcs között van pontosan egy irányított él. Azt kell belátnunk, hogy bármilyen irányba mutatnak is a nyilak, mindig lesz a gráfban irányított Hamilton-út. Ezt a csúcsok n száma szerinti indukcióval látjuk be.

Az $n = 1$ eset triviális. Ha feltesszük, hogy n-re már beláttuk, $n+1$-re járjunk el a következőképpen: Hagyjuk el valamelyik pontot (v) a gráfból, ekkor egy n-pontú gráfot kapunk, melyre működik az indukció, tehát van benne Hamilton-út, mondjuk $v_1, v_2, \ldots, v_n$ ebben a sorrendben egy irányított út. Az $(n+1)$-edik csúcs többiekhez való viszonya alapján három esetet különböztetünk meg:

• Ha a v és v_1 közötti él v_1-be mutat, akkor $v, v_1, v_2, \ldots, v_n$ egy Hamilton-út.

• Ha a v és v_n közötti él v-be mutat, akkor $v_1, v_2, \ldots, v_n, v$ egy Hamilton-út.

• Ha a fenti két eset egyike sem teljesül, akkor legyen i a legkisebb olyan index, melyre v és v_i között a nyíl v_i-be mutat. Ilyen mindenképpen van, mert v_n-be megy v-ből nyíl. Ekkor $v_1, v_2, \ldots, v_{i-1}, v, v_i, v_{i+1}, \ldots, v_n$ egy Hamilton-út. Az ábrán folytonos vonallal látható ez az út.



Az indukciós lépés mindhárom esetben működik. ■

3.1-15. Legyen k pozitív egész. Igazoljuk a következőket:

• **Ha egy véges összefüggő gráfban van k olyan csúcs, melyek elhagyásával a gráf több mint k komponensre esik szét, akkor a gráfban nem találhatunk Hamilton-kört.**

• **Ha egy véges összefüggő gráfban van k olyan csúcs, melyek elhagyásával a gráf több mint $k+1$ komponensre esik szét, akkor a gráfban nincs Hamilton-út.**

Útmutatás. Legfeljebb hány részre esik szét egy út (kör), ha töröljük k pontját? ■

Megoldás. Legyen $G = (V, E)$ egy véges gráf, $W \subseteq V$, $E' \subseteq E$. Ha a V ponthalmazából a W halmaz elemeit elhagyjuk, és a kapott gráfnak l komponense van, akkor a (V, E') gráfból a W csúcsok törlésével kapott gráfnak is legalább l komponense van. Ez nyilvánvaló, hiszen mindkét kapott gráf csúcshalmaza $V - W$, és az utóbbi élhalmaza az előbbiének része.

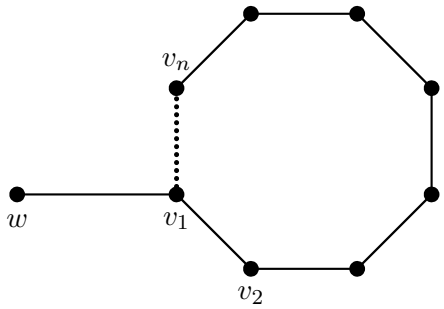
Vagyis, tegyük fel, hogy egy gráf tartalmaz Hamilton-utat (-kört). Ha a gráf bizonyos k csúcsának elhagyásával l komponensre esik szét, akkor a Hamilton-útnak (-körnek) is legalább ennyi komponensre kell szétesnie. Márpedig, egy útból k pont elhagyásával legfeljebb $k+1$, egy körből pedig legfeljebb k komponens keletkezhet. Ezért, ha a gráf ennél több komponensre esik szét, nem lehet benne Hamilton-út illetve -kör. Ezt kellett belátnunk. ■

3.1-16. Bizonyítsuk be, hogy ha egy véges összefüggő gráf K köré-

ből egy élt eltörölve a gráf egy leghosszabb útját kapjuk, akkor K Hamilton-köre a gráfnak.

Útmutatás. Indirekt módon gondolkodjunk. Tegyük fel, hogy K nem Hamilton-kör. Használjuk fel, hogy a gráf összefüggő, és mutassunk egy utat, melyben több pont szerepel mint K-ban. ■

Megoldás. Jelöljük K csúcsait $v_1, v_2, \ldots, v_n$-nel. Ha K-ból törlünk egy élt, akkor n csúcsú utat kapunk. Ha ez egy leghosszabb út, akkor minden útnak legfeljebb ennyi csúcsa lehet. Tegyük fel indirekte, hogy K nem Hamilton-kör. Ekkor van olyan pont a gráfban, mely nem szerepel K-ban. De ekkor az összefüggőség miatt létezik olyan él, amely egy K-beli (feltehetjük, hogy ez v_1) és egy nem K-beli (w) csúcsot köt össze. Ekkor $w, v_1, v_2, \ldots, v_n$ egy $n+1$ csúcsból álló út, ez ellentmondás. Az ábrán ezt a feltételeknek ellentmondó hosszú utat láthatjuk.



■

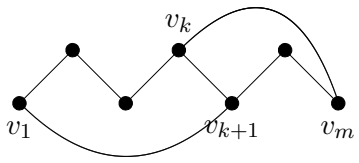
3.1-17. Legyen $n \geq 3$ pozitív egész, és G egy n pontú egyszerű összefüggő gráf. Igazoljuk, hogy ha G minden csúcsának foka legalább $\frac{n}{2}$, akkor G-nek van Hamilton-köre.

Útmutatás. Próbáljuk meg belátni, hogy egy leghosszabb úthoz mindig találhatunk kört, mely ugyanazokat a csúcsokat tartalmazza. Majd használjuk fel az előző feladat állítását. ■

Megoldás. Legyen $v_1, v_2, \ldots, v_m$ a gráf egy leghosszabb útjának a pontsorozata. Be fogjuk látni, hogy van a gráfban m hosszú kör, melyet K-val jelölünk.

Ekkor K egy élének törlésével a gráf egy leghosszabb útját kapjuk, ami a 16. feladat alapján azt jelenti, hogy K Hamilton-kör, és készen leszünk.

A leghosszabb úton van v_1 és v_m összes szomszédja. A v_1 szomszédai legyenek $v_{i_1}, v_{i_2}, \ldots, v_{i_d}$, v_m-é pedig $v_{j_1}, v_{j_2}, \ldots, v_{j_e}$, ahol $d, e \geq n/2$. Az $i_1 - 1, i_2 - 1, \ldots, i_d - 1$ illetve a $j_1, j_2, \ldots, j_e$ számok mindegyike 1 és $m-1$ közötti. Mivel $d + e \geq n \geq m$, ezért a skatulyaelv alapján van olyan x és y, hogy $i_x - 1 = j_y$. Ez szemléletesen azt jelenti, hogy v_1-nek van olyan szomszédja, mely v_m egy szomszédja után következik az úton. Mondjuk v_1 és v_{k+1}, illetve v_m és v_k között megy él. Az ábra ezt a helyzetet mutatja. Az egyszerűség kedvéért csak az utat és a most említett éleket rajzoltuk be.



Ekkor $v_1, v_2, \ldots, v_k, v_m, v_{m-1}, \ldots, v_{k+1}, v_1$ egy m hosszú kör, és nekünk pontosan ilyenre volt szükségünk. Ezzel az állítást beláttuk. ■

3.1.4. Síkbeli gráfok

3.1-18.

a. Bizonyítsuk be, hogy ha egy G gráf pontszáma legalább 11, akkor vagy G, vagy G komplementere nem síkgráf.

b. Adjunk meg 8 pontú síkgráfot úgy, hogy komplementere is síkgráf legyen.

Útmutatás.

a. Használjuk a síkgráf csúcsainak és éleinek számára vonatkozó becslést.

b. A fenti becslés annál élesebb, minél több háromszög van a síkba rajzolt gráfban. Keressünk olyan 8-pontú síkgráfot, melyben sok a háromszög alakú tartomány. Minél több háromszögünk van, annál több éle van a gráf-

nak, a komplementerének így kevesebb, és akkor nagyobb az esély arra, hogy a komplementer is síkba rajzolható. ■

Megoldás.

a. Egy n pontú teljes gráf éleinek száma $\binom{n}{2}$. Ennyi éle van egy n pontú egyszerű gráfnak és a komplementerének együttvéve. Másrészről, egy n pontú síkgráfnak legfeljebb $3n-6$ éle lehet. Tehát ha egy gráf és a komplementere is síkba rajzolható, akkor $2(3n-6) \geq \binom{n}{2}$. Kifejtve:

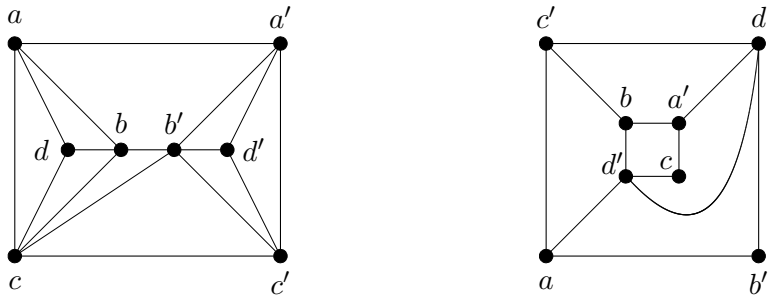
$$\begin{aligned} 12n - 24 &\geq n^2 - n \\ 0 &\geq n^2 - 13n + 24 = \frac{1}{4}\left((2n-13)^2 - 73\right) \end{aligned}$$

Mindez nem teljesül, ha $n \geq 11$. Az $n^2 - 13n + 24$ kifejezés előjelének vizsgálatát a következőképpen is elvégezhetjük. A másodfokú kifejezés két gyöke

$$n_{1,2} = \frac{13 \pm \sqrt{13^2 - 4 \cdot 24}}{2} = \frac{13 \pm \sqrt{73}}{2}$$

melynek közelítő megoldása $n_1 \approx 10{,}77$ és $n_2 \approx 2{,}23$. A kifejezés értéke a két gyök közötti zárt intervallumon kívül pozitív, vagyis minden olyan egész számra is, melyre $n \geq 11$.

b. Az ábrán egy lehetséges gráf és komplementere látható.



■

3.1-19. Hány éle van egy n pontú összefüggő síkgráfnak, ha minden tartománya (a külső is)

a. háromszög,

b. négyszög?

Útmutatás. Használjuk az Euler-féle képletet, mely a tartományok, a csúcsok és az élek számára ad összefüggést. ■

Megoldás. Az Euler-képlet szerint, ha egy síkgráf tartományainak száma t, éleié e, csúcsaié pedig n, akkor

$$n + t = e + 2.$$

Ha még azt is tudjuk, hogy minden tartományt ugyanannyi él határol, akkor t és e között további összefüggést fedezhetünk fel:

a. Ha minden tartományt három él zár körül, akkor $e = \frac{3}{2}t$, mert ha az éleket tartományonként számoljuk össze, akkor minden élt kétszer számolunk, hiszen két tartományt választ el. (A külső tartományt ezért kell szintén számba venni). Az Euler-képlet most tehát így szól:

$$t + n = \frac{2}{3}e + n = e + 2.$$

Átrendezve $e = 3n - 6$.

b. Itt azt kapjuk, hogy $e = \frac{4}{2}t = 2t$. Ezért

$$t + n = \frac{1}{2}e + n = e + 2,$$

és ebből $e = 2n - 4$.

Megjegyzés. A képletek helyességét leellenőrizhetjük pl. a szabályos testek hálóin: A tetraéder ($6 = 3 \cdot 4 - 6$), az oktaéder ($12 = 3 \cdot 6 - 6$), az ikozaéder ($30 = 3 \cdot 12 - 6$), illetve a kocka ($12 = 2 \cdot 8 - 4$) esete alátámasztja számításaink helyességét. ■

3.1-20. Hány éle lehet legfeljebb egy síkba rajzolható, n pontú egyszerű páros gráfnak?

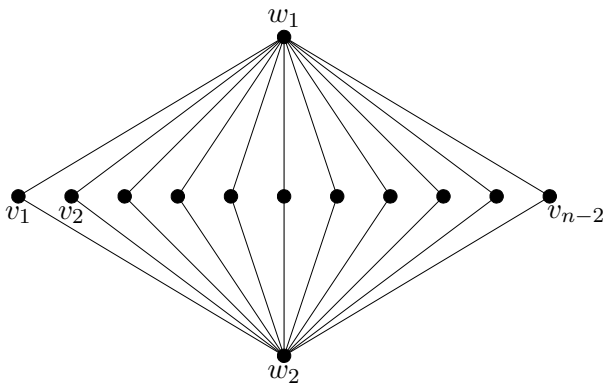
Útmutatás. Használjuk az Euler-képletet. Gondoljunk még arra, hogy páros gráfban minden kör hossza páros, márpedig egy tartományt határoló élek kört alkotnak. ■

Megoldás. Egy egyszerű páros gráfban minden kör hossza legalább 4, hiszen egyszerű gráfokra ez a hossz legább 3, és 3 hosszú kör páros gráfban nem lehet. Ezért minden tartományt legalább 4 él határol. Másrészt minden él két tartomány határán szerepel. Ezért az élek e és a tartományok t számára fennáll: $e \geq \frac{4}{2}t = 2t$. Az Euler-képletet alkalmazva a gráfra:

$$e + 2 = n + t \leq n + \frac{1}{2}e.$$

Átrendezve kapjuk, hogy $e \leq 2n - 4$. Legfeljebb ennyi éle van egy n pontú egyszerű páros gráfnak.

Be kellene még látni, hogy ez a becslés éles, vagyis létezik olyan páros gráf, melynek pont ennyi éle van. Ehhez tekintsünk egy olyan gráfot, melyben $n-2$ pont helyezkedik el vízszintesen egymás mellett, és egy-egy pont felettük, illetve alattuk. Kössük össze a középső pontok mindegyikét a felső és alsó pontokkal. Ekkor a behúzott élek nem keresztezik egymást, és számuk $2n-4$. A csúcsokat pedig két diszjunkt halmazba sorolhatjuk úgy, hogy a halmazokon belül nem megy él, ezért a gráf páros. Az egyik halmaz kételemű, és a felső ill. alsó pontot (w_1 és w_2) tartalmazza, a másik pedig a vízszintesen elhelyezkedő $n-2$ pontból áll ($v_1, v_2, \ldots, v_{n-2}$). Egy ilyen gráfot láthatunk az ábrán.



■

3.2. Csoportok

3.2.1. Félcsoport, csoport

3.2-1. Vizsgáljuk meg az alábbi példákban, hogy a művelet vajon művelet-e az adott halmazon, s ha igen, akkor a halmaz a művelettel félcsoport-e, csoport-e.

a. $(\mathbb{Z}, \circ)$, **ha** $a \circ b = (a+b)/2 \quad (a, b \in \mathbb{Z})$;

b. $(\mathbb{Q}, \circ)$, **ha** $a \circ b = (a+b)/2 \quad (a, b \in \mathbb{Q})$;

c. $(A, \circ)$, **ha** A **a** $[0,1]$ **intervallumon értelmezett valós függvények halmaza és** $(f \circ g)(x) = \max(f(x), g(x))$;

d. $(\mathbb{R}$, **osztás);**

e. $(\mathbb{R} \setminus \{0\}$, **osztás);**

Megoldás.

a. $(\mathbb{Z}, \circ)$, ha $a \circ b = (a+b)/2 \quad (a, b \in \mathbb{Z})$ esetén $\circ$ nem művelet a halmazon, hiszen két egész szám számtani közepe nem feltétlenül egész szám. Például $3 \circ 2 = \frac{5}{2} \notin \mathbb{Z}$. Így $(\mathbb{Z}, \circ)$ nem algebrai struktúra.

b. $(\mathbb{Q}, \circ)$, ha $a \circ b = (a+b)/2 \quad (a, b \in \mathbb{Q})$ esetén $\circ$ művelet. Nem asszociatív, mert egyrészt

$$(a \circ b) \circ c = \frac{\frac{a+b}{2} + c}{2} = \frac{a+b+2c}{4},$$

másrészt

$$a \circ (b \circ c) = \frac{a + \frac{b+c}{2}}{2} = \frac{2a+b+c}{4}.$$

Ennek a két kifejezésnek az értéke nem mindig egyezik meg, például legyen $a = b = 1,\ c = 0$. Ekkor

$$(a \circ b) \circ c = \frac{1}{2} \neq \frac{3}{4} = a \circ (b \circ c).$$

Így a struktúra nem félcsoport.

c. $(A, \circ)$, ha A a $[0,1]$ intervallumon értelmezett valós függvények halmaza és $(f \circ g)(x) = \max(f(x), g(x))$ esetén a $\circ$ művelet a halmazon. Asszociatív,

tehát $(f \circ g) \circ h = f \circ (g \circ h) \quad f, g, h \in A$ esetén. Kommutatív, de nincs egységelem, így a struktúra kommutatív félcsoport.

d. ($\mathbb{R}$, osztás) esetén az osztás nem művelet (a nevezőben nem szerepelhet a 0).

e. ($\mathbb{R} \setminus \{0\}$, osztás) esetén az osztás művelet. Nem asszociatív. Egyrészt

$$(a/b)/c = \frac{\frac{a}{b}}{c} = \frac{a}{b \cdot c},$$

másrészt

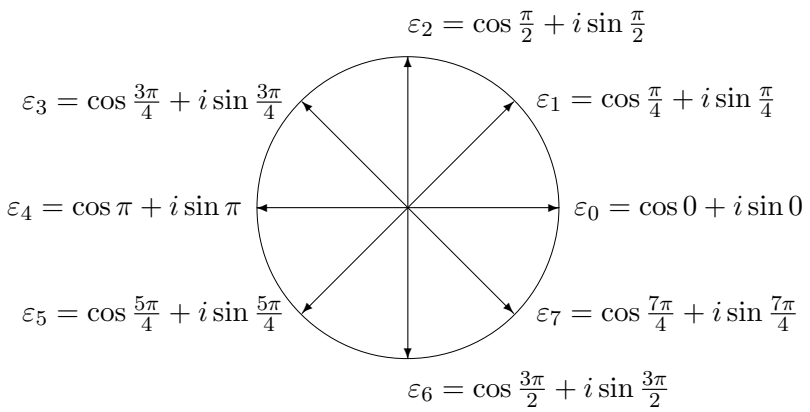
$$a/(b/c) = \frac{a}{\frac{b}{c}} = \frac{a \cdot c}{b}.$$

Ez a két kifejezés nem mindig veszi fel ugyanazt az értéket. Legyen például $a = 1,\ b = 2,\ c = 2$. Ekkor az első kifejezés értéke $\frac{1}{4}$, a másodiké pedig 1. Nem kommutatív a struktúra, $\frac{a}{b}$ értéke nem minden esetben egyezik meg $\frac{b}{a}$ értékével. Mivel a művelet nem asszociatív, így a stuktúra nem félcsoport, és természetesen nem is csoport. ■

3.2-2. Lássuk be, hogy a 8-adik komplex egységgyökök a szorzással csoportot alkotnak.

Megoldás. A 8-adik komplex egységgyökök (lásd az 1. ábrát):

$$\varepsilon_k = \cos k\frac{2\pi}{8} + i \sin k\frac{2\pi}{8}, \quad 0 \leq k \leq 7 \qquad (*)$$



1. ábra. A 8-adik komplex egységgyökök

Belátjuk, hogy (*) csoportot alkot a szorzással.

I. Bármelyik két 8-adik egységgyök szorzata is nyolcadik egységgyök, s így a szorzás *művelet* a halmazon. Ugyanis $\varepsilon_k \cdot \varepsilon_m = \varepsilon_{k+m}$, és ha $k+m$-et modulo 8 tekintjük, akkor (*) valamelyik elemét kapjuk.

II. Az asszociativitás teljesül. Ha a, b, és c tetszőleges elemei a halmaznak, akkor

$$(a \cdot b) \cdot c = a \cdot (b \cdot c).$$

Ez most fennáll, ugyanis a halmaz a komplex számok részhalmazát képezi, és a komplex számokon a szorzás asszociatív, hiszen testet alkotnak az összeadás és szorzás műveletekre.

III. Egységelem az 1, mert $\varepsilon_k \cdot 1 = 1 \cdot \varepsilon_k = \varepsilon_k$.

IV. Mindegyik elemnek van inverze az 1-re vonatkozóan, mert az $\varepsilon_k \cdot x = 1$ megoldása az $x = \frac{1}{\varepsilon_k} = \varepsilon_{-k}$. Ha $-k$-t modulo 8 tekintjük, akkor ismét megkapjuk (*) valamelyik elemét. Az $x \cdot \varepsilon_k = 1$ egyenlet megoldása ugyanez, s így x inverz.

I., II., III. és IV alapján (*) a szorzással csoport. A csoport kommutatív is (megint hivatkozhatunk arra, hogy a komplex számok testet alkotnak az összeadás és szorzás műveletekre, s (*) ennek részhalmaza). ■

3.2-3. Legyen n rögzített pozitív egész szám. Lássuk be, hogy az n-edik egységgyökök halmaza a szorzásra nézve csoportot alkot.

Megoldás. $a \in \mathbb{C}$ n-edik egységgyök, ha $a^n = 1$. Az n-edik egységgyökök:

$$\varepsilon_k = \cos k\frac{2\pi}{n} + i \sin k\frac{2\pi}{n}, \quad 0 \leq k \leq n-1 \qquad (*)$$

I. Először belátjuk, hogy a szorzás művelet a (*) halmazon. Legyen a és b n-edik egységgyök, tehát $a^n = 1$ és $b^n = 1$. Ekkor $(a \cdot b)^n = a^n \cdot b^n = 1$, tehát $a \cdot b$ is n-edik egységgyök.

II. A művelet asszociatív, vagyis ha a, b, és c tetszőleges elemei a halmaznak, akkor

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Ez most teljesül, ugyanis $\mathbb{C}$ test, rajta a $\cdot$ művelet asszociatív, (*) pedig $\mathbb{C}$-nek részhalmaza.

III. Egységelem az 1. Ugyanis 1 is n-edik egységgyök, és ha a eleme (*)-nak, akkor $1 \cdot a = a \cdot 1 = a$.

IV. Létezik mindegyik a n-edik egységgyöknek inverze az 1-re vonatkozóan. Ugyanis az $\varepsilon_k \cdot x = 1$ megoldása az $x = \frac{1}{\varepsilon_k} = \varepsilon_{-k} = \varepsilon_{n-k}$, ε_{n-k} pedig (*) egyik eleme. Az $x \cdot \varepsilon_k = 1$ egyenlet megoldása ugyanez, s így x inverz.

I., II., III. és IV alapján (*) a szorzással csoport. A csoport kommutatív is (megint hivatkozhatunk arra, hogy a komplex számok testet alkotnak az összeadás és szorzás műveletekre, s (*) ennek részhalmaza). ■

3.2-4. Lássuk be, hogy az összes n-edik egységgyök halmaza (n befutja a pozitív egész számokat) a szorzásra nézve csoportot alkot.

Megoldás.

I. Először belátjuk, hogy a szorzás művelet a (*) halmazon. Legyen a n-edik, b pedig k-adik egységgyök, tehát $a^n = 1$ és $b^k = 1$. Ekkor $(a \cdot b)^{n \cdot k} = (a^n)^k \cdot (b^k)^n = 1$, $a \cdot b$ tehát $n \cdot k$-adik egységgyök.

II. A művelet asszociatív, vagyis ha a, b, és c tetszőleges elemei a halmaznak, akkor

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)$$

Ez teljesül, ugyanis $\mathbb{C}$ test, rajta a $\cdot$ művelet asszociatív, (*) pedig $\mathbb{C}$-nek részhalmaza.

III. Egységelem az 1. Ugyanis 1 n-edik egységgyök minden n esetén és ha a n-edik egységgyök, akkor $1 \cdot a = a \cdot 1 = a$.

IV. Létezik mindegyik a n-edik egységgyöknek inverze az 1-re vonatkozóan. Lásd az előző példa IV. pontját.

I., II., III. és IV alapján a halmaz a szorzással csoport. A csoport kommutatív is. ■

3.2-5.

a. Vizsgáljuk meg, hogy a modulo 5 maradékosztályok a maradékosztályok szorzására csoportot alkotnak-e.

b. Állapítsuk meg, hogy a modulo 5 maradékosztályok halmazából elhagyva a 0 által reprezentált maradékosztályt, a maradékosztályok szorzására csoportot kapunk-e?

Megoldás. A modulo 5 maradékosztályok halmaza:

$$\{\overline{0}, \quad \overline{1}, \quad \overline{2}, \quad \overline{3}, \quad \overline{4} \pmod 5\}, \tag{$*$}$$

ahol például $\overline{0}$ a modulo 5 tekintett 0 által reprezentált maradékosztályt jelöli.

a. A maradékosztályok szorzását a következő összefüggés definiálja:

$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}, \tag{$**$}$$

vagyis a maradékosztályok reprezentánsait összeszorozzuk, és vesszük azt a maradékosztályt, amelyiknek ez a reprezentánsa. Belátható hogy ez a szorzás nem függ a reprezentánstól. Ezért maradékosztályok szorzata maradékosztály.

Nézzük a szorzás művelettábláját:

$\cdot \pmod 5$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A szorzásokat modulo 5 végeztük. Például $\overline{3} \cdot \overline{4} = \overline{2}$, mert

$$3 \cdot 4 \equiv 12 \equiv 2 \pmod 5.$$

I. A fenti táblából látjuk, hogy a maradékosztályok szorzása művelet a halmazon, mert bármely két (*)-beli maradékosztály szorzata (*)-beli.

Azt is látjuk, hogy a művelet kommutatív. Ez abban jut kifejezésre, hogy a művelettábla a főátlóra szimmetrikus.

II. A maradékosztályok szorzása asszociatív. (**) alapján ugyanis

$$(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{(a \cdot b) \cdot c}$$

és

$$\overline{a} \cdot (\overline{b} \cdot \overline{c}) = \overline{a \cdot (b \cdot c)},$$

a jobb oldalak pedig megegyeznek, mert az egész számok szorzása asszociatív.

III. A táblából látható, hogy az $\overline{1}$ egységelem, hiszen az $\overline{1}$ sorában ismétlődik a fejléc, az oszlopában pedig az oldalléc jelenik meg.

IV. Keressünk inverzet. Például $\overline{3}$ sorában megtaláljuk az egységelemet a $\overline{2}$ oszlopával való metszéspontban, tehát $\overline{3} \cdot \overline{2} = \overline{1}$. Mivel kommutatív a művelet, $\overline{2} \cdot \overline{3} = \overline{1}$, s így $\overline{3}$ inverze $\overline{2}$.

Baj van azonban a $\overline{0}$-val. Bármivel való szorzata $\overline{0}$, nem pedig $\overline{1}$, így nincs inverze.

Mivel nem minden elemnek van inverze, (*) a szorzással nem alkot csoportot, csupán kommutatív félcsoportot.

b. Most a következő maradékosztályhalmazt vizsgáljuk:

$$\{\overline{1}, \quad \overline{2}, \quad \overline{3}, \quad \overline{4} \pmod 5\}, \qquad (***)$$

Nézzük ezen a szűkített halmazon a művelettáblát:

$\cdot \pmod 5$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{1}$	$\overline{3}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{4}$	$\overline{2}$
$\overline{4}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

I. A fenti táblából látjuk, hogy a maradékosztályok szorzása művelet a halmazon, mert bármely két (***)-beli maradékosztály szorzata (***)-beli.

A művelet kommutatív.

II. A maradékosztályok szorzása asszociatív.

III. A táblából látható, hogy az $\overline{1}$ egységelem.

IV. Most minden elemnek van inverze, mert az $\overline{1}$ a művelettábla mindegyik sorában (és mindegyik oszlopában) megjelenik.

I., II., III. és IV. alapján (***) a szorzással csoport.

Megjegyzés. Figyeljük meg ezt az utóbbi művelettáblát, tehát egy csoport művelettábláját. Minden sorban (és minden oszlopban) mindegyik elem legfeljebb egyszer fordul elő. Csoportban mindig ez a helyzet. Mivel most véges a csoport, az is elmondható, hogy minden sorban (és minden oszlopban) mindegyik elem pontosan egyszer fordul elő. ■

3.2-6. a. Vizsgáljuk meg, hogy a modulo 8 maradékosztályok a maradékosztályok szorzására csoportot alkotnak-e.

b. Állapítsuk meg, hogy a modulo 8 maradékosztályok halmazából elhagyva a 0 által reprezentált maradékosztályt, a maradékosztályok szorzására csoportot kapunk-e?

c. Állapítsuk meg, hogy a modulo 8 vett redukált maradékosztályok a maradékosztályok szorzására csoportot alkotnak-e?

Megoldás. A modulo 8 maradékosztályok halmaza:

$$\{\overline{0},\quad \overline{1},\quad \overline{2},\quad \overline{3},\quad \overline{4},\quad \overline{5},\quad \overline{6},\quad \overline{7}\pmod 8\} \qquad (*)$$

a.

Nézzük a szorzás műveletábláját:

$\cdot \pmod 8$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{0}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{0}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{0}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A szorzásokat modulo 8 végeztük. Például $\overline{6}\cdot\overline{5}=\overline{6}$, mert

$$6\cdot 5\equiv 30\equiv 6 \pmod 8.$$

I. A fenti táblából látjuk, hogy a maradékosztályok szorzása művelet a halmazon, mert bármely két (*)-beli maradékosztály szorzata (*)-beli.

Azt is látjuk, hogy a művelet kommutatív, mert a a művelettábla a főátlóra szimmetrikus.

II. A maradékosztályok szorzása asszociatív. (Lásd az előző példa a.II. pontját.)

III. A táblából látható, hogy az $\overline{1}$ egységelem, hiszen az $\overline{1}$ sorában ismétlődik a fejléc, az oszlopában pedig az oldalléc jelenik meg.

IV. Keressünk inverzet. $\overline{0}$ bármivel való szorzata $\overline{0}$, nem pedig $\overline{1}$, így nincs inverze.

Mivel nem minden elemnek van inverze, (*) a szorzással nem alkot csoportot, csupán kommutatív félcsoportot.

b. Most a következő maradékosztályhalmazt vizsgáljuk:

$$\{\overline{1},\quad \overline{2},\quad \overline{3},\quad \overline{4},\quad \overline{5},\quad \overline{6},\quad \overline{7}\pmod 8\} \qquad (**)$$

Nézzük ezen a szűkített halmazon a művelettáblát:

$\cdot \pmod 8$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{2}$	$\overline{3}$	$\overline{4}$	$\overline{5}$	$\overline{6}$	$\overline{7}$
$\overline{2}$	$\overline{2}$	$\overline{4}$	$\overline{6}$	$\overline{0}$	$\overline{2}$	$\overline{4}$	$\overline{6}$
$\overline{3}$	$\overline{3}$	$\overline{6}$	$\overline{1}$	$\overline{4}$	$\overline{7}$	$\overline{2}$	$\overline{5}$
$\overline{4}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$	$\overline{0}$	$\overline{4}$
$\overline{5}$	$\overline{5}$	$\overline{2}$	$\overline{7}$	$\overline{4}$	$\overline{1}$	$\overline{6}$	$\overline{3}$
$\overline{6}$	$\overline{6}$	$\overline{4}$	$\overline{2}$	$\overline{0}$	$\overline{6}$	$\overline{4}$	$\overline{2}$
$\overline{7}$	$\overline{7}$	$\overline{6}$	$\overline{5}$	$\overline{4}$	$\overline{3}$	$\overline{2}$	$\overline{1}$

A fenti táblából látjuk, hogy a maradékosztályok szorzása nem művelet a halmazon, mert a művelettábla belsejében több helyen megjelenik az $\overline{0}$, ami viszont nem eleme az alaphalmaznak. Tehát vannak olyan elempárok, amelyek szorzata nem eleme (*)-nak (például $\overline{4}\cdot\overline{2}=\overline{0}$.)

Mivel a szorzás nem művelet a halmazon, (*) a szorzással nem csoport, még csak nem is félcsoport, sőt nem is algebrai struktúra.

c. Redukált az a maradékosztály modulo 8, amelyiknek az elemei 8-hoz relatív prímek. A következő maradékosztályhalmazt vizsgáljuk:

$$\{\overline{1},\quad \overline{3},\quad \overline{5},\quad \overline{7}\pmod 8\} \qquad (***)$$

Nézzük ezen a halmazon a művelettáblát:

$\cdot \pmod 8$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{1}$	$\overline{1}$	$\overline{3}$	$\overline{5}$	$\overline{7}$
$\overline{3}$	$\overline{3}$	$\overline{1}$	$\overline{7}$	$\overline{5}$
$\overline{5}$	$\overline{5}$	$\overline{7}$	$\overline{1}$	$\overline{3}$
$\overline{7}$	$\overline{7}$	$\overline{5}$	$\overline{3}$	$\overline{1}$

I. A fenti táblából látjuk, hogy a maradékosztályok szorzása művelet a halmazon, mert bármely két (***)-beli maradékosztály szorzata (***)-beli.

A művelet kommutatív.

II. A maradékosztályok szorzása asszociatív.

III. A táblából látható, hogy az $\overline{1}$ egységelem.

IV. Minden elemnek van inverze, mert az $\overline{1}$ a művelettábla mindegyik sorában (és mindegyik oszlopában) megjelenik.

I., II., III. és IV. alapján (***) a szorzással csoport. ■

3.2-7.

a. Vizsgáljuk meg, hogy a modulo m vett maradékosztályok a szorzásra nézve csoportot alkotnak-e.

b. Vizsgáljuk meg, hogy a modulo m vett redukált maradékosztályok a szorzásra nézve csoportot alkotnak-e.

Megoldás.

I. A maradékosztályok szorzása művelet a halmazon, mert bármely két maradékosztály szorzata maradékosztály a maradékosztályok szorzásának definíciója szerint.

A művelet kommutatív.

II. A maradékosztályok szorzása asszociatív. (Lásd az 5. példa a.II. pontját.)

III. $\overline{1}$ egységelem

IV. Keressünk inverzet. $\overline{0}$ bármivel való szorzata $\overline{0}$, nem pedig $\overline{1}$, így nincs inverze.

Mivel nem minden elemnek van inverze, a modulo m vett maradékosztályok halmaza a szorzással nem alkot csoportot, csupán kommutatív félcsoportot.

b. Redukált az a maradékosztály modulo n, amelyiknek az elemei n-hez relatív prímek.

I. A maradékosztályok szorzása művelet a halmazon, mert bármely két redukált maradékosztály szorzata redukált maradékosztály.

A művelet kommutatív.

II. A maradékosztályok szorzása asszociatív.

III. $\overline{1}$ is redukált maradékosztály, és $\overline{1}$ egységelem.

IV. Minden elemnek van inverze. Nézzük ugyanis az

$$\overline{a} \cdot \overline{x} = \overline{1} \qquad (****)$$

egyenlet megoldását. Ez ekvivalens azzal, ha az

$$a \cdot x \equiv 1 \pmod{n}$$

egyenlet megoldását keressük. Ennek az utóbbinak van megoldása, mert

$$(a, n) = 1 \mid 1.$$

Megoldás például az

$$x = a^{\varphi(n)-1} \pmod{n}$$

(lásd az Euler-tételt számelméletből.) Így (****) megoldása az $\overline{a^{\varphi(n)-1}}$ modulo n tekintett maradékosztály.

I., II., III. és IV. alapján a modulo n vett redukált maradékosztályok halmaza a szorzással csoportot alkot. ■

3.2-8. Csoportot alkotnak-e a következő konstrukciók?

a. A modulo 35 maradékosztályok közül az

$$A = \{0, 5, 10, 15, 20, 25, 30\}$$

által reprezentáltak a maradékosztály összeadásra;

b. A modulo 35 maradékosztályok közül

$$A = \{0, 5, 10, 15, 20, 25, 30\}$$

által reprezentáltak a maradékosztály szorzásra;

c. A modulo 35 maradékosztályok közül az

$$A \setminus \{0\}$$

által reprezentáltak a maradékosztály szorzásra;

d. A modulo 25 maradékosztályok közül a

$$B = \{5, 10, 15, 20\}$$

által reprezentáltak a maradékosztály szorzásra.

Megoldás.

a. Nézzük a művelettáblát.

$+ \pmod{35}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{0}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{5}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$	$\overline{0}$
$\overline{10}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$	$\overline{0}$	$\overline{5}$
$\overline{15}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$	$\overline{0}$	$\overline{5}$	$\overline{10}$
$\overline{20}$	$\overline{20}$	$\overline{25}$	$\overline{30}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$
$\overline{25}$	$\overline{25}$	$\overline{30}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$
$\overline{30}$	$\overline{30}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$

Az összeadást modulo 35 végeztük.

I. Az összeadás művelet, mert bármelyik két maradékosztály összege olyan maradékosztály, amelyiknek a reprezentánsa A-ban van.

II. Asszociatív a művelet. Maradékosztályok összeadása asszociatív, mert az összeadás definíciójából ($\overline{a} + \overline{b} = \overline{a+b}$) látható, hogy az egész számok összeadására vezethető vissza, ami asszociatív.

III. Egységelem a $\overline{0}$.

IV. Inverze mindegyik elemnek van, mert minden sorban (és mindegyik oszlopban is) szerepel az egységelem, így például $\overline{20}$ additív inverze $\overline{15}$.

I., II., III. és IV. alapján az A halmaz által reprezentáltak az összeadásra csoportot alkotnak.

b. Nézzük a művelettáblát.

$\cdot \pmod{35}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{5}$	$\overline{0}$	$\overline{25}$	$\overline{15}$	$\overline{5}$	$\overline{30}$	$\overline{20}$	$\overline{10}$
$\overline{10}$	$\overline{0}$	$\overline{15}$	$\overline{30}$	$\overline{10}$	$\overline{25}$	$\overline{5}$	$\overline{20}$
$\overline{15}$	$\overline{0}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{20}$	$\overline{0}$	$\overline{30}$	$\overline{25}$	$\overline{20}$	$\overline{15}$	$\overline{10}$	$\overline{5}$
$\overline{25}$	$\overline{0}$	$\overline{20}$	$\overline{5}$	$\overline{25}$	$\overline{10}$	$\overline{30}$	$\overline{15}$
$\overline{30}$	$\overline{0}$	$\overline{10}$	$\overline{20}$	$\overline{30}$	$\overline{5}$	$\overline{15}$	$\overline{25}$

I. A művelettábláról leolvashatjuk, hogy a szorzás művelet a halmazon, mert bármely két olyan maradékosztálynak, amelynek reprezántánsai A-ban vannak, a szorzata is olyan hogy a reprezentáns A-beli.

II. A maradékosztályok szorzása általában is asszociatív.

III. A művelettábláról leolvasható, hogy egységelem a $\overline{15}$ maradékosztály.

IV. A $\overline{0}$-nak nincs inverze.

A struktúra egységelemes félcsoport.

c. Nézzük a szűkített halmazon a művelettáblát.

$\cdot \pmod{35}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{5}$	$\overline{25}$	$\overline{15}$	$\overline{5}$	$\overline{30}$	$\overline{20}$	$\overline{10}$
$\overline{10}$	$\overline{15}$	$\overline{30}$	$\overline{10}$	$\overline{25}$	$\overline{5}$	$\overline{20}$
$\overline{15}$	$\overline{5}$	$\overline{10}$	$\overline{15}$	$\overline{20}$	$\overline{25}$	$\overline{30}$
$\overline{20}$	$\overline{30}$	$\overline{25}$	$\overline{20}$	$\overline{15}$	$\overline{10}$	$\overline{5}$
$\overline{25}$	$\overline{20}$	$\overline{5}$	$\overline{25}$	$\overline{10}$	$\overline{30}$	$\overline{15}$
$\overline{30}$	$\overline{10}$	$\overline{20}$	$\overline{30}$	$\overline{5}$	$\overline{15}$	$\overline{25}$

I. A művelettábláról leolvashatjuk, hogy a szorzás művelet a halmazon, mert bármely két olyan maradékosztálynak, amelynek reprezántánsai $A \setminus \{0\}$-ban vannak, a szorzata is olyan hogy a reprezentáns $A \setminus \{0\}$-beli.

II. A maradékosztályok szorzása általában is asszociatív.

III. A művelettábláról leolvasható, hogy egységelem a $\overline{15}$ maradékosztály.

IV. A művelettábláról leolvasható, hogy mindegyik elemnek van inverze, hiszen a $\overline{15}$ mindegyik sorban (és mindegyik oszlopban is) megjelenik.

A stuktúra csoport.

d. Ebben a struktúrában a szorzás nem művelet, mert van két olyan elem, amelyik szorzatának reprezentánsa nincs B-ben. Például $\overline{5} \cdot \overline{20} = \overline{0}$. ■

3.2-9. Az alábbi struktúrák közül válassza ki a félcsoportokat, illetve csoportokat:

a. A természetes számok halmaza az összeadásra nézve.

b. A páros számok halmaza az összeadásra nézve.

c. A páratlan számok halmaza a szorzásra nézve.

d. Az egész számok halmaza az összeadásra nézve.

e. Az egész számok halmaza a szorzásra nézve.

f. A nemnegatív racionális számok halmaza a szorzásra nézve.

g. A pozitív racionális számok halmaza a szorzásra nézve.

h. A nullától különböző valós számok halmaza a szorzásra nézve.

i. A sík vektorainak halmaza az összeadásra nézve.

j. A komplex számok halmaza az összeadásra nézve.

k. A valós elemű n-ed rendű mátrixok halmaza a szorzásra nézve. (n rögzített természetes szám.)

l. A valós elemű n-ed rendű nem szinguláris, (n rangú) mátrixok halmaza a szorzásra nézve.

Megoldás. a. Egységelemes félcsoport, **b.** csoport, **c.** egységelemes félcsoport, **d.** csoport, **e.** egységelemes félcsoport, **f.** egységelemes félcsoport, **g.** csoport, **h.** csoport, **i.** csoport, **j.** csoport, **k.** egységelemes félcsoport, **l.** csoport. ■

3.2-10. Legyen $(G, \cdot)$ csoport, $u \in G$ rögzített elem. Definiáljunk G-n egy új $\circ$ műveletet $a \circ b := a \cdot u \cdot b$ segítségével. Csoport lesz-e $(G, \circ)$?

Megoldás.

I. $\circ$ művelet G-n, mert tetszőleges két G-beli elemhez G-beli elemet rendel.

II. A művelet asszociatív:

$$(a \circ b) \circ c = (a \cdot u \cdot b) \cdot u \cdot c =$$

mivel $(G, \cdot)$ csoport, ezért a $\cdot$ asszociatív G-n, ami miatt

$$= a \cdot u \cdot (b \cdot u \cdot c) = a \circ (b \circ c)$$

III. Jelölje $(G, \cdot)$ egységelemét e. Keressük $(G, \circ)$ egységelemét, amit ε-nal jelölünk.

$$\begin{aligned} a \circ \varepsilon &= a \\ a \cdot u \cdot \varepsilon &= a \\ a \cdot u \cdot \varepsilon &= a \cdot e \end{aligned}$$

G csoport, így minden elemének van inverze. Beszorozzuk az egyenletet balról a^{-1}-gyel:

$$\begin{aligned} a^{-1} \cdot a \cdot u \cdot \varepsilon &= a^{-1} \cdot a \cdot e \\ e \cdot u \cdot \varepsilon &= e \cdot e \\ u \cdot \varepsilon &= e \end{aligned}$$

Most beszorozzuk az egyenletet balról u^{-1}-gyel:

$$\begin{aligned} \varepsilon &= u^{-1} \cdot e \\ \varepsilon &= u^{-1} \end{aligned}$$

Tehát u^{-1} jobb oldali egységelem. Hasonlóan kereshetünk bal oldali egységelemet:

$$\begin{aligned} \varepsilon \circ a &= a \\ \varepsilon \cdot u \cdot a &= a \\ \varepsilon \cdot u \cdot a &= e \cdot a \\ \varepsilon \cdot u &= e \\ \varepsilon &= e \cdot u^{-1} \\ \varepsilon &= u^{-1} \end{aligned}$$

Tehát u^{-1} bal oldali egységelem is és így egységelem.

III. Keressük tetszőleges a elem inverzét.

$$a \circ x = \varepsilon$$

$$a \cdot u \cdot x = u^{-1}$$

$$u \cdot x = a^{-1} \cdot u^{-1}$$

$$x = u^{-1} \cdot a^{-1} \cdot u^{-1}$$

Tehát az $a \circ x = \varepsilon$ egyenlet megoldása $x = u^{-1} \cdot a^{-1} \cdot u^{-1}$. Ugyanezt kapjuk az $x \circ a = \varepsilon$ egyenlet megoldására is. Tehát a-nak van inverze $(G, \circ)$-ben, és ez az $u^{-1} \cdot a^{-1} \cdot u^{-1}$.

I., II., III., és IV. alapján $(G, \circ)$ is csoport. ■

3.2-11. Lássuk be, hogy ha egy csoport minden elemének inverze önmaga, akkor a csoport kommutatív.

Megoldás.

Be kell tehát látnunk, hogy

$$a \cdot b = b \cdot a$$

a csoport bármely két a és b-beli eleme esetén teljesül.

1. *megoldás.* Legyen a és b tetszőleges két eleme a csoportnak.

A feltétel szerint:

$$a \cdot b = (a \cdot b)^{-1}$$

Másrészt szorzat inverze a tényezők inverzének **fordított sorrendben vett** szorzata:

$$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1}$$

Ismét a feltételt alkalmazva:

$$b^{-1} \cdot a^{-1} = b \cdot a$$

Tehát

$$a \cdot b = b \cdot a$$

Mivel ez bármely két csoportbeli elemre igaz, a csoport kommutatív.

2. *megoldás.*

Legyen megint a és b tetszőleges két eleme a csoportnak.

A feltétel szerint:

$$(a \cdot b) \cdot (a \cdot b) = e$$
$$a \cdot (b \cdot a) \cdot b = e$$

Szorozzuk be az egyenletet balról a-val

$$a \cdot a \cdot (b \cdot a) \cdot b = a$$

Szorozzuk be az egyenletet jobbról b-vel

$$a \cdot a \cdot (b \cdot a) b \cdot b = a \cdot b$$

Mivel a feltétel szerint $a \cdot a = e$ és $b \cdot b = e$

$$b \cdot a = a \cdot b$$

Ez bármely két csoportbeli elemre igaz, így a csoport kommutatív. ■

3.2-12. Bizonyítsuk be, hogy ha a $(G, \cdot)$ csoport minden a, b elempárjára $(a \cdot b)^2 = a^2 \cdot b^2$, akkor a csoport kommutatív.

Megoldás. Legyen a és b tetszőleges két eleme a csoportnak.

A feltétel szerint:

$$(a \cdot b)^2 = a^2 \cdot b^2$$

A bal oldal a következőképpen írható:

$$(a \cdot b)^2 = a \cdot b \cdot a \cdot b$$

A jobb oldal kifejtése:

$$a^2 \cdot b^2 = a \cdot a \cdot b \cdot b$$

Ez a két utóbbi jobb oldal megegyezik:

$$a \cdot b \cdot a \cdot b = a \cdot a \cdot b \cdot b$$

Szorzunk a^{-1}-gyel balról, b^{-1}-gyel pedig jobbról:

$$b \cdot a = a \cdot b$$

Mivel ez bármely két csoportbeli elemre igaz, a csoport kommutatív. ■

3.2.2. Csoport rendje, elem rendje, részcsoport, generátum, Lagrange-tétel

3.2-13.

a. A 8-adik komplex egységgyökök szorzással alkotott csoportjában határozzuk meg a csoport rendjét és az egyes elemek rendjét.

b. Ebben a csoportban határozzuk meg az egyes elemek generátumát.

c. Ciklikus-e ez a csoport?

Megoldás. A 8-adik komplex egységgyökök (lásd az 1. ábrát):

$$\varepsilon_k = \cos k\frac{2\pi}{8} + i \sin k\frac{2\pi}{8}, \quad 0 \leq k \leq 7 \qquad (*)$$

a. A csoport rendje 8, mert 8 elemű az alaphalmaz.

Az elemek rendje:

Nézzük ε_1 hatványait sorban. (Hatványozásnál alkalmazzuk a Moivre-azonosságot.)

n	ε_1^n
1	ε_1
2	$\varepsilon_1^2 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^2 = \cos\frac{\pi}{2} + i\sin\frac{\pi}{2} = \varepsilon_2$
3	$\varepsilon_1^3 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^3 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = \varepsilon_3$
4	$\varepsilon_1^4 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^4 = \cos\pi + i\sin\pi = \varepsilon_4$
5	$\varepsilon_1^5 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^5 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = \varepsilon_5$
6	$\varepsilon_1^6 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^6 = \cos\frac{3\pi}{2} + i\sin\frac{3\pi}{2} = \varepsilon_6$
7	$\varepsilon_1^7 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^7 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = \varepsilon_7$
8	$\varepsilon_1^8 = (\cos\frac{\pi}{4} + i\sin\frac{\pi}{4})^8 = \cos 2\pi + i\sin 2\pi = \varepsilon_0$

$|\varepsilon_1| = 8$, mert $\varepsilon_1^8 = 1$, és ε_1 8-nál kisebb pozitív kitevős hatványai nem állítják elő az 1-et (az egységelemet).

$|\varepsilon_2| = 4$, mert $\varepsilon_2^4 = 1$, és ε_1 4-nél kisebb pozitív kitevős hatványai nem állítják elő az 1-et (az egységelemet.)

Hasonló gondolatmenettel kapjuk a többit is.

$|\varepsilon_3| = 8$, $|\varepsilon_4| = 2$, $|\varepsilon_5| = 8$, $|\varepsilon_6| = 4$, $|\varepsilon_7| = 8$ és $|\varepsilon_0| = 1$.

Elem	rendje	generátuma
ε_0	1	$\{\varepsilon_0\}$
ε_1	8	$\{\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7\}$
ε_2	4	$\{\varepsilon_0, \varepsilon_2, \varepsilon_4, \varepsilon_6\}$
ε_3	8	$\{\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7\}$
ε_4	2	$\{\varepsilon_0, \varepsilon_4\}$
ε_5	8	$\{\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7\}$
ε_6	4	$\{\varepsilon_0, \varepsilon_2, \varepsilon_4, \varepsilon_6\}$
ε_7	8	$\{\varepsilon_0, \varepsilon_1, \varepsilon_2, \varepsilon_3, \varepsilon_4, \varepsilon_5, \varepsilon_6, \varepsilon_7\}$

b. Az elemek generátuma:

$\varepsilon_1, \varepsilon_3, \varepsilon_5$ és ε_7 generátuma az egész csoport, mert bármelyikük pozitív egész kitevős hatványait képezve megkapjuk az összes többi elemet, s ezek csoportot alkotnak.

ε_2 és ε_6 generátuma $\{\varepsilon_2, \varepsilon_4, \varepsilon_6, \varepsilon_0\}$. Például ε_2 pozitív egész kitevős hatványait képezve megkapjuk a többi elemet, s ezek csoportot is alkotnak, a 8-adik komplex egységgyökök szorzással vett csoportjának részcsoportját.

ε_4 generátuma $\{\varepsilon_4, \varepsilon_0\}$.

ε_0 generátuma $\{\varepsilon_0\}$.

Ezek mind részcsoportjai a kiinduló csoportnak.

c. A csoport ciklikus, mert generálható egyetlen elemmel, például ε_1-gyel.

Megjegyzés. A Lagrange-tétel következménye szerint elem rendje osztója a csoport rendjének. Figyeljük meg, hogy az elemrendekre (1, 2, 4, 8) ez most is teljesül. ■

3.2-14. Vizsgáljuk meg, hogy a következő algebrai struktúrák csoportot alkotnak-e? Ha igen, adjuk meg a csoport rendjét. A csoportok közül melyek ciklikusak?

a. Az m-mel osztható (m pozitív egész) egész számok az összeadásra nézve.

b. Az egész számok halmaza az $a \circ b = a + b + 1$ műveletre nézve.

Megoldás.

a. Az összeadás művelet a halmazon, mert két m-mel osztható egész szám összege is m-mel osztható. A művelet asszociatív, egységelem a 0, bármelyik a elem inverze $-a$, tehát csoportot alkot. Mivel kommutatív ez a művelet, Abel-csoportról van szó. A csoport végtelen rendű és ciklikus, ugyanis m generálja.

b. $\circ$ művelet a halmazon, mert ha $a,\ b \in \mathbb{Z}$, akkor $a \circ b = a + b + 1 \in \mathbb{Z}$ is teljesül. A művelet asszociatív. Egyrészt ugyanis

$$(a \circ b) \circ c = (a + b + 1) \circ c = (a + b + 1) + c + 1 = a + b + c + 2,$$

másrészt

$$a \circ (b \circ c) = a \circ (b + c + 1) = a + (b + c + 1) + 1 = a + b + c + 2,$$

s ez a két kifejezés megegyezik egymással. A művelet kommutatív.

Bal oldali egységelem az $a \circ e = a + e + 1 = a$ egyenlet megoldása, az $e = -1$. Mivel a művelet kommutatív, ez jobb oldali egységelem is, tehát egységelem.

Inverz az $a \circ a^{-1} = a + a^{-1} + 1 = -1$ egyenlet megoldása, az $a^{-1} = -a - 2$.

Tehát a struktúra csoport, és mivel kommutatív, Abel-csoport.

Végtelen rendű és ciklikus, generátor elem a 0. Lássuk ugyanis a 0 néhány hatványát:

$$0^1 = 0 \quad 0^2 = 1 \quad 0^3 = 2 \quad \dots \quad 0^k = k - 1 \quad \dots$$

A negatív kitevőjű hatványokat az inverz segítségével számíthatjuk ki ($a^{-1} = -a - 2$).

$$0^{-1} = -2 \quad 0^{-2} = -3 \quad 0^{-3} = -4 \quad \dots \quad 0^{-k} = -(k-1) - 2 = -k - 1 \quad \dots$$

$0^0 = e = -1$ definíció szerint. Tehát a 0 hatványai (a pozitívak és a negatívak, valamint a nulladik hatvány együtt) kiadják az egész csoportot. ■

Diédercsoport

A D_n *diédercsoport* a síknak egy szabályos n oldalú sokszögét önmagába vivő egybevágósági transzformációkból áll, művelet a transzformációk egymás utáni végrehajtása. Ha φ a $\frac{2\pi}{n}$-nel való forgatást,

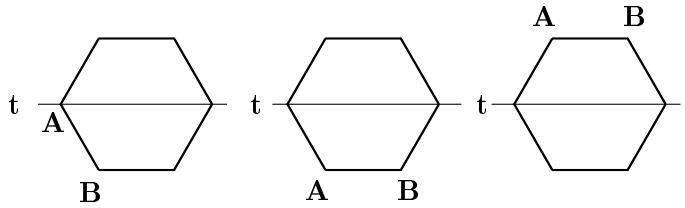
τ pedig egy szimmetriatengelyre való tükrözést jelöl, akkor D_n elemei:

$$\{e, \varphi, \varphi^2, \ldots, \varphi^{n-1}, \tau, \tau \cdot \varphi, \tau \cdot \varphi^2 \ldots, \tau \cdot \varphi^{n-1}\}$$

A számolás szabályai:

$$\varphi^n = \tau^2 = e \quad \varphi \cdot \tau = \tau \cdot \varphi^{n-1}$$

Belátható, hogy D_n a fenti művelettel csoportot alkot.



2. ábra. Szabályos hatszög elforgatása a középpontja körül $\frac{\pi}{6} = 60°$-kal, majd tükrözés a t tükörtengelyre

Az $n = 2$ esetben a ***Klein-féle*** csoportot kapjuk. Ez az egyetlen kommutatív diédercsoport. $D_2 = \{e, a, b, c\}$, az egységelem kivételével mindegyik elem másodrendű, és bármelyik két elem szorzata a harmadik elem.

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

3.2-15. Adott egy sík és abban egy szabályos háromszög. Tekintsük azon síkbeli egybevágósági transzformációk G halmazát, amelyek a szabályos háromszöget önmagába viszik át. A G halmazon értelmezzük a műveletet a transzformációk egymás utáni végrehajtásával (függvénykompozícióként). (Két háromszöget akkor tekintünk azonosnak, ha a megfelelő csúcsok ugyanott vannak.)

a. Bizonyítsuk be, hogy G csoportot alkot.

b. Határozzuk meg a G csoport rendjét.

c. Jelölje φ a szabályos háromszög középpontja körüli pozitív irányú $\frac{2\pi}{3} = 120°$-os elforgatást, τ pedig egy (a síkban rögzített) magasságvonalra vonatkozó tükrözést. Írjuk fel ezek segítségével G összes elemét, határozzuk meg az egyes elemek rendjét, inverzét, valamint a $\{\varphi\}$, a $\{\tau\}$, illetve a $\{\varphi, \tau\}$ halmazok által generált részcsoportokat.

d. Kommutatív-e ez a csoport?

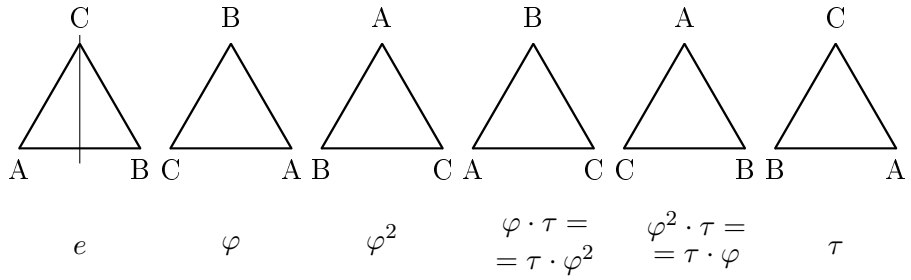
e. Ciklikus-e ez a csoport?

Megoldás.

a. G csoport, mert a transzformációk egymásutánja művelet a halmazon, hiszen két egymásután végrehajtott transzformációnak megfelel G valamelyik eleme. A művelet asszociatív (transzformációk egymásutáni végrehajtása asszociatív), létezik egységelem (a „helybenhagyás"), és mindegyik transzformációnak létezik inverze (a transzformáció „visszafelé" elvégezve).

b. G rendje (az elemeinek a számossága) $|G| = 3! = 6$, mert a háromszög három csúcsának ennyi különböző helyzete lehet.

c. φ jelölje a középpont körüli $\frac{2\pi}{3}$-mal való elforgatást, τ a síkban rögzített magasságvonalra való tükrözést. Keressük meg ezekkel kifejezve G többi elemét.



3. ábra. A D_3 diédercsoport elemei

A 3. ábra első háromszöge az alaphelyzet, ebbe a „helybenhagyás" transzformáció viszi a háromszöget, ehhez tartozik tehát az egységelem, amit e jelöl. A második háromszög az elsőből a középpont körüli $\frac{2\pi}{3}$ szöggel való elforgatással adódik, ehhez tartozik tehát a φ transzformáció. Az utolsó háromszög az alaphelyzetből a függőleges helyzetű tengelyre való tükrözéssel keletkezik, így ehhez tartozik a τ transzformáció. A harmadik háromszöghöz juthatunk

az alaphelyzetből, ha a középpont körül kétszer forgatjuk el a háromszöget $\frac{2\pi}{3}$ szöggel (φ^2). A negyedik háromszöget megkapjuk, ha alkalmazzuk először a φ, majd a τ transzformációt, tehát a $\varphi \cdot \tau$-t, de ugyanide jutunk, ha először a τ-t, majd a φ^2-et végezzük el. Tehát ebben a csoportban $\varphi \cdot \tau = \tau \cdot \varphi^2$. A $\varphi^2 \cdot \tau$ és a $\tau \cdot \varphi$ egyaránt az ötödik háromszöghöz tartozik, amiből az is következik, hogy ebben a csoportban $\tau \cdot \varphi \neq \varphi \cdot \tau$, tehát a csoport nem kommutatív.

elem		rend	inverz
e		1	e
τ	$\tau^2 = e$	2	$\tau^{-1} = \tau$
φ	$\varphi^3 = e$	3	$\varphi^{-1} = \varphi^2$
φ^2	$(\varphi^2)^3 = (\varphi^3)^2 = e$	3	$(\varphi^2)^{-1} = \varphi$
$\tau \cdot \varphi = \varphi^2 \cdot \tau$	$(\tau \cdot \varphi)^2 = \tau \cdot \varphi \cdot \tau \cdot \varphi = \tau \cdot \varphi \cdot \varphi^2 \cdot \tau = e$	2	$(\tau \cdot \varphi)^{-1} = \tau \cdot \varphi$
$\varphi \cdot \tau = \tau \cdot \varphi^2$	$(\varphi \cdot \tau)^2 = \varphi \cdot \tau \cdot \varphi \cdot \tau = \varphi \cdot \tau \cdot \tau \cdot \varphi^2 = e$	2	$(\varphi \cdot \tau)^{-1} = \varphi \cdot \tau$

A generátumok:

$$< \varphi >= \{e, \varphi, \varphi^2\} =< \varphi^2 >, \qquad < \tau >= \{e, \tau\} \qquad < \varphi, \tau >= G$$

Részcsoportok az előbbieken kívül még:

$$< \tau \cdot \varphi >= \{e, \tau \cdot \varphi\} \qquad < \varphi \cdot \tau >= \{e, \varphi \cdot \tau\} \qquad < \varphi, \varphi \cdot \tau >= G =< \varphi \cdot \tau, \tau \cdot \varphi >$$

d. Nem kommutatív a csoport, hiszen például $\tau \cdot \varphi \neq \varphi \cdot \tau$

e. A csoport mindegyik elemének a rendje kisebb, mint a csoport rendje, így egyik elem sem generálja a teljes csoportot, a D_3 csoport tehát nem ciklikus. ■

3.2-16. Tekintsük a 15. példában szereplő síkbeli, szabályos háromszöget önmagába vivő egybevágósági transzformációk G csoportját. Határozzuk meg a részcsoportok rendjét.

Megoldás. Csoport rendje a csoport elemeinek számossága.

részcsoport	részcsoport rendje
$\{e\}$	1
$\{e, \tau\}$	2
$\{e, \varphi \cdot \tau\}$	2
$\{e, \tau \cdot \varphi\}$	2
$\{e, \varphi, \varphi^2\}$	3
$\{e, \varphi, \varphi^2, \tau, \tau \cdot \varphi, \varphi \cdot \tau\}$	6

Megjegyzés. Lagrange-tétele szerint részcsoport rendje osztója a csoport rendjének. Ebben a példában a részcsoportok rendje mind osztója a 6-nak, ami a teljes csoport rendje. ■

3.2-17. Írjuk fel a D_4 diédercsoport elemeit, és a számolás szabályait.

Megoldás. Négyzet esetén legyen φ a középpont körüli $\frac{\pi}{2}$-vel való elforgatás, τ az egyik átlónak megfelelő tengelyre való tükrözés.

$$G = \{e, \varphi, \varphi^2, \varphi^3, \tau, \tau \cdot \varphi, \tau \cdot \varphi^2, \tau \cdot \varphi^3\}$$

A számolás szabályai: $\varphi^4 = \tau^2 = e \qquad \varphi \cdot \tau = \tau \cdot \varphi^3$

■

3.2-18. Bizonyítsuk be, hogy $(G, \cdot)$ csoportban a és a^{-1} rendje egyenlő.

Megoldás. Jelöljük G egységelemét e-vel.

Tegyük fel, hogy $a \in G$ rendje véges, $|a| = n$, ami azt jelenti, hogy

$$a^n = e, \tag{$*$}$$

és a-nak n-nél kisebb pozítív kitevőjű hatványa nem egyenlő e-vel. Vizsgáljuk meg a következő kifejezést, amelyben a^{-1} n-szer szerepel szorzótényezőként, majd a szintén n-szer lép fel:

$$a^{-1} \cdot a^{-1} \cdot \ldots \cdot a^{-1} \cdot a \cdot a \cdot \ldots \cdot a \cdot a$$

Ennek az értéke e, mert középen $a^{-1} \cdot a = e$, s ezt n-szer ismételhetjük. Tehát

$$(a^{-1})^n \cdot a^n = e \tag{$**$}$$

(*) miatt $a^n = e$, s igy $(a^{-1})^n = e$ is teljesül. Ez azt jelenti, hogy $|a^{-1}|$ legfeljebb n. Beláttuk tehát, hogy $|a^{-1}| \leq |a|$.

Az előbbi gondolatmenetet elvégezve mégegyszer úgy, hogy a^{-1} és a szerepét felcseréljük, azt kapjuk, hogy $|a| \leq |a^{-1}|$. Ezt összevetve az előbbivel, ha a rendje véges, (vagy a^{-1} rendje véges), akkor

$$|a^{-1}| = |a|.$$

Ha a és a^{-1} közül az egyik rendje végtelen, akkor az előbbiek szerint a másik rendje is végtelen, tehát megint megegyeznek a rendek. ■

3.2-19. Bizonyítsuk be, hogy $(G, \cdot)$ csoportban az a és $b^{-1} \cdot a \cdot b$ elemek rendje egyenlő.

Megoldás. Jelöljük G egységelemét e-vel.

a. Tegyük fel, hogy $a \in G$ rendje véges, $|a| = n$, ami azt jelenti, hogy

$$a^n = e, \qquad (*)$$

és a-nak n-nél kisebb pozítív kitevőjű hatványa nem egyenlő e-vel. Vizsgáljuk meg a következő kifejezést, amelyben $b^{-1} \cdot a \cdot b$ n-szer szerepel szorzótényezőként.

$$(b^{-1} \cdot a \cdot b) \cdot (b^{-1} \cdot a \cdot b) \cdot \ldots \cdot (b^{-1} \cdot a \cdot b) =$$
$$= b^{-1} \cdot a \cdot b \cdot b^{-1} \cdot a \cdot b \cdot \ldots \cdot b^{-1} \cdot a \cdot b =$$
$$= b^{-1} \cdot a^n \cdot b, \qquad (**)$$

mert az egymás mellett álló b és b^{-1} szorzata e. Másrészt (*) miatt $a^n = e$, és így (**) értéke $b^{-1} \cdot e \cdot b = b^{-1} \cdot b = e$. Ez azt jelenti, hogy $|b^{-1} \cdot a \cdot b|$ legfeljebb n. Beláttuk tehát, hogy $|b^{-1} \cdot a \cdot b| \leq |a|$.

b. Most tegyük fel, hogy $b^{-1} \cdot a \cdot b$ rendje véges, $|b^{-1} \cdot a \cdot b| = n$, ami azt jelenti, hogy

$$(b^{-1} \cdot a \cdot b)^n = e, \qquad (***)$$

és $b^{-1} \cdot a \cdot b$-nek n-nél kisebb pozítív kitevőjű hatványa nem egyenlő e-vel. Az előbb láttuk, hogy

$$(b^{-1} \cdot a \cdot b)^n = b^{-1} \cdot a^n \cdot b.$$

(***) miatt ez e. Tehát

$$b^{-1} \cdot a^n \cdot b = e.$$

Szorozzuk be ezt az egyenletet balról b-vel, jobbról b^{-1}-gyel.

$$a^n = b \cdot e \cdot b^{-1}$$

$$a^n = e$$

Ez azt jelenti, hogy $|a|$ legfeljebb n. Beláttuk tehát, hogy $|a| \leq |b^{-1} \cdot a \cdot b|$, amit összevetve az előbbivel azt kapjuk, hogy ha a rendje véges, (vagy $b^{-1} \cdot a \cdot b$ rendje véges), akkor

$$|a| = |b^{-1} \cdot a \cdot b|.$$

Ha a és $b^{-1} \cdot a \cdot b$ közül az egyik rendje végtelen, akkor az előbbiek szerint a másik rendje is végtelen, tehát megint megegyeznek a rendek. ■

3.2-20. Legyen $(G, \cdot)$ véges, páros rendű csoport. Bizonyítsuk be, hogy G-nek van olyan az egységelemtől különböző eleme, amelynek az inverze önmaga.

Megoldás. Párosítsuk az elemeket saját inverzükkel. Mivel az egységelem inverze önmaga és rajta kívűl páratlan sok elem van, ezért biztosan lesz legalább még egy elem, amelyiknek az inverze önmaga.

Megjegyzés. A példa szerint tehát véges, páros rendű csoportban van másodrendű elem. ■

3.2-21. Bizonyítsuk be, hogy ha $(G, \cdot)$ véges csoport, akkor minden $a \in G$-re

$$a^{|G|} = e,$$

ahol e a csoport egységeleme.

Megoldás. Lagrange-tételének következménye szerint elem rendje osztója a csoport rendjének. Legyen $|a| = n$. Mivel $|a| \big| |G|$, ezért $|G| = n \cdot s$ valamilyen s pozitív egész számmal. Ezek alapján

$$a^{|G|} = a^{n \cdot s} = (a^n)^s = e^s = e$$

■

3.2-22. Egy multiplikatív csoport c elemére $c^{100} = e$ és $c^{1999} = e$. Határozzuk meg c-t.

Megoldás.

1. *megoldás.* Tudjuk, hogy

$$c^{100} = e, \qquad (*)$$

valamint

$$c^{1999} = e. \qquad (**)$$

Ezeket felhasználva

$$c^{1999} = c^{100\cdot 19+99} = (c^{100})^{19} \cdot c^{99} = c^{99}.$$

(**) miatt ez egyenlő e-vel, tehát

$$c^{99} = e. \qquad (***)$$

$$c^{100} = c^{99} \cdot c = e \cdot c = c$$

(*) miatt $c = e$, tehát c maga az egységelem.

2. *megoldás.* Be lehet látni, hogy ha valamely a csoportbeli elemre $a^n = e$, akkor $|a|\big|n$. Ezt felhasználva, (*) miatt $|c|\big|100$, (**) miatt $|c|\big|1999$, s így $|c|\big|(100, 1999) = 1$, tehát c az egységelem. ■

3.2-23. Bizonyítsuk be, hogy ha egy $(G, \cdot)$ csoportnak van az egységelemtől különböző véges rendű eleme, akkor van prímrendű eleme is.

Megoldás. Legyen

$$|a| = n. \qquad (*)$$

Ez azt jelenti, hogy $a^n = e$, és nincs n-nél kisebb pozitív egész szám, amire emelve a-t megkapnánk az egységelemet.

Ha n prím, akkor készen vagyunk, ha nem prím, akkor van p prímosztója, melyre $n = p \cdot k$ valamilyen $1 < k < n$ pozitív egésszel.

$$a^n = a^{k\cdot p} = (a^k)^p = e$$

A korábbiak miatt a^k nem az egységelem, másrészt p-edik hatványa az egységelem. a^k-nak p-nél kisebb pozitív egész kitevőjű hatványa nem adhatja ki az egységelemet, mert az ellentmondana (*)-nak. Tehát a^k prímrendű eleme a csoportnak. ■

3.2.3. Mellékosztályok, invariáns részcsoportok

3.2-24. Tekintsük a 15. példában szereplő síkbeli, szabályos háromszöget önmagába vivő egybevágósági transzformációk G csoportját.

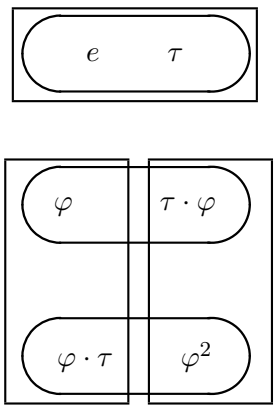
a. Jelölje H a τ által generált részcsoportot. Határozzuk meg G-nek a H szerinti bal, illetve jobb oldali mellékosztályait. Invariáns részcsoportja-e H a G csoportnak?

b. Jelölje K a φ által generált részcsoportot. Határozzuk meg G-nek a K szerinti bal, illetve jobb oldali mellékosztályait. Invariáns részcsoportja-e K a G csoportnak?

Megoldás.

a. $G = \{e, \varphi, \varphi^2, \tau, \tau\cdot\varphi = \varphi^2\cdot\tau, \varphi\cdot\tau = \tau\cdot\varphi^2\}$, $H = \{e, \tau\}$ G részcsoportja.

elem	bal oldali mellékosztályok, $x \cdot H$,	jobb oldali mellékosztályok, $H \cdot x$
e	$e \cdot H = \{e, \tau\}$	$H \cdot e = \{e, \tau\}$
τ	$\tau \cdot H = \{\tau, e\}$	$H \cdot \tau = \{\tau, e\}$
φ	$\varphi \cdot H = \{\varphi, \varphi \cdot \tau\}$	$H \cdot \varphi = \{\varphi, \tau \cdot \varphi\}$
φ^2	$\varphi^2 \cdot H = \{\varphi^2, \tau \cdot \varphi\}$	$H \cdot \varphi^2 = \{\varphi^2, \varphi \cdot \tau\}$
$\varphi \cdot \tau$	$\varphi \cdot \tau \cdot H = \{\varphi \cdot \tau, \varphi\}$	$H \cdot \varphi \cdot \tau = \{\varphi \cdot \tau, \varphi^2\}$
$\tau \cdot \varphi$	$\tau \cdot \varphi \cdot H = \{\tau \cdot \varphi, \varphi^2\}$	$H \cdot \tau \cdot \varphi = \{\tau \cdot \varphi, \varphi\}$

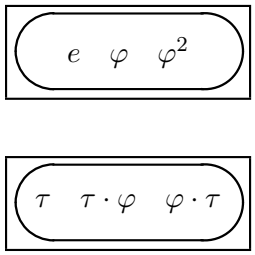


4. ábra. A G csoport H részcsoportja szerinti bal oldali mellékosztályok (téglalapok), és jobb oldali mellékosztályok (oválisok).

H nem invariáns részcsoport G-ben, mert a bal és jobb oldali mellékosztályok nem egyeznek meg.

b. $K =< \varphi >= \{e, \varphi, \varphi^2\}$ részcsoportja G-nek.

elem	bal oldali mellékosztályok, $x \cdot K$,	jobb oldali mellékosztályok, $K \cdot x$
e	$e \cdot K = \{e, \varphi, \varphi^2\}$	$K \cdot e = \{e, \varphi, \varphi^2\}$
τ	$\tau \cdot K = \{\tau, \tau \cdot \varphi, \varphi \cdot \tau\}$	$K \cdot \tau = \{\tau, \varphi \cdot \tau, \tau \cdot \varphi\}$
φ	$\varphi \cdot K = \{\varphi, \varphi^2, e\}$	$K \cdot \varphi = \{\varphi, \varphi^2, e\}$
φ^2	$\varphi^2 \cdot K = \{\varphi^2, e, \varphi\}$	$K \cdot \varphi^2 = \{\varphi^2, e, \varphi\}$
$\varphi \cdot \tau$	$\varphi \cdot \tau \cdot K = \{\varphi \cdot \tau, \tau, \tau \cdot \varphi\}$	$K \cdot \varphi \cdot \tau = \{\varphi \cdot \tau, \tau \cdot \varphi, \tau\}$
$\tau \cdot \varphi$	$\tau \cdot \varphi \cdot K = \{\tau \cdot \varphi, \varphi \cdot \tau, \tau\}$	$K \cdot \tau \cdot \varphi = \{\tau \cdot \varphi, \tau, \varphi \cdot \tau, \}$



5. ábra. A G csoport K részcsoportja szerinti bal oldali mellékosztályok (téglalapok), és jobb oldali mellékosztályok (oválisok).

K invariáns részcsoport G-ben, mert a bal és jobb oldali mellékosztályok megegyeznek.

■

3.2.4. Homomorfizmus, izomorfizmus

3.2-25. A komplex számok $\mathbb{C}$ halmazában a $*$ és $\circ$ műveleteket az alábbi módon értelmezzük:

$$a * b = a + b + 1, \qquad a \circ b = a + b + i.$$

a. Igazoljuk, hogy a $(\mathbb{C}, *)$ és a $(\mathbb{C}, \circ)$ struktúrák csoportok.

b. Igazoljuk, hogy az $\varphi : a \mapsto ai$ leképezés izomorfizmust létesít a $(\mathbb{C}, *)$ és a $(\mathbb{C}, \circ)$ csoportok között.

Megoldás.

a. $(\mathbb{C}, *)$ csoport, mert $*$ művelet a komplex számok halmazán, (ha a és b komplex számok, akkor $a + b + 1$ is az). A művelet asszociatív, egységelem a -1, a inverze $-a - 2$.

$(\mathbb{C}, \circ)$ csoport, mert $\circ$ művelet a komplex számok halmazán, (ha a és b komplex számok, akkor $a + b + i$ is az). A művelet asszociatív, egységelem a $-i$, a inverze $-a - 2i$.

b. Belátjuk, hogy $a \mapsto ai$ izomorfizmust létesít a két csoport között. A leképezés injektív ($ai = bi$-ből következik, hogy $a = b$), szürjektív ($z + iw$-hez van olyan $x + iy$, amelyiknek éppen $z + iw$ a képe), és így bijektív is.

A művelettartás is teljesül:

$$\varphi(a * b) = \varphi(a + b + 1) = ai + bi + i \qquad (*)$$

$$\varphi(a) \circ \varphi(b) = (ai) \circ (bi) = ai + bi + i \qquad (**)$$

Mivel (*) és (**) jobb oldala megegyezik, művelettartó a leképezés (így homomorfizmus), és mivel bijektív is, ezért izomorfizmus. ■

3.2-26. Az alábbi struktúrák közül melyek izomorfak?

a. a valós számok az összeadásra;

b. a pozitív valós számok a szorzásra;

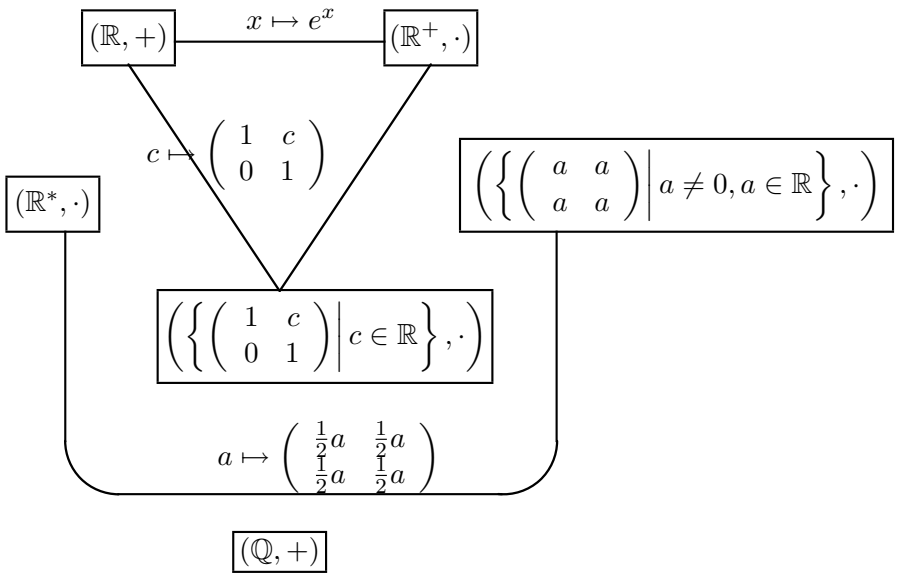
c. a nem nulla valós számok a szorzásra;

d. az $\left\{ \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} \middle| \, c \in \mathbb{R} \right\}$ **mátrixok a mátrixszorzásra;**

e. az $\left\{ \begin{pmatrix} a & a \\ a & a \end{pmatrix} \middle| \, a \neq 0, a \in \mathbb{R} \right\}$ **mátrixok a mátrixszorzásra;**

f. a racionális számok az összeadásra $(\mathbb{Q}, +)$.

Megoldás. A struktúrák közötti kapcsolatokat a 6. ábra mutatja.



6. ábra. A struktúrák közötti kapcsolatok

f. nem izomorf egyikkel sem, mert az alaphalmaz számossága megszámlálható, míg a többi esetben kontinuum, s így nem létezik közöttük bijektív leképezés.

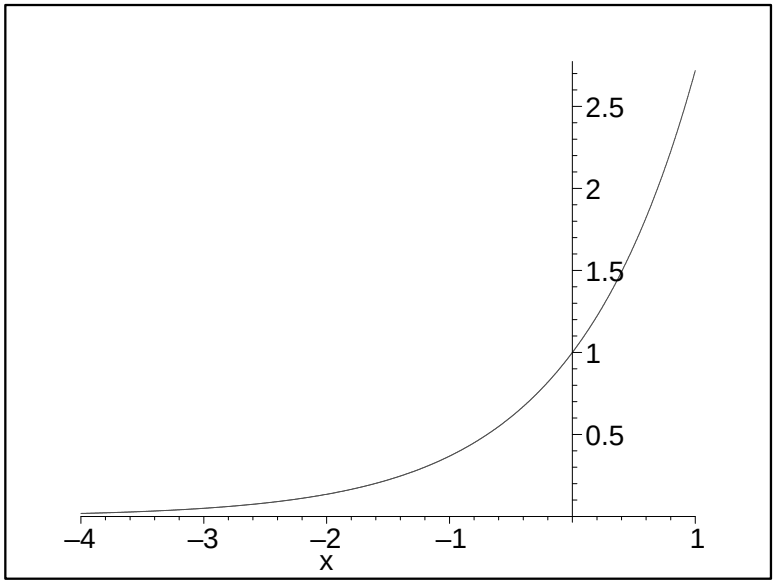
a. izomorf **d.**-vel: nézzük a $c \mapsto \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$ leképezést. Ez egyrészt bijektív, másrészt művelettartó:

$$\varphi\left(c_1 + c_2\right) = \begin{pmatrix} 1 & c_1 + c_2 \\ 0 & 1 \end{pmatrix}$$

$$\varphi(c_1) \cdot \varphi(c_2) = \begin{pmatrix} 1 & c_1 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 1 & c_2 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1 & c_1 + c_2 \\ 0 & 1 \end{pmatrix}$$

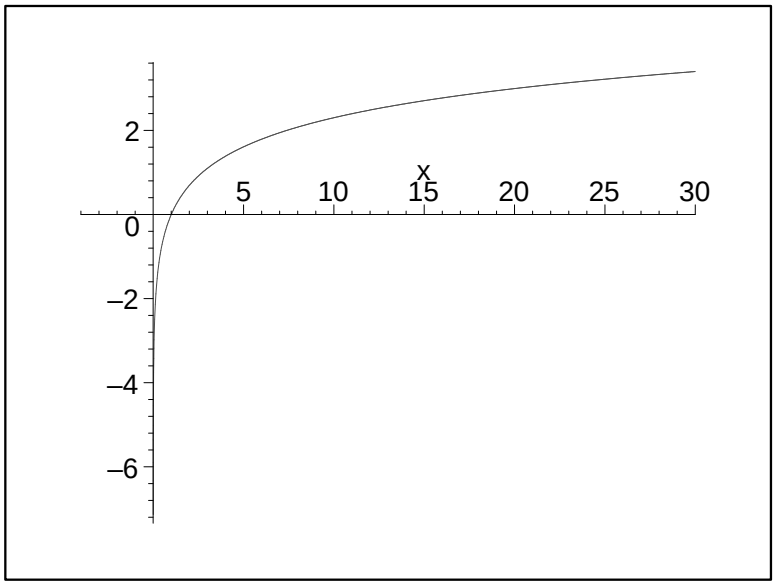
a. izomorf **b.**-vel: az $x \mapsto e^x$ **a.**-ról **b.**-re való leképezés bijektív (lásd a 7. ábrát), és művelettartó:

$$\varphi(x+y) = e^{x+y} = e^x \cdot e^y = \varphi(x) \cdot \varphi(y)$$



7. ábra. Az e^x függvény grafikonja

(Az $x \mapsto ln(x)$ leképezés **b.**-ről **a.**-ra való izomorfizmust valósít meg. Lásd a 8. ábrát.)



8. ábra. Az $ln(x)$ függvény grafikonja

Mivel **a.** izomorf **b.**-vel és **a.** izomorf **d.**-vel, ezért **b.** izomorf **d.**-vel is.

a. nem izomorf **c.**-vel, mert valamely elem rendje, és a képelem rendje izomorfizmusnál meg kell egyezzen. Ha valamely elem rendje véges, akkor a képelem rendje is véges és ugyanakkora. Ha $|a| = n,\ a^n = e$, akkor $\varphi(a^n) = (\varphi(a))^n = e'$, ahol e' a másik struktúra egységeleme. Izomorfizmus esetén ez a másik irányban is elmondható, s így $|a| = |\varphi(a)|$. **a.**-ban csak a 0 rendje véges, míg **c.**-ben végesrendű az 1 és a -1 is.

c. izomorf **e.**-vel. Ha meg akarjuk találni a megfelelő leképezést, vizsgáljuk meg **e.** tulajdonságait. **e.**-n a szorzás művelet, mert

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \cdot \begin{pmatrix} b & b \\ b & b \end{pmatrix} = \begin{pmatrix} 2ab & 2ab \\ 2ab & 2ab \end{pmatrix}$$

Egységelem az

$$\begin{pmatrix} a & a \\ a & a \end{pmatrix} \cdot \begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

és az

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} \cdot \begin{pmatrix} a & a \\ a & a \end{pmatrix} = \begin{pmatrix} a & a \\ a & a \end{pmatrix}$$

egyenletek megoldása. Azt kapjuk, hogy az egységelem.

$$\begin{pmatrix} x & x \\ x & x \end{pmatrix} = \begin{pmatrix} \frac{1}{2} & \frac{1}{2} \\ \frac{1}{2} & \frac{1}{2} \end{pmatrix}$$

Mivel izomorfizmusnál egységelem képe egységelem, az

$$a \mapsto \begin{pmatrix} \frac{1}{2}a & \frac{1}{2}a \\ \frac{1}{2}a & \frac{1}{2}a \end{pmatrix}$$

leképezés látszik megfelelőnek. Ez valóban izomorfizmust biztosít. Egyrészt bijektív, másrészt pedig:

$$\varphi(a) \cdot \varphi(b) = \begin{pmatrix} \frac{1}{2}a & \frac{1}{2}a \\ \frac{1}{2}a & \frac{1}{2}a \end{pmatrix} \cdot \begin{pmatrix} \frac{1}{2}b & \frac{1}{2}b \\ \frac{1}{2}b & \frac{1}{2}b \end{pmatrix} = \begin{pmatrix} \frac{1}{2}ab & \frac{1}{2}ab \\ \frac{1}{2}ab & \frac{1}{2}ab \end{pmatrix} = \varphi(ab)$$

■

3.2-27. Az alábbi csoportok közül melyek izomorfok?

a. a modulo 15 redukált maradékosztályok a szorzásra;

b. a modulo 24 redukált maradékosztályok a szorzásra;

c. a nyolcadik komplex egységgyökök a szorzásra;

d. a négyzet szimmetriacsoportja (a D_4 diédercsoport) a transzformációk egymás utáni végrehajtására, mint műveletre.

Megoldás.

a. A modulo 15 redukált maradékosztályok száma 8, mert $\varphi(15) = 8$.

maradékosztályok	$\overline{1}$	$\overline{2}$	$\overline{4}$	$\overline{7}$	$\overline{8}$	$\overline{11}$	$\overline{13}$	$\overline{14}$
rend	1	4	2	4	4	2	4	2

b. A modulo 24 redukált maradékosztályok száma 8, mert $\varphi(24) = 8$.

maradékosztályok	$\overline{1}$	$\overline{5}$	$\overline{7}$	$\overline{11}$	$\overline{13}$	$\overline{17}$	$\overline{19}$	$\overline{23}$
rend	1	2	2	2	2	2	2	2

c. A nyolcadik komplex egységgyökök elemeinek a száma 8.

egységgyökök	1	ε_1	ε_2	ε_3	ε_4	ε_5	ε_6	ε_7
rend	1	8	4	8	2	8	4	8

d. A négyzet szimmetriacsoportja (a D_4 diédercsoport) 8 elemű.

egységgyökök	e	φ	φ^2	φ^3	τ	$\tau \cdot \varphi$	$\tau \cdot \varphi^2$	$\tau \cdot \varphi^3$
rend	1	4	2	4	2	2	2	2

Izomorfizmusnál a csoportok rendje azonos kell legyen. Ez itt teljesül, mindegyik csoport 8-rendű. Izomorfizmusnál elem rendje megegyezik a képelem rendjével. Ezekben a struktúrákban az elemrendek nem feleltethetők meg íly módon egymásnak, tehát egyik sem izomorf a másikkal. ■

3.3. Gyűrűk

3.3.1. Gyűrű, test, integritási tartomány, nullosztó

3.3-1. Vizsgáljuk meg, hogy gyűrűt alkotnak-e a az alábbi kétműveletes struktúrák:

a. egész számok az összeadásra és a szorzásra nézve;

b. a páros számok az összeadásra és szorzásra nézve;

c. $\left\{a+b\sqrt{2} \,|\, a,b\in\mathbb{Z}\right\}$ **az összeadásra és szorzásra nézve;**

d. $\{a+bi \,|\, a,b\in\mathbb{Z}\}$ **az összeadásra és szorzásra nézve (Gauss-egészek);**

e. $(\mathbb{Z}_m,+,\cdot)$**, a modulo m tekintett maradékosztályok a maradékosztály összeadásra és szorzásra nézve.**

Megoldás. A gyűrű definíciójában szereplő feltételek teljesülését kell megvizsgálni.

a. Két egész szám összege, szorzata egész, így mindkettő művelet. Mindkét művelet asszociatív, kommutatív. Rögzített n,m egész esetén az $n+x=m$ egyenlet megoldható, így az egész számok az összeadással csoportot alkotnak. A disztributivitás szintén teljesül, így a feltételek teljesülnek, a struktúra gyűrű.

b. Két páros szám összege, szorzata páros. Rögzített n,m páros szám esetén az $n+x=m$ egyenlet megoldható, így a páros számok az összeadással csoportot alkotnak. Az előzőek alapján a többi feltétel nyilván teljesül, így ez a struktúra is gyűrű.

c. Jelöljük H-val a vizsgált struktúrát. Elég belátni, hogy H részgyűrűje a valós számok gyűrűjének. Ehhez meg kell mutatni, hogy $(H,+)$ részcsoportja $(\mathbb{R},+)$-nak, és hogy a $\cdot$ művelet. Mivel $(a+b\sqrt{2})-(c+d\sqrt{2})=(a-c)+(b-c)\sqrt{2}$ ezért $H-H\subseteq H$, ami azt jelenti, hogy $H\subseteq\mathbb{R}$ részcsoport $\mathbb{R}$-ben. Így a kommutativitás is nyilván teljesül. Másrészről $(a+b\sqrt{2})(c+d\sqrt{2})=(ac+2bd)+(ad+cb)\sqrt{2}$, ami azt jelenti, hogy a halmaz zárt a szorzásra, $H\cdot H\subseteq H$, tehát részgyűrű $\mathbb{R}$-ben.

d. Hasonlóan látható be, mint az előző példa, csak a komplex számok gyűrűjében kell vizsgálódni, és figyelembe kell venni, hogy $i\cdot i=-1$.

e. $\mathbb{Z}_m$ zárt a maradékosztályokon értelmezett műveletekre, és ezek asszociatív, ill. kommutatív műveletek. Teljesül a disztributivitás, így a csoporttulajdonságot kell csak ellenőrizni az összeadásra vonatkozóan. Mivel az $a+x\equiv b$

(mod m) kongruencia minden a, b egész esetén megoldható, ezért az összeadással $\mathbb{Z}_m$ csoport, így gyűrű is egyben.

■

3.3-2. Teljesüljenek az $(R, +, \cdot)$ struktúrában a következő tulajdonságok:

a. $(R, +)$ csoport,

b. $(R, \cdot)$ egységelemes félcsoport,

c. a szorzás az összeadásra nézve disztributív.

Bizonyítsuk be, hogy $(R, +, \cdot)$ gyűrű.

Megoldás. Be kell látni, hogy $(R, +)$ kommutatív, azaz minden $a, b \in R$ esetén $a + b = b + a$. Nézzük a következő kifejezést: $(e + e)(a + b)$, ahol $e \in R$ az $(R, \cdot)$ félcsoport egységeleme, $a, b \in R$ tetszőleges. Legyen $c = (e + e)$, ill. $d = (a + b)$. A kétoldali disztributivitás miatt egyrészről

$$(e + e)(a + b) = c(a + b) = ca + cb = (e + e)a + (e + e)b = a + a + b + b,$$

másrészről

$$(e + e)(a + b) = (e + e)d = ed + ed = e(a + b) + e(a + b) = a + b + a + b.$$

Azt kaptuk, hogy

$$a + a + b + b = a + b + a + b.$$

Innen az összeadás regularitása miatt $a + b = b + a$. ■

3.3-3. Bizonyítsuk be, hogy ha az $(R, +, \cdot)$ egységelemes gyűrű minden elemének van multiplikatív inverze, akkor a gyűrűnek csak egyetlen eleme van.

Megoldás. Gyűrűben igaz, hogy $a \cdot 0 = 0$ minden $a \in R$ elemre, ahol $0 \in R$ a gyűrű nulleleme. Feltételünkből következik, hogy 0-nak is van multiplikatív inverze, így $0 \cdot 0^{-1} = e$, ahol $e \in R$ a gyűrű egységeleme. De $0 \cdot 0^{-1} = 0$ is teljesül, így $e = 0$. Ekkor minden $a \in R$ elemre $a = a \cdot e = 0$ teljesül. ■

3.3-4. Testet alkotnak-e a mod $2m$ **maradékosztályok közül a párosak, $\{\overline{0}, \overline{2}, \overline{4}, \ldots, \overline{2m-2}\}$ a maradékosztályok közötti összeadásra és szorzásra nézve, ha**

a. $2m = 10$,

b. $2m = 20$.

Megoldás.

a. A szóban forgó halmaz a $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$. Nyilvánvaló, hogy az összeadás asszociatív, kommutatív, hiszen a halmaz a már látott $(\mathbb{Z}_m, +, \cdot)$ gyűrű részhalmaza. Az összeadás művelet, hiszen $(2a + l_1 \cdot 10) + (2b + l_2 \cdot 10) = 2(a+b)+(l_1+l_2)10$, és $(a+b) = c+l\cdot 5$, ahol $0 \leq c \leq 4$, s így $2(a+b) = 2c+l\cdot 10$, ahol $2c$ a $\{0, 2, 4, 6, 8\}$ halmaz egy eleme. Ezek szerint az összeadás művelet, és $\overline{2a} + \overline{2b} = \overline{2(a+b)}$. A halmaz $\overline{0}$ eleme nullelem. Egy $\overline{x}$ elem additív inverze $\overline{2m - x}$ lesz.

Nézzük meg most a szorzás műveletet $(R^*, \cdot)$-ban. A szorzótáblából minden kiolvasható.

$\cdot$	**2**	**4**	**6**	**8**
2	4	8	2	6
4	8	6	4	2
6	2	4	6	8
8	6	2	8	4

A táblázat elemei a hozzájuk tartozó sor, ill. oszlop első elemeinek összeszorzásával kapott maradékosztály reprezentánsát adják meg. Látható, hogy a szorzás művelet, a $\overline{6}$ osztály egységelemmel ($\overline{6} \cdot \overline{2} = \overline{2}$; $\overline{6} \cdot \overline{4} = \overline{4}$; $\overline{6} \cdot \overline{6} = \overline{6}$; $\overline{6} \cdot \overline{8} = \overline{8}$). Egy elem multiplikatív inverze a következőképpen olvasható ki a táblázatból:

Keressük pl. $\overline{8}$ multiplikatív inverzét. Keressük meg a $\overline{8}$ elemhez tartozó sorban a $\overline{6}$ elemet. Jelen esetben ez a $\overline{2}$-höz tartozó oszlopban van, így teljesül a következő: $\overline{8} \cdot \overline{2} = \overline{6}$, azaz $\overline{8}$ multiplikatív inverze $\overline{2}$. A művelet asszociatív és kommutatív is (ld. összeadás műveletnél az indoklást). A két műveletre teljesül a kétoldali disztributivitás, ezért a kapott struktúra test.

b. A szóban forgó halmaz a $\{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}, \overline{10}, \overline{12}, \overline{14}, \overline{16}, \overline{18}\}$. Felírva a szorzótáblát azt találjuk, hogy $\overline{2} \cdot \overline{10} = \overline{0}$, azaz van nullosztó a halmazban, így nem lehet test. ■

3.3-5. Bizonyítsuk be, hogy ha $(T,+,\cdot)$ véges, legalább két elemet tartalmazó integritási tartomány, akkor test.

Megoldás. Be kell látni, hogy $(T^*,\cdot)$ csoport. Mivel T nullosztómentes, ezért ha egy $a \in T^*$ elemet rögzítünk, akkor az $a \cdot x$ kifejezés rendre különböző elemet jelent T^*-ban, ha x helyére T^* különböző elemeit helyettesítjük. Ez azt jelenti, hogy amennyiben $x_1, x_2 \in T^*$, $x_1 \neq x_2$, akkor $a \cdot x_1 \neq a \cdot x_2$ (hiszen ha megegyeznének, $a \cdot x_1 = a \cdot x_2$, akkor mindkét oldalhoz hozzáadva $a \cdot x_1$ inverzét, $a \cdot (x_1 - x_2) = 0$ lenne, de $x_1 - x_2$ nem 0, s így nem lenne nullosztómentes T). Mivel T^* véges, ezért ha x végigfut T^* elemein, akkor $a \cdot x$ is azt teszi. Azt kaptuk, hogy T^*-ban az $a \cdot x = b$ egyenlet megoldható minden $a, b \in T^*$-ra. Innen $(T^*,\cdot)$ csoport, s így a $(T,+,\cdot)$ integritási tartomány test. ■

3.3-6. Határozzuk meg a modulo 12 maradékosztályok gyűrűjében a nullosztókat.

Megoldás. Felírva a szorzótáblát, a táblázat belsejében előforduló 0 elemhez tarozó sor ill. oszlop első elemeiből alkotott párok lesznek a nullosztópárok. Ezek alapján a nullosztópárok a következők:

$(2,6)\,;\ (3,4)\,;\ (6,10)\,;\ (6,8)\,;\ (4,9)\,;\ (6,6)\,;\ (3,8)\,;\ (9,8)\,;\ (4,6).$ ■

3.3-7. Legyen $(R,+,\cdot)$ egységelemes gyűrű, jelölje a nullelemet 0, az egységelemet e. Bizonyítsuk be, hogy ha az $a \in R$ elemre fennáll az $a^n = 0$ valamilyen $n \in \mathbb{N}$-re (a nilpotens), akkor az $e - a$ elemnek van inverze.

Megoldás. Mivel a hatványai és e felcserélhetők, és teljesül a disztributivitás, ezért:

$$(e-a)(e+a+\cdots+a^{n-1}) = e(e+a+\cdots+a^{n-1}) - a(e+a+\cdots+a^{n-1}) =$$

$$= e + a + \cdots + a^{n-1} - a - a^2 - \cdots - a^n =$$

$$= e - a^n = e.$$

Tehát $e - a$ inverze $(e + a + \cdots + a^{n-1})$. ■

3.3-8. Bizonyítsuk be, hogy ha egy $(R, +, \cdot)$ egységelemes gyűrű a elemének van bal oldali multiplikatív inverze, akkor az a elem nem lehet a gyűrű bal oldali nullosztója.

Megoldás. Tegyük fel, hogy a-nak van bal oldali multiplikatív inverze. Ekkor $ab = 0$, $b \neq 0$ nem teljesülhet, hiszen $a^{-1}(ab) = (a^{-1}a)b = b = 0$ is fennállna, ami lehetetlen. ■

3.3.2. Karakterisztika

3.3-9. Mutassuk meg, hogy ha egy R gyűrű minden a elemére $a^2 = a$ teljesül, akkor R kommutatív és karakterisztikája 2.

Megoldás. A feltételünk miatt: $(a + a) = (a + a)^2$. A disztributivitás miatt

$$(a + a)^2 = (a + a)a + (a + a)a = a^2 + a^2 + a^2 + a^2.$$

Ez utóbbira a feltétel miatt:

$$a^2 + a^2 + a^2 + a^2 = a + a + a + a.$$

Mivel $(a + a) = a + a + a + a$, a regularitás miatt $a + a = 0$. Ez teljesül a gyűrű minden elemére, tehát $\mathrm{char}(R) = 2$. A kommutativitás teljesül, mert

$$(a + b) = (a + b)^2$$

teljesül a feltételünk miatt minden $a, b \in R$ esetén, továbbá disztributivitás miatt érvényes a következő :

$$(a + b) = (a + b)^2 =$$

$$= (a + b)a + (a + b)b = a^2 + ba + ab + b^2 = a + ba + ab + b,$$

ezért a regularitás miatt $ba + ab = 0$. Mivel $\mathrm{char}(R) = 2$ ezért $ab + ab = 0$, így $ba = ab$, a szorzás kommutatív. ■

3.3.3. Oszthatóság, osztó, egység, felbonthatatlan, prím

3.3-10.

a. Tekintsük a $\mathbb{Z}_{10}$ maradékosztály-gyűrűt. Írjuk fel ebben minden elem (minden maradékosztály) osztóit.

b. Mik az egységek, és mik a nullosztók?

c. Legyen $\overline{a}$ a $\mathbb{Z}_m$ maradékosztály-gyűrű egy maradékosztálya. Adjunk szükséges és elégséges feltételt arra, hogy mikor osztható minden maradékosztály $\overline{a}$-val - vagyis hogy az $\overline{a}$ maradékosztály mikor egység.

Megjegyzés. $\mathbb{Z}_{10}$ nem nullosztómentes, nem integritási tartomány, de alkalmazható az oszthatóság definíciója.

Megoldás.

a. Írjuk fel a szorzótáblát:

$\cdot$	**0**	**1**	**2**	**3**	**4**	**5**	**6**	**7**	**8**	**9**
0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9
2	0	2	4	6	8	0	2	4	6	8
3	0	3	6	9	2	5	8	1	4	7
4	0	4	8	2	6	0	4	8	2	6
5	0	5	0	5	0	5	0	5	0	5
6	0	6	2	8	4	0	6	2	8	4
7	0	7	4	1	8	5	2	9	6	3
8	0	8	6	4	2	0	8	6	4	2
9	0	9	8	7	6	5	4	3	2	1

Látjuk, hogy a $\overline{0}$ maradékosztálynak minden elem osztója. Az $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$ maradékosztályok minden maradékosztálynak osztói, mert $\{1x : 1 \leq x \leq 10\}$, $\{3x : 1 \leq x \leq 10\}$, $\{7x : 1 \leq x \leq 10\}$, $\{9x : 1 \leq x \leq 10\}$ mindegyike teljes maradékrendszer. Másrészt ezeknek a maradékosztályoknak nincs is több osztójuk, csak az $\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$. A $\overline{2}$, $\overline{4}$, $\overline{6}$, $\overline{8}$ maradékosztályok kölcsönösen osztói egymásnak: $2*2 \equiv 4$, $4*8 \equiv 2$, $2*8 \equiv 6$, $6*2 \equiv 2$, $2*4 \equiv 8$, $8*4 \equiv 2$, $4*4 \equiv$

$6, 6*4 \equiv 4, 4*2 \equiv 8, 8*8 \equiv 4, 6*8 \equiv 8, 8*2 \equiv 6 \pmod{10}$. Ezeknek a maradékosztályoknak az $\overline{5}$ és $\overline{0}$ kivételével minden maradékosztály az osztójuk. Az $\overline{5}$ maradékosztálynak viszont csak az $\overline{1}$, $\overline{3}$, $\overline{5}$, $\overline{7}$, $\overline{9}$ maradékosztályok az osztói.

b. Egységek:$\overline{1}$, $\overline{3}$, $\overline{7}$, $\overline{9}$
Nullosztók: $\overline{2}$, $\overline{4}$, $\overline{6}$, $\overline{8}$, $\overline{5}$

c. Ha a relatív prím m-hez, akkor $\{ax : 1 \leq x \leq m\}$ teljes maradékrendszer modulo m. Tetszőleges b elemhez van tehát olyan x, amelyre $ax = b$. Tehát a osztója minden elemnek. Ha viszont a nem relatív prím m-hez, de b az, akkor nincs olyan x, amelyre $ax = b$, hiszen az $ax \equiv b \pmod{m}$ akkor és csak akkor megoldható, ha $(a, m)|b$. a tehát pontosan akkor egység, ha nem nullosztó, azaz ha $(a, m) = 1$.

■

3.3-11.

a. Felbonthatatlan-e $\mathbb{Z}_{10}$-ben $\overline{5}$?

b. Prím-e $\mathbb{Z}_{10}$-ben $\overline{5}$?

Megjegyzés A 3.3.3. példához hasonlóan itt is kiterjesztjük a prím és felbonthatatlan definícióját tetszőleges egységelemes gyűrűre.

Megoldás.

a. Nem felbonthatatlan, hiszen $\overline{5} \cdot \overline{5} = \overline{5}$, ugyanis $5 \equiv 5^2 \pmod{10}$ és $\overline{5}$ nem egység $\mathbb{Z}_{10}$-ben. (lásd 3.3.3. példa)

b. $\overline{5}$ prím $\mathbb{Z}_{10}$-ben, hiszen ha $\overline{5}|\overline{a} \cdot \overline{b}$, akkor $\overline{5}|\overline{a}$ vagy $\overline{5}|\overline{b}$.

■

3.3-12. Lássuk be, hogy testben minden, a nullelemtől különböző elem egység.

Megoldás. Legyen $(T, +, \cdot)$ test. Ekkor $(T^*, \cdot)$ csoport, tehát T^*-ban megoldható az $ax = b$ egyenlet bármely $a, b \in T^*$ esetén, ami azt mutatja, hogy T^* minden eleme egység. ■

3.3.4. Euklideszi gyűrű

3.3-13. Lássuk be, hogy ha integritási tartományban létezik prím, akkor van egységelem.

Megoldás. Legyen p egy prímelem. Ekkor az oszthatóság definíciója alapján $p|p \cdot p$. Mivel p prím, ezért $p|p$ is teljesül. Ekkor pedig van egy ϵ elem a gyűrűben, melyre $\epsilon p = p$ is teljesül. Szorozzuk be egy a elemmel az egyenlőséget. Ekkor $a\epsilon p = ap$ miatt $(a\epsilon - a)p = 0$ kell teljesüljön, vagyis $a\epsilon - a = 0$, hiszen nincsenek nullosztók az integritási tartományban. Tehát $a\epsilon = a$ minden a elemre teljesül, tehát ϵ egységelem.

■

3.3-14. Legyen $L := \{a + bi\sqrt{5} \mid a, b \in \mathbb{Z}\}$ a szokásos műveletekkel.

a. Bizonyítsuk be, hogy az L egészek körében $1+i\sqrt{5}$, $1-i\sqrt{5}$, 2, 3 felbonthatatlan elemek, de nem prímelemek.

b. Bizonyítsuk be, hogy az $(L, +, \cdot)$ gyűrű nem euklideszi gyűrű.

Megoldás.

a. Mivel $(1 + i\sqrt{5})(1 - i\sqrt{5}) = 1 + 5 = 6 = 2 \cdot 3$ ezért $1 \pm i\sqrt{5} | 2 \cdot 3$, de a $(1 \pm i\sqrt{5})(a + bi\sqrt{5})$ kifejezés nem veheti fel a $2, 3$ értékeket, ha a, b egészek. Ez azt jelenti, hogy $1 \pm i\sqrt{5} \not| 2$ és $1 \pm i\sqrt{5} \not| 3$, azaz egyik sem prím. Ugyanezt a gondolatmenetet 2-re és 3-ra alkalmazva látjuk, hogy ezek sem prímek.

Ha $1 + i\sqrt{5} = \alpha\beta$, akkor $(1 + i\sqrt{5})(1 - i\sqrt{5}) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\,\overline{\beta}$ is teljesül. Mivel $(1+i\sqrt{5})(1-i\sqrt{5}) = 6$ és $\alpha\overline{\alpha}$, $\beta\overline{\beta}$ egészek, ezért $\alpha\overline{\alpha}\beta\overline{\beta} = 1 \cdot 6$ vagy $2 \cdot 3$. Mivel $\alpha\overline{\alpha} = (a + bi\sqrt{5})(a - bi\sqrt{5}) = a^2 + 5b^2 = 2$ nem teljesül a, b egészek esetén, ezért az $\alpha\overline{\alpha}\beta\overline{\beta} = 2 \cdot 3$ felbontás nem jöhet szóba. Mivel α és β szerepe felcserélhető, ezért mondjuk $\alpha = a + bi\sqrt{5}$ jelöléssel $1 = \alpha\overline{\alpha} = a^2 + 5b^2$, ami csak úgy lehet, ha $a = \pm 1$, azaz α egység. Azt kaptuk, hogy ha $1+i\sqrt{5} = \alpha\beta$, akkor α vagy β egység.

b. Az előbbiek miatt L nem lehet euklideszi gyűrű, hiszen ott a prímek és felbonthatatlanok ugyanazok az elemek lesznek. ■

3.3.5. Részgyűrű, ideál, faktorgyűrű

3.3-15. Melyek $(\mathbb{Z}_4, +, \cdot)$ részgyűrűi? Van-e köztük ideál?

Megoldás. A $\{\overline{0}\}$ részgyűrű, hiszen $I - I \subseteq I$ és $I \cdot I \subseteq I$. Egyben ideál is, hiszen $\overline{0} - \overline{0} = \overline{0}$ és $\overline{r} \cdot \overline{0} = \overline{0}$. $\{\overline{0}, \overline{2}\}$ részgyűrű, hiszen $I - I \subseteq I$ és $I \cdot I \subseteq I$. Egyben ideál is, hiszen $\overline{0} - \overline{2} = \overline{2}$ és $\overline{r} \cdot \overline{2} = \overline{0}$ vagy $\overline{2}$ attól függően, hogy r páros, vagy páratlan. Az előzőekhez hasonlóan $\{\overline{0}, \overline{1}, \overline{2}, \overline{3}\}$ részgyűrű és egyben ideál is. Nem részgyűrű, és így ideál sem lehet pl. $\{\overline{0}, \overline{2}, \overline{3}\}$, hiszen $\overline{2} + \overline{3} = \overline{1}$ és $\overline{1}$ nincs benne az előbb megadott halmazban. ■

3.3-16. Legyen R véges gyűrű, I ideál R-ben, és $R \neq I$. Bizonyítsuk be, hogy I minden nullelemtől különböző eleme nullosztó R-ben.

Megoldás. Legyen $i \in I$ nem nullelem. Ekkor az ri kifejezés nem vehet fel csupa különböző értékeket, ha r végigfut R elemein (ugyanis $ri \in I$, ha $r \in R$ mivel I ideál), különben R végessége miatt $R = I$ is fennállna. Ekkor viszont van olyan $r_1, r_2 \in R$, $r_1 \neq r_2$ pár, hogy $r_1 i = r_2 i$. Ez pedig azt jelenti, hogy $(r_1 - r_2)i = 0$, s így i nullosztó R-ben. ■

3.3-17. Határozzuk meg $(T, +, \cdot)$ ideáljait, ha T tetszőleges test. (Lássuk be, hogy testben nincs nem triviális ideál.)

Megoldás. Nyilvánvaló, hogy $\{0\}$ és T ideálok T-ben. Más ideál nincs, hiszen ha $\{0\} \neq I \subseteq T$ ideál, akkor egy $0 \neq t \in I$ elemre $e = t^{-1}t \in I$ is teljesül. Ekkor viszont $T = T\{e\} \subseteq TI \subseteq I$ miatt $I = T$. ■

3.3-18.

a. Lássuk be, hogy a páros számok halmaza (P) az egész számok gyűrűjének részgyűrűjét, sőt ideálját alkotja.

b. Határozzuk meg a $\mathbb{Z}/P$ maradékosztály-gyűrűt.

Megoldás.

a. Páros számok különbsége páros, így $P - P \subseteq P$ teljesül. Páros számot egész számmal szorozva szintén páros számot kapunk, ezért $\mathbb{Z}P \subseteq P$, és $P\mathbb{Z} \subseteq P$.

b. Meg kell keresni a $\mathbb{Z}$ gyűrű P ideál szerinti osztályait. Mivel $0 \in \mathbb{Z}$ ezért lesz egy osztály, amely a $0+P$-nek felel meg (páros számok halmaza). Ezt az osztályt jelölje $\overline{0}$. Ebbe az osztályba az 1 szám nem tartozik bele. Ezek szerint van egy másik osztály is, ami az $1+P$ osztály. Jelölje ezt $\overline{1}$ (páratlan számok). Látható, hogy a két osztály diszjunkt, és egyesítésük kiadja az egész számok halmazát. Azt kaptuk, hogy $\mathbb{Z}/P$ kételemű, és elemei: $\overline{0}$, $\overline{1}$. ■

3.3-19. Legyen $R = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in \mathbb{Z} \right\}$, **és** $I = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in 2\mathbb{Z} \right\}$

a. Mutassuk meg, hogy I ideál R-ben.

b. Hány elemű az R/I faktorgyűrű?

Megoldás.

a. A mátrix összeadás definíciója alapján két I-beli mátrix összegének elemeit úgy kapjuk meg, hogy az összeadandó mátrixok megfelelő elemeit adjuk össze. Mivel ez utóbbiak páros számok, ezért az összeg elemei is párosak lesznek. Ez azt jelenti, hogy $I-I \subseteq I$ teljesül. Meg kell még vizsgálni $RI \subseteq I$ feltétel teljesülését is. $M \in R$, $S \in I$ esetén legyen $\quad M = \begin{pmatrix} m_{11} & m_{12} \\ m_{21} & m_{22} \end{pmatrix}; \quad S = \begin{pmatrix} s_{11} & s_{12} \\ s_{21} & s_{22} \end{pmatrix}.$

Ekkor

$$MS = \begin{pmatrix} m_{11}s_{11} + m_{12}s_{21} & m_{11}s_{12} + m_{12}s_{22} \\ m_{21}s_{11} + m_{22}s_{21} & m_{21}s_{12} + m_{22}s_{22} \end{pmatrix}$$

ezért MS elemei is párosak, hiszen S elemei párosak, azaz $MS \in I$, vagyis $RI \subseteq I$. Mivel

$$SM = \begin{pmatrix} s_{11}m_{11} + s_{12}m_{21} & s_{11}m_{12} + s_{12}m_{22} \\ s_{21}m_{11} + s_{22}m_{21} & s_{21}m_{12} + s_{22}m_{22} \end{pmatrix},$$

ezért az előző gondolatmenettel kapjuk, hogy $IR \subseteq I$, így I ideál R-ben.

b. Az előző példa módszerét követve $\mathbf{0} \in R$ beletartozik az egyik osztályba, ahol $\mathbf{0}$ a csupa nullákat tartalmazó mátrix. Van tehát egy osztályunk, amit $\overline{\mathbf{0}}$-val jelölve a $\mathbf{0}+I$ formulával adhatunk meg. Nyilvánvaló, hogy ebbe az

osztályba a csupa páros elemekből álló mátrixok tartoznak. Ha ebben az osztályban megváltoztatjuk egy elem paritását, akkor az egy másik osztályba fog tartozni. Másrészről, ha $M \in R$ beletartozik egy osztályba, akkor azok a mátrixok amelyben az elemek paritása megegyezik az M mátrix azonos indexű elemeinek paritásával, ugyanebbe az osztályba tartoznak. Ezek alapján annyi osztály van, ahányféleképpen a mátrix elemeinek paritását lényegesen különböző módon megválaszthatjuk. Ha egy elem paritását változtatjuk, akkor ezt $\binom{4}{1}$ féleképpen tehetjük meg. Ugyanígy ha két elem paritását változtatjuk, akkor $\binom{4}{2}$ lehetőségünk van. Ezekhez hozzá kell adni a 3, ill. 4 elemhez tarozó kombinációk számát, azaz $\binom{4}{1} + \binom{4}{2} + \binom{4}{3} + \binom{4}{4} = 2^4$ osztály van.

Másképp: mivel 4 elemű mátrixokról van szó, és a paritás kétféle lehet, ezért itt egy 2 elemű 4-ed osztályú ismétléses variációról van szó, 2^4 különböző osztály van. ■

3.3-20. Jelöljük N-nel az R kommutatív gyűrűben a nullosztók és a 0 által alkotott halmazt.

a. Lehet-e, hogy N nem részgyűrű?

b. Lehet-e, hogy N részgyűrű, de nem ideál?

c. Bizonyítsuk be, hogy ha N ideál, akkor R/N nullosztómentes.

Megoldás.

a. Lehet, pl. $\mathbb{Z}_6$-ban $\overline{2}, \overline{3} \in N$, de $\overline{2} + \overline{3} \notin N$

b. Nem lehet, mert ha $n \in N \setminus \{0\}$, akkor ha $m \in M \setminus \{0\}$ a nullosztópárja, akkor $\forall r \in R \setminus \{0\}$ esetén $(rn)m = r(nm) = 0$ teljesül, és így $rn \in R$ is nullosztó vagy 0, azaz $RN \subseteq N$.

c. R/N nullelemét alkotó osztály N, hiszen N szerint osztályoztunk. Ezek szerint ha $a_1, a_2 \in R \setminus N$ akkor $a_1 a_2 \notin N$ miatt $(a_1+N)(a_2+N) = (a_1 a_2+N)$ különbözik N-től, a nullelemtől, s így $a_1 + N$ és $a_2 + N$ nem nullosztók. ■

3.3.6. Homomorfizmus, izomorfizmus

3.3-21. Legyen $M = \left\{ \begin{pmatrix} a & b \\ 2b & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$**. Bizonyítsuk be, hogy az** $(M, +, \cdot)$ **struktúra izomorf az** $E = (\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \cdot)$ **gyűrűvel.**

Megoldás. Legyen $a, b \in \mathbb{Z}$, és $\varphi : M \to E$ olyan, hogy $\varphi\left(\begin{pmatrix} a & b \\ 2b & a \end{pmatrix}\right) = a + b\sqrt{2}$. Ez a függvény nyílván bijektív, hiszen minden $a + b\sqrt{2}$ számhoz van egy M-beli mátrix, és csak egy ilyen van. Nézzük a művelettartást.

$$\varphi\left(\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} + \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a_1 + a_2 & b_1 + b_2 \\ 2(b_1 + b_2) & a_1 + a_2 \end{pmatrix}\right) =$$

$$= (a_1 + a_2) + (b_1 + b_2)\sqrt{2} =$$

$$= a_1 + b_1\sqrt{2} + a_2 + b_2\sqrt{2} = \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix}\right) + \varphi\left(\begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix}\right)$$

Másrészről:

$$\varphi\left(\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix} \cdot \begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix}\right) = \varphi\left(\begin{pmatrix} a_1a_2 + 2b_1b_2 & a_1b_2 + b_1a_2 \\ 2(a_1b_2 + b_1a_2) & a_1a_2 + 2b_1b_2 \end{pmatrix}\right) =$$

$$= (a_1a_2 + 2b_1b_2) + (a_1b_2 + b_1a_2)\sqrt{2} =$$

$$= (a_1 + b_1\sqrt{2})(a_2 + b_2\sqrt{2}) = \varphi\left(\begin{pmatrix} a_1 & b_1 \\ 2b_1 & a_1 \end{pmatrix}\right) \cdot \varphi\left(\begin{pmatrix} a_2 & b_2 \\ 2b_2 & a_2 \end{pmatrix}\right)$$

■

3.3-22. Izomorfak-e a következő gyűrűk?

$$G = (\{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}, +, \cdot) \quad \textbf{és} \quad K = (\{a + b\sqrt{3} \mid a, b \in \mathbb{Z}\}, +, \cdot)$$

Megoldás. Nem izomorfak, ugyanis ha azok lennének, akkor φ-val jelölve az izomorfizmust G és K között a következőknek is teljesülniük kellene: Mivel $\varphi(u) = \varphi(1 \cdot u) = \varphi(1)\varphi(u)$ minden $u \in G$-re, ezért $\varphi(1) = 1$, $\varphi(2) = \varphi(1 + 1) = \varphi(1) + \varphi(1) = 1 + 1 = 2$. Indukcióval következik, hogy $\varphi(m) = m$

minden $m \in \mathbb{Z}$-re. Mivel G-ben megoldható az $x^2 = 2$ egyenlet, ezért $\varphi(x^2) = \varphi(2) = 2$ teljesül K-ban. Tehát

$$\varphi(x^2) = (\varphi(x))^2 = 2 \tag{3.1}$$

kellene teljesüljön. Legyen $\varphi(x) = a + b\sqrt{3}$
Ebből

$$(a + b\sqrt{3})^2 = 2$$
$$a^2 + 2ab\sqrt{3} + 3b^2 = 2$$

amiből

$$a^2 + 3b^2 = 2 \tag{3.2}$$

és

$$2ab = 0 \tag{3.3}$$

együtt kellene teljesüljön. (3.2)-ből $b^2 = 0$, és $a^2 = 2$ következik. Mivel a egész szám, ez ellentmondás. (3.1)-nek tehát nincs megoldása K-ban, s így G és K között nem létezik izomorf leképezés. ■

4. Ajánlott irodalom

Bagyinszkiné Orosz Anna – Csörgő Piroska – Gyapjas Ferenc:
Példatár a bevezető fejezetek a matematikába c. tárgyhoz
Tankönyvkiadó, Budapest, 1983.

Bálintné Szendrei Mária – Czédli Gábor – Szendrei Ágnes:
Absztrakt algebrai feladatok
Tankönyvkiadó, Budapest, 1988.

Elekes György: *Kombinatorika feladatok*
ELTE jegyzet, 1992.

Freud Róbert: *Lineáris algebra.*
ELTE Eötvös Kiadó, Budapest, 1996.

Hajnal Péter: *Elemi kombinatorikai feladatok*
Polygon, Szeged 1997.

Surányi László: *Algebra. Testek, gyűrűk, polinomok.*
Typotex, Budapest, 1997.