

Absztrakt algebrai feladatgyűjtemény

Dr. Szalkai István
Veszprémi Egyetem, 2004.

2004.02.09.

Tartalomjegyzék

1	Feladatok	1
1.1	Halmazok, relációk, függvények	1
1.1.1	Halmazok	1
1.1.2	Relációk	1
1.1.3	Függvények, műveletek	5
1.2	Általános struktúrák	6
1.3	Félcsoportok és csoportok	7
1.3.1	Gruppoidok, félcsoportok	7
1.3.2	Speciális elemek félcsoportokban	8
1.3.3	Csoportok	9
1.3.4	Szimmetria- és permutációcsoportok	9
1.4	Gyűrűk	10
1.4.1	Alapfogalmak	10
1.4.2	A $\mathbb{Z}_m$ maradékosztályok	11
1.4.3	Euklideszi gyűrűk	14
1.5	Testek	16
1.6	Boole-algebrák, hálók	17
2	Megoldások	19
2.1	Halmazok, relációk, függvények	19
2.1.1	Relációk	19
2.1.2	Függvények, műveletek	20
2.2	Általános struktúrák	20
2.3	Félcsoportok és csoportok	21
2.3.1	Gruppoidok, félcsoportok	21
2.3.2	Speciális elemek félcsoportokban	22
2.3.3	Csoportok	23
2.3.4	Szimmetria- és permutációcsoportok	23
2.4	Gyűrűk	24
2.4.1	A $\mathbb{Z}_m$ maradékosztályok	24
2.4.2	Euklideszi gyűrűk	27

2.5	Testek	35
Függelék		37
.1	Jelölések, definíciók	37
.2	Felhasznált és ajánlott irodalom	40

Fejezet 1

Feladatok

SK:>D:>\Szalkai\Sk-muvek\AlgFgy\5\AlgFgy5i-diak.tex., 2004.02.09., 20:00'

1.1 Halmazok, relációk, függvények

1.1.1 Halmazok

- 1) Adjon meg *öt* (minőségileg) független halmazt⁽¹⁾ az $\mathbb{I}_{32} = \{0, 1, \dots, 31\}$ halmazon!
Ld. még [SzI] 1. fejezetét.

1.1.2 Relációk

- 1) Adja meg az alábbi relációk alaphalmazát és típusát:
- a) n prímszám, páros egész szám,
 - b) x negatív valós szám,
 - c) a sík/tér két pontja *kollineáris* (egy egyenesbe esnek),
 - d) a sík/tér három pontja kollineáris,
 - e) a tér négy pontja *koplanáris* (egysíkú),
 - f) $\underline{u}_1, \dots, \underline{u}_n \in V$ lineárisan független vektorok a V vektortérben,
 - g) $A \subseteq B$ ahol A, B tetszőleges halmazok,
 - h) $A \subseteq B$ ahol $A, B \subseteq X$ egy adott $X \neq \emptyset$ rögzített halmaz részhalmazai,
 - i) $f = \mathcal{O}(g)$ ("nagy ordó" - ld. Algoritmuselmélet alapjai),
a következő relációkban $x, y \in \mathbb{N}$ természetes számok
 - j) x és y *relatív prímek*⁽²⁾,
 - k) $x \sim_k y$ ha $3 \mid x + y$,

¹⁾ **Definíció:** az $A_1, \dots, A_k$ halmazok **minőségileg függetlenek**, ha tetszőleges $\varepsilon_1, \dots, \varepsilon_k \in \{+1, -1\}$ esetén $A^{\varepsilon_1} \cap \dots \cap A^{\varepsilon_k} \neq \emptyset$ ahol $A^{+1} = A$ és $A^{-1} = \bar{A}$. $\square$

²⁾ **Definíció:** $x, y \in \mathbb{Z}$ **relatív prímek** ha $\text{luko}(x, y) = 1$. $\square$

- l) $x \sim_\ell y$ ha $x \mid 2 - y$,
 m) $x \sim_m y$ ha $x = y^2$,
 n_i) $x \sim_{ni} y$ ha $i \mid a^2 - b^2$ ($i = 1, 2, 3, \dots$ esetén) ,
 o_i) $x \sim_{oi} y$ ha $i \nmid a^2 - b^2$ ($i = 1, 2, 3, \dots$ esetén) ,
 p)
 q)
 r) .

2) Vizsgálja meg az előző feladatban szereplő és az alábbi *bináris* relációk tulajdonságait (reflexív, irreflexív, szimmetrikus, antiszimmetrikus, tranzitív, teljes, ekvivalencia, rendezés, sűrű- ill. jól-rendezés). Az ekvivalencia relációk esetében adja meg az ekvivalencia osztályokat és egy lehetséges reprezentáns-rendszert (az alaphalmaz faktorizációját) is!

- a) $H :=$ egy osztály tanulói, $X \sim_a Y$ ha egyneműek,
 b) $E :=$ emberek, $X \sim_b Y$ ha barátok,
 c) $F :=$ földrajzi nevek, $X \sim_F Y$ ha az X város az Y folyó partján épült,
 d) $C :=$ városok, $X \sim_C Y$ ha az X várost vízi út köti össze az Y várossal,
 e) $V :=$ egy gráf csúcsai, $X \sim_c Y$ ha van út X és Y között,
 f) $a \mid b$ ha $a, b \in \mathbb{Z}$ egész számok és a osztója b -nek,
 g) $a \mid b$ ha $a, b \in \mathbb{N}$ természetes számok,
 h) $a \equiv_m b$ ha $m \mid a - b$, $a, b, m \in \mathbb{Z}$ egész számok, m rögzített, (vizsgálja meg külön az $m = 0$, $m = 1$ speciális eseteket),
 i₁) $a \sim_m b$ ha $|a - b| \leq m$ ($a, b \in \mathbb{Z}$, $m \in \mathbb{N}$ tetszőleges rögzített), (vizsgálja meg külön az $m = 0$ és $m \neq 1$ eseteket),
 i₂) $a \sim_{i2} b$ ha $0 \leq a - b \leq 6$ ($a, b \in \mathbb{Z}$),
 j) $e \parallel f$ ha az e és f síkbeli/térbeli egyenesek párhuzamosak,
 k) $u \parallel v$ ahol $u, v \in V$ egy (tetszőleges) $V \neq \{\emptyset\}$ vektortér vektorai⁽³⁾,
 l) $x \sim_{\mathbb{Q}} y$ ha $x, y \in \mathbb{R}$ valós számok és $x - y \in \mathbb{Q}$,
 m) $A \sim B$ ha $A, B \in \mathbb{R}^{n \times n}$ és $B = C \cdot A \cdot C^{-1}$ valamely $C \in (\mathbb{R}^{n \times n})^*$ invertálható mátrixra (**mátrixok hasonlósága**),
 n) $\iota := \{ (a, a) \mid a \in A \}$ (**egyenlőség**),
 o) $\Delta := A \times A$ (**azonosság**), A tetszőleges halmaz,
 p₁) $A \sim_{p1} B$ ha az A és B síkidomok *végyszerűen egyenlőek*⁽⁴⁾ ,

³⁾ **Definíció:** Az $u, v \in V$ (absztrakt) vektorok **párhuzamosak**, vagyis $u \parallel v$, ha $u = \lambda v$ vagy $v = \mu u$ valamely $\lambda \in \mathbb{R}$ vagy $\mu \in \mathbb{R}$ valós számra. $\square$

Például: $\sin(3x) \parallel e^{3x}$ és $\sin(3x) \parallel 7 \sin(3x) + 2$ de $\sin(3x) \nparallel 7 \sin(3x)$.

⁴⁾ Bolyai Farkas **definíciója**: Két síkidom **végyszerűen egyenlő**, ha véges számú, páronként egybevágó darabokra (diszjunkt részhalmazokra) oszthatók. *Azaz*: bármelyik síkidomot ollóval feldarabolhatjuk (nem csak egyenes vágásokkal) úgy, hogy a részekből a másik síkidom kirakható. $\square$

- $p_2)$ $A \sim_{p_2} B$ ha az A és B síkidomok *hasonlóak*,
 $p_3)$ $A \sim_{p_3} B$ ha az A és B síkidomok *egybevágóak*,
 $p_1)$ $A \sim_{p_4} B$ ha az A és B síkidomok *területe egyenlő*,
 $q)$

3) Adja meg az előző feladatban szereplő *ekvivalencia relációk* által meghatározott partíciókat és ekvivalencia-osztályokat!

4) Legyen $R \subset (\mathbb{Z}^- \times \mathbb{Z}^-)^2$ a következő reláció:

$$(a, b) R (c, d) \stackrel{def}{\iff} ad = bc \quad .$$

Mutassa meg, hogy R ekvivalencia reláció, és

$$\mathbb{Z}^- \times \mathbb{Z}^- / R \cong \mathbb{Q} \setminus \{0\} \quad .$$

5) Rajzolja fel az alábbi $\rho \subseteq \mathbb{R}^2$ relációk gráfjait:

- $a)$ $x = y$, $x < y$, $x \leq y$,
 $b)$ $x \equiv_m y$ ($x, y, m \in \mathbb{Z}$ egész számok) ,
 $c)$
 $d)$

6) Az alábbi rajzon mely $\tau \subseteq \mathbb{R}^2$ relációk gráfjait láthatjuk? Adjuk meg a megadott relációk tulajdonságait!

.

.

.

.

.

7) Hogyan olvashatók le relációk gráfjairól a relációk tulajdonságai (mint pl. reflexív, szimmetrikus, teljes, antiszimmetrikus, stb.) ?

8) Keressen olyan relációt, amely

- $a)$ reflexív, szimmetrikus de nem tranzitív,
 $b)$ reflexív, nem szimmetrikus és nem tranzitív,
 $c)$ reflexív, antiszimmetrikus és nem tranzitív,
 $d)$ nem reflexív, szimmetrikus de nem antiszimmetrikus és tranzitív,
 $e)$ nem reflexív, nem szimmetrikus de tranzitív.

9) Legyen $W \leq V$ altér a V vektortérben.

a) Mutassa meg, hogy $\Pi := \{W + y \mid y \in V\}$ *partíciója* V -nek,

b) Adja meg az $x \sim_{\Pi} y$ relációt.

10)* Vizsgálja meg a különböző *modulusokhoz* tartozó $\equiv_m$ relációk kapcsolatát (tartalmazás szempontjából), azaz melyik *finomabb*, melyik *durvább*⁽⁵⁾?

11)* Mely $A \subseteq \mathbb{R}$ részhalmaz esetén lesz a $\sim_A \subseteq \mathbb{R}^2$ reláció ekvivalencia, ha tetszőleges $x, y \in \mathbb{R}$ valós számok esetén $x \sim_A y \stackrel{def}{\iff} x - y \in A$.

12)** Vizsgálja meg, hogy a (1.3.2) fejezet 6*) feladatában szereplő reláció mely struktúrákban ekvivalencia, és adja meg az ekvivalenciaosztályokat ezekben a struktúrákban!

13) Van-e legkisebb/minimális/legnagyobb/maximális elem az 1) feladatban található rendezett halmazokban? Adja meg ezeket az elemeket!

14) Az alábbi relációk közül melyek rendezések, teljesek, sűrű- ill. jól-rendezések? Melyikben van legkisebb/minimális/legnagyobb/maximális elem?

a) $<$ és $\leq \subseteq \mathbb{R}^2$, $\leq \subseteq \mathbb{Q}^2$,

b) $\leq \subseteq \mathbb{N}^2$ és $\leq \subseteq \mathbb{Z}^2$,

c) $|\mathbb{N}| \subseteq \mathbb{N}^2$ és $|\mathbb{Z}| \subseteq \mathbb{Z}^2$ (oszthatóság),

d)

e)

15)a) Tegye teljessé az $|\mathbb{N}| \subseteq \mathbb{N}^2$ és $|\mathbb{Z}| \subseteq \mathbb{Z}^2$ és (oszthatóság) parciális rendezéseket!

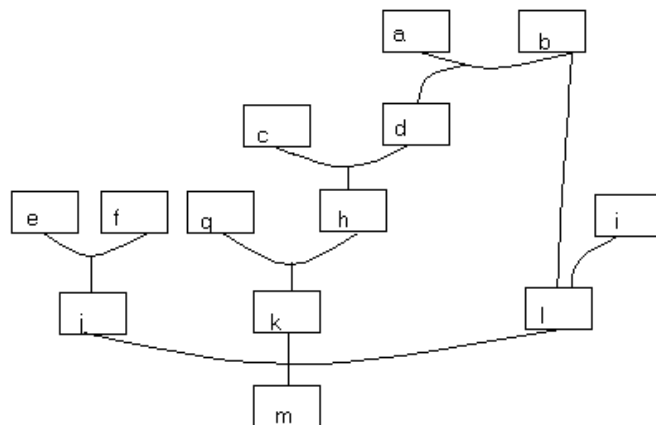
b) Vizsgálja meg az $|\mathbb{Z}|$ és a $|\mathbb{Z}| \subseteq \mathbb{Z}^2$ ($\mathbb{Z}$ mint 1-dimenziós algebra⁽⁶⁾ $\mathbb{Z}$ felett).

16) Adja meg az $(\mathbb{N}, |)$ és $(\mathbb{R}, \leq)$ rendezett halmazokban tetszőleges véges H részhalmaz supremumát és infimumát!

17)* Legyenek $x_1 < x_2 < x_3 < x_4 < x_5$ tetszőleges (nem ismert) különböző valós számok. Tekintsük az $A := \{x_i + x_j : 1 \leq i < j \leq 5\}$ alaphalmazon a szokásos $\leq$ rendezést. Rajzolja fel a $< A, \leq >$ rendezett halmaz gráfját!

⁵⁾ **Definíció:** az $R, S \subseteq A^n$ relációk közül R **finomabb** mint S , vagyis S **durvább** mint R ha $R \subseteq S$, azaz xRy esetén xSy . *Másképpen:* R osztályai részhalmazai S osztályainak: $[a]_R \subseteq [a]_S$ minden $a \in A$ esetén. $\square$

⁶⁾ **Definíció:** a V_{Γ} struktúrát **algebrának** nevezzük, ha teljesíti a vektortér axiómáit, de Γ -ról csak annyit követelünk meg, hogy gyűrű legyen. $\square$



ábra 1.1:

18)* Keressünk a szokásostól eltérő *rendezési* relációkat az $\mathbb{N}$, $\mathbb{Z}$ és $\mathbb{R}$ számhalmazokhoz.

1.1.3 Függvények, műveletek

1) Legyen $(L, \preccurlyeq)$ egy tetszőleges jólrendezett⁽⁷⁾ halmaz. Vizsgáljuk meg L -en a következő műveletet:

$$a * b := S(b) \quad (a, b \in L) \quad .$$

.

.

.

⁷⁾ **Definíció:** az $(L, \preccurlyeq)$ rendezett halmaz **jólrendezett**, ha tetszőleges $A \subseteq L$ nemüres részhalmazának van minimális eleme. $\square$

Következmények: (i) ekkor $(L, \preccurlyeq)$ teljes (azaz lineáris) rendezés.

(ii) ekkor minden $x \in L$ elemnek van $(S(x)$ vagy x^+ -al jelölt) **rákövetkezője** (**successor**) : $x^+ \preccurlyeq x$, $x^+ \neq x$ és L egyetlen eleme sincs x és x^+ között. $\square$

1.2 Általános struktúrák

1) Elsőrendű struktúrák-e a következők, és ha igen, mi a típusuk? Ha nem, miért nem?

- a) $\mathcal{R} := (\mathbb{R}, +, -, \cdot, \div)$, $\mathcal{R}_{\leq} := (\mathbb{R}, +, -, \cdot, \div, \leq)$,
- b) $\mathcal{R}_1 := (\mathbb{R}, \sin, 0)$,
- c) $\mathcal{R}_2 := (\mathbb{R}, +, \cdot, \ln, \frac{\cdot}{\cdot}, 0)$,
- d) $\mathcal{R}_+^n := (\mathbb{R}^n, +)$ (vektorok összeadása),
- e) $\mathcal{R}^n := (\mathbb{R}^n, +, \cdot)$ (vektortér),
- f) $\mathcal{R}^{n \times n} := (\mathbb{R}^{n \times n}, +, \cdot)$ (mátrixok),
- g) $\mathcal{A} := (A, \leq)$ ($A \neq \emptyset$ tetszőleges rendezett halmaz),
- h) $\mathcal{P}_X := (P(X), \cup, \cap, \subset, \emptyset, X, \subset)$ ($X \neq \emptyset$ tetszőleges halmaz),
- i) $\mathcal{G} := (V, E)$ (gráf),
- j) $\mathcal{P}_{\mathbb{P}} := (\mathbb{P}, \cdot)$,
- k) $\mathcal{O} := (\emptyset, *, \emptyset)$,
- l)
- m)
- n)

2) Döntse el, hogy az alábbi struktúrák közül melyek végesen generáltak ill. ciklikusak:

- a) $(\mathbb{Z}_{12}, +)$, $(\mathbb{Z}_{12}, +) \times (\mathbb{Z}_{12}, +)$,
- b)

3) Mutassa meg, hogy $\mathbb{R}^{\mathbb{R}}$ alábbi részhalmazai részstruktúrái $(\mathbb{R}^{\mathbb{R}}, \circ)$ -nak:

- a) $\mathbb{R}[x]$, b) $\mathbb{R}_{Lin}^{\mathbb{R}}$, c) $\mathbb{R}_{LinRac}^{\mathbb{R}}$

4) Mutasson példát olyan struktúrákra, amelyeknek nincs (valódi) részstruktúrája!

5) Homomorfizmusok-e az alábbi függvények a megadott struktúrák között? Melyik beágyazás, izo- vagy automorfizmus?

- a) $\alpha : (\mathbb{N}, +, \cdot) \rightarrow (\mathbb{N}, +, \cdot)$, $\alpha : n \mapsto 2n$,
- b) $\beta : (\mathbb{N}, |) \rightarrow (\mathbb{N}, |)$, $\beta : n \mapsto 2n$,
- c) $\gamma : (\mathbb{Z}, |) \rightarrow (\mathbb{N}, |)$, $\gamma : m \mapsto |m|$,
- d) $\delta : (\mathbb{N}, |) \rightarrow (\mathbb{N}, \leq)$, $\delta : n \mapsto n$,
- e) $\varepsilon : (\mathbb{Z}_6 \times \mathbb{Z}_9, +, \cdot) \rightarrow (\mathbb{Z}_{54}, +, \cdot)$, $\varepsilon : (i, j) \mapsto i \cdot j$,
- f) $\varphi : (\mathbb{Z}_6 \times \mathbb{Z}_7, +, \cdot) \rightarrow (\mathbb{Z}_{42}, +, \cdot)$, $\varphi : (i, j) \mapsto i \cdot j$,
- g) $\rho : (\mathbb{Z}[\sqrt{2}], +, \cdot) \rightarrow (\mathbb{Z}[\sqrt{2}], +, \cdot)$, $\rho : a + b\sqrt{2} \mapsto a - b\sqrt{2}$,
- h) $\vartheta : (\mathbb{Z}[\sqrt{2}], +) \rightarrow (\mathbb{Z}^2, +)$, $\vartheta : a + b\sqrt{2} \mapsto (a, b)$,
- i) $\iota : (\mathbb{Z}, +, \cdot) \rightarrow (\mathbb{Z}_m, +, \cdot)$, $\iota : k \mapsto k$ -nak m -el való osztási maradéka,
- j) $\zeta : (\mathbb{R}, +, \cdot) \rightarrow (\mathbb{C}, +, \cdot)$, $\zeta : x \mapsto x$,

k)

l) .

6) Adja meg a fenti φ leképezés inverzét!

7) Kongruencia -e a $\equiv_m \subset \mathbb{Z} \times \mathbb{Z}$ reláció a $(\mathbb{Z}, +, \cdot)$ struktúrán ?
 Ha igen, akkor mi az általa nyert $\mathbb{Z}/\equiv_m$ faktorhalmaz és $(\mathbb{Z}, +, \cdot)/\equiv_m$ faktorstruktúra?

1.3 Félcsoportok és csoportok

1.3.1 Gruppoidok, félcsoportok

1) Asszociatívok -e és kommutatívok -e az alábbi műveletek:

- a) $a \oplus b := a + b + ab \quad (a, b \in \mathbb{R})$,
- b) $a \otimes b := a \cdot b + \sqrt{(a^2 - 1) \cdot (b^2 - 1)} \quad (a, b \in [1, \infty))$,
- c) $a \boxtimes b := \frac{a+b}{1-ab} \quad (a, b \in (0, 1))$, $\#\#\# \operatorname{tg}(\alpha + \beta)$
- e) $\operatorname{lko}(m, n) := m$ és n legnagyobb közös osztója $(m, n \in \mathbb{Z})$,
- f) $\operatorname{lkt}(m, n) := m$ és n legkisebb közös többszöröse $(m, n \in \mathbb{Z})$,
- g) $A \setminus B \quad (A, B \subset X, X \neq \emptyset \text{ tetszőleges})$,
- h) $\max(x, y), \min(x, y) \quad (x, y \in \mathbb{R})$?

2) Milyen $f, g \in A^A$ függvényekre teljesül $f \circ g = g \circ f$?3) Mutassa meg, hogy $\mathbb{R}^{n \times n}$ -ben a szorzás művelete asszociatív de nem kommutatív!4) Vizsgálja meg az alábbi félcsoportok adott részhalmazait, hogy azok *rész-félcsoportok* illetve *csoportok* -e:

- a) $(\mathbb{R}^{n \times n}, \cdot)$ -ben $\mathbb{R}_{\Delta}^{n \times n}, \mathbb{R}_{\setminus}^{n \times n}, (\mathbb{R}^{n \times n})^*, (\mathbb{R}_{\Delta}^{n \times n})^*, (\mathbb{R}_{\setminus}^{n \times n})^*$,
- b) $(\mathbb{R}[x], \circ)$ -ben $\mathbb{R}_{Lin}^{\mathbb{R}}, \mathbb{R}_{LinRac}^{\mathbb{R}}$,
- c) $(\mathbb{R}[x], +)$ -ben $\mathbb{R}_{Lin}^{\mathbb{R}}, \mathbb{R}_{LinRac}^{\mathbb{R}}$,
- d) .

5) Legyen $(A, \circ)$ egy tetszőleges félcsoport, és tekintsük A -n a következő binér relációt:

$$x \overset{\circ}{\sim} y \Leftrightarrow x \circ y = y \circ x \quad .$$

Vizsgálja meg a $\overset{\circ}{\sim}$ reláció tulajdonságait

a) általában,

b) a következő struktúrákban:

$$\mathcal{R} = (\mathbb{R}, \cdot) \quad , \quad \mathcal{R}^{n \times n} = (\mathbb{R}^{n \times n}, \cdot) \quad , \quad \mathcal{A}_{\circ} = (A^A, \circ) \quad .$$

1.3.2 Speciális elemek félcsoporthokban

1) Vannak-e az alábbi struktúrákban bal- és jobboldali *zérus*-, *egység*- (=null-) illetve *nullosztó* elemek? Mely elemekkel lehet balról vagy jobbról *egyszerűsíteni*? Mely elemeknek van bal- illetve jobboldali *inverze*?

- a) $\mathcal{A}_\circ := (A^A, \circ)$, $A \neq \emptyset$ tetszőleges halmaz,
- b) $\mathcal{S}_\mathbb{N} := (S_\mathbb{N}, \circ)$,
- c) $\mathcal{Z}^{(\cdot)} := (\mathbb{Z}, \cdot)$, $\mathcal{Z}^{(+)} := (\mathbb{Z}, +)$, $\mathcal{N}^{(\cdot)} := (\mathbb{N}, \cdot)$,
- d) $\mathcal{Z}_m^{(\cdot)} := (\mathbb{Z}_m, \cdot)$, $\mathcal{Z}_m^{(+)} := (\mathbb{Z}_m, +)$ ($m \in \mathbb{Z}$ tetszőleges⁽⁸⁾ egész szám),
 $\mathcal{Z}_m^* := (\mathbb{Z}_m^*, \cdot)$, $\mathcal{Z}_p^* := (\mathbb{Z}_p^*, \cdot)$ (p prímszám),
 $\mathcal{R}_{2\pi}^{(+)} := (\mathbb{R}_{2\pi}, +)$, $\mathcal{R}_{2\pi}^{(\cdot)} := (\mathbb{R}_{2\pi}, \cdot)$,
- e) $\mathcal{R} := (\mathbb{R}^\mathbb{R}, \circ)$,
- f) $\mathcal{N}_\circ := (\mathbb{N}^\mathbb{N}, \circ)$,
- g) $\mathcal{R}_{Lin} := (\mathbb{R}_{Lin}^\mathbb{R}, \circ)$,
- h) $\mathcal{R}_{LinRac} := (\mathbb{R}_{LinRac}^\mathbb{R}, \circ)$,
- i) $\mathcal{R}^{n \times n} := (\mathbb{R}^{n \times n}, \cdot)$,
- j) $\mathcal{F}_X := (X^*, \wedge)$,
- k)
- l)
- m)
- n)

2) Tekintsük az $\mathcal{N}_\circ$ struktúra $g : \mathbb{N} \rightarrow \mathbb{N}$, $g : x \mapsto 2x$ elemét. Döntsük el: nullosztó-e, invertálható-e, lehet-e vele jobbról- ill. balról egyszerűsíteni!

3) Keressünk *idempotens* elemeket⁽⁹⁾ az alábbi struktúrákban:

- o) $(2 \cdot \mathbb{Z}, \cdot)$ (a páros egész számok multiplikatív félcsoporthja),
- a) $(\mathbb{Z}_m, \cdot)$ tetszőleges $m \in \mathbb{Z}$ egész számra (pl. $m = 10$, ...),
- b) $(\mathbb{R}^{n \times n}, \cdot)$,
- c) $(\mathbb{R}^\mathbb{R}, \circ)$,
- d) $\mathcal{S}_\mathbb{R}$, $\mathcal{S}_\mathbb{N}$, $\mathcal{S}_n$,
- e) síkbeli geometriai transzformációk $(= (A^A, \circ)$ ahol $A = \mathbb{R}^2)$,
- f)
- g) $(G, \cdot)$ (tetszőleges G multiplikatív csoport),
- h) $(P(X), \cup)$, $(P(X), \cap)$ (X tetszőleges halmaz),
- i)

4) Keressünk *involutorius* műveleteket⁽¹⁰⁾ (!) az alábbi halmazokon: $P(X)$, $\mathbb{C}$, $\mathbb{R}$, $\{i, h\}$, $\mathbb{R}^2$, $\mathbb{R}^3$.

⁸⁾ az $m = 1$ és $m = 0$ eset külön vizsgálatot igényel!

⁹⁾ **Definíció:** $x \in S$ **idempotens** elem ha $x^2 (= x \cdot x) = x$ ($(S, \cdot)$ félcsoporth). $\square$

¹⁰⁾ **Definíció:** az $f : A \rightarrow A$ *egyváltozós művelet* **involutorius**, ha $f^2(a) = f(f(a)) = a$ minden $a \in A$ elemre. $\square$

5) Mely $f \in A^A$ függvény lesz önmaga inverze?

6)* Keressen az alábbi félcsoportokban *kommutáló* elemeket⁽¹¹⁾ ! Van-e a félcsoportnak olyan eleme, amely *minden* elemmel kommutál?

- a) $\mathcal{A}_o := (A^A, \circ)$,
- b) $(\mathbb{R}^{n \times n}, \cdot)$,
- c)

1.3.3 Csoportok

1) Vizsgálja meg az alábbi csoportok adott részhalmazait, hogy azok részcsoportok-e, adja meg az általuk meghatározott bal- és jobboldali mel-
lékosztályokat. Melyek normálosztók közülük?

- a) $(\mathbb{R}^2, +)$ -ben (sík) $\mathbb{R}^1$ (origón átmenő egyenes),
- b) $(\mathbb{R}^{n \times n}, +)$ -ben $\mathbb{R}_{\Delta}^{n \times n}$, $\mathbb{R}_{\setminus}^{n \times n}$, $(\mathbb{R}^{n \times n})^*$, $(\mathbb{R}_{\Delta}^{n \times n})^*$, $(\mathbb{R}_{\setminus}^{n \times n})^*$,
- c) $(\mathbb{R}^{n \times n}, \cdot)^*$ -ben $(\mathbb{R}^{n \times n})^*$, $(\mathbb{R}_{\Delta}^{n \times n})^*$, $(\mathbb{R}_{\setminus}^{n \times n})^*$,
- d) $(\mathbb{Z}, +)$ -ban (m) ,
- e) .

2) a) Írja fel $\mathbb{Z}_{20}^*$ elemeit.

- b) Zárt-e ez a halmaz a szorzásra (és miért)?
- c) Számítsa ki elemeinek rendjét!
- d) Adja meg a vizsgált elemek által generált részcsoportokat.
- e) Mutassa meg, hogy minden elemnek van multiplikatív inverze (azaz $(\mathbb{Z}_{20}^*, \cdot)$ csoport).

3) Adja meg a következő *Abel-csoportok* exponenseit: $(\mathbb{Z}, +)$, $(\mathbb{Z}_m, +)$, $(\mathbb{Z}_m[x], +)$, $(\mathbb{Z}_m^*, +)$, $(\mathbb{Z}_m, +) \times (\mathbb{Z}_n, +)$.

4) Adja meg az összes 19, 20 és 27 elemű Abel-csoportot.

5) a) Sorolja fel a legfeljebb 30 elemű Abel-csoportokat!

b) Sorolja fel a legfeljebb 20 elemű *tetszőleges* csoportot!

1.3.4 Szimmetria- és permutációcsoportok

1) Adja meg az alábbi mértani alakzatok szimmetriacsoportjait:

- a) szabályos (síkbeli) sokszögek,
- b) szabályos (térbeli) testek,
- c)

¹¹⁾ **Definíció:** Tetszőleges $(S, \cdot)$ félcsoport $x, y \in S$ elemei **kommutálnak**, ha $x \cdot y = y \cdot x$. $\square$

- $$H := \left\{ id, \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\} \quad .$$

- a)

2	3	1	
11	6	15	4
5	8	7	9
10	13	12	14

b)

15	6	14	8
2	7	10	11
1	4	5	3
9	13	12	

c)

- 8) Hány ciklus van S_n -ben?

1.4.1 Alapfogalmak

- ¹²⁾ a játékot Sam Loyd (1841-1911) amerikai matematikus találta ki 1870 -ben.

3) Mik az *egységek* és az *asszociált* elemek a $(A^A, \circ)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{R}[x], \cdot)$, $(\mathbb{R}^{n \times n}, \cdot)$ struktúrákban?

4) Mik az *irreducibilis* és a *prímelemek* a fenti struktúrákban?

5) Mutassa meg, hogy $\mathbb{R}^{n \times n}$ ($n \geq 2$) azon elemeinek (mátrixok) halmaza, amelyek első sorának minden eleme 0, $\mathbb{R}^{n \times n}$ -nek jobbideálját alkotják. Balideál-e ez a halmaz? Keressen balideált $\mathbb{R}^{n \times n}$ -ben!

1.4.2 A $\mathbb{Z}_m$ maradékosztályok

Alapműveletek

0) Igaz-e, hogy $7 \cdot 3 \equiv -3 \pmod{12}$?

1) Mennyi maradékot adnak az alábbi kifejezések:

a) $9136 + 143^5 + 731 \cdot 54329 \cdot 42437 - 437^3 + 1$, 18 -al osztva?

b) $79346 + 146^{100} \cdot 1723 + 1$, 13 -al osztva?

c) $3^{29} + 4^{30} + 6^{32} + 7^{33}$, 5 -tel osztva?

(Varga Tamás matematikaverseny 2002., 7. osztály megyei forduló.)

d) $1 \cdot 7 \cdot 13 \cdot 19 \cdot \dots \cdot 1993 \cdot 1999$, 6 -tal osztva?

(Abacus Int. Math.Competition, 2001.Nov., grade 5-6, <http://www.gcschool.org/abacus.html>)

e) Milyen jegyre végződik (tízes számrendszerben) $9^{2002} + 2002^9$?

Mi az utolsó két jegye? Mennyi a kifejezés 5 -ös maradéka?

(Bem J. városi matematikaverseny 2002., 7. osztály.)

f) Hány lába van összesen egy tyúknak, hat kutyanak és hét palpigradinak?

(A palpigradi egy állat latin neve.) Az alábbi öt válasz közül *pontosan egy* helyes:

A) 46, B) 52, C) 66, D) 78, E) 82.

(Zrínyi Ilona matematikaverseny 2001. 3.osztály, megyei forduló.)

g) Mutassuk meg, hogy $5 + 5^2 + \dots + 5^{150}$ osztható 186 -tal !

h) Igaz -e, hogy "*páros+páros=páros*" $\pmod{9}$?

2) a) Adja meg 5 (multiplikatív) inverzét $\pmod{9}$!

b) Oldja meg az $5x = 3$ egyenletet $GF(9)$ -ben!

3) Számítsa ki $5/3$ értékét $\pmod{20}$!

4) Számítsa ki $\sqrt{7}$ értékét $\pmod{13}$!

5) a) Ellenőrizze, hogy $g = 3$ primitív gyök -e $\pmod{17}$.

b) Számítsa ki $6/7$ és $\sqrt{-4}$ értékét $\pmod{17}$.

c) A primitív-gyök⁽¹³⁾ táblázat felhasználásával keresse meg 7 (multiplikatív) inverzét mod 47 , majd oldja meg a $7x \equiv 11 \pmod{47}$ egyenletet.

6) A 10839 és a 11863 számokat ugyanazzal a háromjegyű számmal elosztva mind a kétszer ugyanaz a maradék. Mennyi ez a maradék?

(Összefoglaló feladatgyűjtemény matematikából, 3945.feladat)

7) Három egymást követő pozitív egész szám köbének összege osztható 18 -cal. Mennyit kapunk maradékkul, ha a legkisebb és legnagyobb szám szorzatát 18 -cal osztjuk el?

(Felvételi feladat 2001.V.22.de.7.példa.)

8) Oldja meg az alábbi egyenleteket a megadott struktúrákban:

a) $5x + 7 \equiv 9 \pmod{13}$,

b) $\frac{3x+2}{5-x} \equiv 7 \pmod{GF(47)}$ -ben,

c) $x^2 - 5x + 6 = 0 \pmod{GF(13)}$ -ban,

d) $x^2 + 3x + 9 = 0 \pmod{GF(17)}$ -ban,

e) $x^3 + 4x^2 - 5x + 6 = 0 \pmod{GF(17)}$ -ban,

f) $5x + 3y \equiv 9 \pmod{13}$.

9) Határozza meg az $f(x) = x^2 + 2x - 1$ kifejezés szélsőértékeit $\mathbb{Z}_{11}$ -ben

10) Mutassuk meg, hogy tetszőleges n természetes szám esetén a 3^n oldalú konvex sokszög oldalait és átlóit be tudjuk színezni 3 színnel úgy, hogy a színezett élek lefedhetők 3^{n-1} homogén (egyszínű) háromszöggel!

(Lásd még a (1.4.3) fejezet feladatait is.)

Egyetemi felvételi feladatok

1) Mutassa meg, hogy minden 6 -ra végződő négyzetszámban a tízesek helyén páratlan számjegy áll!

(Országos egyetemi felvételi feladatsor)

2) Bizonyítsa be, hogy tetszőlegesen választott öt egész szám között mindig van olyan három, amelynek összege osztható 3 -mal!

(Országos egyetemi felvételi feladatsor)

3) Legyen n tetszőleges pozitív egész szám. Mennyi a maradék, ha az $1^n + 2^n + 3^n + 4^n$ összeget elosztjuk 4 -gyel?

(Országos egyetemi felvételi feladatsor)

¹³⁾ **Definíció:** $g \in \mathbb{Z}_p$ **primitív-gyök** mod p ($p \in \mathbb{P}$ prímszám), ha $[g] = (\mathbb{Z}_p, \cdot)$, azaz g hatványai kiadják $\mathbb{Z}_p$ összes elemét. $\square$ (Lásd még a könyv végén levő táblázatokat.)

Euler és Fermat tételei, nagy kitevőjű hatványok

- 1) Hány jegyű a 3425^{5432} kifejezés a tízes számrendszerben felírva?
 b) És kettes számrendszerben?

2) a) Számítsa ki $\varphi(p)$ és $\varphi(p \cdot q)$ értékét tetszőleges $p, q \in \mathbb{P}$ prím-számokra.

b) Határozza meg tetszőleges $n \in \mathbb{N}$ természetes szám *Euler-féle* φ - függvényének értékét!

c) Határozza meg $\varphi(1500)$, $\varphi(\dots)$ és $\varphi(\dots)$ értékeit.

3) Számítsa ki az alábbi hatványokat:

a) $6456^{4652} \pmod{9786}$,

b) $4326^{1818} \pmod{1003}$,

c) $2222^{5555} \pmod{137}$.

Struktúrák vizsgálata

1) a) Adja meg tetszőleges $m \in \mathbb{Z}$ természetes szám esetén (m) -et, az m által generált főideált!

b) Mutassa meg, hogy

$$(\mathbb{Z}_m, +, \cdot) \cong (\mathbb{Z}_m, +, \cdot) / (m) \quad .$$

2) Írja fel a $(\mathbb{Z}_3, +) \times (\mathbb{Z}_4, +)$ struktúra Cayley tábláját! Ciklikus -e a struktúra ?

3) a) Írja fel a $(\mathbb{Z}_4, +)$ és a $(\mathbb{Z}_2, +) \times (\mathbb{Z}_2, +)$ struktúrák művelet-tábláit! Izomorf -e a két struktúra?

b) Izomorfak -e a $(\mathbb{Z}_4, +)$ és $(\mathbb{Z}_2, +) \times (\mathbb{Z}_4, +)$ struktúrák?

4) Izomorf -e a $(\mathbb{Z}_{12}, +)$ és a $(\mathbb{Z}_3, +) \times (\mathbb{Z}_4, +)$ struktúra? Adjon meg konkrét izomorfizmust a két struktúra között!

5) Sorolja fel az összes

a) 12 elemű- ,

b) 15 elemű kommutatív (Abel) csoportot!

1.4.3 Euklideszi gyűrűk

Alapfogalmak

1) Vizsgálja meg, hogy az (1.4.1) fejezet 1) feladatában szereplő gyűrűk közül melyek Euklideszi gyűrűk!

2)

Prímfelbontás

1)

2) Mutassa meg, hogy a $(\mathbb{Z} \cdot 2, +, \cdot)$ struktúrában (a páros számok gyűrűje) nem teljesül az egyértelmű prímfelbontás tulajdonsága.

3) Végezze el a következő polinomok maradékos osztását:

a) $(x^3 + 3x + 5) : (2x^2 - 7x + 9)$,

b) $(4x^5 + 5x - 2) : (2x^3 + 3)$.

4) műveletek mod $f(x)$ polinomra

5) Irreducibilis -e az

a) $x^2 - 5$ polinom $\mathbb{Z}[x]$ illetve $\mathbb{R}[x]$ -ben,

b) $x^4 + 1$ polinom $\mathbb{R}[x]$ illetve $\mathbb{C}[x]$ -ben,

c) $x^2 + 1$ polinom $\mathbb{Z}_2[x]$, $\mathbb{Q}[x]$, $\mathbb{R}[x]$ illetve $\mathbb{C}[x]$ -ben,

d) $x^2 + x + 1$ polinom a c) -ben felsorolt gyűrűkben?

6) Bontsa fel az alábbi polinomokat irreducibilis tényezőkre $\mathbb{R}[x]$ illetve $\mathbb{C}[x]$ -ben:

a) $x^2 - 3x + 1$,

b) $x^2 - 2x + 2$,

c)

d) $x^4 + 1$ ### *red-próba*

7) Adja meg a $(\mathbb{Z}_2[x], +, \cdot) / (x^2 + x + 1)$ faktorhalmaz elemeit és a reprezentánsok közötti műveletek táblázatait! Test-e az így kapott struktúra?

Euklidesz algoritmus

- 1) Keresse meg az alábbi számok legnagyobb közös osztóját:
 - a) 94542 és 24981 ,
 - b) 7732 és 149 .
- 2) Keresse meg az 56354 és 2956 számok *legkisebb közös többszörösét!*
- 3) Keresse meg a 65924, 33284 és 53142 számok legnagyobb közös osztóját!
- 4) Határozza meg az alábbi polinomok legnagyobb közös osztóját:
 - a) $p(x) = x^3 + 2x^2 - 2x + 1$ és $q(x) = x^2 - x - 2$,
 - b) $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ és $g(x) = 3x^3 + 10x^2 + 2x - 3$.
- 5) Négyzetmentesek -e a következő polinomok:
- 6) Hányszoros gyöke
 - a) $x_0 = 1$ az $f(x) = x^3 + 3x^2 + 2x - 6$ polinomnak ?
 - b)
- 7)* Adj meg szükséges és elégséges feltételt arra, hogy egy másodfokú polinomnak egyszeres gyökei legyenek.

Lineáris Diophantikus egyenletek

- 1) Adja meg az alábbi egyenletek egész gyökeit !
 - a)
 - b) $5682x + 4836y = 30$
 - c) $10518x + 5682y = 6$
 - d) $4512x + 1111y = 3248$
 - e) $1683x + 114y = 3$
- 2) a) Oldja meg a $114x \equiv 3 \pmod{1683}$ egyenletet.
 b) Keresse meg 18 multiplikatív inverzét mod 175 .
- 3) Melyik az a négyjegyű szám, amellyel 25707 -et elosztva 32 -őt, 37568 -at elosztva 43 -at kapunk maradékul ?
 (Összefoglaló feladatgyűjtemény matematikából, 3946. feladat)
- 4) Oldja meg az alábbi egyenleteket az egész számok körében:
 - a) $12x + 30y + 15z = 18$,
 - a) $4x + 3y = 7z$,
 - b) $6x + 10y + 15z = 7$,

5)* Írja fel a $3x + 4y + 7z = n$ egyenlet (összes) egész gyökét!

6) Keresse meg az (összes) olyan $u(x)$ és $v(x)$ polinomokat, amelyekre

$$f(x) \cdot u(x) + g(x) \cdot v(x) = d(x)$$

ahol $f(x) = x^3 - x^2 + 3x - 10$, $g(x) = x^3 + 6x^2 - 9x - 14$ és $d(x) = \text{lnko}(f(x), g(x))$ a legnagyobb közös osztó.

Kínai maradéktétel

1) Oldja meg az alábbi kongruenciarendszert:

$$\text{a) } \begin{cases} x \equiv 2 \pmod{7} \\ x \equiv 3 \pmod{9} \\ x \equiv 3 \pmod{11} \end{cases}, \quad \text{b) } \begin{cases} x \equiv 5 \pmod{7} \\ x \equiv 2 \pmod{12} \\ x \equiv 3 \pmod{25} \\ x \equiv 0 \pmod{11} \end{cases}$$

2) Oldja meg az alábbi kongruenciarendszereket:

$$\text{a) } \begin{cases} 3x \equiv 2 \pmod{7} \\ 2x \equiv 3 \pmod{9} \end{cases}, \quad \text{b) } \begin{cases} x \equiv 3 \pmod{4} \\ x \equiv 3 \pmod{5} \\ x \equiv 2 \pmod{7} \\ 5x \equiv 4 \pmod{11} \end{cases}$$

(nem $x \equiv a_i$ alakú!)

3) Melyik az a legkisebb természetes szám, amely 2 -vel osztva 1, 3 -mal osztva 2, 4 -gyel osztva 3 és 5 -tel osztva 4 maradékot ad?

(Összefoglaló feladatgyűjtemény matematikából, 3937.feladat)

4)

1.5 Testek

1) ### konkrét polinomműveletek $(\text{mod } f(x))$ polinomra

2) Adja meg a $GF(4)$ testet (elemeit és művelet tábláit) !

(*Segítség:* a $(\mathbb{Z}_2[x], +, \cdot)$ gyűrűt kell faktorizálni az $f(x) := x^2 + x + 1$ irreducibilis polinommal.)

3) Adja meg az alábbi véges testeket:

a) $GF(9)$,

(*Segítség:* $q = p^n$ esetén a $(\mathbb{Z}_p[x], +, \cdot)$ gyűrűt kell faktorizálni egy n -edfokú irreducibilis $f(x) \in \mathbb{Z}_p[x]$ polinommal.)

1.6 Boole-algebrák, hálók

1) Legyen $\mathfrak{R}$ egy tetszőleges (elsőrendű algebrai) struktúra, legyen $Sub(\mathfrak{R})$ $\mathfrak{R}$ részalgebráinak halmaza, és tekintsük a $SUB(\mathfrak{R}) := (Sub(\mathfrak{R}), \leq)$ struktúrát, ahol $\leq$ a részstruktúra-reláció. Mutassuk meg, hogy $SUB(\mathfrak{R})$ háló. Van-e legkisebb, legnagyobb, minimális ill. maximális eleme, és ez melyik részstruktúrája $\mathfrak{R}$ -nek? Disztributív háló-e?

Fejezet 2

Megoldások

2.1 Halmazok, relációk, függvények

2.1.1 Relációk

1)

.

.

e) (oszthatóság $\mathbb{Z}$ -n): nem antiszimmetrikus mert pl. $2|-2$ és $-2|2$, de nem is szimmetrikus mert pl. $3|6$ és $6 \nmid 3$, vagyis $|$ *nem* rendezés $\mathbb{Z}$ -n.

f) (oszthatóság $\mathbb{N}$ -n): $m|n$ -ből $m \leq n$ következik kivéve ha $m = 0$, vagyis 0 a *legnagyobb* elem, mert $m|0$ minden $m \in \mathbb{N}$ elemre, és hasonlóan 1 a legkisebb elem.

.

.

.

2)

g) $m|a - b$ pontosan azt jelenti, hogy a és b *ugyanazt a maradékot adják* m -el elosztva,

h) $\mathbb{Z}/_{\equiv m} \cong \mathbb{Z}_m$,

j) (párhuzamos egyenesek) egy lehetséges reprezentáns rendszer: egy ponton átmenő összes egyenes (egyenesserreg/sugársor),

k) V -n nem tranzitív (mert $\underline{0}$ minden vektoral párhuzamos), de $V \setminus \{\underline{0}\}$ -n már igen.

10)

$\equiv_1 = \Delta = \mathbb{Z}^2$ (bármely két elem kongruens), $\equiv_0$ értelmetlen,

$=$ (az egyenlőség) csak $\equiv_\infty$ lehetne.

$\mathbb{Z}/\equiv \cong \mathbb{Z}$, $\mathbb{Z}/\equiv_1 \cong \mathbb{Z}_1 = \{0\}$, $\mathbb{Z}/\equiv_m \cong \mathbb{Z}_m$.

$\equiv_n$ pontosan akkor finomabb $\equiv_m$ -nél, ha $n > m$, és $=$ a legfinomabb reláció.

12)**

A szimmetria és a reflexivitás minden esetben nyilvánvaló.

14)

c) $|\mathbb{Z}| \subseteq \mathbb{Z}^2$ nem szimmetrikus és nem antiszimmetrikus.

15) a) $(\mathbb{N}, |)$ -ban 0 maximális, 1 minimális elem.

$|\mathbb{N} \setminus \{0\} \subset \leq_{\mathbb{N} \setminus \{0\}}$ míg $|\mathbb{N} \not\subseteq \leq_{\mathbb{N}}$.

b) Mivel tetszőleges $u, v \in \mathbb{Z}$ vektorokra

$$u \parallel v \Leftrightarrow (u | v \text{ vagy } v | u),$$

így $|\subset \parallel$, sőt $|\cup |\cdot^{-1} \parallel$.

17)

18) Például: minden páros $<$ minden páratlan $\mathbb{N}$ ill. $\mathbb{Z}$ -ben.

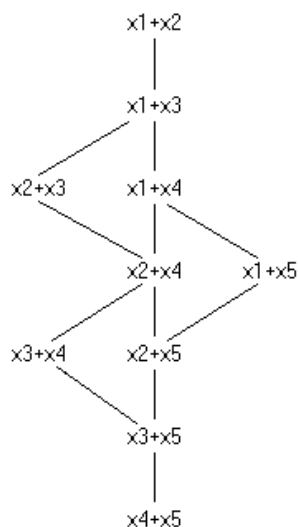
2.1.2 Függvények, műveletek

1) A $*$ művelet nem asszociatív, nem kommutatív, balról egy elemmel sem lehet egyszerűsíteni, de jobbról minden elemmel lehet egyszerűsíteni.

2.2 Általános struktúrák

.

4) pl. $\mathbb{Z}_p$.



ábra 2.1:

2.3 Félcsoportok és csoportok

2.3.1 Gruppoidok, félcsoportok

- 1) a) $\oplus$ nyilván kommutatív, asszociatív (közvetlenül számolható),
 b) $[1, \infty)$ először is zárt-e a $\otimes$ műveletre? Ha $a, b \geq 1$, akkor nyilván $a \otimes b \geq a \cdot b \geq 1$, vagyis OK.

$\otimes$ nyilván kommutatív. Az asszociativitás közvetlen (kissé hosszadalmas) számolással is ellenőrizhető, vagy az alábbi észrevétel alapján: $a, b, c \geq 1$ esetén vannak olyan $x, y, z \in \mathbb{R}$ valós számok, amelyekre $a = ch(x)$, $b = ch(y)$ és $c = ch(z)$. Ekkor pedig (a hiperbolikus függvényekre érvényes azonosságok alapján)

$$a \otimes b = ch(x) \otimes ch(y) = ch(x + y)$$

ami alapján

$$(a \otimes b) \otimes c = ch(x + y) \otimes ch(z) = ch(x + y + z) = ch(x) \otimes ch(y + z) = a \otimes (b \otimes c) \quad .$$

(A részleteket megtalálhatjuk a *Középiskolai Mat.Lapok* 2000.februári számában a 90. oldalon, az F 3185 feladat megoldásánál.)

c) $a \boxtimes b := \frac{a+b}{1-ab}$ hiába kommutatív, de a $(0, 1)$ halmaz nem zárt erre a műveletre!

e) $lnko(m, n)$ nyilván kommutatív. Asszociatív is

f) $lkkt(m, n)$ nyilván kommutatív. Asszociatív is

g) $A \setminus B$ nem kommutatív és nem asszociatív.

h) $\max(x, y)$ és $\min(x, y)$ nyilván kommutatív. Asszociatív is.

4) b) $\mathbb{R}_{Lin}^{\mathbb{R}}$ zárt a $\circ$ (kompozíció) műveletére⁽¹⁾, így rész-félcsoport.

$\underline{0} := 0x + 0$ zéruselem, vagyis nincs inverze, $\mathbb{R}_{Lin}^{\mathbb{R}} \setminus \{\underline{0}\}$ azonban már csoport.

$\mathbb{R}_{LinRac}^{\mathbb{R}}$ is zárt a $\circ$ (kompozíció) műveletére: $f(x) = \frac{ax+b}{cx+d}$ és $g(x) = \frac{\alpha x+\beta}{\gamma x+\delta}$ esetén

$$(f \circ g)(x) = \frac{a \frac{\alpha x+\beta}{\gamma x+\delta} + b}{c \frac{\alpha x+\beta}{\gamma x+\delta} + d} = \frac{(a\alpha + b\gamma)x + (a\beta + b\delta)}{(c\alpha + d\gamma)x + (c\beta + d\delta)}$$

hiszen $|c\alpha + d\gamma| + |c\beta + d\delta| \neq 0$ mert $|c| + |d| \neq 0$ és $|\gamma| + |\delta| \neq 0$

c) $\mathbb{R}_{Lin}^{\mathbb{R}}$ könnyen láthatóan zárt a $+$ műveletre, míg $\mathbb{R}_{LinRac}^{\mathbb{R}}$ nem ! .

2.3.2 Speciális elemek félcsoportokban

1) a) $\mathcal{A}_o := (A^A, \circ)$ -ban: id_A kétoldali *egységelem*,

a $\underline{c}$ konstans függvények a baloldali zéruselemek, jobboldali *zéruselem* nincs,

$f : A \rightarrow A$ pontosan akkor *baloldali* nullosztó ha *nem* injektív, $g : A \rightarrow A$ pontosan akkor *jobboldali* nullosztó ha *nem* szürjektív.

Az $f : A \rightarrow A$ függvénnyel pontosan akkor lehet balról *egyszerűsíteni*, ha injektív, jobbról pontosan akkor ha szürjektív.

Baloldali *inverze* pontosan csak az injektív függvényeknek van, jobboldali pedig a szürjektíveknek. Csak a bijekcióknak (=permutációknak) van egyértelmű (bármely oldali) inverze, ami egyúttal kétoldali inverz is.

3) o) $(2 \cdot \mathbb{Z}, \cdot)$ -ben nincs ,

a) $(\mathbb{Z}_{10}, \cdot)$ -ben 0,1,5,6 ,

b) $(\mathbb{R}^{n \times n}, \cdot)$ -ben pl. olyan átlós (diagonális) mátrix amelynek főátlójában csak 0 vagy 1 áll; vagy egy olyan mátrix, amelynek minden eleme 0 kivéve egyetlen sorát vagy oszlopát amelyben csupa 1 áll,

c) $(\mathbb{R}^{\mathbb{R}}, \circ)$ vagy általában $(A^A, \circ)$ -ben $f \in A^A$ pl. ha f felcseréli A két pontját és A többi elemét fixen hagyja (azaz $f(a) = a$) . Pontosabban, $f \in$

¹⁾ $f(x) = ax + b$ és $g(x) = cx + d$ esetén $(f \circ g)(x) = a(cx + d) + b = acx + (ad + b)$.

A^A pontosan akkor, ha $A = \bigcup_{i \in I} \{x_i, y_i\}$ (legfeljebb) kételemű halmazokra partícionálható, amelyekre $f(x_i) = y_i$ és $f(y_i) = x_i$ minden $i \in I$ esetén.

d) $\mathcal{S}_{\mathbb{R}}, \mathcal{S}_{\mathbb{N}}, \mathcal{S}_n$,

e) $(\mathbb{R}^2(\mathbb{R}^2), \circ)$ -ben egyenesre vagy pontra való tükrözés, inverzió,

f)

g) $(G, \cdot)$ (tetszőleges G multiplikatív csoport),

h)

5) általában $(A^A, \circ)$ -ben $f \in A^A$ pl. ha f felcseréli A két pontját és A többi elemét fixen hagyja (azaz $f(a) = a$). Pontosabban, $f \in A^A$ pontosan akkor, ha $A = \bigcup_{i \in I} \{x_i, y_i\}$ (legfeljebb) kételemű halmazokra partícionálható, amelyekre $f(x_i) = y_i$ és $f(y_i) = x_i$ minden $i \in I$ esetén. .

6)* Az egységelemek id_A és $E \in \mathbb{R}^{n \times n}$ minden elemmel kommutálnak.

2.3.3 Csoportok

4) 19 elemű csak $(\mathbb{Z}_{19}, +)$.

20 eleműek $(\mathbb{Z}_{20}, +)$ és $(\mathbb{Z}_2, +) \times (\mathbb{Z}_{10}, +)$.

27 eleműek $(\mathbb{Z}_{27}, +)$, $(\mathbb{Z}_3, +) \times (\mathbb{Z}_9, +)$ és $(\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +) \times (\mathbb{Z}_3, +)$.

2.3.4 Szimmetria- és permutációcsoportok

5) a) $\sigma = (5, 2, 3) = (5, 2) \circ (5, 3)$,

b) $\rho = (1, 3, 7, 5) = (1, 5) \circ (1, 7) \circ (1, 3)$,

c) $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 3 & 2 & 6 & 4 & 7 & 1 \end{pmatrix} = (1, 5, 4, 6, 7) \circ (2, 3) = (1, 5) \circ (1, 4) \circ (1, 6) \circ (1, 7) \circ (2, 3)$,

d) $\mu = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 2 & 4 & 7 & 5 & 8 & 3 & 10 & 9 & 1 & 6 & 11 \end{pmatrix} = (1, 2, 4, 5, 8, 9) \circ (3, 7, 10, 6) = (1, 2) \circ (1, 4) \circ (1, 5) \circ (1, 8) \circ (1, 9) \circ (3, 7) \circ (3, 10) \circ (3, 6)$.

6) Jelölje σ a $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ permutációt, azaz legyen $H := \{id, \sigma\}$.

a) Nyilván csak azt kell ellenőriznünk, hogy $\sigma^2 \in H$, de $\sigma^2 = id$.

b) Természetesen

$$H \cdot id = id \cdot H = H$$

és $\sigma^2 = id$ miatt

$$H \cdot \sigma = \sigma \cdot H = H \quad .$$

Egyéb jobboldali mellékosztályok:

$$\begin{aligned} H \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} &= H \cdot \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \right\} = J_1, \\ H \cdot \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} &= H \cdot \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} = J_2, \end{aligned}$$

baloldali mellékosztályok:

$$\begin{aligned} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \cdot H &= \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \cdot H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \right\} = B_1, \\ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} \cdot H &= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \cdot H = \left\{ \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \right\} = B_2. \end{aligned}$$

2.4 Gyűrűk

2.4.1 A $\mathbb{Z}_m$ maradékosztályok

Alapműveletek

4) Nincs olyan szám mod 13 amelynek négyzete 7 lenne, vagyis $\sqrt{7}$ nem létezik mod 13.

5) a) Számítsuk ki rendre 3 hatványait (mod 17): $3^1 = 3$, $3^2 = 9$, $3^3 = 10$, $3^4 = 13$, $3^5 = 5$, $3^6 = 15 (= -2)$, $3^7 = 11 (= -6)$, $3^8 = 16 (= -1)$, $3^9 = 14 (= -3)$, $3^{10} = 8 (= -9)$, $3^{11} = 7 (= -10)$, $3^{12} = 4 (= -13)$, $3^{13} = 12 (= -5)$, $3^{14} = 2 (= -15)$, $3^{15} = 6 (= -11)$, $3^{16} = 1 (= -16)$. Mivel $(\text{mod } 17) \setminus \{0\}$ (azaz $\mathbb{Z}_{17}^*$) összes eleme szerepel a felsorolásban, ezért $g = 3$ valóban primitív gyök (mod 17).

b) Az a) részben láttuk, hogy $3^{11} \equiv 7 \pmod{17}$, így $7^{-1} \equiv 3^{16-11} \equiv 5$ és $6/7 \equiv 6 \cdot 5 \equiv 13 \pmod{17}$. Ellenőrzés: $13 \cdot 7 \equiv 6 \pmod{17}$. Mivel $3^4 \equiv 13 \equiv -4 \pmod{17}$, így $\sqrt{-4} \equiv 3^2 = 9 \pmod{17}$.

c) A táblázat szerint $g = 5$ primitív gyök (mod 47), $g^{32} \equiv 7$, amik alapján $7^{-1} \equiv g^{46-32} \equiv g^{14} \equiv 27 \pmod{47}$. Így az egyenlet gyöke $x \equiv 11/7 \equiv g^{7-14} \equiv g^{-7} \equiv g^{-7+46} \equiv g^{39} \equiv 30 \pmod{47}$ mivel (a táblázat szerint) $11 \equiv g^7$ és $g^{39} \equiv 30 \pmod{47}$.

6) A feladat szerint $10839 \equiv 11863 \pmod{m}$ vagyis $m \mid 11863 - 10839 = 1024$ ahonnan $m = 128, 256$ vagy 512 . A lehetséges *maradék* mindhárom esetben $10839 \equiv 11863 = 87 \pmod{m}$.

8) a) $x \equiv 2/5 \equiv 2 \cdot 8 \equiv 3 \pmod{13}$. Ellenőrzés: HF.

b) Átalakítva kapjuk: $3x + 2 \equiv 35 - 7x$ azaz $x \equiv 33/10 \pmod{47}$. A mod 47 primitív gyök ($g = 5$) táblázatát felhasználva látjuk, hogy $g^{27} \equiv 33$, $g^{19} \equiv 10$ és így $x \equiv g^{27-19} \equiv g^8 \equiv 8 \pmod{47}$ $GF(47)$ -ben.

c) $x^2 - 5x + 6 = 0 \pmod{13}$ -ban,

- d) $x^2 + 3x + 9 = 0$ $GF(17)$ -ban,
 e) $x^3 + 4x^2 - 5x + 6 = 0$ $GF(17)$ -ban,
 f) $5x + 3y \equiv 9 \pmod{13}$.

9) Számoljuk ki a függvény helyettesítései értékeit az $x = 0, 1, \dots, 10$ helyeken.

Euler és Fermat tételei, nagy kitevőjű hatványok

- 1) A tízes számrendszerben $x \in \mathbb{N}$ pontosan akkor k jegyű, ha

$$10^{k-1} \leq x < 10^k.$$

Ezek alapján $k - 1 \leq \lg(3425^{5432}) = 5432 \cdot \lg(3425) \approx 19200.276$, vagyis a kérdéses mennyiség 19201 jegyű 10-es számrendszerben felírva.

b) Kettes számrendszerben pedig $\log_2(3425^{5432}) \approx 63781.936$ alapján 63782 jegyű!

2) a) $\varphi(p) = p - 1$, továbbá a logikai szitaformula (egyszerűbb változata) alapján

$$\varphi(p \cdot q) = pq - p - q + 1 = (p - 1) \cdot (q - 1)$$

ahol $p, q \in \mathbb{P}$ tetszőleges prímszámok.

b) A [SzI] Feladatgyűjtemény 4. fejezetében (Logikai szitaformula) leírtak miatt

$$\varphi(n) = \prod_{p_i | n} \left(1 - \frac{1}{p_i}\right)$$

ahol $n = \prod_{i=1}^k p_i^{\alpha_i}$ az n szám prímtényezős felbontása.

c) A fentiek (azaz a logikai szitaformula) alapján

$$\begin{aligned} \varphi(1500) &= 1500 - \frac{1500}{2} - \frac{1500}{3} - \frac{1500}{5} + \frac{1500}{2 \cdot 3} + \frac{1500}{2 \cdot 5} + \frac{1500}{3 \cdot 5} - \frac{1500}{2 \cdot 3 \cdot 5} \\ &= \end{aligned}$$

$6456^{4652} \pmod{9786}$ kiszámítása:

$k = 1001000101100$ (bin) ,

$$\begin{aligned}
 u[0] &= u = 6456 = u^{2^0} \pmod{9786} \\
 u[1] &= (u[0])^2 = u^{2^1} = 6456^2 \equiv 1362 \pmod{9786} \\
 u[2] &= (u[1])^2 = u^{2^2} = 1362^2 \equiv \mathbf{5490} \pmod{9786} \\
 u[3] &= (u[2])^2 = u^{2^3} = 5490^2 \equiv \mathbf{9006} \pmod{9786} \\
 u[4] &= (u[3])^2 = u^{2^4} = 9006^2 \equiv 1668 \pmod{9786} \\
 u[5] &= (u[4])^2 = u^{2^5} = 1668^2 \equiv \mathbf{3000} \pmod{9786} \\
 u[6] &= (u[5])^2 = u^{2^6} = 3000^2 \equiv 6666 \pmod{9786} \\
 u[7] &= (u[6])^2 = u^{2^7} = 6666^2 \equiv 7116 \pmod{9786} \\
 u[8] &= (u[7])^2 = u^{2^8} = 7116^2 \equiv 4692 \pmod{9786} \\
 u[9] &= (u[8])^2 = u^{2^9} = 4692^2 \equiv \mathbf{6150} \pmod{9786} \\
 u[10] &= (u[9])^2 = u^{2^{10}} = 6150^2 \equiv 9396 \pmod{9786} \\
 u[11] &= (u[10])^2 = u^{2^{11}} = 9396^2 \equiv 5310 \pmod{9786} \\
 u[12] &= (u[11])^2 = u^{2^{12}} = 5310^2 \equiv \mathbf{2634} \pmod{9786}
 \end{aligned}$$

így

$$\begin{aligned}
 u^k &= 5490 \cdot 9006 \cdot 3000 \cdot 6150 \cdot 2634 \equiv 4068 \cdot 3000 \cdot 6150 \cdot 2634 \equiv 858 \cdot 6150 \cdot 2634 \\
 &\equiv 2046 \cdot 2634 \equiv 6864 \pmod{9786}
 \end{aligned}$$

Tehát

$$6456^{4652} \equiv 6864 \pmod{9786}$$

$4326^{1818} \pmod{1003}$ kiszámítása:

$k = 11100011010$ (bin) ,

$$\begin{aligned}
 u[0] &= u \equiv 314 = u^{2^0} \pmod{1003} \\
 u[1] &= (u[0])^2 = u^{2^1} \equiv 302 \pmod{1003} \\
 u[2] &= (u[1])^2 = u^{2^2} \equiv 934 \pmod{1003} \\
 u[3] &= (u[2])^2 = u^{2^3} \equiv 749 \pmod{1003} \\
 u[4] &= (u[3])^2 = u^{2^4} \equiv 324 \pmod{1003} \\
 u[5] &= (u[4])^2 = u^{2^5} \equiv 664 \pmod{1003} \\
 u[6] &= (u[5])^2 = u^{2^6} \equiv 579 \pmod{1003} \\
 u[7] &= (u[6])^2 = u^{2^7} \equiv 239 \pmod{1003} \\
 u[8] &= (u[7])^2 = u^{2^8} \equiv 953 \pmod{1003} \\
 u[9] &= (u[8])^2 = u^{2^9} \equiv 494 \pmod{1003} \\
 u[10] &= (u[9])^2 = u^{2^{10}} \equiv 307 \pmod{1003}
 \end{aligned}$$

Tehát

$$4326^{1818} \equiv 314^{1818} \equiv 302 \cdot 749 \cdot 324 \cdot 953 \cdot 494 \cdot 307 \equiv 64 \pmod{1003}$$

2.4.2 Euklideszi gyűrűk

Prímfelbontás

2) $60 = 6 \cdot 10 = 2 \cdot 30$, ez két különböző felbontás irreducibilis elemekre.

3) a) $(x^3 + 3x + 5) : (2x^2 - 7x + 9) = \frac{1}{2}x + \frac{7}{4}$, a maradék $\frac{43}{4}x - \frac{43}{4}$.

b) $p(x) = 4x^5 + 5x - 2$.

$q(x) = 2x^3 + 3$.

A hányados: $s(x) = 2x^2$

A maradék: $r(x) = -6x^2 + 5x - 2$

5) a) $x^2 - 5 = (x - \sqrt{5})(x + \sqrt{5})$, így $\mathbb{R}[x]$ -ben felbontható (*reducibilis*) míg $\mathbb{Z}[x]$ -ben nem.

b) Az *Algebra Alaptétele* szerint $x^4 + 1$ nem lehet irreducibilis sem $\mathbb{R}[x]$ sem $\mathbb{C}[x]$ -ben.

A polinom komplex gyökei a $\sqrt[4]{-1}$ értékei, így $\mathbb{C}[x]$ -beli felbontása (a gyöktényező felbontás):

$$x^4 + 1 = (x - \varepsilon) \cdot (x - \varepsilon\delta) \cdot (x - \varepsilon\delta^2) \cdot (x - \varepsilon\delta^3)$$

ahol $\varepsilon = \sqrt[4]{-1} = \cos(45^\circ) + i \cdot \sin(45^\circ)$ és $\delta = \cos(90^\circ) + i \cdot \sin(90^\circ) = i$.

$\mathbb{R}[x]$ -ben csak másodfokú tényezőket kereshetünk. A fenti (komplex együtthatós) felbontás megfelelő tagjainak összeszorozása után kapjuk:

$$x^4 + 1 = (x^2 + \sqrt{2}x + 1) \cdot (x^2 - \sqrt{2}x + 1) \quad .$$

Megjegyzés: Ha a felbontandó polinom gyökeit nem mind ismerjük, akkor próbálkozhatunk az együtthatók összehasonlításának módszerével is: példánkban $x^4 + 1 = (x^2 + ax + b) \cdot (x^2 + cx + d)$ alakban.

Euklidesz algoritmusa

1)a) $lnko(94542, 24981)$ meghatározása

$$\begin{aligned}
 < 94542 > = < 24981 > * 3 + < 19599 > \\
 < 24981 > = < 19599 > * 1 + < 5382 > \\
 < 19599 > = < 5382 > * 3 + < 3453 > \\
 < 5382 > = < 3453 > * 1 + < 1929 > \\
 < 3453 > = < 1929 > * 1 + < 1524 > \\
 < 1929 > = < 1524 > * 1 + < 405 > \\
 < 1524 > = < 405 > * 3 + < 309 > \\
 < 405 > = < 309 > * 1 + < 96 > \\
 < 309 > = < 96 > * 3 + < 21 > \\
 < 96 > = < 21 > * 4 + < 12 > \\
 < 21 > = < 12 > * 1 + < 9 > \\
 < 12 > = < 9 > * 1 + < 3 > \\
 < 9 > = < 3 > * 3 + < 0 >
 \end{aligned}$$

Így $lnko(94542, 24981) = 3$.

b) $lnko(7732, 149)$ meghatározása

$$\begin{aligned}
 < 7732 > = < 149 > * 51 + < 133 > \\
 < 149 > = < 133 > * 1 + < 16 > \\
 < 133 > = < 16 > * 8 + < 5 > \\
 < 16 > = < 5 > * 3 + < 1 > \\
 < 5 > = < 1 > * 5 + < 0 >
 \end{aligned}$$

Így $lnko(7732, 149) = 1$.

2) A

$$lkkt(a, b) = \frac{a \cdot b}{lnko(a, b)}$$

összefüggés alapján $lkkt(56354, 2956) = \frac{56354 \cdot 2956}{2} = 83291212$.

3) Használjuk a

$$lnko(a, b, c) = (lnko(a, b), c)$$

összefüggést:

Mivel $\text{lnko}(65924, 33284) = 4$, így $\text{lnko}(65924, 33284, 53142) = \text{lnko}(4, 53142) = 2$.

4)a) Az Euklideszi algoritmus alapján:

$$\begin{aligned}(x^3 + 2x^2 - 2x + 1) &= (x^2 - x - 2) \cdot (x + 3) + (3x + 7) \\(x^2 - x - 2) &= (3x + 7) \cdot \left(\frac{1}{3}x - \frac{10}{9}\right) + \frac{52}{9} \\(3x + 7) &= \frac{52}{9} \cdot \left(\frac{27}{52}x + \frac{63}{52}\right) + 0\end{aligned}$$

amiből

$$\text{lnko}(p(x), q(x)) = \frac{52}{9} \sim 1 \text{ .}$$

Mivel az eredmény asszociált 1 -hez, ezért a két polinom *relatív prím* egymáshoz.

b) $f(x) = x^4 + 3x^3 - x^2 - 4x - 3$ és $g(x) = 3x^3 + 10x^2 + 2x - 3$. (Kuros 148.o.)

Az első osztás:

A hányados: $s(x) = 0.333 \cdot x - 0.111$

A maradék: $r(x) = -0.556 \cdot x^2 - 2.778 \cdot x - 3.333$

6) Mivel $f(x_0) = 0$ és $f'(x_0) \neq 0$, ezért x_0 csak 1 -szeres gyöke $f(x)$ -nek.

7)* Egy polinom gyökei egyszeresek pontosan akkor, ha négyzetmentes, azaz $\text{lnko}(p, p') \approx 1$. A $p(x) = ax^2 + bx + c$ polinomot deriváltjával maradékosan elosztva kapjuk

$$(ax^2 + bx + c) = (2ax + b) \cdot \left(\frac{1}{2}x + \frac{b}{4a}\right) + \left(c - \frac{b^2}{4a}\right)$$

ahonnan

$$\text{lnko}(p, p') = c - \frac{b^2}{4a}$$

hiszen p' elsőfokú. Vagyis a gyökök egyszerességének kritériuma a jólismert

$$\frac{-1}{4a}D = \frac{-1}{4a}(b^2 - 4ac) \neq 0$$

feltétel.

Lineáris Diophantikus egyenletek

1) b) $5682x + 4836y = 30$ egyenlet megoldása:

$$\langle 5682 \rangle = \langle 4836 \rangle * 1 + \langle 846 \rangle$$

$$\langle 4836 \rangle = \langle 846 \rangle * 5 + \langle 606 \rangle$$

$$\langle 846 \rangle = \langle 606 \rangle * 1 + \langle 240 \rangle$$

$$\langle 606 \rangle = \langle 240 \rangle * 2 + \langle 126 \rangle$$

$$\langle 240 \rangle = \langle 126 \rangle * 1 + \langle 114 \rangle$$

$$\langle 126 \rangle = \langle 114 \rangle * 1 + \langle 12 \rangle$$

$$\langle 114 \rangle = \langle 12 \rangle * 9 + \langle 6 \rangle$$

$$\langle 12 \rangle = \langle 6 \rangle * 2 + \langle 0 \rangle$$

tehát $\text{lko}(5682, 4836) = 6$

így

$$\begin{aligned} 6 &= 1 * \langle 114 \rangle + -9 * \langle 12 \rangle = \\ &= 1 * \langle 114 \rangle + -9 * (\langle 126 \rangle - 1 * \langle 114 \rangle) = -9 * \langle 126 \rangle + 10 * \langle 114 \rangle = \\ &= -9 * \langle 126 \rangle + 10 * (\langle 240 \rangle - 1 * \langle 126 \rangle) = 10 * \langle 240 \rangle + -19 * \langle 126 \rangle = \\ &= 10 * \langle 240 \rangle + -19 * (\langle 606 \rangle - 2 * \langle 240 \rangle) = -19 * \langle 606 \rangle + 48 * \langle 240 \rangle = \\ &= -19 * \langle 606 \rangle + 48 * (\langle 846 \rangle - 1 * \langle 606 \rangle) = 48 * \langle 846 \rangle + -67 * \langle 606 \rangle = \\ &= 48 * \langle 846 \rangle + -67 * (\langle 4836 \rangle - 5 * \langle 846 \rangle) = -67 * \langle 4836 \rangle + 383 * \langle 846 \rangle = \\ &= -67 * \langle 4836 \rangle + 383 * (\langle 5682 \rangle - 1 * \langle 4836 \rangle) = 383 * \langle 5682 \rangle + -450 * \langle 4836 \rangle = \end{aligned}$$

$$x_0 = 383 * C/d = 1915, \quad y_0 = -450 * C/d = -2250.$$

Az egyenlet általános megoldása:

$$x = x_0 + k * b/d = 1915 + k * 806, \quad y = y_0 + k * a/d = -2250 + k * 947 \quad (k \in \mathbb{Z})$$

1)c) $10518x + 5682y = 6$ egyenlet megoldása

$$\langle 10518 \rangle = \langle 5682 \rangle * 1 + \langle 4836 \rangle$$

$$\langle 5682 \rangle = \langle 4836 \rangle * 1 + \langle 846 \rangle$$

$$\langle 4836 \rangle = \langle 846 \rangle * 5 + \langle 606 \rangle$$

$$\langle 846 \rangle = \langle 606 \rangle * 1 + \langle 240 \rangle$$

$$\begin{aligned}
\langle 606 \rangle &= \langle 240 \rangle * 2 + \langle 126 \rangle \\
\langle 240 \rangle &= \langle 126 \rangle * 1 + \langle 114 \rangle \\
\langle 126 \rangle &= \langle 114 \rangle * 1 + \langle 12 \rangle \\
\langle 114 \rangle &= \langle 12 \rangle * 9 + \langle 6 \rangle \\
\langle 12 \rangle &= \langle 6 \rangle * 2 + \langle 0 \rangle \\
\text{Inko}(10518, 5682) &= 6 = 1 * \langle 114 \rangle + -9 * \langle 12 \rangle = \\
&= 1 * \langle 114 \rangle + -9 * (\langle 126 \rangle - 1 * \langle 114 \rangle) = -9 * \langle 126 \rangle + 10 * \langle 114 \rangle = \\
&= -9 * \langle 126 \rangle + 10 * (\langle 240 \rangle - 1 * \langle 126 \rangle) = 10 * \langle 240 \rangle + -19 * \langle 126 \rangle = \\
&= 10 * \langle 240 \rangle + -19 * (\langle 606 \rangle - 2 * \langle 240 \rangle) = -19 * \langle 606 \rangle + 48 * \langle 240 \rangle = \\
&= -19 * \langle 606 \rangle + 48 * (\langle 846 \rangle - 1 * \langle 606 \rangle) = 48 * \langle 846 \rangle + -67 * \langle 606 \rangle = \\
&= 48 * \langle 846 \rangle + -67 * (\langle 4836 \rangle - 5 * \langle 846 \rangle) = -67 * \langle 4836 \rangle + 383 * \langle 846 \rangle = \\
&= -67 * \langle 4836 \rangle + 383 * (\langle 5682 \rangle - 1 * \langle 4836 \rangle) = 383 * \langle 5682 \rangle + -450 * \langle 4836 \rangle = \\
&= 383 * \langle 5682 \rangle + -450 * (\langle 10518 \rangle - 1 * \langle 5682 \rangle) = -450 * \langle 10518 \rangle + 833 * \langle 5682 \rangle \\
x_0 &= -450 * C/d = -450, \quad y_0 = 833 * C/d = 833.
\end{aligned}$$

Az általános megoldás:

$$x = x_0 + k * b/d = -450 + k * 947, \quad y = y_0 + k * a/d = 833 + k * 1753 \quad (k \in \mathbb{Z})$$

1)d) $4512x + 1111y = 3248$ egyenlet megoldása

$$\begin{aligned}
\langle 4512 \rangle &= \langle 1111 \rangle * 4 + \langle 68 \rangle \\
\langle 1111 \rangle &= \langle 68 \rangle * 16 + \langle 23 \rangle \\
\langle 68 \rangle &= \langle 23 \rangle * 2 + \langle 22 \rangle \\
\langle 23 \rangle &= \langle 22 \rangle * 1 + \langle 1 \rangle \\
\langle 22 \rangle &= \langle 1 \rangle * 22 + \langle 0 \rangle \\
\text{Inko}(4512, 1111) &= 1 = \\
&= 1 * \langle 23 \rangle + (-1) * \langle 22 \rangle = \\
&= 1 * \langle 23 \rangle + -1 * (\langle 68 \rangle - 2 * \langle 23 \rangle) = -1 * \langle 68 \rangle + 3 * \langle 23 \rangle = \\
&= -1 * \langle 68 \rangle + 3 * (\langle 1111 \rangle - 16 * \langle 68 \rangle) = 3 * \langle 1111 \rangle + (-49) * \langle 68 \rangle = \\
&= 3 * \langle 1111 \rangle + -49 * (\langle 4512 \rangle - 4 * \langle 1111 \rangle) = -49 * \langle 4512 \rangle + 199 * \langle 1111 \rangle =
\end{aligned}$$

$$x_0 = 199 \cdot C/d = 646352, \quad y_0 = -49 \cdot C/d = -159152.$$

Az általános megoldás:

$$x = x_0 + k \cdot b/d = 646352 + k \cdot 4512, \quad y = y_0 + k \cdot a/d = -159152 + k \cdot 1111$$

$(k \in \mathbb{Z})$

2) a) Átalakítás után a $114x - 1683y = 3$ lineáris Diophantikus egyenletet kapjuk, aminek megoldása:

$$\langle 114 \rangle = \langle -1683 \rangle \cdot 0 + \langle 114 \rangle$$

$$\langle -1683 \rangle = \langle 114 \rangle \cdot -14 + \langle -87 \rangle$$

$$\langle 114 \rangle = \langle -87 \rangle \cdot -1 + \langle 27 \rangle$$

$$\langle -87 \rangle = \langle 27 \rangle \cdot -3 + \langle -6 \rangle$$

$$\langle 27 \rangle = \langle -6 \rangle \cdot -4 + \langle 3 \rangle$$

$$\langle -6 \rangle = \langle 3 \rangle \cdot -2 + \langle 0 \rangle,$$

$$\text{így } \text{lnko}(114, -1683) = 3 =$$

$$= 1 \cdot \langle 27 \rangle + 4 \cdot \langle -6 \rangle$$

$$= 1 \cdot \langle 27 \rangle + 4 \cdot (\langle -87 \rangle - 3 \cdot \langle 27 \rangle) = 4 \cdot \langle -87 \rangle + 13 \cdot \langle 27 \rangle$$

$$= 4 \cdot \langle -87 \rangle + 13 \cdot (\langle 114 \rangle - 1 \cdot \langle -87 \rangle) = 13 \cdot \langle 114 \rangle + 17 \cdot \langle -87 \rangle$$

$$= 13 \cdot \langle 114 \rangle + 17 \cdot (\langle -1683 \rangle - 14 \cdot \langle 114 \rangle) = 17 \cdot \langle -1683 \rangle + 251 \cdot \langle 114 \rangle$$

$$= 17 \cdot \langle -1683 \rangle + 251 \cdot (\langle 114 \rangle - 0 \cdot \langle -1683 \rangle) = 251 \cdot \langle 114 \rangle + 17 \cdot \langle -1683 \rangle$$

$$x_0 = 251 \cdot C/d = 251, \quad y_0 = 17 \cdot C/d = 17,$$

Az általános megoldás:

$$x = x_0 + k \cdot b/d = 251 + k \cdot 561, \quad y = y_0 + k \cdot a/d = 17 + k \cdot 38 \quad (k \in \mathbb{Z}).$$

A fentiek alapján a kongruencia megoldása: $x \equiv 251 \pmod{1683}$.

b) Átalakítás után a $18x - 175y = 1$ lineáris Diophantikus egyenletet kapjuk, aminek megoldása:

$$\langle 18 \rangle = \langle -175 \rangle \cdot 0 + \langle 18 \rangle$$

$$\langle -175 \rangle = \langle 18 \rangle \cdot -9 + \langle -13 \rangle$$

$$\langle 18 \rangle = \langle -13 \rangle \cdot -1 + \langle 5 \rangle$$

$$\langle -13 \rangle = \langle 5 \rangle \cdot -2 + \langle -3 \rangle$$

$$\langle 5 \rangle = \langle -3 \rangle \cdot -1 + \langle 2 \rangle$$

$$\begin{aligned} \langle -3 \rangle &= \langle 2 \rangle * -1 + \langle -1 \rangle \\ \langle 2 \rangle &= \langle -1 \rangle * -2 + \langle 0 \rangle, \text{ így} \end{aligned}$$

$$\begin{aligned} \text{lko}(18, -175) &= -1 = \\ &= 1 * \langle -3 \rangle + 1 * \langle 2 \rangle \\ &= 1 * \langle -3 \rangle + 1 * (\langle 5 \rangle - -1 * \langle -3 \rangle) = 1 * \langle 5 \rangle + 2 * \langle -3 \rangle \\ &= 1 * \langle 5 \rangle + 2 * (\langle -13 \rangle - -2 * \langle 5 \rangle) = 2 * \langle -13 \rangle + 5 * \langle 5 \rangle \\ &= 2 * \langle -13 \rangle + 5 * (\langle 18 \rangle - -1 * \langle -13 \rangle) = 5 * \langle 18 \rangle + 7 * \langle -13 \rangle \\ &= 5 * \langle 18 \rangle + 7 * (\langle -175 \rangle - -9 * \langle 18 \rangle) = 7 * \langle -175 \rangle + 68 * \langle 18 \rangle \\ &= 7 * \langle -175 \rangle + 68 * (\langle 18 \rangle - 0 * \langle -175 \rangle) = 68 * \langle 18 \rangle + 7 * \langle -175 \rangle \end{aligned}$$

$$x_0 = 68 * C/d = -68, y_0 = 7 * C/d = -7.$$

Az általános megoldás:

$$x = x_0 + k * b/d = -68 + k * 175, y = y_0 + k * a/d = -7 + k * -18 \quad (k \in \mathbb{Z}).$$

A fentiek alapján a 18 multiplikatív inverze: $18^{-1} \equiv -68 \equiv 107 \pmod{175}$

3) Ha m jelöli a keresett számot, akkor

$$\begin{cases} 25707 \equiv 32 \pmod{m} \\ 37568 \equiv 43 \pmod{m} \end{cases}$$

ahonnan

$$\begin{cases} 25707 = k \cdot m + 32 \\ 37568 = \ell \cdot m + 43 \end{cases}$$

vagyis

$$m \mid \text{lko}(25707 - 32, 37568 - 43) = \text{lko}(25675, 37525) = 1975.$$

Mivel m négyjegyű, ezért $m = 1975$ lehet csak a megoldás.

4)a) Mivel teljesül a $3 = \text{lko}(12, 30, 15) \mid 18$ (szükséges) feltétel, ezért az egyenletnek léteznek egész gyökei.

Egyszerűsítés után a

$$4x + 10y + 5z = 6 \quad (2.1)$$

egyenletet kapjuk.

Először megoldjuk a *kétismeretlenes*

$$4x + 10y = 6 - 5z \quad (2.2)$$

egyenletet ($z \in \mathbb{Z}$ paraméter): $lnko(4, 10) = 2$ és $lkkt(4, 10) = 20$ alapján a megoldás

$$x = \left(-2 - \frac{20}{4}k\right) \cdot \left(\frac{6 - 5z}{2}\right), \quad y = \left(1 + \frac{20}{10}k\right) \cdot \left(\frac{6 - 5z}{2}\right) \quad (2.3)$$

feltéve, hogy $6 - 5z$ osztható 2 -vel. Ez utóbbi feltétel

$$6 - 5z = 2\ell, \quad \text{vagyis} \quad 6 = 5z + 2\ell$$

alakban írható, amely egyenlet megoldása:

$$z = 6 + t * 2, \quad \ell = -12 + t * 5 \quad (t \in \mathbb{Z}),$$

ami alapján a (2.1) egyenlet általános megoldása

$$\begin{aligned} x_0 &= \left(-2 - \frac{20}{4}k\right) \cdot \ell = \left(-2 - \frac{20}{4}k\right) \cdot (-12 + t * 5), \\ y_0 &= \left(1 + \frac{20}{10}k\right) \cdot \ell = \left(1 + \frac{20}{10}k\right) \cdot (-12 + t * 5), \\ z_0 &= 6 + t * 2, \quad k, t \in \mathbb{Z}. \end{aligned}$$

Az eredeti egyenlet megoldása tehát $(lnko(12, 30, 15) = 3)$ alapján

$$\begin{aligned} x &= 3 \cdot \left(-2 - \frac{20}{4}k\right) \cdot (-12 + t * 5), \\ y &= 3 \cdot \left(1 + \frac{20}{10}k\right) \cdot (-12 + t * 5), \\ z &= 3 \cdot (6 + t * 2), \quad k, t \in \mathbb{Z}. \end{aligned}$$

Kínai maradéktétel

Mivel a $7, 9, 11$ modulusok páronként relatív prímek, ezért $\Pi = lkkt(7, 9, 11) = 7 \cdot 9 \cdot 11 = 693$. Ekkor az $y_i \cdot \frac{\Pi}{m_i} \equiv 1 \pmod{m_i}$ alakú

$$y_1 \cdot 99 \equiv y_1 \cdot 1 \equiv 1 \pmod{7}$$

$$y_2 \cdot 77 \equiv y_2 \cdot 5 \equiv 1 \pmod{9}$$

$$y_3 \cdot 63 \equiv y_3 \cdot 8 \equiv 1 \pmod{11}$$

kongruenciákat kell először megoldanunk, amelyek (egyik) megoldása $y_1 = 1$, $y_2 = 2$ és $y_3 = 7$. Az eredeti kongruenciarendszer megoldása

$$x \equiv \sum_{i=1}^3 a_i y_i \frac{\Pi}{m_i} \equiv 2 \cdot 1 \cdot 99 + 3 \cdot 2 \cdot 77 + 3 \cdot 7 \cdot 63 \equiv 597 \pmod{693} .$$

az eredeti kongruenciarendszer :

$$\begin{cases} x \equiv 1 \pmod{2} \\ x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$$

de itt a modulusok nem relatív prímek. !!!

Mivel az első kongruencia következik a harmadikból, így elegendő csak az utolsó hármat tekintenünk:

$$\begin{cases} x \equiv 2 \pmod{3} \\ x \equiv 3 \pmod{4} \\ x \equiv 4 \pmod{5} \end{cases}$$

Ennek megoldása: $M = 60$, $A_1 = 20$, $A_2 = 15$, $A_3 = 12$ és $y_1 = -1$, $y_2 = -1$, $y_3 = -2$, ami alapján $x = -1 \equiv 59 \pmod{60}$ vagyis $x = 59 + 60k$ ($k \in \mathbb{Z}$) .

A kongruenciarendszert kielégítő legkisebb *természetes* szám $x = 59$.

II. megoldás (rövidebb): Mivel a kongruenciarendszer *speciális* alakú:

$$x \equiv m_i - 1 \pmod{m_i} \quad /m_1 = 2, m_2 = 3, m_3 = 4, m_4 = 5/ ,$$

ezért a megoldás

$$x \equiv M - 1 \pmod{M} \quad ahol \quad M = lkkt(m_1, \dots, m_4) = 60 .$$

2.5 Testek

- 3) a) $GF(4) = (\mathbb{Z}_2[x], +, \cdot) / (x^2 + x + 1)$,
 b) $GF(9) = (\mathbb{Z}_3[x], +, \cdot) / (x^2 - 2)$,

Függelék

.1 Jelölések, definíciók

$\circ :=$ függvények kompozíciója (összetett függvény képzése),

$\underline{0}, \underline{1} :=$ az azonosan 0 ill. 1 mátrix,

$\underline{0} := \underline{c}$ az azonosan 0 függvény (ld. $\underline{c}$),

$A^B := \{f : B \rightarrow A \mid f \text{ függvény} \}$,

$A^A := \{f : A \rightarrow A \mid f \text{ függvény} \}$,

$\mathcal{A}_\circ := (A^A, \circ)$ (félcsoporth),

$A^n := A^{\mathbb{I}_n} = \{(a_1, \dots, a_n) \mid a_i \in A\} =$ az A halmaz Descartes-hatványa,

$A^0 := \{\emptyset\}$,

$A^* := \bigcup_{n=0}^{\infty} A^n =$ az A halmaz elemeiből képezhető összes rendezett n -es

(véges hosszú sorozat, string) halmaza,

$A_n := \{\sigma \in S_n : \sigma \text{ páros} \}$,

$\mathcal{A}_n := (A_n, \circ)$ az n -edrendű alternáló csoport⁽²⁾,

$a \hat{\ } b :=$ az $a, b \in A^*$ sorozatok egymáshoz fűzése (összefűzése, konkatenációja),

$a|b :=$ a osztója b -nek, vagyis b osztható a -val,

$a \equiv_m b$ vagy $a \equiv b \pmod{m} : \stackrel{def}{\iff} m|a - b$ ($\Leftrightarrow$ a és b ugyanazt a maradékot adja m -el elosztva),

$a \approx b =$ asszociált elemek egységelemes gyűrűkben,

$(a, b) := luko(a, b) :=$ a és b legnagyobb közös osztója,

$[a, b] := lkkt(a, b) :=$ a és b legkisebb közös többszöröse,

$[H] :=$ a H részhalmaz által generált részstruktúra,

$[\underline{u}_1, \dots, \underline{u}_k] :=$ az $\underline{u}_1, \dots, \underline{u}_k$ vektorok által kifeszített (generált) altér,

²⁾ $\mathcal{A}_n \leq S_n$ az n -edrendű **alternáló csoport** ahol $\mathcal{A}_n$ alaphalmaza $A_n :=$

$\{\pi \in S_n \mid sgn(\pi) = 1\}$. $\square$

$\underline{c} :=$ az azonosan c függvény ($c \in A$): $\underline{c} : A \rightarrow A$, $\underline{c}(x) := c$ minden $x \in A$ elemre,

$\mathbb{C}[x] :=$ komplex együtthatójú polinomok halmaza,

$D_n := [\{f, t\}] =$ a szabályos n -szög transzformációcsoportja = az n -edrendű f forgatás és a másodrendű tengelyes tükrözés által generált csoport, az ún. n -edrendű **diédercsoport**,

$D_\infty := [\{f, t\}] =$ a kör transzformációcsoportja = a ∞ -edrendű f forgatás és a másodrendű tengelyes tükrözés által generált csoport, a ∞ -rendű **diédercsoport**,

$\deg(p) :=$ a $p(x)$ polinom fokszáma,

$\Delta := A \times A =$ **azonosság reláció**, ,

$E \in \mathbb{R}^{n \times n} :=$ az egységmátrix,

$\mathcal{F}_X := (X^*, \wedge)$ az $X \neq \emptyset$ halmaz által generált **szabad félcsoport**,

$\varphi(n) :=$ Euler-féle φ függvény = az n természetes számnál kisebb, hozzá relatív prím természetes számok száma,

$GF(q) :=$ a $q = p^n$ -edrendű véges test, azaz **Galois-test** ,

$\Gamma :=$ tetszőleges test,

$\Gamma[x] :=$ a Γ test feletti (együtthatójú) egyhatározatlanú (egyismeretlenes) polinomok halmaza,

$\Gamma_n[x] :=$ a legfeljebb n -edfokú, $\Gamma[x]$ -beli polinomok halmaza,

$\iota := \{ (a, a) \mid a \in A \}$ **egyenlőség**,

$id_A : A \rightarrow A$ az *identikus* leképezés (függvény): $id_A(a) = a$ minden $a \in A$ elemre,

$\mathbb{I}_n^0 := \{0, 1, \dots, n-1\}$ ($n \in \mathbb{N}$ természetes szám),

$\mathbb{I}_n := \{1, 2, \dots, n\}$ ($n \in \mathbb{N}$ természetes szám),

$\mathbb{I}_n = \mathbb{I}_n^0 = \emptyset$ (az előzőből következik),

$(m) := \{m \cdot x : x \in \mathbb{Z}\}$ (m többszörösei) = az m által generált főideál $\mathbb{Z}$ -ben,

$\mathbb{P} :=$ prímszámok halmaza,

$P(X) := \{A \mid A \subseteq X\}$ az X halmaz **hatványhalmaza** ("power set"),

$\Pi := (T, \cdot)$ az 1-dimenziós **tórusz**, ahol $T := \{z \in \mathbb{C} \mid |z| = 1\}$.

$\mathbb{Q} :=$ racionális számok halmaza,

$\mathbb{Q}[\alpha] := \{q_0 + q_1\alpha + q_2\alpha^2 + \dots + q_{n-1}\alpha^{n-1} \mid q_i \in \mathbb{Q}\}$ a $\mathbb{Q}$ test **algebrai bővítése** ha $\alpha \in \mathbb{R}$ n -edrendű **algebrai szám**⁽³⁾

³⁾ **Definíció:** az $\alpha \in \mathbb{R}$ valós szám **n -edrendű algebrai szám** a $\mathbb{Q}$ test felett, ha α gyöke egy valamilyen n -edfokú racionális együtthatójú polinomnak. $\square$

$\mathcal{Q} := (\{ 1, -1, i, -i, j, -j, k, -k \} , \cdot)$ a **kvaterniócsoport**: $ij = -ji = k, jk = -kj = i, ki = -ik = j$, a többi művelet értelemszerűen,

$\mathcal{Q} := (\{ a + bi + cj + dk \mid a, b, c, d \in \mathbb{R} \} , +, \cdot)$ a **kvaterniók teste**,

$(\mathbb{R}/r, +, \cdot) := ([0, r), +, \cdot)$ a valós számok szokásos műveleteit modulo r végezzük,

$\mathbb{R}^{n \times n} := n \times n$ méretű (négyzetes) valós mátrixok halmaza,

$(\mathbb{R}^{n \times n})^* :=$ invertálható mátrixok halmaza,

$\mathbb{R}_{\Delta}^{n \times n} :=$ alsó háromszögmátrixok halmaza,

$(\mathbb{R}_{\Delta}^{n \times n})^* :=$ invertálható alsó háromszögmátrixok halmaza,

$\mathbb{R}_{\nabla}^{n \times n} :=$ felső háromszögmátrixok halmaza,

$(\mathbb{R}_{\nabla}^{n \times n})^* :=$ invertálható felső háromszögmátrixok halmaza,

$\mathbb{R}_{\setminus}^{n \times n} :=$ diagonális mátrixok halmaza,

$(\mathbb{R}_{\setminus}^{n \times n})^* :=$ invertálható diagonális mátrixok halmaza,

$\mathbb{R}^{\mathbb{R}} := \{ f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ függvény} \}$,

$\mathbb{R}[x] :=$ valós együtthatójú polinomok halmaza,

$\mathbb{R}_{Lin}^{\mathbb{R}} := \{ f : \mathbb{R} \rightarrow \mathbb{R} \mid f \text{ lineáris függvény}^{(4)} \}$,

$\mathbb{R}_{LinRac}^{\mathbb{R}} := \{ f : \mathbb{R} \rightarrow \mathbb{R} \mid f(x) = \frac{ax+b}{cx+d} \text{ lineáris racionális törtfüggvény}^{(5)}, c \neq 0 \text{ vagy } d \neq 0 \}$,

$S_A := \{ f : A \rightarrow A \mid f \text{ bijekció} \}$ ($A \neq \emptyset$ tetszőleges halmaz),

$S_A := (S_A, \circ) =$ **szimmetrikus csoport** A -n,

$S_n := S_H$ ahol $H = \mathbb{I}_n$,

$S_n := (S_n, \circ) = n$ -edrendű **szimmetrikus csoport**,

$\mathbb{Z}^- := \mathbb{Z} \setminus \{0\}$,

$\mathbb{Z}_m := \{0, 1, \dots, m-1\} = a \bmod m$ - szerinti **maradékosztályok**,

$\mathbb{Z}_m^* := \{ i < m : \lnko(i, m) = 1 \} = \bmod m$ **redukált maradékosztályok**,

$\mathbb{Z}[u] := \{ a + bu \mid a, b \in \mathbb{Z} \} = \mathbb{Z}$ algebrai bővítése ahol $u \in \mathbb{C}$ egy tetszőleges másodfokú algebrai szám (másodfokú egyenlet gyöke),

$\mathbb{Z}[x] :=$ egész együtthatójú polinomok halmaza

⁴⁾ **Definíció:** $f : \mathbb{R} \rightarrow \mathbb{R}$ **lineáris függvény**, ha $f(x) = ax + b$ alakú ($a, b \in \mathbb{R}$)

. □

⁵⁾ **Definíció:** az $f(x) = \frac{ax+b}{cx+d}$ alakú ($a, b, c, d \in \mathbb{R}$, c és d egyszerre nem 0) függvényeket **lineáris racionális függvényeknek** hívjuk. □

.2 Felhasznált és ajánlott irodalom

[*BCzSz*] **Bálintné Sz.Mária, Czédli Gábor, Szendrei Ágnes:** *Abstract algebrai feladatok*, Egyetemi jegyzet, JATE, Szeged, 1993.

[*SA*] **Sárközy András:** *Számelmélet*, példatár, ("Bolyai Könyvek" sorozat), Műszaki Kiadó, Budapest, 1976.

[*SASJ*] **Sárközy András, Surányi János:** *Számelmélet feladatgyűjtemény*, Egyetemi jegyzet, ELTE, Budapest, 1979.

[*SzÁ*] **Szendrei Ágnes:** *Diszkrét matematika*, Polygon könyvtár, Szeged, 1994

[*SzI*] **Szalkai István:** *Diszkrét Matematika Feladatgyűjtemény*, Veszprémi Egyetemi Kiadó, 1997. .

Tárgymutató

15-ös játék, 10

algebra, 4

algebrai szám, 38

algebrai testbővítés, 38

alternáló

 csoport, 37

azonosság

 - reláció, 38

azonosság - reláció, 2

csoport

 alternáló, 37

 diéder-, 38

 n-edrendű szimmetrikus, 39

 szimmetrikus, 39

diédercsoport

 n -edrendű, 38

 végtelenrendű, 38

egyenesserreg, 19

egyenlőség

 reláció, 38

egyenlőség - reláció, 2

elem rákövetkezője, 5

független halmazok (minőségileg),

 1

függvény

 lineáris, 39

 racionális tört-, 39

félcsoport

 szabad, 38

Galois - test, 38

halmaz

 jólrendezett, 5

hasonló mátrixok, 2

hatványhalmaz, 38

idempotens elem, 8

involutorius művelet, 8

jólrendezett halmaz, 5

kollineáris (pontok), 1

kombinett játék, 10

kommutáló elemek, 9

koplanáris (pontok), 1

kvaternió - test, 39

kvaterniócsoport, 39

lineáris

 függvény, 39

Loyd, Sam, 10

mátrixok hasonlósága, 2

maradékosztályok, 39

 redukált, 39

minőségileg független halmazok, 1

párhuzamos

 vektorok, 2

power set, 38

primitív gyök, 12

rákövetkező, 5

racionális tört

 függvény, 39

redukált

maradékosztályok, 39

reláció

azonosság, 38

durvább, 4

egyenlőség, 38

finomabb, 4

relatív prím (egész számok), 1

successor, 5

sugársor, 19

szabad

félcsoport, 38

szimmetrikus

csoport, 39

szimmetrikus csoport

n -edrendű, 39

tórusz, 1-dimenziós, 38

test

algebrai bővítése, 38

végyszerűen egyenlő síkidomok, 2