ALGEBRA

Andrei Marcus

Babeş-Bolyai Tudományegyetem
Matematika és Informatika Kar
Algebra Tanszék

2005. szeptember 15.

Előszó

A XX. század első felében az algebra a matematika egyik igen fontos és teljesen önálló módszerekkel dolgozó ágává fejlődött. Napjainkban bizonyos mértékig kihat a matematika más ágainak fejlődésére is.

E könyv bevezetést szeretne nyújtani az ú.n. „absztrakt algebrába”, célja megismertetni az olvasóval az alapvető csoport-, gyűrűelméleti és lineáris algebrai fogalmakat és eredményeket. Az anyag jobb megértésének érdekében az elméletet gyakorlatok és feladatok egészítik ki. A könyvet elsősorban matematika, informatika és fizika szakos egyetemi halgatóknak állítottuk össze, de figyelmébe ajáljuk a liceum felső osztályaiban tanuló diákoknak és tanárainak. Tekintetbe véve az algebra számtalan alkalmazási lehetőségét, a könyv hasznos lehet a mérnöki vagy a közgazdasági területeken dolgozó, ezen eredményeket alkalmazó szakemberek számára is.

Tartalomjegyzék

1. Algebrai struktúrák **1**
1.1. Halmazok és relációk . . . 1
1.1.1. Számhalmazok . . . 1
1.1.2. Egész számok aritmetikája . . . 1
1.1.3. Relációk és függvények . . . 3
1.1.4. Rendezési és ekvivalencia relációk . . . 3
1.1.5. Kardinális számok . . . 5
1.2. Csoportok . . . 6
1.2.1. A csoport fogalma. Példák . . . 6
1.2.2. Csoportmorfizmusok . . . 8
1.2.3. Részcsoportok . . . 8
1.2.4. Az S_n szimmetrikus csoport . . . 10
1.3. Gyűrűk és testek . . . 11
1.3.1. A gyűrű fogalma. Példák . . . 11
1.3.2. Gyűrűmorfizmusok . . . 13
1.3.3. Részgyűrűk, résztestek . . . 16
1.4. Polinomok . . . 18
1.4.1. A polinomgyűrű szerkesztése . . . 18
1.4.2. Polinomgyűrű univerzális tulajdonsága . . . 19
1.4.3. A maradékos osztástétel. Polinomok gyökei . . . 20
1.5. Modulusok, vektorterek, algebrák . . . 21
1.5.1. Alapfogalmak . . . 21
1.5.2. Részmodulusok, részterek, részalgebrák . . . 23
1.5.3. Lineáris függvények . . . 24

2. Lineáris algebra **26**
2.1. Lineáris függőség és függetlenség. Bázis . . . 26
2.1.1. Lineáris kombinációk. Szabad modulus . . . 26
2.1.2. Szabad modulusok univerzális tulajdonsága . . . 28
2.1.3. Steinitz-tétel. Vektortér dimenziója . . . 29
2.1.4. Dimenzióra vonatkozó képletek . . . 30
2.1.5. Lineáris függvény mátrixa . . . 31
2.1.6. Báziscsere . . . 33
2.2. Determinánsok és mátrixok . . . 34
2.2.1. A determináns értelmezése . . . 34
2.2.2. A determináns induktív értelmezése . . . 35
2.2.3. Determinánsok tulajdonságai. Invertálható mátrixok . . . 38
2.2.4. Mátrix rangja . . . 43
2.3. Lineáris egyenletrendszerek . . . 44
2.3.1. A Kronecker–Capelli-tétel . . . 44
2.3.2. Egyenletrendszerek megoldása . . . 45
2.3.3. Algoritmikus módszerek . . . 48
2.4. Sajátértékek és sajátvektorok . . . 53
2.4.1. Karakterisztikus polinom . . . 53
2.4.2. Triangularizálható endomorfizmusok . . . 55
2.4.3. Diagonalizálható endomorfizmusok . . . 57
2.4.4. Jordan-féle kanonikus alak . . . 59
2.5. Bilineáris és kvadratikus alakok . . . 70
2.5.1. Bilineáris és kvadratikus alakok . . . 70
2.5.2. Valós kvadratikus alakok négyzetösszegre való redukciója . . . 72

2.5.3. Sylvester-féle tehetetlenségi törvény . . . 74
2.5.4. Hermitikus alakok . . . 74
2.6. Euklideszi tér és unitér tér . . . 76
2.6.1. Skaláris szorzat . . . 76
2.6.2. Ortonormált bázis . . . 77
2.6.3. Ortogonális és unitér transzformációk . . . 79
2.6.4. Adjungált transzformáció . . . 80
2.6.5. Normális transzformációk . . . 81

3. Csoportok **84**
3.1. Részcsoportok . . . 84
3.1.1. Részcsoportok hálója . . . 84
3.1.2. Részhalmaz által generált részcsoport . . . 85
3.1.3. Ciklikus részcsoport . . . 85
3.1.4. Ciklikus permutációk . . . 87
3.1.5. A diédercsoport . . . 89
3.2. Kongruenciarelációk és normális részcsoportok . . . 90
3.2.1. Részcsoport szerinti mellékosztályok . . . 90
3.2.2. Normális részcsoport . . . 91
3.3. Faktorcsoport. Izomorfizmustételek . . . 93
3.4. Elem rendje . . . 96
3.5. Csoportok és részcsoportok direkt szorzata . . . 99
3.6. Belső automorfizmus. Konjugáltsági reláció . . . 101
3.7. Struktúratételek: p-, $2p$- és p^2-ed rendű csoportok . . . 104
3.8. Karakterisztikus és teljesen invariáns részcsoportok . . . 106
3.8.1. Kommutátorok. A derivált részcsoport . . . 106
3.9. Csoportok láncai . . . 108
3.9.1. A felső centrális lánc . . . 109
3.9.2. A derivált lánc és az alsó centrális lánc . . . 109
3.9.3. Kompozícióláncok . . . 110
3.10. Nilpotens csoportok . . . 113
3.11. Feloldható csoportok . . . 116

4. Gyűrűk, testek, polinomok **118**
4.1. Ideálok . . . 118
4.2. Részgyűrűk és ideálok hálója . . . 119
4.3. Faktorgyűrű . . . 121
4.3.1. Kongruenciarelációk . . . 121
4.3.2. Faktorgyűrű szerkesztése . . . 122
4.3.3. Izomorfizmustételek . . . 122
4.3.4. Modulo n maradékosztályok gyűrűje . . . 123
4.4. Gyűrűk direkt szorzata . . . 124
4.5. Prímtest. Test karakterisztikája . . . 124
4.6. Hányadosgyűrűk . . . 126
4.7. Polinomok és algebrai egyenletek . . . 131
4.7.1. Polinom deriváltja. Többszörös gyökök . . . 131
4.7.2. Többhatározatlanú polinomok . . . 133
4.7.3. Szimmetrikus polinomok . . . 134
4.7.4. Diszkrimináns és rezultáns . . . 137
4.7.5. Algebrai egyenletek . . . 139
4.8. Integritástartományok aritmetikája . . . 141
4.8.1. Oszthatóság. Prímelem és irreducibilis elem . . . 141
4.8.2. Faktoriális gyűrűk . . . 143
4.8.3. Főideálgyűrűk . . . 144
4.8.4. Euklideszi gyűrűk . . . 145
4.8.5. Polinomgyűrűk aritmetikája . . . 147
4.9. Prímideálok és maximális ideálok . . . 150

5. Testbővítések és Galois-elmélet **152**
5.1. Véges bővítések . . . 152
5.2. Algebrai bővítések . . . 153
5.3. Egy gyök adjunkciója. Polinom felbontási teste . . . 158
5.4. Véges testek . . . 162
5.5. Algebrailag zárt testek. Egy test algebrai lezártja . . . 167
5.6. Szeparábilis algebrai bővítések . . . 169
5.7. Normális algebrai bővítések . . . 171
5.8. Galois-csoport . . . 173
5.9. A Galois-elmélet alaptétele . . . 177
5.10. Gyökképlettel megoldható algebrai egyenletek . . . 182
5.11. Geometriai szerkeszthetőség . . . 184
5.11.1. Körzővel és vonalzóval szerkeszthető komplex számok . . . 184
5.11.2. Körzővel és vonalzóval való szerkeszthetőség első kritériuma . . . 186
5.11.3. Szögharmadolás . . . 187
5.11.4. A Déloszi probléma (kockakettőzés) . . . 187
5.11.5. Háromszögszerkesztési feladat . . . 187
5.11.6. A kör négyszögesítése . . . 188
5.11.7. Szerkeszthetőség második kritériuma . . . 188
5.11.8. Szabályos n-szög szerkesztése . . . 189
5.11.9. Szabályos ötszög és tízszög szerkesztése . . . 189

6. Elemi és algebrai számelmélet **191**
6.1. Oszthatósag $\mathbb{Z}$-ben . . . 191
6.1.1. Maradékos osztás . . . 191
6.1.2. Oszhatóság. Legnagyobb közös osztó . . . 192
6.1.3. Prímszámok . . . 193
6.1.4. Számelméleti függvények . . . 195
6.2. Kongruenciák . . . 198
6.2.1. A $\mathbb{Z}_n$ gyűrű . . . 198
6.2.2. Pszeudoprímszámok . . . 201
6.2.3. A kínai maradéktétel . . . 202
6.2.4. Magasabbfokú kongruenciák . . . 203
6.2.5. Az $(U(\mathbb{Z}_m), \cdot)$ csoport struktúrája . . . 204
6.2.6. Primitív gyökök és indexek . . . 207
6.2.7. Binom kongruenciák megoldása . . . 208
6.3. Kvadratikus maradékok . . . 212
6.3.1. A másodfokú kongruencia . . . 212
6.3.2. A Legendre-szimbólum . . . 212
6.3.3. Kvadratikus reciprocitás . . . 213
6.3.4. A Jakobi-szimbólum . . . 216
6.4. Kvadratikus egészek . . . 218
6.4.1. Kvadratikus egészek . . . 218
6.4.2. Prímszámok felbontása A_K-ban . . . 219
6.4.3. Euklideszi gyűrűk . . . 221
6.5. Diofantikus egyenletek . . . 223
6.5.1. Az $a_1x_1 + \cdots + a_nx_n = m$ elsőfokú egyenlet . . . 223
6.5.2. Redukció modulo p . . . 224
6.5.3. A Pithagoraszi számhármasok . . . 225
6.5.4. A $\mathbb{Z}[i]$ Gauss-egészek gyürüje. Négyzetszámok összege . . . 226
6.5.5. Az Euler-egészek gyűrűje. Az $x^3 + y^3 = z^3$ egyenlet . . . 229
6.5.6. A Pell-egyenlet . . . 231

Irodalomjegyzék **234**

1. fejezet

Algebrai struktúrák

1.1. Halmazok és relációk

1.1.1. Számhalmazok

Ismertnek tekintjük a következő számhalmazokat, és a valós számokkal végzett műveletek tulajdonságait:

- $\mathbb{N} = \{0, 1, 2, \dots\}$ – természetes számok;
- $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ – egész számok;
- $\mathbb{Q} = \{\frac{m}{n} \mid m, n \in \mathbb{Z},\ n \neq 0\}$ – racionális számok;
- $\mathbb{R}$ – valós számok;

Továbbá, $\mathbb{N}^* = \mathbb{N} \setminus \{0\}$, $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$, $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$, $\mathbb{R}^* = \mathbb{R} \setminus \{0\}$, $\mathbb{R}^*_+ = \{x \in \mathbb{R} \mid x > 0\}$.
Alapvető tulajdonság, hogy $\mathbb{N}$ minden nemüres részhalmazának van legkisebb eleme.

1.1.2. Egész számok aritmetikája

A következőkben néhány fontos fogalmat és tételt említünk. A bizonyításukra később kerül sor egy általánosabb kontextusban.

1.1.1. tétel (Maradékos osztás tétele). *Ha* $a, b \in \mathbb{Z}$ *és* $b \neq 0$*, akkor léteznek és egyértelműen meghatározottak* q *és* $r \overset{\text{jel}}{=} (a \mod b)$ *egész számok úgy, hogy*

$$a = bq + r, \qquad 0 \leq r < |b|.$$

Bizonyítás. Legyen $r := \min(\{a - kb \mid k \in \mathbb{Z}\} \cap \mathbb{N})$, és legyen $q := (a - r)/b$, téhát q és r léteznek.
Ha $a = bq + r = bq_1 + r_1$, ahol $0 \leq r, r_1 < |b|$, akkor $|b||q - q_1| = |r - r_1| < |b|$, tehát $q - q_1 = 0$, és innen $r = r_1$. ■

A következő eljárást **Euklideszi algoritmus**nak nevezzük.

$$\begin{aligned}
a &= bq_1 + r_1, \quad 0 < r_1 < |b|;\\
b &= r_1 q_2 + r_2, \quad 0 < r_2 < r_1;\\
r_1 &= r_2 q_3 + r_3, \quad 0 < r_3 < r_2;\\
&\dots\\
r_{n-3} &= r_{n-2} q_{n-1} + r_{n-1}, \quad 0 < r_{n-1} < r_{n-2};\\
r_{n-2} &= r_{n-1} q_n + r_n, \quad 0 < r_n < r_{n-1};\\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, \quad r_{n+1} = 0.
\end{aligned}$$

Valóban, mivel az (r_k) sorozat szigorúan csökkenő, létezik n úgy, hogy $r_{n+1} = 0$. Azt mondjuk, hogy r_n az *utolsó nemnulla maradék.*

1.1.2. definíció. Legyenek a és b egész számok.
a) a **osztója** b-nek (jelölés: $a|b$) ha létezik $x \in \mathbb{Z}$ úgy, hogy $b = ax$.
b) Egy $d \in \mathbb{N}$ szám az a és b **legnagyobb közös osztója**, (jelölés: $d = (a, b)$) ha

1. $d|a$ és $d|b$;
2. ha $d' \in \mathbb{Z}$, $d'|a$ és $d'|b$, akkor $d'|d$.

c) Egy $m \in \mathbb{N}$ szám az a és b **legkisebb közös többszöröse**, (jelölés: $m = [a, b]$) ha

1. $a|m$ és $b|m$;
2. ha $m' \in \mathbb{Z}$, $a|m'$ és $b|m'$, akkor $m|m'$.

d) a és b relatív prímek ha $(a, b) = 1$.
e) $p \in \mathbb{N}$ **prímszám**, ha $p \neq 1$, és ha $a \in \mathbb{Z}$, $a|p$, akkor $a = \pm 1$ vagy $a = \pm p$.

1.1. feladat. a) 0 osztható minden számmal; minden szám osztható 1-gyel.
b) $a|b,\ a|c \Rightarrow a|b \pm c$.
c) $a|b \Rightarrow ax|bx$ minden $x \in \mathbb{Z}$ esetén. Fordítva, ha $ax|bx,\ x \neq 0$, akkor $a|b$.

1.2. feladat. a) Legyen $a, b \in \mathbb{Z}$. Ha $a = b = 0$, akkor $(a, b) = 0$. Ellenkező esetben, legyen

$$d := \min\{ax + by \mid x, y \in \mathbb{Z},\ ax + by > 0\}$$

és igazoljuk, hogy ekkor $d = (a, b)$.
(Tehát (a, b) létezik, és mitöbb, léteznek az $u, v \in \mathbb{Z}$ úgy, hogy $(a, b) = au + bv$.)
b) $(a, b) = 1 \Leftrightarrow (\exists) u, v \in \mathbb{Z}$ úgy, hogy $au + bv = 1$. (Ebben az esetben azt mondjuk, hogy a és b *relatív prímek.*)

1.3. feladat. a) Ha $a = bq + r$, akkor $(a, b) = (b, r)$.
b) Az Euklideszi algoritmusban $\boxed{r_n = (a, b)}$.
c) Igazoljuk, hogy az Euklideszi algoritmus segítségével meg lehet határozni az u és v számokat úgy, hogy $(a, b) = au + bv$.
d) Az euklideszi algoritmust alkalmazva, számítsuk ki a következő számok legnagyobb közös osztóját, és fejezzük ki a két szám lineáris kombinációjaként:
(1) $a = 19,\ b = 26$.
(2) $a = 1082,\ b = 458$.
(3) $a = -187,\ b = 34$.
(4) $a = -841,\ b = -160$.
(5) $a = 2613,\ b = -2171$.
e) Ha $x \in \mathbb{N}$, akkor $(ax, bx) = (a, b)x$.
f) Ha $d = (a, b)$, $a = da'$ és $b = db'$, akkor $(a', b') = 1$.
g) Legyen $a, b, c \in \mathbb{Z}$ úgy, hogy $(a, b) = 1$. Igazoljuk, hogy :
(1) $(a, c) = 1 \Rightarrow (a, bc) = 1$; (2) $a|bc \Rightarrow a|c$; (3) $a|c$ és $b|c \Rightarrow ab|c$.
h) Ha $d = (a, b)$, $a = da'$ és $b = db'$, akkor

$$[a, b] = a'b'd = \frac{ab}{d}.$$

i) Legyen $p \in \mathbb{N}$, $p > 1$. Igazoljuk, hogy p prímszám $\Leftrightarrow$ minden $a, b \in \mathbb{Z}$ esetén, ha $p|ab$, akkor $p|a$ vagy $p|b$.

1.1.3. definíció. Legyenek $x_1, \ldots, x_n$ egész számok, ahol $n \in \mathbb{N}^*$, és legyen $d, m \in \mathbb{N}$. Értelmezés szerint,

a) $d = (x_1, \ldots, x_n) \Longleftrightarrow \begin{cases} d|x_1, \ldots, d|x_n, \\ \text{ha } d'|x_1, \ldots, d'|x_n, \text{ akkor } d'|d. \end{cases}$

b) $m = [x_1, \ldots, x_n] \Longleftrightarrow \begin{cases} x_1|m, \ldots, x_n|m, \\ \text{ha } x_1|m', \ldots, x_n|m', \text{ akkor } m|m'. \end{cases}$

1.4. feladat. Legyenek $x_1, \ldots, x_n$ egész számok. Igazoljuk, hogy:
a) $(x_1, \ldots, x_{n-1}, x_n) = ((x_1, \ldots, x_{n-1}), x_n)$; $[x_1, \ldots, x_{n-1}, x_n] = [[x_1, \ldots, x_{n-1}], x_n]$.
b) $(x_1, \ldots, x_n) = \min\{x \in \mathbb{N}^* \mid \exists u_i \in \mathbb{Z}$ úgy, hogy $x = \sum_{i=1}^n u_i x_i\}$. Partikulárisan, $(x_1, \ldots, x_n) = d \Rightarrow \exists u_i \in \mathbb{Z}$ úgy, hogy $\sum_{i=1}^n u_i x_i = d$.
c) $(x_1, \ldots, x_n) = 1 \Leftrightarrow \exists u_i \in \mathbb{Z}$ úgy, hogy $\sum_{i=1}^n u_i x_i = 1$.
d) $(x_1 x, \ldots, x_n x) = (x_1, \ldots, x_n)x$ minden $x \in \mathbb{N}$ esetén.
e) Ha $(x, x_i) = 1$, $i = 1, \ldots, n$, akkor $(x, x_1 \ldots x_n) = 1$.
f) Ha $(x_i, x_j) = 1$ minden $i, j = 1, \ldots, n$, $i \neq j$ esetén, akkor $[x_1, \ldots, x_n] = x_1 \ldots x_n$. (Ebben az esetben azt mondjuk, hogy az x_i, $i = 1, \ldots, n$ számok *páronként relatív prímek.*)

1.1.4. tétel (Az aritmetika alaptétele). *Minden $a \neq 0, 1$ egész szám felirható egyértelműen a következő alakban:*

$$a = \pm p_1^{k_1} \ldots p_r^{k_r},$$

ahol p_i páronként különböző prímszámok és $k_i \in \mathbb{N}^*$, $1 \leq i \leq r$.

1.1.5. következmény. *Ha $a = \pm p_1^{k_1} \ldots p_r^{k_r}$ és $b = \pm p_1^{l_1} \ldots p_r^{l_r}$, ahol $k_i, l_i \geq 0$, $1 \leq i \leq r$, akkor*

$$(a, b) = p_1^{\min\{k_1, l_1\}} \ldots p_r^{\min\{k_r, l_r\}} \quad \text{és} \quad [a, b] = p_1^{\max\{k_1, l_1\}} \ldots p_r^{\max\{k_r, l_r\}}.$$

1.1.3. Relációk és függvények

1.1.6. definíció. Legyen A és B két halmaz.

a) Ha $R \subseteq A \times B = \{(a, b) \mid a \in A,\ b \in B\}$ akkor a $\rho = (A, B, R)$ rendszert **reláció**nak nevezzük; A a reláció **értelmezési tartománya**, B az **értékkészlete** és R a **grafikon**ja.

Jelölés: $x\rho y \Leftrightarrow (x, y) \in R$.

b) Ha $x \in A$, legyen $\rho\langle x\rangle := \{y \in B \mid x\rho y\} \subseteq B$. Azt mondjuk, hogy $\rho\langle x\rangle$ a ρ relációnak az x szerinti **metszete.**

c) Az $f = (A, B, F)$ relációt **függvény**nek nevezzük (*leképezésnek, függvényrelációnak*), ha minden $x \in A$ esetén, $f\langle x\rangle$ pontosan egy elemet tartalmaz.

Jelölések: $f\langle x\rangle = \{f(x)\}$; $f : A \to B$, $x \mapsto f(x)$; $A \xrightarrow{f} B$; $\mathrm{Hom}(A, B) = B^A = \{f \mid f : A \to B\}$.

d) az $\mathbf{1}_A : A \to A$, $\mathbf{1}_A(x) = x$ függvényt az A halmaz **identikus függvény**ének nevezzük.

e) Ha $f : A \to B$ és $g : B \to C$ függvények, akkor $g \circ f : A \to C$, $(g \circ f)(x) = g(f(x))$ az f és g **összetétele**.

f) $f : A \to B$ **invertálható** függvény, ha létezik $g : B \to A$ úgy, hogy $g \circ f = \mathbf{1}_A$ és $f \circ g = \mathbf{1}_B$.

Jelölés: $g = f^{-1} : B \to A$.

1.5. feladat. Adottak $f : A \to B$, $g : B \to C$ és $h : C \to D$ függvények. Igazoljuk, hogy:

a) $\mathbf{1}_B \circ f = f \circ \mathbf{1}_A = f$;

b) $(h \circ g) \circ f = h \circ (g \circ f)$;

c) Ha f és g invertálhatók, akkor $g \circ f$ is invertálható, és $(g \circ f)^{-1} = f^{-1} \circ g^{-1}$.

1.1.7. definíció. Legyen $f : A \to B$ egy függvény.

a) f **injektív**, ha minden $x_1, x_2 \in A$ esetén, $x_1 \neq x_2 \Rightarrow f(x_1) \neq f(x_2)$ (azaz, $f(x_1) = f(x_2) \Rightarrow x_1 = x_2$).

b) f **szürjektív**, ha minden $y \in B$ esetén létezik $x \in A$ úgy, hogy $f(x) = y$.

c) f **bijektív**, ha f injektív és szürjektív (azaz, minden $y \in B$ esetén létezik az egyértelműen meghatározott $x \in A$ elem úgy, hogy $f(x) = y$).

1.6. feladat. Legyen $f : A \to B$ és $g : B \to C$ két függvény. Igazoljuk, hogy:

a) Ha f és g injektív (szürjektív), akkor $g \circ f$ is injektív (szürjektív).

b) Ha $g \circ f$ injektív (szürjektív), akkor f injektív (g szürjektív).

c) Ha $g \circ f$ injektív és f szürjektív, akkor g injektív.

d) Ha $g \circ f$ szürjektív és g injektív, akkor f szürjektív.

e) Az $\mathbf{1}_A$ identikus függvény bijektív.

f) f bijektív $\Leftrightarrow$ f invertálható.

1.7. feladat. Legyen $f : A \to B$ egy függvény, $X \subseteq A, Y \subseteq B$, és legyen

$$f(X) = \{f(x) \mid x \in X\}, \qquad f^{-1}(Y) = \{a \in A \mid f(a) \in Y\}.$$

Igazoljuk, hogy:

a) $f(X_1 \cup X_2) = f(X_1) \cup f(X_2)$ minden $X_1, X_2 \subseteq A$ esetén.

b) f injektív $\Leftrightarrow$ $f(X_1 \cap X_2) = f(X_1) \cap f(X_2)$ minden $X_1, X_2 \subseteq A$ esetén.

c) $f^{-1}(Y_1 \cup Y_2) = f^{-1}(Y_1) \cup f(Y_2)$ minden $Y_1, Y_2 \subseteq B$ esetén.

d) $f^{-1}(Y_1 \cap Y_2) = f^{-1}(Y_1) \cap f(Y_2)$ minden $Y_1, Y_2 \subseteq B$ esetén.

1.8. feladat. Legyen A egy halmaz, $\mathcal{P}(A) = \{X \mid X \subseteq A\}$ az A **hatványhalmaza** és $\varphi_A : \mathcal{P}(A) \to \mathrm{Hom}(A, \{0, 1\})$, $\varphi_A(X) = \chi_X$, ahol

$$\chi_X : A \to \{0, 1\}, \quad \chi_X(a) = \begin{cases} 1, & \text{ha } a \in X \\ 0, & \text{ha } a \notin X \end{cases}$$

az X **karakterisztikus függvénye**. Igazoljuk, hogy φ_A bijektív és $\varphi_A^{-1}(\chi) = \chi^{-1}(1)$, $\forall\, \chi : A \to \{0, 1\}$.

1.1.4. Rendezési és ekvivalencia relációk

1.1.8. definíció. Legyen $\rho = (A, A, R)$ egy **homogén** reláció. Azt mondjuk, hogy:

a) ρ **reflexív** ha minden $x \in A$ esetén, $x\rho x$;

b) ρ **tranzitív** ha minden $x, y, z \in A$ esetén, $x\rho y,\ y\rho z \Rightarrow x\rho z$;

c) ρ **szimmetrikus** ha minden $x, y \in A$ esetén, $x\rho y \Rightarrow y\rho x$;

d) ρ **antiszimmetrikus** ha minden $x, y \in A$ esetén, $x\rho y,\ y\rho x \Rightarrow x = y$;

Rendezett halmazok

1.1.9. definíció. a) ρ **előrendezés** ha reflexív és tranzitív. Ebben az esetben azt mondjuk, hogy (A, ρ) előrendezett halmaz.

b) ρ **rendezési reláció** ha reflexív, tranzitív és antiszimmetrikus. Ebben az esetben azt mondjuk, hogy (A, ρ) **rendezett halmaz**.

c) (A, ρ) **teljesen rendezett halmaz**, ha minden $x, y \in A$ esetén, $x\rho y$, vagy $y\rho x$.

d) $a \in A$ **minimális** eleme az $(A, \leq)$ rendezett halmaznak, ha $x \in A,\ x \leq a \Rightarrow x = a$; duálisan, a **maximális** eleme A-nak, ha $x \in A,\ x \geq a \Rightarrow x = a$.

e) Az $f : (A, \leq) \to (B, \leq)$ függvényt **növekvő**nek nevezzük, ha minden $x, x' \in A$ esetén, $x \leq x' \Rightarrow f(x) \leq f(x')$; f **csökkenő**, ha minden $x, x' \in A$ esetén, $x \leq x' \Rightarrow f(x) \geq f(x')$.

1.1.10. példa. a) $(\mathbb{N}, \leq)$, $(\mathbb{Z}, \leq)$, $(\mathbb{Q}, \leq)$, $(\mathbb{R}, \leq)$ teljesen rendezett halmazok, ahol „$\leq$” a természetes rendezés.

b) $(\mathcal{P}(A), \subseteq)$ rendezett halmaz, általában nem teljesen rendezett, ahol „$\subseteq$” a bennfoglalási reláció.

1.9. feladat. a) $(\mathbb{Z}, |)$ előrendezett halmaz, „$|$” nem szimmetrikus és nem antiszimmetrikus.

b) $(\mathbb{N}, |)$ rendezett halmaz.

1.10. feladat. a) Ha M egy halmaz, határozzuk meg a $(\mathcal{P}(M), \subseteq)$ és $(\mathcal{P}(M) \setminus \{\emptyset, M\}, \subseteq)$ rendezett halmazok minimális és maximális elemeit.

b) Határozzuk meg az $(\mathbb{N}, \leq)$, $(N, |)$, $(\mathbb{N}^*, |)$ és $(\mathbb{N} \setminus \{0, 1\}, |)$ rendezett halmazok minimális és maximális elemeit.

c) Ha $a = \min A$ az $(A, \leq)$ rendezett halmaz legkisebb eleme, akkor a az egyetlen minimális eleme. Igazoljuk, hogy a fordított állítás nem igaz.

Jelentsük ki és bizonyítsuk be a duális állítást is.

1.11. feladat. Legyenek $(A, \leq)$, $(B, \leq)$ és $(C, \leq)$ rendezett halmazok és $f : A \to B$, $g : B \to C$ két függvény.

a) Ha f és g növekvő (csökkenő), akkor $g \circ f$ növekvő.

b) Ha f növekvő (csökkenő) és g csökkenő (növekvő), akkor $g \circ f$ csökkenő.

Bizonyításokban többször is fogjuk alkalmazni az un. Zorn-lemmát, amit halmazelméleti axiómaként is elfogathatunk.

1.1.11. tétel (Zorn-lemma). *Legyen $(A, \leq)$ egy nem üres rendezett halmaz. Ha minden $L \subseteq A$ teljesen rendezett részhalmaznak van felső korlátja, akkor minden $a \in A$ esetén létezik olyan $m \in A$ maximális elem, hogy $a \leq m$.*

Ekvivalenciareláció és faktorhalmaz

1.1.12. definíció. Azt mondjuk, hogy $\rho = (A, A, R))$ **ekvivalenciareláció** az A halmazon, ha reflexív, tranzitív és szimmetrikus.

1.12. feladat. Legyen $f : A \to B$ egy függvény. Az A halmazon definiáljuk a $\ker f$ relációt:

$$a_1(\ker f)a_1 \iff f(a_1) = f(a_2).$$

Igazoljuk, hogy $\ker f$ ekvivalenciareláció A-n.

1.1.13. lemma. *Ha ρ egy ekvivalenciareláció A-n, akkor*

a) $x \in \rho\langle x\rangle$ *minden* $x \in A$ *esetén.*

b) *Minden* $x, y \in A$ *esetén a következő állítások ekvivalensek:*

(i) $x\rho y$; (ii) $y \in \rho\langle x\rangle$; (iii) $\rho\langle x\rangle \cap \rho\langle y\rangle \neq \emptyset$; (iv) $\rho\langle x\rangle = \rho\langle y\rangle$.

Bizonyítás. a) Mivel ρ reflexív, $x\rho x$ minden $x \in A$ esetén, azaz $x \in \rho\langle x\rangle$.

b) A $\rho\langle x\rangle$ definíciójából következik, hogy (i) $\Leftrightarrow$ (ii). Ha $x\rho y$, akkor a)-szerint $y \in \rho\langle x\rangle \cap \rho\langle y\rangle$, tehát (i) $\Leftrightarrow$ (iii). Fordítva, ha $z \in \rho\langle x\rangle \cap \rho\langle y\rangle$, akkor $x\rho z$, $y\rho z$; továbbá $y\rho z$, $z\rho x$ mivel ρ szimmetrikus; a ρ tranzitivitásából kapjuk, hogy $y\rho x$, vagyis $x\rho y$.

Ha (iv) igaz, akkor $y \in \rho\langle y\rangle = \rho\langle x\rangle$, tehát $x\rho y$. Fordítva, feltételezzük, hogy $x\rho y$, és legyen $z \in \rho\langle x\rangle$. Akkor $z\rho x$, $x\rho y$, tehát $z\rho y$, azaz $z \in \rho\langle y\rangle$. Ezzel igazoltuk, hogy $\rho\langle x\rangle \subseteq \rho\langle y\rangle$, és a szimmetria miatt $\rho\langle y\rangle \subseteq \rho\langle x\rangle$. ■

1.1.14. definíció. Ha ρ egy ekvivalenciareláció A-n, akkor az $\{\rho\langle x\rangle \mid x \in A\}$ halmazt A/ρ-val jelöljük, és A-nak az ρ-szerinti **faktorhalmaz**ának nevezzük.

Az mondjuk, hogy $\rho\langle x\rangle$ az $x \in A$ elem **ekvivalenciaosztálya**. A fentiekből következik, hogy A-nak minden eleme pontosan egy $\rho\langle x\rangle$ alakú osztályhoz tartozik, és azt mondjuk, hogy az A/ρ faktorhalmaz A-nak egy **osztályfelbontása**.

A $p_\rho : A \to A/\rho$, $p_\rho(x) = \rho\langle x\rangle$ szürjektív függvényt **kanonikus projekciónak** nevezzük.

1.13. feladat (Kongruencia reláció; modulo n maradékosztályok halmaza). Legyen $n \in \mathbb{N}$, és tekintsük a $\mathbb{Z}$ halmazon értelmezett relációt:

$$a \equiv b \pmod{n} \overset{\text{def}}{\Leftrightarrow} n | b - a.$$

Igazoljuk, hogy: a) $\equiv \pmod{n}$ ekvivalencia reláció;

b) $\hat{a} = \{a + nk \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$, ahol $\hat{a}$-val jelöltük az $a \in \mathbb{Z}$ elem ekvivalencia osztályát. Jelölés: $\mathbb{Z}_n = \{\hat{a} \mid a \in \mathbb{Z}\}$.

c) Ha $n = 0$, akkor $\mathbb{Z}_0 = \{\{a\} \mid a \in \mathbb{Z}\}$ (ezt $\mathbb{Z}$-vel azonosítjuk).

d) Ha $n = 1$, akkor $\mathbb{Z}_1 = \{\mathbb{Z}\}$.

e) Ha $n \geq 2$, akkor

$$a \equiv b \pmod{n} \Leftrightarrow a \mod n = b \mod n.$$

Ebben az esetben, igazoljuk, hogy $\mathbb{Z}_n$-nek pontosan n eleme van:

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}.$$

1.1.5. Kardinális számok

1.1.15. definíció. Azt mondjuk, hogy A és B **ekvipotens** halmazok (jelölés: $A \sim B$), ha létezik egy $f : A \to B$ bijektív függvény.

1.14. feladat. „$\sim$” ekvivalencia reláció.

1.1.16. definíció. a) Az A halmaz ekvipotencia osztályát az A **számosság**ának vagy **kardinális szám**ának nevezzük. Jelölés:

$$|A| = \{B \mid A \sim B\}.$$

(Jegyezzük meg, hogy $|A|$ *osztály*, nem halmaz). Azt mondjuk, hogy az A halmaz *reprezentánsa* az $\alpha = |A|$ kardinális számnak.

Legyen $\alpha = |A|$ és $\beta = |B|$ két kardinális szám.

b) (Kardinális számok rendezése) Értelmezés szerint, $\alpha \leq \beta$ ha létezik egy $f : A \to B$ injektív függvény.

(Be lehet bizonyítani, hogy „$\leq$” teljes rendezési reláció. E bizonyítás kissé bonyolult.)

c) (Műveletek kardinális számokkal)

1. $\alpha + \beta = |A \cup B|$, ha $A \cap B = \emptyset$;
2. $\alpha\beta = |A \times B|$;
3. $\beta^\alpha = |B^A| = |\mathrm{Hom}(A, B)|$.

Igazolható, hogy a fenti definiciók nem függnek a reprezentánsoktól.

d) Legyen A egy halmaz. A következő állítások ekvivalensek:

1. Létezik egy $f : \mathbb{N} \to A$ injektív függvény;
2. A-nak van egy valódi részhalmaza amely ekvipotens A-val.

Ebben az esetben, azt mondjuk, hogy A **végtelen** halmaz; A-t **véges** halmaznak nevezzük, ha A nem végtelen.

e) A **megszámlálható** halmaz ha $A \sim \mathbb{N}$; az $\mathbb{N}$ számosságát $\aleph_0$-val jelöljük.

A fenti értelmezésekből következik, hogy $\aleph_0$ a legkisebb végtelen (*transzfinit*) kardinális szám.

1.15. feladat (Szitaformula, tartalmazás és kizárás elve). Legyenek $A_1, \ldots, A_n$ véges halmazok. Bizonyítsuk be, hogy

$$|\bigcup_{i=1}^{n} A_i| = \sum_{i=1}^{n} |A_i| - \sum_{1 \leq i_1 < i_2 \leq n} |A_{i_1} \cap A_{i_2}| + \sum_{1 \leq i_1 < i_2 < i_3 \leq n} |A_{i_1} \cap A_{i_2} \cap A_{i_3}|$$
$$- \cdots + (-1)^{k+1} \sum_{1 \leq i_1 < \cdots < i_k \leq n} |A_{i_1} \cap \cdots \cap A_{i_k}| + \cdots + (-1)^{n+1} |\bigcap_{i=1}^{n} A_i|.$$

Alkalmazások. a) (**Euler-függvény**) Legyen $m \in \mathbb{N}$. Számitsuk ki $\phi(m)$-et ha $m = p_1^{k_1} \ldots p_n^{k_n}$, ahol

$$\phi(m) = |\{a \in \mathbb{N} \mid 1 \leq a \leq m,\ (a, m) = 1\}|.$$

b) Legyen $\sigma \in S_n$ egy n-ed fokú permutáció. Értelmezés szerint, $i \in \{1, \ldots, n\}$ *fix-pontja* σ-nak, ha $\sigma(i) = i$. Hány n-ed fokú permutációnak nincs fix-pontja?

1.16. feladat. Legyen A és B két véges halmaz, $|A| = k$ és $|B| = n$. Bizonyítsuk be, hogy:
a) Az $f : A \to B$ függvének száma $\overline{V}_n^k = n^k$ (n elem k tagú **ismétléses variációi**).
b) Ha $k \le n$, akkor az $f : A \to B$ injektív függvények száma $V_n^k = \frac{n!}{(n-k)!}$ (n elem k tagú **variációi**).
c) Ha $k = n$, akkor az $f : A \to B$ bijektív függvények száma $P_n = n!$ (n elem **permutációi**).
d) Ha $k \ge n$, akkor az $f : A \to B$ szürjektív függvények száma az **elsőfajú Stirling szám**:

$$s(n,k) = n^k - C_n^1(n-1)^k + C_n^2(n-2)^k + \cdots + (-1)^{n-1}C_n^{n-1}.$$

1.17. feladat. Legyen A egy véges halmaz.
a) Ha $f : A \to A$ injektív, akkor f szürjektív.
b) Ha $f : A \to A$ szürjektív, akkor f injektív.

1.18. feladat. Bizonyítsuk be, hogy:
a) $\aleph_0 + \aleph_0 = \aleph_0$; $\aleph_0 \cdot \aleph_0 = \aleph_0$.
b) Ha $A_n \sim \mathbb{N}$ minden $n \in \mathbb{N}$ esetén, akkor $\bigcup_{n\in\mathbb{N}} A_n \sim \mathbb{N}$.
c) $\mathcal{P}_f(\mathbb{N}) = \{X \subset \mathbb{N} \mid X \text{ véges}\}$ megszámlálható halmaz.
d) A racionális számok halmaza megszámlálható.

1.2. Csoportok

1.2.1. A csoport fogalma. Példák

1.2.1. definíció. Legyen G egy halmaz és $\phi : G \times G \to G$ egy függvény.
a) Az (G, ϕ) elempárt **gruppoidnak** nevezzük. Ha $x, y \in G$, akkor $\phi(x, y)$ helyett gyakran az

$$x + y,\ x \cdot y,\ x \circ y,\ x \cap y,\ x \cup y,\ x * y$$

stb. jelöléseket használjuk.
A „+” (illetve „·”) jelölést *additív* (illetve *multiplikatív*) jelölésnek nevezzük.
b) $(G, *)$ **félcsoport**, ha „$*$” **asszociatív** művelet, azaz minden $x, y, z \in G$ esetén

$$(x * y) * z = x * (y * z).$$

c) $(G, *)$ **monoíd**, ha „$*$” asszociatív művelet, és G-ben létezik **semleges elem**:

$$(\exists)e \in G\ (\forall)x \in G\ x * e = e * x = x.$$

Additív (illetve multiplikatív) jelölés esetén e-t 0-val (illetve 1-gyel) szoktuk jelölni.
d) $(G, *)$ **csoport**, ha $(G, *)$ monoid és minden eleme **szimmetrizálható (invertálható)**:

$$(\forall)x \in G\ (\exists)x' \in G\ x * x' = x' * x = e.$$

Additív (illetve multiplikatív) jelölés esetén x'-et $-x$-el (illetve x^{-1}-gyel) jelöljük.
e) Azt mondjuk, hogy az $(G, *)$ csoport **kommutatív** vagy **Abel-csoport**, ha minden $x, y \in G$ esetén, $x * y = y * x$.
f) Az $|G|$ kardinális számot az $(G, *)$ csoport **rend**jének nevezzük.

1.2.2. lemma. *Legyen* $(M, \cdot)$ *egy monoid.*
a) *Ha* $e, e' \in M$ *semleges elemek, akkor* $e = e'$.
b) *Ha* $x \in M$ *és* $x', x'' \in M$ x*-nek inverzei, akkor* $x' = x''$.
c) *Legyen* $U(M) = \{x \in M \mid x \text{ invertálható}\}$ *az* M *egységeinek a halmaza. Akkor* $(U(M), \cdot)$ *csoport.*

Bizonyítás. a) $e = ee' = e'$.
b) $x' = x'e = x'(xx'') = (x'x)x'' = ex'' = x''$.
c) Az M semleges eleme invertálható, mert $ee = e$. Ha $x \in U(M)$, akkor $x' \in U(M)$ és $(x')' = x$, mert $x'x = xx' = e$. Ha $x, y \in U(M)$, akkor

$$(xy)(y'x') = (y'x')(xy) = e,$$

tehát $xy \in U(M)$ és $(xy)' = y'x'$. Az asszociatívitás öröklődik. ■

1.2.3. példa. a) $(\mathbb{N}^*, +)$ félcsoport, $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$ monoidok, nem csoportok.
b) $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$ Abel-csoportok.
c) $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$ kommutatív monoidok, $(U(\mathbb{Z}) = \{1, -1\}, \cdot)$, $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$ Abel-csoportok.

1.2.4. példa. Legyen M egy halmaz és $\mathcal{F}(M) = \{f \mid f : M \to M\}$. Akkor $(\mathcal{F}(M), \circ)$ monoid. Az

$$S_M := U(\mathcal{F}(M)) = \{f \in \mathcal{F}(M) \mid f \text{ bijektív}\}$$

csoportot az M halmaz **szimmetrikus-csoport**jának nevezzük.

1.19. feladat. Legyen $M = \mathbb{R} \setminus \{0, 1\}$, $G = \{f_i \mid i = 1, \dots, 6\}$, ahol $f_i : M \to M$,

$$f_1(t) = t, \quad f_2(t) = \frac{1}{1-t}, \quad f_3(t) = \frac{t-1}{t}, \quad f_4(t) = \frac{1}{t},$$

$$f_5(t) = 1 - t, \quad f_6(t) = \frac{t}{t-1}, \quad (\forall) t \in M.$$

Igazoljuk, hogy $(G, \circ)$ nemkommutatív csoport (készítsünk művelettáblát).

1.20. feladat (Csoportok direkt szorzata). Legyen G_1 és G_2 két csoport, és legyen

$$G := G_1 \times G_2 = \{g = (g_1, g_2) \mid g_1 \in G_1,\ g_2 \in G_2\}.$$

Értelmezés szerint, legyen

$$(g_1, g_2)(g_1', g_2') = (g_1 g_1', g_2 g_2').$$

Akkor G csoport.

1.2.5. megjegyzés (Számítási szabályok). a) Legyen $(G, \cdot)$ egy csoport és $a, b \in G$. Az $ax = b$ egyenlet egyetlen megoldása $x = a^{-1}b$, és az $ya = b$ egyenlet egyetlen megoldása $y = ba^{-1}$; következik, hogy a

$$t_a : G \to G, \quad t_a(x) = ax$$

és

$$t_a' : G \to G, \quad t_a'(x) = xa$$

bijektív függvények (ezeket *bal oldali* illetve *jobb oldali transzlációnak* nevezzük). Ha $x, y \in G$, akkor $ax = ay \Rightarrow x = y$ és $xa = ya \Rightarrow x = y$.

b) (*Hatványozás*) Legyen $(G, \cdot)$ egy csoport, $x \in G$ és $n \in \mathbb{N}^*$. A „$\cdot$" asszociatívitását felhasználva, értelmezzük az x^n-et:

$$x^1 = x, \quad x^{n+1} = x^n \cdot x = x \cdot x^n.$$

Továbbá, legyen $x^0 = e$ és $(x^{-1})^n = (x^n)^{-1}$.

1.21. feladat. Igazoljuk, hogy $x^{n+m} = x^n x^m$ és $(x^n)^m = x^{mn}$ minden $x \in G$ és $m, n \in \mathbb{Z}$ esetén.

Ha a $(G, +)$ additív jelölést alkalmazzuk, akkor legyen $1 \cdot x = x$, $(n+1)x = nx + x = x + nx$, $0 \cdot x - 0$, $(-n)x = -(nx) = n(-x)$. Ebben az esetben, $(m+n)x = mx + nx$ és $m(nx) = (mn)x$ minden $m, n \in \mathbb{Z}$ esetén.

1.22. feladat. Legyen $(G, \cdot)$ egy félcsoport. Igazoljuk, hogy G csoport akkor és csak akkor, ha:
a) $(\exists) e \in G$ úgy, hogy $(\forall) x \in G$ $xe = x$.
b) $(\forall) x \in G$ $(\exists) x' \in G$ úgy, hogy $xx' = e$.

1.23. feladat. Legyen $(G, \cdot)$ egy nemüres félcsoport, és $t_a, t_a' : G \to G$, $t_a(x) = ax$, $t_a'(x) = xa$, ahol $a \in G$. Bizonyítsuk be, hogy:
a) G csoport $\Leftrightarrow$ t_a, t_a' szürjektívek, $(\forall) a \in G$.
b) Ha G véges, akkor G akkor és csak akkor csoport, ha $(\forall) a, x, y \in G$ $ax = ay \Rightarrow x = y$ és $xa = ya \Rightarrow x = y$.

1.24. feladat. Legyen $(G, \cdot)$ egy csoport és $x, y \in G$. Igazoljuk, hogy:
a) $x^2 = y^6 = e,\ xy = y^4 x \Rightarrow y^3 = e,\ xy = yx$.
b) $x^5 = y^4 = e,\ xy = yx^3 \Rightarrow x^2 y = yx,\ xy^3 = y^3 x^2$.
c) $x^3 = y^4 = e,\ yx = xy^3 \Rightarrow xy = yx$.

1.25. feladat. Legyen $(G, \cdot)$ egy csoport és $x, y \in G$. Igazoljuk, hogy :
a) Ha $xy = yx$, akkor $x^m y^n = y^n x^m$ és $(xy)^n = x^n y^n$ $(\forall) m, n \in \mathbb{Z}$.
b) Ha $n \in \mathbb{Z}$ és $(xy)^k = x^k y^k$, ahol $k = n-1, n, n+1$, akkor $xy = yx$.

1.2.2. Csoportmorfizmusok

1.2.6. definíció. Legyen $(G, *)$ és $(G', \circ)$ két csoport és $f : G \to G'$ egy függvény,
a) Azt mondjuk, hogy f **csoportmorfizmus**, ha minden $x, y \in G$ esetén

$$f(x * y) = f(x) \circ f(y).$$

Az f-et **endomorfizmusnak** nevezzük, ha $(G, *) = (G', \circ)$.
b) Azt mondjuk, hogy f **izomorfizmus**, ha létezik egy $f' : G' \to G$ morfizmus úgy, hogy $f' \circ f = \mathbf{1}_G$ és $f \circ f' = \mathbf{1}_{G'}$. Az f izomorfizmust **automorfizmusnak** nevezzük, ha $(G, *) = (G, \circ)$.
Jelölések: $\mathrm{End}(G)$ – az endomorfizmusok halmaza, $\mathrm{Aut}(G)$ – az automorfizmusok halmaza.

1.2.7. lemma. *Legyen* $f : G \to G'$ *és* $f' : G' \to G''$ *két morfizmus.*
a) $f(e) = e'$*;*
b) $f(x^{-1}) = f(x)^{-1}$ *minden* $x \in G$ *esetén.*
c) $\mathbf{1}_G : G \to G$ *és* $f' \circ f : G \to G''$ *morfizmusok.*
d) f *akkor és csak akkor izomorfizmus, ha bijektív.*

Bizonyítás. a) $e'f(e) = f(e) = f(ee) = f(e)f(e)$, tehát $f(e) = e'$.
b) Ha $x \in G$, akkor $xx^{-1} = x^{-1}x = e$, tehát $f(x)f(x^{-1}) = f(x^{-1})f(x) = e'$, és következik, hogy $f(x)^{-1} = f(x^{-1})$.
c) Minden $x, y \in G$ esetén $\mathbf{1}_G(x, y) = xy = \mathbf{1}_G(x)\mathbf{1}_G(y)$ és

$$(f' \circ f)(xy) = f'(f(xy)) = f'(f(x)f(y)) = f'(f(x))f'(f(y)) = (f' \circ f)(x)(f' \circ f)(y).$$

d) Ha f izomorfizmus, akkor bijektív, mert van inverze. Fordítva, feltételezzük, hogy f bijektív, és igazoljuk, hogy f^{-1} izomorfizmus. Legyen $u, v \in G'$, $x = f^{-1}(u)$ és $y = f^{-1}(v)$. Ekkor

$$f^{-1}(uv) = f^{-1}(f(x)f(y)) = f^{-1}(f(xy)) = xy = f^{-1}(u)f^{-1}(v). \quad \blacksquare$$

1.26. feladat. Ha $a \in \mathbb{R}_+^* \setminus \{1\}$, és $f : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$, $f(x) = a^x$, akkor f izomorfizmus, és $f^{-1}(x) = \log_a(x)$.

1.27. feladat. A $p_i : G_1 \times G_2 \to G_i$, $p_i(x_1, x_2) = x_i$ **kanonikus projekciók** szürjektív morfizmusok, $i = 1, 2$.

1.28. feladat. Ha $(G, \cdot)$ egy csoport, akkor $(\mathrm{End}(G), \circ)$ monoid, és $U(\mathrm{End}(G)) = \mathrm{Aut}(G)$ (tehát $(\mathrm{Aut}(G), \circ)$ csoport).

1.29. feladat (Lorenz-csoport). Legyen $a > 0$, $G = (-a, a)$ és $x * y = \frac{x+y}{1+xy/a^2}$. Igazoljuk, hogy:
a) $(G, *)$ Abel-csoport;
b) létezik egy $f : (\mathbb{R}_+^*, \cdot) \to (G, *)$, $f(x) = \frac{\alpha x+\beta}{\gamma x+\delta}$ alakú izomorfizmus.

1.30. feladat. Legyen M egy halmaz és $(G, \cdot)$ egy csoport. A $G^M = \{f \mid f : M \to G\}$ halmazon értelmezzük a következő műveletet: $(fg)(x) = f(x)g(x)$, $(\forall)x \in M$, $f, g \in G^M$. Igazoljuk, hogy $(G^M, \cdot)$ csoport, és létezik egy $\phi : G \to G^M$ injektív morfizmus.

1.31. feladat. Legyen $(G, \cdot)$ egy csoport és $f, g : G \to G$, $f(x) = x^{-1}$, $g(x) = x^2$. A következő állítások ekvivalensek:
(i) G Abel-csoport.
(ii) $f \in \mathrm{Aut}(G)$.
(iii) $g \in \mathrm{End}(G)$.

1.32. feladat. Legyen $(G, \cdot)$ egy csoport, és $i_g : G \to G$, $i_g(x) = gxg^{-1}$, ahol $g \in G$. Igazoljuk, hogy $i_g \in \mathrm{Aut}(G)$. (i_g-t **belső automorfizmus**nak nevezzük. Jelölés: $\mathrm{Int}(G) = \{i_g \mid g \in G\}$).

1.33. feladat. Legyen M és N két halmaz és $f : M \to N$ egy bijektív függvény. Igazoljuk, hogy $(S_M, \circ) \simeq (S_N, \circ)$.

1.2.3. Részcsoportok

1.2.8. definíció. Legyen $(G, \cdot)$ egy csoport és H egy részhalmaza G-nek. Azt mondjuk, hogy H **részcsoport**ja G-nek (jelölés: $H \leq (G, \cdot)$), ha H zárt a műveletre nézve (azaz minden $x, y \in H$ esetén $xy \in H$-nak) és $(H, \cdot)$ csoportot alkot a „$\cdot$" által indukált művelettel.

1.2.9. tétel (részcsoport jellemzése). *Legyen* $(G, \cdot)$ *egy csoport és* H *részhalmaza* G*-nek. A következő állítások ekvivalensek:*
1) H *részcsoportja* G*-nek.*
2) $H \neq \emptyset$ *és* $xy, x^{-1} \in H$ *minden* $x, y \in H$ *esetén.*
3) $H \neq \emptyset$ *és* $xy^{-1} \in H$ *minden* $x, y \in H$ *esetén.*

Bizonyítás. (1)$\Longrightarrow$(2) Mivel $(H,\cdot)$ csoport következik, hogy van egy e' semleges eleme. Ha e a G semleges eleme, akkor $e'e' = e' = e'e$, vagyis $e = e' \in H$.

Minden $x \in H$ esetén létezik $x' \in H$ úgy, hogy $xx' = x'x = e$, és létezik $x^{-1} \in G$ úgy, hogy $xx^{-1} = x^{-1}x = e$. Az inverz elem egyértelműségéből következik, hogy $x' = x^{-1} \in H$.

(2)$\Longrightarrow$(3) Ha $x, y \in H$, akkor $x, y^{-1} \in H$ és $xy^{-1} \in H$.

(3)$\Longrightarrow$(1) Feltevés szerint $H \neq \emptyset$; ha $x \in H$, akkor $e = xx^{-1} \in H$ és $ex^{-1} = x^{-1} \in H$ Ha $x, y \in H$, akkor $x, y^{-1} \in H$ és $x(y^{-1})^{-1} \in H$, vagyis $xy \in H$.

Ezzel igazoltuk, hogy H zárt a műveletre nézve, H-ban létezik semleges elem, és H minden elemének van inverze. Mivel az indukált művelet asszociativitása öröklődik, a fentiekből következik, hogy $(H,\cdot)$ csoport és a G részcsoportja. ■

1.2.10. példa. 1) $\mathbb{Z}$ részcsoportja $(\mathbb{Q},+)$-nak, $\mathbb{Q}$ részcsoportja $(\mathbb{R},+)$-nak és $\mathbb{R}$ részcsoportja $(\mathbb{C},+)$-nak.

2) $(\mathbb{Q}^*,\cdot)$ részcsoportja $(\mathbb{R}^*,\cdot)$-nak és $(\mathbb{R}^*,\cdot)$ részcsoportja $(\mathbb{C}^*,\cdot)$-nak.

3) $n\mathbb{Z}$ részcsoportja $(\mathbb{Z},+)$-nak, ahol $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ és $n \in \mathbb{Z}$ rögzített.

4) $\{e\}$ és a G részcsoportjai $(G,\cdot)$-nak, ezeket a G csoport *triviális részcsoportjainak* nevezzük. Ha $H \leq G$ és $H \neq \{e\}$, $H \neq G$, akkor H-t *valódi részcsoportnak* nevezzük.

5) $(U_n,\cdot)$ részcsoportja $(\mathbb{C}^*,\cdot)$-nak, ahol $n \in \mathbb{N}^*$-nak és

$$U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \mid 0 \leq k \leq n-1,\ k \in \mathbb{Z}\}$$

az **n-ed rendű egységgyökök** halmaza.

6) Legyen $(G,\cdot)$ egy csoport, és

$$Z(G) = \{g \in G \mid gx = xg \quad \forall x \in G\}$$

a G **centruma**. Akkor $Z(G)$ részcsoportja G-nek.

Vegyük észre, hogy G akkor és csak akkor kommutatív csoport, ha $Z(G) = G$.

1.2.11. lemma. *Legyen $f : G \longrightarrow G'$ egy csoportmorfizmus.*

1) *Ha H részcsoportja G-nek, akkor $f(H)$ részcsoportja G'-nek.*

2) *Ha H' részcsoportja G'-nek, akkor $f^{-1}(H)$ részcsoportja G-nek.*

Bizonyítás. 1) Mivel $H \neq \emptyset$ következik, hogy $f(H) \neq \emptyset$.

Ha $x', y' \in f(H)$, akkor létezik $x, y \in H$ úgy, hogy $x' = f(x)$ és $y' = f(y)$, tehát $x'y' = f(x)f(y)$. Mivel f morfizmus $f(x)f(y) = f(xy)$, ahol $xy \in H$-nak (mert H részcsoport), tehát $x'y' = f(xy) \in f(H)$.

Továbbá, $(x')^{-1} = f(x)^{-1} = f(x^{-1})$ (mert f morfizmus), de $x^{-1} \in H$ (mert H csoport), tehát $f(x^{-1}) \in f(H)$. A részcsoportok jellemzési tételéből következik, hogy $f(H)$ részcsoportja G'-nek.

2) Mivel H' részcsoportja G'-nek és f morfizmus, fennáll az, hogy $f(e) = e'$, (ahol e a G semleges eleme és e' a G' semleges eleme); következik, hogy $e \in f^{-1}(e')$, vagyis $f^{-1}(H') \neq \emptyset$.

Ha $x, y \in f^{-1}(H')$, vagyis $f(x), f(y) \in H'$, akkor $f(x)f^{-1}(y) = f(x)f(y^{-1}) = f(xy^{-1}) \in H'$, vagyis $xy^{-1} \in f^{-1}(H')$. ■

1.2.12. definíció. Legyen $f : G \longrightarrow G'$ egy morfizmus.

1) Az $\operatorname{Im} f = f(G) = \{f(x) \mid x \in G\}$ halmazt az f **kép**ének nevezzük.

2) A $\operatorname{Ker} f = \{x \in G \mid f(x) = e'\} = f^{-1}(e')$ halmazt az f **mag**jának nevezzük.

1.2.13. megjegyzés. 1) A fenti lemmából következik, hogy $\operatorname{Ker} f \leq G$ és $\operatorname{Im} f \leq G'$.

2) Ha H részcsoportja G-nek és $i : H \longrightarrow G$, $i(h) = h$, akkor i injektív morfizmus.

Fordítva, ha $f : G \longrightarrow G'$ injektív morfizmus, akkor $f(G) = \operatorname{Im} f$ részcsoportja G'-nek és $H \simeq f(H)$. Egy injektív morfizmust *beágyazás*nak is nevezünk.

1.2.14. tétel (Injektív morfizmusok jellemzése). *Az $f : G \longrightarrow G'$ morfizmus akkor és csak akkor injektív, ha $\operatorname{Ker} f = \{e\}$.*

Bizonyítás. Feltételezzük, hogy f injektív és legyen $x \in \operatorname{Ker} f$, vagyis $f(x) = e' = f(e)$; következik, hogy $x = e$, tehát $\operatorname{Ker} f = \{e\}$.

Fordítva, feltételezzük, hogy $\operatorname{Ker} f = \{e\}$. Legyen $x_1, x_2 \in G$ úgy, hogy $f(x_1) = f(x_2)$. Ekkor $f(x_1)f^{-1}(x_2) = e'$, és mivel f morfizmus $f(x_1x_2^{-1}) = e'$, vagyis $x_1x_2^{-1} \in \operatorname{Ker} f = \{e\}$; következik, hogy $x_1x_2^{-1} = e$ tehát $x_1 = ex_2 = x_2$. ■

1.2.15. tétel (Cayley). *Minden csoport beágyazható egy szimmetrikus csoportba.*

Bizonyítás. Legyen $(G,\cdot)$ egy csoport, $a \in G$ és $t_a : G \longrightarrow G$, $t_a(x) = ax$ (t_a a bal oldali transzláció). Mivel t_a bijektív függvény, következik, hogy $t_a \in S_G := \{f : G \to G \mid f \text{ bijektív}\}$.

Legyen $\varphi : G \longrightarrow S_G$ úgy, hogy $\varphi(a) = t_a$ és igazoljuk, hogy φ injektív morfizmus. Valóban, $\varphi(ab) = t_{ab}$ és $\varphi(a) \circ \varphi(b) = t_a \circ t_b$, és minden $x \in G$ esetén

$$t_{ab}(x) = (ab)x = a(bx) = t_a(bx) = t_a(t_b(x)) = (t_a \circ t_b)(x). \tag{1.1}$$

Továbbá, legyen $a, b \in G$ úgy, hogy $\varphi(a) = \varphi(b)$, vagyis $t_a = t_b$. Ez azt jelenti, hogy $t_a(x) = t_b(x)$ minden $x \in G$ esetén, tehát $ax = bx$ és $a = b$, vagyis φ injektív. ■

1.34. feladat. Legyen $(G, \cdot)$ egy csoport és $H_1, H_2, H_3 \leq G$. Igazoljuk, hogy:
a) $H_1 \cup H_2$ akkor és csak akkor részcsoport, ha $H_1 \leq H_2$ vagy $H_2 \leq H_1$.
b) $H_1 \cup H_2 = G$ akkor és csak akkor, ha $H_1 = G$ vagy $H_2 = G$.
c) $H_3 \subseteq H_1 \cup H_2$ akkor és csak akkor, ha $H_3 \leq H_1$ vagy $H_3 \leq H_2$.

1.35. feladat. Legyen $(A, +)$ egy Abel-csoport, $mA = \{ma \mid a \in A\}$ és $A_m = \{a \in A \mid ma = 0\}$, ahol $m \in \mathbb{Z}$. Bizonyítsuk be, hogy:
a) $mA,\ A_m \leq (A, +)$.
b) Ha $f : (A, +) \to (B, +)$ egy morfizmus, akkor $f(mA) \subseteq mB$ és $f(A_m) \subseteq B_m$.
c) Legyen $G = (S_3, \circ)$. Igazoljuk, hogy G^3 és G_2 nem részcsoportok.

1.36. feladat. Legyen $(G, \cdot)$ egy csoport és $H \subseteq G$ egy véges nemüres részhalmaz. Igazoljuk, hogy $H \leq G$ akkor és csak akkor, ha H zárt részhalmaza G-nek.

1.37. feladat. Legyen $(G, \cdot)$ egy csoport és $Z(G) = \{x \in G \mid xg = gx\ (\forall) g \in G\}$ a G *centruma.*
a) Bizonyítsuk be, hogy $Z(G) \leq G$.
b) Ha $f : G \to G'$ egy izomorfizmus, akkor $f(Z(G)) = Z(G')$.

1.2.4. Az S_n szimmetrikus csoport

Legyen $S_n = S_{\{1,\dots,n\}} = \{f : \{1, \dots, n\} \to \{1, \dots, n\} \mid f \text{ bijektív}\}$. Az $(S_n, \circ)$ csoportot **n-ed fokú szimmetrikus csoport**nak nevezzük. Egy $\sigma \in S_n$ elemet n-ed fokú **permutáció**nak nevezzük, és gyakran egy táblázat segítségével adjuk meg:

$$\sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}, \quad e = \begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}.$$

(e-t az *identikus permutáció*nak nevezzük.) Ha $\sigma, \tau \in S_n$, akkor

$$\tau \circ \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ \tau(\sigma(1)) & \tau(\sigma(2)) & \dots & \tau(\sigma(n)) \end{pmatrix},$$

és

$$\sigma^{-1} = \begin{pmatrix} \sigma(1) & \sigma(2) & \dots & \sigma(n) \\ 1 & 2 & \dots & n \end{pmatrix}.$$

Matematikai indukcióval könnyen igazolható, hogy $|S_n| = n!$.

1.2.16. definíció. Legyen $\sigma \in S_n$.
a) Az (i, j) elempárt **inverzió**nak nevezzük, ha $1 \leq i < j \leq n$ és $\sigma(i) > \sigma(j)$; $\mathrm{inv}(\sigma)$-val jelöljük a σ inverzióinak a számát.
b) $\mathrm{sgn}(\sigma) = (-1)^{\mathrm{inv}(\sigma)} \in \{1, -1\}$ a σ **szignatúrája**; σ **páros** permutáció, ha $\mathrm{sgn}(\sigma) = 1$, és σ **páratlan** permutáció, ha $\mathrm{sgn}(\sigma) = -1$.
A páros permutációk halmazát A_n-nel jelöljük.

1.38. feladat. a) Minden $\sigma \in S_n$ esetén, $0 \leq \mathrm{inv}(\sigma) \leq \frac{n(n-1)}{2}$.
b) $\mathrm{inv}(\sigma) = 0 \Leftrightarrow \sigma = e$; $\mathrm{inv}(\sigma) = \frac{n(n-1)}{2} \Leftrightarrow \sigma = \begin{pmatrix} 1 & 2 & \dots & n \\ n & n-1 & \dots & 1 \end{pmatrix}$.;
c) Ha $n \geq 2$ és $1 \leq j < k \leq n$, legyen $\tau_{jk} \in S_n$,

$$\tau_{jk}(i) = \begin{cases} k, & i = j \\ j, & i = k \\ i, & i \neq j, k \end{cases}.$$

Akkor $\mathrm{inv}(\tau_{jk}) = 2(k - j) - 1$ és $\mathrm{sgn}(\tau_{jk}) = -1$. ($\tau_{jk}$-t **transzpozíció**nak nevezzük).

1.39. feladat. Legyen $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 1 & 3 \end{pmatrix}$ és $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}$. Határozzuk meg az $\mathrm{inv}(\sigma)$-t, $\mathrm{sgn}(\sigma)$-t, σ^{-1}-t, $\sigma\tau$-t, $\tau\sigma$-t és σ^{1457}-t!

1.40. feladat. Írjuk fel az összes 3-ad és 4-ed fokú transzpozíciókat.

1.41. feladat. Számítsuk ki $\mathrm{inv}(\sigma)$-t ha:

a) $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & \dots & n & n+1 & n+2 & \dots & 2n \\ 1 & 3 & 5 & 7 & \dots & 2n-1 & 2 & 4 & \dots & 2n \end{pmatrix}$

b) $\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n & n+1 & n+2 & n+3 & \dots & 2n \\ 2 & 4 & 6 & \dots & 2n & 1 & 3 & 5 & \dots & 2n-1 \end{pmatrix}$

1.2.17. tétel. a) *Minden* $\sigma \in S_n$ *esetén,*

$$\mathrm{sgn}(\sigma) = \prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}.$$

b) $\mathrm{sgn} : (S_n, \circ) \to (\{1, -1\}, \cdot)$ *szürjektív morfizmus.*

c) $(A_n, \circ)$ *csoport és* $|A_n| = \frac{n!}{2}$. (A_n*-et* **alternáló csoport***nak nevezzük*).

Bizonyítás. a) Mivel σ bijektív függvény, minden $i, j \in \{1, \dots, n\}$ esetén léteznek az egyértelműen meghatározott $k, l \in \{1, \dots, n\}$ elemek, $k \neq l$, úgy, hogy $\sigma(k) = i$ és $\sigma(l) = j$; továbbá, $k > l$ pontosan akkor ha (i, j) σ-nak egy inverziója. Következik, hogy a $\prod_{1 \le i < j \le n} \frac{\sigma(j) - \sigma(i)}{j - i}$ szorzatban, az egyszerűsítések után, a (-1)-gyel egyenlő tényezők száma $\mathrm{inv}(\sigma)$.

b) Mivel $\mathrm{sgn}(e) = 1$, és ha τ_{ij} egy transzpozíció, akkor $\mathrm{sgn}(\tau) = -1$, következik, hogy sgn szürjektív.

Legyen $\sigma, \tau \in S_n$. Mivel τ bijektív, minden $i, j \in \{1, \dots, n\}$ esetén léteznek az egyértelműen meghatározott $k, l \in \{1, \dots, n\}$ elemek, $k \neq l$, úgy, hogy $\tau(k) = i$ és $\tau(l) = j$. Ekkor

$$\begin{aligned} \mathrm{sgn}(\sigma\tau) &= \prod_{1 \le i < j \le n} \frac{(\sigma\tau)(j) - (\sigma\tau)(i)}{j - i} = \prod_{1 \le i < j \le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{j - i} \\ &= \prod_{1 \le i < j \le n} \frac{\sigma(\tau(j)) - \sigma(\tau(i))}{\tau(j) - \tau(i)} \cdot \prod_{1 \le i < j \le n} \frac{\tau(j) - \tau(i)}{j - i} \\ &= \mathrm{sgn}(\sigma)\mathrm{sgn}(\tau). \end{aligned}$$

c) Vegyük észre, hogy $A_n = \mathrm{Ker}(\mathrm{sgn})$, tehát A_n részcsoport.

Legyen $\tau \in S_n$ egy transzpozíció. Mivel S_n csoport és sgn csoportmorfizmus, $\phi : A_n \to S_n \setminus A_n$, $\phi(\sigma) = \sigma\tau$ jólértelmezett bijektív függvény; következik, hogy $|A_n| = |S_n \setminus A_n| = \frac{n!}{2}$. ■

1.3. Gyűrűk és testek

1.3.1. A gyűrű fogalma. Példák

1.3.1. definíció. a) Az $(R, +, \cdot)$ algebrai struktúrát **gyűrű**nek nevezzük, ha:

1. $(R, +)$ Abel-csoport (az R *additív csoportja*);
2. A szorzás **disztributív** az összeadásra nézve, azaz minden $a, b, c \in R$ esetén,

$$a(b + c) = ab + ac, \qquad (b + c)a = ba + ca.$$

b) R **egységelemes gyűrű**, ha létezik $1 \in R$ úgy, hogy $1 \cdot a = a \cdot 1 = a$ $(\forall) a \in R$ esetén.

c) R **asszociatív** (**kommutatív**) gyűrű, ha $(R, \cdot)$ asszociatív (kommutatív) gruppoid.

d) R **test**, ha R asszociatív egységelemes gyűrű, $1 \neq 0$, és R minden nemnulla eleme invertálható.

e) R **Lie-gyűrű**, ha minden $a, b, c \in R$ esetén

1. $a^2 = 0$;
2. $(ab)c + (bc)a + (ca)b = 0$ (*Jacobi-azonosság*).

Az alábbiakban a „gyűrű” mindig „asszociatív gyűrűt” fog jelenteni.

1.42. feladat (Számítási szabályok). a) Ha $(R, +, \cdot)$ gyűrű és $a \in R$, akkor igazoljuk, hogy

$$t_a, t'_a : (R, +) \to (R, +), \quad t_a(r) = ar, \quad t'_a(r) = ra$$

csoportmorfizmusok. Következtessük, hogy minden $a, b, c \in R$ esetén
(1) $a \cdot 0 = 0 \cdot a = 0$;
(2) $a(-b) = (-a)b = -ab$; $(-a)(-b) = ab$;
(3) $(-a)^n = a$ ha n páros, és $(-a)^n = -a$ ha n páratlan.
(4) $a(b - c) = ab - ac$, $(b - c)a = ba - ca$.
b) Ha R-ben $1 = 0$ akkor $R = \{0\}$, azaz R *null-gyűrű*.
Az alábbiakban, ha létezik $1 \in R$, akkor feltételezzuk, hogy $1 \neq 0$.
c) Az R egységelemes gyűrű test $\Leftrightarrow$ $(R^*, \cdot)$ csoport, ahol $R^* = R \setminus \{0\}$. Általában, $(R^*, \cdot)$ monoid, és $(U(R), \cdot)$ csoport.
d) Ha R Lie-gyűrű, akkor R **antikommutatív**, azaz $ab = -ba$ minden $a, b \in R$ esetén.

1.43. feladat. Ha R kommutatív gyűrű, akkor érvényesek a következő azonosságok:
a) $(\sum_{i=1}^{n} a_i)(\sum_{j=1}^{m} b_j) = \sum_{i=1}^{n} \sum_{j=1}^{m} a_i b_j$;
b) $(a + b)^n = \sum_{k=0}^{n} C_n^k a^{n-k} b^k$ (**Newton binomiális képlete**).

1.44. feladat. Legyen R egy (asszociatív) gyűrű, $[a, b] = ab - ba$, $(\forall) a, b \in R$. Igazoljuk, hogy $(R, +, [-, -])$ Lie-gyűrű.

1.3.2. definíció. Legyen R egy gyűrű és $a, b \in R$.
a) Ha $a, b \neq 0$ és $ab = 0$ akkor azt mondjuk, hogy a **bal oldali zérusosztó** és b **jobb oldali zérusosztó**.
b) R **zérusosztómentes gyűrű**, ha minden $r, s \in R$ esetén $rs = 0 \Rightarrow r = 0$ vagy $s = 0$. Egy kommutatív, zérusosztómentes, egységelemes gyűrűt **integritástartomány**nak nevezünk.
c) a **idempotens**, ha $a^2 = a$. Jelölés: $\mathrm{Idemp}(R) = \{a \in R \mid a \text{ idempotens}\}$.
d) a **nilpotens**, ha létezik $n \in \mathbb{N}^*$ úgy, hogy $a^n = 0$.
Jelölés: $r(R) = \{a \in R \mid a \text{ nilpotens}\}$.

1.45. feladat. a) 0, 1 idempotens elemek; ha $e \neq 0, 1$ idempotens, akkor zérusosztó, $e(1 - e) = (1 - e)e = 0$, és $1 - e$ is idempotens.
b) Ha $a \in R$ invertálható, akkor a nem zérusosztó.
c) (*Egyszerűsítés*) Ha $a \in R$ nem zérusosztó, és $ab = ac$ vagy $ba = ca$, akkor $b = c$.
d) Ha R test, akkor R zérusosztómentes gyűrű; fordítva nem igaz.

1.3.3. tétel. *Minden véges integritástartomány test.*

Bizonyítás. Legyen $a \in R^*$ és $t_a : R \to R$, $t_a(x) = ax$. Azonnal következik, hogy t_a injektív. Mivel R véges, következik, hogy t_a szürjektív, tehát létezik $x \in R$ úgy, hogy $ax = 1$. ■

1.46. feladat. Legyen R egy egységelemes gyűrű és $a, b \in R$.
a) Ha R kommutatív, a nilpotens és b invertálható, akkor $a + b$ invertálható.
b) Ha $1 - ab$ invertálható, akkor $1 - ba$ invertálható.
c) Ha $a, b, ab - 1$ invertálható elemek, akkor $a - b^{-1}$, $(a - b^{-1})^{-1} - a^{-1}$ invertálhatók, és $((a - b^{-1})^{-1} - a^{-1})^{-1} = aba - a$.

1.47. feladat. Legyen R egy gyűrű és $Z(R) = \{r \in R \mid rx = xr, \ \forall x \in R\}$ az R **centruma**. Igazoljuk, hogy
a) R kommutatív $\Leftrightarrow$ $Z(R) = R$.
a) Ha R-ben nem léteznek nemnulla nilpotens elemek, akkor minden idempotens elem centrális (azaz eleme $Z(R)$-nek).
b) Ha $(\forall) x \in R$ $x^2 - x \in Z(R)$, akkor R kommutatív.

1.48. feladat. Legyen R egy véges gyűrű.
a) Ha R egységelemes, akkor minden nemnulla elem vagy bal oldali zérusosztó vagy invertálható.
b) Feltételezzük, hogy $(\exists) a \in R$, a nem bal oldali zérusosztó, és $(\exists) b \in R$, b nem jobb oldali zérusosztó. Akkor R egységelemes gyűrű.

1.49. feladat. Legyen R egy egységelemes gyűrű és $a \in R$. Ha a-nak több bal oldali inverze van, akkor végtelen sok van.

1.3.2. Gyűrűmorfizmusok

1.3.4. definíció. Legyen R és R' két gyűrű.

a) Az $f : R \to R'$ függvényt **gyűrűmorfizmus**nak nevezzük, ha minden $a, b \in R$ esetén

(1) $f(a + b) = f(a) + f(b)$; (2) $f(ab) = f(a)f(b)$.

Az f-morfizmust *endomorfizmusnak* nevezzük, ha $(R, +, \cdot) = (R', +, \cdot)$.

b) Ha R és R' egységelemes gyűrűk, és $f(1) = 1$, akkor azt mondjuk, hogy f **unitér** morfizmus.

c) f **izomorfizmus**, ha létezik egy $f' : R' \to R$ morfizmus úgy, hogy $f' \circ f = 1_R$ és $f \circ f' = 1_{R'}$.

Jelölések:

- $\mathrm{Hom}(R, R')$ – a morfizmusok halmaza;
- $\mathrm{End}(R)$ – az endomorfizmusok halmaza;
- $\mathrm{Aut}(R)$ – az automorfizmusok halmaza.

1.50. feladat. a) $\theta : R \to R'$, $\theta(a) = 0$, és $1_R : R \to R, 1_R(a) = a$ gyűrűmorfizmusok.

b) Ha $f : R \to R'$ morfizmus, akkor $f(0) = 0$ és $f(-a) = -f(a)$ minden $a \in R$ esetén; ha f unitér és $a \in U(R)$, akkor $f(a^{-1}) = f(a)^{-1}$.

c) Ha R, R' egységelemes gyűrűk és $f : R \to R'$ szürjektív morfizmus, akkor f unitér.

1.51. feladat. a) $f : R \to R'$ izomorfizmus $\Leftrightarrow$ f bijektív morfizmus.

b) Morfizmusok összetétele morfizmus.

c) $(\mathrm{End}(R), \circ)$ monoid, és $(\mathrm{Aut}(R), \circ)$ csoport.

1.52. feladat. Ha K és K' testek és $f : K \to K'$ egy morfizmus, akkor vagy $f = \theta$ (*null-morfizmus*), vagy f unitér és injektív.

1.53. feladat (modulo n maradékosztályok gyűrűje). Legyen $n > 1$, $\mathbb{Z}_n = \{\hat{a} \mid a \in \mathbb{Z}\}$, és értelmezzük a következő műveleteket:

$$\hat{a} + \hat{b} = \widehat{a + b}, \qquad \hat{a}\hat{b} = \widehat{ab},$$

minden $a, b \in \mathbb{Z}$ esetén. Igazoljuk, hogy:

a) A fenti definiciók nem függnek a reprezentánsoktól.

b) $(\mathbb{Z}_n, +, \cdot)$ kommutatív egységelemes gyűrű.

c) Ha $a \equiv b \pmod{n}$, akkor $(a, n) = (b, n)$.

d) Ha $(a, n) = 1$, akkor $\hat{a}$ invertálható $\mathbb{Z}_n$-ben.

e) Ha $(a, n) = d > 1$, akkor $\hat{a}$ zérusosztó.

f) Ha p prímszám, akkor $\mathbb{Z}_p$ test.

g) Ha n nem prímszám, akkor $\mathbb{Z}_n$ nem integritástartomány.

h) Számítsuk ki a 7 inverzét modulo 16 és a 11 inverzét modulo 27.

1.54. feladat (komplex számok teste). Az $\mathbb{R} \times \mathbb{R} = \{z = (x, y) \mid x, y \in \mathbb{R}\}$ halmazon értelmezzük a következő műveleteket:

$$(x, y) + (x', y') = (x + x', y + y'), \qquad (x, y)(x', y') = (xx' - yy', xy' + yx').$$

Igazoljuk, hogy:

a) $(\mathbb{R} \times \mathbb{R}, +, \cdot)$ kommutatív test és $\phi : \mathbb{R} \to \mathbb{R} \times \mathbb{R}$, $x \mapsto (x, 0)$ injektív testmorfizmus.

b) Azonosítjuk x-et $(x, 0)$-val, és legyen $i = (0, 1)$. Ekkor $i^2 = -1$ és $(x, y) = x + yi$. Ez a felírás egyértelmű, vagyis ha $(x, y) = x' + y'i$, akkor $x = x'$ és $y = y'$.

Jelölés: $\mathbb{C} = \{z = x + yi \mid x, y \in \mathbb{R},\ i^2 = -1\}$ a *komplex számok teste*, i az **immaginárius egység**; ha $z = x + yi$, akkor $\Re z = x$ a z **valós része** és $\Im z = yi$ a z **immaginárius része**.

c) Ha $z = x + yi$, legyen $\bar{z} = x - yi$ a z **konjugáltja** és $|z| = \sqrt{z\bar{z}}$ a z **modulusza**. Ekkor, $z \in \mathbb{R} \Leftrightarrow \bar{z} = z$, $z = 0 \Leftrightarrow |z| = 0$, és

$$\overline{z + z'} = \bar{z} + \bar{z}', \quad \overline{zz'} = \bar{z}\bar{z}', \quad \bar{\bar{z}} = z;$$

$$|zz'| = |z| \cdot |z'|, \qquad |z + z'| \le |z| + |z'|.$$

d) Oldjuk meg a $z^2 = a + bi$ egyenletet. Alkalmazás: $a = 3$, $b = 4$.

e) Ha $z = x + yi \in \mathbb{C}$ és $r = |z|$, akkor trigonometriából tudjuk, hogy létezik egyetlen $t \in [0, 2\pi)$ úgy, hogy $\cos t = \frac{x}{r}$ és $\sin t = \frac{y}{r}$, tehát $z = r(\cos t + i \sin t) = \exp(it)$. Ez a z **trigonometrikus alakja**. Ekkor:

- $zz' = rr'(\cos(t + t') + i \sin(t + t'))$;
- $\frac{1}{z} = \frac{1}{r}(\cos(-t) + i \sin(-t))$;
- $z^n = r^n(\cos(nt) + i \sin(nt))$.

f) Ha $z = r(\cos t + i \sin t)$ és $n \geq 1$, akkor a $Z^n = z$ egyenletnek pontosan n megoldása van $\mathbb{C}$-ben:

$$Z_k = \sqrt[n]{r}(\cos \frac{t + 2k\pi}{n} + i \sin \frac{t + 2k\pi}{n}), \quad k = 0, \ldots, n-1.$$

g) Legyen $U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \{\omega_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k = 0, \ldots, n-1\}$ az **n-ed rendű egységgyökök** halmaza. Ekkor:
- $(U_n, \cdot)$ a $(\mathbb{Z}_n, +)$ csoporttal izomorf csoport;
- $Z_k = Z_0 \omega_k$, minden $k = 0, \ldots, n-1$ esetén.

1.55. feladat (gyűrűk direkt szorzata). Legyenek $R_1, \ldots, R_n$ gyűrűk, és $R = R_1 \times \cdots \times R_n$. Ha $r = (r_1, \ldots, r_n)$ és $r' = (r'_1, \ldots, r'_n)$, akkor értelmezés szerint,

$$r + r' = (r_1 + r'_1, \ldots, r_n + r'_n), \qquad rr' = (r_1 r'_1, \ldots, r_n r'_n).$$

Igazoljuk, hogy:
a) $(R, +, \cdot)$ gyűrű.
b) R egységelemes gyűrű $\Leftrightarrow$ R_i egységelemes gyűrűk, $i = 1, \ldots, n$; ebben az esetben $U(R) = U(R_1) \times \cdots \times U(R_n)$.
c) $\mathrm{Idemp}(R) = \mathrm{Idemp}(R_1) \times \cdots \times \mathrm{Idemp}(R_n)$.
d) $r(R) = r(R_1) \times \cdots \times r(R_n)$.

1.56. feladat (függvények gyűrűje). Legyen M egy nemüres halmaz és R egy gyűrű. Az

$$R^M = \{\alpha \mid \alpha : M \to R\}$$

halmazon értelmezzük a következő műveleteket:

$$(\alpha + \beta)(x) = \alpha(x) + \beta(x); \quad (\alpha\beta)(x) = \alpha(x)\beta(x)$$

$(\forall) x \in M$.
a) R^M gyűrű; R^M kommutatív (egységelemes gyűrű) $\Leftrightarrow$ R kommutatív (egységelemes gyűrű).
b) $\alpha \in R^M$ invertálható (idempotens, nilpotens) $\Leftrightarrow$ $(\forall) x \in M$, $\alpha(x)$ invertálható (idempotens, nilpotens (ha M véges)).
c) Ha $|R| \geq 2$ és $|M| \geq 2$, akkor R^M-ben léteznek zérusosztók.
d) Létezik egy $\phi : R \to R^M$ injektív morfizmus.
e) Ha $f : M' \to M$ egy függvény és $g : R \to R'$ egy gyűrű morfizmus, akkor $g^f : R^M \to R'^{M'}$, $(g^f)(\alpha) = g \circ \alpha \circ f$ is morfizmus.

1.57. feladat. Legyen R egy gyűrű és értelmezzük $\mathbb{Z} \times R$-en a következő műveleteket:

$$(m, r) + (n, s) = (m + n, r + s), \quad (m, r)(n, s) = (mn, ms + nr + rs).$$

Igazoljuk, hogy $\mathbb{Z} \times R$ egységelemes gyűrű, és létezik $\phi : R \to \mathbb{Z} \times R$ injektív morfizmus (tehát *minden gyűrű beágyazható egy egységelemes gyűrűbe*).

1.58. feladat (másodfokú algebrai számok). Legyen $d \in \mathbb{Z}$ négyzetmentes,

$$\mathbb{Z}[\sqrt{d}] = \{z = a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$$

és legyen

$$N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}, \ N(z) = |z\bar{z}|,$$

a **norma** függvény, ahol $\bar{z} = a - b\sqrt{d}$ a z *konjugáltja*. Igazoljuk, hogy:
a) $\sqrt{d} \notin \mathbb{Q}$; $a + b\sqrt{d} = x + y\sqrt{d} \Leftrightarrow a = x$ és $b = y$.
b) $(\mathbb{Z}[\sqrt{d}], +, \cdot)$ integritástartomány.
c) $N(zw) = N(z)N(w)$; z invertálható $\Leftrightarrow$ $N(z) = 1$.
d) $U(\mathbb{Z}[i]) = \{\pm 1, \pm i\}$; $U(\mathbb{Z}[i\sqrt{d}]) = \{\pm 1\}$ ha $d \geq 2$; $U(\mathbb{Z}[\sqrt{2}])$ végtelen csoport.
e) Ha $e \in \mathbb{Z}$ négyzetmentes, $d \neq e$, akkor $\mathbb{Z}[\sqrt{d}] \cap \mathbb{Z}[\sqrt{e}] = \mathbb{Z}$.

1.59. feladat (kvadratikus testek). Legyen $d \in \mathbb{Z}$ négyzetmentes és $\mathbb{Q}(\sqrt{d}) = \{z = a + b\sqrt{d} \mid a, b \in \mathbb{Q}\}$. Igazoljuk, hogy $(\mathbb{Q}(\sqrt{d}), +, \cdot)$ kommutatív test.

1.60. feladat. Igazoljuk, hogy a következő struktúrák *véges testek*:
a) $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, \cdot)$, ahol $(a, b) + (c, d) = (a + c, b + d)$, $(a, b)(c, d) = (ac + bd, ad + bc + bd)$.
b) $(\mathbb{Z}_3 \times \mathbb{Z}_3, +, \cdot)$, ahol $(a, b) + (c, d) = (a + c, b + d)$, $(a, b)(c, d) = (ac - bd, ad + bc)$.

1.61. feladat (mátrixgyűrű). Legyen R egy gyűrű és $m, n \in \mathbb{N}^*$. Egy $A : \{1, \dots, m\} \times \{1, \dots, n\} \to R$ függvényt $m \times n$-típusú R-feletti *mátrix*nak nevezünk, és az

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & & \dots & \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix} = [a_{ij}]_{\substack{1 \le i \le m \\ 1 \le j \le n}} \in M_{m,n}(R)$$

jelöléseket használjuk. Ha $A, A' \in M_{m,n}(R)$ és $B \in M_{n,p}(R)$, akkor értelmezés szerint

$$A + A' = [a_{ij} + a'_{ij}] \in M_{m,n}(R), \qquad AB = [\sum_{k=1}^{n} a_{ik} b_{kj}] \in M_{m,p}(R).$$

Legyen $A = (a_{ij}) \in M_{k,m}(R)$, $B = (b_{ij}), B' = (b'_{ij}) \in M_{m,n}(R)$, $C = (c_{ij}) \in M_{n,p}(R)$. Igazoljuk, hogy:
a) $(AB)C = A(BC)$, $A(B + B') = AB + AB'$ és $(B + B')C = BC + B'C$.
b) $(M_n(R), +, \cdot)$ gyűrű, ahol $M_n(R) := M_{n,n}(R)$.
c) $M_n(R)$ egységelemes gyűrű $\Leftrightarrow$ R egységelemes gyűrű. Ebben az esetben, $AI_n = I_m A = A$ $(\forall) A \in M_{m,n}(R)$, ahol $I_n = (\delta_{ij})_{1 \le i,j \le n} \in M_n(R)$, és $\delta_{ij} = \begin{cases} 1, & i = j, \\ 0, & i \ne j \end{cases}$ a *Kronecker-szimbólum.*
d) $M_n(R)$ kommutatív $\Leftrightarrow$ $R \cdot R = 0$.
e) Ha R egységelemes gyűrű, $n \ge 2$ és $\phi, \psi : R \to M_n(R)$, $\phi(r) = rI_n$, $\psi(r) = E_{11}$, akkor ϕ és ψ injektív morfizmusok, ϕ unitér, ψ nem unitér.
f) Ha R kommutatív gyűrű, akkor $\phi : M_n(R) \to M_n(R)$, $\phi(A) = A^t = (a_{ji})$ antiautomorfizmus, $\phi^2 = 1_{M_n(R)}$, és ha A invertálható, akkor $(A^{-1})^t = (A^t)^{-1}$.
g) $M_n(M_m(R)) \simeq M_{mn}(R)$.

1.62. feladat. Ha $f : R \to S$ egy morfizmus, legyen

$$M_n(f) : M_n(R) \to M_n(S), \ M_n(f)((a_{ij})) = (f(a_{ij})).$$

Bizonyítsuk be, hogy:
a) $M_n(f)$ morfizmus.
b) $M_n(1_R) = 1_{M_n(R)}$ és $M_n(g \circ f) = M_n(g) \circ M_n(f)$.

1.63. feladat. Legyen $K = \left\{ \begin{pmatrix} x & y \\ -y & x \end{pmatrix} \mid x, y \in \mathbb{R} \right\}$ és $A_k = \left\{ \begin{pmatrix} a & b \\ kb & a \end{pmatrix} \mid a, b \in \mathbb{Z} \right\}$, $k \in \mathbb{Z}$. Igazoljuk, hogy:
a) $(K, +, \cdot)$ test és $K \simeq \mathbb{C}$.
b) $(A_k, +, \cdot)$ kommutatív egységelemes gyűrű.
c) A_k integritástartomány $\Leftrightarrow$ k nem teljes négyzet.
d) $A_k \simeq B_k$, ahol $B_k = (\mathbb{Z} \times \mathbb{Z}, +, \cdot)$, $(a, b) + (c, d) = (a + c, b + d)$ és $(a, b)(c, d) = (ac + kbd, ad + bc)$.
e) Ha $d \in \mathbb{Z}$ négyzetmentes szám, akkor $\mathbb{Z}[\sqrt{d}] \simeq A_d \simeq B_d$.

1.64. feladat (kvaterniók teste). Legyen $\mathbb{H} = \left\{ \begin{pmatrix} z & w \\ -\bar{w} & \bar{z} \end{pmatrix} \mid z, w \in \mathbb{C} \right\} \subseteq M_2(\mathbb{C})$. Bizonyítsuk be, hogy:
a) $(\mathbb{H}, +, \cdot)$ nemkommutatív test és létezik egy $\psi : \mathbb{C} \to \mathbb{H}$ injektív testmorfizmus. *Jelölés*:

$$\mathbf{1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \ \mathbf{i} = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}, \ \mathbf{j} = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \ \mathbf{k} = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix},$$

tehát

$$\mathbb{H} = \{x = a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{R}\}.$$

b) $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -\mathbf{1}$; $\mathbf{ij} = -\mathbf{ji} = \mathbf{k}$; $\mathbf{jk} = -\mathbf{kj} = \mathbf{i}$; $\mathbf{ki} = -\mathbf{ik} = \mathbf{j}$.
c) $\mathbb{H} \simeq \mathbb{H}_1$, ahol $\mathbb{H}_1 = \left\{ \begin{pmatrix} a & b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$.
d) $\mathbb{H}_0$ test, ahol $\mathbb{H}_0 := \{a\mathbf{1} + b\mathbf{i} + c\mathbf{j} + d\mathbf{k} \mid a, b, c, d \in \mathbb{Q}\}$ (*racionális kvaterniók*).
e) Ha $\mathbb{I} := \{\frac{a}{2}\mathbf{1} + \frac{b}{2}\mathbf{i} + \frac{c}{2}\mathbf{j} + \frac{d}{2}\mathbf{k} \mid a, b, c, d \in \mathbb{Z}$ mind páros vagy mind páratlan$\}$, akkor $\mathbb{I}$ gyűrű és nem test.
f) $Q_8 := \{\pm\mathbf{1}, \pm\mathbf{i}, \pm\mathbf{j}, \pm\mathbf{k}\}$ csoport (készítsünk művelettáblát). Q_8-cat a nyolcelemű **kvaterniócsoport**nak nevezzük.

1.65. feladat. Ha $x = a1 + bi + cj + dk$, legyen $\bar{x} = a1 - bi - cj - dk$, $N(x) = x\bar{x}$ és $\mathrm{Tr}(x) = x + \bar{x}$. Igazoljuk, hogy :

a) $\phi : \mathbb{H} \to \mathbb{H}$, $x \mapsto \bar{x}$ másodrendű antiautomorfizmusa $\mathbb{H}$-nak, és $\phi \circ \phi = 1_{\mathbb{H}}$. (Azt mondjuk, hogy ϕ *involució*).

b) $N(xy) = N(x)N(y)$, és ha $x \neq 0$ akkor $x^{-1} = \bar{x}/N(x)$.

1.66. feladat (Abel-csoport endomorfizmusgyűrűje). Legyen $(A, +)$ egy Abel-csoport, és legyen

$$f + g : A \to A, \quad (f + g)(x) = f(x) + g(x)$$

minden $f, g \in \mathrm{End}(A, +)$ esetén.

a) Igazoljuk, hogy $(\mathrm{End}(A, +), +, \circ)$ egységelemes gyűrű.

b) Ha $(R, +, \cdot)$ egy egységelemes gyűrű, akkor $\phi : R \to \mathrm{End}(R, +)$, $\phi(a) = t_a$ injektív unitér gyűrűmorfizmus, ahol $t_a : R \to R$, $t_a(r) = ar$.

c) Határozzuk meg az $\mathrm{End}(\mathbb{Z}, +)$ és $\mathrm{End}(\mathbb{Q}, +)$ gyűrűket.

d) Határozzuk meg a $(\mathbb{Z}, +)$ automorfizmusait. Igazoljuk, hogy $(\mathrm{Aut}(\mathbb{Z}, +), \circ) \simeq (U_2, \cdot)$.

e) Határozzuk meg a $(\mathbb{Q}, +)$ automorfizmusait. Igazoljuk, hogy $(\mathrm{Aut}(\mathbb{Q}, +), \circ) \simeq (\mathbb{Q}^*, \cdot)$.

1.67. feladat. a) Határozzuk meg a $(\mathbb{Z}, +, \cdot)$ endomorfizmusait.

b) Határozzuk meg a $\mathrm{Hom}(\mathbb{Z}, \mathbb{Q})$ halmazt.

c) Legyen R egy gyűrű. Igazoljuk, hogy $\phi : \mathrm{Hom}(\mathbb{Z}, R) \to \mathrm{Idemp}(R)$, $\phi(f) = f(1)$ bijektív függvény.

d) Határozzuk meg a $\mathrm{Hom}(\mathbb{Q}(\sqrt{d}), \mathbb{Q}(\sqrt{e}))$ halmazt és az $(\mathrm{Aut}(\mathbb{Q}(\sqrt{d})), \circ)$ csoportot, ahol $d \neq e$ négyzetmentes egész számok.

1.68. feladat. Határozzuk meg az $(\mathrm{Aut}(\mathbb{R}), \circ)$ csoportot.

1.69. feladat. Ha $n \in \mathbb{N}$, $n \geq 2$ és $(\mathbb{Z}_n, +, *)$ egységelemes gyűrű, akkor $(\mathbb{Z}_n, +, *) \simeq (\mathbb{Z}_n, +, \cdot)$.

1.70. feladat. Határozzuk meg az összes 4-elemű nemizomorf egységelemes gyűrűt.

1.71. feladat. a) Ha $(R, +, \cdot) \simeq (S, +, \cdot)$, akkor $(U(R), \cdot) \simeq (U(S), \cdot)$.

b) Igazoljuk, hogy $(\mathbb{R} \times \mathbb{R}, +, \cdot) \not\simeq (\mathbb{C}, +, \cdot)$.

1.72. feladat. a) Ha K egy kommutatív test, akkor $(K, +) \not\simeq (K^*, \cdot)$.

b) Határozzuk meg az $f : (\mathbb{Q}, +) \to (\mathbb{Q}^*, \cdot)$ homomorfizmusokat.

1.73. feladat (injektív morfizmusok jellemzése). Legyen $f : R \to S$ egy gyűrűhomomorfizmus. A következő állítások ekvivalensek:

(i) f injektív.

(ii) $\mathrm{Ker}\, f = \{0\}$.

(iii) f **monomorfizmus**, (azaz minden $\alpha, \beta : R' \to R$ gyűrűmorfizmus esetén, $f \circ \alpha = f \circ \beta \Rightarrow \alpha = \beta$).

1.74. feladat. Legyen $f : R \to S$ egy gyűrűmorfizmus. Azt mondjuk, hogy f **epimorfizmus**, ha minden $\alpha, \beta : S \to S'$ gyűrűmorfizmusok esetén $\alpha \circ f = \beta \circ f \Rightarrow \alpha = \beta$. Igazoljuk, hogy:

a) Ha f szürjektív, akkor f epimorfizmus.

b) $\mathbb{Z} \to \mathbb{Q}$, $n \mapsto n$ epimorfizmus és nem szürjektív.

c) $\mathbb{Z} \to \mathbb{Z}[\sqrt{d}]$, $n \mapsto n$ nem epimorfizmus.

1.75. feladat. Legyenek R és S egységelemes gyűrűk és $f : R \to S$ egy szürjektív (tehát unitér) morfizmus. Igazoljuk, hogy:

a) ha $r \in R$ invertálható (centrális, idempotens, nilpotens), akkor $f(r)$ invertálható (centrális, idempotens, nilpotens);

b) a fordított állítás nem igaz.

1.3.3. Részgyűrűk, résztestek

1.3.5. definíció. a) Legyen $(R, +, \cdot)$ egy gyűrű és $S \subseteq R$. Azt mondjuk, hogy S **részgyűrűje** R-nek (*jelölés*: $S \leq R$), ha S zárt részhalmaza R-nek az „+”-ra és „·”-ra nézve és, ha az $(S, +, \cdot)$ szintén gyűrű.

Ha R egységelemes és $1 \in S$, az S részgyűrűje R-nek, akkor S **unitér részgyűrű**.

b) Legyen $(K, +, \cdot)$ test , $L \subseteq K$. Azt mondjuk, hogy L **részteste** K-nak (*jelölés*: $L \leq K$), ha az L zárt a két műveletre nézve és az $(L, +, \cdot)$ szintén test.

1.3.6. tétel (részgyűrűk és résztestek jellemzése). a) *Adott az* $(R, +, \cdot)$ *gyűrű és legyen* $S \subseteq R$. S *akkor és csak akkor részgyűrűje az* R*-nek, ha*

1. $S \neq \emptyset$;

2. *minden* $a, b \in S$ *esetén* $a - b, ab \in S$.

b) *Adott a* $(K, +, \cdot)$ *test és* $L \subseteq K$. L *akkor és csak akkor részteste* K*-nak, ha*

1. $|L| \geq 2$;

2. *minden* $a, b \in L$, $b \neq 0$ *esetén,* $a - b, ab^{-1} \in L$.

Bizonyítás. a)„$\Longrightarrow$" Feltételezzűk, hogy S részgyűrűje R-nek. Ebből következik, hogy S gyűrű az indukált műveletekkel. Alkalmazva a részcsoportok jellemzési tételét következik, hogy $S \neq \emptyset$, minden $a, b \in S$ esetén $a - b \in S$. A „$\cdot$" indukált művelet értelmezéséből következik, hogy $a \cdot b \in S$.

„$\Longleftarrow$" Mivel $S \neq \emptyset$ és minden $a, b \in S$ esetén $a - b \in S$, a részcsoportok jellemzési tételéből következik, hogy S részcsoportja $(R, +)$-nak, tehát S zárt az összeadásra nézve és $(S, +)$ csoport. Mivel S zárt a szorzásra nézve is, és a műveletek tulajdonságai öröklődnek, következik, hogy $(S, +, \cdot)$ gyűrű.

b) „$\Longrightarrow$" Feltételezzük, hogy L részteste K-nak. Akkor L test, tehát L-nek van legalább két eleme. Az $(L, +)$ részcsoportja $(K, +)$-ból, következik, hogy minden $a, b \in L$ esetén $a - b \in L$. Abból, hogy $(L^*, \cdot)$ csoport, következik, hogy minden $a, b \in L$ esetén $ab^{-1} \in L$.

„$\Longleftarrow$" Mivel $|L| \geq 2$ és minden $a, b \in L$ esetén $a - b \in L$, következik, hogy L részcsoportja $(K, +)$-nak. Minden $a, b \in L^*$ esetén $ab^{-1} \in L$, de egy testben nincsenek zérusosztók és nem nulla elem inverze nemnulla, következik, hogy $ab^{-1} \in L^*$. Tehát L^* részcsoportja $(K^*, \cdot)$. Mivel L zárt a két műveletre nézve is, és a műveletek tulajdonságai öröklődnek, következik, hogy $(L, +, \cdot)$ test. ■

1.3.7. példa. $\mathbb{Z}$ részgyűrűje $(\mathbb{Q}, +, \cdot)$-nak, $\mathbb{Q}$ részteste $(\mathbb{R}, +, \cdot)$-nak és $\mathbb{R}$ részteste $(\mathbb{C}, +, \cdot)$-nak.

2) Ha R gyűrű, akkor $\{0\}$ és R részgyűrűi R-nek. Ezeket *triviális* részgyűrűknek nevezzük. Ha S az R-nek olyan részgyűrűje, hogy $S \neq \{0\}$ és $S \neq R$, akkor S-et *valódi részgyűrűnek* nevezzük.

3) Ha R egy gyűrű (test), akkor

$$Z(R) = \{r \in R \mid rx = xr, \ \forall x \in R\}$$

részgyűrűje (részteste) R-nek. A $Z(R)$-et az R **centrum**ának nevezzük.

1.76. feladat. a) $R = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \leq M_2(\mathbb{C})$; R-ben nem létezik jobb oldali egységelem, és végtelen sok bal oldali egységelem létezik.

b) $S = \left\{ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mid a, b \in \mathbb{C} \right\}$ unitér részgyűrűje $M_2(\mathbb{C})$-nek.

c) $T = \left\{ \begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{C} \right\} \leq M_2(\mathbb{C})$, nem unitér, de T egységelemes gyűrű.

1.77. feladat (trianguláris mátrixok). Legyen R egy gyűrű és

$$T_n(R) = \{A = (a_{ij}) \in M_n(R) \mid a_{ij} = 0 \text{ ha } i > j\}$$

a *felső trianguláris mátrixok* halmaza. Bizonyítsuk be, hogy:

a) $T_n(R) \leq M_n(R)$.

b) $f : T_n(R) \to R^n$, $f((a_{ij})) = (a_{11}, \ldots, a_{nn})$ szürjektív homomorfizmus.

c) Ha $A \in \operatorname{Ker} f$, akkor $A^n = 0_n$.

1.78. feladat. Ha R egységelemes gyűrű, akkor $Z(M_n(R)) = Z(T_n(R)) = \{aI_n \mid a \in Z(R)\}$.

1.79. feladat. Legyen p egy prímszám és

$$\mathbb{Q}(\sqrt[3]{p}) = \{z = a + b\sqrt[3]{p} + c\sqrt[3]{p^2} \mid a, b, c \in \mathbb{Q}\}.$$

Bizonyítsuk be, hogy:

a) $a + b\sqrt[3]{p} + c\sqrt[3]{p^2} = 0 \Leftrightarrow a = b = c = 0$.

b) $\mathbb{Q}(\sqrt[3]{p})$ részteste $\mathbb{R}$-nek.

c) $\{a + b\sqrt[3]{p} \mid a, b \in Q\}$ nem részteste $\mathbb{R}$-nek.

1.80. feladat. Legyen $S \subseteq \mathbb{Z}[\sqrt{d}]$. Igazoljuk, hogy S unitér részgyűrűje $\mathbb{Z}[\sqrt{d}]$-nek $\Leftrightarrow (\exists) n \in \mathbb{N}$ úgy, hogy $S = \mathbb{Z} + n\sqrt{d}\mathbb{Z}$.

1.81. feladat. Legyen $C([0, 1]) = \{\alpha : [0, 1] \to \mathbb{R} \mid \alpha \text{ folytonos}\}$. Igazoljuk, hogy:

a) $C([0, 1]) \leq (\mathbb{R}^{[0,1]}, +, \cdot)$.

b) α invertálható $\Leftrightarrow \alpha > 0$ vagy $\alpha < 0$.

c) α idempotens $\Leftrightarrow \alpha = 0$ vagy $\alpha = 1$.

d) α nilpotens $\Leftrightarrow \alpha = 0$.

e) α zérusosztó $\Leftrightarrow (\exists) \varnothing \neq I \subseteq [0, 1]$ nyílt intervallum úgy, hogy $\alpha(t) = 0$ $(\forall) t \in I$.

1.82. feladat. Legyen R egy gyűrű, $X \subseteq R$ és

$$C_R(X) = \{r \in R \mid rx = xr \ (\forall) x \in X\}$$

az X **centralizátora** (tehát $C_R(R) = Z(R)$, az R *centruma*). Igazoljuk, hogy:
a) $C_R(X) \leq R$; ha R test, akkor $C_R(X)$ résztest.
b) $X \subseteq Y \Rightarrow C_R(X) \supseteq C_R(Y)$.
c) $X \subseteq C_R(C_R(X))$.
d) $C_R(C_R(C_R(X))) = C_R(X)$.
e) Határozzuk meg $Z(\mathbb{H})$-t és $C_{\mathbb{H}}(\mathbf{i})$-t.

1.4. Polinomok

Ebben a paragrafusban, A-val jelölünk egy kommutatív egységelemes gyűrűt.

1.4.1. A polinomgyűrű szerkesztése

Legyen $A^{\mathbb{N}} = \{f \mid f : \mathbb{N} \to A\}$ a *sorozatok* halmaza. Ha $f \in A^{\mathbb{N}}$, akkor az $f = (a_0, a_1, \dots)$ jelölést alkalmazzuk, ahol $a_n = f(n)$ minden $n \in \mathbb{N}$ esetén.

Az $A^{\mathbb{N}}$ halmazon értelmezzük a következő műveleteket: ha $f = (a_0, a_1, \dots), g = (b_0, b_1, \dots) \in A^{\mathbb{N}}$, akkor

$$(f+g)(n) = f(n) + g(n) = a_n + b_n,$$
$$(fg)(n) = \sum_{i+j=n} f(i)g(j) = \sum_{i+j=n} a_i b_j.$$

Továbbá, legyen

$$\operatorname{supp}(f) = \{n \in \mathbb{N} \mid a_n \neq 0\}$$

az f **tartóhalmaza**, és legyen

$$A^{(\mathbb{N})} = \{f \in A^{\mathbb{N}} \mid \operatorname{supp}(f) \text{ véges halmaz}\}.$$

1.4.1. tétel. a) *$A^{\mathbb{N}}$ kommutatív egységelemes gyűrű.*
b) *$A^{(\mathbb{N})}$ unitér részgűrűje $A^{\mathbb{N}}$-nek és*

$$\iota_A : A \to A^{(\mathbb{N})}, \quad \iota_A(a) = (a, 0, 0, \dots)$$

injektív unitér morfizmus. (Azonosítani fogjuk a-t $\iota_A(a)$-val.)
c) *Legyen $X = (0, 1, 0, \dots)$. Ha $f \in A^{(\mathbb{N})}$ úgy, hogy $a_i = 0$ minden $i > n$ esetén, akkor*

$$f = a_0 + a_1 X + \dots a_n X^n = \sum_{k=0}^{n} a_k X^k,$$

és ez a felírás egyértelmű.

Bizonyítás. a) Azonnal belátható, hogy $(A^{\mathbb{N}}, +)$ Abel-csoport. Vizsgáljuk a szorzás tulajdonságait. Mivel A kommutatív gyűrű, következik, hogy „$\cdot$” kommutatív művelet. Ha $f, g, h \in A^{\mathbb{N}}$, akkor minden $n \in \mathbb{N}$ esetén,

$$\begin{aligned}((f+g)h)(n) &= \sum_{i+j=n} (f+g)(i)h(j) \\ &= \sum_{i+j=n} (f(i) + g(i))h(j) \\ &= \sum_{i+j=n} (f(i)h(j) + g(i)h(j)) \\ &= \sum_{i+j=n} f(i)h(j) + \sum_{i+j=n} g(i)h(j) \\ &= (fh)(n) + (gh)(n) = (fh + gh)(n),\end{aligned}$$

$$\begin{aligned}((fg)h)(n) &= \sum_{i+j=n} (fg)(i)h(j)\\ &= \sum_{i+j=n} (\sum_{k+l=i} (f(k)g(l))h(j)\\ &= \sum_{k+l+j=n} f(k)g(l)h(j)\\ &= \sum_{k+m=n} f(k) \sum_{l+j=m} g(l)h(j)\\ &= \sum_{k+m=n} (f(k)(gh)(m) = (f(gh))(n).\end{aligned}$$

Végűl, az $A^{\mathbb{N}}$ egységeleme $1 = (1, 0, 0, \dots)$.

b) Vegyük észre, hogy $0 = (0, 0, \dots)$, $1 = (1, 0, \dots) \in A^{(\mathbb{N})}$, és ha $f, g \in A^{(\mathbb{N})}$ úgy, hogy $f(i) = 0$ ha $i > m$, $g(j) = 0$ ha $j > n$, akkor $(f + g)(i) = 0$ ha $i > \max\{m, n\}$, $(-f)(i) = 0$ ha $i > m$, és $(fg)(i) = 0$ ha $i > m + n$. A műveletek tulajdonságai öröklődnek, és könnyen belátható, hogy ι_A injektív unitér morfizmus.

c) Vegyük észre, hogy $X^k(i) = \delta_{ik}$ azaz,

$$X^k = (\underset{0}{0}, \underset{1}{0}, \dots, 0, \underset{k}{1}, 0, \dots),$$

és ha $a = \iota_A(a) = (a, 0, \dots)$, akkor $(aX^k)(i) = a\delta_{ik}$; következik, hogy

$$\begin{aligned}f &= (a_0, a_1, \dots, a_n, 0, \dots)\\ &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, 0, \dots, 0, a_n, 0, \dots)\\ &= \sum_{k=0}^{n} a_k X^k,\end{aligned}$$

és a felírás egyértelműsége evidens. ■

1.4.2. definíció. a) $A^{\mathbb{N}}$-et az A-feletti **formális sor**ok gyűrűjének nevezzük, és $A^{(\mathbb{N})}$ az A-feletti *polinomgyűrű*. X-et **határozatlannak** nevezzük, és az $a_i = f(i) \in A$ elemek az f **együtthatói**.

Jelölések: $A^{\mathbb{N}} = A[[X]]$, $A^{(\mathbb{N})} = A[X] = \{f = \sum_{i=0}^{n} a_i X^i \mid n \in \mathbb{N},\ a_i \in A\}$.

Ha $f = (a_0, a_1, \dots) \in A[[X]]$, akkor az $f = \sum_{i=0}^{\infty} a_i X^i$ formális jelölést használjuk.

b) Ha $f = \sum_{i=0}^{n} a_i X^i \in A[X]$ egy nemnulla polinom, akkor $\deg(f) = \max\{i \in \mathbb{N} \mid a_i \neq 0\}$ az f **foka**. Ha $\deg(f) = n$ akkor a_n az f **főegyütthatója**. Értelmezés szerint, $\deg 0 = -\infty$.

Ha $f \in A[[X]]$ egy formális sor, akkor $o(f) = \min\{n \in \mathbb{N} \cup \{\infty\} \mid a_n \neq 0\}$ az f **rendje**.

1.83. feladat. a) Ha $f, g \in A[X]$, akkor

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}, \qquad \deg(fg) \leq \deg(f)\deg(g).$$

b) Ha A integritástartomány, akkor $A[X]$ is integritástartomány , és $\deg(fg) = \deg(f)\deg(g)$.

c) $a \in A$ invertálható $A[X]$-ben $\Leftrightarrow$ a invertálható A-ban.

d) Ha A integritástartomány, akkor $U(A[X]) = U(A)$.

1.84. feladat. Legyen A egy kommutatív egységelemes gyűrű, és $f = a_0 + a_1X + \dots + a_nX^n \in A[X]$. Igazoljuk, hogy:

a) f zérusosztó $A[X]$-ben $\Leftrightarrow$ $(\exists)a \in A,\ a \neq 0$ úgy, hogy $af = 0$.

b) f invertálható $A[X]$-ben $\Leftrightarrow$ a_0 invertálható A-ban és a_i nilpotensek, ha $i \geq 1$.

c) f nilpotens $A[X]$-ben $\Leftrightarrow$ $a_0, \dots, a_n$ nilpotens elemek.

1.85. feladat. Legyen $f, g \in A[[X]]$.

a) $o(f + g) \geq \min\{o(f), o(g)\}$; $o(fg) \geq o(f) + o(g)$.

b) Ha A integritástartomány, akkor $A[[X]]$ integritástartomány.

c) f invertálható $A[[X]]$-ben $\Leftrightarrow$ a_0 invertálható A-ban. Számítsuk ki az $1 + X$ inverzét.

1.4.2. Polinomgyűrű univerzális tulajdonsága

A következő tulajdonság jellemzi a polinomgyűrűt.

1.4.3. tétel. *Legyenek* A *és* B *egységelemes gyűrűk,* A *kommutatív,* $\phi : A \to B$ *egy unitér morfizmus, és* $x \in B$ *úgy, hogy* $x\phi(a) = \phi(a)x$ *minden* $a \in A$ *esetén. Ekkor létezik az egyértelműen meghatározott* $\bar{\phi}_x : A[X] \to B$ *unitér morfizmus, amelyre* $\bar{\phi}_x \circ \iota_A = \phi$ *és* $\bar{\phi}_x(X) = x$.

Bizonyítás. Feltételezzük, hogy $\bar{\phi}_x$ létezik, és igazoljuk, hogy egyértelműen meghatározott. Valóban, ha $f = \sum_{i=0}^{n} a_i X^i$, akkor

$$\bar{\phi}_x(f) = \sum_{i=0}^{n} \bar{\phi}_x(a_i)\bar{\phi}_x(X)^i = \sum_{i=0}^{n} \phi(a_i)x^i.$$

Legyen tehát

$$\bar{\phi}_x : A[X] \to B, \qquad \bar{\phi}_x(f) = \sum_{i=0}^{n} \phi(a_i)x^i,$$

és igazoljuk, hogy $\bar{\phi}_x$ rendelkezik a kijelentett tulajdonságokkal. Ha $a \in A$, akkor

$$(\bar{\phi}_x \circ \iota_A)(a) = \bar{\phi}_x(\iota_A(a)) = \bar{\phi}_x(a) = \phi(a).$$

Ha $f = \sum_{i\geq 0} a_i X^i,\ g = \sum_{j\geq 0} b_j X^j \in A[X]$, akkor

$$\begin{aligned}
\bar{\phi}_x(f+g) &= \bar{\phi}_x(\sum_{k\geq 0}(a_k + b_k)X^k) = \sum_{k\geq 0}(\phi(a_k) + \phi(b_k))x^k \\
&= \sum_{k\geq 0}\phi(a_k)x^k + \sum_{k\geq 0}\phi(b_k)x^k = \bar{\phi}_x(f) + \bar{\phi}_x(g). \\
\bar{\phi}_x(fg) &= \bar{\phi}_x(\sum_{k\geq 0}(\sum_{i+j=k} a_i b_j)X^k) = \sum_{k\geq 0}(\sum_{i+j=k}\phi(a_i)\phi(b_j))x^k \\
&= (\sum_{i\geq 0}\phi(a_i)x^i)(\sum_{k\geq 0}\phi(b_j)x^j) = \bar{\phi}_x(f)\bar{\phi}_x(g). \qquad \blacksquare
\end{aligned}$$

1.86. feladat. Legyenek $\phi : A \to B$ és $\psi : B \to C$ unitér homomorfizmusok. Bizonyítsuk be, hogy:

a) Létezik egyetlen $\phi[X] : A[X] \to B[X]$ morfizmus úgy, hogy $i_B \circ \phi = \phi[X] \circ i_A$, ahol $i_A : A \to A[X]$ a kanonikus injekció.

b) $1_A[X] = 1_{A[X]}$ és $(\psi \circ \phi)[X] = \psi[X] \circ \phi[X]$.

1.4.4. definíció. A fenti tételben legyen $A = B$ és $\phi = 1_A$. Ekkor az $\tilde{f} : A \to A,\ \ \tilde{f}(a) = \phi_x(f)$ függvényt **polinomfüggvény**nek nevezzük, és azt mondjuk, hogy $f(x) = \tilde{f}(x) \in A$ f-nek az x-beli **helyettesítési értéke**.

1.4.3. A maradékos osztástétel. Polinomok gyökei

1.4.5. tétel. *Legyen* A *egy integritástartomány és* $f = a_0 + a_1X + \cdots + a_mX^m,\ g = b_0 + b_1X + \cdots + b_nX^n \in A[X]$, *úgy, hogy* b_n *invertálható elem. Ekkor léteznek az egyértelműen meghatározott* $q, r \in A[X]$ *polinomok, amelyekre*

$$f = gq + r, \qquad \deg(r) < \deg(g).$$

Bizonyítás. m szerinti indukciót alkalmazunk. Ha $m < n$, akkor $q = 0$ és $r = f$. Legyen $m \geq n$ és feltételezzük, hogy az állítás igaz m-nél kisebb fokú polinomok esetén. Legyen

$$f' = f - ga_m b_n^{-1} X^{m-n}.$$

Mivel $\deg(f') < m$, léteznek $q', r \in A[X]$ úgy, hogy $f' = gq' + r',\ \deg(r) < \deg(g)$; következik, hogy

$$f = f' + ga_m b_n^{-1} X^{m-n} = (a_m b_n^{-1} X^{m-n} + q')g + r.$$

Ha $f = gq + r = gq_1 + r_1$, $\deg(r), \deg(r') < \deg(g)$, akkor $r - r_1 = (q_1 - q)g,\ \deg(r - r_1) < \deg(g)$, tehát $q = q_1,\ r = r_1$. $\blacksquare$

1.4.6. definíció. a) Ha $f(a) = 0$, akkor azt mondjuk, hogy $x \in A$ **gyöke** f-nek.

b) Azt mondjuk, hogy a k-**szeres gyöke** f-nek ($k \geq 0$), ha létezik $q \in A[X]$ úgy, hogy

$$f = (X - a)^k q, \quad q(a) \neq 0.$$

1.4.7. következmény. *Feltételezzük, hogy A egy integritástartomány.*
a) **(Bezout-tétel)** $a \in A$ *gyöke az* f *polinomnakakkor és csak akkor, ha ha* $f = (X - a)q$, *ahol* $q \in A[X]$.
b) *Ha* $\deg(f) = n$, *akkor* f*-nek legfennebb* n *gyöke van* A*-ban.* (A gyökök *multiplicitását* is számoljuk.)

Bizonyítás. a) Vegyük észre, hogy minden $a \in A$ esetén, $f = (X - a)q + f(a)$.
b) Indukció n-szerint. Ha $n = 1$, $f = a_1X + a_0 \in K[X]$, akkor $a = a_1^{-1}a_0 \in K$ gyöke f-nek.
Feltételezzük, hogy $n > 1$ és a gyöke f-nek; akkor $f = (X - a)g$ és $\deg g = n - 1$. Az indukció feltevéséből következik, hogy g-nek legfennebb $n - 1$ gyöke van K-ban, tehát f-nek legfennebb n gyöke van K-ban. ■

1.87. feladat (Viéte-formulák). Ha $x_1, \dots, x_n \in A$ gyöke az $f = a_n + a_{n-1}X + \cdots + a_1X^{n-1} + a_0X^n \in A[X]$ polinomnak, akkor

$$\begin{aligned}
-a_1 &= a_0(x_1 + x_2 + \cdots + x_n)\\
a_2 &= a_0(x_1x_2 + x_1x_3 + \cdots + x_{n-1}x_n)\\
&\dots\\
(-1)^k a_k &= a_0(x_1 \dots x_k + \cdots + x_{n-k+1} \dots x_n)\\
&\dots\\
(-1)^n a_n &= a_0(x_1 \dots x_n).
\end{aligned}$$

1.88. feladat. Határozzuk meg az $f \in K[X]$ g-vel való osztási maradékát, ha:
a) $g = (X - a)(X - b)$, $a \neq b$.
b) $g = (X - a)^2$.

1.89. feladat. Legyen $\psi : A[X] \to A^A$, $\psi(f) = \tilde{f}$. Igazoljuk, hogy:
a) ϕ unitér gyűrűmorfizmus.
b) Ha A véges test, akkor ψ szürjektív és nem injektív.
c) Ha A végtelen integritástartomány, akkor ψ injektív és nem szürjektív.

A következő tételt a *klasszikus algebra alaptételének* is szokták nevezni. A bizonyítása több ismeretet igényel.

1.4.8. tétel (Gauss–d'Alembert). *Minden* $\mathbb{C}$*-beli együtthatós legalább első fokú polinomnak van* $\mathbb{C}$*-ben gyöke.*

1.90. feladat. Minden $\mathbb{C}$-beli együtthatós n-ed fokú polinomnak pontosan n gyöke van $\mathbb{C}$-ben.

1.91. feladat. Igazoljuk, hogy $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ gyöke az $X^2 - \mathrm{Tr}(z)X + N(z)$ polinomnak, ahol $\mathrm{Tr}(z) := z + \bar{z}$ és $N(z) := z\bar{z}$.

1.92. feladat. a) Legyen $f \in \mathbb{R}[X]$ és $k \in \mathbb{N}$. Ha $z = a + bi \in \mathbb{C}$ k-szeres gyöke f-nek, akkor $\bar{z} = a - bi$ is k-szeres gyöke f-nek.
b) Legyen $f \in \mathbb{Q}[X]$ és $k \in \mathbb{N}$. Ha $z = a + b\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ k-szeres gyöke f-nek, akkor $\bar{z} = a - b\sqrt{d}$ is k-szeresgyöke f-nek.

1.93. feladat. Legyen $f = a_nX^n + \cdots + a_1X + a_0 \in \mathbb{Z}[X]$ és $a = \frac{r}{s}$ egy irreducibilis tört. Ha a gyöke f-nek, akkor $r|a_0$ és $s|a_n$.

1.94. feladat. a) $X^2 - \hat{1}$-nek 4 gyöke van $\mathbb{Z}_{15}$-ben.
b) $X^2 + 1$-nek végtelen sok gyöke van $\mathbb{H}$-ban.
c) Általánosabban, ha $x = a1 + bi + cj + dk$, legyen $\bar{x} = a1 - bi - cj - dk$, $N(x) = x\bar{x}$ és $\mathrm{Tr}(x) = x + \bar{x}$. Igazoljuk, hogy x gyöke az $X^2 - \mathrm{Tr}(x)X + N(x)$ polinomnak; ennek a polinomnak végtelen sok gyöke van $\mathbb{H}$-ban, ha $\mathrm{Tr}(x)$, $N(x)$ rögzitett és $b^2 + c^2 + d^2 > 0$.

1.5. Modulusok, vektorterek, algebrák

1.5.1. Alapfogalmak

Legyen R egy asszociatív, kommutatív egységelemes gyűrű és K egy kommutatív test.

1.5.1. definíció. a) Legyen $(M, +)$ egy Abel-csoport. Azt mondjuk, hogy $M = (M, +, R)$ R-*modulus*, ha értelmezett egy

$$\phi : R \times M \to M, \qquad \phi(a, x) = ax$$

függvény (külső művelet) úgy, hogy a következő négy axióma teljesül:
(M1) $a(x + y) = ax + ay$,

(M2) $(a+b)x = ax + bx$,
(M3) $(ab)x = a(bx)$,
(M4) $1x = x$,
minden $a, b \in R$ és $x, y \in M$ esetén.

Az R gyűrű elemeit **skalár**oknak nevezzük, és a ϕ külső műveletet *skalárokkal való szorzásnak*. $(M, +)$ az M modulus *additív csoportja*.

b) Ha $V = (V, +, K)$ egy K-modulus, akkor V-t K-**feletti vektortér**nek (vagy **lineáris tér**nek) nevezzük, és V elemeit pedig **vektor**oknak.

c) Azt mondjuk, hogy $A = (A, +, \cdot, R)$ R-**algebra**, ha:
(A1) $(A, +, \cdot)$ gyűrű,
(A2) $(A, +, R)$ R-modulus,
(A3) $a(xy) = (ax)y = x(ay)$ minden $a \in R$ és $x, y \in A$ esetén.
A *asszociatív* (*kommutatív*) R-algebra ha $(A, +, \cdot)$ asszociatív (kommutatív) gyűrű.
A **Lie-algebra** ha $(A, +, [-, -])$ Lie-gyűrű.

1.5.2. megjegyzés (Számítási szabályok). a) Legyen M egy R-modulus, és tekintsük az $f_a : M \to M$, $f_a(x) = ax$ és $f'_x : A \to M$, $f'_x(a) = ax$ függvényeket. Az (M1)–(M4) axiomákból következik, hogy $f_a : (M, +) \to (M, +)$ és $f'_x : (A, +) \to (M, +)$ csoportmorfizmusok, tehát minden $a, b \in R$ és $x, y \in M$ esetén
(1) $a0_M = 0_R x = 0_M$.
(2) $(-a)x = a(-x) = -ax$, $(-a)(-x) = ax$.
(3) $a(x - y) = ax - ay$.
(4) $(a - b)x = ax - bx$.
b) Ha R test és $ax = 0$, akkor $a = 0$ vagy $x = 0$.
Valóban, ha $a \neq 0$, akkor létezik $a^{-1} \in R$. Ekkor $x = 1x = (a^{-1}a)x = a^{-1}(ax) = a^{-1}0 = 0$.

1.95. feladat. Ha $(M, +)$ Abel-csoport, akkor M $\mathbb{Z}$-modulus, ahol $\phi(n, x) = nx$, $\forall n \in Z$.

1.96. feladat. Ha $(A, +, \cdot)$ gyűrű, akkor A $\mathbb{Z}$-algebra.

1.97. feladat. R R-algebra, ahol $\phi(a, x) = ax$ $\forall a, x \in R$. Általánosabban, $R^n = \{x = (x_1, \ldots, x_n) \mid x_i \in R\}$ R-algebra, ahol

$$\begin{aligned} x + y &= (x_1 + y_1, \ldots, x_n + y_n), \\ xy &= (x_1 y_1, \ldots, x_n y_n), \\ ax &= (ax_1, \ldots, ax_n) \end{aligned}$$

minden $x, y \in R^n$ és $a \in R$ esetén.

1.98. feladat (függvényalgebra). Legyen I egy halmaz és $R^I = \{f \mid f : I \to R\}$. Igazoljuk, hogy R^I R-algebra, ahol

$$\begin{aligned} (f + g)(i) &= f(i) + g(i), \\ (fg)(i) &= f(i)g(i), \\ (af)(i) &= af(i) \end{aligned}$$

minden $f, g \in R^I$ és $a \in R$ esetén. Vegyük észre, hogy $R^n = R^{\{1,\ldots,n\}}$

1.99. feladat (szabad vektorok). a) $\mathcal{V}_2 = \{\vec{v} = x\vec{i} + y\vec{j} \mid x, y \in \mathbb{R}\}$, (a síkbeli szabad vektorok halmaza) $\mathbb{R}$-feletti vektortér, és azonosítható $\mathbb{R}^2$-tel.

b) $\mathcal{V}_3 = (\mathcal{V}_3, +, \times, \mathbb{R}) = \{\vec{v} = x\vec{i} + y\vec{j} + z\vec{k} \mid x, y, z \in \mathbb{R}\}$, (a térbeli szabad vektorok halmaza) $\mathbb{R}$-feletti Lie-algebra, és azonosítható $\mathbb{R}^3$-nel.

Megemlítjük, hogy ha $\vec{v}_1 = x_1\vec{i} + y_1\vec{j} + z_1\vec{k}$, $\vec{v}_2 = x_2\vec{i} + y_2\vec{j} + z_2\vec{k} \in \mathcal{V}_3$, akkor

$$\vec{v}_1 \times \vec{v}_2 = (y_1 z_2 - z_1 y_2)\vec{i} + (z_1 x_2 - x_1 z_2)\vec{j} + (x_1 y_2 - y_1 x_2)\vec{k}.$$

c) Azonosítsuk $\vec{v}$-t az $x\mathbf{i} + y\mathbf{j} + z\mathbf{k}$ tiszta kvaternióval. Igazoljuk, hogy minden $a_1, a_2 \in \mathbb{R}$ esetén,

$$(a_1 + \vec{v}_1)(a_2 + \vec{v}_2) = (a_1 a_2 - \vec{v}_1 \cdot \vec{v}_2) + (a_1\vec{v}_2 + a_2\vec{v}_1) + \vec{v}_1 \times \vec{v}_2.$$

1.100. feladat. Igazoljuk, hogy $\mathbb{C}$ és $\mathbb{H}$ $\mathbb{R}$-algebrák.

1.101. feladat. Legyen $V = R_+^* = (0, +\infty)$, $K = \mathbb{R}$, $x \oplus y = xy$ és $a \odot x = x^a$, $\forall\ a \in K,\ x, y \in V$. Akkor V K-feletti vektortér.

1.102. feladat. Legyen $V \neq \{0\}$ egy K-feletti vektortér. Igazoljuk, hogy $|K| \leq |V|$.

1.5.2. Részmodulusok, részterek, részalgebrák

1.5.3. definíció. a) Legyen M egy R-modulus és N egy nemüres részhalmaza. Azt mondjuk, hogy N *részmodulusa* $M-$nek (jelölés: $N \leq_R M$ ha

(1) $\forall x, y \in N, \quad x + y \in N.$

(2) $\forall a \in R, \ x \in N, \quad ax \in N.$

b) Ha V K-feletti vektortér, akkor a V részmodulusait *részterekeknek* nevezzük.

c) Legyen A egy R-algebra és B egy nemüres részhalmaza. Azt mondjuk, hogy B *részalgebrája* A-nak (jelölés: $B \leq_R A$, vagy $B \leq (A, +, \cdot, R)$) ha

(1) $\forall x, y \in B, \quad x + y \in B.$

(2) $\forall x, y \in B, \quad xy \in B.$

(3) $\forall a \in R, \ x \in B, \quad ax \in B.$

1.5.4. megjegyzés. a) Ha $N \leq_R M$, akkor N R-modulus az indukált műveletekkel. Ha $B \leq_R A$, akkor B R-algebra az indukált műveletekkel.

b) $\emptyset \neq N \leq_R M$ akkor és csak akkor, ha $\forall\ x, y \in N, \ a, b \in R \ \ ax + by \in N$. $\emptyset \neq B \leq_R A$ akkor és csak akkor, ha $\forall\ x, y \in A, \ a, b \in R \ \ ax + by, xy \in B$.

c) $\{0\}, \ M \leq_R M$. Ezek a *triviális* részmodulusok. Ha $N \leq_R M$, $N \neq \{0\}, \ M$, akkor N *valódi* részmodulus.

1.103. feladat. Legyenek $N_1, \ldots, N_n$ részmodulusok. Akkor

$$\bigcap_{i=1}^{n} N_i := N_1 \cap \cdots \cap N_n,$$

$$\sum_{i=1}^{n} N_i := N_1 + \cdots + N_n = \{x_1 + \cdots + x_n \mid x_i \in N_i\}$$

is részmodulusok.

1.104. feladat. Legyenek N_1, N_2 részmodulusok. Akkor $N_1 \cup N_2 \leq_R M \Leftrightarrow \ N_1 \subseteq N_2$ vagy $N_2 \subseteq N_1$.

1.105. feladat. A $\mathcal{V}_2$ valódi részterei azonosíthatók az origót tartalmazó egyenesekkel.

A $\mathcal{V}_3$ valódi részterei azonosíthatók az origót tartalmazó egyenesekkel vagy síkokkal.

1.106. feladat. Legyen $\mathcal{P} = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(-t) = f(t) \ (\forall) t \in \mathbb{R}\}$ a páros függvények halmaza és $\mathcal{I} = \{f \in \mathbb{R}^{\mathbb{R}} \mid f(-t) = -f(t) \ (\forall) t \in \mathbb{R}\}$ a páratlan függvények halmaza. Igazoljuk, hogy

a) $\mathcal{P}, \ \mathcal{I} \leq \mathbb{R}^{\mathbb{R}}$.

b) Bármely $f \in \mathbb{R}^{\mathbb{R}}$ esetén léteznek az egyértelműen meghatározott $g \in \mathcal{P}$ és $h \in \mathcal{I}$ elemek úgy, hogy $f = g + h$.

c) Ha $f, g \in \mathcal{P} \cup \mathcal{I}$, tanulmányozzuk az fg és $f \circ g$ párosságát. Igazoljuk, hogy $\mathcal{P} \leq (\mathbb{R}^{\mathbb{R}}, +, \cdot, \mathbb{R})$.

1.107. feladat (mátrixalgebra). Igazoljuk, hogy:

a) $(M_{m,n}(R), +, R)$ R-modulus.

b) $a(AB) = (aA)B = A(aB) \ (\forall) A \in M_{m,n}(R), \ B \in M_{n,p}(R), \ a \in R$.

c) $(M_n(R), +, \cdot, R)$ R-algebra. Ha A egy R-algebra, akkor $M_n(A)$ is R-algebra.

d) Legyen $T_n(R) = \{(a_{ij}) \in M_n(R) \mid a_{ij} = 0 \text{ ha } i > j\}$ a *felső trianguláris mátrixok* halmaza. Igazoljuk, hogy $T_n(R)$ részalgebrája $M_n(R)$-nek.

1.108. feladat. Igazoljuk, hogy $\mathbb{C} \leq_{\mathbb{R}} \mathbb{H} \leq_{\mathbb{R}} M_2(\mathbb{C})$, és $\mathbb{H}$ nem $\mathbb{C}$-algebra.

1.109. feladat. Legyen $\mathcal{C}[0,1] = \{\alpha : [0,1] \to \mathbb{R} \mid \alpha \text{ folytonos }\}$ és $\mathcal{D}[0,1] = \{\alpha : [0,1] \to \mathbb{R} \mid \alpha \text{ deriválható}\}$. Igazoljuk, hogy:

a) $\mathcal{D}[0,1] \leq_{\mathbb{R}} \mathcal{C}[0,1] \leq_{\mathbb{R}} (\mathbb{R}^{[0,1]}, +, \cdot, \mathbb{R})$.

Ha $\alpha \in \mathcal{C}[0,1]$, akkor:

b) α invertálható $\Leftrightarrow \alpha > 0$ vagy $\alpha < 0$.

c) α idempotens $\Leftrightarrow \alpha = 0$ vagy $\alpha = 1$.

d) α nilpotens $\Leftrightarrow \alpha = 0$.

e) α zérusosztó $\Leftrightarrow (\exists) \emptyset \neq I \subseteq [0,1]$ nyílt intervallum úgy, hogy $\alpha(t) = 0 \ (\forall) t \in I$.

1.5.3. Lineáris függvények

1.5.5. definíció. a) Legyen M és M' két R-modulus és $f : M \to M'$ egy függvény. Azt mondjuk, hogy f R-**morfizmus** vagy R-**lineáris**, ha

(1) $f(x+y) = f(x) + f(y)$,

(2) $f(ax) = af(x)$.

minden $x, y \in M$ és $a \in R$ esetén.

Az $f : M \to M'$ linearis függvény **izomorfizmus** ha létezik $f' : M' \to M$ úgy, hogy $f' \circ f = \mathbf{1}_M$ és $f \circ f' = \mathbf{1}_{M'}$.

A következő jelöléseket gyakran fogjuk használni:

- $\mathrm{Hom}_R(M, M') = \{f : M \to M' \mid f \ \ R\text{-lineáris}\}$.
- $\mathrm{End}_R(M) = \mathrm{Hom}_R(M, M)$ (**endomorfizmusok** halmaza).
- $\mathrm{Aut}_R(M) = \{f : M \to M \mid f \ \ R\text{-izomorfizmus}\}$ (**automorfizmusok** halmaza).
- $M \simeq M'$ ha létezik $f : M \to M'$ izomorfizmus.

b) Legyen A és A' két R-algebra és $f : A \to A'$ egy függvény. Azt mondjuk, hogy f R-**algebramorfizmus**, ha

(1) $f(x+y) = f(x) + f(y)$,

(2) $f(xy) = f(x)f(y)$,

(3) $f(ax) = af(x)$.

Hasonlómódon értelmezzük az izomorfizmus, endomorfizmus és automorfizmus fogalmakat.

1.110. feladat. a) $f : M \to M'$ R-lineáris $\Leftrightarrow f(ax + by) = af(x) + bf(y)$ minden $x, y \in M$ és $a, b \in R$ esetén.

b) Ebben az esteben $f(0) = 0$ és $f(-x) = -f(x) \ \ \forall x \in M$.

1.111. feladat. Legyen $f : A \to A'$ egy morfizmus. f izomorfizmus $\Leftrightarrow$ f bijektív (érvényes modulusokra is).

1.112. feladat. Legyenek $f, f' : M \to M'$, $g : N \to M$ és $h : M' \to P$ R-lineáris függvények.

a) $f \circ g : N \to M'$ R-lineáris.

b) $h \circ (f + f') \circ g = h \circ f \circ g + h \circ f' \circ g$.

c) $(\mathrm{Hom}_R(M, M'), +, R)$ R-modulus és $(\mathrm{End}_R(M), +, \circ, R)$ R-algebra, ahol

$$(f + f')(x) = f(x) + f'(x)$$
$$(af)(x) = af(x) \quad \forall\ a \in R, x \in M.$$

1.5.6. definíció. Legyen M és M' két modulus és $f : M \to M'$ egy lineáris függvény. Ha $N \leq_R M$ és $N' \leq_R M'$, akkor értelmezzük a következő részhalmazokat:

a) $f(N) = \{f(x) \mid x \in N\} \subseteq M'$.

b) $\mathrm{Im}(f) = f(M) \subseteq M'$ (az f **képe**.)

c) $f^{-1}(N') = \{x \in M \mid f(x) \in N'\}$.

d) $\mathrm{Ker}(f) = f^{-1}(\{0\}) = \{x \in M \mid f(x) = 0\}$ (az f **magja**.)

1.113. feladat. a) $f(N) \leq_R M'$ és $f^{-1}(N') \leq M$. Partikulárisan, $\mathrm{Im}(f) \leq_R M'$ és $\mathrm{Ker} f \leq_R M$.

b) f injektív $\Leftrightarrow \mathrm{Ker} f = \{0\} \Leftrightarrow \ (f(x) = 0 \ \Rightarrow \ x = 0)$.

A következő két feladatban $R = \mathbb{Z}$.

1.114. feladat. Legyen $(A, +)$ és $(B, +)$ két Abel-csoport. Bizonyítsuk be, hogy:

a) $f : A \to B$ csoportmorfizmus $\Leftrightarrow$ f $\mathbb{Z}$-lineáris függvény.

b) $(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}, A), +) \simeq (A, +)$.

c) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Q}, \mathbb{Z}) = \{0\}$.

1.115. feladat. Legyen $(A, +)$ egy Abel-csoport és $m, n \geq 2$. Igazoljuk, hogy:

a) $(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, A), +) \simeq (A_n, +)$, ahol $A_n = \{a \in A \mid na = 0\}$.

b) $\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}) = \{0\}$.

c) $(\mathrm{Hom}_{\mathbb{Z}}(\mathbb{Z}_n, \mathbb{Z}_m), +) \simeq (\mathbb{Z}_{(n,m)}, +)$.

d) $(\mathrm{Aut}_{\mathbb{Z}}(\mathbb{Z}_n, +), \circ) \simeq (U(\mathbb{Z}_n), \cdot)$.

1.116. feladat. Legyenek U és V K-feletti vektorterek. Igazoljuk, hogy:

a) $(U \times V, +, K)$ is K-feletti vektortér, ahol $(u, v) + (u', v') = (u + u', v + v')$ és $\alpha(u, v) = (\alpha u, \alpha v)$.

b) $p_U : U \times V \to U$, $(u, v) \mapsto u$ és $p_V : U \times V \to V$, $(u, v) \mapsto v$ szürjetív lineáris függvények.

c) $U \simeq U \times \{0\} = \mathrm{Ker} p_V \leq_K U \times V$ és $V \simeq \{0\} \times V = \mathrm{Ker} p_U \leq_K U \times V$.

1.117. feladat. Legyen V egy K-feletti vektortér, $S, T \leq_K V$ és $f : S \times T \to V$, $f(s, t) = s + t$. Igazoljuk, hogy:

a) f K-lineáris.

b) $\mathrm{Im}(f) = S + T$.

c) $\mathrm{Ker} f \simeq S \cap T$.

1.118. feladat. Legyen I egy halmaz. Igazoljuk, hogy:
a) Ha $x_0 \in I$ és $\phi : K^I \to K,\ f \mapsto f(x_0)$ lineáris függvény.
b) Ha $(I, +)$ csoport és $U = \{f \in K^I \mid f : (I, +) \to (K, +)$ csoportmorfizmus$\}$, akkor $U \leq_K K^I$.

1.119. feladat (mátrix transzponáltja). Legyen $\phi : M_{m,n}(R) \to M_{n,m}(R)$, $\phi(A) = A^t$, ahol $a^t_{ji} = a_{ij}$. Igazoljuk, hogy:
a) ϕ lineáris függvény.
b) $(AB)^t = B^tA^t$; ha $A \in M_n(R)$ invertálható, akkor $(A^{-1})^t = (A^t)^{-1}$.
c) $f : GL_n(R) \to GL_n(R)$, $f(A) = (A^{-1})^t$ csoportautomorfizmus, ahol $GL_n(R) = U(M_n(R))$ az invertáható mátrixok csoportja.

1.120. feladat. Legyen $\mathcal{S}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A^t = A\}$ (**szimmetrikus mátrix**ok halmaza), és $\mathcal{A}_n(\mathbb{R}) = \{A \in M_n(\mathbb{R}) \mid A^t = -A\}$ (**antiszimmetrikus mátrix**ok halmaza). Igazoljuk, hogy:
a) $\mathcal{S}_n(\mathbb{R}), \mathcal{A}_n(\mathbb{R}) \leq_{\mathbb{R}} M_n(\mathbb{R})$.
b) Bármély $A \in M_n(\mathbb{R})$ esetén léteznek az egyértelműen meghatározott $B \in \mathcal{S}_n(\mathbb{R})$ és $C \in \mathcal{A}_n(R)$ elemek úgy, hogy $A = B + C$.
c) Ha $A, B \in \mathcal{S}_n(\mathbb{R})$, akkor $AB \in \mathcal{S}_n(\mathbb{R}) \Leftrightarrow AB = BA$.
d) $(\forall)B \in M_n(\mathbb{R})$ BB^t szimmetrikus.

1.121. feladat. Ha $A \in M_n(\mathbb{C})$, legyen $A^h = \bar{A}^t$. Igazoljuk, hogy:
a) $(A + B)^h = A^h + B^h$; $(\alpha A)^h) = \bar{\alpha}A^h$.
b) $(AB)^h = B^hA^h$; $(A^{-1})^h = (A^h)^{-1}$.
c) Ha $A = BB^h$ akkor A *hermitikus mátrix* (azaz, $A^h = A$).

1.122. feladat. $A \in M_n(K)$ **idempotens** ha $A^2 = A$; $A \in M_n(K)$ **involució** ha $A^2 = I_n$; $A \in M_n(\mathbb{R})$ *ortogonális* ha $A^{-1} = A^t$. Igazoljuk, hogy:
a) Ha A idempotens, akkor $B = 2A - I_n$ involució.
b) Ha B involució, akkor $A = \frac{1}{2}(I_n + B)$ idempotens.
c) Ha $A \in M_n(\mathbb{R})$ szimmetrikus és ortogonális, akkor involució; ha A ortogonális és involució, akkor szimmetrikus; ha A involució és szimmetrikus, akkor ortogonális.

1.123. feladat (mátrix nyoma). Legyen $\mathrm{Tr} : M_n(R) \to R$, $\mathrm{Tr}(A) = \sum_{i=1}^n a_{ii}$. ($\mathrm{Tr}(A)$ az A **nyoma**.) Igazoljuk, hogy:
a) Tr R-lineáris függvény.
b) $\mathrm{Tr}(AB) = \mathrm{Tr}(BA)$.

1.124. feladat. Legyen $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{C})$, $\mathrm{Tr}(A) = a + d$ és $\det(A) = ad - bc$. Igazoljuk, hogy:
a) $A^2 - \mathrm{Tr}(A)A + \det(A)I_2 = 0_2$.
b) $A^n = a_nA + b_nI_2$ $(\forall)n \in \mathbb{N}$, ahol $a_{n+2} - \mathrm{Tr}(A)a_{n+1} + \det(A)a_n = 0$ és $b_{n+2} - \mathrm{Tr}(A)b_{n+1} + \det(A)b_n = 0$ $(\forall)n \in \mathbb{N}$.
c) Oldjuk meg az $A^2 = A$, $A^2 = 0_2$, $A^3 = 0_2$ és $A^2 = I_2$ egyenleteket.

1.125. feladat. A következő függvények lineárisak:
a) $F : \mathcal{D}[0, 1] \to \mathbb{R}$, $F(f) = f'$.
b) $G : \mathcal{C}[0, 1] \to \mathbb{R}$, $G(f) = \int_0^1 f(t)\,dt$

1.126. feladat. a) Legyen A egy R-algebra úgy, hogy $R \subseteq A$, és legyen $f \in \mathrm{Aut}(A)$ egy gyűrű automorfizmus. Igazoljuk, hogy f R-algebraautomorfizmus (azaz, f R-lineáris) $\Leftrightarrow f(a) = a$ minden $a \in R$ esetén.
b) Határozzuk meg az $(\mathrm{Aut}_{\mathbb{R}}(\mathbb{C}), \circ)$ csoportot.

1.127. feladat (polinomalgebra és függvényalgebra). Legyenek A és B egységelemes gyűrűk, A kommutatív. Legyen $\phi : A \to Z(B)$ egy unitér gyűrűmorfizmus. Igazoljuk, hogy:
a) B A-algebra, az $ab := \phi(a)b$ skalarokkal való szorzással. (Fordítva is igaz: ha B A-algebra, akkor létezik $\phi : A \to Z(B)$ unitér gyűrűmorfizmus.)
c) Igazoljuk, hogy $A[[X]]$ A-algebra, $A[X]$ részalgebrája $A[[X]]$-nek, és $A_n[X] := \{f \in A[X] \mid \deg(f) \leq n\}$ részmodulusa $A[X]$-nek, de nem részalgebra.
d) Az 1.4.3. tételbeli $\bar{\phi}_x : A[X] \to B$ függvény A-algebramorfizmus.
e) Az 1.89. feladatbeli $\psi : A[X] \to A^A$, $\psi(f) = \tilde{f}$ függvény A-algebramorfizmus.

1.128. feladat. Legyen R egy integritástartomány.
a) Alkalmazva a polinomalgebra univerzális tulajdonságát, igazoljuk, hogy

$$\mathrm{Aut}_R(R[X]) = \{\phi : R[X] \to R[X] \mid \phi(r) = r,\ \phi(X) = aX + b,\ a \in U(R),\ b, r \in R\}.$$

b) Legyen $G = \{f_{a,b} = aX + b \in R[X] \mid a \in U(R),\ b \in R\}$. Igazoljuk, hogy $(G, \circ)$ csoport, és $\Gamma : \mathrm{Aut}_R(R[X]) \to G$, $\Gamma(\phi) = \phi(X)$ csoportizomorfizmus.

2. fejezet

Lineáris algebra

A lineáris algebra tárgya a vektorterek és leképezések vizsgálata. Eredete a vektorok és a lineáris egyenletrendszerek tanulmányozására vezethető vissza.

2.1. Lineáris függőség és függetlenség. Bázis

Legyen R egy asszociatív, kommutatív egységelemes gyűrű és K egy kommutatív test.

2.1.1. Lineáris kombinációk. Szabad modulus

2.1.1. definíció. a) Legyen M egy R-modulus, $x_1, \dots, x_n \in M$ és $a_1, \dots, a_n \in R$. Azt mondjuk, hogy $x = a_1x_1 + \cdots + a_nx_n \in M$ az $x_1, \dots, x_n$ elemeknek egy **lineáris kombinációja**. Jelölés:

$$\langle x_1, \dots, x_n \rangle = \{a_1x_1 + \cdots + a_nx_n \mid a_1, \dots, a_n \in R\}.$$

b) $\{x_1, \dots, x_n\}$ *generátorrendszere* M-nek, ha

$$\langle x_1, \dots, x_n \rangle = M.$$

Azt mondjuk, hogy M **végesen generált** ha van egy (véges) $\{x_1, \dots, x_n\}$ generátorrendszere.

c) $x_1, \dots, x_n \in M$ **lineárisan független** elemek ha minden $a_1 \dots, a_n \in R$ esetén

$$a_1x_1 + \cdots + a_nx_n = 0 \quad \Rightarrow \quad a_1 = \cdots = a_n = 0.$$

d) Ellenkező esetben azt mondujuk, hogy az $\{x_1, \dots, x_n\}$ rendszer **lineárisan összefüggő**, azaz, léteznek a nem mind nulla $a_1 \dots, a_n \in R$ skalárok úgy, hogy

$$a_1x_1 + \cdots + a_nx_n = 0.$$

e) Egy lineárisan független generátorrendszert **bázis**nak nevezünk. Ha M-nek van bázisa, akkor azt mondjuk, hogy M **szabad R-modulus**.

2.1.2. lemma. *Legyenek* $x, x_1, \dots, x_n \in M$.

a) $\langle x_1, \dots, x_n \rangle \leq_R M$.

b) $x \in \langle x_1, \dots, x_n \rangle \Leftrightarrow \langle x, x_1, \dots, x_n \rangle = \langle x_1, \dots, x_n \rangle$

c) $\{x_1, \dots, x_n\}$ *akkor és csak akkor bázisa* M*-nek, ha minden* $x \in M$ *egyértelműen felírható az* $x_1, \dots, x_n$ *elemek lineáris kombinációjaként.*

Bizonyítás. a) Legyen $x, y \in \langle x_1, \dots, x_n \rangle$, $x = a_1x_1 + \cdots + a_nx_n$, $y = b_1x_1 + \cdots + b_nx_n$, és legyen $a \in R$. Ekkor

$$x + y = (a_1 + b_1)x_1 + \cdots + (a_n + b_n)x_n \in \langle x_1, \dots, x_n \rangle,$$
$$ax = a_1x_1 + \cdots + a_nx_n \in \langle x_1, \dots, x_n \rangle.$$

b) Vegyük észre, hogy $\langle x_1, \dots, x_n \rangle \subseteq \langle x, x_1, \dots, x_n \rangle$. Fordítva, ha $x = a_1x_1 + \cdots + a_nx_n$ és $y = bx + b_1x_1 + \cdots + b_nx_n \in \langle x, x_1, \dots, x_n \rangle$, akkor $y = (a_1b + b_1)x_1 + \cdots + (a_nb + b_n)x_n \in \langle x_1, \dots, x_n \rangle$.

c) „$\Rightarrow$” Ha $\{x_1, \dots, x_n\}$ bázis, akkor minden $x \in M$ lineáris kombinációja $x_1, \dots, x_n$-nek. Feltételezzük, hogy

$$x = a_1x_1 + \cdots + a_nx_n = a_1'x_1 + \cdots + a_n'x_n.$$

Akkor $(a_1 - a_1')x_1 + \cdots + (a_n - a_n')x_n = 0$, és mivel $\{x_1, \dots, x_n\}$ lineárisan független, következik, hogy $a_i = a_i'$, $i = 1, \dots, n$.

„$\Leftarrow$” Elég igazolni, hogy $\{x_1, \dots, x_n\}$ lineárisan független rendszer. Valóban, ha

$$a_1x_1 + \cdots + a_nx_n = 0 = 0x_1 + \cdots + 0x_n,$$

akkor $a_i = 0,\ i = 1, \dots, n$. ■

2.1. feladat. $\mathbb{C}$ $\mathbb{R}$-feletti vektortér és $\{1, i\}$ bázisa.

2.2. feladat. $\{\vec{i}, \vec{j}\}$ bázisa a $\mathcal{V}_2$ $\mathbb{R}$-feletti vektortérnek, és $\{\vec{i}, \vec{j}, \vec{k}\}$ bázisa a $\mathcal{V}_3$ $\mathbb{R}$-feletti vektortérnek.

2.3. feladat. $\{1, X, \dots, X^n\}$ bázisa az $R_n[X]$ R-modulusnak. $R[X]$ nem végesen generált R-modulus.

2.4. feladat. R^n-ben tekintsük a következő elemeket:

$$\begin{aligned} e_1 &= (1, 0, 0, \dots, 0) \\ e_2 &= (0, 1, 0, \dots, 0) \\ e_3 &= (0, 0, 1, \dots, 0) \\ &\dots \\ e_n &= (0, 0, 0, \dots, 1) \end{aligned}$$

Akkor $e = \{e_1, \dots, e_n\}$ bázisa R^n-nek. e-t *kanonikus bázisnak* nevezzük.

2.5. feladat. Az üres halmaz lineárisan független és bázisa $\{0\}$-nak.

2.1.3. tétel. *Legyen V egy K-feletti vektortér.*
a) *$x_1 \in V$ lineárisan független $\Leftrightarrow x_1 \neq 0$.*
b) *Az $x_1, \dots, x_n \in V$ vektorok akkor és csak akkor összefüggők, ha létezik $i \in \{1, \dots, n\}$ úgy, hogy x_i felírható a többi vektor egy lineáris kombinációjaként.*
c) *Ha V végesen generált, akkor minden generátorrendszeréből kiválszatható egy bázis.*

Bizonyítás. a) Mivel $1 \cdot 0_V = 0_V$ és $1 \neq 0$, következik, hogy $\{0_V\}$ lineárisan összefüggő rendszer.
Ha $x_1 \neq 0$ és $a_1x_1 = 0$, akkor (1.2.b)-ből következik, hogy $a_1 = 0$.
b) Ha $a_1x_1 + \cdots + a_nx_n = 0$ és $a_i \neq 0$, akkor

$$x_i = a_i^{-1}a_1x_1 + \cdots + a_i^{-1}a_{i-1}x_{i-1} + a_i^{-1}a_{i+1}x_{i+1} + \cdots + a_i^{-1}a_nx_n.$$

Fordítva, ha $x_i = b_1x_1 + \cdots + b_{i-1}x_{i-1} + b_{i+1}x_{i+1} + \cdots + b_nx_n$, akkor

$$b_1x_1 + \cdots + b_{i-1}x_{i-1} + (-1)x_i + b_{i+1}x_{i+1} + \cdots + b_nx_n = 0,$$

és $-1 \neq 0$.
c) Feltételezhetjük, hogy $V \neq \{0\}$, és hogy az $X = \{x_1, \dots, x_n\}$ generátorrendszerben minden vektor nemnulla. n szerinti indukciót alkalmazunk.
Ha $n = 1$, akkor $X = \{x_1\}$ generátorrendszer, és a)-szerint lineárisan független, mert $x_1 \neq 0$.
Feltételezzük, hogy $n \geq 1$ és hogy az állítás igaz $n-1$-re, és legyen $X = \{x_1, \dots, x_n\}$ generátorrendszer. Két eset van:
(i) Ha létezik $i \in \{1, \dots, n\}$ úgy, hogy x_i lineáris kombinációja a többi vektornak, akkor b) szerint, $X' = X \setminus \{x_i\}$ generátorrendszer. Mivel X'-nek $n-1$ eleme van, X'-ből kiválasztható egy bázis, tehát X-ből is kiválasztható.
(ii) Ellenkező esetben b)-ből következik, hogy X lineárisan független, tehát X bázis. ■

2.6. feladat. Igazoljuk, hogy a következő rendszerek lineárisan függetlenek $\mathbb{R}^{\mathbb{R}}$-ben:
a) $\sin \lambda_1 t, , \dots, \sin \lambda_n t$, ahol $\lambda_1, \dots, \lambda_n \in \mathbb{R}_+^*$ különböző számok.
b) $1, \sin t, \dots, \sin nt, \cos t, \dots, \cos nt$, ahol $n \in \mathbb{N}^*$.

2.7. feladat. $\mathbb{Q}$-ban bármely két elem összefüggő $\mathbb{Z}$ felett, és $\mathbb{Q}$ nem végesen generált $\mathbb{Z}$-modulus.

2.8. feladat. Legyen $(S, \cdot)$ egy monoid, $\sigma_i : (S, \cdot) \to (K^*, \cdot)$ különböző homomorfizmusok, $i = 1, \dots, n$. Igazoljuk, hogy $\sigma_1, \dots, \sigma_n$ lineárisan függetlenek K^S-ben.

2.1.2. Szabad modulusok univerzális tulajdonsága

2.1.4. tétel. *Legyenek M és M' R-modulusok, $X = \{x_1, \dots, x_n\}$ bázisa M-nek, és $f : X \to M'$ egy függvény. Ekkor létezik egyetlen $\bar{f} : M \to M'$ lineáris függvény úgy, hogy az $\bar{f}$ leszükítése X-re megeggyezik f-el.*

Bizonyítás. Tételezzük fel, hogy $\bar{f}$ létezik. Ha $x \in M$, akkor léteznek az egyértelműen meghatárrozott $a_1, \dots a_n \in R$ skalárok úgy, hogy $x = a_1x_1 + \dots + a_nx_n$ Ekkor

$$\bar{f}(x) = \bar{f}(\sum_{i=1}^{n} a_ix_i) = \sum_{i=1}^{n} a_i\bar{f}(x_i) = \sum_{i=1}^{n} a_if(x_i),$$

tehát $\bar{f}$ egyértelműen van meghatározva.

Legyen most $\bar{f} : M \to M'$, $\bar{f}(x) = \sum_{i=1}^{n} a_if(x_i)$ ahol $x = a_1x_1 + \dots + a_nx_n \in M$. Igazoljuk, hogy $\bar{f}$ lineáris és $\bar{f}_{|X} = f$. Valóban, ha $x' = a'_1x_1 + \dots + a'_nx_n \in M$ és $a \in R$, akkor

$$\begin{aligned}
\bar{f}(x + x') &= \bar{f}(\sum_{i=1}^{n} (a_i + a'_i)x_i) = \sum_{i=1}^{n} (a_i + a'_i)f(x_i) \\
&= \sum_{i=1}^{n} a_if(x_i) + \sum_{i=1}^{n} a'_if(x_i) = \bar{f}(x) + \bar{f}(x'), \\
\bar{f}(ax) &= \bar{f}(a\sum_{i=1}^{n} a_ix_i) = \bar{f}(\sum_{i=1}^{n} aa_ix_i) \\
&= \sum_{i=1}^{n} aa_if(x_i) = a(\sum_{i=1}^{n} a_if(x_i)) = a\bar{f}(x).
\end{aligned}$$

Ha $x_i \in X$, akkor $x_i = 1 \cdot x_i$, tehát $\bar{f}(x_i) = 1 \cdot f(x_i) = f(x_i)$. ■

2.1.5. lemma. *Legyen $f : M \to M'$ egy R-lineáris függvény és $X = \{x_1, \dots, x_n\} \subseteq M$.*

a) *Ha X lineárisan független és f injektív, akkor $f(X) = \{f(x_1), \dots, f(x_n)\}$ is lineárisan független.*

b) *Ha $\langle X \rangle = M$ és f szürjektív, akkor $\langle f(X) \rangle = M'$*

c) *Ha X bázis és $f(X)$ független, akkor f injektív.*

d) *Ha X bázis és $\langle f(X) \rangle = M'$, akkor f injektív.*

e) *f akkor és csak akkor izomorfizmus, ha minden bázist egy bázisba visz át.*

Bizonyítás. a) Legyen $a_1, \dots, a_n \in R$ úgy, hogy $\sum_{i=1}^{n} a_if(x_i) = 0$; következik, hogy $f(\sum_{i=1}^{n} a_ix_i) = 0$, tehát $\sum_{i=1}^{n} a_ix_i = 0$, mivel f injektív, és $a_1 = \dots = a_n = 0$ mivel X lineárisan független.

b) Ha $x' \in M'$, akkor létezik $x \in M$ úgy, hogy $f(x) = x'$. Mivel $\langle X \rangle = M$, létezik $a_1, \dots, a_n \in R$ úgy, hogy $x = \sum_{i=1}^{n} a_ix_i$, es ekkor

$$x' = f(x) = f(\sum_{i=1}^{n} a_ix_i) = \sum_{i=1}^{n} a_if(x_i) \in \langle f(X) \rangle,$$

tehát $\langle f(X) \rangle = M'$.

c) Legyen $x \in M$ és tételezzük fel, hogy $f(x) = 0$. Mivel X bázis, léteznek az $a_1, \dots, a_n \in R$ skalárok úgy, hogy $x = \sum_{i=1}^{n} a_ix_i$. Mivel $0 = f(x) = \sum_{i=1}^{n} a_if(x_i)$ és $f(X)$ független, következik, hogy $a_1 = \dots = a_n = 0$, tehát $x = 0$, és f injektív.

d) Legyen $x' \in M'$. Mivel $\langle f(X) \rangle = M'$, következik, hogy léteznek az $a_1, \dots, a_n \in R$ skalárok úgy, hogy $x' = \sum_{i=1}^{n} a_if(x_i)$, tehát $x' = f(\sum_{i=1}^{n} a_ix_i)$ és f szürjektív.

e) az a), b), c) és d) pontokbol következik. ■

2.1.6. következmény. a) *A 2.1.4. Tételben*

- *$\bar{f}$ injektív $\Leftrightarrow$ $f(X)$ független.*
- *$\bar{f}$ szürjektív $\Leftrightarrow$ $\langle f(X) \rangle = M'$.*
- *$\bar{f}$ izomorfizmus $\Leftrightarrow$ $f(X)$ bázisa M'-nek.*

b) *Ma M szabad R-modulus és $M \simeq M'$, akkor M' is szabad.*

c) *Ha az M R-modulusnak van egy n-elemű X bázisa, akkor $M \simeq R^n$.*

Bizonyítás. a) a 2.1.5 Lemmából következik.

b) a 2.1.5. e)-ből következik.

c) Legyen $e = \{e_1, \dots, e_n\}$ az R^n R-modulus kanonikus bázisa, és legyen $f : X \to R^n$, $f(x_i) = e_i$, $i = 1, \dots, n$. Ekkor az a) pont szerint, $\bar{f}$ izomorfizmus. ■

2.1.3. Steinitz-tétel. Vektortér dimenziója

2.1.7. tétel. *Legyen* V *egy* K*-feletti vektortér,* $r, n \in \mathbb{N}^*$, $\{x_1, \dots, x_r\}$ *egy lineárisan független rendszer és legyen* $\{y_1, \dots, y_n\}$ *egy generátorrendszer. Ekkor* $r \leq n$*, és az* $y_1, \dots, y_n$ *vektorok közül* r *vektor kicserélhető az* $x_1, \dots, x_r$ *vektorokkal úgy, hogy*

$$\langle x_1, \dots, x_r, y_{r+1}, \dots, y_n \rangle = V.$$

Bizonyítás. r szerinti indukciót alkalmazunk. Ha $r = 1$, akkor $r \leq n$. Legyen $a_1, \dots, a_n \in K$ úgy, hogy $x_1 = a_1 y_1 + \dots + a_n y_n$. Mivel $x_1 \neq 0$, létezik i úgy, hogy $a_i \neq 0$; feltételezhetjük, hogy $a_1 \neq 0$. Ekkor

$$y_1 = a_1^{-1} x_1 - a_1^{-1} a_2 y_2 - \dots - a_1^{-1} a_n y_n$$

és $V = \langle y_1, y_2 \dots, y_n \rangle = \langle x_1, y_2 \dots, y_n \rangle$.

Feltételezzük, hogy az állítás igaz $(r-1)$-re és legyen $\{x_1, \dots, x_r\}$ egy lineárisan független rendszer. Akkor $\{x_1, \dots, x_{r-1}\}$ is lineárisan független. Az indukció hipotézisából következik, hogy $r - 1 \leq n$ és

$$V = \langle y_1, y_2 \dots, y_n \rangle = \langle x_1, \dots x_{r-1}, y_r \dots, y_n \rangle.$$

Ha $r - 1 = n$, akkor $V = \langle x_1, \dots, x_{r-1} \rangle$ és x_r függ $x_1, \dots, x_r$-től, ellentmondás, tehát $r - 1 < n$ és $r \leq n$. Mivel $x_r \in V = \langle x_1, \dots x_{r-1}, y_r \dots, y_n \rangle$, következik, hogy

$$x_r = b_1 x_1 + \dots + b_{r-1} x_{r-1} + b_r y_r + \dots + b_n y_n.$$

Mivel $x_1, \dots, x_r$ függetlenek, létezik i, $r \leq i \leq n$ úgy, hogy $b_i \neq 0$; feltételezhetjük, hogy $b_r \neq 0$. Ekkor

$$y_r = -a_r^{-1} b_1 x_1 - \dots - a_r^{-1} b_{r-1} x_{r-1} + a_r^{-1} x_r - a_r^{-1} b_{r+1} y_{r+1} - \dots - a_r^{-1} b_n y_n,$$

tehát $V = \langle y_1, y_2 \dots, y_n \rangle = \langle x_1, \dots x_r, y_{r+1} \dots, y_n \rangle$. ■

2.1.8. következmény. a) *Ha* $B, B' \subseteq V$ *bázisok, akkor* $|B| = |B'|$.

b) *Ha* V*-nek van egy* n*-elemű bázisa, akkor* $V \simeq K^n$.

2.1.9. definíció. Ha V-nek van egy n-elemű bázisa, akkor minden bázisának n eleme van. A bázis számosságát a V (K-feletti) *dimenziójának* nevezzük. Jelölés: $\dim_K V = n$.

Jegyezzük meg, hogy ha $\dim_K V = \dim_K V'$, akkor $V \simeq V'$.

2.1.10. következmény (alternatíva tételek). *Feltételezzük, hogy* $\dim_K V = n$.

a) *Ha* $B \subseteq V$ *és* $|B| = n$*, akkor a következő állítások ekvivalensek:*

1. B *bázis*
2. B *lineárisan független.*
3. B *generátorrendszer.*

b) *Ha* $f \in \mathrm{End}_K(V)$ *a következő állítások ekvivalensek:*

1. f *izomorfizmus*
2. f *injektív.*
3. f *szürjektív.*

Bizonyítás. a) Ha B független, akkor a Steinitz-tételből következik, hogy $|B| \leq \dim_K V$ és létezik egy bázis amely tartalmazza B-t. Mivel $|B| = n = \dim_K V$, következik, hogy B bázis.

Ha $\langle B \rangle = V$, akkor létezik egy B' bázis úgy, hogy $B' \subseteq B$. Mivel $|B'| = n$, következik, hogy $B' = B$, tehát B bázis.

b) Legyen B egy bázis. Ha f injektív, $|f(B)| = n$ és 2.1.5.a) szerint $f(B)$ független; a)-ból következik, hogy $f(B)$ bázis, es 2.1.5.d)-ből következik, hogy f szürjektív.

Ha f szürjektív, akkor 2.1.5.b) szerint $\langle f(B) \rangle = V$, és a) szerint $f(B)$ bázisa V-nek, tehát lineárisan független. 2.1.5.c)-ből következik, hogy f injektív. ■

2.9. feladat. a) Ha I véges halmaz, akkor $\dim_K K^I = |I|$.

b) $\dim_K M_{m,n}(K) = mn$.

c) $\dim_{\mathbb{R}} \mathcal{S}_n(\mathbb{R}) = \frac{n(n+1)}{2}$; $\dim_{\mathbb{R}} \mathcal{A}_n(\mathbb{R}) = \frac{n(n-1)}{2}$;

2.10. feladat. Ha $\dim_K U = m$ és $\dim_K V = n$, akkor $\dim_K U \times V = m + n$.

2.11. feladat. Legyen $f : U \to V$ egy K-homomorfizmus. Igazoljuk, hogy:

a) f akkor és csak akkor injektív, ha létezik $g \in \mathrm{Hom}_K(V, U)$ úgy, hogy $g \circ f = 1_U$.

b) f akkor és csak akkor szürjektív, ha létezik $g \in \mathrm{Hom}_K(V, U)$ úgy, hogy $f \circ g = 1_V$.

2.12. feladat. Legyen A egy véges dimenziós K-algebra (pl. $A = M_n(K)$). Igazoljuk, hogy $a \in A$ nem zérusosztó $\iff$ a invertáható A-ban .

2.1.4. Dimenzióra vonatkozó képletek

2.1.11. tétel. *Legyenek* V *és* V' K*-feletti vektorterek és* $f : V \to V'$ *egy lineáris függvény. Ekkor*

$$\dim_K V = \dim_K \operatorname{Ker} f + \dim_K \operatorname{Im} f.$$

Bizonyítás. Legyen $\{x_1, \dots, x_r\} \subset V$ bázisa $\operatorname{Ker} f$-nek, és legyen $\{x'_{r+1}, \dots, x'_n\} \subset V'$ bázisa $\operatorname{Im} f$-nek. Ekkor léteznek az $x_{r+1}, \dots, x_n \in V$ vektorok úgy, hogy $f(x_i) = x'_i$, $i = r+1, \dots, n$, és elég igazolni, hogy $\{x_1, \dots, x_r, x_{r+1}, \dots, x_n\}$ bázisa V-nek.

Feltételezzük, hogy $\sum_{i=1}^n a_i x_i = 0$. Ekkor

$$\begin{aligned} 0 &= f(\sum_{i=1}^n a_i x_i) = \sum_{i=1}^n a_i f(x_i) \\ &= \sum_{i=1}^r a_i f(x_i) + \sum_{i=r+1}^n a_i f(x_i) \\ &= \sum_{i=r+1}^n a_i x'_i; \end{aligned}$$

következik, hogy $a_{r+1} = \dots = a_n = 0$, $\sum_{i=1}^r a_i x_i = 0$, és végűl, $a_1 = \dots = a_r = 0$, tehát $\{x_1, \dots, x_r, x_{r+1}, \dots, x_n\}$ lineárisan független rendszer.

Ha $x' = f(x) \in \operatorname{Im} f$, akkor léteznek az $a_{r+1}, \dots, a_n \in K$ skalárok úgy, hogy

$$f(x) = x' = \sum_{i=r+1}^n a_i x'_i = \sum_{i=r+1}^n a_i f(x_i) = f(\sum_{i=r+1}^n a_i x_i);$$

következik, hogy $f(x - \sum_{i=r+1}^n a_i x_i) = 0$, és legyen $y = x - \sum_{i=r+1}^n a_i x_i$. Mivel $y \in \operatorname{Ker} f$, léteznek az $a_1, \dots, a_r \in K$ skalárok úgy, hogy $y = \sum_{i=1}^r a_i x_i$, tehát

$$x = y + \sum_{i=r+1}^n a_i x_i = \sum_{i=1}^n a_i x_i \in \langle x_1, \dots, x_n \rangle. \blacksquare$$

2.1.12. tétel. *Legyen egy* V K*-feletti vektortér és* $U, W \leq_K V$. *Ekkor*

$$\dim_K (U + W) = \dim_K U + \dim_K W - \dim_K (U \cap W).$$

Bizonyítás. Tekintsük az $U \times W = \{(u, w) \mid u \in U,\ w \in W\}$ vektorteret. Könnyű igazolni hogy, ha $\{u_1, \dots, u_n\}$ bázisa U-nak és $\{w_1, \dots, w_m\}$ bázisa W-nek, akkor $\{(u_1, 0), \dots, (u_n, 0), (0, w_1), \dots, (0, w_m)\}$ bázisa $U \times W$-nek, tehát $\dim_K (U \times W) = n + m$.

Legyen $f : U \times W \to U + W$, $f(u, w) = u + w$; ekkor f lineáris, szürjektív (azaz $\operatorname{Im} f = U + W$), és

$$\begin{aligned} \operatorname{Ker} f &= \{(u, w) \in U \times W \mid f(u, w) = 0\} \\ &= \{(u, w) \in U \times W \mid u + w = 0\} \\ &= \{(u, -u) \in U \times W \mid u \in U \cap W\}. \end{aligned}$$

Mivel $g : U \cap W \to \operatorname{Ker} f$, $g(u) = (u, -u)$ izomorfizmus, következik, hogy $\dim_K \operatorname{Ker} f = \dim_K (U \cap W)$, és végül,

$$\begin{aligned} \dim_K U + \dim_K W &= \dim_K (U \times W) \\ &= \dim_K \operatorname{Ker} f + \dim_K \operatorname{Im} f \\ &= \dim_K (U \cap W) + \dim_K (U + W). \blacksquare \end{aligned}$$

2.13. feladat. Legyen V egy K-feletti vektortér, $\dim_K V = n$, $S, T \leq_K V$. Igazoljuk, hogy:
a) Ha $\dim_K S = n - 1$ és $T \not\subseteq S$, akkor $S + T = V$ és $\dim_K (S \cap T) = \dim_K T - 1$.
b) Ha $\dim_K (S + T) = \dim_K (S \cap T) + 1$, akkor $S \subseteq T$ vagy $T \subseteq S$.

2.14. feladat. Legyen $\dim_K V = n$ és $f, g \in \operatorname{End}_K(V)$. Igazoljuk, hogy, ha $f \circ g = \theta$ és $f + g \in \operatorname{Aut}_K(V)$, akkor $\dim_K \operatorname{Im} f + \dim_K \operatorname{Im} g = n$.

2.15. feladat (Sylvester). Legyenek $f : U \to V$, $g : V \to W$ K-homomorfizmusok, $\dim_K U = m$, $\dim_K V = n$, $\dim_K W = p$. Igazoljuk, hogy $\dim_K \operatorname{Ker}(g \circ f) \leq \dim_K \operatorname{Ker} f + \dim_K \operatorname{Ker} g$.

2.1.5. Lineáris függvény mátrixa

Tudjuk, hogy, ha U és V R-modulusok, akkor $\mathrm{Hom}_R(U,V)$ R-modulus és $\mathrm{End}_R(U)$ R-algebra. Ha U és V szabad R-modulusok, akkor részletesebben vizsgálhatjuk a lineáris függvényeket.

Legyen $u = (u_1, \dots, u_n)$ U-nak egy bázisa és $v = (v_1, \dots, v_m)$ V-nek egy bázisa. (Figyelembe vesszük az elemek sorrendjét, azaz rendezett bázisokat tekintünk.)

Ha $x \in U$, akkor léteznek az egyértelműen meghatározott $x_1, \dots, x_n \in R$ skalárok, úgy, hogy $x = \sum_{i=1}^n x_i u_i$. Azt mondjuk, hogy $(x_1, \dots, x_n)$ az x vektor az u bázisra vonatkozó *koordinátavektora*, és legyen

$$M_u(x) = [x]_u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(R)$$

az x vektor az u *bázisra vonatkozó mátrixa.*

2.16. feladat. Igazoljuk, hogy:
a) $M_u : U \to M_{n,1}(R)$, $M_u(x) = [x]_u$ R-izomorfizmus;
b) $M_{n,1}(R) \simeq R^n$.

Legyen $f : U \to V$ egy lineáris függvény. A szabad modulusok univerzális tulajdonságából következik, hogy az $f(u_1), \dots, f(u_n) \in V$ elemek meghatározzák f-et. Legyen

$$f(u_j) = \sum_{i=1}^m a_{ij} v_i, \quad 1 \le j \le n.$$

Az $a_{ij} \in R$ skalárok egyértelműen meghatározottak, és legyen

$$M_{uv}(f) = [f]_{uv} = [a_{ij}]_{\substack{1 \le i \le m \\ 1 \le j \le n}} \in M_{m,n}(R)$$

az f függvény az (u, v) *bázispárra vonatkozó mátrixa.* Vegyük észre, hogy $[f(u_j)]_v$ egyenlő az $[f]_{uv}$ mátrix j-edik oszlopával.

Ha $A \in M_{m,n}(R)$, a következő jelöléseket fogjuk használni:
- o_j^A = az A mátrix j-edik oszlopa.
- s_i^A = az A mátrix i-edik sora.

2.1.13. tétel. *Legyenek U és V a fenti szabad R-modulusok, legyen W egy szabad R-modulus és $w = (w_1, \dots, w_p)$ W-nek egy bázisa. Továbbá, legyenek $f, f' \in \mathrm{Hom}_R(U,V)$ és $g \in \mathrm{Hom}_R(V,W)$.*
a) $[f(x)]_v = [f]_{uv}[x]_u$, *minden* $x \in U$ *esetén.*
b) $[f + f']_{uv} = [f]_{uv} + [f']_{uv}$
c) $[af]_{uv} = a[f]_{uv}$, *minden* $a \in R$ *esetén.*
d) $[g \circ f]_{uw} = [g]_{vw} \cdot [f]_{uv}$.

Bizonyítás. a) Legyen $y = f(x) = \sum_{i=1}^m y_i v_i$, tehát

$$[y]_v = [f(x)]_v = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}.$$

Ekkor

$$\sum_{i=1}^m y_i v_i = y = f(x) = f(\sum_{j=1}^n x_j u_j) = \sum_{j=1}^n x_j f(u_j)$$
$$= \sum_{j=1}^n x_j \sum_{i=1}^m a_{ij} v_i = \sum_{i=1}^m (\sum_{j=1}^n a_{ij} x_j) v_i.$$

Mivel $\{v_1, \dots, v_m\}$ bázis, következik, hogy

$$y_i = \sum_{j=1}^n a_{ij} x_j, \quad 1 \le i \le m,$$

vagy mátrixokkal,

$$[f(x)]_v = [f]_{uv}[x]_u.$$

b) Ki kell számítani az $(f+f')(u_j)$ koordinátáit, ha $1 \le j \le n$:

$$(f+f')(u_j) = f(u_j) + f'(u_j) = \sum_{i=1}^{m} a_{ij}v_i + \sum_{i=1}^{m} a'_{ij}v_i = \sum_{i=1}^{m}(a_{ij}+a'_{ij})v_i,$$

tehát

$$[f+f']_{uv} = [a_{ij}+a'_{ij}] = [a_{ij}] + [a'_{ij}] = [f]_{uv} + [f']_{uv}.$$

c) Hasonlómódon, minden $1 \le j \le n$ esetén,

$$(af)(u_j) = af(u_j) = a(\sum_{i=1}^{m} a_{ij}v_i) = \sum_{i=1}^{m}(aa_{ij})v_i,$$

tehát

$$[af]_{uv} = [aa_{ij}] = a[a_{ij}] = a[f]_{uv}.$$

d) Ha $1 \le j \le n$, legyen

$$(g \circ f)(u_j) = \sum_{k=1}^{p} c_{kj}w_k,$$

azaz

$$[g \circ f]_{u,w} = [c_{kj}]_{\substack{1\le k\le p\\ 1\le j\le n}} \in M_{p,n}(R).$$

Megismételve a fenti számításokat,

$$\begin{aligned}(g \circ f)(u_j) &= g(f(u_j)) = g(\sum_{i=1}^{m} a_{ij}v_i) = \sum_{i=1}^{m} a_{ij}g(v_i)\\ &= \sum_{i=1}^{m} a_{ij}\sum_{k=1}^{p} b_{ki}w_k = \sum_{k=1}^{p}(\sum_{i=1}^{m} b_{ki}a_{ij})w_k.\end{aligned}$$

Mivel $\{w_1,\dots,w_p\}$ W egy bázisa, következik, hogy

$$c_{kj} = \sum_{i=1}^{m} b_{ki}a_{ij}, \quad 1 \le k \le p,\ 1 \le j \le n,$$

és mátrixokkal,

$$[g \circ f]_{uw} = [c_{kj}] = [\sum_{i=1}^{m} b_{ki}a_{ij}] = [g]_{vw} \cdot [f]_{uv}. \qquad \blacksquare$$

2.1.14. következmény. a) $M_{u,v} : \mathrm{Hom}(U,V) \to M_{m,n}(R)$ R-*modulusizomorfizmus.*
b) $M_{v,v} : \mathrm{End}_R(V) \to M_n(R)$ R-*algebraizomorfizmus.*

Bizonyítás. A szabad modulusok univerzális tulajdonságából következik, hogy $M_{u,v}$ jól értelmezett és bijektív, és az előző tételből következik, hogy izomorfizmus. ■

2.17. feladat. Ha $\dim_K U = m$ és $\dim_K V = n$, akkor $\dim_K \mathrm{Hom}_K(U,V) = mn$.

2.18. feladat. Legyen $t \in \mathbb{R}$, $f_t, g_t : \mathbb{R}^2 \to \mathbb{R}^2$, $f_t(x) = (x_1\cos t - x_2\sin t, x_1\sin t + x_2\cos t)$, $g_t(x) = (x_2\cos t + x_2\sin t, x_1\sin t - x_2\cos t)$.
a) Igazoljuk, hogy f_t, $g_t \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^2)$.
b) Határozzuk meg az $[f_t]_{e,e}$ és $[g_t]_{e,e}$ mátrixokat, ahol $e = (e_1, e_2)$ a kanonikus bázis.
c) Határozzuk meg az $f_t \circ f_{t'}$, $g_t \circ g_{t'}$, $f_t \circ g_{t'}$, $g_t \circ f_{t'}$ morfizmusok mátrixát.

2.19. feladat. Legyen $V = \mathbb{R}_n[X] = \{f \in \mathbb{R}[X] \mid gr(f) \le n\}$, $a \in \mathbb{R}$, $f \in \mathbb{R}[X]$ és legyen $B = (1, X-a, \dots, (X-a)^n/n!)$.
a) Igazoljuk, hogy B bázisa V-nek.
b) Határozzuk meg az f koordinátáit a B bázisban (**Taylor-képlet**).
c) Legyen $D : V \to V$, $D(f) = f'$. Határozzuk meg a D mátrixát a kanonikus bázisban.

2.20. feladat. Igazoljuk, hogy:
a) $\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2, +) = \mathrm{Aut}_{\mathbb{Z}_2}(\mathbb{Z}_2 \times \mathbb{Z}_2)$.
b) $(\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2, +), \circ) \simeq (S_3, \circ)$.

2.21. feladat. Határozzuk meg a $(\mathbb{Z} \times \mathbb{Z}, +)$ csoport automorfizmusait.

2.1.6. Báziscsere

Legyen U egy szabad R-modulus, és $u = (u_1, \dots, u_n)$ egy bázisa. Ha $u' = (u'_1, \dots, u'_n)$ egy elemrendszer, $u'_j \in U$, akkor léteznek az egyértelműen meghatározott $t_{ij} \in R$ skalárok úgy, hogy

$$u'_j = \sum_{i=1}^{n} t_{ij} u_i, \quad 1 \le j \le n,$$

azaz,

$$[u'_j]_u = \begin{pmatrix} t_{1j} \\ \vdots \\ t_{nj} \end{pmatrix} = o_j^T,$$

ahol

$$T = T_u^{u'} = [t_{ij}]_{1 \le i,j \le n} \in M_n(R).$$

Azt mondjuk, hogy $T = T_u^{u'}$ *az* u *bázisról az* u' *rendszerre való áttérési mátrix.*

2.1.15. tétel. a) $u' = (u'_1, \dots, u'_n)$ *bázis* $\Leftrightarrow$ $T = T_u^{u'}$ *invertálható mátrix.* (Informálisan, u a „régi" bázis és u' az „új"bázis.)

b) *Ha* u' *bázis, akkor minden* $x \in U$ *esetén*

$$\boxed{[x]_{u'} = (T_u^{u'})^{-1}[x]_u}.$$

c) *Legyen* V *egy szabad modulus,* $v = (v_1, \dots, v_m)$ *és* $v' = (v'_1, \dots, v'_m)$ *két bázisa, és legyen*

$$S = T_v^{v'} = [s_{ij}]_{1 \le i,j \le m} \in M_m(R)$$

az áttérési mátrix, ahol

$$v'_j = \sum_{i=1}^{m} s_{ij} v_i, \quad 1 \le j \le m.$$

Ha $f : U \to V$ *egy lineáris függvény, akkor*

$$\boxed{[f]_{u',v'} = S^{-1}[f]_{u,v}T}.$$

Bizonyítás. a) A szabad modulusok univerzális tulajdonságából következik, hogy létezik egy egyértelműen meghatározott $h : U \to V$ lineáris függvény úgy, hogy $h(u_j) = u'_j$, $1 \le j \le n$, és vegyük észre, hogy $[h]_{u,u} = T$. A 2.1.5. Lemmából és 2.1.14.-ből következik, hogy $u' = (h(u_1), \dots, h(u_n))$ bázis $\Leftrightarrow$ h izomorfizmus $\Leftrightarrow$ $T = [h]_{u,u} \in M_n(R)$ invertálható mátrix.

b) Legyen $x = \sum_{i=1}^{n} x_i u_i = \sum_{j=1}^{n} x'_j u'_j \in U$. Ekkor

$$\begin{aligned} x &= \sum_{j=1}^{n} x'_j u'_j = \sum_{j=1}^{n} x'_j \sum_{i=1}^{n} t_{ij} u_i \\ &= \sum_{i=1}^{n} (\sum_{j=1}^{n} t_{ij} x'_j) u_i = \sum_{i=1}^{n} x_i u_i. \end{aligned}$$

Mivel $u = \{u_1, \dots, u_n\}$ bázis, következik, hogy

$$x_i = \sum_{j=1}^{n} t_{ij} x'_j, \quad 1 \le i \le n,$$

azaz,

$$[x]_u = T[x]_{u'}.$$

c) Kétféleképpen kiszámítva az $[f(x)]_v$ mátrixot, kapjuk, hogy

$$[f(x)]_v = [f]_{u,v}[x]_u = [f]_{u,v}T[x]_{u'},$$

és

$$[f(x)]_v = S[f(x)]_{v'} = S[f]_{u',v'}[x]_{u'}.$$

Rendre behelyetesítve $[x]_{u'}$-et az $\begin{pmatrix}1\\0\\\vdots\\0\end{pmatrix}, \begin{pmatrix}0\\1\\\vdots\\0\end{pmatrix}, \dots, \begin{pmatrix}0\\0\\\vdots\\1\end{pmatrix} \in M_{m,1}(R)$ mátrixokkal, következik, hogy $[f]_{u,v}T = S[f]_{u',v'}$, tehát

$$[f]_{u',v'} = S^{-1}[f]_{u,v}T. \qquad \blacksquare$$

2.2. Determinánsok és mátrixok

2.2.1. A determináns értelmezése

A. Másod és harmad rendű determinánsok

Legyen R egy kommutatív gyűrű, és tekintsük a következő egyenletrendszert:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1 \\ a_{21}x_1 + a_{22}x_2 = b_2. \end{cases}$$

Legyen $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in M_2(R)$ az *egyenletrendszer mátrixa* és $B = \begin{pmatrix} b_1 \\ b_2 \end{pmatrix} \in M_{21}(R)$ a *szabad tagok oszlopmátrixa.*

Alkalmazva a kiküszöbölési módszert, kapjuk, hogy az egyenletrendszer ekvivalens a következő egyenletrendszerrel:

$$\begin{cases} (a_{11}a_{22} - a_{12}a_{21})x_1 = b_1a_{22} - a_{12}b_2 \\ (a_{11}a_{22} - a_{12}a_{21})x_2 = b_2a_{22} - a_{21}b_1. \end{cases}$$

Definíció szerint, legyen

$$\det A = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} = a_{11}a_{22} - a_{12}a_{21} \in R$$

as A mátrix *determinánsa.*

Vegyük észre, hogy ha $A_1 = \begin{pmatrix} b_1 & a_{12} \\ b_2 & a_{22} \end{pmatrix}$ és $A_2 = \begin{pmatrix} a_{11} & b_1 \\ a_{21} & b_2 \end{pmatrix}$, akkor

$$x_1 \det A = \det A_1, \quad x_2 \det A = \det A_2.$$

Tekintsük most a következő egyenletrendszert:

$$\begin{cases} a_{11}x_1 + a_{12}x_2 + a_{13}x_3 = b_1 \\ a_{21}x_1 + a_{22}x_2 + a_{23}x_3 = b_2 \\ a_{31}x_1 + a_{32}x_2 + a_{33}x_3 = b_3, \end{cases}$$

és legyenek $A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$, $A_1 = \begin{pmatrix} b_1 & a_{12} & a_{13} \\ b_2 & a_{22} & a_{23} \\ b_3 & a_{32} & a_{33} \end{pmatrix}$, $A_2 = \begin{pmatrix} a_{11} & b_1 & a_{13} \\ a_{21} & b_2 & a_{23} \\ a_{31} & b_3 & a_{33} \end{pmatrix}$

és $A_3 = \begin{pmatrix} a_{11} & a_{12} & b_1 \\ a_{21} & a_{22} & b_2 \\ a_{31} & a_{32} & b_3 \end{pmatrix} \in M_3(R)$. Hasonló módon kapjuk a következő ekvivalens egyenletrendszert:

$$x_1 \det A = \det A_1, \quad x_2 \det A = \det A_2. \quad x_3 \det A = \det A_3,$$

ahol definíció szerint,

$$\det A = \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{vmatrix}$$
$$= a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{11}a_{23}a_{32} - a_{13}a_{22}a_{31} - a_{12}a_{21}a_{33}$$

2.22. feladat. Számítsuk ki a következő determinánsokat:

a) $\begin{vmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{vmatrix}$; b) $\begin{vmatrix} a & b & c \\ b & c & a \\ c & a & b \end{vmatrix}$; c) $\begin{vmatrix} 1 & 1 & 1 \\ a & b & c \\ a^2 & b^2 & c^2 \end{vmatrix}$.

B. n-ed rendű determináns

A fenti számításokat folytatni bonyolult lenne, de szugerálják a következő általánosítást:

2.2.1. definíció. Ha $A = [a_{ij}] \in M_n(R)$, akkor az A mátrix **determinánsa**nak nevezzük a következő R-beli elemet:

$$\det A = \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma(1)} a_{2\sigma(2)} \dots a_{n\sigma(n)}.$$

Az összegnek $n!$ tagja van, és mindegyik szorzat tartalmaz az A mátrix minden sorából és minden oszlopából pontosan egy elemet.

2.2.2. lemma. $\det A = \det A^t$.

Bizonyítás. Legyen $A^t = [a^t_{ij}] \in M_n(R)$ az A mátrix transzponáltja, ahol $a^t_{ij} = a_{ji}$, $1 \le i, j \le n$. Ekkor

$$\begin{aligned} \det A^t &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a^t_{1\sigma(1)} a^t_{2\sigma(2)} \dots a^t_{n\sigma(n)} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{\sigma(1)1} a_{\sigma(2)2} \dots a_{\sigma(n)n} \\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma) a_{1\sigma^{-1}(1)} a_{2\sigma^{-1}(2)} \dots a_{n\sigma^{-1}(n)} \\ &= \sum_{\tau \in S_n} \operatorname{sgn}(\tau) a_{1\tau(1)} a_{2\tau(2)} \dots a_{n\tau(n)} \\ &= \det A. \end{aligned}$$

Az utolsó előtti egyelőségben felhasználtuk az R kommutatívitását és a következő tényeket:

- Az $S_n \to S_n$, $\sigma \mapsto \tau = \sigma^{-1}$ bijektív függvény;
- $\operatorname{sgn}(\sigma) = \operatorname{sgn}(\sigma^{-1})$. ■

2.2.2. A determináns induktív értelmezése

A. Multilineáris alakok

Legyen R egy kommutatív gyűrű, M, N R-modulusok és legyen $M^n = M \times \dots \times M$.

2.2.3. definíció. a) A $\phi : M^n \to N$ függvényt n-*lineárisnak* nevezzük, ha

$$\phi(x_1, \dots, ax_i + a'x'_i, \dots, x_n) = a\phi(x_1, \dots, x_i, \dots, x_n) + a'\phi(x_1, \dots, x'_i, \dots, x_n)$$

minden $a, a' \in R$ és $x_1, \dots, x_i, x'_i, \dots, x_n \in M$ esetén (azaz, ϕ minden változójában lineáris).

Ha $N = R$, akkor ϕ-t *alaknak* nevezzük.

b) Azt mondjuk, hogy $\phi : M^n \to R$ *alternáló alak*, ha

$$x_i = x_{i+1} \;\Rightarrow\; \phi(x_1, \dots, x_i, x_{i+i}, \dots, x_n) = 0$$

minden $i \in \{1, \dots, n-1\}$ esetén.

2.2.4. példa. a) Minden $\phi \in \operatorname{Hom}_R(M, N)$ 1-lineáris függvény.

b) Ha A egy R-algebra, akkor

$$\phi : A \to A, \quad \phi(x_1, \dots, x_n) = x_1 \dots x_n$$

n-lineáris függvény.

c) Legyen $M = M_{2,1}(R)$, $n = 2$, $x_1 = \begin{pmatrix} a_{11} \\ a_{21} \end{pmatrix}$ és $x_2 = \begin{pmatrix} a_{12} \\ a_{22} \end{pmatrix}$. Ekkor

$$\phi : M \times M \to R, \quad \phi(x_1, x_2) = a_{11}a_{22} - a_{21}a_{12}$$

2-lineáris alternáló alak.

2.2.5. lemma. *Legyen* $\phi : M^n \to R$ *egy* n*-lineáris alternáló alak.*
a) *Ha* $i < j$*, akkor* $\phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\phi(x_1, \dots, x_j, \dots, x_i, \dots, x_n)$;
b) *Ha* $i \neq j$ *és* $x_i = x_j$*, akkor* $\phi(x_1, \dots, x_n) = 0$*;*
c) *Ha* $i \neq j$ *és* $a \in R$*, akkor* $\phi(x_1, \dots, x_i + ax_j, \dots, x_n) = \phi(x_1, \dots, x_i, \dots, x_n)$.

Bizonyítás. a) Legyen $k = j - i$; k-szerinti indukciót alkalmazunk. Ha $k = 1$, akkor

$$\begin{aligned}\phi(\dots, x_i + x_{i+1}, x_i + x_{i+1}, \dots) &= \phi(\dots, x_i, x_i, \dots) + \phi(\dots, x_i, x_{i+1}, \dots)\\ &\quad + \phi(\dots, x_{i+1}, x_i, \dots) + \phi(\dots, x_{i+1}, x_{i+1}, \dots)\\ &= \phi(\dots, x_i, x_{i+1}, \dots) + \phi(\dots, x_{i+1}, x_i, \dots),\end{aligned}$$

tehát

$$\phi(x_1, \dots, x_i, x_{i+1}, \dots, x_n) = -\phi(x_1, \dots, x_{i+1}, x_i, \dots, x_n).$$

Legyen $k > 1$, és feltételezzük, hogy az állítás igaz $k-1$-re. Felcsréljük x_i-t x_{i+k}-val három lépésben: felcseréljük x_i-t x_{i+k-1}-gyel, utánna x_{i+k}-t x_i-vel, és végűl x_{i+k-1}-et x_{i+k}-val. Az indukció hipotézisából és a $k = 1$ esetből következik, hogy ϕ háromszor vált előjelet, tehát

$$\phi(x_1, \dots, x_i, \dots, x_{i+k}, \dots, x_n) = -\phi(x_1, \dots, x_{i+k}, \dots, x_i, \dots, x_n).$$

b) Feltételezhetjük, hogy $k = j - i > 1$; ekkor

$$\phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n) = -\phi(x_1, \dots, x_{j-1}, \dots, x_i, x_j, \dots, x_n) = -0 = 0.$$

c) Az $i < j$ esetet vizsgálva,

$$\begin{aligned}\phi(\dots, x_i + ax_j, \dots, x_j, \dots) &= \phi(\dots, x_i, \dots, x_j, \dots) + a\phi(\dots, x_j, \dots, x_j, \dots)\\ &= \phi(x_1, \dots, x_i, \dots, x_j, \dots, x_n). \qquad \blacksquare\end{aligned}$$

2.2.6. lemma. *Legyen* $\phi : M^n \to R$ *egy* n*-lineáris alternáló alak,* $A = [a_{ij}] \in M_n(R)$*,* $x_1, \dots, x_n \in R$*, és legyenek*

$$y_j = \sum_{i=1}^{n} a_{ij}x_i, \quad 1 \le j \le n,$$
$$z_i = \sum_{j=1}^{n} a_{ij}x_j, \quad 1 \le i \le n.$$

Ekkor

$$\phi(y_1, \dots, y_n) = \phi(z_1, \dots, z_n) = \det(A)\phi(x_1, \dots, x_n).$$

Bizonyítás. Mivel ϕ n-lineáris, következik, hogy

$$\begin{aligned}\phi(z_1, \dots, z_n) &= \phi(\sum_{j=1}^{n} a_{1j}x_j, \dots, \sum_{j=1}^{n} a_{nj}x_j) =\\ &= \sum_{1 \le i_1 \le \dots \le i_n \le n} a_{1i_1} \dots a_{ni_n}\phi(x_{i_1}, \dots, x_{i_n}).\end{aligned}$$

Legyen $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$, $\sigma(k) = i_k$; ha σ injektív, akkor σ bijektív, tehát $\sigma \in S_n$; ha σ nem injektív, akkor $\phi(x_{i_1}, \dots, x_{i_n}) = 0$, mert ϕ alternáló.

Következik, hogy

$$\begin{aligned}\phi(z_1, \dots, z_n) &= \sum_{\sigma \in S_n} a_{1\sigma(1)} \dots a_{n\sigma(n)}\phi(x_{\sigma(1)}, \dots, x_{\sigma(n)}) =\\ &= \sum_{\sigma \in S_n} \operatorname{sgn}(\sigma)a_{1\sigma(1)}a_{2\sigma(2)} \dots a_{n\sigma(n)}\phi(x_{i_1}, \dots, x_{i_n}) =\\ &= \det(A)\phi(x_1, \dots, x_n)\end{aligned}$$

Vegyük észre, hogy

$$y_i = \sum_{j=1}^{n} a_{ji}x_j = \sum_{j=1}^{n} a^t_{ij}x_j,$$

tehát a második egyenlőség következik az elsőből, és abból, hogy $\det A = \det A^t$. $\blacksquare$

B. Determinánsok alaptétele

Ha $A = [a_{ij}] \in M_n(R)$, és $M := M_{n,1}(R)$ akkor legyen

- $o_j^A = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{nj} \end{pmatrix} \in M$ az A j-edik oszlopa, $1 \le j \le n$;
- $s_i^A = \begin{pmatrix} a_{i1} \dots a_{1n} \end{pmatrix} \in M_{1,n}(R) \simeq M$ az A i-edik sora, $1 \le i \le n$.

Vegyük észre, hogy ha $I = I_n := [\delta_{ij}] \in M_n(R)$ az n-ed rendű egységmátrix, akkor $(e_1 = o_1^I, \dots, e_n = o_n^I)$ az M kanonikus bázisa.

2.2.7. tétel. *Létezik az egyértelműen meghatározott $\delta_n : M^n \to R$ n-lineáris alternáló alak úgy, hogy*

$$\delta_n(e_1, \dots, e_n) = 1.$$

Minden $A \in M_n(R)$ esetén,

$$\det(A) = \delta_n(o_1^A, \dots, o_n^A).$$

Bizonyítás. Feltételezzük, hogy létezik egy $\delta_n : M^n \to R$ n-lineáris alternáló alak úgy, hogy $\delta_n(e_1, \dots, e_n) = 1$. Legyen $x_1, \dots, x_n \in M$,

$$x_j = \sum_{i=1}^{n} a_{ij} e_i, \quad 1 \le j \le n$$

és legyen $A = [a_{ij}]$, azaz $o_j^A = x_j$. A 2.2.6. lemmából következik, hogy

$$\delta_n(x_1, \dots, x_n) = \det(A)\delta_n(e_1, \dots, e_n) = \det(A),$$

tehát bebizonyítottuk az *egyértelműséget* és az utolsó állítást.

A δ_n *létezését* n-szerinti indukcióval bizonyítjuk. Ha $n = 2$, akkor 2.2.4.c)-ből következik, hogy δ_2 létezik.

Feltételezzük, hogy δ_{n-1} létezik, és megszerkesszük δ_n-et. Legyen $A = [a_{ij}] \in M_n(R)$, $x_j = o_j^A$, és legyen A_{ij} az az $(n-1)$-ed rendű mátrix amit A-ból kapunk az i-edik sorának és a j-edik oszlopának elhagyásával.

Ha $1 \le i \le n$ rögzített, legyen

$$\delta_n(o_1^A, \dots, o_n^A) = \sum_{j=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}).$$

Igazoljuk hogy $(-1)^{i+j} a_{ij} \det(A_{ij})$ lineárisan függ x_k-tól, ahol $x_k = o_k^A$, $1 \le k \le n$. Tudjuk, hogy δ_{n-1} létezik és

$$\det(A_{ij}) = \delta_{n-1}(o_1^{A_{ij}}, \dots, o_{n-1}^{A_{ij}}).$$

Ha $j = k$, akkor $\det(A_{ij})$ nem függ x_k-tól (mert o_k^A-t elhagytuk), de $a_{ij} = a_{ik}$ R-lineárisan függ x_k-tól. Ha $j \ne k$, akkor $\det(A_{ij})$ lineárisan függ x_k-tól mert δ_{n-1} multilineáris, és a_{ij} nem függ x_k-tól.

Következik, hogy δ_n n-lineáris, és nyilvánvaló, hogy $\delta_n(e_1, \dots, e_n) = \delta_{ii} \det(I_{n-1}) = 1$. Igazoljuk, hogy δ_n alternáló.

Feltételezzük, hogy $x_k = x_{k+1}$, tehát $o_k^A = o_{k+1}^A$. Ekkor $A_{ik} = A_{i\,k+1}$, $a_{ik} = a_{i\,k+1}$, és ha $j \ne k$ és $j \ne k+1$, akkor A_{ij}-nek van két egyenlő oszlopa, tehát $\det(A_{ij}) = 0$; következik, hogy

$$\delta_n(o_1^A, \dots, o_n^A) = (-1)^{i+k} a_{ik} \det(A_{ik}) + (-1)^{i+k+1} a_{i\,k+1} \det(A_{i\,k+1}) = 0. \qquad \blacksquare$$

2.2.8. definíció. a) $\det : M_n(R) \to R, \quad A \mapsto \det(A)$ függvényt n-ed *rendű determinánsnak* nevezzük.

b) A $\Gamma_{ij} = (-1)^{i+j} \det(A_{ij}) \in R$ elem az a_{ij} elem *algebrai komplementuma.*

c) Azt mondjuk, hogy a

$$\det(A) = \sum_{j=1}^{n} a_{ij} \Gamma_{ij}$$

képlet az A determinánsának az i-edik *sora szerinti kifejtése*, $1 \le i \le n$.

2.2.9. következmény (Determinánsok alaptulajdonságai). a) *Az A determinánsa lineárisan függ az A oszlopaitól.*

b) *Ha A-nak van két egyenlő oszlopa, akkor* $\det(A) = 0$.

c) *Ha A két oszlopát felcsréljük, akkor a determinánsa (-1)-szeresére változik.*

d) *Az* A *determinánsa nem változik, ha egy oszlopának skalárszorosát egy másik oszlopához adjuk.*
e) *Mivel* $\det(A) = \det(A^t)$, *a fenti állítások sorokra is igazak.*
f) $\det(A)$ j*-edik oszlopa szerinti kifejtése:*

$$\det(A) = \sum_{i=1}^{n} (-1)^{i+j} a_{ij} \det(A_{ij}), \quad 1 \le j \le n.$$

2.23. feladat. Számítsuk ki a következő determinansokat:

$$\text{a)} \begin{vmatrix} 0 & a & b & c \\ -a & 0 & d & e \\ -b & -d & 0 & f \\ -c & -e & -f & 0 \end{vmatrix}; \quad \text{b)} \begin{vmatrix} a+b & b+c & c+a \\ a^2+b^2 & b^2+c^2 & c^2+a^2 \\ a^3+c^3 & b^3+c^3 & c^3+a^3 \end{vmatrix}; \quad \text{c)} \begin{vmatrix} 1 & 1 & 1 & 1 \\ a & b & c & d \\ a^2 & b^2 & c^2 & d^2 \\ a^3 & b^3 & c^3 & d^3 \end{vmatrix}.$$

2.24. feladat. a) Számítsuk ki az $A = (a_{ij}) \in M_n(K)$ determinánsát, ha $a_{ij} = 0,\ i > j$.
b) Számítsuk ki az $A = (a_{ij}) \in M_n(K)$ determinánsát, ha $a_{ij} = 0,\ i + j \le n$.

2.25. feladat. Számítsuk ki a következő determinánsokat:

$$\text{a) } A_n = \begin{vmatrix} a & x & x & \dots & x \\ x & a & x & \dots & x \\ x & x & a & \dots & x \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ x & x & x & \dots & a \end{vmatrix} \qquad \text{b) } D_n = \begin{vmatrix} a & b & 0 & 0 & \dots & 0 & 0 \\ c & a & b & 0 & \dots & 0 & 0 \\ 0 & c & a & b & \dots & 0 & 0 \\ 0 & 0 & c & a & \dots & 0 & 0 \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & 0 & \dots & a & b \\ 0 & 0 & 0 & 0 & \dots & c & a \end{vmatrix}$$

$$\text{c) } B_n = \begin{vmatrix} x & y & y & y & \dots & y & y \\ z & x & y & y & \dots & y & y \\ z & z & x & y & \dots & y & y \\ z & z & z & x & \dots & y & y \\ \vdots & \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ z & z & z & z & \dots & x & y \\ z & z & z & z & \dots & z & x \end{vmatrix} \qquad \text{d) } V_n = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_1^{n-1} & a_2^{n-1} & a_3^{n-1} & \dots & a_n^{n-1} \end{vmatrix}$$

$$\text{e) } S_n = \begin{vmatrix} 0 & a_{12} & a_{13} & \dots & a_{1n} \\ -a_{12} & 0 & a_{23} & \dots & a_{2n} \\ -a_{13} & -a_{23} & 0 & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -a_{1n} & -a_{2n} & -a_{3n} & \dots & 0 \end{vmatrix} \quad (S_n\text{-nél } n \text{ páratlan}).$$

2.26. feladat. Igazoljuk, hogy:

$$V_n^i(a_1, \dots, a_n) = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 \\ a_1 & a_2 & a_3 & \dots & a_n \\ a_1^2 & a_2^2 & a_3^2 & \dots & a_n^2 \\ \dots & & & \dots & \\ a_1^{i-1} & a_2^{i-1} & a_3^{i-1} & \dots & a_n^{i-1} \\ a_1^{i+1} & a_2^{i+1} & a_3^{i+1} & \dots & a_n^{i+1} \\ \dots & & & \dots & \\ a_1^n & a_2^n & a_3^n & \dots & a_n^n \end{vmatrix} = s_{n-i}(a_1, \dots, a_n) V_n,$$

ahol

$$s_k = X_1 \dots X_k + \dots + X_{n-k+1} \dots X_n$$

a k-adik elemi szimmetrikus polinom és $V_n = V_n(a_1, \dots, a_n)$ a **Vandermonde-determináns**.

2.2.3. Determinánsok tulajdonságai. Invertálható mátrixok

2.2.10. tétel (Cramer-szabály). *Ha* $A \in M_n(R)$ *és* $b = \sum_{j=1}^{n} x_j o_j^A \in M_{n,1}(R)$, *akkor*

$$\delta_n(o_1^A, \dots, \underset{i}{b}, \dots, o_n^A) = x_i \det(A).$$

Bizonyítás. Mivel δ_n n-lineáris alternáló, következik, hogy

$$\begin{aligned}\delta_n(o_1^A,\dots,b,\dots,o_n^A) &= \delta_n(o_1^A,\dots,\sum_{j=1}^n x_j o_j^A,\dots,o_n^A)\\ &= \sum_{j=1}^n x_j\delta_n(o_1^A,\dots,o_j^A,\dots,o_n^A)\\ &= x_i\delta_n(o_1^A,\dots,o_i^A,\dots,o_n^A)\\ &= x_i\det(A). \qquad \blacksquare\end{aligned}$$

2.2.11. tétel (Determinánsok szorzástétele). *Ha* $A, B \in M_n(R)$*, akkor*

$$\det(AB) = \det(A)\det(B).$$

Bizonyítás. Legyen $(e_1,\dots,e_n)$ az $M = M_{n,1}(R)$ kanonikus bázisa. Az $x_j = \sum_{i=1}^n a_{ij}e_i$, $1 \le j \le n$ összefüggéseket a mátrix formában írva:

$$\begin{pmatrix} x_1\\ \vdots\\ x_n\end{pmatrix} = A\begin{pmatrix} e_1\\ \vdots\\ e_n\end{pmatrix}.$$

Ebben az esetben, a 2.2.6. Lemmából következik, hogy

$$\delta_n(x_1,\dots,x_n) = \det(A)\delta_n(e_1,\dots,e_n) = \det(A).$$

Vegyük észre, hogy

$$\begin{pmatrix} z_1\\ \vdots\\ z_n\end{pmatrix} := (AB)\begin{pmatrix} e_1\\ \vdots\\ e_n\end{pmatrix} = A(B\begin{pmatrix} e_1\\ \vdots\\ e_n\end{pmatrix}) \text{ és legyen } B\begin{pmatrix} e_1\\ \vdots\\ e_n\end{pmatrix} =: \begin{pmatrix} y_1\\ \vdots\\ y_n\end{pmatrix}.$$

Ekkor

$$\begin{aligned}\det(AB) &= \det(AB)\delta_n(e_1,\dots,e_n) = \delta_n(z_1,\dots,z_n) =\\ &= \det(A)\delta_n(y_1,\dots,y_n)\\ &= \det(A)\det(B)\delta_n(e_1,\dots,e_n)\\ &= \det(A)\det(B). \qquad \blacksquare\end{aligned}$$

2.2.12. tétel (Adjungált mátrix). *Legyen* $A = [a_{ij}] \in M_n(R)$ *és legyen* $\tilde{A} = [\tilde{a}_{ij}] \in M_n(R)$*, ahol*

$$\tilde{a}_{ij} = \Gamma_{ji} = (-1)^{i+j}\det A_{ji}.$$

$\tilde{A}$*-t az* A *adjungáltjának nevezzük, és fennáll a következő egyenlőség:*

$$A\tilde{A} = \tilde{A}A = \det(A)\cdot I_n.$$

Bizonyítás. Mivel $A\tilde{A} = [\sum_{k=1}^n a_{ik}\tilde{a}_{kj}]_{1\le i,j\le n}$ és $\tilde{A}A = [\sum_{k=1}^n \tilde{a}_{ik}a_{kj}]_{1\le i,j\le n}$, igazolni kell, hogy

$$\sum_{k=1}^n a_{ik}\Gamma_{jk} = \delta_{ij}\det(A) \quad \text{és} \quad \sum_{k=1}^n a_{kj}\Gamma_{ki} = \delta_{ij}\det(A),$$

ahol δ_{ij} a Kronecker szimbólum.

Bizonyítsuk be az első egyenlőséget. Ha $i = j$, akkor valóban $\sum_{k=1}^n a_{ik}\Gamma_{ik} = \det(A)$ (i-edik sor szerinti kifejtés). Feltételezzük, hogy $i \ne j$ és legyen $A' = [a'_{ij}] \in M_n(R)$ úgy, hogy $s_l^{A'} = s_l^A$ ha $j \ne i$, és $s_i^{A'} = s_j^A$. Mivel A'-nek van két egyenlő sora, következik, hogy

$$0 = \det A' = \sum_{k=1}^n a'_{ik}\Gamma'_{ik} = \sum_{k=1}^n a_{jk}\Gamma_{ik}. \qquad \blacksquare$$

2.27. feladat. Ha $A \in T_n(K)$ akkor $\tilde{A} = (\Gamma_{ji}) \in T_n(K)$.

2.2.13. tétel (Invertáható mátrixok). *Ha* $A = [a_{ij}] \in M_n(R)$*, akkor a következő állítások ekvivalensek:*
(i) A *invertáható mátrix.*
(ii) $\det(A) \in R$ *invertálható elem.*
(iii) $(o_1^A, \dots, o_n^A)$ *bázisa* M*-nek.*
(iv) $(s_1^A, \dots, s_n^A)$ *bázisa* $M_{1,n}(R)$*-nek.*

Bizonyítás. „(i)⇒(ii)" Ha létezik $B \in M_n(R)$ úgy, hogy $AB = BA = I_n$, akkor $\det(A)\det(B) = \det(I_n) = 1$, tehát $\det(A) \in U(R)$.

„(ii)⇒(i)" Ha $\det(A) \in U(R)$, akkor az előző tételből következik, hogy $A^{-1} = \det(A)^{-1}\tilde{A}$.

„(i)⇔(iii)" Létezik az egyértelműen meghatározott $f : M \to M$ lineáris függvény úgy, hogy $f(e_j) = o_j^A$, $1 \le j \le n$. Mivel $o_j^A = \sum_{i=1}^n a_{ij}e_i$, következik, hogy $[f]_{e,e} = A$. Ekkor 2.1.5. és 2.1.14.-ből következik, hogy A invertáható ⇔ f izomorfizmus ⇔ $(f(e_1), \dots, f(e_n))$ bázis ⇔ $(o_1^A, \dots, o_n^A)$ bázis. ■

Jegyezzük meg, hogy ha $\det(A) \in U(R)$, akkor

$$A^{-1} = \det(A)^{-1}\tilde{A} \quad \text{és} \quad \det(A^{-1}) = \det(A)^{-1}.$$

Az invertalható mátrixok halmazát $GL_n(R)$-el jelöljuk. Mivel $GL_n(R)$ az $(M_n(R), +, \cdot)$ gyűrű invertálható elemeinek a halmaza, következik, hogy $(GL_n(R), \cdot)$ csoport. Ezt a csoportot az **általános lineáris csoport**nak nevezzük. A fentiekből következik, hogy a

$$\det : GL_n(R) \to U(R), \qquad A \mapsto \det(A)$$

függvény csoportmorfizmus.

2.28. feladat. Igazoljuk, hogy $SL_n(K) := \{A \in GL_n(K) \mid \det A = 1\}$ részcsoportja $(GL_n(K), \cdot)$-nak. ($SL_n(K)$-t a **speciális lineáris csoport**nak nevezzük.)

2.29. feladat. Igazoljuk, hogy $GL_n(\mathbb{Q})$-nak van egy S_n-nel izomorf részcsoportja.

2.30. feladat (Ortogonális és unitér csoportok). Legyen $n \in \mathbb{N}^*$,

$$O(n) := \{A \in M_n(R) \mid A \cdot A^t = I_n\}$$

az **ortogonális** mátrixok halmaza és

$$U(n) := \{A \in M_n(\mathbb{C}) \mid A \cdot A^h = I_n\}$$

az **unitér** mátrixok halmaza, ahol: $A^h := \bar{A}^t$, $\bar{A} := [\bar{a}_{ij}]_{1 \le i,j \le n}$. Igazoljuk, hogy:
a) Ha $A \in O(n)$, akkor $A^tA = I_n$ és $\det A = \pm 1$.
b) Ha $A \in U(n)$, akkor $A^hA = I_n$ és $|\det A| = 1$.
c) $SO(n) \le O(n) \le GL_n(\mathbb{R})$, ahol $SO(n) := \{A \in O(n) \mid \det A = 1\}$ a **speciális ortogonális csoport**.
d) $SU(n) \le U(n) \le GL_n(\mathbb{C})$, ahol $SU(n) := \{A \in U(n) \mid \det A = 1\}$ a **speciális unitér csoport**.
e) $O(2) = \left\{ \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}, \begin{pmatrix} \cos t & \sin t \\ \sin t & -\cos t \end{pmatrix} \mid t \in [0, 2\pi) \right\}$.

2.31. feladat (Blokkmátrix inverze). Legyen K egy kommutatív test, $A = \begin{pmatrix} A_{11} & A_{12} \\ A_{21} & A_{22} \end{pmatrix} \in M_n(K)$, ahol $A_{11} \in M_p(K), A_{22} \in M_q(K)$, $p + q = n$, és feltételezzük, hogy A_{22} invertálható. Igazoljuk, hogy A invertálható akkor és csak akkor ha $A_{11} - A_{12}A_{22}^{-1}A_{21} \in M_p(K)$ invertálható. Ebben az esetben, fejezzük ki az A inverzét A_{22}^{-1} és $(A_{11} - A_{12}A_{22}^{-1}A_{21})^{-1}$ segítségével.

Alkalmazás. Számítsuk ki az $A = \begin{pmatrix} 1 & 2 & 0 & 2 \\ 1 & 1 & 1 & 1 \\ 1 & 1 & 2 & 4 \\ 0 & 1 & 0 & 1 \end{pmatrix} \in M_n(\mathbb{Q})$ mátrix inverzét.

2.32. feladat. Számítsuk ki az $A \in M_n(K)$ inverzét, ahol

$$A = \begin{pmatrix} 1 + a_1 & 1 & \dots & 1 \\ 1 & 1 + a_2 & \dots & 1 \\ \vdots & \vdots & \ddots & \vdots \\ 1 & 1 & \dots & 1 + a_n \end{pmatrix}.$$

2.33. feladat (Gauss-szám). Feltételezzük, hogy $|K| = q$, és legyen

$$G_n^k(q) = |\{U \leq_K K^n \mid \dim_K U = k\}|.$$

Igazoljuk, hogy:
a) $|\mathrm{GL}_n(K)| = (q^n - 1)(q^n - q)(q^n - q^2)\dots(q^n - q^{n-1})$.
b) $G_n^0(q) = G_n^n(q) = 1$.
c) $G_n^k(q) = \frac{(q^n-1)(q^{n-1}-1)\dots(q^{n-k+1}-1)}{(q^k-1)(q^{k-1}-1)\dots(q-1)}$, $k = 1, \dots, n-1$.
d) $G_n^k(q) = G_n^{n-k}(q)$.
e) $G_n^k(q) = q^n G_{n-1}^k(q) + G_{n-1}^{k-1}(q)$, $k = 1, \dots, n-1$.
f) Hány rendezett bázisa és hány bázisa van a K^n vektortérnek?

Legyen $\det(A)$ egy n-ed rendű determináns, $1 \leq i_1 < \dots < i_r \leq n$, $1 \leq j_1 < \dots < j_r \leq n$ és $D_{i_1\dots i_r}^{j_1\dots j_r}$ az a minor (aldetermináns), amelyet a $\det(A)$ $i_1, \dots, i_r$ sorainak és $j_1, \dots, j_r$ oszlopainak a kiválasztásával kapunk. Jelöljük $\tilde{D}_{i_1\dots i_r}^{j_1\dots j_r}$-el a $D_{i_1\dots i_r}^{j_1\dots j_r}$ *kiegészítő aldeterminánsát* (amelyet a megmaradt sorok és oszlopok természetes sorrendbeli kiválasztásával kapunk). Végül, $(-1)^{i_1+\dots+i_r+j_1+\dots+j_r}\tilde{D}_{i_1\dots i_r}^{j_1\dots j_r}$ a $D_{i_1\dots i_r}^{j_1\dots j_r}$ *adjungált minora.*

2.2.14. tétel (Laplace-kifejtés).

$$\det(A) = \sum_{1 \leq j_1 < \dots < j_r \leq n} (-1)^{i_1+\dots+i_r+j_1+\dots+j_r} D_{i_1\dots i_r}^{j_1\dots j_r} \tilde{D}_{i_1\dots i_r}^{j_1\dots j_r}.$$

($\det(A)$ kifejtése az $i_1, \dots, i_r$ sorok szerint; az összegnek C_n^r tagja van.)

Bizonyítás. Felhasználjuk a determináns definicióját:

$$\det(A) = \sum_{\sigma \in S_n} \mathrm{sgn}(\sigma) a_{1\sigma(1)} \dots a_{n\sigma(n)}.$$

Ha $\det(A)$-ből kiválasztunk r oszlopot, akkor a kiválasztott sorok és oszlopok egy r-ed rendű aldeterminánst határoznak meg. Ennek szorzata adjungáltjával $\det(A)$-nek $r!(n-r)!$ tagját szolgáltatja, mégpedig helyes előjellel. Mivel r oszlop C_n^r-féleképpen választható ki, az összes ilyen módon nyert determinánsszorzatok a $\det(A)$ determináns $C_n^r \cdot r!(n-r)! = n!$ tagját állítják elő. Ezek között $\det(A)$ mindegyik tagja szerepel (éspedig akkor csak egyszer). ■

2.2.15. következmény (Determinánsok szorzástétele). *Ha* $A, B \in M_n(R)$, *akkor*

$$\det(AB) = \det(A)\det(B).$$

Bizonyítás. Tekintsük a

$$C = \begin{pmatrix} A & 0_n \\ -I_n & B \end{pmatrix} \in M_{2n}(R)$$

blokkmátrixot. Laplace tétele szerint,

$$\det(C) = \det(A)\det(B)(-1)^{2\cdot\frac{n(n-1)}{2}} = \det(A)\det(B).$$

Minden $j = 1, \dots, n$ esetén adjunk hozzá az első oszlop b_{j1}-szeresét, a második oszlop b_{j2}-szeresét stb, az n-edik oszlop b_{jn}-szeresét az $n+j$-edik oszlophoz. Eljutottunk a

$$C' = \begin{pmatrix} A & AB \\ -I_n & 0_n \end{pmatrix}$$

mátrixhoz, és

$$\begin{aligned} \det(A)\det(B) &= \det(C) = \det(C') \\ &= (-1)^{n+\sum_{k=1}^{n} k + \sum_{k=n+1}^{2n} k} \det(AB) \\ &= \det(AB). \qquad ■ \end{aligned}$$

2.34. feladat (Ciklikus determináns). Igazoljuk, hogy:

$$C_n = \begin{vmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{vmatrix} = f(\epsilon_0)\dots f(\epsilon_{n-1}),$$

ahol $f = a_1 + a_2X + \dots + a_nX^{n-1}$, és ϵ_i, $i = 0, \dots, n-1$ az n-ed rendű egységgyökök.

2.35. feladat. a) Alkalmazva a Laplace-képletet, számítsuk ki a következő determinánst:

$$D = \begin{vmatrix} a_1 & 0 & a_2 & 0 & a_3 \\ 0 & x_1 & 0 & x_2 & 0 \\ b_1 & 0 & b_2 & 0 & b_3 \\ 0 & y_1 & 0 & y_2 & 0 \\ c_1 & 0 & c_2 & 0 & c_3 \end{vmatrix}.$$

b) Számítsuk ki a következő determinánst:

$$D = \begin{vmatrix} a_1 & b_1 & c_1 & d_1 & 0 & 0 \\ a_2 & b_2 & c_2 & d_2 & 0 & 0 \\ a_3 & b_3 & c_3 & d_3 & 0 & 0 \\ 0 & 0 & a_1 & b_1 & c_1 & d_1 \\ 0 & 0 & a_2 & b_2 & c_2 & d_2 \\ 0 & 0 & a_3 & b_3 & c_3 & d_3 \end{vmatrix}.$$

c) Számítsuk ki a $d_{2n} = \det(A)$ determinánst, ahol $A = [a_{ij}] \in M_{2n}(R)$,

$$a_{ij} = \begin{cases} x_i, & i = j \\ 0, & i \neq j,\ i + j = 2n + 1 \\ y_i, & i + j = 2n + 1 \end{cases}, \qquad x_i, y_i \in R.$$

d) Ha $A \in M_m(R)$, $B \in M_{m,n}(R)$ és $C \in M_n(R)$, akkor $\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A)\det(C)$.

e) Ha $A, B, C \in M_n(R)$, akkor $\det \begin{pmatrix} 0 & A \\ B & C \end{pmatrix} = (-1)^n \det(A)\det(B)$.

2.36. feladat. a) Legyen $A, B \in M_n(\mathbb{R})$ és $i = \sqrt{-1} \in \mathbb{C}$. Igazoljuk, hogy $\det \begin{pmatrix} A & -B \\ B & A \end{pmatrix} = |\det(A + iB)|^2$, és számítsuk ki a

$$D = \begin{vmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{vmatrix}$$

determinánst, ahol $a, b, c, d \in \mathbb{R}$.

b) Számítsuk ki a

$$D = \begin{vmatrix} a & -b & c & d \\ -b & a & -d & c \\ -c & d & a & -b \\ -d & -c & b & a \end{vmatrix}$$

determinánst, ahol $a, b, c, d \in \mathbb{R}$.

2.37. feladat (Binet–Cauchy). Legyen $A = (a_{ij}) \in M_{nm}(R)$, $B = (b_{kl}) \in M_{mn}(R)$ és $C = AB$. Bizonyítsuk be, hogy:

$$\det C = \sum_{1 \le j_1 < \dots < j_n \le m} \begin{vmatrix} a_{1j_1} & a_{2j_1} & a_{3j_1} & \dots & a_{nj_1} \\ a_{1j_2} & a_{2j_2} & a_{3j_2} & \dots & a_{nj_2} \\ a_{1j_3} & a_{2j_3} & a_{3j_3} & \dots & a_{nj_3} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_{1j_n} & a_{2j_n} & a_{3j_n} & \dots & a_{nj_n} \end{vmatrix} \cdot \begin{vmatrix} b_{j_1 1} & b_{j_1 2} & b_{j_1 3} & \dots & b_{j_1 n} \\ b_{j_2 1} & b_{j_2 2} & b_{j_2 3} & \dots & b_{j_2 n} \\ b_{j_3 1} & b_{j_3 2} & b_{j_3 3} & \dots & b_{j_3 n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ b_{j_n 1} & b_{j_n 2} & b_{j_n 3} & \dots & b_{j_n n} \end{vmatrix}$$

(tehát $\det C = \det A \det B$ ha $m = n$ és $\det C = 0$ ha $n > m$).

Alkalmazás. Ha $A \in M_{mn}(R)$, $m \ge n$, akkor $\det(A^t \cdot A) = \sum_B B^2$, ahol B végig fut az A n-edrendű minorainak a halmazán.

2.38. feladat (Gram-determináns). Ha $x = (x_1, \dots, x_n)$, $y = (y_1, \dots, y_n) \in \mathbb{R}^n$, legyen $\langle x, y \rangle = \sum_{i=1}^n x_i y_i$ az x, y *kanonikus skaláris szorzata.* Legyen $v^1, \dots, v^n \in \mathbb{R}^n$, $a_{ij} = \langle v^i, v^j \rangle$, $1 \le i, j \le n$, és $G(v^1, \dots, v^n) = \det(a_{ij})$.

Igazoljuk, hogy $\{v^1, \dots, v^n\}$ akkor és csak akkor független ha $G(v^1, \dots, v^n) \neq 0$.

2.2.4. Mátrix rangja

2.2.16. definíció. Legyenek U és V K-feletti vektorterek, $f : U \to V$ egy lineáris függvény, és $u_1, \dots, u_m \in U$ vektorok.

a) Értelmezés szerint, a *vektorrendszer rangja* egyenlő a vektorok által generált résztér dimenziójával:

$$\operatorname{rang}(u_1, \dots, u_m) = \dim_K \langle u_1, \dots, u_m \rangle.$$

b) A *lineáris függvény rangja* egyenlő a képtér dimenziójával:

$$\operatorname{rang} f = \dim_K \operatorname{Im} f.$$

2.2.17. megjegyzés. a) A 2.1.11. tételből következik, hogy $\operatorname{rang} f = \dim_K U - \dim_K \operatorname{Ker} f$.

b) Feltételezzük, hogy $(e_1, \dots, e_n)$ U-nak egy bázisa, tehát $U = \{x = \sum_{i=1}^n x_i e_i \mid x_i \in K\}$. Ekkor

$$\begin{aligned}\operatorname{Im} f = f(U) &= \{f(x) \mid x \in U\} \\ &= \{\sum_{i=1}^n x_i f(e_i) \mid x_i \in K\} \\ &= \langle f(e_1), \dots, f(e_n) \rangle \leq_K V,\end{aligned}$$

tehát, $\operatorname{rang} f = \operatorname{rang}(f(e_1), \dots, f(e_n))$.

2.2.18. definíció. Legyen $A = [a_{ij}] \in M_{m,n}(K)$, és legyen $0 \leq r \leq \min\{m, n\}$. Azt mondjuk, hogy az A **rangja** egyenlő r-el (jelölés: $\operatorname{rang} A = r$), ha A-nak van egy r-ed rendű nemnulla minora (aldeterminánsa), és minden r-nél nagyobb rendű minor egyenlő 0-val.

2.2.19. tétel (Kronecker-tétel). *Minden $A \in M_{m,n}(K)$ mátrix esetén,*

$$\operatorname{rang} A = \operatorname{rang}(o_1^A, \dots, o_n^A) = \operatorname{rang}(s_1^A, \dots, s_m^A).$$

Bizonyítás. Legyen $r = \operatorname{rang} A$. Ekkor A-nak van egy r-ed rendű nemnulla minora, és egyszerűség kedvéért, feltételezhetjük, hogy $\det(B) \neq 0$, ahol

$$B = \begin{pmatrix} a_{11} & \dots & a_{1r} \\ \vdots & \ddots & \vdots \\ a_{r1} & \dots & a_{rr} \end{pmatrix}$$

Következik, hogy az $o_1^B, \dots, o_r^B$ oszlopok lineárisan függetlenek, tehát az $o_1^A, \dots, o_r^A$ oszlopok is lineárisan függetlenek; következik, hogy $r \leq \operatorname{rang}(o_1^A, \dots, o_n^A)$.

Kiegészítjük B-t egy sorral és egy oszloppal, és legyen

$$D_{ij} = \begin{vmatrix} a_{11} & \dots & a_{1r} & a_{ij} \\ \vdots & \ddots & \vdots & \vdots \\ a_{r1} & \dots & a_{rr} & a_{rj} \\ a_{i1} & \dots & a_{ir} & a_{ij} \end{vmatrix}, \quad 1 \leq i \leq m, \quad r < j \leq n.$$

Igazoljuk, hogy $D_{ij} = 0$ minden $1 \leq i \leq m, \quad r < j \leq n$ esetén. Valóban, ha $1 \leq i \leq r$, akkor D_{ij}-nek van két egyenlő sora (az i-edik és az $r+1$-edik) tehát $D_{ij} = 0$; ha pedig $i > r$, akkor D_{ij} A-nak egy $r+1$-ed rendű minora, tehát feltevés szerint $D_{ij} = 0$.

Legyen $d = \det(B) \neq 0$, és legyenek $d_1, \dots, d_r, d$ az $a_{i1}, \dots, a_{ir}, a_{ij}$ elemek algebrai komplementumai; vegyük észre, hogy ezek az elemek nem függnek i-től. Kifejtjük D_{ij}-t az $r+1$-edik sora szerint; következik, hogy

$$0 = D_{ij} = a_{i1} d_1 + \dots a_{ir} d_r + a_{ij} d.$$

Legyen $\alpha_k = -d^{-1} d_k$, $1 \leq k \leq r$. Ekkor

$$a_{ij} = \alpha_1 a_{i1} + \alpha_2 a_{i2} + \dots + \alpha_r a_{ir}, \quad 1 \leq i \leq m, \ r < j \leq n.$$

Következik, hogy minden $r < j \leq n$ esetén,

$$o_j^A = \alpha_1 o_1^A + \dots + \alpha_r o_r^A \in \langle o_1^A, \dots o_r^A \rangle,$$

tehát $\operatorname{rang}(o_1^A, \dots o_r^A) \leq r$. ■

2.2.20. megjegyzés. A tétel bizonyításában csak azt használtuk fel, hogy A-nak van egy r-ed rendű nemnulla minora, és minden $r+1$-ed rendű *kiegészítő minor* egyenlő 0-val.

2.2.21. példa. Tekintsük az

$$A = \begin{pmatrix} 1 & -2 & 1 & 3 \\ 1 & -2 & -1 & 1 \\ 2 & -4 & 0 & 1 \end{pmatrix} \in M_{3,4}(\mathbb{R})$$

mátrixot. Ha $B_1 = [1]$, akkor $\det B_1 \neq 0$, és ha $B_2 = \begin{pmatrix} 1 & 1 \\ 1 & -1 \end{pmatrix}$, akkor $\det B_2 \neq 0$, tehát $\operatorname{rang} A \geq 2$. Van két kiegészítő minor; mivel

$$\begin{vmatrix} 1 & -2 & 1 \\ 1 & -2 & -1 \\ 2 & -4 & 0 \end{vmatrix} = 0 \quad \text{és} \quad \begin{vmatrix} 1 & 1 & 3 \\ 1 & -1 & 1 \\ 2 & 0 & 1 \end{vmatrix} = 0,$$

következik, hogy $\operatorname{rang} A = 2$.

2.39. feladat. Határozzuk meg az $A = (x_i y_j)_{1 \leq i \leq m, 1 \leq j \leq n} \in M_n(K)$ mátrix rangját.

2.40. feladat. Igazoljuk, hogy $\operatorname{rang}(AB) \leq \min\{\operatorname{rang} A, \operatorname{rang} B\}$.

2.3. Lineáris egyenletrendszerek

2.3.1. A Kronecker–Capelli-tétel

Legyen K egy kommutatív test, $m, n \in \mathbb{N}^*$, és feltételezzük, hogy adottak az $a_{ij} \in K$, $b_i \in K$ elemek, $1 \leq i \leq m$, $1 \leq j \leq n$.

Lineáris egyenletrenszernek nevezzük a következő feladatot: határozzuk meg az $x_1, \ldots, x_n \in K$ elemeket úgy, hogy

$$(S): \quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n & = b_2 \\ \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \cdots + a_{mn}x_n & = b_m \end{cases}$$

Vezessük be a következő mátrixokat:

$$A = [a_{ij}]_{\substack{1 \leq i \leq m \\ 1 \leq j \leq n}} \in M_{m,n}(K), \quad b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix} \in M_{m,1}(K), \quad x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in M_{n,1}(K).$$

Ekkor könnyen észrevehető, hogy (S) egyenértékű a következő mátrixegyenletekkel:

$$(S) \iff Ax = b \iff \sum_{j=1}^{n} x_j o_j^A = b.$$

2.3.1. definíció. a) Az a_{ij} elemeket *együtthatóknak*, a b_i elemeket *szabadtagoknak* és az x_j elemeket *ismeretleneknek* nevezzük.

b) Azt mondjuk, hogy A az *egyenletrendszer mátrixa*, és

$$\bar{A} = [A \vdots b] = \begin{pmatrix} a_{11} & \ldots & a_{1n} & b_1 \\ \vdots & & \vdots & \vdots \\ a_{m1} & \ldots & a_{mn} & b_m \end{pmatrix} \in M_{m,n+1}(K)$$

az *egyenletrendszer bővített mátrixa.*

c) Ha $b = 0$, akkor (S) *homogén egyenletrendszer.*

d) (S) *kompatibilis* ha létezik $x \in M_{n,1}(K) \simeq K^n$ úgy, hogy $Ax = b$; ellenkező esetben, (S) *inkompatibilis.*

2.3.2. tétel (Kronecker–Capelli). *Az* (S) *egyenletrendszer kompatibilis akkor és csak akkor, ha*

$$\operatorname{rang} A = \operatorname{rang} \bar{A}.$$

Bizonyítás. Feltételezzük, hogy (S) kompatibilis. Ekkor léteznek az $x_1, \dots, x_n \in K$ elemek úgy, hogy $b = \sum_{j=1}^{n} x_j o_j^A$, azaz $b \in \langle o_1^A, \dots, o_n^A \rangle$. Következik, hogy $\langle o_1^A, \dots, o_n^A \rangle = \langle o_1^A, \dots, o_n^A, b \rangle$, tehát

$$\operatorname{rang} A = \dim_K \langle o_1^A, \dots, o_n^A \rangle = \dim_K \langle o_1^A, \dots, o_n^A, b \rangle = \operatorname{rang} \bar{A}.$$

Fordítva, feltételezzük, hogy $\operatorname{rang} A = \operatorname{rang} \bar{A}$, azaz

$$\dim_K \langle o_1^A, \dots, o_n^A \rangle = \dim_K \langle o_1^A, \dots, o_n^A, b \rangle.$$

Mivel $\langle o_1^A, \dots, o_n^A \rangle \leq_K \langle o_1^A, \dots, o_n^A, b \rangle$, az alternatíva tételből következik, hogy

$$\langle o_1^A, \dots, o_n^A \rangle = \langle o_1^A, \dots, o_n^A, b \rangle.$$

Akkor $b \in \langle o_1^A, \dots, o_n^A \rangle$, tehát léteznek az $x_1, \dots, x_n \in K$ elemek úgy, hogy $b = \sum_{j=1}^{n} x_j o_j^A$. ■

2.3.3. következmény (Rouché-tétel). *Feltételezzük, hogy* $\operatorname{rang} A = r$ *és* $\det B = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0$ *az* (S) *fődeterminánsa.* Az $\bar{A}$ bővített mátrix azon $(r+1)$-ed rendű minorjait amelyek bővítik B-t és tartalmaznak szabadtagokat **karakterisztikus minoroknak** nevezzük.

a) *A karakterisztikus minorok száma* $m - r$.

b) (S) *kompatibilis* $\iff$ *minden karakterisztikus minor egyenlő nullával.*

2.3.2. Egyenletrendszerek megoldása

Az előző paragrafus jelöléseit használjuk.

A. A megoldasok halmaza

Azonosítsuk az $M_{n,1}(K)$ és K^n vektortereket, valamint az $M_{m,1}(K)$ és K^m vektortereket, és jelöljük e-vel a kanonikus bázisokat. Legyen $f : K^n \to K^m$ az egyértelműen meghatározott lineáris függvény úgy, hogy $[f]_{e,e} = A$. A fenti azonosí tásokból következik, hogy $f(x) = Ax$ minden $x \in K^n$ esetén. Vegyük észre, hogy az

$$f^{-1}(b) = \{x \in K^n \mid f(x) = b\}$$

halmaz megegyezik az (S) megoldásainak a halmazával.

2.3.4. tétel. a) *Ha* x^0 *az* (S) *egyenletrendszernek egy partikuláris megoldása, akkor*

$$f^{-1}(b) = x^0 + \operatorname{Ker} f.$$

b) $\dim_K \operatorname{Ker} f = n - \operatorname{rang} A$.

c) **(Cramer-szabály)** *Feltételezzük, hogy* $m = n$*;* (S)*-nek akkor és csakis akkor van egyetlen megoldása, ha* $\det A \neq 0$.

Ebben az esetben

$$x_j = (\det A)^{-1} \cdot \det(o_1^A, \dots, \underset{j}{b}, \dots, o_n^A).$$

d) *Feltételezzük, hogy* (S) *kompatibilis,* $\operatorname{rang} A = r$, $\det B = \begin{vmatrix} a_{11} & \dots & a_{1r} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rr} \end{vmatrix} \neq 0$, *és legyen*

$$(S') : \quad \begin{cases} a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n & = b_1 \\ a_{21}x_1 + a_{22}x_2 + \dots + a_{2n}x_n & = b_2 \\ \dots \\ a_{r1}x_1 + a_{r2}x_2 + \dots + a_{rn}x_n & = b_r \end{cases}$$

a redukált egyenletrendszer. (Az utolsó $m - r$ egyenletet *mellékegyenletnek* nevezzük.)

Ekkor minden $x \in K^n$ *esetén,* x *megoldása* (S)*-nek* $\iff$ x *megoldása* (S')*-nek.*

Bizonyítás. a) Feltételezzük, hogy $f(x^0) = b$.

Ha $x \in f^{-1}(b)$, akkor $f(x) = b = f(x^0)$, tehát $f(x - x^0) = 0$, azaz $y := x - x^0 \in \operatorname{Ker} f$; következik, hogy $x = x^0 + y \in x^0 + \operatorname{Ker} f$.

Fordítva, ha $x = x^0 + y \in x^0 + \operatorname{Ker} f$, ahol $y \in \operatorname{Ker} f$, akkor $f(x) = f(x^0) + f(y) = f(x^0) = b$, tehát $x \in f^{-1}(b)$.

b) Tudjuk, hogy $\operatorname{Ker} f \leq_K K^n$, és $n = \dim_K K^n = \dim_K \operatorname{Ker} f + \dim_K \operatorname{Im} f$. Továbbá,

$$\begin{aligned}\operatorname{Im} f = f(K^n) &= \{f(x) \mid x \in K^n\} = \{Ax \mid x \in K^n\}\\ &= \{\sum_{j=1}^{n} x_j o_j^A \mid x_j \in K,\ j = 1, \dots, n\}\\ &= \langle o_1^A, \dots, o_n^A \rangle.\end{aligned}$$

Kronecker tétele szerint, $\operatorname{rang} A = \dim_K \langle o_1^A, \dots, o_n^A \rangle$, tehát $\dim_K \operatorname{Ker} f = n - \operatorname{rang} A$.

c) Feltételezzük, hogy $m = n$. Ekkor

$$\begin{aligned}|f^{-1}(b)| = 1 &\iff \operatorname{Ker} f = \{0\} \text{ és } f^{-1}(b) \neq \emptyset\\ &\iff f \text{ injektív és } f^{-1}(b) \neq \emptyset\\ &\iff f \text{ bijektív} \quad \text{(alternatíva tétel szerint)}\\ &\iff A = [f]_{e,e} \text{ invertálható}\\ &\iff \det A \neq 0.\end{aligned}$$

Ebben az esetben, mivel $b = Ax = \sum_{k=1}^{n} x_k o_k^A$, következik, hogy

$$\begin{aligned}\det(o_1^A, \dots, \underset{j}{b}, \dots, o_n^A) &= \det(o_1^A, \dots, \sum_{k=1}^{n} x_k o_k^A, \dots, o_n^A)\\ &= \sum_{k=1}^{n} x_k \det(o_1^A, \dots, o_k^A, \dots, o_n^A)\\ &= x_j \det(o_1^A, \dots, o_j^A, \dots, o_n^A)\\ &= x_j \det(A).\end{aligned}$$

d) Ha $x^0 \in K^n$ megoldása (S)-nek, akkor nyilvánvaló, hogy x^0 megoldása (S')-nek is. Legyen

$$A' = \begin{pmatrix} a_{11} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{r1} & \dots & a_{rn} \end{pmatrix}$$

az (S') egyenletrenszer mátrixa, $b' = \begin{pmatrix} b_1 \\ \vdots \\ b_r \end{pmatrix}$, és legyen $f' : K^n \to K^r$, $\ f'(x) = A'x$.

Ha $f(x) = Ax = 0$, akkor $0 = A'x = f'(x)$, tehát $\operatorname{Ker} f \leq_K \operatorname{Ker} f'$. Mivel

$$\dim_K \operatorname{Ker} f' = n - \operatorname{rang} A' = n - r = n - \operatorname{rang} A = \dim_K \operatorname{Ker} f,$$

következik, hogy $\operatorname{Ker} f' = \operatorname{Ker} f$, és végül, $f^{-1}(b) = x^0 + \operatorname{Ker} f = x^0 + \operatorname{Ker} f' = f'^{-1}(b)$. ■

2.3.5. következmény. *Legyen* (S) *egy homogén egyenletrendszer. Ekkor*

a) (S) *kompatibilis.*

b) *Ha* $m = n$, *akkor* (S)*-nek van nemtriviális megoldása* $\Leftrightarrow \det A = 0$.

2.41. feladat. Tárgyaljuk és oldjuk meg a következő egyenletrendszereket:

a) $\begin{cases} 2x_1 - x_2 + x_3 - x_4 &= 1 \\ x_1 + x_2 + \alpha x_3 + x_4 &= -1 \\ x_1 - x_2 + x_3 + \beta x_4 &= \gamma \end{cases}$

b) $\begin{cases} ax_1 + (a+1)x_2 + (a+2)x_3 &= a + 3 \\ bx_1 + (b+1)x_2 + (b+2)x_3 &= b + 3 \\ x_1 + cx_2 + c^2 x_3 &= c^3 \end{cases}$

B. A mátrixegyenlet tárgyalása

A fenti egyenletrendszereket a Rouché és Cramer tételei alapján oldottuk meg. A következő módszer mátrixegyenletként kezeli (S)-et.

Ha (S) kompatibilis, akkor a 2.3.4. tétel d) pontjából következik, hogy feltételezhetjük, hogy $\operatorname{rang} A = m \leq n$, és legyen $\det B \neq 0$ az (S) **fődeterminánsa**, ahol

$$B = \begin{pmatrix} a_{11} & \dots & a_{1m} \\ \vdots & & \vdots \\ a_{m1} & \dots & a_{mm} \end{pmatrix} \in M_{mm}(K).$$

Felírjuk A-t az $A = [B \vdots S]$ alakban, ahol

$$S = \begin{pmatrix} a_{1,m+1} & \dots & a_{1n} \\ \vdots & & \vdots \\ a_{m,m+1} & \dots & a_{mm} \end{pmatrix} \in M_{m,n-m}(K),$$

és legyen $x = \begin{pmatrix} x_B \\ x_S \end{pmatrix}$, ahol $x_B = \begin{pmatrix} x_1 \\ \vdots \\ x_m \end{pmatrix}$ a **főismeretlenek** mátrixa, és $x_S = \begin{pmatrix} x_{m+1} \\ \vdots \\ x_n \end{pmatrix}$ a **mellékismeretlenek** mátrixa. Ekkor (S)-et felírhatjuk a következő alakban:

$$(S): \qquad Bx_B + Sx_S = b.$$

Tekinsük először az (S)-hez rendelt $Bx_B + Sx_S = 0$ **homogén** mátrixegyenletet. Ennek a megoldása

$$x_B = -B^{-1}Sx_S, \qquad x_S \in K^{n-m}.$$

Legyen $x_S^{(1)} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$, $x_S^{(2)} = \begin{pmatrix} 0 \\ 1 \\ \vdots \\ 0 \end{pmatrix}, \dots, x_S^{(n-m)} = \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 1 \end{pmatrix}$ a K^{n-m} kanonikus bázisa, $x_B^{(j)} = -B^{-1}Sx_S^{(j)}$, $1 \leq j \leq n-m$, és legyen

$$x^{(j)} = \begin{pmatrix} x_B^{(j)} \\ x_S^{(j)} \end{pmatrix} \in \operatorname{Ker} f, \quad 1 \leq j \leq n-m.$$

Mivel $\dim_K \operatorname{Ker} f = n - m$, következik, hogy $x^{(1)}, \dots, x^{(n-m)}$ bázisa $\operatorname{Ker} f$-nek, tehát

$$\operatorname{Ker} f = \langle x^{(1)}, \dots, x^{(n-m)} \rangle.$$

Továbbá, egy x^0 partikuláris megoldást a következő képpen kapunk: legyen $x_S^0 = 0 \in K^{n-m}$, $x_B^0 = B^{-1}b - B^{-1}Sx_S^0 = B^{-1}b \in K^m$, tehát

$$x^0 = \begin{pmatrix} B^{-1}b \\ 0 \end{pmatrix} \in K^n$$

megoldása (S)-nek.

Megkaptuk tehát az (S) megoldásainak a halmazát:

$$\begin{aligned} f^{-1}(b) &= x^0 + \operatorname{Ker} f \\ &= x^0 + \langle x^{(1)}, \dots, x^{(n-m)} \rangle \\ &= \{x^0 + \lambda_1 x^{(1)} + \dots + \lambda_{n-m} x^{(n-m)} \mid \lambda_1, \dots, \lambda_{n-m} \in K\}. \end{aligned}$$

Azt mondjuk, hogy $\lambda_1, \dots, \lambda_{n-m} \in K$ *szabad paraméterek.*

2.3.6. példa. Tekintsük az

$$(S): \quad \begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \\ x_1 + 3x_2 + 2x_3 + 5x_4 + 4x_5 & = 2 \end{cases}$$

egyenletrendszert. A fenti jelöléseket alkalmazva,

$$A = \begin{pmatrix} 1 & 2 & 1 & 3 & 3 \\ -1 & -1 & -1 & -2 & -2 \\ 1 & 3 & 2 & 5 & 4 \end{pmatrix}, \quad b = \begin{pmatrix} 3 \\ -2 \\ 2 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 2 & 1 \\ -1 & -1 & -1 \\ 1 & 3 & 2 \end{pmatrix},$$

$$-B^{-1}S = \begin{pmatrix} 0 & -1 \\ -1 & -1 \\ -1 & 0 \end{pmatrix}, \quad B^{-1}b = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix},$$

tehát az (S) megoldásainak a halmaza

$$\{x^0 + \lambda_1 x^{(1)} + \lambda_2 x^{(2)} \mid \lambda_1, \lambda_2 \in K\},$$

ahol

$$x^0 = \begin{pmatrix} 3 \\ 1 \\ -2 \\ 0 \\ 0 \end{pmatrix}, \quad x^{(1)} = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad x^{(2)} = \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

2.42. feladat. Oldjuk meg a következő egyenletrendszereket:

a) $\begin{cases} x_1 + 3x_2 - x_3 - 2x_4 & = 3 \\ 2x_1 - x_2 + 3x_3 - 4x_4 & = -1 \end{cases}$

b) $\begin{cases} x_1 - 2x_2 - 2x_3 - 2x_4 - x_5 & = 0 \\ x_1 - x_2 - x_3 - 3x_4 + x_5 & = 1 \\ x_1 + x_2 - 5x_3 - x_4 + 7x_5 & = 2 \end{cases}$

c) $\begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \end{cases}$

d) $\begin{cases} \hat{2}x_1 + x_2 - 2x_3 & = \hat{1} \\ x_1 + \hat{5}x_2 + \hat{2}x_3 & = \hat{2} \end{cases}, \quad (K = \mathbb{Z}_7)$

Gyakorlatban, ha m és n nagy számok, akkor a fenti módszerek nem hatékonyak. A következő paragrafusban egy sokkal gyorsabb eljárást mutatunk be.

2.3.3. Algoritmikus módszerek

A. Kicserélési lemma (Elemi báziscsere)

Legyen V egy K-feletti vektortér és $e = (e_1, \dots, e_n)$ egy rendezett bázisa,

2.3.7. lemma. *Legyen $v = a_1e_1 + \cdots + a_ne_n \in V$ és tekintsük az $e' = (e_1, \dots, \underset{i}{v}, \dots, e_n)$ vektorrendszert.*

a) *e' akkor és csak akkor bázisa V-nek, ha $a_i \neq 0$.*

b) *Feltételezzük, hogy $a_i \neq 0$, és legyen*

$$x = x_1e_1 + \cdots + x_ie_i + \cdots + x_ne_n = x'_1e_1 + \cdots + x'_iv + \cdots + x'_ne_n \in V.$$

Ekkor

$$x'_i = \frac{x_i}{a_i}, \quad x'_j = \frac{x_ja_i - x_ia_j}{a_i}, \ j \neq i.$$

Bizonyítás. a) Az alternatíva tétel szerint, e' akkor és csak akkor bázis, ha független. Ha $b_1, \dots, b_n \in K$, akkor

$$\begin{aligned} b_1e_1 + \cdots + b_iv + \cdots + b_ne_n = 0 &\iff b_1e_1 + \cdots + b_i\sum_{j=1}^{n} a_je_j + \cdots + b_ne_n = 0 \\ &\iff (b_1 + b_ia_1)e_1 + \cdots + b_ia_iv + \cdots + (b_n + b_ia_n)e_n = 0 \\ &\iff b_ia_i = 0, \quad b_j + b_ia_j = 0, \ j \neq i. \end{aligned}$$

Ha $a_i \neq 0$, akkor $b_i = 0$; következik, hogy $b_1 = \cdots = b_n = 0$, tehát e' bázis.
Ha $a_i = 0$, akkor legyen $b_i = 1$, és $b_j = -a_j,\ j \neq i$; következik, hogy e' nem független.
b) Ha $a_i \neq 0$, akkor

$$\begin{aligned} x &= x_1 e_1 + \cdots + x_i e_i + \cdots + x_j e_j + \cdots + x_n e_n \\ &= x_1' e_1 + \cdots + x_i' v + \cdots + x_j' e_j + \cdots + x_n' e_n \\ &= (x_1' + x_i' a_1) e_1 + \cdots + x_i' a_i e_i + \cdots + (x_j' + x_i' a_j) e_j + \cdots + (x_n' + x_i' a_n) e_n. \end{aligned}$$

Mivel e bázis, következik, hogy $x_i = x_i' a_i$ és $x_j = x_j' + x_i' a_j$ ha $j \neq i$, tehát

$$x_i' = \frac{x_i}{a_i}, \quad x_j' = x_j - \frac{x_i}{a_i} a_j,\ j \neq i. \qquad \blacksquare$$

Az $a_i \neq 0$ elemet *generáló elemnek* nevezzük. A fenti számításokat egy táblázatban rendszerezzük:

	v	x
e_1	a_1	x_1
$\vdots$	$\vdots$	$\vdots$
e_i	$\boxed{a_i}$	x_i
$\vdots$	$\vdots$	$\vdots$
e_j	a_j	x_j
$\vdots$	$\vdots$	$\vdots$
e_n	a_n	x_n

$\longrightarrow$

	v	x
e_1	0	$x_1' = \frac{x_1 a_i - x_i a_1}{a_i}$
$\vdots$	$\vdots$	$\vdots$
v	1	$x_i' = \frac{x_i}{a_i}$
$\vdots$	$\vdots$	$\vdots$
e_j	0	$x_j' = \frac{x_j a_i - x_i a_j}{a_i}$
$\vdots$	$\vdots$	$\vdots$
e_n	0	$x_n' = \frac{x_n a_i - x_i a_n}{a_i}$

Az alapműveletet könnyű megjegyezni: a generáló elem sorát osztjuk a generáló elemmel, a többi elemet az ún. *téglalap-szabállyal* számítjuk ki.

B. Alkalmazások

a) Báziscsere. Legyen $v = (v_1, \ldots, v_n)$ egy vektorrendszer, ahol

$$v_j = \sum_{i=1}^{n} a_{ij} e_i, \qquad 1 \leq j \leq n,$$

és legyen $T_e^v = [a_{ij}] \in M_n(K)$ az áttérési mátrix. Tudjuk, hogy v akkor és csak akkor bázis, ha T invertálható, és ha

$$x = x_1 e_1 + \cdots + x_n e_n = x_1' v_1 + \cdots + x_n' v_n,$$

akkor $[x]_v = T^{-1}[x]_e$. n-szer alkalmazva a kicserélési lemmát, meghatározhatjuk az $[x]_v$ mátrixot.

	v_1	$\ldots$	v_n	x
e_1	a_{11}	$\ldots$	a_{1n}	x_1
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
e_n	a_{n1}	$\ldots$	a_{nn}	x_n

$\xrightarrow{n \text{ lépés}}$

	v_1	$\ldots$	v_n	x
v_1	1	$\ldots$	0	x_1'
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$
v_n	0	$\ldots$	1	x_n'

Ha T nem invertálható, akkor az $e_1, \ldots, e_n$ vektorokat nem lehet kicserélni a $v_1, \ldots, v_n$ vektorokkal.

Például, legyen $V = \mathbb{R}^3$, $e = (e_1, e_2, e_3)$ a kanonikus bázisa, és legyen $v_1 = (1, 4, 2)$, $v_2 = (1, 3, 1)$, $v_3 = (1, 2, 1)$ és $x = (1, -2, -2)$.

	v_1	v_2	v_3	x
e_1	$\boxed{1}$	1	1	1
e_2	4	3	2	-2
e_3	2	1	1	-2
v_1	1	1	1	1
e_2	0	$\boxed{-1}$	-2	-6
e_3	0	-1	-1	-4
v_1	1	0	-1	-5
v_2	0	1	2	6
e_3	0	0	$\boxed{1}$	2
v_1	1	0	0	-3
v_2	0	1	0	2
v_3	0	0	1	2

Az utolsó táblázatból következik, hogy v bázis és $x = -3v_1 + 2v_2 + 2v_3$.

2.43. feladat. Igazoljuk, hogy $v = (v_1, \dots, v_n)$ bázisa V-nek és határozzuk meg az x koordinátáit a v bázisban, ahol:

a) $V = \mathbb{Z}_5^3$, $v_1 = (\hat{2}, \hat{3}, \hat{1})$, $v_2 = (\hat{1}, \hat{2}, \hat{4})$, $v_3 = (\hat{0}, \hat{1}, \hat{1})$, $x = (\hat{4}, \hat{2}, \hat{1})$.
b) $V = \mathbb{R}^4$, $v_1 = (2, 1, 3, -2)$, $v_2 = (-1, 1, -2, 1)$, $v_3 = (4, 5, 3, -1)$, $v_4 = (1, 5, -3, 1)$, $x = (1, 1, 1, 1)$.
c) $V = \mathbb{R}^3$, $v_1 = (1, 2, 1)$, $v_2 = (2, 3, 3)$, $v_3 = (3, 7, 1)$, $x = (1, 1, 1)$.

2.44. feladat. Határozzuk meg az $U, V, U + V, U \cap V \leq_{\mathbb{R}} \mathbb{R}^3$ részterek egy-egy bázisát, ahol:

a) $U = \langle (1, 0, 4), (2, 1, 0), (1, 1, -4) \rangle$, $V = \langle (-3, -2, 4), (5, 2, 4), (-2, 0, -8) \rangle$.
b) $U = \langle (1, 1, 0), (0, 1, 0), (0, 1, 1) \rangle$, $V = \langle (1, 1, -1), (2, 0, 1) \rangle$.

b) Mátrix rangja. Ha $A \in M_{m,n}(K)$, akkor $\operatorname{rang} A = \dim_K \langle o_1^A, \dots o_n^A \rangle$, tehát alkalmazhatjuk a kicserélési lemmát. Például, legyen $A = \begin{pmatrix} 1 & -2 & 1 & 3 \\ 1 & -2 & -1 & 1 \\ 2 & -4 & 0 & 4 \end{pmatrix}$.

	o_1^A	o_2^A	o_3^A	o_4^A
e_1	$\boxed{1}$	-2	1	3
e_2	1	-2	-1	1
e_3	2	-4	0	4
o_1^A	1	-2	1	3
e_2	0	0	$\boxed{-2}$	-2
e_3	0	0	-2	-2
o_1^A	1	-2	0	2
o_3^A	0	0	1	1
e_3	0	0	0	0

Az utolsó táblázatból következik, hogy $o_2^A = -2o_1^A$, $o_4^A = 2o_1^A + o_3^A$, és o_1^A, o_3^A lineárisan függetlenek, tehát $\operatorname{rang} A = 2$.

2.45. feladat. Határozzuk meg a következő mátrixok rangját:

a) $\begin{pmatrix} 1 & -1 & 1 & 2 & 2 \\ 1 & -1 & -1 & 1 & 3 \\ 2 & 2 & 0 & 3 & 5 \end{pmatrix}$ b) $\begin{pmatrix} 1 & -2 & 1 & 3 \\ 1 & -2 & -1 & 1 \\ 1 & -4 & 0 & 4 \end{pmatrix}$

c) Mátrix inverze és determinánsa. Az $A = [a_{ij}] \in M_n(K)$ mátrix akkor és csak akkor invertálható, ha $(o_1^A, \dots, o_n^A)$ bázis. Legyen $I = I_n$ az n-ed rendű egységmátrix, és tekintsük a következő táblázatokat:

	o_1^A	$\dots$	o_n^A	o_1^I	$\dots$	o_n^I
e_1	a_{11}	$\dots$	a_{1n}	1	$\dots$	0
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
e_n	a_{n1}	$\dots$	a_{nn}	0	$\dots$	1

$\xrightarrow{n \text{ lépés}}$

	v_1	$\dots$	v_n	o_1^I	$\dots$	o_n^I
o_1^A	1	$\dots$	0	b_{11}	$\dots$	b_{1n}
$\vdots$	$\vdots$	$\ddots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$
o_n^A	0	$\dots$	1	b_{n1}	$\dots$	b_{nn}

Legyen $B = [b_{ij}]$. Az utolsó táblázatból következik, hogy minden $1 \le j \le n$ esetén, $o_j^I = \sum_{k=1}^n o_k^A b_{kj}$, azaz

$$\delta_{ij} = \sum_{k=1}^{n} a_{ik} b_{kj}, \quad 1 \le i, j \le n,$$

tehát $I_n = AB$ és $B = A^{-1}$.

Legyen $a_{i_k j_k}^{(k)}$ a k-adik generáló elem. A determinánsok tulajdonságaiból következik, hogy

$$\det A = \prod_{k=1}^{n} (-1)^{i_k + j_k} a_{i_k j_k}^{(k)}.$$

Például, legyen $A = \begin{pmatrix} \hat{2} & \hat{4} & \hat{2} \\ \hat{1} & \hat{1} & \hat{1} \\ \hat{3} & \hat{2} & \hat{1} \end{pmatrix} \in M_3(\mathbb{Z}_5)$. Előállítjuk a következő táblázatokat:

	o_1^A	o_2^A	o_3^A	o_1^I	o_2^I	o_3^I
e_1	$\boxed{\hat{2}}$	$\hat{4}$	$\hat{2}$	$\hat{1}$	$\hat{0}$	$\hat{0}$
e_2	$\hat{1}$	$\hat{1}$	$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{0}$
e_3	$\hat{3}$	$\hat{2}$	$\hat{1}$	$\hat{0}$	$\hat{0}$	$\hat{1}$
o_1^A	$\hat{1}$	$\hat{2}$	$\hat{1}$	$\hat{3}$	$\hat{0}$	$\hat{0}$
e_2	$\hat{0}$	$\boxed{\hat{4}}$	$\hat{0}$	$\hat{2}$	$\hat{1}$	$\hat{0}$
e_3	$\hat{0}$	$\hat{1}$	$\hat{3}$	$\hat{1}$	$\hat{0}$	$\hat{1}$
o_1^A	$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	$\hat{2}$	$\hat{0}$
o_2^A	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
e_3	$\hat{0}$	$\hat{0}$	$\boxed{\hat{3}}$	$\hat{3}$	$\hat{1}$	$\hat{1}$
o_1^A	$\hat{1}$	$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{3}$
o_2^A	$\hat{0}$	$\hat{1}$	$\hat{0}$	$\hat{3}$	$\hat{4}$	$\hat{0}$
o_3^A	$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{2}$

Az utolsó táblázatból következik, hogy $A^{-1} = \begin{pmatrix} \hat{1} & \hat{0} & \hat{3} \\ \hat{3} & \hat{4} & \hat{0} \\ \hat{1} & \hat{2} & \hat{2} \end{pmatrix}$, és $\det A = \hat{2} \cdot \hat{4} \cdot \hat{3} = \hat{4}$.

2.46. feladat. Határozzuk meg a következő mátrixok inverzét:

a) $\begin{pmatrix} \hat{2} & \hat{0} & \hat{1} \\ \hat{1} & \hat{2} & \hat{1} \\ \hat{2} & \hat{1} & \hat{1} \end{pmatrix} \in M_3(\mathbb{Z}_3)$ b) $\begin{pmatrix} \hat{2} & \hat{4} & \hat{2} \\ \hat{1} & \hat{1} & \hat{1} \\ \hat{0} & \hat{2} & \hat{1} \end{pmatrix} \in M_3(\mathbb{Z}_5)$.

2.47. feladat. Legyen $f \in \mathrm{End}_{\mathbb{R}}(\mathbb{R}^4)$, $[f]_{e,e} = \begin{pmatrix} 2 & 2 & 0 & 1 \\ 3 & 0 & -1 & 2 \\ 2 & 5 & 3 & 1 \\ 1 & 2 & 1 & 3 \end{pmatrix}$, $e' = (e_1', e_2', e_3', e_4')$, $e_1' = e_1, e_2' = e_1 + e_2, e_3' = e_1 + e_2 + e_3, e_4' = e_1 + e_2 + e_3 + e_4$. Határozzuk meg az f mátrixát az (e', e') bázispárban.

2.48. feladat. Legyen $u = (u_1, u_2, u_3, u_4)$, $v = (v_1, v_2, v_3, v_4)$, ahol $u_1 = (1, 2, -1, 0)$, $u_2 = (1, -1, 1, 1)$, $u_3 = (-1, 2, 1, 1)$, $u_4 = (-1, -1, 0, 1)$, $v_1 = (2, 1, 0, 1)$, $v_2 = (0, 1, 2, 2)$, $v_3 = (-2, 1, 1, 2)$, $v_4 = (1, 3, 1, 2) \in \mathbb{R}^4$. Igazoljuk, hogy u, v bázisok és határozzuk meg a T_u^v áttérési mátrixot.

d) Egyenletrendszerek megoldása. Tekintsük az $Ax = b \iff Bx_B + Sx_S = b$ egyenletrendszert, ahol a 2.3.2. paragrafus jelölései használjuk. Ha $B \in M_m(K)$ invertálható, akkor az egyenletrendszer megoldasait megkapjuk m lépés után. A számítások azt is kimutatják, ha a rendszer összeférhetetlen, mert ebben az esetben $\operatorname{rang} A < \operatorname{rang} \bar{A}$.

	o_1^A	$\dots$	o_m^A	o_{m+1}^A	$\dots$	o_n^A	b
e_1							
$\vdots$		B			S		b
e_m							

$\downarrow$ m lépés

	$o_1^A \ \dots \ o_m^A$	$o_{m+1}^A \ \dots \ o_n^A$	b
o_1^A $\vdots$ o_m^A	I_m	$B^{-1}S$	$B^{-1}b$

Például oldjuk meg az

$$(S): \quad \begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \\ x_1 + 3x_2 + 2x_3 + 5x_4 + 4x_5 & = 2 \end{cases}$$

egyenletrendszert.

	o_1^A	o_2^A	o_3^A	o_4^A	o_5^A	b
e_1	$\boxed{1}$	2	1	3	3	3
e_2	-1	-1	-1	-2	-2	-2
e_3	1	3	2	5	4	2
o_1^A	1	2	1	3	3	3
e_2	0	$\boxed{1}$	0	1	1	1
e_3	0	1	1	2	1	-1
o_1^A	1	0	1	1	1	1
o_2^A	0	1	0	1	1	1
e_3	0	0	$\boxed{1}$	1	0	-2
o_1^A	1	0	0	0	1	3
o_2^A	0	1	0	1	1	1
o_3^A	0	0	1	1	0	-2

Az utolsó táblázatból következik, hogy

$$-B^{-1}S = \begin{pmatrix} 0 & -1 \\ -1 & -1 \\ -1 & 0 \end{pmatrix}, \quad B^{-1}b = \begin{pmatrix} 3 \\ 1 \\ -2 \end{pmatrix},$$

tehát az (S) megoldásainak a halmaza

$$\{x^0 + \lambda_1 x^{(1)} + \lambda_2 x^{(2)} \mid \lambda_1, \lambda_2 \in K\},$$

ahol

$$x^0 = \begin{pmatrix} 3 \\ 1 \\ -2 \\ 0 \\ 0 \end{pmatrix}, \quad x^{(1)} = \begin{pmatrix} 0 \\ -1 \\ -1 \\ 1 \\ 0 \end{pmatrix}, \quad x^{(2)} = \begin{pmatrix} -1 \\ -1 \\ 0 \\ 0 \\ 1 \end{pmatrix}.$$

2.49. feladat. Oldjuk meg a következő egyenletrendszereket:

a) $$\begin{cases} x_1 + 3x_2 - x_3 - 2x_4 & = 3 \\ 2x_1 - x_2 + 3x_3 - 4x_4 & = -1 \\ 3x_1 - 5x_2 + 7x_3 - 6x_4 & = 1 \end{cases}$$

b) $$\begin{cases} x_1 - 2x_2 - 2x_3 - 2x_4 - x_5 & = 0 \\ x_1 - x_2 - x_3 - 3x_4 + x_5 & = 1 \\ x_1 + x_2 - 5x_3 - x_4 + 7x_5 & = 2 \end{cases}$$

c) $$\begin{cases} x_1 + 2x_2 + x_3 + 3x_4 + 3x_5 & = 3 \\ -x_1 - x_2 - x_3 - 2x_4 - 2x_5 & = -2 \\ x_1 + 3x_2 + 2x_3 + 5x_4 + 4x_5 & = 2 \end{cases}$$

d) $$\begin{cases} \hat{2}x_1 + x_2 - 2x_3 & = \hat{1} \\ \hat{2}x_1 + \hat{2}x_2 + \hat{2}x_3 & = \hat{0}, \\ x_1 + \hat{4}x_2 + \hat{2}x_3 & = \hat{2} \end{cases} \quad (K = \mathbb{Z}_5)$$

2.50. feladat. Legyen $f : \mathbb{R}^n \to \mathbb{R}^m$ egy lineáris leképezés. Határozzuk meg a $\operatorname{Ker} f$ és $\operatorname{Im} f$ vektorterek egy-egy bázisát, ha adott az f mátrixa a kanonikus bázisokban:

a) $[f]_{e,e} = \begin{pmatrix} 3 & -1 & -1 & 1 \\ 1 & 2 & -1 & -1 \end{pmatrix}$

b) $[f]_{e,e} = \begin{pmatrix} 0 & -1 & 5 \\ 1 & 0 & 0 \\ 0 & 1 & -5 \end{pmatrix}$

c) $[f]_{e,e} = \begin{pmatrix} 1 & 0 & -3 & 2 \\ -2 & 3 & 0 & 1 \\ 3 & -3 & -1 & 1 \end{pmatrix}$

d) $[f]_{e,e} = \begin{pmatrix} 2 & 2 & 1 \\ -1 & -3 & 1 \\ 1 & 2 & -1 \end{pmatrix}$

2.4. Sajátértékek és sajátvektorok

2.4.1. Karakterisztikus polinom

Legyen V egy K-feletti vektortér, $e = (e_1, \dots, e_n)$ egy bázis V-ben, $f \in \operatorname{End}_K(V)$ egy endomorfizmus, és legyen

$$A = [f]_{e,e} \in M_n(K),$$

az f mátrixa.

2.4.1. definíció. a) Azt mondjuk, hogy $\lambda \in K$ **sajátértéke** az f endomorfizmusnak, ha létezik $x \in V$, $x \neq 0$ úgy, hogy $f(x) = \lambda x$.

b) Ebben az esetben, azt mondjuk, hogy x a λ-hoz tartozó **sajátvektor**.

c) A $P_A(X) = \det(A - XI_n) \in K[X]$ polinomot az A matrix **karakterisztikus polinom**jának nevezzük.

2.4.2. megjegyzés. a) Vegyük észre, hogy

$$\begin{aligned} P_A(X) &= \begin{vmatrix} a_{11} - X & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} - X & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n1} & a_{n2} & \dots & a_{nn} - X \end{vmatrix} \\ &= (-1)^n (X^n - \operatorname{Tr}(A) X^{n-1} + \dots + (-1)^n \det A). \end{aligned}$$

Például, ha $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, akkor $P_A(X) = x^2 - (a+d)X + (ad - bc)$.

b) A $P_A(X)$ polinom nem függ az e bázistól, ezért beszélhetünk az f karakterisztikus polinomjáról: értelmezés szerint, legyen

$$P_f(X) = P_{[f]_{e,e}}(X).$$

Valóban, legyen $e' = (e'_1, \dots, e'_n)$ egy második bázis, $T = T_e^{e'}$ az áttérési mátrix, és legyen $A' = [f]_{e',e'} = T^{-1}AT$. Ekkor

$$\begin{aligned} P_{A'}(X) &= \det(A' - XI_n) \\ &= \det(T^{-1}AT - T^{-1}XI_nT) \\ &= \det(T^{-1}) \det(A - XI_n) \det(T) \\ &= \det(A - XI_n) = P_A(X). \end{aligned}$$

2.4.3. tétel. $\lambda \in K$ *akkor és csak akkor sajátértéke* f*-nak, ha* $P_f(\lambda) = 0$.

Bizonyítás. Azonosítva a V és K^n vektortereket, látható, hogy minden $x \in V$ esetén,

$$f(x) = \lambda x \iff A[x]_e = \lambda [x]_e \iff (A - \lambda I_n)[x]_e = 0.$$

A kapott homogén egyenletrendszernek akkor és csak akkor van nemnulla megoldása, ha $\det(A - \lambda I_n) = 0$, azaz, ha λ gyöke $P_A(X)$-nek. ■

2.4.4. definíció. a) Az f endomorfizmus sajátértékeinek a halmazát az f **spektrumának** nevezik.
b) Ha λ r-szeres gyöke $P_f(X)$-nek, akkor r-et a λ **algebrai multiplicitás**ának nevezzük. Jelölés: $m_{\text{alg}}(\lambda) = r$.
c) A $V(\lambda) = \{x \in V \mid f(x) = \lambda x\} = \operatorname{Ker}(f - \lambda 1_V)$ részteret a λ-hoz tartozó **sajátrésztérnek** nevezzük.
d) A $V(\lambda)$ résztér dimenzióját a λ sajátérték **geometriai multiplicitás**ának nevezzük. Jelölés: $m_{\text{geom}}(\lambda)$.

2.51. feladat. Határozzuk meg a következő mátrixok sajátértékeit és sajátrésztereit:

a) $\begin{pmatrix} 1 & 2 & -2 \\ 2 & 1 & -2 \\ 2 & 2 & -3 \end{pmatrix}$ b) $\begin{pmatrix} 2 & 1 & 1 \\ 2 & 3 & 2 \\ 3 & 3 & 4 \end{pmatrix}$

c) $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$ d) $\begin{pmatrix} 0 & 2 & 1 \\ -2 & 0 & 3 \\ -1 & -3 & 0 \end{pmatrix}$

e) $\begin{pmatrix} 5 & 6 & -3 \\ -1 & 0 & 1 \\ 1 & 2 & -1 \end{pmatrix}$ f) $\begin{pmatrix} \cos t & -\sin t \\ \sin t & \cos t \end{pmatrix}$

2.52. feladat. Határozzuk meg a következő mátrixok sajátértékeit:

$$\begin{pmatrix} 0 & x & x & \dots & x \\ y & 0 & x & \dots & x \\ y & y & 0 & \dots & x \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ y & y & y & \dots & 0 \end{pmatrix}; \quad \begin{pmatrix} a_1 & a_2 & a_3 & \dots & a_n \\ a_n & a_1 & a_2 & \dots & a_{n-1} \\ a_{n-1} & a_n & a_1 & \dots & a_{n-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ a_2 & a_3 & a_4 & \dots & a_1 \end{pmatrix}; \quad \begin{pmatrix} 0 & 1 & 0 & \dots & 0 \\ -1 & 0 & 1 & \dots & 0 \\ 0 & -1 & 0 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}.$$

2.53. feladat. Igazoljuk, hogy bármely $A, B \in M_n(\mathbb{C})$ esetén $P_{AB}(X) = P_{BA}(X)$.

2.54. feladat. Legyen $p = a_0 + a_1X + \dots + a_{n-1}X^{n-1} + X^n \in K[X]$ egy polinom. Igazoljuk, hogy az

$$A_p = \begin{pmatrix} 0 & 0 & 0 & \dots & 0 & -a_0 \\ 1 & 0 & 0 & \dots & 0 & -a_1 \\ 0 & 1 & 0 & \dots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \dots & 1 & -a_{n-1} \end{pmatrix}$$

mátrix karakterisztikus polinomja egyenlő p-vel.

Cayley–Hamilton-tétel

Ha $p = a_mX^m + a_{m-1}X^{m-1} + \dots + a_1X + a_0 \in K[X]$, akkor a polinomalgebra unverzális tulajdonságából következik, hogy van értelme a

$$p(f) = a_mf^n + a_{m-1}f^{m-1} + \dots + a_1f + a_0 1_V \in \operatorname{End}_K(V)$$

endomorfizmusnak, és a

$$p(A) = a_mA^n + a_{m-1}A^{m-1} + \dots + a_1A + a_0I_n \in M_n(K)$$

mátrixnak.

Ha $B(X) = [b_{ij}(X)] \in M_n(K[X])$, akkor $B(X)$ egyértelműen felírható a

$$B(X) = A_rX^r + A_{r-1}X^{r-1} + \dots + A_1X + A_0,$$

alakban, ahol $A_i \in M_n(K)$, és $r = \max\{\deg b_{ij}(X) \mid 1 \le i, j \le n\}$.

2.4.5. tétel (Cayley–Hamilton). *Minden endomorfizmus gyöke a karakterisztikus polinomjának.*

Bizonyítás. Legyen $P(X) = P_f(X) = a_0 + a_1X + \dots + a_nX^n \in K[X]$ az f karakterisztikus polinomja. A tétel állítása ekvivalens a $P(A) = 0_n$ egyenlőséggel, ahol $A = [f]_{e,e}$.

Legyen $B(X) \in M_n(K[X])$ az $A - XI_n \in M_n(K[X])$ mátrix adjungáltja. Ekkor

$$B(X) \cdot (A - XI_n) = \det(A - XI_n) \cdot I_n = P(X) \cdot I_n.$$

Mivel $B(X)$ felírható a

$$B(X) = B_{n-1}X^{n-1} + \dots + B_1X + B_0$$

alakban, ahol $B_i \in M_n(K)$, $1 \le i \le n-1$, következik, hogy

$$(B_{n-1}X^{n-1} + \cdots + B_1X + B_0)(A - XI_n) = P(X) \cdot I_n.$$

A két polinom együtthatóit azonosítva, kapjuk, hogy

$$\begin{cases} AB_0 & = a_0 I_n \\ AB_1 - B_0 & = a_1 I_n \\ & \vdots \\ AB_{n-1} - B_{n-2} & = a_{n-1} I_n \\ -B_{n-1} & = a_n I_n. \end{cases}$$

A második egyenlőséget beszorozzuk A-val, a harmadikat A^2-el, ..., az utolsót A^n-el, és összeadjuk az eredményeket; következik, hogy

$$P(A) = a_0 I_n + a_1 A + \cdots + a_n A^n = 0_n. \qquad \blacksquare$$

2.4.2. Triangularizálható endomorfizmusok

Legyen V egy n-dimenziós K-feletti vektortér, $e = (e_1, \ldots, e_n)$ egy bázisa, és $f \in \mathrm{End}_K(V)$ egy endomorfizmus.

2.4.6. definíció. Azt mondjuk hogy f **triangularizálható**, ha létezik egy $v = (v_1, \ldots, v_n)$ bázis úgy, hogy az $[f]_{e,e} \in M_n(K)$ mátrix trianguláris.

2.4.7. tétel (triangularizálható endomorfizmusok jellemzése). *Az $f \in \mathrm{End}_K(V)$ endomorfizmus akkor és csak akkor triangularizálható, ha a P_f karakterisztikus polinomnak n gyöke van K-ban.*

Bizonyítás. Feltételezzük, hogy létezik egy $v = (v_1, \ldots, v_n)$ bázis amelyre

$$[f]_{e,e} = \begin{pmatrix} a_{11} & & * \\ \vdots & \ddots & \vdots \\ 0 & & a_{nn} \end{pmatrix}.$$

Ekkor

$$P_f(X) = \det([f]_{v,v} - XI_n) = (a_{11} - X) \ldots (a_{nn} - X),$$

tehát a P_f gyökei $a_{11}, a_{22}, \ldots, a_{nn} \in K$.

Fordítva, feltételezzük, hogy a P_f $\lambda_1, \ldots, \lambda_n$ gyökei K-ban vannak. n-szerinti indukciót alkalmazunk.

Ha $n = 1$, akkor $[f]_{e,e} = [a_{11}]$ trianguláris mátrix.

Legyen $n > 1$, és feltételezzük, hogy az állítás igaz minden $(n-1)$-dimenziós V' vektortér és minden $f' \in \mathrm{End}_K(V)$ endomorfizmus esetén.

Legyen $\lambda_1 \in K$ P_f-nek egy gyöke és $v_1 \in V$, $v_1 \neq 0$ egy λ_1-hez tartozó sajátérték, azaz, $f(v_1) = \lambda_1 v_1$. Mivel $\{v_1\}$ lineárisan független, Steinitz tétele szerint e_1 kicserélhető v_1-el, és $u = (v_1, e_2, \ldots, e_n)$ bázis V-ben. Ebben a bázisban, az f mátrixa

$$[f]_{u,u} = \begin{pmatrix} \lambda_1 & a_{12} & a_{13} & \ldots & a_{1n} \\ 0 & a_{22} & a_{23} & \ldots & a_{2n} \\ 0 & a_{32} & a_{33} & \ldots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & a_{n3} & \ldots & a_{nn} \end{pmatrix}$$

alakú, ahol $f(v_1) = \lambda_1 v_1$, $f(e_j) = a_{1j} v_1 + \sum_{i=2}^{n} a_{ij} e_i$, $2 \le j \le n$. Tekintsük a $V_1 = \langle v_1 \rangle$ és a $V' = \langle e_2, \ldots, e_n \rangle$ résztereket, ahol $e' := (e_2, \ldots, e_n)$ bázis V'-ben. Ha $x \in V$ egy tetszőleges vektor, akkor léteznek az egyértelműen meghatározott $x_1, x_2, \ldots, x_n \in K$ koordináták, úgy, hogy

$$x = x_1 v_1 + x_2 e_2 + \cdots + x_n e_n = x_1 v_1 + x',$$

ahol $x_1 v_1 \in V_1$ és $x' \in V'$. Könnyen igazolható, hogy a $p : V \to V'$, $p(x) = x'$ függvény lineáris, tehát az

$$f' : V' \to V', \quad f'(x') = p(f(x'))$$

is lineáris.

Vegyük észre, hogy mivel $f'(e_j) = p(f(e_j)) = \sum_{i=2}^{n} a_{ij}e_i$, $2 \le j \le n$, következik, hogy

$$[f']_{e',e'} = \begin{pmatrix} a_{22} & a_{23} & \dots & a_{2n} \\ a_{32} & a_{33} & \dots & a_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ a_{n2} & a_{n3} & \dots & a_{nn} \end{pmatrix},$$

és

$$P_f(X) = \begin{pmatrix} \lambda_1 - X & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & a_{22} - X & a_{23} & \dots & a_{2n} \\ 0 & a_{32} & a_{33} - X & \dots & a_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & a_{n2} & a_{n3} & \dots & a_{nn} - X \end{pmatrix} = (\lambda_1 - X)P_{f'}(X),$$

tehát $P_{f'}$-nek $(n-1)$ gyöke van K-ban.

Mivel $\dim_K(V') = n - 1$ és $f' \in \mathrm{End}_K(V')$, az indukció hipotézisából következik, hogy létezik V'-ben egy $v' = (v_2, \dots, v_n)$ bázis úgy, hogy

$$[f']_{v',v'} = \begin{pmatrix} b_{22} & b_{23} & \dots & b_{2n} \\ b_{32} & b_{33} & \dots & b_{3n} \\ \vdots & \vdots & \ddots & \vdots \\ b_{n2} & b_{n3} & \dots & b_{nn} \end{pmatrix}$$

trianguláris mátrix. Végűl, $v := (v_1, v_2, \dots, v_n)$ bázis V-ben és

$$[f]_{v,v} = \begin{pmatrix} \lambda_1 & a_{12} & a_{13} & \dots & a_{1n} \\ 0 & b_{22} & b_{23} & \dots & b_{2n} \\ 0 & 0 & b_{33} & \dots & b_{3n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & b_{nn} \end{pmatrix} \qquad \blacksquare$$

2.55. feladat. A fenti tétel jelöléseivel, igazoljuk, hogy:
a) p és f' lineáris függvények;
b) v bázis, és ellenőrizzük az $[f]_{v,v}$ mátrixra vonatkozó egyenlőséget.

2.56. feladat. Adott az $f \in \mathrm{End}_{\mathbb{C}}(\mathbb{C}^n)$ endomorfizmus mátrixa a kanonikus bázisra vonatkozóan. Mindegyik esetben határozzunk meg egy olyan v bázist, amelyre $[f]_{v,v}$ trianguláris.

a) $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$; b) $\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$; c) $\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix}$; d) $\begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$;

e) $\begin{pmatrix} 0 & 1 & 1 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$; f) $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$; g) $\begin{pmatrix} 2 & 2 & 1 \\ 1 & 3 & 3 \\ 0 & 0 & 1 \end{pmatrix}$.

2.57. feladat. Legyen $A \in M_n(K)$ és fetételezzük, hogy $P_A(0) \neq 0$. Igazoljuk, hogy A invertálható, és

$$P_{A^{-1}}(X) = \frac{(-1)^n X^n}{P_A(0)} P_A(\frac{1}{X}).$$

2.58. feladat. Feltételezzük, hogy az $A \in M_n(K)$ mátrix sajátértékei $\lambda_1, \dots, \lambda_n$.
a) Határozzuk meg az A^{-1}, A^2 és A^m sajátértékeit.
b) Ha $p \in K[X]$, akkor $\det(p(A)) = \prod_{i=1}^{n} p(\lambda_i)$.
c) Ha $p \in K[X]$, $\lambda \in K$ sajátértéke A-nak és $x \in K^n$ sajátvektora A-nak, akkor $p(\lambda)$ sajátértéke és x sajátvektora $p(A)$-nak. Határozzuk meg az $p(A)$ sajátértékeit.

2.59. feladat. Bizonyítsuk be, hogy:
a) Minden trianguláris mátrix, amely főátlóján nullák vannak, nilpotens.
b) Ha az $f \in \mathrm{End}_K(V)$ karakterisztikus polinomja $(-1)^n X^n$, akkor f nilpotens.
c) Ha $A \in M_n(K)$ nilpotens, akkor a karakterisztikus polinomja $(-1)^n X^n$.
d) Adjunk példát olyan f lineáris operátorra, amely nem nilpotens, de 0 az egyetlen sajátértéke.
e) Ha $A \in M_n(K)$ idempotens, akkor az A minden sajátértéke egyenlő 0-val vagy 1-el.

2.4.3. Diagonalizálható endomorfizmusok

2.4.8. lemma. *Legyen* $f \in \mathrm{End}_K(V)$ *egy endomorfizmus.*

a) *Ha* $\lambda_0 \in K$ *sajátértéke az* f*-nek, akkor*

$$1 \le m_{\mathrm{geom}}(\lambda_0) \le m_{\mathrm{alg}}(\lambda_0).$$

b) *Feltételezzük, hogy* $\lambda_1, \dots, \lambda_m \in K$ $(m \le n)$ *páronként különböző sajátértékek, és legyen* v_i *egy a* λ_i*-hez tartozó sajátvektor,* $1 \le i \le m$*. Ekkor a* $(v_1, \dots, v_m)$ *rendszer lineárisan független.*

c) *Ha* f*-nek* n *különböző* $\lambda_1, \dots, \lambda_n \in K$ *sajátértéke van, és* v_i *egy a* λ_i*-hez tartozó sajátvektor,* $1 \le i \le n$*, akkor* $v := (v_1, \dots, v_n)$ *bázis, és*

$$[f]_{v,v} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$$

Bizonyítás. a) Legyen $r = \dim_K V(\lambda_0)$; $r \ge 1$ mert létezik egy λ_0-hoz tartozó (nemnulla) sajátvektor. Elég igazolni, hogy $(X - \lambda_0)^r$ osztja a $P_f(X)$ karakterisztikus polinomot.

Legyen $(v_1, \dots, v_r)$ $V(\lambda_0)$-nak egy bázisa. Steinitz tétele szerint, ezt a bázist ki lehet egészíteni egy $v = (v_1, \dots, v_r, e_{r+1}, \dots, e_n)$ V-beli bázisig. Vegyük észre, hogy az f mátrixa

$$[f]_{v,v} = \begin{pmatrix} \lambda_0 & 0 & \dots & 0 & a_{1,r+1} & \dots & a_{1n} \\ 0 & \lambda_0 & \dots & 0 & a_{2,r+1} & \dots & a_{2n} \\ \vdots & \vdots & \ddots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_0 & a_{r,r+1} & \dots & a_{rn} \\ \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 0 & 0 & \dots & 0 & a_{n,r+1} & \dots & a_{nn} \end{pmatrix}$$

alakú, tehát

$$P_f(X) = \det([f]_{v,v} - XI_n) = (\lambda_0 - X)^r Q(X),$$

ahol $Q(X)$ egy $K[X]$-beli polinom.

b) m-szerinti indukciót alkalmazunk. Ha $m = 1$, akkor, mivel $v_1 \ne 0$, következik, hogy $\{v\}$ lineárisan független.

Legyen $m > 1$, és feltételezzük, hogy az állítás igaz $m - 1$ sajátérték esetén. Legyen $a_1, \dots, a_n \in K$ úgy, hogy

$$a_1 v_1 + \dots + a_{m-1} v_{m-1} + a_m v_m = 0_V.$$

Mivel $f(v_i) = \lambda_i v_i$, következik, hogy

$$a_1 \lambda_1 v_1 + \dots + a_{m-1} \lambda_{m-1} v_{m-1} + a_m \lambda_m v_m = 0_V.$$

Ha az első egyenlőséget beszorozzuk $(-\lambda_m)$-el és az eredményt hozzáadjuk a másodikhoz, kapjuk, hogy

$$a_1(\lambda_1 - \lambda_m)v_1 + \dots + a_{m-1}(\lambda_{m-1} - \lambda_m)v_{m-1} = 0_V.$$

Az indukció hipotézisából következik, hogy $a_i(\lambda_i - \lambda_m) = 0$, $1 \le i \le m - 1$, tehát $a_1 = \dots = a_{m-1} = 0$, mert $\lambda_i \ne \lambda_m$, ha $i < m$. Végűl, $a_m v_m = 0_V$, tehát $a_m = 0$.

c) A b) pontból következik, hogy $v := (v_1, \dots, v_n)$ lineárisan független, tehát az alternatíva tétel szerint v bázis. Mivel $f(v_j) = \lambda_j v_j$, $1 \le j \le n$, következik, hogy

$$[f]_{v,v} = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}. \qquad \blacksquare$$

2.4.9. definíció. Azt mondjuk hogy az $f \in \mathrm{End}_K(V)$ endomorfizmus *diagonalizálható*, ha létezik egy $v = (v_1, \dots, v_n)$ bázis úgy, hogy az $[f]_{e,e} \in M_m(K)$ mátrix diagonális.

Jelölés: $\mathrm{diag}(\lambda_1, \dots, \lambda_n) = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}.$

2.4.10. tétel (diagonalizálható endomorfizmusok jellemzése). *Az* $f \in \mathrm{End}_K(V)$ *endomorfizmus akkor és csak akkor diagonalizálható, ha teljesíti a következő két feltételt:*
(1) *A* P_f *karakterisztikus polinomnak* n *gyöke van* K*-ban.*
(2) *Ha* λ *sajátértéke* f*-nek, akkor* $m_{\mathrm{geom}}(\lambda) = m_{\mathrm{alg}}(\lambda)$.

Bizonyítás. Feltételezzük, hogy f diagonalizálható, és legyen $e = (e_1, \dots, e_n)$ egy bázis úgy, hogy

$$[f]_{e,e} = \mathrm{diag}(\underbrace{\lambda_1, \dots, \lambda_1}_{r_1}, \underbrace{\lambda_2, \dots, \lambda_2}_{r_2}, \dots, \underbrace{\lambda_m, \dots, \lambda_m}_{r_m}),$$

ahol $1 \le r_i \le n$, $m \le n$, $r_1 + \dots + r_m = n$. Ekkor

$$P_f(X) = (\lambda_1 - X)^{r_1}(\lambda_2 - X)^{r_2} \dots (\lambda_m - X)^{r_m},$$

tehát P_f-nek n gyöke van K-ban, és $m_{\mathrm{alg}}(\lambda_i) = r_i \ge m_{\mathrm{geom}}(\lambda_i)$, $1 \le i \le m$. Elég igazolni, hogy $V(\lambda_i)$ tartalmaz r_i független vektort. Valóban, ezek a vektorok $e_{r_1+\dots+r_{i-1}+1}, \dots, e_{r_1+\dots+r_{i-1}+r_i}$; következik, hogy $\dim_K V(\lambda_i) \ge r_i$, tehát $m_{\mathrm{geom}}(\lambda_i) = m_{\mathrm{alg}}(\lambda_i)$.

Fordítva, feltételezzük, hogy az (1), (2) feltételek teljesülnek. Legyenek $\lambda_1, \dots, \lambda_m$ a P_f páronként különböző gyökei, és legyen

$$P_f(X) = (\lambda_1 - X)^{r_1}(\lambda_2 - X)^{r_2} \dots (\lambda_m - X)^{r_m},$$

ahol $1 \le r_i \le n$, $r_i = m_{\mathrm{alg}}(\lambda_i)$, és $\sum_{i=1}^m r_i = n$.

Mivel $m_{\mathrm{geom}}(\lambda_i) = m_{\mathrm{alg}}(\lambda_i) = r_i$, következik, hogy $V(\lambda_i)$-nek van egy $(v_{i1}, \dots, v_{ir_i})$ bázisa, $1 \le i \le m$. Igazoljuk, hogy

$$v := (v_{11}, \dots, v_{1r_1}, v_{21}, \dots, v_{2r_2}, \dots, v_{m1}, \dots, v_{mr_m})$$

bázis V-ben. Mivel a v rendszer n vektort tartalmaz, az alternatíva tétel szerint elég igazolni, hogy v lineárisan független. Feltételezzük, hogy

$$\underbrace{a_{11}v_{11} + \dots + a_{1r_1}v_{1r_1}}_{\in V(\lambda_1)} + \underbrace{a_{21}v_{21} + \dots + a_{2r_2}v_{2r_2}}_{\in V(\lambda_2)} + \dots + \underbrace{a_{m1}v_{m1} + \dots + a_{mr_m}v_{mr_m}}_{\in V(\lambda_m)} = 0.$$

A 2.4.8. lemma b) pontjaból következik, hogy

$$a_{i1}v_{i1} + \dots + a_{ir_1}v_{ir_1} = 0, \quad 1 \le i \le m,$$

tehát $a_{i1} = \dots = a_{ir_i} = 0$, $1 \le i \le m$. Végül, mivel $f(v_{ij}) = \lambda_i v_{ij}$, $1 \le j \le r_i$, $1 \le i \le m$, következik, hogy

$$[f]_{v,v} = \mathrm{diag}(\underbrace{\lambda_1, \dots, \lambda_1}_{r_1}, \underbrace{\lambda_2, \dots, \lambda_2}_{r_2}, \dots, \underbrace{\lambda_m, \dots, \lambda_m}_{r_m}). \qquad \blacksquare$$

2.4.11. példa. Legyen $f : \mathbb{R}^3 \to \mathbb{R}^3$, $[f]_{e,e} = A = \begin{pmatrix} 2 & 0 & -2 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}$. Ekkor $P_A(X) = (2 - X)(3 - X)^2$, tehát a P_A gyökei $\lambda_1 = 2$, $\lambda_2 = 3$, ahol $m_{\mathrm{alg}}(\lambda_1) = 1$, és $m_{\mathrm{alg}}(\lambda_2) = 2$.

$$\lambda_1 = 2 \Rightarrow \left\{ \begin{array}{rcl} 2x_3 & = & 0 \\ x_2 & = & 0 \\ x_3 & = & 0 \end{array} \right. \Leftrightarrow \left\{ \begin{array}{rcl} x_1 & = & \alpha \\ x_2 & = & 0 \\ x_3 & = & 0 \end{array} \right. \Rightarrow V(\lambda_1) = \left\langle \begin{pmatrix} 1 \\ 0 \\ 0 \end{pmatrix} \right\rangle,$$

tehát $m_{\mathrm{geom}}(\lambda_1) = 1 = m_{\mathrm{alg}}(\lambda_1)$.

$$\lambda_2 = 3 \Rightarrow -x_1 - 2x_3 = 0 \Leftrightarrow \left\{ \begin{array}{rcr} x_1 & = & -2\alpha \\ x_2 & = & \beta \\ x_3 & = & \alpha \end{array} \right. \Rightarrow V(\lambda_2) = \left\{ \begin{pmatrix} -2\alpha \\ \beta \\ \alpha \end{pmatrix} \mid \alpha,\ \beta \in \mathbb{R} \right\} = \left\langle \begin{pmatrix} -2 \\ 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \\ 0 \end{pmatrix} \right\rangle,$$

tehát $m_{\mathrm{geom}}(\lambda_2) = 2 = m_{\mathrm{alg}}(\lambda_2)$.

Következik, hogy a f diagonalizálható. Legyen $v = ((1,0,0),\ (-2,0,1),\ (0,1,0))$. Akkor

$$T := T_e^v = \begin{pmatrix} 1 & -2 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad T^{-1} = \begin{pmatrix} 1 & 0 & 2 \\ 0 & -1 & 1 \\ 0 & 1 & 0 \end{pmatrix}, \qquad [f]_v^v = T^{-1}AT = \begin{pmatrix} 2 & 0 & 0 \\ 0 & 3 & 0 \\ 0 & 0 & 3 \end{pmatrix}.$$

2.60. feladat. Diagonalizálhatók-e a következő mátrixok ($\mathbb{C}$-fölött)? Ha igen, akkor határozzuk meg az új bázist és az áttérési mátrixot.

a) $\begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$; b) $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 1 & 0 & 0 \end{pmatrix}$; c) $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}$; d) $\begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{pmatrix}$;

e) $\begin{pmatrix} 4 & -3 & 1 & 2 \\ 5 & -8 & 5 & 4 \\ 6 & -12 & 8 & 5 \\ 1 & -3 & 2 & 2 \end{pmatrix}$; f) $\begin{pmatrix} 0 & 0 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{pmatrix}$; g) $\begin{pmatrix} 1 & 1 & 0 & 2 \\ 1 & -1 & 0 & 2 \\ 0 & 0 & 2 & 3 \\ 0 & 0 & 0 & 2 \end{pmatrix}$.

2.61. feladat. Igazoljuk, hogy a

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

mátrix $\mathbb{C}$ fölött diagonalizálható, de $\mathbb{R}$ fölött nem.

2.62. feladat. Legyen $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{R})$. Igazoljuk, hogy:

a) Ha $\mathrm{Tr}(A)^2 - 4\det A > 0$, akkor A diagonalizálható.

b) Ha $\mathrm{Tr}(A)^2 - 4\det A = 0$, akkor A diagonalizálható $\Leftrightarrow$ A diagonális.

c) Ha $\mathrm{Tr}(A)^2 - 4\det A < 0$, akkor A nem diagonalizálható. Ebben az esetben létezik $T \in GL_2(\mathbb{C})$ úgy, hogy $T^{-1}AT = \begin{pmatrix} \alpha_1 & 0 \\ 0 & \alpha_2 \end{pmatrix} \in M_2(\mathbb{C})$.

d) Tanulmányozzuk az $A = \begin{pmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{pmatrix}$ mátrixot, ahol $t \in \mathbb{R}$.

2.4.4. Jordan-féle kanonikus alak

Legyen $\dim_K V = n$, $e = \{e_1, \dots, e_n\}$ bázis V-ben, $f \in \mathrm{End}_K(V)$, $A = [f]_{e,e}$, és feltételezzük, hogy a $P_f(X)$ karakterisztikus polinomnak n gyöke van K-ban.

Az alábbiakban bebizonyítjuk, hogy létezik ν bázis V-ben úgy, hogy

$$[f]_{\nu,\nu} = J_1 \oplus J_2 \oplus \cdots \oplus J_k := \begin{pmatrix} J_1 & 0 & \dots & 0 \\ 0 & J_2 & \dots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \dots & J_k \end{pmatrix}$$

ahol J_i négyzetmátrix amely $(\lambda) \in M_1(K)$ alakú, vagy

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

alakú, ahol λ sajátértékre f-nek.

2.4.12. definíció. a) A fenti J_i mátrixot λ-nak megfelelő **Jordan-blokk**nak nevezzünk[1].

b) Azt mondjuk, hogy $[f]_{\nu,\nu} = J_1 \oplus J_2 \oplus \dots \oplus J_k$ az f endomorfizmus (vagy az A mátrix) **Jordan-féle kanonikus alakja** (vagy **Jordan-féle normálalakja**).

c) A ν bázist f-nek megfelelő **Jordan-féle kanonikus bázis**nak nevezzük.

Ebben a paragrafusban a mátrixok és endomorfizmusok Jordan-féle kanonikus alakjának létezését és egyértelműségét mutatjuk be.

[1] Camille Jordan (1838-1922) francia matematikus, az École Polytechnique és a Collége de France tanára volt. 1881-től a Francia Tudományos Akadémia tagja. 1870-ben adta ki a "Traité de substitutions et des équations algébriques" című könyvét a permutációcsoportokról és az egyenletek Galois-elméletről. 1882-1887 között adta ki a háromkötetes "Cours d'analyse" című munkáját. Jordan nagy mértékben hozzájárult az abban az időben tanulmányozott matematikai kérdések megoldásában, és az előadásai nagy hatással voltak más matematikusokra.

2.4.13. megjegyzés. 1) Ha J az A mátrix Jordan-féle kanonikus alakja, akkor J és A hasonló mátrixok, azaz ha ν egy f-nek megfelelő Jordan-féle kanonikus bázis és $T = T_e^\nu$, akkor $J = T^{-1}AT$.

2) $[f]_{\nu,\nu}$ diagonális mátrix akkor és csak akkor, ha minden J_i Jordan blokk $(\lambda) \in M_1(K)$ alakú. Minden diagonális mátrix Jordan-féle kanonikus alakú.

3) Legyen $f : \mathbb{Q}^8 \to \mathbb{Q}^8$, $[f]_{\nu,\nu} = J$, ahol

$$J = J_1 \oplus J_2 \oplus J_3 \oplus J_4 = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

kanonikus alakú, és $\nu = \{x_1, x_2, \dots, x_8\}$. Ekkor $P_f(X) = P_J(X) = \det(J - XI) = (X-2)^4(X-3)^2X^2$. Az $x_1, \dots, x_8$ vektorok közül csak x_1, x_4, x_5 és x_7 (a bázis vektorok melyek megfelelnek a J_1, J_2, J_3 illetve J_4 Jordan blokkok első oszlopainak) sajátvektorai J-nek.

4) A karakterisztikus polinomok nem határozza meg a Jordan-féle kanonikus alakot. Például a

$$J' = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 3 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}$$

mátrix karakterisztikus polinomja ugyancsak $(X-2)^4(X-3)^2X^2$.

Általánosított sajátvektorok

2.4.14. megjegyzés. Tekintsük újból a J mátrixot. Láttuk, hogy az x_1 és x_4 sajátvektorok a $\lambda_1 = 2$ sajátértékhez tartóznak, de x_2 és x_3 nem sajátvektorok, mert $(f - 2\mathbf{1}_V)(x_1) = (f - 2\mathbf{1}_V)(x_4) = 0$, miközben $(f - 2\mathbf{1}_V)(x_2) \neq 0$ és $(f - 2\mathbf{1}_V)(x_3) \neq 0$. Mivel $f(x_2) = x_1 + 2x_2$ és $f(x_3) = x_2 + x_3$, kapjuk, hogy

$$(f - 2\mathbf{1}_V)^2(x_2) = (f - 2\mathbf{1}_V)(f(x_2) - 2x_2) = (f - 2\mathbf{1}_V)(x_1) = 0,$$

$$(f - 2\mathbf{1}_V)^3(x_3) = (f - 2\mathbf{1}_V)^2(f(x_3) - 2x_3) = (f - 2\mathbf{1}_V)^2(x_2) = 0.$$

Tehát $(f - 2\mathbf{1}_V)(x_2) \neq 0$, $(f - 2\mathbf{1}_V)(x_3) \neq 0$, de $(f - 2\mathbf{1}_V)^p(x_2) = (f - 2\mathbf{1}_V)^p(x_3) = 0$, ha $p \geq 3$.

2.4.15. definíció. Azt mondjuk, hogy $x \in V \setminus \{0\}$ a λ skalárhoz tartozó **általánosított sajátvektor**a f-nek, ha létezik egy $p > 1$ egész szám úgy, hogy $(f - \lambda\mathbf{1}_V)^p(x) = 0$.

2.4.16. megjegyzés. 1) Ha x egy λ-hoz tartozó általánosított sajátvektora f-nek, akkor λ sajátértéke f-nek. Valóban, ha p a legkisebb pozitív egész szám, amelyre $(f - \lambda\mathbf{1}_V)^p(x) = 0$, akkor $y := (f - \lambda\mathbf{1}_V)^{p-1}(x)$ a λ sajátértékhez tartozó sajátvektora f-nek.

2) Ha ν Jordan-féle kanonikus bázis V-ben, akkor a ν elemei sajátvektorai vagy általánosított sajátvektorai f-nek.

2.4.17. definíció. Legyen x a λ sajátértékhez tartozó általánosított sajátvektora f-nek, és legyen p a legkisebb pozitív egész szám úgy hogy $(f - \lambda\mathbf{1}_V)^p(x) = 0$. Akkor az

$$(f - \lambda\mathbf{1}_V)^{p-1}(x), (f - \lambda\mathbf{1}_V)^{p-2}(x), \dots, (f - \lambda\mathbf{1}_V)(x), x$$

vektorrendszert f-nek megfelelő λ-hoz tartozó **ciklus**nak nevezzük, melynek $(f - \lambda\mathbf{1}_V)^{p-1}(x)$ a **kezdővektora** és x a **végvektora**. Azt mondjuk, hogy a ciklus **hossza** p.

2.4.18. példa. Az előző J mátrix esetén, látjuk hogy $\nu_1 = \{x_1, x_2, x_3\}$, $\nu_2 = \{x_4\}$, $\beta_3 = \{x_5, x_6\}$, $\beta_4 = \{x_7, x_8\}$ a 2, 2, 3 illetve 0 sajátértékekhez tartozó ciklusok. Legyen $W_i := \langle \nu_i \rangle \leq_{\mathbb{Q}} V$, $i = 1, \dots, 4$. Mivel $f(x_1) = 2x_1$, $f(x_2) = x_1 + 2x_2$, és $T(x_3) = x_2 + 2x_3$, következik, hogy W_1 f-invarians résztér. Ugyanígy W_2, W_3 és W_4 is f-invariáns részterek. Könnyű belátni, hogy $[f_{|W_i}]_{\nu_i,\nu_i} = J_i$, $i = 1, \dots, 4$.

2.4.19. lemma. *Legyen w egy a λ sajátértékhez tartozó ciklusa f-nek, és legyen v egy bázis V-ben.*
1) *A w kezdővektora λ-hoz tartozó sajátvektora f-nek.*
2) *w lineárisan független.*
3) *v Jordan-féle kanonikus bázis akkor és csak akkor, ha v diszjunkt ciklusok egyesítése.*

Bizonyítás. 1) lásd a 2.4.16. 1) megjegyzést.

2) Indukció a w ciklus hossza szerint. Ha a w hossza 1, akkor $v = \{x_1\}$ lineárisan független, mert az $x_1 \neq 0$. Feltételezzük, hogy $k > 1$ és a $k-1$ hosszúságú ciklusok lineárisan függetlenek.

Legyen $w = \{x_1, x_2, \ldots, x_k\}$, és tételezzük fel, hogy $\sum_{i=1}^{k} a_i x_i = 0$, ahol $a_1, a_2, \ldots, a_k \in K$. Mivel $(f - \lambda 1_V)(x_i) = x_{i-1}$, kapjuk $\sum_{i=2}^{k} a_i x_{i-1} = 0$. De $\{x_1, x_2, \ldots, x_{k-1}\}$ $(k-1)$ hosszúságú ciklus, tehát $a_i = 0$, $i = 2, 3, \ldots, k$. Következik, hogy $a_1 x_1 = 0$. De $x_1 \neq 0$, tehát $a_1 = 0$.

A 3) állítást az olvasóra bizzuk. ■

2.4.20. definíció. Legyen λ sajátérték f-nek. Az f transzformáció λ-hoz tartozó **általánosított sajátrésztere** a következő halmaz:

$$\widetilde{V(\lambda)} = \{x \in V \mid \exists p \in \mathbb{N}^* : \ (f - \lambda 1_V)^p(x) = 0\}.$$

2.4.21. lemma. *Legyen λ sajátétéke f-nek. Akkor $\widetilde{V(\lambda)}$ résztere V-nek, amely tartalmazza a $V(\lambda)$ sajátrésztért.*

Bizonyítás. Evidens, hogy $0 \in \widetilde{V(\lambda)}$. Tételezzük fel, hogy $x, y \in \widetilde{V(\lambda)}$; akkor léteznek p és q pozitív egész számok úgy, hogy $(f - \lambda 1_V)^p(x) = 0$ és $(f - \lambda 1_V)^q(y) = 0$. Most

$$\begin{aligned}
(f - \lambda 1_V)^{p+q}(x + y) &= (f - \lambda 1_V)^p(x) + (f - \lambda 1_V)^q(y) \\
&= (f - \lambda 1_V)^q(f - \lambda 1_V)^p(x) + (f - \lambda 1_V)^p(f - \lambda 1_V)^q(y) \\
&= (f - \lambda 1_V)^q(0) + (f - \lambda 1_V)^p(0) = 0,
\end{aligned}$$

tehát $x + y \in \widetilde{V(\lambda)}$. Végül, $\forall a \in K$

$$(f - \lambda 1_V)^p(ax) = a(f - \lambda 1_V)^p(x) = 0,$$

tehát $ax \in \widetilde{V(\lambda)}$. Nyilván $V(\lambda) = \mathrm{Ker}(f - \lambda 1_V) \subseteq \widetilde{V(\lambda)}$.

Másképpen, vegyük észre, hogy $\widetilde{V(\lambda)} = \bigcup_{p \in \mathbb{N}^*} \mathrm{Ker}(f - \lambda 1_V)^p$, és $\mathrm{Ker}(f - \lambda 1_V)^p \subseteq \mathrm{Ker}(f - \lambda 1_V)^{p+1}$. ■

2.4.22. lemma. *Legyenek $\lambda_1, \lambda_2, \ldots, \lambda_m$ az f páronként különböző sajátértékei. Akkor minden $i = 1, \ldots, m$ esetén*

$$\widetilde{V(\lambda_i)} \cap (\sum_{j \neq 1} \widetilde{V(\lambda_j)}) = \{0\}.$$

Bizonyítás. Az egyszerűség kedvéért feltételezzük, hogy $i = 1$. Feltételezzük, hogy

$$a_2 x_2 + \cdots + a_m x_m = x_1$$

ahol $x_j \in \widetilde{V(\lambda_j)}$, $1 \leq j \leq m$. Legyen p_j, $(1 \leq j \leq m)$ a legkisebb pozitív egész szám úgy, hogy $(f - \lambda_j 1_V)^{p_j}(x_j) = 0$. Tegyük fel, hogy $x_1 \neq 0$, tehát $(f - \lambda_1 1_V)^{p_1 - 1}(x_1) \neq 0$ λ_1-hez tartozó sajátvektor. Kapjuk, hogy

$$\begin{aligned}
0 &= (f - \lambda_1 1_V)^{p_1 - 1}(f - \lambda_2 1_V)^{p_2} \ldots (f - \lambda_m 1_V)^{p_m}(x_1) \\
&= (f - \lambda_2 1_V)^{p_2} \ldots (f - \lambda_m 1_V)^{p_m}((f - \lambda_1 1_V)^{p_1 - 1}(x_1)) \\
&= (\lambda_1 - \lambda_2)^{p_2} \ldots (\lambda_1 - \lambda_m)^{p_m}(f - \lambda_1 1_V)^{p_1 - 1}(x_1).
\end{aligned}$$

Mivel $\lambda_1, \ldots, \lambda_m$ különbözőek, következik, hogy $(f - \lambda_1 1_V)^{p_1 - 1}(x_1) = 0$, ellentmondás. Tehát $x_1 = 0$. ■

2.4.23. lemma. *Legyenek S_i, $i = 1, \ldots, k$ ciklusai f-nek amelyek a λ sajátértékhez tartoznak. Legyen p_i és y_i az S_i hossza, illetve kezdővektora. Ha $\{y_1, \ldots y_k\}$ lineárisan független halmaz, akkor $S := \bigcup_{i=1}^{k} S_i$ lineárisan független halmaz, amely $\sum_{i=1}^{k} p_i$ vektort tartalmaz.*

Bizonyítás. Tegyük fel, hogy $p_1 \geq p_2 \geq \ldots \geq p_k$. A bizonyitás indukció p_1 szerint. Ha $p_1 = 1$, akkor $p_1 = \cdots = p_k = 1$. Tehát minden S_i ciklus tartalmaz csak egy elemet, és ahipotézis szerint $\bigcup_{i=1}^{k} S_i = \{y_1, \ldots, y_k\}$ lineárisan független halmaz, amely $\sum_{i=1}^{k} p_i = k$ elemet tartalmaz.

Most tegyük fel, hogy a tétel igaz ha $1 \leq p_1 < n$. Tegyük fel, hogy $n = p_1 \geq p_2 \geq \ldots \geq p_k$ és legyen r úgy, hogy $1 < r \leq k$ és $p_r > 1$. Legyen S_i' az a ciklus, amelyet úgy kapunk, hogy eltávolítjuk az utolsó x_i vektort S_i-ből. Akkor S_i' λ-hoz tartozó $p_i - 1$ hosszúságú ciklus y_i kezdővektorral. Mivel $\{y_1, y_2, \ldots, y_k\}$ lineárisan független, az indukció hipotézisa szerint $S' := \bigcup_{i=1}^{r} S_i'$ lineárisan független halmaz, amely $\sum_{i=1}^{r}(p_i - 1)$ vektort tartalmaz.

Következik, hogy $S = S' \cup \{x_1, \dots, x_k\}$ diszjunkt egyesítés, tehát S tartalmaz $\sum_{i=1}^{r}(p_i - 1) + k = \sum_{i=1}^{k}(p_i - 1) + k = \sum_{i=1}^{k} p_i$ vektort.

Ki kell mutassuk, hogy S lineárisan független halmaz. Tegyük fel, hogy $\sum_{z \in S} a_z z = 0$. Mivel $(f - \lambda 1_V)(y_i) = 0$, $i = 1, \dots, k$, kapjuk, hogy

$$0 = \sum_{z \in S} a_z (f - \lambda 1_V)(z) = \sum_{z \in Z} a_z (f - \lambda 1_V)(z),$$

ahol $S'' = \{v \in S \mid v \neq y_i,\ 1 \leq i \leq k\}$. De a fenti összeg lineáris kombinációja az S' elemeinek. Mivel S' lineárisan független, következik, hogy minden $z \in S''$ esetén $a_z = 0$. Tehát a fenti egyenlet egyenlet lineáris kombinációja $\{y_1, \dots, y_k\}$-nak, amely lineárisan független, hipotézis szerint. Tehát minden a_z együttható egyenlő nullával. ■

2.4.24. tétel (Jordan-féle kanonikus bázis létezése). *Legyen $f \in \mathrm{End}_K(V)$ és feltételezzük, hogy a $P_f(X)$ karakterisztikus polinomnak n gyöke van K-ban, ahol $\dim_K V = n$. Akkor V-ben létezik f-nek megfelelő Jordan-féle kanonikus v bázis, amely diszjunkt egyesítése az f sajátvektoraihoz tartozó ciklusoknak.*

Bizonyítás. A bizonyítás indukció n szerint. Ha $n = 1$, az állítás igaz, mivel minden 1×1-es mátrix Jordan-féle kanonikus alakú. Tételezzük fel, hogy az állítás igaz n-nél kisebb dimenziójú vektorterek esetén, ahol $n > 1$.

1. eset. $\dim_K \mathrm{Im}(f) < n$. Mivel $\mathrm{Im}(f)$ f-invariáns résztere V-nek (azaz $f(\mathrm{Im} f) \subseteq \mathrm{Im} f$), definiálhatjuk az $f_1 = f_{|\mathrm{Im} f} : \mathrm{Im} f \to \mathrm{Im} f$ leszűkítést. Ekkor f_1-re alkalmazva az indukció hipotézisát következik, hogy létezik f_1-nek megfelelő w Jordan-féle kanonikus bázis $\mathrm{Im} f$-ben, amely r elemet tartalmaz, ahol $r < n$. A 2.4.19. 3) lemma alapján w diszjunkt ciklosok egyesítése. Legyenek $S_1, S_2, \dots, S_k$ a w-beli ciklusok, amelyek a 0 sajátértékhez tartoznak, és legyen y_i és w_i az első és utolsó vektora S_i-nek. Mivel $w_i \in w \subseteq \mathrm{Im} f$, létezik $x_i \in V$ úgy, hogy $f(x_i) = w_i$. Legyen $Y := \{y_1, y_2, \dots, y_k\}$, $X := \{x_1, x_2, \dots, x_k\}$, és $w_0 := \bigcup_{i=1}^{k} S_i$. Tegyük fel, hogy w_0 p elemet tartalmaz, ahol $p \leq r$. A 2.4.19 1) lemma alapján minden y_i 0-hoz tartozó sajátvektor, tehát $Y \subseteq \mathrm{Ker} f$. Mivel Y lineárisan független, kiterjeszthető egy $Y \cup Z$ $\mathrm{Ker} f$-beli bázisra. Itt $|Z| = n - r - k$, mivel $\dim \mathrm{Ker} f = n - \dim \mathrm{Im} f = n - r$. Legyen $S_i' := S_i \cup \{x_i\}$; akkor S_i' f-nek megfelelő 0-hoz tartozó ciklus, és y_i a kezdővektora. Mi több, ha $z \in Z$, akkor $\{z\}$ a nulla sajátértékhez tartozó ciklus. Akkor az előző lemma szerint $(\bigcup_{i=1}^{k} S_i') \cup Z = (\gamma_0 \cup X) \cup Z$ lineárisan független halmaz, amely $p + k + (n - r - k) = n - (r - p)$ elemet tartalmaz, mivel $Y \cup Z$ lineárisan független halmaz amely 0-hoz tartozó ciklusok kezd H ovektorait tartalmaz.

Bebizonyítjuk, hogy $v := \gamma \cup X \cup Z$ a keresett bázis. Ha $w_0 = w$ (azaz $p = r$), akkor $v = w_0 \cup X \cup Z$ lineárisan független halmaz, amely $n - (r - p) = n$ elemet tartalmaz. Tehát v bázis f-ben. Ha pedig $w_0 \neq w$, akkor $w' := \{x \in w \mid x \notin w_0\}$ a $\lambda_2, \dots, \lambda_m$ nem nulla sajátértékekhez tartozó diszjunkt ciklusok egyesítése. Tegyük fel, hogy

$$0 = \sum_{x \in v} a_x x = \sum_{x \in w_0 \cup X \cup Z} a_x x + \sum_{x \in w'} a_x x.$$

Akkor $\sum_{x \in w_0 \cup X \cup Z}(-a_x x) = \sum_{x \in w'} a_x x$. De a baloldal $\widetilde{V(\lambda_1)}$-beli elem, ahol $\lambda_1 = 0$, és a jobboldal $\widetilde{V(\lambda_2)} + \dots + \widetilde{V(\lambda_m)}$-beli elem. A 2.4.22 tétel alapján mindkét oldal egyenlő 0-val. Mivel $w_0 \cup X \cup Z$ és w' lineárisan független halmazok következik, hogy $a_x = 0$ minden $x \in v$ esetén. Tehát v lineárisan független, és mivel $v = w \cup X \cup Z$ tartalmaz $r + k + (n - r - k) = n$ elemet, v bázisa V-nek. Mivel v diszjunkt egyesítése az f-nek megfelelő ciklusoknak, következik, hogy v Jordan-féle kanonikus bázis, a 2.4.19. lemma alapján.

2. eset. $\dim_K \mathrm{Im}(f) < n$. Legyen λ sajátértéke f-nek. Alkalmazzuk az 1. esetet az $f - \lambda 1_V$ nem invertálható endomorfizmusra. Kepunk egy v bázist V-ben úgy, hogy $[f - \lambda 1_V]_{v,v} =: J$ Jordan-féle kanonikus mátrix. De akkor $[f]_{v,v} = J + \lambda 1_V$ is Jordan-féle kanonikus mátrix. ■

2.4.25. tétel. *Legyenek $\lambda_1, \dots, \lambda_m$ az f páronként különböző sajátértékei és legyen r_i a λ_i algebrai multiplicitása. Legyen v egy f-nek megfelelő Jordan-féle kanonikus bázis V-ben, és legyen $v_i := v \cap \widetilde{V(\lambda_i)}$, $i = 1, \dots, m$. Akkor:*

1) *Minden $x \in V$ esetén léteznek az egyértelműen meghatározott $x_i \in \widetilde{V(\lambda_i)}$ vektorok, $i = 1, \dots, m$, úgy, hogy $x = x_1 + \dots + x_m$.*

Azt mondjuk, hogy V a $\widetilde{V(\lambda_1)}, \dots \widetilde{V(\lambda_m)}$ részterek **direkt összege**, és a következőképpen jelöljük:

$$V = \widetilde{V(\lambda_1)} \oplus \dots \oplus \widetilde{V(\lambda_m)}.$$

2) *v_i bázisa $\widetilde{V(\lambda_i)}$-nek. Fordítva, ha w_i olyan λ_i-hez tartozó ciklusok egyesítése, amely bázisa $\widetilde{V(\lambda_i)}$-nek, akkor $\bigcup_{i=1}^{k} w_i$ f-nek megfelelő Jordan-féle kanonikus bázis V-ben.*

3) *$\widetilde{V(\lambda_i)} = \mathrm{Ker}(f - \lambda_i 1_V)^{r_i}$ f-invariáns résztere V-nek, és $\dim_K \widetilde{V(\lambda_i)} = r_i$.*

4) *f diagonalizálható akkor és csak akkor, ha $V(\lambda_i) = \widetilde{V(\lambda_i)}$, minden $i = 1, \dots, m$ esetén.*

Bizonyítás. 1) Nyilván $\langle v_i \rangle \subseteq \widetilde{V(\lambda_i)}$. Mivel $\langle \bigcup_{i=1}^{m} v_i \rangle = \langle v \rangle = V$, következik, hogy $\widetilde{V(\lambda_1)} + \dots + \widetilde{V(\lambda_m)} = V$. Az egyértelműség következik a 2.4.22 lemmából.

2) Legyen $W_i := \langle v_i \rangle$. Akkor $W_i \subseteq \widetilde{V(\lambda_i)}$ és $\dim_K W_i \leq \dim(K_{\lambda_i})$. Mivel v egyesítése a $v_1, \dots, v_m$ diszjunkt halmazoknak, és $\langle v \rangle = V$, következik, hogy $V = W_1 \oplus \cdots \oplus W_m$. Az 1) pont szerint

$$\dim_K V = \sum_{i=1}^{m} \dim_K W_i \leq \sum_{i=1}^{m} \dim_K \widetilde{V(\lambda_i)} = \dim_K V.$$

Tehát $\dim_K W_i = \dim_K \widetilde{V(\lambda_i)}$. Mivel $W_i \subseteq \widetilde{V(\lambda_i)}$ és $\dim_K W_i = \dim_K \widetilde{V(\lambda_i)}$, következik, hogy $\langle v_i \rangle = W_i = \widetilde{V(\lambda_i)}$. Mivel v_i lineárisan független (mert részhalmaza v-nek), v_i bázisa $\widetilde{V(\lambda_i)}$-nek.

3) Tudjuk, hogy $\widetilde{V(\lambda_i)}$ résztere V-nek, és v_i bázisa $\widetilde{V(\lambda_i)}$-nek, amely λ_i-hez tartozó ciklusok egyesítése. De egy ciklus bármely vektorának a képe lineáris kombinációja a ciklus vektorainak, tehát eleme $\widetilde{V(\lambda_i)}$-nek. Tehát $f(v_i) \subseteq \widetilde{V(\lambda_i)}$, bebizonyítva, hogy $\widetilde{V(\lambda_i)}$ f-invariáns.

Legyen f_i az f leszűkítése $\widetilde{V(\lambda_i)}$-re. A 2) pont alapján $A_i := [f_i]_{v_i, v_i}$ Jordan-féle kanonikus alakja f_i-nek és $[f]_{v,v} = A_1 \oplus \cdots \oplus A_m$. Ha $n_i := \dim_K \widetilde{V(\lambda_i)}$, akkor az f_i karakterisztikus polinomja $\det(A_i - XI_{n_i}) = (\lambda_i - X)^{n_i}$, mert $A_i - XI_{n_i}$ trianguláris mátrix, amelynek átlóin $\lambda_i - X$ szerepel. Akkor

$$P_f(X) = (\lambda_1 - X)^{n_1} \dots (\lambda_k - X)^{n_k},$$

tehát $r_i = n_i = \dim_K \widetilde{V(\lambda_i)}$.

Nilván $\operatorname{Ker}(f - \lambda_i \mathbf{1}_V)^{m_i} \subseteq \widetilde{V(\lambda_i)}$. Legyen $x \in \widetilde{V(\lambda_i)}$. Akkor az S ciklus amelynek x az végvektora lineárisan független részhalmaza $\widetilde{V(\lambda_i)}$-nek. Mivel $\dim_K \widetilde{V(\lambda_i)} = r_i$, következik, hogy az S hossza nem lehet nagyobb m_i-nél; tehát létezik $p \leq m_i$ pozitív egész úgy, hogy $(f - \lambda_i \mathbf{1}_V)^p(x) = 0$. Tehát $x \in \operatorname{Ker}(f - \lambda_i \mathbf{1}_V)^{m_i}$, bebizonyitva, hogy $\widetilde{V(\lambda_i)} = \operatorname{Ker}(f - \lambda_i \mathbf{1}_V)^{m_i}$.

4) Ha $V(\lambda_i) = \widetilde{V(\lambda_i)}$ bármely i-re, akkor az 1) pont alapján

$$V(\lambda_1) \oplus \cdots \oplus V(\lambda_m) = \widetilde{V(\lambda_1)} \oplus \cdots \oplus \widetilde{V(\lambda_m)} = V,$$

tehát f diagonalizálható.

Fordítva, ha f diagonalizálható, akkor $\dim_K V(\lambda_i) = r_i$. De mivel $V(\lambda_i)$ résztere $\widetilde{V(\lambda_i)}$-nek és $\dim_K \widetilde{V(\lambda_i)} = r_i$ következik a 3) pont alapján, hogy $V(\lambda_i) = \widetilde{V(\lambda_i)}$, bármely $i = 1, \dots, m$ esetén. ■

2.4.26. példa. Határozzuk meg a következő endomorfizmusok sajátrésztereit és általánosított sajátrésztereit.

a) Legyen $f : \mathbb{R}^3 \to \mathbb{R}^3$, ahol

$$[f_{e,e}] = A = \begin{pmatrix} 3 & 1 & -2 \\ -1 & 0 & 5 \\ -1 & -1 & 4 \end{pmatrix}.$$

Az A karakterisztikus polinomja $P_A(X) = \det(A - XI) = -(X-3)(X-2)^2$. Tehát $\lambda_1 = 3$ és $\lambda_2 = 2$ az f sajátértékei, 1 és 2 algebrai multiplicitással. A 2.4.25. tétel alapján $\dim_K \widetilde{V(\lambda_1)} = 1$, $\dim_K \widetilde{V(\lambda_2)} = 2$, $\widetilde{V(\lambda_1)} = \operatorname{Ker}(f - 3\mathbf{1}_V)$ és $\widetilde{V(\lambda_2)} = \operatorname{Ker}(f - 2\mathbf{1}_V)^2$.

Kapjuk, hogy $\{(-1, 2, 1)\}$ bázisa $\widetilde{V(\lambda_1)} = V(\lambda_1)$-nek. Hasonlóan $\{(1, -3, -1)\}$ bázisa $V(\lambda_2)$-nek. Továbbá

$$(A - 2I)^2 = \begin{pmatrix} 2 & 1 & -1 \\ -4 & -2 & 2 \\ -2 & -1 & 1 \end{pmatrix}.$$

A $\widetilde{V(\lambda_2)}$ meghatározása ekvivalens a következő homogén egyenletrendszerrel:

$$\begin{cases} 2x_1 + x_2 - x_3 & = 0 \\ -4x_1 - 2x_2 + 2x_3 & = 0 \\ -2x_1 - x_2 + x_3 & = 0. \end{cases}.$$

Kapjuk, hogy $\{(1, -3, -1), (-1, 2, 0)\}$ bázis $\widetilde{V(\lambda_2)}$-ben. Észrevesszük, hogy ez a bázis λ_2-höz tartozó ciklus. Az 2.4.25. tétel 2) pontja alapján $v := \{(-1, 2, 1), (1, -3, -1), (-1, 2, 0)\}$ bázisa $\mathbb{R}^3$-nak, és

$$[f]_{v,v} = \begin{pmatrix} 3 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}$$

Jordan-féle kanonikus alakja f-nek.

2.4.27. példa. Legyen $f : \mathbb{C}_2[X] \to \mathbb{C}_2[X]$, $f(P) = -P - P'$. Akkor $e := \{1, X, X^2\}$ kanonikus bázis $V = \mathbb{C}_2[X]$-ben, és

$$A := [f]_{e,e} = \begin{pmatrix} -1 & -1 & 0 \\ 0 & -1 & -2 \\ 0 & 0 & -1 \end{pmatrix}.$$

Az f karakterisztikus polinomja $P_f(X) = \det(A - XI) = -(X+1)^3$. Tehát $\lambda = -1$ az f egyetlen sajátértéke, és $\widetilde{V(\lambda)} = \mathbb{C}_2[X]$ a 2.4.25. tétel alapján. Továbbá $V(\lambda) = \mathrm{Ker}(f - \lambda \mathbf{1}_V) = \mathrm{Ker}(f + \mathbf{1}_V)$. Ha $P = a + bX + cX^2 \in \mathbb{C}_2[X]$, akkor $P \in V(\lambda)$ akkor és csak akkor, ha

$$0 = f(P) + P = (-(a + bX + cX^2) - (b + 2cX)) + (a + bX + cX^2) = -(b + 2cX).$$

De $-(b + 2cX) = 0$ akkor és csak akkor, ha $b = c = 0$. Innen $P \in V(\lambda)$ akkor és csak akkor, ha $P = a$ konstans polinom, tehát $\{1\}$ bázisa $V(\lambda)$-nak. Vegyük észre, hogy $v := \{2, -2X, X^2\}$ l-hoz tartozó ciklus, és

$$[f]_{v,v} = \begin{pmatrix} -1 & 1 & 0 \\ 0 & -1 & 1 \\ 0 & 0 & -1 \end{pmatrix}$$

Jordan-féle kanonikus alakja f-nek.

2.63. feladat. Határozzuk meg a következő mátrixok endomorfizmusok sajátrésztereit és általánosított sajátrésztereit:

a) $A = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$; b) $A = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$; c) $A = \begin{pmatrix} 11 & -4 & -5 \\ 21 & -8 & -11 \\ 3 & -1 & 0 \end{pmatrix}$;

d) $f : \mathbb{C}_2[X] \to \mathbb{C}_2[X]$, $f(P) = 2P - P'$; e) $f : \mathbb{C}_2[X] \to \mathbb{C}_2[X]$, $f(P) = P - 2P'$.

2.64. feladat. Legyen $[f]_{v,v} = J_1 \oplus J_2 \oplus \ldots \oplus J_k$, ahol J_i Jordan-blokk. Legyen λ sajátértéke f-nek, és legyen s azon Jordan-blokkok száma, amelyek főátlóján λ van. Bizonyítsuk be, hogy $1 \le s \le \dim_K V(\lambda)$.

2.65. feladat. Legyen $f \in \mathrm{End}_K(V)$, λ sajátértéke f-nek és $k \in \mathbb{N}^*$. Bizonyítsuk be, hogy:

a) $\mathrm{Ker}(f^k) \subseteq \mathrm{Ker}(f^{k+1})$.

b) Ha $\mathrm{rang}(f^f) = \mathrm{rang}(f^{k+1})$, akkor $\mathrm{rang}(f^i) = \mathrm{rang}(f^k)$ és $\mathrm{Ker}(f^i) = \mathrm{Ker}(f^k)$ bármely $i \ge k$ esetén.

c) Ha $\mathrm{rang}((f - \lambda \mathbf{1}_V)^k) = \mathrm{rang}((f - \lambda \mathbf{1}_V)^{k+1})$, akkor $\widetilde{V(\lambda)} = \mathrm{Ker}((f - \lambda \mathbf{1}_V)^k)$.

e) f diagonalizálható akkor és csak akkor, ha minden λ sajátérték esetén

$$\mathrm{rang}(f - \lambda \mathbf{1}_V) = \mathrm{rang}((f - \lambda \mathbf{1}_V)^2).$$

A Jordan-féle kanonikus alak meghatározása

Legyenek $\lambda_1, \ldots, \lambda_m$ az f különböző sajátértékei. Legyen v egy f-nek megfelelő Jordan-féle kanonikus bázis V-ben, $J := [f]_{v,v}$ egy Jordan-féle kanonikus alakja f-nek. Tudjuk, hogy minden $i = 1, \ldots, m$-ra létezik egy v_i bázis $\widetilde{V(\lambda_i)}$-ben úgy, hogy β_i diszjunkt egyesítése a λ_i-hez tartozó ciklusoknak, és $v = \bigcup_{i=1}^k v_i$.

Legyen f_i az f leszűkítése $\widetilde{V(\lambda_i)}$-re. Akkor $A_i := [f_i]_{v_i,v_i}$ Jordan-féle kanonikus alakja f_i-nek, és $J = [f]_{v,v} = A_1 \oplus \cdots \oplus A_m$ Jordan-féle kanonikus alakja f-nek.

A J-re vonatkozó egyértelműségi tétel megfogalmazására elfogadjuk a következő **konvenció**t: a v_i bázisokat olyan sorrendbe helyezzük, hogy a ciklusok hossza csökkenő sorrendben jelenjenek meg. Ha v_i diszjunkt egyesítése az $S_1, S_2, \ldots, S_{m_i}$ ciklusoknak és, ha az S_j ciklus hossza p_j, a ciklusokat úgy indexeljük, hogy $p_1 \ge \cdots \ge p_{m_i}$.

Ahogyan látni fogjuk nem létezik egy hasonló egyértelműségi tétel a v_i vagy v bázisokra. Megmutatjuk, hogy az m_i ciklusok száma, és a p_j hossúságok egyértelműen meghatározottak, és ezek a számok meghatározzák A_i-t.

Az A_i és v_i meghatározásának segítségére, bevezetünk egy pontokból álló tömböt, amit **pont-diagram**nak nevezünk. A v_i pont-diagramja a következő szabály alapján van megszerkesztve:

1. A tömb m_i oszlopot tartalmaz (egy oszlopot minden ciklusnak);

2. Balról jobbra a j-edik oszlop p_j pontot tartalmaz, amelyek megfelelnek az S_j elemeinek a következő módon: ha x_j az S_j végvektora, akkor $(f - \lambda_i \mathbf{1}_V)^{p_j - 1}(x_j)$ megfelel az első pontnak; $(f - \lambda_i \mathbf{1}_V)^{p_j - 2}(x_j)$ megfelel a második pontnak; és így tovább. Az utolsó pontnak az oszlopból az x_j vektor felel meg.

Tehát a v_i-nek megfelelő pont-diagramm a következő:

$$\begin{array}{llll}
\bullet(f-\lambda_i\mathbf{1}_V)^{p_j-1}(x_1) & \bullet(f-\lambda_i\mathbf{1}_V)^{p_2-1}(x_2) & \cdots & \bullet(f-\lambda_i\mathbf{1}_V)^{p_{m_i}-1}(x_{m_i}) \\
\bullet(f-\lambda_i\mathbf{1}_V)^{p_1-2}(x_1) & \bullet(f-\lambda_i\mathbf{1}_V)^{p_2-2}(x_2) & & \bullet(f-\lambda_i\mathbf{1}_V)^{p_{m_i}-2}(x_{m_i}) \\
\cdot & \cdot & & \vdots \\
\cdot & \cdot & & \bullet(f-\lambda_i\mathbf{1}_V)(x_{m_i}) \\
\cdot & \bullet(f-\lambda_i\mathbf{1}_V)(x_2) & & \bullet x_{k_i} \\
\bullet(f-\lambda_i\mathbf{1}_V)(x_1) & \bullet x_2 & & \\
\bullet x_1 & & &
\end{array}$$

Észrevesszük, hogy a sorok száma p_1, és ha r_j a j-edik sor pontjainak a száma, akkor $r_1 \geq \cdots \geq r_{p_1}$. A $p_1 \geq \cdots \geq p_{m_i}$ és az $r_1 \geq \cdots \geq r_{p_1}$ számrendszrek kölcsonösen meghatározzák egymást. A pont-diagram egyértelműségén pontosan azt értjük, hogy ha v_i és v_i' két Jordan-féle kanonikus bázis $\widetilde{V(\lambda_i)}$-ben, akkor a v_i és v_i'-nek megfelelő pont-diagram megegyezik.

2.4.28. példa. Tegyük fel, hogy $m_i = 4$, $p_1 = 3$, $p_2 = 3$, $p_3 = 2$ és $p_4 = 1$. Akkor

$$A_i = \begin{pmatrix}
\lambda_i & 1 & 0 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & \lambda_i & 1 & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & \lambda_i & 0 & 0 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & \lambda_i & 1 & 0 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & \lambda_i & 1 & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & \lambda_i & 0 & 0 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & \lambda_i & 1 & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_i & 0 \\
0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & \lambda_i
\end{pmatrix} = J_1 \oplus J_2 \oplus J_3 \oplus J_4.$$

A v_i pont-diagramja a következő:

$$\begin{array}{cccc}
\bullet & \bullet & \bullet & \bullet \\
\bullet & \bullet & \bullet & \\
\bullet & \bullet & &
\end{array}$$

2.66. feladat. Legyen egy m oszlopból és k sorból alló pont-diagram. Tegyük fel, hogy a j-edik oszlop p_j pontot és az i-edik sor r_i pontot tartalmaz. Ha $p_1 \geq p_2 \geq \ldots \geq p_m$, bizonyítsuk be, hogy:

a) $k = p_1$ és $m = r_1$.
b) $p_i = \max\{j \mid r_j \geq i\}$, ahol $1 \leq i \leq m$, és $r_i = \max\{j \mid p_j \geq i\}$, ahol $1 \leq i \leq m$.
c) $r_1 \geq r_2 \geq \cdots \geq r_m$.
d) Ha egy pont-diagramban ismertek az r_i számok, akkor a p_j számok meghatározhatók.

2.4.29. tétel (az r_j számok meghatározása). *Minden $r \in \mathbb{N}^*$ esetén a v_i vektorai, amelyek a v_i pont-diagramjának első r sorában levő pontokkal vannak azonosítva, bázist alkotnak* $\operatorname{Ker}((f-\lambda_i\mathbf{1}_V)^r)$*-ben. Tehát a v_i-nek megfelelő pont-diagram első r sorában levő pontok száma* $\dim_K \operatorname{Ker}((f-\lambda_i\mathbf{1}_V)^r)$.

Bizonyítás. A v_i vektorai, amelyek a v_i pont-diagramjának első r sorában levő pontokkal vannak azonosítva az $S_1, \ldots, S_{k_i}$ ciklusok első r elemei. Tehát ezek a vektorok elemei $\operatorname{Ker}((f-\lambda_i\mathbf{1}_V)^r)$-nek. Mi több, ezek a vektorok lineárisan függetlenek, mert v_i-nek elemei. Tehát elég bebizonyítani, hogy ezek a vektorok generálják $\operatorname{Ker}((f-\lambda_i\mathbf{1}_V)^r)$-t.

Legyen $W_j := \langle S_j \rangle$. Mivel W_j f-invariáns, következik, hogy W_j $(f-\lambda_i\mathbf{1}_V)^r$-invariáns. Mi több, $\widetilde{V(\lambda_i)} = W_1 \oplus \cdots \oplus W_{k_i}$. Ha $x \in \operatorname{Ker}((f-\lambda_i\mathbf{1}_V)^r)$, akkor $x \in \widetilde{V(\lambda_i)}$. Tehát léteznek a $w_j \in W_j$ egyértelmű elemek úgy, hogy $x = w_1 + \cdots + w_{k_i}$. Ezért

$$0 = (f-\lambda_i\mathbf{1}_V)^r(x) = (f-\lambda_i\mathbf{1}_V)^r(w_1) + \cdots + (f-\lambda_i\mathbf{1}_V)^r(w_{k_i}).$$

Következik, hogy $(f-\lambda_i\mathbf{1}_V)^r(w_j) = 0$ minden $j = 1, 2, \ldots, k_i$ esetén. Tegyük fel, hogy minden j-re

$$S_j = \{(f-\lambda_i\mathbf{1}_V)^{p_j-1}(x_j), (f-\lambda_i\mathbf{1}_V)^{p_j-2}(x_j), \ldots, (f-\lambda_i\mathbf{1}_V)(x_j), x_j\}.$$

Akkor mivel

$$w_j = a_{p_j-1}(f-\lambda_i\mathbf{1}_V)^{p_j-1}(x_j) + \cdots + a_1(f-\lambda_i\mathbf{1}_V)(x_j) + a_0x_j,$$

ahol $a_{p_j-1}, \ldots, a_1, a_0 \in K$, kapjuk, hogy

$$0 = (f-\lambda_i\mathbf{1}_V)^r(w_j) = a_{p_j-r-1}(f-\lambda_i\mathbf{1}_V)^{p_j-1}(x_j) + \cdots + a_0(f-\lambda_i\mathbf{1}_V)^r(x_j).$$

Mivel S_j lineárisan független következik, hogy $a_{p_j-r-1} = \cdots = a_0 = 0$. Tehát

$$w_j = a_{p_j-1}(f-\lambda_i \mathbf{1}_V)^{p_j-1}(x_j) + a_{p_j-2}(f-\lambda_i \mathbf{1}_V)^{p_j-2}(x_j) + \cdots + a_{p_j-r}(f-\lambda_i \mathbf{1}_V)^{p_j-r}(x_j).$$

Tehát w_j lineáris kombinációja a v_i vektorainak, amelyek azonosítva vannak a v_i pontdiagramjának a j-edik oszlop első r sorában levő pontjaival. Tehát $x = w_1 + w_2 + \cdots + w_{k_i}$ lineáris kombinációja a v_i elemeinek, amelyek azonosítva vannak a v_i pontdiagramjának első r sorában levő pontokkal. ■

Ha $r = 1$, akkor a 2.4.29 tétel a következőképpen alakul:

2.4.30. következmény. $m_i = \dim_K V(\lambda_i)$.

A következő ké[letekből megfogalmazhatunk egy algoritmust a v_i pont-diagramjának megszerkesztésére.

2.4.31. tétel. *Legyen r_j a v_i-nek megfelelő pont-diagram j-edik sorában levő pontok száma. Akkor:*
1) $r_1 = \dim_K V - \operatorname{rang}(f-\lambda_i \mathbf{1}_V)$.
2) $r_j = \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^{j-1}) - \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^j)$ *ha* $j > 1$.

Bizonyítás. A 2.4.29 tétel alapján, minden $j \geq 1$ esetén

$$r_1 + r_2 + \cdots + r_j = \dim_K \operatorname{Ker}((f-\lambda_i \mathbf{1}_V)^j) = \dim_K V - \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^j).$$

Tehát $r_1 = \dim_K V - \operatorname{rang}(f-\lambda_i \mathbf{1}_V)$ és ha $j > 1$, akkor

$$\begin{aligned} r_j &= (r_1 + r_2 + \ldots + r_j) - (r_1 + r_2 + \ldots + r_{j-1}) \\ &= (\dim_K V - \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^j)) - (\dim_K V - \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^{j-1})) \\ &= \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^{j-1}) - \operatorname{rang}((f-\lambda_i \mathbf{1}_V)^j). \qquad ■ \end{aligned}$$

2.4.32. következmény. *A fenti konvenciót elfogadva, a v_i pontdiagramja egyértelműen meghatározott.*
Tehát egy lineáris operátor Jordan-féle kanonikus alakja egyértelműen meghatározott, eltekinve a sajátértékek sorrendjétől.

Az következő példakban és feladatokban az általánosított sajátrészterek dimenziója elég kicsi. Itt nem adunk meg egy általános algoritmust a Jordan-féle kanonikus bázis meghatározására.

2.4.33. példa. Legyen $V = \mathbb{R}^4$, $f : \mathbb{R}^4 \to \mathbb{R}^4$

$$[f]_{e,e} = A = \begin{pmatrix} 2 & -1 & 0 & 1 \\ 0 & 3 & -1 & 0 \\ 0 & 1 & 1 & 0 \\ 0 & -1 & 0 & 3 \end{pmatrix}$$

Meghatározzuk az A Jordan-féle kanonikus alakját és egy f-nek meffelelő Jordan-féle kanonikus bázist. Az A karakterisztikus polinomja: $P_A(X) = \det(A - XI) = (X-2)^3(X-3)$. Tehát $m = 2$ mert A-nak két különböző sajátértéke van, $\lambda_1 = 2$ és $\lambda_2 = 3$, és $m_{alg}(\lambda_1) = 3$, $m_{alg}(\lambda_2) = 1$.

Következik, hogy $\dim_K \widetilde{V(\lambda_1)} = 3$, tehát a v_1 pont-diagramja három pontot tartalmaz. A 2.4.25 tétel alapján $r_1 = 4 - \operatorname{rang}(A-2I) = 4-2 = 2$ és $r_2 = \operatorname{rang}(A-2I) - \operatorname{rang}((A-2I)^2) = 2-1 = 1$. Innen a v_1 pont-diagramja a következő:

$$\begin{matrix} \bullet & \bullet \\ \bullet & \end{matrix}$$

Következik, hogy

$$A_1 := [f_1]_{v_1,v_1} = \begin{pmatrix} 2 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}.$$

Mivel $\dim_K \widetilde{V(\lambda_2)} = 1$, v_2 egyetlen vektort tartalmaz, tehát a v_2 pont-diagramja $\bullet$ és $A_2 := [v_2]_{v_2,v_2} = (3)$.
Kapjuk, hogy $v = v_1 \cup v_2$ és az A Jordan-féle kanonikus alakja

$$J = [f]_{v,v} = A_1 \oplus A_2 = \begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$$

Most keresünk egy f-nek megfelelő Jordan kanonikus bázist $\mathbb{R}^4$-ben. Tudjuk, hogy a ν_1 pont-diagramja

$\bullet(f-\lambda_i\mathbf{1}_V)(x_1)$ $\bullet x_2$
$\bullet x_1$

A diagrammból látjuk, hogy egy x_1 vektort kell válasszunk úgy, hogy $x_1 \in \mathrm{Ker}((f-\lambda_1\mathbf{1}_V)^2)$, de $x_1 \notin \mathrm{Ker}((f-\lambda_1\mathbf{1}_V))$. Itt

$$A-2I=\begin{pmatrix}0&-1&0&1\\0&1&-1&0\\0&1&-1&0\\0&-1&0&1\end{pmatrix},\qquad (A-2I)^2=\begin{pmatrix}0&-2&1&1\\0&0&0&0\\0&0&0&0\\0&-2&1&1\end{pmatrix}.$$

Könnyű belátni, hogy $\{(1,0,0,0),\ (0,1,2,0),\ (0,1,0,2)\}$ bázisa $\mathrm{Ker}((f-\lambda_1\mathbf{1}_V)^2)=\widetilde{V(\lambda_1)}$-nek. A $(0,1,2,0)$ és $(0,1,0,2)$ vektorok nem elemei $\mathrm{Ker}((f-\lambda_1\mathbf{1}_V)$-nek. x_1 lehet bármelyik a két vektor közül; legyen $x_1=(0,1,2,0)$. Akkor

$$[(f-\lambda_1\mathbf{1}_V)(x_1)]_{e,e}=(A-2I)[x_1]_{e,e}=\begin{pmatrix}0&-1&0&1\\0&1&-1&0\\0&1&-1&0\\0&-1&0&1\end{pmatrix}\begin{pmatrix}0\\1\\2\\0\end{pmatrix}=\begin{pmatrix}-1\\-1\\-1\\-1\end{pmatrix}.$$

Most kiválasztunk egy $0\neq x_2\in V(\lambda_2)$ vektort, például, legyen $x_2=(1,0,0,0)$. Tehát a

$$\nu_1=\{(-1,-1,-1,-1),\ (0,1,2,0),\ (1,0,0,0)\}$$

pont-diagramja

$\bullet(-1,-1,-1,-1)$ $\bullet(1,0,0,0)$
$\bullet(0,1,2,0)$

A $\lambda_2=3$ sajátértéknek esetén $V(\lambda_2)=\widetilde{V(\lambda_2)}$, és legyen x_1 egy sajátvektor, például legyen $\nu_2=\{(1,0,0,1)\}$. Akkor $\nu=\nu_1\cup\nu_2$ f-nek megfelelő Jordan-féle kanonikus bázis V-ben, és $J=T^{-1}AT$, ahol

$$T:=T_e^\nu=\begin{pmatrix}-1&0&1&1\\-1&1&0&0\\-1&2&0&0\\-1&0&0&1\end{pmatrix}.$$

2.4.34. példa. Legyen

$$A=\begin{pmatrix}2&-4&2&2\\-2&0&1&3\\-2&-2&3&3\\-2&-6&3&7\end{pmatrix}$$

Az A karakterisztikus polinomja $P_A(X)=\det(A-XI)=(X-2)^2(X-4)^2$. Legyen $\lambda_1=2$ és $\lambda_2=4$.

Mivel $r_1=4-\mathrm{rang}(A-2I)=4-2=2$, a ν_1 pontdiagramja $\bullet\quad\bullet$, tehát $A_1=[f_1]_{\nu_1,\nu_1}=\begin{pmatrix}2&0\\0&2\end{pmatrix}$.

Most megszerkesztjük a ν_2 pont-diagramját. Mivel $\mathrm{rang}(A-4I)=3$, a diagram első sorában csak $4-3=1$ pont van. Mivel a $\dim_K\widetilde{V(\lambda_2)}=2$, a ν_2 pont-diagramja $\begin{matrix}\bullet\\\bullet\end{matrix}$, tehát $A_2=[f_2]_{\nu_2,\nu_2}=\begin{pmatrix}4&1\\0&4\end{pmatrix}$.

Ha $\nu:=\nu_1\cup\nu_2$, akkor az A Jordan-féle kanonikus alakja

$$J=[f]_{\nu,\nu}=\begin{pmatrix}2&0&0&0\\0&2&0&0\\0&0&4&1\\0&0&0&4\end{pmatrix}.$$

A ν_1 pont-diagramja azt mutatja, hogy a ν_1 bázis $V(\lambda_1)$-ben. Például legyen $\nu_1=\{(2,1,0,2),\ (0,1,2,0)\}$.

ν_2-nek kell találjunk egy $x_1\in\widetilde{V(\lambda_2)}=\mathrm{Ker}((f-\lambda_2\mathbf{1}_V)^2)$ vektort úgy, hogy $x_1\notin\mathrm{Ker}(f-\lambda_2\mathbf{1}_V)$. Az egyik módszert az előző példában láttuk; most egy másik módszert alkalmazunk. Kapjuk, hogy

$$\mathrm{Ker}(f-\lambda_2\mathbf{1}_V)=\langle(0,1,1,1)\rangle.$$

Legyen x_1 úgy, hogy $(f-\lambda_2 \mathbf{1}_V)(x_1) = (0,1,1,1)$. Tekintsük a következő mátrixegyenletet:

$$\begin{pmatrix} -2 & -4 & 2 & 2 \\ -2 & -4 & 1 & 3 \\ -2 & -2 & -1 & 3 \\ -2 & -6 & 3 & 3 \end{pmatrix} \begin{pmatrix} a_1 \\ a_2 \\ a_3 \\ a_4 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \\ 1 \\ 1 \end{pmatrix},$$

és kapjuk az $x_1 = (1,-1,-1,0)$ megoldást. Akkor $v_2 = \{(f-\lambda_2 \mathbf{1}_V)(x_1),\ x_1\}$, és

$$v = v_1 \cup v_2 = \{(2,1,0,2),\ (0,1,2,0),\ (0,1,1,1),\ (1,-1,-1,0)\}$$

A-nek megfelelő Jordan-féle kanonikus bázis $\mathbb{R}^4$-ben, és $J = T^{-1}AT$, ahol

$$T := T_e^v = \begin{pmatrix} 2 & 0 & 0 & 1 \\ 1 & 1 & 1 & -1 \\ 0 & 2 & 1 & -1 \\ 2 & 0 & 1 & 0 \end{pmatrix}.$$

2.4.35. példa. Legyen $V = \{\phi \in \mathbb{R}[x,y] \mid \deg \phi \leq 2\}$, tehát $e = \{1, x, y, x^2, y^2, xy\}$ a V kanonikus bázisa. Legyen

$$f : V \to V, \quad f(\phi) = \frac{\partial}{\partial x}\phi,$$

tehát

$$A := [f]_{e,e} \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Meghatározzuk a f Jordan-féle kanonikus alakját. Az f karakterisztikus polinomja $P_f(X) = \det(A - XI) = X^6$, tehát $m = 1$, $\lambda = 0$ és $\widetilde{V(\lambda)} = V$. Legyen v egy f-nek megfelelő Jordan-féle kanonikus bázis. Itt $r_1 = 6 - \operatorname{rang}(A) = 6 - 3 = 3$, és $r_2 = \operatorname{rang}(A) - \operatorname{rang}(A^2) = 3 - 1 = 2$. Mivel $r_1 = 3$, $r_2 = 2$, és a a v pont-diagramja 6 pontot tartalmaz, következik, hogy $r_3 = 1$. Tehát a v pont-diagramja a következő:

$$\begin{array}{lll} \bullet & \bullet & \bullet \\ \bullet & \bullet & \\ \bullet & & \end{array}$$

és az f Jordan-féle kanonikus alakja a következő:

$$J := [f]_{v,v} = \begin{pmatrix} 0 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 \end{pmatrix}.$$

Most keresünk egy f-nek megfelelő Jordan-féle kanonikus bázist V-ben. Mivel a v pont-diagramja az első oszlopban három pontot tartalmaz, olyan ϕ_1 vektort kell találjunk, amelyre $\frac{\partial^2}{\partial x^2}\phi_1 \neq 0$. Észrevesszük, hogy $x_1 = x^2$ megfelel; azt kapjuk, hogy

$$(f-\lambda \mathbf{1}_V)(\phi_1) = f(\phi_1) = \frac{\partial}{\partial x}\phi_1 = 2x, \qquad (f-\lambda \mathbf{1}_V)^2(\phi_1) = f^2(\phi_1) = \frac{\partial^2}{\partial x^2}\phi_1 = 2.$$

Mivel a v pont-diagramjának második sora két pontot tartalmaz, olyan ϕ_2 vektort keresünk, amelyre $\frac{\partial}{\partial x}\phi_2 \neq 0$. Észreveszszük, hogy $\phi_2 = xy$ megfelel. Akkor

$$(f-\lambda \mathbf{1}_V)(\phi_2) = f(\phi_2) = \frac{\partial}{\partial x}(xy) = y.$$

Végül legyen $x_3 = y^2$. Tehát $v = \{2, 2x, x^2, y, xy, y^2\}$ Jordan-féle kanonikus bázis, amelynek pont-diagramja

$$\begin{array}{lll} \bullet 2 & \bullet y & \bullet y^2 \\ \bullet 2x & \bullet xy & \\ \bullet x^2 & & \end{array}$$

2.4.36. definíció. Azt mondjuk, hogy $A, B \in M_n(K)$ **hasonló** mátrixok, ha létezik $T \in GL_n(K)$ úgy, hogy $B = T^{-1}AT$. Jelölés: $A \sim B$.

2.67. feladat. Igazoljuk, hogy a mátrixok hasonlósága ekvivalenciareláció.

2.4.37. tétel (Hasonló mátrixok jellemzése). *Legyen $A, B \in M_n(K)$. Akkor A és B hasonló akkor és csak akkor, ha a két mátrix Jordan-féle kanonikus alakja megegyezik.*

Bizonyítás. Legyenek J_A és J_B az A és B Jordan-féle kanonikus alakjai. Ha $J_A = J_B$, akkor mivel $A \sim J_A$ és $B \sim J_B$, következik, hogy $A \sim B$.

Fordítva, ha $A \sim B$ akkor $J_A \sim J_B$, tehát létezik $f \in \mathrm{End}_K(V)$ és v, w bázisok V-ben úgy, hogy $[f]_{v,v} = J_A$ és $[f]_{w,w} = J_B$. Tehát J_A és J_B Jordan-féle kanonikus alakjai ugyannak az endomorfizmusnak. Az egyértelműség alapján következik, hogy $J_A = J_B$. ■

2.4.38. példa. Határozzuk meg az alábbi mátrixok közül melyek hasonlóak:

$$A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}, \quad B = \begin{pmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{pmatrix}, \quad C = \begin{pmatrix} 0 & -1 & -1 \\ -3 & -1 & -2 \\ 7 & 5 & 6 \end{pmatrix}, \quad D = \begin{pmatrix} 0 & 1 & 2 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Észrevesszük, hogy A, B és C-nek ugyanaz a karakterisztikus polinomja: $-(X-1)(X-2)^2$, a D karakterisztikus polinomja pedig $-X(X-1)(X-2)$. Következik, hogy D nem hasonló sem A, sem B sem C-vel. A, B és C-nek ugyanazok a sajátértékei: $\lambda_1 = 1$ és $\lambda_2 = 2$. Ha J_A, J_B és J_C az A, B és C mátrixok Jordan-féle kanonikus alakja, akkor

$$J_A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}, \quad J_B = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}, \quad J_C = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 1 \\ 0 & 0 & 2 \end{pmatrix}.$$

Mivel $J_A = J_C$ következik, hogy A és C hasonlóak, B nem hasonló A-val sem és C-vel sem.

2.68. feladat. Legyenek $\lambda_1 = 2$, $\lambda_2 = 4$ és $\lambda_3 = -3$ az f különböző sajátértékei. Határozzuk meg a f Jordan-féle kanonikus alakját, ha a v_1, v_2, v_3 pont-diagramjai a következőképpen néznek ki:

$$\begin{array}{ccc} \bullet & \bullet & \bullet \\ \bullet & \bullet & \\ \bullet & & \end{array} \qquad \begin{array}{cc} \bullet & \bullet \\ \bullet & \\ \bullet & \end{array} \qquad \begin{array}{cc} \bullet & \bullet \\ & \\ & \end{array}$$

2.69. feladat. Az $f \in \mathrm{End}_{\mathbb{Q}}(\mathbb{Q}^7)$ Jordan-féle kanonikus alakja

$$J = \begin{pmatrix} 2 & 1 & 0 & 0 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 2 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 3 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 3 \end{pmatrix}.$$

a) Határozzuk meg az f sajátértékeinek megfelelő pont-diagramokat.

b) Minden λ_i sajátértékre, határozzuk meg azt a legkisebb $p_i \in \mathbb{N}^*$ számot, amelyre $\widetilde{V(\lambda_i)} = \mathrm{Ker}((f - \lambda_i \mathbf{1}_V)^{p_i})$.

c) Legyen $g_i : \widetilde{V(\lambda_i)} \to \widetilde{V(\lambda_i)}$ a $f - \lambda_i \mathbf{1}_V$ leszűkítése $\widetilde{V(\lambda_i)}$-re. Határozzuk meg a következőket:
(1) $\mathrm{rang}(g_i)$; (2) $\mathrm{rang}(g_i^2)$; (3) $\dim_K \mathrm{Ker}(g_i)$; (3) $\dim_K \mathrm{Ker}(g_i^2)$.

2.70. feladat. Az alábbi A mátrixok esetén, határozzuk meg a Jordan kanonikus alakjukat és azt a T mátrixot, amelyre $J = T^{-1}AT$.

a) $A = \begin{pmatrix} -3 & 3 & -2 \\ -7 & 6 & -3 \\ 1 & -1 & 2 \end{pmatrix}$; b) $A = \begin{pmatrix} 0 & 1 & -1 \\ -4 & 4 & -2 \\ -2 & 1 & 1 \end{pmatrix}$; c) $A = \begin{pmatrix} 0 & -1 & -1 \\ -3 & -1 & -2 \\ 7 & 5 & 6 \end{pmatrix}$;

d) $A = \begin{pmatrix} 0 & -3 & 1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & 1 & -1 & 2 \\ -2 & -3 & 1 & 4 \end{pmatrix}$.

2.71. feladat. Legyen $V = \langle e^t,\ te^t,\ t^2e^t,\ e^{2t} \rangle \leq \mathbb{R}^{\mathbb{R}}$, $f : V \to V$, $f(\phi) = \phi'$. Határozzuk meg az f Jordan-féle kanonikus alakját és egy f-nek megfelelő Jordan-féle kanonikus bázist V-ben.

2.72. feladat. Legyen $A \in M_n(K)$. Bizonyítsuk be, hogy:
1) $\operatorname{rang}((A-\lambda I)^r) = \operatorname{rang}((A^t-\lambda I)^r)$, minden λ sajátérték és $r \in \mathbb{N}^*$ esetén.
2) $A \sim A^t$.

2.73. feladat (mátrix hatványai). Legyenek $\lambda_1, \dots, \lambda_m$ az $f \in \operatorname{End}_K(V)$ különböző sajátértékei. Legyen

$$g : V \to V, \quad g(x) = (f-\lambda_1 1_V)(x_1) + \cdots + (f-\lambda_m 1_V)(x_m),$$

ahol ahol $x = x_1 + \cdots + x_m \in V$, $x_i \in \widetilde{V(\lambda_i)}$. Legyen $\nu = \nu_1 \cup \cdots \cup \nu_m$ f-nek megfelelő Jordan-féle kanonikus bázis V-ben, ahol ν_i bazis $\widetilde{V(\lambda_i)}$-ben, és legyen $A := [f]_{e,e}$, $J := [f]_{\nu,\nu}$, $N := [g]_{\nu,\nu}$ és $D = J - N$. Igazoljuk, hogy:
a) g lineáris, nilpotens, és $g \circ f = f \circ g$.
b) D diagonális mátrix, $n_{ij} = 0$ ha $i \geq j$, és $DN = ND$.
c) Legyen $p \in \mathbb{N}^*$ a legkisebb szám, amelyre $N^p = 0$; akkor

$$J^r = \begin{cases} D^r + rD^{r-1}N + \frac{r(r-1)}{2!}D^{r-2}N^2 + \cdots + rDN^{r-1} + N^r, & \text{ha} \quad r < p, \\ D^r + rD^{r-1}N + \frac{r(r-1)}{2!}D^{r-2}N^2 + \cdots + \frac{r!}{(r-p+1)!(p-1)!}D^{r-p+1}N^{p-1}, & \text{ha} \quad r \geq p. \end{cases}$$

d) Ha $T := T_e^\nu$, akkor $A^r = TJ^rT^{-1}$ minden $r \in \mathbb{N}$ esetén.

2.74. feladat. Legyen $J \in M_p(K)$ a λ sajátértéknek megfelelő Jordan-blokk, és legyen $N = J - \lambda I_p$, tehát

$$J = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 & 0 \\ 0 & \lambda & 1 & \cdots & 0 & 0 \\ 0 & 0 & \lambda & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & \lambda & 1 \\ 0 & 0 & 0 & \cdots & 0 & \lambda \end{pmatrix}, \qquad N = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ 0 & 0 & 0 & \cdots & 0 & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 0 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

Bizonyítsuk be, hogy $N^p = 0$, és ha $r \geq p$, akkor

$$\begin{aligned} J^r &= \lambda^r I_m + r\lambda^{r-1}N + \frac{r(r-1)}{2!}\lambda^{r-2}N^2 + \cdots + \frac{r(r-1)\dots(r-p+2)}{(p-1)!}\lambda^{r-p+1}N^{p-1} \\ &= \begin{pmatrix} \lambda^r & r\lambda^{r-1} & \frac{r(r-1)}{2!}\lambda^{r-2} & \cdots & \frac{r(r-1)\dots(r-p+2)}{(p-1)!}\lambda^{r-p+1} \\ 0 & \lambda^r & r\lambda^{r-1} & \cdots & \frac{r(r-1)\dots(r-p+3)}{(p-2)!}\lambda^{r-p+2} \\ \vdots & \vdots & \vdots & & \vdots \\ 0 & 0 & 0 & \cdots & \lambda^r \end{pmatrix}. \end{aligned}$$

2.5. Bilineáris és kvadratikus alakok

2.5.1. Bilineáris és kvadratikus alakok

Legyen V egy K-feletti vektortér, $\dim_K V = n$, és $e = (e_1, \dots, e_n)$ egy bázisa.

2.5.1. definíció. a) A $\beta : V \times V \to K$ függvényt **bilineáris alak**nak nevezzük ha minden $a, b \in K$ és minden $x, x_1, x_2, y, y_1, y_2 \in V$ esetén

$$\beta(ax_1 + bx_2, y) = a\beta(x_1, y) + b\beta(x_2, y),$$

$$\beta(x, ay_1 + by_2) = a\beta(x, y_1) + b\beta(x, y_2).$$

b) Ha $a_{ij} = \beta(e_i, e_j)$, $1 \leq i, j \leq n$, és $A = [a_{ij}]_{1 \leq i,j \leq n} \in M_n(K)$, akkor azt mondjuk, hogy A a β-nak az e bázisra vonatkozó mátrixa. Jelölés: $A = [\beta]_e$.
c) Értelmezés szerint, a β alak **rangja** egyenlő a $[\beta]_e$ mátrix rangjával: $\operatorname{rang}\beta = \operatorname{rang}[\beta]_e$.
Azt mondjuk, hogy β **degenerált**, ha $\operatorname{rang}\beta < n$ (azaz $\det[\beta]_e = 0$), és β **nem degenerált** ha $\operatorname{rang}\beta = n$.
d) A β bilineáris alak **szimmetrikus**, ha

$$\beta(x, y) = \beta(y, x)$$

minden $x, y \in V$ esetén.
e) Ha $\beta : V \times V \to K$ egy szimmetrikus bilineáris alak, akkor

$$q : V \to K, \quad q(x) = \beta(x, x)$$

a β-hoz tartozó **kvadratikus alak**.
f) Azt mondjuk, hogy β (vagy q) **kanonikus alakú** az e-bázisban, ha $[\beta]_e$ diagonális mátrix.

2.5.2. lemma. *Legyen* $\beta : V \times V \to K$ *egy bilineáris alak.*
a) *Minden* $x, y \in V$ *esetén*

$$\beta(x, y) = [x]_e^t [\beta]_e [y]_e.$$

b) β *akkor és csak akkor szimmetrikus alak, ha* $A = [\beta]_e$ *szimmetrikus mátrix.*
c) *Legyen* $e' = (e'_1, \dots, e'_n)$ *egy második bázis, és* $T = T_e^{e'}$ *az* e *bázisról az* e' *bázisra való áttérési mátrix. Ekkor*

$$[\beta]_{e'} = T^t [\beta]_e T.$$

Bizonyítás. a) Ha $x = \sum_{i=1}^n x_i e_i$ és $y = \sum_{j=1}^n y_j e_j$, akkor

$$\beta(x, y) = \beta(\sum_{i=1}^n x_i e_i, \sum_{j=1}^n y_j e_j) = \sum_{i=1}^n \sum_{j=1}^n x_i y_j \beta(e_i, e_j)$$
$$= \sum_{i=1}^n \sum_{j=1}^n x_i a_{ij} y_j = [x]_e^t A [y]_e.$$

b) Ha β szimmetrikus, akkor $a_{ij} = \beta(e_i, e_j) = \beta(e_j, e_i) = a_{ji}$, minden $i, j \in \{1, \dots, n\}$ esetén, tehát $A = A^t$.
Fordítva, ha $A = A^t$, akkor minden $x, y \in V$ esetén,

$$\beta(x, y) = \sum_{i=1}^n \sum_{j=1}^n x_i a_{ij} y_j = \sum_{j=1}^n \sum_{i=1}^n y_j a_{ji} x_i = \beta(y, x).$$

c) Ha $x, y \in V$, akkor $[x]_e = T[x]_{e'}$ és

$$\beta(x, y) = [x]_e^t [\beta]_e [y]_e = [x]_{e'}^t [\beta]_{e'} [y]_{e'} = [x]_{e'}^t T^t [\beta]_e T [y]_{e'}$$

Behelyesítve az $[x]_{e'}$ és $[y]_{e'}$ oszlopmátrixokat az $e_1, \dots, e_n$ mátrixokkal, kapjuk, hogy $T^t [\beta]_e T = [\beta]_{e'}$. ■

2.5.3. megjegyzés. a) Mivel $T = T_e^{e'}$ invertálható mátrix, következik, hogy $\operatorname{rang}\beta = \operatorname{rang}[\beta]_e$ nem függ az e bázistól.
b) Ha β szimmetrikus és $[\beta]_e = A$, akkor

$$q(x) = \sum_{i,j=1}^n a_{ij} x_i x_j = \sum_{i=1}^n a_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n} a_{ij} x_i x_j.$$

c) Ha β-nak kanonikus alakú az e bázisban, $[\beta]_e = \operatorname{diag}(\lambda_1, \dots, \lambda_n)$, akkor

$$\beta(x, y) = \sum_{i=1}^n \lambda_i x_i y_i \quad \text{és} \quad q(x) = \sum_{i=1}^n \lambda_i x_i^2.$$

2.75. feladat. Legyen $e = (e_1, \dots, e_n)$ bázisa V-nek, $B(V, K) = \{\beta : V \times V \to K \mid \beta \text{ bilineáris }\}$, $B_s(V, K)$ a *szimmetrikus alakok* halmaza, $B_a(V, K)$ az *antiszimmetrikus alakok* halmaza, $q : B(V, K) \to K^V$, $q(\beta)(x) = \beta(x, x)$ és $Q(V, K) = \operatorname{Im} q \subseteq K^V$ a *kvadratikus alakok* halmaza. Feltételezzük, hogy K-ban, $1 + 1 \neq 0$. Igazoljuk, hogy:
a) $B(V, K)$ K-feletti vektortér;
b) $\tau : B(V, K) \to B(V, K)$, $\tau(\beta)(x, y) = \beta(y, x)$ lineáris függvény és $\tau \circ \tau = 1$.
c) $\Phi : B(V, K) \to M_n(K)$, $\Phi(\beta) = [\beta]_e$ izomorfizmus.
d) $B_s(V, K)$, $B_a(V, K) \le_K B(V, K)$, $\Phi(B_s(V, K)) = \mathcal{S}_n(K)$ és $\Phi(B_a(V, K)) = \mathcal{A}_n(K)$. Határozzuk meg a két résztér dimenziójat.
e) Bármely $\beta \in B(V, K)$ esetén léteznek az egyértelműen meghatározott $\beta_s \in B_s(V, K)$ és $\beta_a \in B_a(V, K)$ elemek úgy, hogy $\beta = \beta_s + \beta_a$.
f) β antiszimmetrikus $\Leftrightarrow \beta(x, x) = 0$ bármely $x \in V$ esetén.
g) q lineáris és $\ker q = B_a(V, K)$.
h) $\tilde{q} : B_s(V, K) \to Q(V, K)$, $\tilde{q}(\beta) = q(\beta)$ izomorfizmus, és

$$\tilde{q}^{-1}(q(\beta)) = q(x + y) - q(x) - q(y) = \frac{1}{2}[\beta(x, y) + \beta(y, x)].$$

2.5.2. Valós kvadratikus alakok négyzetösszegre való redukciója

Ebben a paragrafusban $K = \mathbb{R}$ a valós számok teste, V egy K-feletti vektortér és $e = (e_1, \dots, e_n)$ egy bázisa. Legyen $\beta : V \times V \to \mathbb{R}$ egy szimmetrikus bilineáris alak, $A = [\beta]_e$, és

$$q(x) = \beta(x, x) = \sum_{i=1}^{n} a_{ii}x_i^2 + 2 \sum_{1 \le i < j \le n} a_{ij}x_ix_j.$$

2.5.4. tétel (Gauss–Lagrange). *Létezik egy* $e' = (e'_1, \dots, e'_n)$ *bázis úgy, hogy*

$$q(x) = \sum_{i=1}^{n} a'_{ii}x'^2_i$$

kanonikus alakú, ahol $A' = \operatorname{diag}(a'_{11}, \dots, a'_{nn}) = [\beta]_{e'}$ *és* $[x]_{e'} = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$

Bizonyítás. n-szerinti matematikai indukciót alkalmazunk.

Ha $n = 1$, akkor $q(x) = a_{11}x_1^2$ kanonikus alakú, tehát $e' = e = (e_1)$.

Legyen $n > 1$, és feltételezzük, hogy az állítás igaz $(n-1)$ változó esetén. Két eset van:

I. *eset.* Létezik $i \in \{1, \dots, n\}$ úgy, hogy $a_{ii} \neq 0$. Feltételezhetjük, hogy $a_{11} \neq 0$. Ekkor

$$\begin{aligned} q(x) &= a_{11}x_1^2 + 2(a_{12}x_1x_2 + \dots + a_{1n}x_1x_n) + q_1(x) \\ &= \frac{1}{a_{11}}[a_{11}^2x_1^2 + 2a_{11}(a_{12}x_1x_2 + \dots + a_{1n}x_1x_n) + (a_{12}x_2 + \dots + a_{1n}x_n)^2] \\ &\quad - \frac{1}{a_{11}}[(a_{12}x_2 + \dots + a_{1n}x_n)^2 - q_1(x)] \\ &= \frac{1}{a_{11}}(a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n)^2 + q_2(x), \end{aligned}$$

ahol $q_1(x)$ és $q_2(x)$ olyan kvadratikus alakok amelyek nem függnek x_1-től.

Legyen $x'_1 = a_{11}x_1 + a_{12}x_2 + \dots + a_{1n}x_n$; az indukció hipotézisából következik, hogy létezik egy $e'' = (e'_2, \dots, e'_n)$ bázis amelyben $q_2(x) = a'_{22}x'^2_2 + \dots + a'_{nn}x'^2_n$ kanonikus alakú, tehát letezik egy $e' = (e'_1, \dots, e'_n)$ bázis amelyben

$$q(x) = \frac{1}{a_{11}}x'^2_1 + a'_{22}x'^2_2 + \dots + a'_{nn}x'^2_n.$$

II. *eset.* Minden $i \in \{1, \dots, n\}$ esetén, $a_{ii} = 0$. Feltételezhetjük, hogy $a_{12} \neq 0$, és legyen

$$\begin{cases} x_1 &= y_1 + y_2 \\ x_2 &= y_1 - y_2 \\ x_3 &= y_3 \\ \vdots & \\ x_n &= y_n \end{cases}$$

Legyen f az a bázis amelyre $[x]_f = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, $[x]_e = T[x]_f$ és

$$T = T_e^f = \begin{pmatrix} 1 & 1 & 0 & \dots & 0 \\ 1 & -1 & 0 & \dots & 0 \\ 0 & 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 0 \end{pmatrix}$$

Következik, hogy $q(x) = a_{12}(y_1^2 - y_2^2) + \dots$, tehát alkalmazhatjuk most az első esetet. ■

2.5.5. példa. Redukáljuk kanonikus alakra a $q(x) = 2x_1x_2 - 6x_2x_3 + 2x_1x_3$ kvadratikus alakot. A II. esetet alkalmazzuk: legyen

$$\begin{cases} x_1 = y_1 - y_2 \\ x_2 = y_1 + y_2 \\ x_3 = y_3 \end{cases}, \quad \begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix} = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \quad T_1 = \begin{pmatrix} 1 & -1 & 0 \\ 1 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

tehát $q(x) = 2y_1^2 - 2y_2^2 - 4y_1y_3 - 8y_2y_3$.

Az első esetet alkalmazva, vegyük észre, hogy $q(x) = \frac{1}{2}(2y_1 - 2y_3)^2 - 2y_2^2 - 8y_2y_3 - 2y_3^2$, és legyen

$$\begin{cases} z_1 = 2y_1 - 2y_3 \\ z_2 = y_2 \\ z_3 = y_3 \end{cases}, \quad \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix} = \begin{pmatrix} 2 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} y_1 \\ y_2 \\ y_3 \end{pmatrix}, \quad T_2^{-1} = \begin{pmatrix} 2 & 0 & -2 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix},$$

tehát $q(x) = \frac{1}{2}z_1^2 - 2z_2^2 - 8z_2z_3 - 2z_3^2 = \frac{1}{2}z_1^2 - \frac{1}{2}(2z_2 + 4z_3)^2 + 6z_3^2$. Végül, legyen

$$\begin{cases} x_1' = z_1 \\ x_2' = 2z_2 + 4z_3 \\ x_3' = z_3 \end{cases}, \quad \begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{pmatrix} \begin{pmatrix} z_1 \\ z_2 \\ z_3 \end{pmatrix}, \quad T_3^{-1} = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 2 & 4 \\ 0 & 0 & 1 \end{pmatrix},$$

tehát $q(x) = \frac{1}{2}x_1'^2 - \frac{1}{2}x_2'^2 - 6x_3'^2$. Az e bázisról az e' bázisra való áttérési mátrix $T_e^{e'} = T = T_1T_2T_3$ és $\begin{pmatrix} x_1' \\ x_2' \\ x_3' \end{pmatrix} = T^{-1}\begin{pmatrix} x_1 \\ x_2 \\ x_3 \end{pmatrix}$.

2.5.6. definíció. Legyen $q : V \to \mathbb{R}$ egy valós kvadratikus alak. Azt mondjuk, hogy
a) q **pozitív definit** ha $q(x) > 0$ minden $x \in V \setminus \{0\}$ esetén.
b) q **pozitív szemidefinit** ha $q(x) \geq 0$ minden $x \in V$ esetén.
c) q **negatív definit** ha $q(x) < 0$ minden $x \in V \setminus \{0\}$ esetén.
d) q **negatív szemidefinit** ha $q(x) \leq 0$ minden $x \in V$ esetén.
e) q **indefinit** a többi esetben, azaz, ha létezenek az $x, y \in V$ vektorok úgy, hogy $q(x) > 0$ és $q(y) < 0$.

2.5.7. megjegyzés. Ha $\text{rang}\beta = \text{rang}A = r$, akkor a $q(x)$ minden kanonikus alakjának pontosan r nem nulla együtthatója van:

$$q(x) = \sum_{i=1}^{r} a_{ii}' x_i'^2, \quad a_{ii}' \neq 0, \quad i = 1, \ldots, n.$$

Könnyen észrevehető, hogy:
a) q pozitív definit $\Leftrightarrow r = n, \quad a_{11}', \ldots, a_{rr} > 0$.
b) q pozitív szemidefinit $\Leftrightarrow a_{11}', \ldots, a_{rr} \geq 0$.
c) q negatív definit $\Leftrightarrow r = n, \quad a_{11}', \ldots, a_{rr} < 0$.
d) q negatív szemidefinit $\Leftrightarrow a_{11}', \ldots, a_{rr} \leq 0$.
e) q indefinit a többi esetben.

2.5.8. tétel. *Ha* $q(x) = \beta(x, x)$ *egy pozitív szemidefinit alak, akkor minden* $x, y \in V$ *esetén*
a) $|\beta(x, y)| \leq \sqrt{q(x)}\sqrt{q(y)}$ (**Cauchy–Schwartz-egyenlőtlenség**).
b) $\sqrt{q(x + y)} \leq \sqrt{q(x)} + \sqrt{q(y)}$ (**Minkowski-egyenlőtlenség**).

Bizonyítás. a) Minden $x, y \in V$ és $a \in \mathbb{R}$ esetén,

$$0 \leq \beta(x - ay, x - ay) = \beta(x, x) - 2a\beta(x, y) + a^2\beta(y, y).$$

Vegyük észre, hogy ha $\beta(y, y) = 0$, akkor $\beta(x, y) = 0$. Tehát feltételezzük, hogy $\beta(y, y) \neq 0$, és így egy másodfokú függvényt kaptunk, amelynek a diszkriminánsa negatív kell legyen:

$$0 \geq \Delta_a = \beta(x, y)^2 - \beta(x, x)\beta(y, y);$$

következik, hogy $|\beta(x, y)| \leq \sqrt{q(x)}\sqrt{q(y)}$.

b) Az előző egyenlőtlenséget felhasználva következik, hogy

$$\begin{aligned} q(x + y) &= \beta(x + y, x + y) = \beta(x, x) + 2\beta(x, y) + \beta(y, y) \\ &\leq q(x) + 2|\beta(x, y)| + q(y) \\ &\overset{a)}{\leq} (\sqrt{q(x)})^2 + 2\sqrt{q(x)}\sqrt{q(y)} + (\sqrt{q(y)})^2 = (\sqrt{q(x)} + \sqrt{q(y)})^2, \end{aligned}$$

tehát $\sqrt{q(x + y)} \leq \sqrt{q(x)} + \sqrt{q(y)}$. ■

2.76. feladat. Redukáljuk négyzetösszegre a következő kvadratikus alakokat (alkalmazzuk a Gauss–Lagrange-módszert):
a) $x_1^2 + 2x_1x_2 + 2x_2^2 + 4x_2x_3 + 5x_3^2$;
b) $x_1^2 - 4x_1x_2 + 2x_1x_3 + 4x_2^2 + x_3^2$;
c) $3x_1^2 - 5x_2^2 - 7x_3^2 - 8x_1x_2 + 8x_2x_3$;
d) $x_1x_2 + x_2x_3 + x_1x_3$;
e) $x_1^2 - 2x_1x_2 + 2x_1x_3 - 2x_1x_4 + x_2^2 + 2x_2x_3 - 4x_2x_4 + x_3^2 - 2x_4^2$;
f) $x_1^2 + x_1x_2 + x_3x_4$.

2.77. feladat. Redukáljuk négyzetösszegre a következő kvadratikus alakokat:
a) $\sum_{i=1}^{n} x_i^2 + \sum_{i<k} x_ix_k$;
b) $\sum_{i<k} x_ix_k$.

2.5.3. Sylvester-féle tehetetlenségi törvény

Egy valós kvadratikus alak négyzetösszegé transzformált alakja nem egyértelmű. Ebben a paragrafusban bebizonyítjuk, hogy ennek ellenére, a pozitív és a negatív együtthatók száma egyértelmű.

2.5.9. tétel (Sylvester). *Legyen* $q(x) = \beta(x,x)$ *egy valós kvadratikus alak,* $\operatorname{rang}\beta = r$. *Feltételezzük, hogy az* $e = (e_1, \dots, e_n)$ *bázisban*

$$q(x) = \sum_{i=1}^{p} a_{ii}x_i^2 - \sum_{j=p+1}^{p+q} a_{jj}x_j^2,$$

ahol $a_{ii}, a_{jj} > 0$, $p + q = r$, *és az* $e' = (e'_1, \dots, e'_n)$ *bázisban*

$$q(x) = \sum_{i=1}^{p'} a'_{ii}{x'_i}^2 - \sum_{j=p'+1}^{p'+q'} a'_{jj}{x'_j}^2,$$

ahol $a'_{ii}, a'_{jj} > 0$, $p' + q' = r$.

Ekkor $p = p'$ *és* $q = q'$. (A (p,q) számpárt a $q(x)$ **szignatúrájának** nevezzük).

Bizonyítás. Legyen $U = \langle e_1, \dots, e_p, e_{r+1}, \dots, e_n\rangle \le \mathbb{R}^n$, $W = \langle e'_{p'+1}, \dots, e'_r\rangle$, és feltételezzük, hogy $p > p'$. Ekkor $\dim_{\mathbb{R}} U = p + n - r$ és $\dim_{\mathbb{R}} W = r - p' > r - p$, tehát $\dim_{\mathbb{R}} U + \dim_{\mathbb{R}} W > r + n - r = n$. Továbbá $\dim_{\mathbb{R}}(U + W) \le n$, mert $U + W \le \mathbb{R}^n$; következik, hogy

$$\dim_{\mathbb{R}}(U \cap W) = \dim_{\mathbb{R}} U + \dim_{\mathbb{R}} W - \dim_{\mathbb{R}}(U + W) \ge 1,$$

tehát az $U \cap W$ résztér tartalmaz egy nemnulla x_0 vektort.

Legyen $x_0 = \xi_{i_1}e_1 + \dots + \xi_{i_p}e_p + \xi_{r+1}e_{r+1} + \dots + \xi_n e_n = \eta_{p'+1}e'_{p'+1} + \dots + \eta_r e'_r \in U \cap W$, ahol $\xi_i, \eta_j \in \mathbb{R}$. Ekkor

$$q(x_0) = \sum_{i=1}^{p} a_{ii}\xi_i^2 = -\sum_{j=p'+1}^{p'+q'} a'_{jj}\eta_j^2,$$

ami ellentmondás, mert $a_{ii} \ge 0$ és $a'_{jj} > 0$. ■

2.5.4. Hermitikus alakok

Ha $K = \mathbb{C}$ a komplex számok teste, akkor célszerű figyelembe venni a $\mathbb{C} \to \mathbb{C}$, $z \mapsto \bar{z}$ testautomorfizmust, ahol $\overline{x + yi} = x - yi$ a $z = x + yi$ komplex szám **konjugáltja**. A hermitikus alakokat Charles Hermite (1822–1901) francia matematikus vezette be.

Legyen V egy $\mathbb{C}$-feletti vektortér, $\dim_{\mathbb{C}} V = n$, és $e = (e_1, \dots, e_n)$ egy bázisa. Megemlítjük, hogy ha $A \in M_{m,n}(\mathbb{C})$, akkor értelmezés szerint, $A^h = \bar{A}^t$ (azaz $a_{ij}^h = \bar{a}_{ij}$) az A mátrix (**klasszikus**) **adjungáltja**. Más jelölés: $A^h = A^*$.

2.5.10. definíció. a) A $\beta : V \times V \to \mathbb{C}$ függvényt **komplex bilineáris alaknak** nevezzük ha minden $a, b \in \mathbb{C}$ és minden $x, x_1, x_2, y, y_1, y_2 \in V$ esetén

$$\beta(ax_1 + bx_2, y) = \bar{a}\beta(x_1, y) + \bar{b}\beta(x_2, y),$$

$$\beta(x, ay_1 + by_2) = a\beta(x, y_1) + b\beta(x, y_2).$$

b) Ha $a_{ij} = \beta(e_i, e_j)$, $1 \le i, j \le n$, és $A = [a_{ij}]_{1\le i,j\le n} \in M_n(K)$, akkor azt mondjuk, hogy A a β mátrixa az e bázisban. Jelölés: $A = [\beta]_e$.

c) Értelmezés szerint, $\operatorname{rang}\beta = \operatorname{rang}[\beta]_e$; azt mondjuk, hogy β **degenerált**, ha $\operatorname{rang}\beta < n$ (azaz $\det[\beta]_e = 0$), és β **nem degenerált** ha $\operatorname{rang}\beta = n$.

d) β **hermitikus alak**, ha

$$\beta(x, y) = \overline{\beta(y, x)}$$

minden $x, y \in V$ esetén.

e) Ha $\beta : V \times V \to \mathbb{C}$ egy hermitikus alak, akkor

$$q : V \to \mathbb{C}, \quad q(x) = \beta(x, x)$$

a β-hoz tartozó **kvadratikus alak**.

f) Azt mondjuk, hogy β (vagy q) **kanonikus alakú** az e-bázisban, ha $[\beta]_e$ diagonális mátrix.

2.5.11. lemma. *Legyen $\beta : V \times V \to K$ egy bilineáris alak.*

a) *Minden $x, y \in V$ esetén*

$$\beta(x, y) = [x]_e^h [\beta]_e [y]_e.$$

b) *β akkor és csak akkor hermitikus alak, ha $A = [\beta]_e$ önadjungált mátrix (vagyis $A^h = A$).*

c) *Legyen $e' = (e'_1, \dots, e'_n)$ egy második bázis, és $T = T_e^{e'}$ az e bázisról az e' bázisra való áttérési mátrix. Ekkor*

$$[\beta]_{e'} = T^h [\beta]_e T.$$

d) *Ha β hermitikus, akkor $q(x) = \beta(x, x) \in \mathbb{R}$ minden $x, y \in V$ esetén.*

Bizonyítás. a) Ha $x = \sum_{i=1}^n x_i e_i$ és $y = \sum_{i=1}^n y_i e_i$, akkor

$$\begin{aligned}\beta(x, y) &= \beta\Big(\sum_{i=1}^n x_i e_i, \sum_{i=1}^n y_i e_i\Big) = \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \beta(e_i, e_j)\\ &= \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i a_{ij} y_j = [x]_e^h A [y]_e.\end{aligned}$$

b) Ha β hermitikus, akkor $a_{ij} = \beta(e_i, e_j) = \overline{\beta(e_j, e_i)} = \overline{a_{ji}}$, minden $i, j \in \{1, \dots, n\}$ esetén, tehát $A = A^h$.
Fordítva, ha $A = A^h$, akkor minden $x, y \in V$ esetén,

$$\begin{aligned}\beta(x, y) &= \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i a_{ij} y_j = \sum_{j=1}^n \sum_{i=1}^n y_j \bar{a}_{ji} \bar{x}_i\\ &= \overline{\sum_{j=1}^n \sum_{i=1}^n \bar{y}_j a_{ji} x_i} = \overline{\beta(y, x)}.\end{aligned}$$

c) Ha $x, y \in V$, akkor $[x]_e = T[x]_{e'}$, $[x]_e^h = [x]_{e'}^h T^h$ és

$$\beta(x, y) = [x]_e^h [\beta]_e [y]_e = [x]_{e'}^h [\beta]_{e'} [y]_{e'} = [x]_{e'}^h T^h [\beta]_e T [y]_{e'}$$

Behelyesítve az $[x]_{e'}$ és $[y]_{e'}$ oszlopmátrixokat az $e_1, \dots, e_n$ mátrixokkal, kapjuk, hogy $T^h [\beta]_e T = [\beta]_{e'}$.

d) $\overline{q(x)} = \overline{\beta(x, x)} = \overline{\overline{\beta(x, x)}} = \beta(x, x) = q(x)$, tehát $q(x) \in \mathbb{R}$. ■

2.5.12. megjegyzés. a) Mivel $T = T_e^{e'}$ invertálható mátrix, $\operatorname{rang}\beta = \operatorname{rang}[\beta]_e$ nem függ az e bázistól.

b) Ha β hermitikus és $[\beta]_e = A$, akkor

$$\beta(x, y) = \sum_{i,j=1}^n \bar{x}_i a_{ij} y_j,$$

$$q(x) = \sum_{i,j=1}^n a_{ij} \bar{x}_i x_j = \sum_{i=1}^n a_{ii} |x_i|^2 + \sum_{i \ne j} a_{ij} \bar{x}_i x_j.$$

c) Ha β hermitikus, akkor $q(x) \in \mathbb{R}$ minden $x \in V$ esetén, tehát értelmezhetjük a következő fogalmakat:
q *pozitív definit*, ha $q(x) > 0$ minden $x \in V \setminus \{0\}$ esetén;

q *pozitív szemidefinit*, ha $q(x) \geq 0$ minden $x \in V$ esetén;
q *negatív definit*, ha $q(x) < 0$ minden $x \in V \setminus \{0\}$ esetén;
q *negatív szemidefinit*, ha $q(x) \leq 0$ minden $x \in V$ esetén;
q *indefinit* a többi esetben.
d) Ha β kanonikus alakú az e bázisban és $[\beta]_e = \mathrm{diag}(\lambda_1, \ldots, \lambda_n)$, akkor

$$\beta(x, y) = \sum_{i=1}^{n} \lambda_i \bar{x}_i y_i \quad \text{és} \quad q(x) = \sum_{i=1}^{n} \lambda_i |x_i|^2.$$

2.78. feladat. Legyen $B(V, \mathbb{C}) = \{\beta : V \times V \to K \mid \beta \text{ komplex bilineáris}\}$, $q : B(V, \mathbb{C}) \to \mathbb{C}^V$, $q(\beta)(x) = \beta(x, x)$ és $Q(V, \mathbb{C}) = \mathrm{Im}\, q \subseteq \mathbb{C}^V$ a *kvadratikus alakok* halmaza. Igazoljuk, hogy:
a) $\beta(x, y) = \frac{1}{4}[\beta(x + y, x + y) + i\beta(ix + y, ix + y) - \beta(-x + y, -x + y) - i\beta(-ix + y, -ix + y)]$.
b) q injektív függvény.
c) β akkor és csak akkor hermitikus, ha $\beta(x, x) \in \mathbb{R}$ minden $x \in V$ esetén.

2.6. Euklideszi tér és unitér tér

Ebben a fejezetben $K = \mathbb{R}$ a valós számok teste, vagy $K = \mathbb{C}$ a komplex számok teste.

2.6.1. Skaláris szorzat

Legyen U egy K-feletti vektortér, $\dim_K U = n$ és $\beta : U \times U \to K$ egy hermitikus alak (ha $K = \mathbb{R}$, akkor β szimmetrikus).

2.6.1. definíció. a) Azt mondjuk, hogy (U, β) **unitér tér** ha β nemdegenerált és pozitív definit hermitikus alak (ha $K = \mathbb{R}$, akkor az (U, β) párt **euklideszi tér**nek nevezzük).
b) $\langle x, y \rangle = \beta(x, y)$ az $x, x \in U$ vektorok **skaláris szorzata**.
c) $\|x\| = \sqrt{q(x)} = \sqrt{\beta(x, x)}$ az x vektor **normája**.
d) Az $x, y \in V$ vektorok **ortogonálisak** (jelölés: $x \perp y$), ha $\langle x, y \rangle = 0$. (A „$\perp$” reláció szimmetrikus.)
e) Ha $X \subseteq U$, akkor $X^\perp = \{y \in U \mid \forall x \in X\ x \perp y\}$ az X **ortogonális komplementuma**.

2.6.2. példa. a) Ha $K = \mathbb{R}$, $U = \mathbb{R}^n$ és $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in V$, akkor

$$\langle x, y \rangle = \sum_{i=1}^{n} x_i y_i$$

az x, y vektorok **standard skaláris szorzata.**
b) Ha $K = \mathbb{C}$, $U = \mathbb{C}^n$ és $e = (e_1, \ldots, e_n)$ a kanonikus bázis, $x = (x_1, \ldots, x_n)$, $y = (y_1, \ldots, y_n) \in V$, akkor

$$\langle x, y \rangle = \sum_{i=1}^{n} \bar{x}_i y_i$$

az x, y **standard skaláris szorzata.**
Vegyük észre, hogy mindkét esetben, $[\beta]_e = I_n$, ahol $e = (e_1, \ldots, e_n)$ az U kanonikus bázisa.

2.6.3. lemma. *Legyen* $(U, \langle -, - \rangle)$ *egy unitér tér és* $x, y \in U$.
a) $\|x\| \geq 0$; $\|x\| = 0 \Leftrightarrow x = 0$.
b) $\|ax\| = |a|\|x\|$, $\forall a \in K$.
c) $|\langle x, y \rangle| \leq \|x\| \cdot \|y\|$ **(Cauchy–Schwartz-egyenlőtlenség).**
d) $\|x + y\| \leq \|x\| + \|y\|$ **(Minkowski-egyenlőtlenség)**.

Bizonyítás. a) következik a β pozitív definitségéből.
b) $\|ax\| = \sqrt{\langle ax, ax \rangle} = \sqrt{a\bar{a}\langle x, x \rangle} = |a| \cdot \|x\|$.

c) Az állítás igaz ha $x = 0$, mert ebben az esetben $\langle x, y\rangle = 0$. Feltételezzük, hogy $x \neq 0$, tehát $\langle x, x\rangle > 0$. Ekkor

$$\begin{aligned}
0 &\leq \langle \frac{\langle x, y\rangle}{\langle x, x\rangle} x - y, \frac{\langle x, y\rangle}{\langle x, x\rangle} x - y\rangle \\
&= \langle \frac{\langle x, y\rangle}{\langle x, x\rangle} x, \frac{\langle x, y\rangle}{\langle x, x\rangle} x\rangle - \langle y, \frac{\langle x, y\rangle}{\langle x, x\rangle} x\rangle - \langle \frac{\langle x, y\rangle}{\langle x, x\rangle} x, y\rangle + \langle y, y\rangle \\
&= \frac{\overline{\langle x, y\rangle}}{\langle x, x\rangle} \frac{\langle x, y\rangle}{\langle x, x\rangle} \langle x, x\rangle - \frac{\langle x, y\rangle}{\langle x, x\rangle} \langle y, x\rangle - \frac{\overline{\langle x, y\rangle}}{\langle x, x\rangle} \langle x, y\rangle + \langle y, y\rangle \\
&= \frac{\langle x, y\rangle \langle y, x\rangle}{\langle x, x\rangle} - \frac{\langle x, y\rangle \langle y, x\rangle}{\langle x, x\rangle} - \frac{\langle y, x\rangle \langle x, y\rangle}{\langle x, x\rangle} + \langle y, y\rangle \\
&= \langle y, y\rangle - \frac{\langle x, y\rangle \langle y, x\rangle}{\langle x, x\rangle}.
\end{aligned}$$

Mivel $\langle x, x\rangle > 0$ következik, hogy $0 \leq \langle x, x\rangle \langle y, y\rangle - \langle x, y\rangle \langle y, x\rangle$, tehát

$$|\langle x, y\rangle|^2 = \langle x, y\rangle \overline{\langle x, y\rangle} = \langle x, y\rangle \langle y, x\rangle \leq \langle x, x\rangle \langle y, y\rangle = \|x\|^2 \|y\|^2.$$

d) A skaláris szorzat tulajdonságaiból következik, hogy

$$\begin{aligned}
\langle x + y, x + y\rangle &= \langle x, x\rangle + \langle x, y\rangle + \langle y, x\rangle + \langle y, y\rangle \\
&= \langle x, x\rangle + \langle x, y\rangle + \overline{\langle x, y\rangle} + \langle y, y\rangle \\
&= \langle x, x\rangle + 2\Re\langle x, y\rangle + \langle y, y\rangle.
\end{aligned}$$

A Cauchy-Schwartz-egyenlőtlenséget felhasználva kapjuk, hogy $2\Re\langle x, y\rangle \leq 2|\langle x, y\rangle| \leq 2\|x\| \, \|y\|$, tehát

$$\|x + y\| \leq \|x\| + 2\|x\| \, \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2. \qquad \blacksquare$$

2.79. feladat. Legyen $(U, \langle -, -\rangle)$ egy unitér tér és $x, y \in U$.
a) $|\langle x, y\rangle| = \|x\| \, \|y\| \Leftrightarrow x, y$ lineárisan független.
b) (Pitagorasz-tétel) Ha $x \perp y$, akkor $\|x + y\|^2 = \|x\|^2 + \|y\|^2$. Ha $K = \mathbb{R}$, akkor a fordított implikáció is igaz.
c) $\|x + y\|^2 + \|x - y\|^2 = 2\|x\|^2 + 2\|y\|^2$ (paralelogramma-azonosság).
d) Ha $K = \mathbb{R}$ és $\|x\| = \|y\|$, akkor $x + y \perp x - y$ (rombusz átlói merőlegesek).
e) (cosinus-tétel) Ha $K = \mathbb{R}$, akkor

$$\|x + y\|^2 = \|x\|^2 + \|y\|^2 + 2\langle x, y\rangle.$$

Ha $K = \mathbb{C}$, akkor

$$\|x + y\|^2 - i\|ix + y\|^2 = \|x\|^2 + \|y\|^2 - i(\|x\|^2 + \|y\|^2) + 2\langle x, y\rangle.$$

2.80. feladat. Ha $X \subseteq U$ egy részhalmaz, akkor
a) $X^\perp \leq_K V$.
b) $X^{\perp\perp} \supseteq X$.
c) $\langle X\rangle^\perp = X^\perp$.

2.81. feladat. Feltételezzük, hogy $K = \mathbb{C}$ és legyen $f \in \mathrm{End}_K(U)$. Igazoljuk, hogy ha $\langle u(x), x\rangle = 0$ minden $x \in U$ esetén, akkor $f = \theta$. Ha $K = \mathbb{R}$, akkor az álítás nem igaz. Például legyen $U = \mathbb{R}^2$ és $[f]_{e,e} = \begin{pmatrix} \cos\frac{\pi}{2} & \sin\frac{\pi}{2} \\ -\sin\frac{\pi}{2} & \cos\frac{\pi}{2} \end{pmatrix}$.

2.6.2. Ortonormált bázis

Legyen $(U, \langle -, -\rangle)$ egy unitér tér.

2.6.4. definíció. a) Legyenek $v_1, \ldots, v_r \in U$ nemnulla vektorok. Az $(v_1, \ldots, v_r)$ rendszert **ortogonális**nak nevezzük, ha $\langle v_i, v_j\rangle = 0$ minden $i \neq j$ esetén.

b) Azt mondjuk, hogy a $(v_1, \ldots, v_r)$ rendszer **ortonormált**, ha ortogonális, és $\|v_i\| = 1$ minden $i \in \{1, \ldots, r\}$ esetén (azaz $\langle v_i, v_j\rangle = \delta_{ij} \ \forall i, j \in \{1, \ldots, r\}$).

2.82. feladat. Ha $(v_1, \ldots, v_r)$ ortogonális rendszer, akkor lineárisan független is.

2.83. feladat. Ha e ortonormált bázis és $x = \sum_{i=1}^{n} x_i e_i$, $y = \sum_{i=1}^{n} y_i e_i$, akkor
a) $x_i = \langle e_i, x\rangle$, $\bar{x}_i = \langle x, e_i\rangle$ $\forall i \in \{1, \dots, n\}$.
b) $\langle x, y\rangle = \sum_{i=1}^{n} \bar{x}_i y_i \in K$ (**Parseval-azonosság**).
c) $\|x\| = \sqrt{\sum_{i=1}^{n} |x_i|^2} \in \mathbb{R}$.

2.84. feladat. Ha $A \in M_n(\mathbb{R})$, akkor a következő állítások ekvivalensek:

1. $A \in O(n)$ (azaz A ortogonális mátrix).
2. $(o_1^A, \dots, o_n^A)$ ortonormált rendszer.
3. $(s_1^A, \dots, s_n^A)$ ortonormált rendszer.

2.6.5. tétel (Bessel-egyenlőtlenség). *Ha $(e_1, \dots, e_r)$ ortonormált rendszer és $x \in U$, akkor*

$$\sum_{i=1}^{r} |\langle e_i, x\rangle|^2 \le \|x\|^2.$$

Bizonyítás. A skaláris szorzat tulajdonságaiból következik, hogy

$$\begin{aligned}
0 &\le \langle x - \sum_{i=1}^{r} \langle e_i, x\rangle e_i, x - \sum_{i=1}^{r} \langle e_i, x\rangle e_i\rangle \\
&= \langle x, x\rangle - \sum_{i=1}^{r} \langle e_i, x\rangle\langle x, e_i\rangle - \sum_{i=1}^{r} \overline{\langle e_i, x\rangle}\langle e_i, x\rangle + \sum_{i=1}^{r}\sum_{j=1}^{r} \langle e_i, x\rangle\overline{\langle e_j, x\rangle}\langle e_i, e_j\rangle \\
&= \langle x, x\rangle - \sum_{i=1}^{r} \langle e_i, x\rangle\overline{\langle e_i, x\rangle} - \sum_{i=1}^{r} \langle e_i, x\rangle\overline{\langle e_i, x\rangle} + \sum_{i=1}^{r} \langle e_i, x\rangle\overline{\langle e_i, x\rangle} \\
&= \|x\|^2 - \sum_{i=1}^{r} |\langle e_i, x\rangle|^2. \qquad \blacksquare
\end{aligned}$$

2.6.6. megjegyzés. a) Legyen $v = x - \sum_{i=1}^{r} \langle e_i, x\rangle e_i$ a bizonyításban szereplő vektor és $V = \langle e_1, \dots, e_r\rangle$ az $e_1, \dots, e_r$ által generált résztér. Ekkor $v \perp e_i$ minden $i \in \{1, \dots, r\}$ esetén, tehát $v \in V^\perp$.

b) A Bessel-egyenlőtlenség általánosítja a Cauchy–Schwartz-egyenlőtlenséget. Valóban, ha $y \ne 0$, akkor $\frac{1}{\|y\|} y$ ortonormált rendszert képez, tehát

$$\frac{1}{\|y\|^2} |\langle x, y\rangle|^2 = |\langle x, \frac{1}{\|y\|} y\rangle|^2 \le \|x\|^2.$$

2.6.7. tétel (Gram–Schmidt-ortogonalizáció). *Ha $(U, \langle -, -\rangle)$ egy unitér tér, akkor U-nak van egy $e = (e_1, \dots, e_n)$ ortonormált bázisa.*

Bizonyítás. Legyen $v = (v_1, \dots, v_n)$ egy bázis V-ben, és indukcióval definiálunk egy $u = (u_1, \dots, u_n)$ ortogonális bázist.

Legyen $u_1 := v_1$ és $u_2 := a_{12} u_1 + v_2$ úgy, hogy $\langle u_1, u_2\rangle = 0$. Mivel

$$0 = \langle u_1, u_2\rangle = a_{12}\langle u_1, u_1\rangle + \langle u_1, v_2\rangle,$$

következik, hogy $a_{12} = -\frac{\langle u_1, v_2\rangle}{\|u_1\|^2}$.

Mivel $(u_1, v_2, \dots, v_n)$ bázis, a kicserélési lemmából következik, hogy $(u_1, u_2, v_3, \dots, v_n)$ is bázis. Vegyük észre azt is, hogy $\langle\{u_1, u_2\}\rangle = \langle\{v_1, v_2\}\rangle$.

Feltételezzük, hogy megszerkesztettük az $(u_1, \dots, u_{j-1})$ ortogonális rendszert úgy, hogy $\langle u_1, \dots u_{j-1}\rangle = \langle v_1, \dots, v_{j-1}\rangle$ és $(u_1, \dots, u_{j-1}, v_j, \dots, v_n)$ bázis. Meghatározzuk az

$$u_j = a_{1j} u_1 + a_{2j} u_2 + \dots + a_{j-1\ j} u_{j-1} + v_j$$

vektort úgy, hogy $\langle u_i, u_j\rangle = 0$, $1 \le i \le j-1$. A feltételből következik, hogy

$$\boxed{a_{ij} = -\frac{\langle u_i, v_j\rangle}{\|u_i\|^2}, \quad 1 \le i \le j-1}.$$

Az u_j értelmezéséből következik, hogy $\langle u_1, \dots, u_j\rangle = \langle v_1, \dots, v_r\rangle$, és a kicserélési lemmából következik, hogy $(u_1, \dots, u_j, v_{j+1}, \dots, v_n)$ is bázis.

Végűl, legyen $e_i = \frac{1}{\|u_i\|} u_i$, $1 \le i \le n$. $\blacksquare$

2.85. feladat. Ortogonalizáljuk a következő vektorrendszereket (*Gram–Schmidt-eljárás*):
a) $(1,-1,2)$, $(2,0,-3)$, $(6,-3,0)$;
b) $(1,2,1,3)$, $(4,1,1,1)$, $(3,1,1,0)$;
c) $(1,2,2,-1)$, $(1,1,-5,3)$, $(3,2,8,-7)$;
d) $(2,1,3,-1)$, $(7,4,3,-3)$, $(1,1,-6,0)$; $(5,7,7,8)$.

2.6.8. tétel. *Legyen* U *egy unitér tér és* $V \leq_K U$. *Ekkor*
a) $V + V^\perp = U$, $V \cap V^\perp = \{0\}$.
b) *Ha* $W \leq_K U$ *úgy, hogy* $W \perp V$, $W + V = U$ *és* $W \cap V = \{0\}$, *akkor* $W = V^\perp$.
c) $V^{\perp\perp} = V$.

Bizonyítás. Ha $V = \{0\}$, akkor $V^\perp = U$ és $V^{\perp\perp} = \{0\}$, tehát feltételezhetjük, hogy $V \neq \{0\}$. Legyen $(e_1, \dots, e_m)$ V-ban ortonormált bázis, és egészítsük ezt ki U egy $(e_1, \dots, e_m, e_{m+1}, \dots, e_n)$ ortonormált bázisává.

a) Nyivánvaló, hogy $V^\perp \geq \langle e_{m+1}, \dots, e_n \rangle$, így $V + V^\perp = \langle V \cup V^\perp \rangle = U$. Ha $x \in V \cap V^\perp$, akkor $\langle x, x \rangle = 0$, tehát $x = 0$.

b) Feltételezzük, hogy $W + V = U$, $W \cap V = \{0\}$ és $W \perp V$. Ekkor $W \subseteq V^\perp$ és $\dim_K W = \dim_K U - \dim_K V = \dim_K V^\perp$, tehát $W = V^\perp$.

c) Legyen $W = V^\perp$; ekkor mivel $V \perp W$, $V + W = U$ és $V \cap W = \{0\}$, a b) pontból következik, hogy $V = W^\perp = V^{\perp\perp}$. ■

2.86. feladat. Határozzunk meg egy ortonormált bázist a $V^\perp$ résztérben, ha V a következő vektorok által generált résztér:
a) $(1,1) \in \mathbb{R}^2$; b) $(1,-2) \in \mathbb{R}^2$;
c) $(1,1,0)$, $(1,1,1) \in \mathbb{R}^3$; d) $(1,-2,2)$, $(-3,0,1) \in \mathbb{R}^3$;
e) $(1,1,1) \in \mathbb{R}^3$; f) $(-1,2,-3) \in \mathbb{R}^3$.

2.87. feladat. Legyen U egy unitér tér és $V, W \leq_K V$. Bizonyítsuk be, hogy

$$(V + W)^\perp = V^\perp \cap W^\perp, \qquad (V \cap W)^\perp = V^\perp + W^\perp.$$

2.6.3. Ortogonális és unitér transzformációk

2.6.9. definíció. Legyenek $(U, \langle -,- \rangle)$ és $(U', \langle -,- \rangle)$ unitér terek. Az $f : U \to U'$ függvényt *izometriának* nevezzük ha

1. f vektortérizomorfizmus
2. minden $x, y \in U$ esetén $\langle f(x), f(y) \rangle = \langle x, y \rangle$.

Ebben az esetben azt mondjuk, hogy U és U' *izomorfak*.

2.6.10. tétel. $(U, \langle -,- \rangle) \simeq (U', \langle -,- \rangle)$ *pontosan akkor, ha* $\dim_K U = \dim_K U'$.

Bizonyítás. Ha $U \simeq U'$, akkor $\dim_K U = \dim_K U'$. Fordítva, feltételezzük, hogy $\dim_K U = \dim_K U'$ és legyen $e = (e_1, \dots, e_n)$ egy ortonormált bázis U-ban és $e' = (e'_1, \dots, e'_n)$ egy ortonormált bázis U'-ben. Létezik egyetlen olyan $f : U \to U'$ lineáris függvény amelyre $f(e_i) = e'_i$, $i = 1, \dots, n$. Mivel e és e' bázisok, következik, hogy f vektortérizomorfizmus.

Ha $x = \sum_{i=1}^n x_i e_i$, $y = \sum_{i=1}^n y_i e_i \in U$ akkor

$$\begin{aligned}
\langle f(x), f(y) \rangle &= \langle \sum_{i=1}^n x_i f(e_i), \sum_{j=1}^n y_j f(e_j) \rangle = \langle \sum_{i=1}^n x_i e'_i, \sum_{j=1}^n y_j e'_j \rangle \\
&= \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \langle e'_i, e'_j \rangle = \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \delta_{ij} \\
&= \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \langle e_i, e_j \rangle = \langle \sum_{i=1}^n y_i e_i, \sum_{j=1}^n y_j e_j \rangle = \langle x, y \rangle. \qquad ■
\end{aligned}$$

Következik, hogy ha $\dim_K U = n$, akkor $(U, \langle -,- \rangle) \simeq (K^n, \langle -,- \rangle)$ (standard skaláris szorzat). Az alábbiakban az $(U, \langle -,- \rangle)$ endomorfizmusait vizsgáljuk.

2.6.11. tétel (unitér transzformáció jellemzése). *Legyen* $f \in \mathrm{End}_K(U)$. *A következő állítások ekvivalensek:*
(i) $\langle f(x), f(y) \rangle = \langle x, y \rangle$, *minden* $x, y \in U$ *esetén.*
(ii) $\|f(x)\| = \|x\|$ *minden* $x \in U$ *esetén.*
(iii) *Ha* $u = (u_1, \dots, u_n)$ U*-beli ortonormált bázis, akkor* $(f(u_1), \dots, f(u_n))$ *is ortonormált bázis.*
(iv) *Ha* $u = (u_1, \dots, u_n)$ U*-beli ortonormált bázis, akkor* $[f]_{u,u}$ *unitér mátrix.*

Ebben az esetben, azt mondjuk, hogy f **unitér transzformáció** (**ortogonális**, ha $K = \mathbb{R}$.)

Bizonyítás. "(i) $\Leftrightarrow$ (ii)" következik a 2.78. feladatból.

"(i)$\Rightarrow$(iii)" Ha u ortonormált bázis, akkor

$$\langle f(u_i), f(u_j)\rangle = \langle u_i, u_j\rangle = \delta_{ij},$$

tehát $f(u)$ is ortonormált bázis.

"(iii)$\Rightarrow$(i)" Minden $x = \sum_{i=1}^n x_i u_i$, $y = \sum_{i=1}^n y_i u_i \in U$ esetén,

$$\begin{aligned}\langle f(x), f(y)\rangle &= \langle \sum_{i=1}^n x_i f(u_i), \sum_{j=1}^n y_j f(u_j)\rangle = \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \langle u_i, u_j\rangle \\ &= \langle \sum_{i=1}^n x_i u_i, \sum_{i=1}^n y_j u_j\rangle = \langle x, y\rangle.\end{aligned}$$

"(iii)$\Leftrightarrow$(iv)" Legyen u ortonormált bázis és $A = [f]_{u,u}$. Ekkor

$$\begin{aligned} f(u) \text{ ortonormált bázis } &\iff \langle f(u_i), f(u_j)\rangle = \delta_{ij} \\ &\iff \langle \sum_{k=1}^n a_{ki} u_k, \sum_{l=1}^n a_{lj} u_l\rangle = \delta_{ij} \\ &\iff \sum_{k=1}^n \sum_{l=1}^n \bar{a}_{ki} a_{lj} \langle u_k, u_l\rangle = \delta_{ij} \\ &\iff \sum_{k=1}^n \bar{a}_{ki} a_{kj} = \delta_{ij} \quad (\text{mivel } \langle u_k, u_l\rangle = \delta_{kl}) \\ &\iff \langle o_i^A, o_j^A\rangle = \delta_{ij} \\ &\iff A \text{ unitér mátrix.} \qquad \blacksquare \end{aligned}$$

2.88. feladat. Legyenek $f, g \in \mathrm{End}_K(U)$ ortogonális (unitér) transzformációk. Igazoljuk, hogy f bijektív, $g \circ f$ és f^{-1} ortogonális (unitér) transzformációk.

2.6.4. Adjungált transzformáció

Legyen $(U, \langle -, -\rangle)$ egy unitér tér, $\dim_K U = n$, $e = (e_1, \dots, e_n)$ egy ortonormált bázisa és $f \in \mathrm{End}_K(U)$ egy lineáris függvény.

2.6.12. tétel. *Létezik az egyértelműen meghatározott* $f^* \in \mathrm{End}_K(U)$ *úgy, hogy minden* $x, y \in U$ *esetén*

$$\langle f(x), y\rangle = \langle x, f^*(y)\rangle.$$

Ha $K = \mathbb{C}$ *akkor* $[f^*]_{e,e} = [f]_{e,e}^h = \overline{[f]}_{e,e}^t$, *és ha* $K = \mathbb{R}$, *akkor* $[f^*]_{e,e} = [f]_{e,e}^t$

Bizonyítás. Feltételezzük először, hogy f^* létezik, és legyen $[f]_{e,e} = A = [a_{ij}]$ és $[f^*]_{e,e} = B = [b_{ij}]$. Ekkor

$$\begin{aligned}\langle f(e_i), e_j\rangle = \langle e_i, f^*(e_j)\rangle &\iff \langle \sum_{k=1}^n a_{ki} e_k, e_j\rangle = \langle e_i, \sum_{l=1}^n b_{lj} e_l\rangle \\ &\iff \sum_{k=1}^n \bar{a}_{ki} \langle e_k, e_j\rangle = \sum_{l=1}^n b_{lj} \langle e_i, e_l\rangle \\ &\iff \bar{a}_{ji} = b_{ij} \\ &\iff B = A^h \quad (\text{illetve } B = A^t \text{ ha } K = \mathbb{R}).\end{aligned}$$

A vektorterek univerzális tulajdonságából következik, hogy f^* egyértelműen meghatározott.

Igazoljuk most, hogy f^* létezik. Legyen $b_{ij} = \bar{a}_{ji}$, $1 \le i, j \le n$, és legyen $f^* \in \mathrm{End}_K(U)$, $f^*(e_j) = \sum_{l=1}^n b_{lj} e_l$, $1 \le j \le n$. A fenti számításokból következik, hogy

$$\langle f(e_i), e_j\rangle = \langle e_i, f^*(e_j)\rangle, \quad 1 \le i, j \le n.$$

Ekkor minden $x = \sum_{i=1}^n x_i e_i$, $y = \sum_{j=1}^n y_j e_i \in U$ esetén,

$$\begin{aligned}\langle f(x), y\rangle &= \langle \sum_{i=1}^n x_i f(e_i), \sum_{j=1}^n y_j e_j\rangle = \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \langle f(e_i), e_j\rangle \\ &= \sum_{i=1}^n \sum_{j=1}^n \bar{x}_i y_j \langle e_i, f^*(e_j)\rangle = \langle \sum_{i=1}^n x_i e_i, f^*(\sum_{j=1}^n y_j e_j)\rangle = \langle x, f^*(y)\rangle. \qquad \blacksquare\end{aligned}$$

2.6.13. definíció. a) Az f^* transzformációt az f **adjungált**jának nevezzük.

b) Azt mondjuk, hogy

• f **önadjungált**, illetve **szimmetrikus** $K = \mathbb{R}$ esetben, ha $f^* = f$ (azaz, ha $[f]_{e,e}$ hermitikus, illetve szimmetrikus mátrix).

• f **ferdén önadjungált**, illetve **antiszimmetrikus** $K = \mathbb{R}$ esetben, ha $f^* = -f$ (azaz, ha $[f]^h_{e,e} = -[f]_{e,e}$, illetve $[f]^t_{e,e} = -[f]_{e,e}$ $K = \mathbb{R}$ esetben).

2.89. feladat. Ha $f \in \mathrm{End}_K(U)$, akkor a következő állítások ekvivalensek:

(i) f unitér. (ii) $f \circ f^* = 1_U$. (ii) $f^* \circ f = 1_U$. (iv) $f^* = f^{-1}$.

2.90. feladat. Ha $f, g \in \mathrm{End}_K(U)$ és $a \in K$, akkor $(f+g)^* = f^* + g^*$, $(af)^* = \bar{a}f^*$, $f^{**} = f$ és $(f \circ g)^* = g^* \circ f^*$.

2.6.14. definíció. Legyen $f \in \mathrm{End}_K(U)$ és $V \leq_K U$. Azt mondjuk, hogy V f-*invariáns résztér*, ha $f(V) \subseteq V$.

2.6.15. lemma. *Legyen* $f \in \mathrm{End}_K(U)$ *és* $V \leq_K U$. *Ekkor* V f-*invariáns* $\Leftrightarrow$ $V^\perp$ f^*-*invariáns.*

Bizonyítás. Ha $x \in V^\perp$, akkor igazoljuk, hogy $f^*(x) \in V^\perp$, azaz $\langle y, f^*(x)\rangle = 0$ minden $y \in V$ esetén. De $\langle y, f^*(x)\rangle = \langle f(y), x\rangle = 0$, hiszen $f(y) \in V$ és $x \in V^\perp$. ■

2.6.16. tétel. *Legyen* $f \in \mathrm{End}_K(U)$ *és* $\lambda \in K$ *az* f-*nek egy sajátértéke.*

a) *Ha* f *önadjungált, akkor* $\lambda \in \mathbb{R}$.

b) *Ha* f *ferdén önadjungált, akkor* $\lambda \in i\mathbb{R}$.

c) *Ha* f *unitér, akkor* $|\lambda| = 1$.

Bizonyítás. Legyen $x \in U$, $x \neq 0$.

a) $\bar{\lambda}\langle x, x\rangle = \langle \lambda x, x\rangle = \langle f(x), x\rangle = \langle x, f^*(x)\rangle = \langle x, f(x)\rangle = \langle x, \lambda x\rangle = \lambda\langle x, x\rangle$. Mivel $\langle x, x\rangle \neq 0$, következik, hogy $\lambda = \bar{\lambda}$, tehát $\lambda \in \mathbb{R}$.

b) $\bar{\lambda}\langle x, x\rangle = \langle \lambda x, x\rangle = \langle f(x), x\rangle = \langle x, f^*(x)\rangle = \langle x, -f(x)\rangle = \langle x, -\lambda x\rangle = -\lambda\langle x, x\rangle$. Mivel $\langle x, x\rangle \neq 0$, következik, hogy $-\lambda = \bar{\lambda}$, tehát $\lambda \in i\mathbb{R}$.

c) $\langle x, x\rangle = \langle x, f^*(f(x))\rangle = \langle f(x), f(x)\rangle = \langle \lambda x, \lambda x\rangle = \bar{\lambda}\lambda\langle x, x\rangle$. Következik, hogy $\bar{\lambda}\lambda = 1$, tehát $|\lambda| = 1$. ■

2.91. feladat. Legyen $f \in \mathrm{End}_K(U)$ egy unitér transzformáció és $V \leq_K U$. Igazoljuk, hogy ha V f-invariáns, akkor $V^\perp$ is f-invariáns.

2.92. feladat. Legyen $f \in \mathrm{End}_K(U)$ és $\lambda \in K$ az f-nek egy sajátértéke. Ha létezik $g \in \mathrm{End}_K(U)$ úgy, hogy $f = g^* \circ g$, akkor $\lambda \in \mathbb{R}_+$.

Megoldás. $\lambda\langle x, x\rangle = \langle x, \lambda x\rangle = \langle x, f(x)\rangle = \langle x, g^*(g(x))\rangle = \langle g(x), g(x)\rangle$, tehát $\lambda = \frac{\|g(x)\|^2}{\|x\|^2} \geq 0$.

2.6.5. Normális transzformációk

Legyen $(U, \langle -, -\rangle)$ egy unitér tér, $e = (e_1, \ldots, e_n)$ egy ortonormált bázisa és $f \in \mathrm{End}_K(U)$ egy lineáris függvény.

2.6.17. definíció. Azt mondjuk, hogy f **normális transzformáció**, ha $f^* \circ f = f \circ f^*$.

2.93. feladat. a) f akkor és csak akkor normális, ha $[f]_{e,e}$ normális, azaz $[f]^*_{e,e}[f]_{e,e} = [f]_{e,e}[f]^*_{e,e}$.

b) Ha f unitér, önadjungált, vagy ferdén önadjungált, akkor f normális.

c) Feltételezzük, hogy f, g önadjungált, és legyen $a \in K$. Ekkor $f + g, af$ is önadjungáltak; $f \circ g$ akkor és csak akkor önadjungált, ha $f \circ g = g \circ f$.

d) Ha f, g normálisak és $f \circ g^* = g^* \circ f$, akkor $f + g, f \circ g$ is normálisak.

e) Ha $|a| = |b|$ akkor $ag + bf^*$ normális.

2.94. feladat. Legyen $f \in \mathrm{End}_K(U)$ egy normális transzformáció.

a) Minden $x \in U$ esetén, $\|f^*(x)\| = \|f(x)\|$.

b) Ha $P \in K[X]$ egy polinom, akkor $P(f)$ is normális.

c) $\mathrm{Ker}\, f \cap \mathrm{Im}\, f = \{0\}$.

2.6.18. lemma. *Ha* $f \in \mathrm{End}_K(U)$ *normális transzformáció, akkor* f-*nek minden sajátvektora* f^*-*nak is sajátvektora. Ha* $x \in U$, $x \neq 0$ *és* $f(x) = \lambda x$, *akkor* $f^*(x) = \bar{\lambda}x$.

Bizonyítás. Feltételezzük, hogy $x \neq 0$ és $(f - \lambda 1_U)(x) = 0$. Ekkor

$$\begin{aligned}
0 &= \langle (f - \lambda 1_U)(x), (f - \lambda 1_U)(x)\rangle \\
&= \langle x, (f - \lambda 1_U)^*((f - \lambda 1_U)(x))\rangle \\
&= \langle x, (f^* - \bar{\lambda} 1_U)((f - \lambda 1_U)(x))\rangle \\
&= \langle x, (f - \lambda 1_U)((f^* - \bar{\lambda} 1_U)(x))\rangle \\
&= \langle x, (f - \lambda 1_U)^{**}((f^* - \bar{\lambda} 1_U)(x))\rangle \\
&= \langle (f - \lambda 1_U)^*(x), (f^* - \bar{\lambda} 1_U)(x)\rangle \\
&= \langle (f^* - \bar{\lambda} 1_U)(x), (f^* - \bar{\lambda} 1_U)(x)\rangle,
\end{aligned}$$

tehát $(f^* - \bar{\lambda} 1_U)(x) = 0$. ■

2.6.19. tétel (Komplex spektráltétel). *Feltételezzük, hogy* $K = \mathbb{C}$. *Az* $f \in \mathrm{End}_K(U)$ *transzformáció akkor és csak akkor normális, ha létezik egy* $u = (u_1, \dots, u_n)$ *ortonormált bázis amelyben* f *mátrixa diagonális.*

(Ebben az esetben $u_1, \dots, u_n$ f-nek sajátvektorai és az $[f]_{u,u}$ diagonális elemei az f sajátértékei.)

Bizonyítás. Feltételezzük, hogy f normális. n-re vonatkozó indukciót alkalmazunk; ha $n = 1$, az állítás triviális, és tegyük fel, hogy $n-1$ dimenziós térre igaz. Legyen λ_1 f-nek egy sajátértéke, u_1 egy a λ_1-hez tartozó sajátvektor, $\|u_1\| = 1$, és legyen $V = \langle u_1 \rangle^\perp$. Ekkor $\langle u_1 \rangle + V = U$ és $\langle u_1 \rangle \cap V = \{0\}$. Az előző lemma szerint, $\langle u_1 \rangle$ f-nek és f^*-nak közös invariáns résztere, tehát $V = \langle u_1 \rangle^\perp$ f^*-ra és $f^{**} = f$-re is invariáns résztér, a 2.6.15. lemma szerint. Legyen $g \in \mathrm{End}_K(V)$ az f leszűkítése. Mivel g normális és $\dim_K(V) = n - 1$, az indukció szerint V-ben van egy $(u_2, \dots, u_n)$ ortonormált bázis amely g (tehát f) sajátvektoraiból áll. Következik, hogy $u = (u_1, u_2, \dots, u_n)$ ortonormált bázis, és $[f]_{u,u}$ diagonális.

Fordítva, feltételezzük hogy létezik egy u ortonormált bázis úgy, hogy

$$[f]_{u,u} = D = \mathrm{diag}(\lambda_1, \dots, \lambda_n),$$

Evidens, hogy $DD^* = D^*D$, tehát f normális. ■

2.6.20. következmény. a) *Ha* $f \in \mathrm{End}_{\mathbb{C}}(U)$ *normális transzformáció, akkor a különböző sajátértékekhez tartozó sajátvektorai ortogonálisak.*

b) **(Valós spektráltétel)** *Feltételezzük, hogy* $K = \mathbb{R}$. *Az* $f \in \mathrm{End}_K(U)$ *transzformáció akkor és csak akkor önadjungált, ha létezik egy* $u = (u_1, \dots, u_n)$ *ortonormált bázis amelyben* f *mátrixa diagonális.*

c) **(Kvadratikus alak négyzetösszegé redukciója)** *Legyen* $\beta : V \times V \to K$ *egy hermitikus alak (illetve szimmetrikus, ha* $K = \mathbb{R}$*). Ekkor létezik egy* u *ortonormált bázis úgy, hogy* $[\beta]_u$ *diagonális.*

d) **(Két kvadratikus alak egyidejű négyzetösszegé redukciója)** *Legyen* $\beta_1 : V \times V \to K$ *egy pozitív definit hermitikus alak és* β_2 *egy hermitikus alak (illetve szimmetrikus, ha* $K = \mathbb{R}$*). Ekkor létezik egy* u *ortonormált bázis úgy, hogy* $[\beta_1]_u$ *egységmátrix és* $[\beta_2]_u$ *diagonális.*

Bizonyítás. a) Alkalmazzuk, a fenti tétel bizonyítási módszerét. Vegyük észre, hogy ha λ_1 f-nek egy sajátértéke, akkor $\lambda_1 \in \mathbb{R}$, mivel f önadjungált. ■

2.95. feladat. Redukáljuk négyzetösszegre a következő kvadratikus alakokat (*ortogonális transzformáció* segítségével):

a) $2x_1x_2 + 2x_1x_3 + 2x_2x_3$;
b) $2x_1^2 + x_2^2 - 4x_1x_2 - 4x_2x_3$;
c) $x_1^2 + 2x_2^2 + 3x_3^2 - 4x_1x_2 - 4x_2x_3$;
d) $3x_1^2 + 4x_2^2 + 5x_3^2 + 4x_1x_2 - 4x_2x_3$;
e) $2x_1^2 + 5x_2^2 + 5x_3^2 + 4x_1x_2 - 4x_1x_3 - 8x_2x_3$;
f) $x_1^2 - 2x_2^2 - 2x_3^2 - 4x_1x_2 + 4x_1x_3 + 8x_2x_3$;
g) $5x_1^2 + 6x_2^2 + 4x_3^2 - 4x_1x_2 - 4x_1x_3$;
h) $3x_1^2 + 6x_2^2 + 3x_3^2 - 4x_1x_2 - 8x_1x_3 - 4x_2x_3$;
i) $2x_1x_2 + 2x_3x_4$.

2.96. feladat. Redukáljuk négyzetösszegre a következő kvadratikus alakokat:

a) $\sum_{i=1}^n x_i^2 + \sum_{i<k} x_ix_k$;
b) $\sum_{i<k} x_ix_k$;
c) $\sum_{i=1}^{n-1} x_1x_{i+1}$.

2.97. feladat. Ha $f \in \mathrm{End}_{\mathbb{C}}(U)$ akkor a következő állítások ekvivalensek:

1. f önadjungált.
2. f normális és minden sajátértéke valós szám.
3. Minden $x \in U$ esetén $\langle f(x), x \rangle \in \mathbb{R}$.

2.98. feladat. $f \in \mathrm{End}_{\mathbb{C}}(U)$ akkor és csak akkor unitér, ha normális, és minden sajátértékének modulusza 1.

2.99. feladat. Ha $f \in \mathrm{End}_K(U)$ akkor a következő állítások ekvivalensek:

1. f önadjungált és unitér.
2. f normális és $f^2 = 1_U$.
3. Létezik $V \leq_K U$ úgy, hogy $f(x) = x$ minden $x \in V$ esetén és $f(x) = -x$ minden $x \in V^\perp$ esetén.

2.100. feladat. Ha $f \in \mathrm{End}_{\mathbb{C}}(U)$, akkor léteznek az egyértelműen meghatározott g, h önadjungált transzformációk úgy, hogy $f = g + ih$.

2.101. feladat. Ha $f \in \mathrm{End}_K(U)$, akkor a következő állítások ekvivalensek:

1. f önadjungált és minden sajátértéke pozití v.
2. Létezik egy g önadjungált transzformáció úgy, hogy $g^2 = f$.
3. Létezik egy h transzformáció úgy, hogy $h^* \circ h = f$.
4. Minden $x \in U$ esetén $\langle f(x), x\rangle \geq 0$.

(Ebben az esetben azt mondjuk, hogy f *pozitív.* g egyértelműen meghatározott és $\sqrt{f}$-el jelöljük).

2.102. feladat (Poláris felbontás). Minden $f \in \mathrm{End}_K(U)$ invertálható transzformációhoz léteznek g_1, g_2 pozitív és h_1, h_2 unitér transzformációk úgy, hogy $f = g_1 \circ h_1 = h_2 \circ g_2$. (Ezek a felbontások egyértelműek.)

3. fejezet

Csoportok

3.1. Részcsoportok

3.1.1. Részcsoportok hálója

Legyen $(G, \cdot)$ egy csoport és $\mathcal{S}(G) = \{H \mid H \leq (G, \cdot)\}$ a G csoport részcsoportjainak a halmaza. Vegyük észre, hogy $(\mathcal{S}(G), \subseteq)$ rendezett halmaz.

3.1.1. lemma. *Részcsoportok metszete részcsoport.*

Bizonyítás. Ha I egy indexhalmaz és a H_i-k részcsoportjai G-nek minden $i \in I$ esetén, akkor igazoljuk, hogy

$$\bigcap_{i \in I} H_i = \{x \in G \mid x \in H_i \ \forall i \in I\}$$

részcsoportja G-nek. Valóban, mivel $e \in H_i$ minden $i \in I$ esetén következik, hogy $e \in \bigcap_{i \in I} H_i$; ha $x, y \in \bigcap_{i \in I} H_i$, akkor $x, y \in H_i$ minden $i \in I$ esetén, de a H_i-k részcsoportjai G-nek, ezért $xy^{-1} \in H_i$ minden $i \in I$ esetén, vagyis $xy^{-1} \in \bigcap_{i \in I} H_i$. ■

3.1.2. megjegyzés. A fenti lemmából következik, hogy $(\mathcal{S}(G), \subseteq)$ teljes háló. Ha $B = \{H_i \mid i \in I\} \subseteq \mathcal{S}(G)$, akkor

$$\inf B = \bigcap_{i \in I} H_i \qquad \text{és} \qquad \sup B = \bigcap_{H \leq G, H_i \subseteq H \ \forall i \in I} H.$$

3.1.3. tétel (Részcsoportok megfeleltetési tétele). *Legyen* $f : G \longrightarrow G'$ *egy morfizmus és* $N := \operatorname{Ker} f$.

1) *Ha* H *részcsoportja* G*-nek, akkor* $f^{-1}(f(H)) = NH = HN$*, ahol*

$$NH := \{nh \mid n \in N, h \in H\} \quad \text{és} \quad HN := \{hn \mid h \in H, n \in N\}.$$

2) *Ha* H' *részcsoportja* G'*-nek és* f *szürjektív, akkor* $f(f^{-1}(H')) = H'$.

3) *Feltételezzük, hogy* f *szürjektív. Tekintsük a kövekező függvényeket:*

$$\phi : \{H \leq G \mid N \subseteq H\} \longrightarrow \mathcal{S}(G'), \quad \phi(H) = f(H) = \{f(h) \mid h \in H\},$$

$$\psi : \mathcal{S}(G') \longrightarrow \{H \leq G \mid N \subseteq H\}, \quad \psi(H') = f^{-1}(H') = \{x \in G \mid f(x) \in H'\}.$$

Ekkor ϕ *és* ψ *bijektív, növekvő függvények és* $\phi^{-1} = \psi$. (Azt mondjuk, hogy ϕ, ψ hálóizomorfizmusok.)

Bizonyítás. 1) Ha $x \in f^{-1}(f(H))$, vagyis $f(x) \in f(H)$, akkor létezik $h \in H$ úgy, hogy $f(x) = f(h)$. Szorozva jobbról az $f(h)$ inverzével következik, hogy $f(xh^{-1}) = e'$, vagyis $xh^{-1} \in N$, tehát $x = nh \in NH$. Fordítva, ha $x = nh \in NH$ akkor

$$f(x) = f(nh) = f(n)f(h) = f(h) \in f(H),$$

tehát $x \in f^{-1}(f(H))$. Hasonló módon igazoljuk, hogy $f^{-1}(f(H)) = HN$.

2) Mivel H' részcsoportja G'-nek következik, hogy $f^{-1}(H')$ részcsoportja G-nek, és mivel f szürjektív függvény, következik, hogy $f(f^{-1}(H')) = H'$.

3) Az 1) és 2) pontokból következik, hogy ϕ és ψ jól értelmezett függvények.

Ha $H_1 \subseteq H_2$, akkor $\phi(H_1) = f(H_1) \subseteq f(H_2) = \phi(H_2)$, vagyis ϕ növekvő függvény. Ha $H_1' \subseteq H_2'$, akkor $\psi(H_1') = f^{-1}(H_2') \subseteq f^{-1}(H_2') = \psi(H_2')$, vagyis ψ is növekvő függvény.

Jelöljük $\mathcal{S}$-sel a $\{H \leq G \mid N \subseteq H\}$ halmazt. Mivel $\phi(\psi(H')) = f(f^{-1}(H')) = H'$, vagyis $\phi \circ \psi = \mathbf{1}_{\mathcal{S}(G')}$ és $\psi(\phi(H)) = f^{-1}(f(H)) = NH = H$, vagyis $\psi \circ \phi = \mathbf{1}_{\mathcal{S}}$, következik, hogy $\phi^{-1} = \psi$. ■

3.1.2. Részhalmaz által generált részcsoport

3.1.4. definíció. Legyen $(G, \cdot)$ egy csoport és $X \subseteq G$ egy részhalmaz. Az

$$\langle X \rangle = \bigcap_{H \leq G, X \subseteq H} H$$

részcsoportot az X-által **generált részcsoport**nak nevezzük.

3.1.5. megjegyzés. 1) Az X által generált részcsoportot a következő tulajdonságok jellemzik:

1. $\langle X \rangle$ részcsoportja $(G, \cdot)$-nek.
2. X részhalmaza $\langle X \rangle$-nek.
3. Ha H részcsoportja G-nek úgy, hogy $X \subseteq H$, akkor $\langle X \rangle \subseteq H$.

2) Az X részhalmaz akkor és csak akkor részcsoportja G-nek, ha $\langle X \rangle = X$.
3) Minden $X \subseteq G$ részhalmaz esetén $\langle \langle X \rangle \rangle = \langle X \rangle$.
4) $\langle \emptyset \rangle = \{e\}$.

3.1.6. tétel (Generált részcsoport jellemzése). *Ha* $(G, \cdot)$ *egy csoport és* $X \subseteq G$*, akkor*

$$\langle X \rangle = \{x_1 \dots x_n \mid n \in \mathbb{N},\ x_i \in X \cup X^{-1},\ 1 \leq i \leq n\}.$$

Additív jelölés esetén: *ha* $(G, +)$ *csoport és* $X \subseteq G$*, akkor*

$$\langle X \rangle = \{x_1 + \dots + x_n \mid n \in \mathbb{N},\ x_i \in X \cup (-X),\ i = 1, \dots, n\}$$

(ahol $X^{-1} := \{x^{-1} \mid x \in X\}$ és $-X := \{-x \mid x \in X\}$).

Bizonyítás. Jelöljük A-val az $\{x_1 \dots x_n \mid n \in \mathbb{N},\ x_i \in X \cup X^{-1},\ 1 \leq i \leq n\}$ halmazt, és igazoljuk, hogy $\langle X \rangle = A$.

Ha $n = 0$, akkor értelmezés szerint $x_1 \dots x_n = e$, tehát $A \neq \emptyset$, mert $e \in A$. Legyen $g, h \in A$, $g = x_1 \dots x_n$ és $h = y_1 \dots y_n$ úgy, hogy $x_i, y_i \in X \cup X^{-1}$; ekkor $gh^{-1} = x_1 \dots x_n y_n^{-1} \dots y_1^{-1} \in A$.

Ha $x \in X$, akkor világos, hogy $x = x_1 \in A$.

Ha $H \leq G$ úgy, hogy $X \subseteq H$, akkor $X^{-1} \subseteq H$. Minden $x_1, \dots, x_n \in X \cup X^{-1} \subseteq H$ esetén, mivel $H \leq G$-nek következik, hogy $x_1 \dots x_n \in H$, vagyis $A \subseteq H$. ■

3.1.7. következmény. *Ha* $f : G \longrightarrow G'$ *egy morfizmus és* $X \subseteq G$*, akkor*

$$f(\langle X \rangle) = \langle f(X) \rangle.$$

Bizonyítás. Tudjuk, hogy $X \subseteq \langle X \rangle$, tehát $f(X) \subseteq f(\langle X \rangle)$. Mivel $\langle X \rangle \leq (G, \cdot)$ és f morfizmus következik, hogy $f(\langle X \rangle) \leq G'$, tehát $\langle f(X) \rangle \subseteq f(\langle X \rangle)$.

Fordítva, legyen $g \in \langle X \rangle$ és igazoljuk, hogy $f(g) \in \langle f(X) \rangle$. Mivel $g \in \langle X \rangle$, létezik $x_1, \dots, x_n \in X \cup X^{-1}$ úgy, hogy $g = x_1 \dots x_n$; mivel f morfizmus, $f(g) = f(x_1) \dots f(x_n)$, és $f(x_i) \in f(X)$ vagy $f(x_i) \in f(X^{-1}) = f^{-1}(X)$, tehát $f(g) \in \langle f(X) \rangle$. ■

3.1.3. Ciklikus részcsoport

3.1.8. definíció. 1) Ha az X halmaz egyetlen elemből áll, éspedig $X = \{x\}$, akkor $\langle X \rangle = \langle x \rangle$ és $\langle x \rangle$-et az x-által generált **ciklikus részcsoport**nak nevezzük.

2) A G csoportot **ciklikus csoport**nak nevezzük, ha létezik $x \in G$ úgy, hogy $\langle x \rangle = G$.

3.1.9. megjegyzés. A 3.1.6. tételből következik, hogy az x-által generált ciklikus részcsoport elemei az x hatványai:

$$\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$$

Additív jelölés esetén: ha $(G, +)$ csoport és $x \in G$, akkor $\langle x \rangle = \{kx \mid k \in \mathbb{Z}\}$.

3.1.10. tétel (Ciklikus csoport részcsoportjai és homomorf képei). *Legyen* $G = \langle x \rangle$ *egy ciklikus csoport.*

1) *Ha* H *részcsoportja* G*-nek, akkor* H *ciklikus részcsoport.*
2) *Ha* $f : G \longrightarrow G'$ *morfizmus, akkor* $f(G)$ *ciklikus csoport.*

Bizonyítás. 1) Ha $H = \{e\}$, akkor $H = \langle e \rangle$ ciklikus.

Feltételezzük, hogy $H \neq \{e\}$; következik, hogy létezik $k \in \mathbb{Z}$ úgy, hogy $x^k \neq e$. Mivel $x^k \in H$ és H csoport, ezért $x^{-k} \in H$, tehát létezik $k \in \mathbb{N}^*$ úgy, hogy $x^k \neq e$ és $x^k \in H$. Legyen

$$n = \min\{k \in \mathbb{N}^* \mid x^k \in H, x^k \neq e\}, \quad y = x^n,$$

és igazoljuk, hogy $\langle y \rangle = H$.

Mivel $y \in H$, következik, hogy $y^k \in H$ minden $k \in \mathbb{Z}$ esetén, vagyis $\langle y \rangle \subseteq H$.

Fordítva, legyen $h = x^k \in H$, ahol $k \in \mathbb{Z}$, és alkalmazzuk a maradékos osztás tételét k-ra: létezik $q, r \in \mathbb{Z}$ úgy, hogy $k = nq + r$ és $0 \leq r < n$. Ekkor

$$h = x^k = x^{nq+r} = (x^n)^q x^r,$$

tehát $x^r = (x^n)^{-q} h \in H$, ezért $x^r = e$ (ellenkező esetben ellentmondás az n minimalitásával); következik, hogy $h = x^k = (x^n)^q = y^q \in \langle y \rangle$.

2) Mivel $G = \langle x \rangle$ ciklikus és f morfizmus, következik, hogy $f(G) = f(\langle x \rangle) = \langle f(x) \rangle$, vagyis $f(G)$ is ciklikus. ■

3.1.11. példa. 1) **(A** $(\mathbb{Z}, +)$ **csoport részcsoportjai)** Vegyük észre, hogy

$$\mathbb{Z} = \langle 1 \rangle = \{k1 \mid k \in \mathbb{Z}\} = \langle -1 \rangle$$

ciklikus csoport. Ha H egy rszcsoportja $\mathbb{Z}$-nek, akkor H is ciklikus, tehát létezik $n \in \mathbb{N}$ úgy, hogy $H = \langle n \rangle = \langle -n \rangle = \{nk \mid k \in \mathbb{Z}\} = n\mathbb{Z}$; következik, hogy

$$\mathcal{S}(\mathbb{Z}, +) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}.$$

Az $\mathcal{S}(\mathbb{Z}, +)$ hálóban érvényesek a következő tulajdonságok:

a) Minden $m, n \in \mathbb{N}$ esetén $n\mathbb{Z} \subseteq m\mathbb{Z} \Longleftrightarrow m|n$.

b) $\inf_{\mathcal{S}(\mathbb{Z})}\{m\mathbb{Z}, n\mathbb{Z}\} = m\mathbb{Z} \cap n\mathbb{Z} = [m, n]\mathbb{Z}$.

c) $\sup_{\mathcal{S}(\mathbb{Z})}\{m\mathbb{Z}, n\mathbb{Z}\} = \langle m\mathbb{Z} \cup n\mathbb{Z} \rangle = (m, n)\mathbb{Z}$.

a) Feltételezzük, hogy $n\mathbb{Z} \subseteq m\mathbb{Z}$. Ekkor $n = n \cdot 1 \in m\mathbb{Z}$, tehát $n = mk$, ahol $k \in \mathbb{Z}$-beli elem; következik, hogy $m|n$-et.

Fordítva, ha $m|n$, akkor létezik $k \in \mathbb{Z}$ úgy, hogy $n = mk$, vagyis $n \in m\mathbb{Z}$; mivel $m\mathbb{Z}$ részcsoport, következik, hogy $n\mathbb{Z} = \langle n \rangle \subseteq m\mathbb{Z}$.

b) Felírható, hogy:

$$m\mathbb{Z} \cap n\mathbb{Z} = \{a \in \mathbb{Z} \mid m|a,\ n|a\} = \{a \in \mathbb{Z} \mid [m, n]|a\} = [m, n]\mathbb{Z}.$$

c) Először igazoljuk, hogy $\langle m\mathbb{Z} \cup n\mathbb{Z} \rangle = m\mathbb{Z} + n\mathbb{Z}$, ahol $m\mathbb{Z} + n\mathbb{Z} = \{mk + nl \mid k, l \in \mathbb{Z}\}$.

Igazolni kell, hogy $m\mathbb{Z} + n\mathbb{Z}$ részcsoportja $(\mathbb{Z}, +)$-nak, $m\mathbb{Z}, n\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$ és ha H részcsoportja $(\mathbb{Z}, +)$-nak úgy, hogy $m\mathbb{Z}, n\mathbb{Z} \subseteq H$, akkor $m\mathbb{Z} + n\mathbb{Z} \subseteq H$.

Mivel $m\mathbb{Z} + n\mathbb{Z} \neq \emptyset$ és minden $x, y \in m\mathbb{Z} + n\mathbb{Z}$ esetén $x - y \in m\mathbb{Z} + n\mathbb{Z}$ (ugyanis ha $x = mp_1 + nq_1, y = mp_2 + nq_2$, akkor $x - y = (mp_1 + nq_1) - (mp_2 + nq_2) = m(p_1 - p_2) + n(q_1 - q_2) \in m\mathbb{Z} + n\mathbb{Z}$), következik, hogy $m\mathbb{Z} + n\mathbb{Z} \leq (\mathbb{Z}, +)$.

Evidens az, hogy $m\mathbb{Z}, n\mathbb{Z} \subseteq m\mathbb{Z} + n\mathbb{Z}$.

Minden $x \in m\mathbb{Z} \subseteq H$, $y \in n\mathbb{Z} \subseteq H$ esetén, mivel H részcsoport, következik, hogy $x + y \in H$, vagyis $m\mathbb{Z} + n\mathbb{Z} \subseteq H$.

A továbbiakban bebizonyítjuk, hogy $m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z}$, ahol $d = (m, n)$ az m, n legnagyobb közös osztója. Valóban, legyen $m = m'd$ és $n = n'd$, tehát $(m', n') = 1$.

Ha $x \in m\mathbb{Z} + n\mathbb{Z}$, akkor $x = mk + nl$ (ahol $k, l \in \mathbb{Z}$), vagyis $x = d(m'k + n'l) \in d\mathbb{Z}$.

Fordítva, mivel $m\mathbb{Z}+n\mathbb{Z}$ részcsoportja a $(\mathbb{Z}, +)$ csoportnak, létezik olyan $d' \in \mathbb{N}$ amelyre $m\mathbb{Z}+n\mathbb{Z} = d'\mathbb{Z} \supseteq d\mathbb{Z}$ (azaz $d|d'$). Igazolnunk kell, hogy $d' = d$. Valóban, $m = m1 + n0 \in d'\mathbb{Z}$ és $n = m0 + n1 \in d'\mathbb{Z}$, tehát $d'|m$-et és $d'|n$-et, de $(m, n) = d$, ezért $d'|d$, tehát $d\mathbb{Z} \subseteq d'\mathbb{Z}$.

2) **(A** $(\mathbb{Z}_n, +)$ **csoport részcsoportjai)** Legyen $p_n : \mathbb{Z} \longrightarrow \mathbb{Z}_n$, $\ p_n(x) = \hat{x}$ a *kanonikus projekció.* Tudjuk, hogy p_n szürjektív morfizmus és $\operatorname{Ker} f = n\mathbb{Z}$, tehát

$$\begin{aligned}\mathcal{S}(\mathbb{Z}_n) &= \{p_n(H) \mid H \leq \mathbb{Z},\ n\mathbb{Z} \subseteq H\} = \\ &= \{p_n(m\mathbb{Z}) \mid m \in \mathbb{N},\ m|n\} = \\ &= \{\hat{m}\mathbb{Z}_n \mid m \in \mathbb{N}, m|n\} = \\ &= \{\langle \hat{m} \rangle \mid m \in \mathbb{N},\ m|n\}.\end{aligned}$$

3.1. feladat. Határozzuk meg az $\langle A \rangle$ részcsoportot, ha $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in GL_2(\mathbb{Q})$.

3.2. feladat. Bizonyítsuk be, hogy:
a) $(\mathcal{S}(\mathbb{Z}), \subseteq)$ és $(\mathbb{N}, |)$ antiizomorf hálók.
b) Határozzuk meg a $\mathbb{Z}_n$ részcsoportjait és adjuk meg az $\mathcal{S}(\mathbb{Z}_n)$ háló Hasse-diagramját, ha $n = 9, 10, 12$.
c) $(\mathcal{S}(\mathbb{Z}_n), \subseteq)$ és $(\{m \in \mathbb{N} \mid m|n\}, |)$ antiizomorf hálók.

3.3. feladat. Legyen $(G, \cdot)$ egy csoport és $H, K \leq G$.
a) $HK \leq G$ akkor és csak akkor, ha $HK = KH$.
b) Ebben az esetben $\sup\{H, K\} = HK$.

3.4. feladat. Igazoljuk, hogy $(\mathbb{Q}, +)$ nem végesen generált csoport (tehát nem ciklikus).

3.1.4. Ciklikus permutációk

A következőkben az S_n csoport néhány generátorrendszerét vizsgáljuk.

3.1.12. definíció. Legyen $l \in \mathbb{N}^*$, $i_1, \ldots, i_l \in \{1, \ldots, n\}$ különböző számok, és tekintsük a következő $\gamma \in S_n$ permutációt:

$$\gamma(i) = \begin{cases} i_{k+1}, & \text{ha } i = i_k, 1 \leq k < l \\ i_1, & \text{ha } i = i_l \\ i, & \text{ha } i \neq \{i_1, \ldots, i_l\} \end{cases}$$

Azt mondjuk, hogy γ **l-hosszúságú ciklus**, és a $\gamma = (i_1 i_2 \ldots i_l)$ jelölést használjuk.
Az $\mathcal{O}_\gamma = \{i_1, \ldots, i_l\}$ halmazt a γ **pályá**jának (**orbit**jának) nevezzük.

Például, $\gamma = (145) = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 2 & 3 & 5 & 1 & 6 \end{pmatrix} \in S_6$, és $2, 3, 6$ fixpontjai γ-nak.

3.1.13. megjegyzés. 1) Minden 1-hosszúságú (i) ciklus egyenlő az e identikus permutációval.
2) A 2-hosszúságú $(ij) = \tau_{ij}$ ciklusokat transzpozícióknak nevezzük.
3) $\gamma = (i_1 i_2 i_3 \ldots i_l) = (i_l i_1 i_2 \ldots i_{l-1}) = (i_{l-1} i_l i_1 \ldots i_{l-2}) = \ldots$
4) Ha $\gamma = (i_1 i_2 i_3 \ldots i_l)$ egy l-hosszuságú ciklus, akkor $\gamma = (i\gamma(i)\gamma^2(i) \ldots \gamma^{l-1}(i))$. Továbbá, vegyük észre, hogy

$$\gamma^2 = (i\gamma^2(i)\gamma^4(i)\ldots), \quad \gamma^3 = (i\gamma^3(i)\gamma^6(i)\ldots), \quad \ldots, \quad \gamma^{l-1} = (i\gamma^{l-1}(i)\ldots),$$

és végül, $\gamma^l = e$.

3.1.14. definíció. Legyenek $\sigma, \tau \in S_n$. A σ és τ-t *diszjunkt permutációknak* nevezzük, ha minden $i \in \{1, \ldots, n\}$ esetén, $\sigma(i) \neq i$-ből következik, hogy $\tau(i) = i$.

3.1.15. lemma. *Ha $\sigma, \tau \in S_n$ diszjunkt permutációk, akkor $\tau \circ \sigma = \sigma \circ \tau$.*

Bizonyítás. Legyen $i \in \{1, 2, \ldots, n\}$. Ha $\sigma(i) = \tau(i) = i$, akkor

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = i = (\tau \circ \sigma)(i).$$

Ha $\sigma(i) = j \neq i$, akkor $\tau(i) = i$ és $\tau(j) = j$, mert $\sigma(j) \neq j$. Így

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(i) = j,$$

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(j) = j,$$

tehát $\sigma \circ \tau = \tau \circ \sigma$.
Ha $\tau(i) = j \neq i$, akkor $\sigma(i) = i$ és $\sigma(j) = j$, mert $\tau(j) \neq j$. Így

$$(\sigma \circ \tau)(i) = \sigma(\tau(i)) = \sigma(j) = j,$$

$$(\tau \circ \sigma)(i) = \tau(\sigma(i)) = \tau(i) = j,$$

tehát $\sigma \circ \tau = \tau \circ \sigma$. ■

3.1.16. tétel. *Minden $\sigma \in S_n$ felbontható diszjunkt ciklusok szorzatára. A felbontás egyértelmű eltekintve a ciklusok sorrendjétől.*

Tekintsünk először egy példát: ha

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 4 & 5 & 12 & 9 & 3 & 10 & 8 & 7 & 1 & 6 & 11 & 2 \end{pmatrix},$$

akkor $\sigma = \gamma_1\gamma_2\gamma_3\gamma_4\gamma_5$, ahol $\gamma_1 = (1\ 4\ 9), \gamma_2 = (2\ 5\ 3\ 12), \gamma_3 = (6\ 10), \gamma_4 = (7\ 8), \gamma_5 = (11)$.

A tétel bizonyítása. Ha $\sigma = e$, akkor $\sigma = (1) \circ (2) \circ \cdots \circ (n)$, tehát feltételezhetjük, hogy $\sigma \neq e$. Legyen $f_\sigma \in \{0, \dots, n\}$ a σ fix-pontjainak száma, és legyen $i \in \{1, \dots, n\}$ úgy, hogy $\sigma(i) \neq i$. Tekintsük a $\gamma_1 = (i\ \sigma(i)\ \sigma^2(i)\ \dots\ \sigma^{l-1}(i))$ l-hosszúságú ciklikus permutációt, ahol $l = \min\{k > 1 \mid \sigma^k(i) = i\}$. (Vegyük észre, hogy l létezik, mert ha $k < m$ és $\sigma^k(i) = \sigma^m(i)$, akkor $\sigma^{m-k}(i) = (i)$.) Következik, hogy ha $j \in \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{l-1}(i)\}$ akkor $\gamma_1(j) = \sigma(j)$, és ha $j \notin \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{l-1}(i)\}$, akkor $\gamma_1(j) = j$. Legyen $\sigma_1 = \sigma \circ \gamma_1^{-1}$; következik, hogy ha $j \in \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{l-1}(i)\}$ akkor $\sigma_1(j) = j$, és ha $j \notin \{i, \sigma(i), \sigma^2(i), \dots, \sigma^{l-1}(i)\}$, akkor $\sigma_1(j) = \sigma(j)$. Ezért $f_{\sigma_1} > f_\sigma$, és folytatva az eljárást, következik, hogy létezik $m \in \mathbb{N}$ és léteznek a $\gamma_1, \dots, \gamma_m$ diszjunkt ciklusok úgy, hogy $\sigma \circ \gamma_1^{-1} \circ \cdots \circ \gamma_m^{-1} = e$, tehát $\sigma = \gamma_1 \circ \cdots \circ \gamma_m$ (mert a fenti lemma szerint, a diszjunkt permutációk felcserélhetők).

Igazoljuk most indukcióval az egyértelműséget. Feltételezzük, hogy $\sigma = \gamma_1 \circ \cdots \circ \gamma_m = \delta_1 \circ \cdots \circ \delta_r$, ahol $\gamma_1, \dots, \gamma_m$ és $\delta_1, \dots, \delta_r$ diszjunkt ciklusok. Ha $i \in \{1, \dots, n\}$ úgy, hogy $\sigma(i) \neq i$, akkor létezik egyetlen $j \in \{1, \dots, m\}$ és egyetlen $k \in \{1, \dots, r\}$ úgy, hogy $\gamma_k(i) \neq i$ és $\delta_k(i) \neq i$. Mivel diszjunkt permutációk felcserélhetők, feltételezhetjük, hogy $j = m$ és $k = r$. A fentiekből következik, hogy $\gamma_m = \delta_r = (i\ \sigma(i)\ \sigma^2(i)\ \dots\ \sigma^{l-1}(i))$, ahol $l = \min\{k > 1 \mid \sigma^k(i) = i\}$. Legyen $\sigma_1 = \sigma \circ \gamma_m^{-1} = \sigma \circ \delta_r^{-1}$. Az indukció hipotézise alapján következik, hogy $m - 1 = r - 1$ és $\gamma_k = \delta_k$, $k = \{1, \dots, m-1\}$, tehát $m = r$ és $\gamma_k = \delta_k$, $k = \{1, \dots, m\}$. ■

3.1.17. definíció. Legyenek $k_1, \dots, k_n \in \{0, \dots, n\}$. Azt mondjuk, hogy $\sigma \in S_n$ *típusa* a $(k_1, \dots, k_n)$ rendszer (ahol $k_1 + 2k_2 + \cdots + nk_n = n$), ha a σ diszjunkt ciklusokra való felbontásában szerepel k_1 1-hosszúságú ciklus, k_2 2-hosszúságú ciklus, ..., k_n n-hosszúságú ciklus.

Például, a

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 1 & 5 & 6 & 4 & 8 & 7 \end{pmatrix} = (2)(1\ 3)(7\ 8)(4\ 5\ 6) = (1\ 3)(7\ 8)(4\ 5\ 6) \in S_8$$

permutáció típusa: $(1, 2, 1, 0, 0, 0, 0, 0)$.

3.1.18. következmény. *A transzpozíciók halmaza generálja az S_n-et.*

Bizonyítás. Elég igazolni, hogy minden ciklikus permutáció felbontható transzpozíciók szorzatára. Valóban, legyen $\gamma = (i_1 i_2 \dots i_l)$ és $\rho = (i_1 i_l)(i_1 i_{l-1}) \dots (i_1 i_3)(i_1 i_2)$; mivel $\rho(i_1) = i_2, \rho(i_2) = i_3, \rho(i_3) = i_4, \dots, \rho(i_{l-1}) = i_l, \rho(i_l) = i_1$ következik, hogy $\rho = \gamma$. ■

3.1.19. megjegyzés. 1) A transzpozíciókra való felbontás nem egyértelmű: például vegyük észre, hogy $(123) = (13)(12) = (12)(13)(23)(12)$.

2) Ha $\sigma = \tau_1 \circ \tau_2 \circ \dots \circ \tau_m$ transzpozíciókra való felbontás akkor $\epsilon(\sigma) = \epsilon(\tau_1)\epsilon(\tau_2) \dots \epsilon(\tau_m)$; következik, hogy ha σ páros, akkor a tényezők száma is páros, és ha σ páratlan, akkor a tényezők száma is páratlan.

Például: $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 3 & 2 & 6 & 5 & 7 & 1 & 4 & 8 \end{pmatrix} = (136)(457) = (16)(13)(47)(45)$, tehát $\epsilon(\sigma) = 1$.

3) Ha γ l-hosszúságú ciklus, akkor $\mathrm{sgn}(\gamma) = (-1)^{l-1}$. Ha $\sigma \in S_n$ permutáció felbontási típusa $(k_1, k_2, ..., k_n)$, akkor

$$\mathrm{sgn}(\sigma) = (-1)^{\sum_{i=1}^{n}(i-1)k_i} = (-1)^{k_2 + 2k_3 + \dots + (n-1)k_n}.$$

3.5. feladat. Bontsuk fel diszjunkt ciklusok szorzatára az S_n elemeit, $n = 1, 2, 3, 4$.

3.6. feladat. Hány l-hosszúságú ciklus van S_n-ben?

3.7. feladat. a) Ha $1 < k < l$ és $\gamma = (i_1 \dots i_{k-1}\ i_k\ i_{k+1} \dots i_l)$ egy l-hosszúságú ciklus, akkor

$$\gamma = (i_1 \dots i_k)(i_k\ i_{k+1} \dots i_l) = (i_1\ i_l) \cdots (i_1\ i_2) = (i_{l-1}\ i_l) \cdots (i_2\ i_l)(i_1\ i_l).$$

b) Igazoljuk, hogy $\epsilon(\gamma) = (-1)^{l-1}$.

3.8. feladat. Igazoljuk, hogy a következő halmazok generálják S_n-et:
a) $\{(1\ 2), (1\ 3), \dots, (1\ n)\}$;
b) $\{(1\ 2), (2\ 3), \dots, (n-1\ n)\}$;
c) $\{(1\ 2), (1\ 2\ \dots\ n)\}$;
d) $\{(1\ 2\ \dots\ n-1), (n-1\ n)\}$.

3.9. feladat. Igazoljuk, hogy a következő halmazok generálják A_n-et:
a) 3-hosszúságú ciklusok;
b) $\{(1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n)\}$;
c) $\{(i\ j)(k\ l) \mid i, j, k, l$ különböző számok$\}$, ha $n \geq 5$.

3.1.5. A diédercsoport

Tekintsük az $E^2 = (\mathbb{R}^2, d)$ euklideszi síkot, és legyen

$$\mathrm{Izom}(E^2) = \{\sigma : R^2 \to \mathbb{R}^2 \mid d(\sigma(P), \sigma(Q)) = d(P, Q)\ \forall P, Q \in R^2\}$$

az E^2 izometriáinak halmaza. Mivel minden izometria bijektív függvény, és izometriák szorzata és inverze is izometria, következik, hogy $(\mathrm{Izom}(E^2), \circ)$ csoport. Továbbá, három nemkollineáris pont képe meghatároz egy izometriát; pontosabban, ha σ, τ izometriák, $Q_1, Q_2, Q_3 \in R^2$ nemkollineáris pontok és $\sigma(Q_i) = \tau(Q_i)$, $i = 1, 2, 3$, akkor $\sigma = \tau$.

Legyen $P_n \subset E^2$ a szabályos n-szög, $n \geq 3$. Értelmezés szerint, az n-ed fokú D_n **diédercsoport** a P_n halmaz **szimmetria csoportja**, azaz

$$D_n = \{\sigma \in \mathrm{Izom}(E^2) \mid \sigma(P_n) = P_n\}.$$

(Igazolható, hogy D_n részcsoportja az $(\mathrm{Izom}(E^2), \circ)$ csoportnak, tehát $(D_n, \circ)$ valóban csoport.)

Jelöljuk 0-val a P_n középpontjat, és $1, \ldots, n$-nel a P_n csúcsait. Ha $\sigma \in D_n$, akkor $\sigma(0) = 0$ és $\sigma(k) \in \{1, \ldots, n\}$, tehát D_n azonosítható egy permutációcsoporttal, így $D_n \leq (S_n, \circ)$. Mivel $\sigma(0) = 0$, következik, hogy $\sigma(1)$ és $\sigma(n)$ meghatározzák σ-t; ha $\sigma(1) = k \in \{1, \ldots, n\}$, akkor $\sigma(n) \in \{k+1, k-1\}$ (ahol $n+1 = 1$ és $1-1 = n$), ezért $|D_n| \leq 2n$.

A továbbiakban igazoljuk, hogy $|D_n| = 2n$. Elég belátni, hogy D_n-ben létezik $2n$ különböző elem. Legyen $\rho = \rho_{2\pi/n}$ a $2\pi/n$-szöggel való elforgatás, tehát

$$\rho(1) = 2,\ \rho(n) = 1,\quad \rho = \begin{pmatrix} 1 & 2 & \ldots & n-1 & n \\ 2 & 3 & \ldots & n & 1 \end{pmatrix},$$

és $\sigma = \sigma_{01}$ a 01-szimmetriatengelyre való tükrözés, tehát

$$\sigma(1) = 1,\ \sigma(n) = 2,\quad \sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n-1 & n \\ 1 & n & n-1 & \ldots & 3 & 2 \end{pmatrix}.$$

Vegyük észre, hogy minden $1 \leq k < n$ esetén $\rho^k = \rho_{2k\pi/n}$ a $2k\pi/n$-szöggel való elforgatás ($\rho^k(1) = k+1$, $\rho^k(n) = k$) és $\rho^n = e$, az identikus transzformáció. Továbbá, $\sigma^2 = e$, és $e, \rho, \ldots, \rho^{n-1}, \sigma, \rho \circ \sigma, \ldots, \rho^{n-1} \circ \sigma$ különböző transzformációk; valóban, ha $0 \leq k < n$, akkor $(\rho^k \circ \sigma)(1) = \rho^k(\sigma(1)) = \rho^k(1) = k+1$ és $(\rho^k \circ \sigma)(n) = \rho^k(\sigma(n)) = \rho^k(2) = k+2$. Következik, hogy

$$D_n = \{e, \rho, \ldots, \rho^{n-1}, \sigma, \rho \circ \sigma, \ldots, \rho^{n-1} \circ \sigma\}.$$

(Könnyen belátható, hogy $\rho^k \circ \sigma$ a d_k egyenesre való tükrözés, ahol d_k az $[1, k+1]$ szakasz felezőmerőlegese; ha $k = 2m$ páros, akkor d_k a 0 $(m+1)$ egyenes; ha $k = 2m+1$ páratlan, akkor d_k az $[m, m+1]$ oldal felezőmerőlegese.)

Végül, vegyük észre, hogy $\sigma \circ \rho = \rho^{n-1} \circ \sigma$; valóban,

$$(\sigma \circ \rho)(1) = \sigma(\rho(1)) = \sigma(2) = n = (\rho^{n-1} \circ \sigma)(1)$$

és

$$(\sigma \circ \rho)(n) = \sigma(\rho(n)) = \sigma(1) = n = (\rho^{n-1} \circ \sigma)(n).$$

3.1.20. megjegyzés. 1) A $\rho^n = 1$, $\sigma^2 = e$ és $\sigma \circ \rho = \rho^{n-1} \circ \sigma$ relációk meghatározzák a D_n művelettábláját. Ezért, a diédercsoport absztrakt definíciója a következő:

$$D_n = \langle x, y \mid x^n = y^2 = e,\ yx = x^{n-1}y \rangle;$$

az x, y elemeket **generátorok**nak nevezzük; $x^n = y^2 = e$, $yx = x^{n-1}y$ a D_n **definiáló relációi**.

2) Mivel $D_3 \leq S_3$ és $|D_3| = 6$, következik, hogy $D_3 = S_3$.

3) Hasonló módon értelmezhetjük a D_1 és D_2 csoportokat: D_1 az egyenlőszárú háromszög szimmetria csoportja, és D_2 a téglalap szimmetria csoportja. Így

$$D_1 = \left\{e, \begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}\right\} = \langle x \mid x^2 = e \rangle \simeq (\mathbb{Z}_2, +),$$

$$D_2 = \left\{e, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}\right\}$$
$$= \langle x, y \mid x^2 = y^2 = e,\ yx = xy \rangle.$$

3.10. feladat. Készítsük el a D_n művelettábláját, ahol $n = 1, 2, 3, 4, 5, 6$.

3.11. feladat. A D_n csoportban, ha $0 \le i, k < n$, $0 \le l, j \le 2$, akkor
a) $(x^k y)^2 = e$.
b) $x^k y^l x^i y^j (x^k y^l)^{-1} = \begin{cases} x^i, & \text{ha } l = j = 0 \\ x^{-i}, & \text{ha } l = 1,\ j = 0 \\ x^{2k+i}y, & \text{ha } l = 0,\ j = 1 \\ x^{2k-i}y, & \text{ha } l = j = 1 \end{cases}$

3.2. Kongruenciarelációk és normális részcsoportok

3.2.1. Részcsoport szerinti mellékosztályok

3.2.1. definíció. Legyen $(G, \cdot)$ egy csoport és H részcsoportja G-nek. Értelmezzünk G-n két relációt:
$x\rho_H y \iff x^{-1}y \in H$ a H szerinti **bal oldali kongruencia**, és
$x\rho'_H y \iff xy^{-1} \in H$ a H szerinti **jobb oldali kongruencia** reláció.

3.2.2. lemma. 1) ρ_H *és* ρ'_H *ekvivalenciarelációk* G*-n.*
2) *Ha* $G/\rho_H = \{\rho_H\langle x\rangle \mid x \in G\}$ *és* $G/\rho'_H = \{\rho'_H\langle x\rangle \mid x \in G\}$*, akkor*

$$\rho_H\langle x\rangle = xH = \{xh \mid h \in H\}$$

x-nek H szerinti bal oldali mellékosztálya *és*

$$\rho'_H\langle x\rangle = Hx = \{hx \mid h \in H\}$$

x-nek H szerinti jobb oldali mellékosztálya.

Bizonyítás. 1) Igazoljuk, hogy ρ_H reflexív, tranzitív és szimmetrikus.
Reflexivitás: $x\rho_H x$ minden $x \in G$ esetén, mert $x^{-1}x = e \in H$.
Tranzitivitás: ha $x\rho_H y$ és $y\rho_H z$, akkor értelmezés szerint $x^{-1}y \in H$ és $y^{-1}z \in H$, tehát $(x^{-1}y)(y^{-1}z) \in H$, vagyis $x^{-1}z \in H$ és $x\rho_H z$.
Szimmetria: ha $x\rho_H y$, akkor $x^{-1}y \in H$, tehát $(x^{-1}y)^{-1} = y^{-1}x \in H$, azaz $y\rho_H x$.
Azt, hogy ρ'_H ekvivalencia reláció hasonlóan igazoljuk.
2) Igazoljuk, hogy $\rho_H\langle x\rangle = xH$. Értelmezés szerint

$$\rho_H\langle x\rangle = \{y \in G \mid x\rho_H y\} = \{y \in G \mid x^{-1}y \in H\}.$$

Legyen $y \in \rho_H\langle x\rangle$; ekkor $h = x^{-1}y \in H$, tehát $y = xh \in xH$.
Fordítva, ha $y = xh \in xH$, akkor $x^{-1}y = h \in H$; következik, hogy $x\rho_H y$, azaz $y \in \rho_H\langle x\rangle$.
Az $\rho'_H\langle x\rangle = Hx$ egyenlőség igazolása hasonló módon történik. ■

3.2.3. tétel (Lagrange-tétel). *Legyen* G *egy csoport és* $H \le G$ *egy részcsoport.*
1) *Fennáll, hogy* $|xH| = |Hx| = |H|$ *minden* $x \in G$ *esetén, vagyis minden osztályban ugyanannyi elem van.*
2) *Ha* $G/H = \{xH \mid x \in G\}$ *és* $H\backslash G = \{Hx \mid x \in G\}$*, akkor* $|G/H| = |H\backslash G|$.
(Jelölés: $[G : H] = |G/H| = |H\backslash G|$; ezt a kardinális számot a H részcsoport G-beli **index**ének nevezzük.)
3) $|G| = |H| \cdot [G : H]$. *Partikulárisan, ha* G *véges, akkor minden részcsoport rendje osztja a csoport rendjét.*
4) *Ha* H, K *részcsoportjai* G*-nek és* $K \subseteq H$*, akkor*

$$[G : K] = [G : H] \cdot [H : K].$$

Bizonyítás. 1) Legyen $f : H \to xH$, $f(h) = xh$. Értelmezés szerint f szürjektív függvény, de injektív is (mert csoportban lehet egyszerűsíteni), tehát f bijektív függvény, ezért $|H| = |xH|$.
Hasonlóan $f' : H \longrightarrow Hx$, $f'(h) = hx$ bijektív függvény, tehát $|H| = |Hx|$.
2) Legyen $\varphi : G/H \longrightarrow H\backslash G$, $\varphi(xH) = Hx^{-1}$. Igazoljuk, hogy φ jól értelmezett: legyen $x' \in xH$, vagyis $x' = xh$ (ez azt is jelenti, hogy $xH = x'H$). Akkor

$$\varphi(x'H) = H(x')^{-1} = H(xh)^{-1} = H(h^{-1}x^{-1}) = Hx^{-1}.$$

Legyen $\psi : H\backslash G \longrightarrow G/H$, $\psi(Hx) = x^{-1}H$. Az előbbihez hasonlóan igazoljuk, hogy ψ jól értelmezett függvény. Mivel

$$(\psi \circ \varphi)(xH) = \psi(\varphi(xH)) = \psi(Hx^{-1}) = (x^{-1})^{-1}H = xH$$

és

$$(\varphi \circ \psi)(Hx) = \varphi(\psi(Hx)) = \varphi(x^{-1}H) = H(x^{-1})^{-1} = Hx$$

következik, hogy $\psi = \varphi^{-1}$ és φ bijektív függvény, tehát $|G/H| = |H/G|$.

3) Létezik egy I halmaz és léteznek az $x_i \in G$ elemek, $i \in I$, úgy, hogy $G/H = \{x_iH \mid i \in I\}$ és $|I| = [G : H] = |G/H|$. Azt mondjuk, hogy $\{x_i \mid i \in I\} \subseteq G$ a G/H faktorhalmaznak egy *teljes reprezentáns rendszere* (vagyis $G = \bigcup_{i\in I} x_iH$ és, ha $i \neq j$, akkor $x_iH \cap x_jH = \emptyset$).

A fentiek alapján $|G| = \sum_{i\in I} |x_iH| = \sum_{i\in I} |H| = |I| \cdot |H| = [G : H] \cdot |H|$.

d) (Ez a pont tulajdonképpen a c)-pont általánositása.) Legyen $\{x_i \mid i \in I\}$ G/H-nak egy teljes reprezentáns rendszere, tehát $|I| = [G : H]$, és legyen $\{y_i \mid j \in J\}$ a H/K-nak egy teljes reprezentáns rendszere, tehát $|J| = [H : K]$.

Elég igazolni, hogy $\{x_iy_j \mid (i, j) \in I \times J\}$ G/K-nak egy teljes reprezentáns rendszere (mert akkor $|G/K| = [G : K] = |I \times J| = |I| \cdot |J| = [G : H][H : K]$).

Ahhoz, hogy $\{x_iy_j \mid (i, j) \in I \times J\}$ G/K-nak egy teljes reprezentáns rendszere legyen, az egyesítésnek fednie kell G-t és két különböző osztálynak diszjunktnak kell lennie. Valóban,

$$\begin{aligned}\bigcup_{(i,j)\in I\times J} x_iy_jK &= \bigcup_{i\in I}\bigcup_{j\in J} x_iy_jK = \bigcup_{i\in I}\bigcup_{j\in J} t_{x_i}(y_jK) = \\ &= \bigcup_{i\in I} t_{x_i}(\bigcup_{j\in J} y_jK) = \\ &= \bigcup_{i\in I} t_{x_i}(H) = \bigcup_{i\in I} x_iH = G;\end{aligned}$$

továbbá, igazoljuk, hogy ha $(i_1, j_1) \neq (i_2, j_2)$, akkor $x_{i_1}y_{j_1}K \cap x_{i_2}y_{j_2}K = \emptyset$. Feltételezzük, hogy $i_1 \neq i_2$, akkor $x_{i_1}y_{j_1}K \cap x_{i_2}y_{j_2}K \subseteq x_{i_1}H \cap x_{i_2}H = \emptyset$. Ha $i_1 = i_2 = i$, akkor $j_1 \neq j_2$, és $x_{i_1}y_{j_1}K \cap x_{i_2}y_{j_2}K = t_{x_i}(y_{j_1}K) \cap t_{x_i}(y_{j_2}K) = t_{x_i}(y_{j_1}K \cap y_{j_2}K) = t_{x_i}(\emptyset) = \emptyset$ (felhasználtuk azt, hogy a t_x transzláció injektív). ■

3.2.2. Normális részcsoport

3.2.4. definíció. Legyen G egy csoport és N G-nek egy részcsoportja. Azt mondjuk, hogy N **normális részcsoport** (jelölés: $N \trianglelefteq G$), ha $xnx^{-1} \in N$ minden $x \in G$ és $n \in N$ esetén.

3.2.5. tétel (Normális részcsoport jellemzése). *Legyen* G *egy csoport és* $N \leq G$*-nek. A következő állítások egyenértékűek:*

1. N *normális részcsoportja* G*-nek.*
2. $\rho_N = \rho'_N$.
3. $xN = Nx$ *minden* $x \in G$ *esetén.*

Bizonyítás. 1) $\Longrightarrow$ 2) Feltételezzük, hogy $N \trianglelefteq G$ és legyen $x, y \in G$. Akkor $x\rho_N y \iff x^{-1}y \in N \iff x(x^{-1}y)x^{-1} \in N \iff yx^{-1} \in N \iff x\rho'_N y$, tehát $\rho_N = \rho'_N$.

2) $\Longrightarrow$ 3) Mivel $\rho'_N = \rho_N$ következik, hogy $\rho'_N\langle x\rangle = \rho_N\langle x\rangle$ minden $x \in G$ esetén, ezért $Nx = xN$ minden $x \in G$ esetén.

3) $\Longrightarrow$ 1) Legyen $x \in G$ és $n \in N$. Akkor $xn \in xN = Nx$, tehát létezik $n' \in N$ úgy, hogy $xn = n'x$, vagyis $xnx^{-1} = n' \in N$. ■

3.2.6. példa. 1) G és $\{e\}$ normális részcsoportjai G-nek, és $\rho_G = G \times G$, $\rho_{\{e\}} = \triangle_G = \{(g, g) \mid g \in G\}$.

2) Ha G kommutatív, akkor minden részcsoportja normális; a fordított állítás nem igaz.

3) Ha $n \in \mathbb{N}$, akkor $n\mathbb{Z} \trianglelefteq \mathbb{Z}$ és $\rho_{nZ} = \equiv \pmod{n}$.

4) Ha G, G' csoportok és $f : G \longrightarrow G'$ morfizmus, akkor $\operatorname{Ker} f \trianglelefteq G$ és $\rho_{\operatorname{Ker} f} = \ker f$.

Valóban, tudjuk, hogy $\operatorname{Ker} f \leq G$. Ha $x \in G$ és $n \in \operatorname{Ker} f$, akkor

$$f(xnx^{-1}) = f(x)f(n)f(x^{-1}) = e',$$

vagyis $xnx^{-1} \in \operatorname{Ker} f$. Legyen $x, y \in G$. Akkor

$$x\rho_{\operatorname{Ker} f}y \Leftrightarrow x^{-1}y \in \operatorname{Ker} f \Leftrightarrow f(x^{-1}y) = e' \Leftrightarrow f(x) = f(y) \Leftrightarrow x \ker f y.$$

3.12. feladat. a) Határozzuk meg a $(Q_8, \cdot)$ nyolcelemű kvaterniócsoport részcsoportjait, a részcsoportok mellékosztályait és normális részcsoportjait. Vegyük észre, hogy $(Q_8, \cdot)$ nem kommutatív, de minden részcsoportja normális.

b) Határozzuk meg az $(S_3, \circ)$ részcsoportjait, a részcsoportok mellékosztályait és normális részcsoportjait.

c) Határozzuk meg az A_4 részcsoportjait és normális részcsoportjait. Vegyük észre, hogy a „$\trianglelefteq$” reláció nem tranzitív.

d) Határozzuk meg a D_n részcsoportjait és normális részcsoportjait, ahol $n = 4, 5, 6$.

3.13. feladat. Ha $(G, \cdot)$ egy csoport, $H \leq G$ és $[G : H] = 2$, akkor $H \trianglelefteq G$.

3.14. feladat. Legyen $(G, \cdot)$ egy csoport és $H, K, L \leq G$. Bizonyítsuk be, hogy:
a) $|H| \cdot |K| = |HK| \cdot |H \cap K|$.
b) Ha $H \leq K$, akkor $[L \cap K : L \cap H] \leq [K : H]$.
c) $[G : H \cap K] \leq [G : H][G : K]$.
d) Ha G véges és $([G : K], [G : H]) = 1$, akkor $[G : K \cap H] = [G : K][G : H]$ és $G = HK$.

3.15. feladat. Ha G egy véges csoport, $H < G$ és $X = G \setminus H$, akkor $\langle X \rangle = G$.

3.16. feladat. Legyen $f : G \to G'$ egy morfizmus, $N \trianglelefteq G$ és $N' \trianglelefteq G'$.
a) Igazoljuk, hogy $f(N) \trianglelefteq f(G)$ és $f^{-1}(N) \trianglelefteq G$.
b) Következtessük hogy, ha f szürjektív, akkor a 3.1.3. tételbeli φ és ψ függvények indukálják az

$$\{N \in \mathcal{S}_n(G) \mid \operatorname{Ker} f \subseteq N\} \simeq \mathcal{S}_n(G')$$

hálóizomorfizmust.

3.2.7. definíció. Legyen $(G, \cdot)$ csoport és $\rho \subseteq G \times G$ egy reláció G-n. ρ-t **kongruenciareláció**nak nevezzük, ha ρ ekvivalenciareláció és kompatibilis a szorzással (azaz, ha $x\rho y$ és $x'\rho y'$, akkor $xx'\rho yy'$ minden $x, y, x', y' \in G$ esetén). Jelölés:

$$\mathcal{C}(G) := \{\rho \subseteq G \times G \mid \rho \text{ kongruenciareláció}\}$$

a kongruenciarelációk halmaza.

3.2.8. megjegyzés. $(\mathcal{C}(G), \subseteq)$ rendezett halmaz, és, ha $\rho_i \in \mathcal{C}(G)$ minden $i \in I$ esetén, akkor $\bigcap_{i \in I} \rho_i \in \mathcal{C}(G)$; következik, hogy $\mathcal{C}(G)$-ben létezik $\inf\{\rho_i \mid i \in I\}$, azaz $\mathcal{C}(G)$ teljes háló.

3.2.9. tétel (A normális részcsoportok és kongruenciák közötti kapcsolat). *Legyen* $(G, \cdot)$ *egy csoport.*

1. *Ha* $N \trianglelefteq G$*, akkor* ρ_N *kongruencia reláció* G*-n.*
2. *Ha* ρ *kongruencia reláció* G*-n, akkor* $\rho\langle e \rangle = \{x \in G \mid r\rho x\} \trianglelefteq G$.
3. *Ha* $\phi : \mathcal{S}_n(G) \longrightarrow \mathcal{C}(G, \cdot)$, $\phi(N) = \rho_N$ *és* $\psi : \mathcal{C}(G, \cdot) \longrightarrow \mathcal{S}_n(G)$, $\psi(\rho) = \rho\langle e \rangle$*, akkor* ϕ, ψ *növekvő, bijektív függvények és* $\psi = \phi^{-1}$*,*

(tehát ϕ *és* ψ *hálóizomorfizmusok.)*

Bizonyítás. 1) Igazolni kell, hogy ρ_N kongruenciareláció G-n. Tudjuk, hogy ρ_N ekvivalenciareláció, ezért elég igazolni, hogy ρ_N kompatibilis a szorzással.

Legyenek $x, y, x', y' \in G$ úgy, hogy $x\rho_N y$ és $x'\rho_N y'$, vagyis $x^{-1}y \in N$ és $x'^{-1}y' \in N$. Mivel $N \trianglelefteq G$ következik, hogy $x'^{-1}(x^{-1}y)x' \in N$ és $x'^{-1}y' \in N$, ezért $x'^{-1}x^{-1}yy' \in N$; következik, hogy $(xx')'^{-1}yy' \in N$, tehát $xx'\rho_N yy'$.

2) Mivel $e\rho e$ következik, hogy $e \in \rho\langle e \rangle$, ezért $\rho\langle e \rangle \neq \emptyset$. Ha $x, y \in \rho\langle e \rangle$, akkor $e\rho x$ és $e\rho y$, és mivel ρ kongruencia reláció, következik, hogy $e\rho xy$, tehát $xy \in \rho\langle e \rangle$. Ha $x \in \rho\langle e \rangle$, akkor $e\rho x$ és $x^{-1}\rho x^{-1}$ tehát $x^{-1}\rho e$. De ρ szimmetrikus, ezért $e\rho x^{-1}$, vagyis $x^{-1} \in \rho\langle e \rangle$. Következik, hogy $\rho\langle e \rangle \leq (G, \cdot)$.

Legyen $x \in G$ és $n \in \rho\langle e \rangle$. Akkor $x\rho x$, $e\rho n$ és $x^{-1}\rho x^{-1}$ tehát $e\rho xnx^{-1}$, vagyis $xnx^{-1} \in \rho\langle e \rangle$ és $\rho\langle e \rangle \trianglelefteq G$.

3) Igazoljuk, hogy ϕ növekvő. Valóban, ha $N_1 \subseteq N_2$ és $x, y \in G$ úgy, hogy $x\rho_{N_1}y$, akkor $x^{-1}y \in N_1$. De $N_1 \subseteq N_2$ ezért $x^{-1}y \in N_2$, vagyis $x\rho_{N_2}y$; következik, hogy $\rho_{N_1} \subseteq \rho_{N_2}$.

Igazoljuk, hogy ψ növekvő. Legyen $\rho_1 \subseteq \rho_2$, ha $x \in \rho_1\langle e \rangle$ következik, hogy $e\rho_1 x$. De $\rho_1 \subseteq \rho_2$, ezért $e\rho_2 x$, vagyis $x \in \rho_2\langle e \rangle$; következik, hogy $\rho_1\langle e \rangle \subseteq \rho_2\langle e \rangle$.

A továbbiakban igazoljuk, hogy $\psi \circ \phi = 1_{\mathcal{S}_n(G)}$ és $\phi \circ \psi = 1_{\mathcal{C}(G)}$.

Ha $N \in \mathcal{S}_n(G)$, akkor $(\psi \circ \phi)(N) = \psi(\phi(N)) = \psi(\rho_N) = \rho_N\langle e \rangle$. De $\rho_N\langle e \rangle = N$, mert $x \in \rho_N\langle e \rangle \iff e\rho_N x \iff e^{-1}x = x \in N$ minden $x \in G$ esetén.

Ha $\rho \in \mathcal{C}(G)$, akkor $(\phi \circ \psi)(\rho) = \rho_{\rho\langle e \rangle}$. De $\rho_{\rho\langle e \rangle} = \rho$, mert

$$x\rho_{\rho\langle e \rangle}y \iff x^{-1}y \in \rho\langle e \rangle \iff e\rho x^{-1}y \iff x\rho y$$

minden $x, y \in G$ esetén. ■

3.17. feladat. Ha $(G, \cdot)$ egy csoport, legyen $(\mathcal{S}_n(G), \subseteq)$ a normális részcsoportok hálója és $(\mathcal{C}(G), \subseteq)$ a kongruenciarelációk hálója. Igazoljuk, hogy:
a) Bármely $N, K \in \mathcal{S}_n(G)$, $N \wedge K = N \cap K$ és $N \vee K = NK = KN$.
b) Ha $N, K, L \in \mathcal{S}_n(G)$ és $N \leq L$, akkor $N \vee (K \wedge L) = (N \vee K) \wedge L$ (*modularitás*).
c) Bármely $\rho, \sigma \in \mathcal{C}(G)$ $\rho \wedge \sigma = \rho \cap \sigma$ és $\rho \vee \sigma = \rho \circ \sigma = \sigma \circ \rho$.
d) Ha $\rho, \sigma, \tau \in \mathcal{C}(G)$ és $\rho \subseteq \tau$, akkor $\rho \vee (\sigma \wedge \tau) = (\rho \vee \sigma) \wedge \tau$).
e) Ha $N, K \in \mathcal{S}_n(G)$ és $\rho, \sigma \in \mathcal{C}(G)$, akkor $\rho_{NK} = \rho_N \circ \rho_K$ és $(\rho \circ \sigma)\langle 1 \rangle = \rho\langle 1 \rangle \cdot \sigma\langle 1 \rangle$.
f) Ha $N_i \in \mathcal{S}_n(G)$, $i \in I$, akkor $\bigcap_{i \in I} N_i$, $\langle \bigcup_{i \in I} N_i \rangle \in \mathcal{S}_n(G)$ (tehát $\mathcal{S}_n(G)$ teljes részhálója $\mathcal{S}(G)$-nek).

3.3. Faktorcsoport. Izomorfizmustételek

Legyen $(G, \cdot)$ egy csoport, $N \trianglelefteq G$, $\rho_N \in \mathcal{C}(G)$ az N-szerinti kongruenciareláció, és tekintsük a $G/N = G/\rho_N = \{xN \mid x \in G\}$ faktorhalmazt és a

$$p_N : G \longrightarrow G/N, \quad p_N(x) = xN$$

kanonikus projekciót.

Faktorcsoport szerkesztése

3.3.1. tétel. *A* G/N *faktorhalmazon értelmezhető egy „·" művelet úgy, hogy* $(G/N, \cdot)$ *csoport, a* $p_N : G \longrightarrow G/N$ *csoportmorfizmus és* $\operatorname{Ker} p_N = N$ (tehát minden normális részcsoport egy morfizmus magja).

Bizonyítás. Legyen $x, y \in G$, és értelmezzük a következő szorzatot:

$$xN \cdot yN = xyN.$$

Igazolni kell, hogy az értelmezés nem függ az x, y reprezentánsoktól. Valóban, legyen $x' \in xN$ és $y' \in yN$. Akkor $x' = xn_1$ és $y' = yn_2$, ahol $n_1, n_2 \in N$; következik, hogy $x'y' = xn_1yn_2 \in N$. Átírva az utolsó egyenlőséget kapjuk, hogy

$$x'y'N = xyy^{-1}n_1yn_2N = xyn_3n_2N,$$

ahol $n_3 = y^{-1}n_1y \in N$, tehát $x'y'N = xyN$.

Igazoljuk, hogy $(G/N, \cdot)$ csoport. Valóban, minden $x, y, z \in G$ esetén

$$\begin{aligned}(xNyN)zN &= (xyN)zN = (xy)zN = \\ &= xN(yz)N = xN(yNzN),\end{aligned}$$

tehát „·" asszociatív; létezik semleges elem, és ez az e osztálya, mert minden $x \in G$ esetén $xNeN = eNxN = xN$; minden $x \in G$ esetén létezik $(xN)^{-1} = x^{-1}N \in xN$, mert $xNx^{-1}N = x^{-1}NxN = N$.

Továbbá, p_N morfizmus mert $p_N(xy) = xyN = xNyN = p_N(x)p_N(y)$, minden $x, y \in G$ esetén, és végűl $\operatorname{Ker} p_N = N$, mert

$$x \in \operatorname{Ker} p_N \Longleftrightarrow p_N(x) = eN \Longleftrightarrow xN = eN \Longleftrightarrow x \in N. \qquad \blacksquare$$

3.3.2. definíció. A $(G/N, \cdot)$ csoportot G-nek az N-szerinti **faktorcsoport**jának nevezzük.

3.3.3. példa (A modulo n maradékosztályok csoportja). Tekintsük a $(\mathbb{Z}, +)$ Abel-csoportot, és legyen $n \in \mathbb{N}$; ekkor $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\}$ normális részcsoportja $\mathbb{Z}$-nek. Láttuk, hogy

$$x\rho_{n\mathbb{Z}}y \Longleftrightarrow y - x \in \mathbb{Z} \Longleftrightarrow n|x - y \Longleftrightarrow x \equiv y \pmod{n},$$

tehát

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \mathbb{Z}/\rho_{n\mathbb{Z}} = \{\hat{x} \mid x \in \mathbb{Z}\},$$

ahol $\hat{x} = x + n\mathbb{Z} = \{x + nk \mid k \in \mathbb{Z}\}$.

Ha $n = 0$, akkor $n\mathbb{Z} = \{0\}$, $\hat{x} = x + \{0\} = \{x\}$ és $\mathbb{Z}_0 = \{\{x\} \mid x \in \mathbb{Z}\} = \mathbb{Z}$.

Ha $n = 1$, akkor $n\mathbb{Z} = \mathbb{Z}$, $\hat{x} = x + \mathbb{Z} = \mathbb{Z}$ és $\mathbb{Z}_1 = \{\mathbb{Z}\}$.

Ha $n \geq 2$, akkor minden $x \in \mathbb{Z}$ esetén, $\hat{x} = \widehat{x \bmod n} \in \{0, \ldots, n-1\}$. Továbbá, ha $0 \leq r, s \leq n-1$ és $r \neq s$, akkor $\hat{r} \neq \hat{s}$, tehát $\mathbb{Z}_n = \{\hat{0}, \ldots, \widehat{n-1}\}$.

3.3.4. tétel (Az I. izomorfizmustétel). *Ha* $f : G \longrightarrow G'$ *egy morfizmus, akkor*

$$G/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Bizonyítás. Tudjuk, hogy $\operatorname{Im} f \leq G'$ és $\operatorname{Ker} f \trianglelefteq G$, tehát $(G/\operatorname{Ker} f, \cdot)$ csoport. Legyen

$$\bar{f} : G/\operatorname{Ker} f \longrightarrow G', \quad \bar{f}(x \operatorname{Ker} f) = f(x),$$

és igazoljuk, hogy $\bar{f}$ jól értelmezett.

Valóban, feltételezzük, hogy $x \operatorname{Ker} f = x' \operatorname{Ker} f$, vagyis $x' = xn$, ahol $n \in \operatorname{Ker} f$. Ekkor

$$\begin{aligned}\bar{f}(x' \operatorname{Ker} f) &= \bar{f}(xn \operatorname{Ker} f) = f(xn) = \\ &= f(x)f(n) = f(x).\end{aligned}$$

Továbbá, $\bar{f}$ morfizmus, mert minden $x, y \in G$ esetén

$$\begin{aligned}\bar{f}(x \operatorname{Ker} f \cdot y \operatorname{Ker} f) &= \bar{f}(xy \operatorname{Ker} f) = \\ &= f(xy) = f(x)f(y) = \\ &= \bar{f}(x \operatorname{Ker} f)\bar{f}(y \operatorname{Ker} f)\end{aligned}$$

Végűl igazoljuk, hogy $\bar{f}$ bijektív. Ha $\bar{f}(x \operatorname{Ker} f) = e'$, akkor $f(x) = e'$, tehát $x \in \operatorname{Ker} f$, és $x \operatorname{Ker} f = \operatorname{Ker} f$; következik, hogy $\bar{f}$ injektív. Minden $x' \in \operatorname{Im} f$ esetén létezik $x \in G$ úgy, hogy $x' = f(x)$; következik, hogy $\bar{f}(x \operatorname{Ker} f) = f(x) = x'$, tehát $\bar{f}$ szürjektív. ■

Alkalmazások

3.3.5. tétel (A kínai maradéktétel). *Ha* $m, n \in \mathbb{N}$ *úgy, hogy* $(m, n) = 1$*, akkor*

$$(\mathbb{Z}_{mn}, +) \simeq (\mathbb{Z}_m \times \mathbb{Z}_n, +).$$

Bizonyítás. Legyen $f : \mathbb{Z} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$, $f(x) = (\bar{x}, \hat{x})$. f morfizmus, mert minden $x, y \in \mathbb{Z}$ esetén

$$\begin{aligned}f(x+y) &= (\overline{x+y}, \widehat{x+y}) = (\bar{x}+\bar{y}, \hat{x}+\hat{y}) = \\ &= (\bar{x}, \hat{x}) + (\bar{y}, \hat{y}) = f(x) + f(y)\end{aligned}$$

Továbbá, meghatározzuk az f magját:

$$\begin{aligned}\operatorname{Ker} f &= \{x \in \mathbb{Z} \mid f(x) = (\bar{0}, \hat{0})\} = \\ &= \{x \in \mathbb{Z} \mid (\bar{x}, \hat{x}) = (\bar{0}, \hat{0})\} = \\ &= \{x \in \mathbb{Z} \mid m|x, n|x\} = \\ &= \{x \in \mathbb{Z} \mid mn|x\} = mn\mathbb{Z}.\end{aligned}$$

Az I. izomorfizmustételből következik, hogy $\bar{f} : \mathbb{Z}/mn\mathbb{Z} \longrightarrow \operatorname{Im} f$, $\bar{f}(\hat{x}) = f(x)$ izomorfizmus.

Igazolni kell még, hogy $\operatorname{Im} f = \mathbb{Z}_m \times \mathbb{Z}_n$. Tudjuk, hogy $\operatorname{Im} f \subseteq \mathbb{Z}_m \times \mathbb{Z}_n$. Mivel $|\mathbb{Z}_{mn}| = mn$ és $\bar{f}$ injektív következik, hogy $|\operatorname{Im} f| = mn$, de $|\mathbb{Z}_m \times \mathbb{Z}_n| = |\mathbb{Z}_m||\mathbb{Z}_n| = mn$, tehát $\operatorname{Im} f = \mathbb{Z}_m \times \mathbb{Z}_n$. ■

3.3.6. tétel (Ciklikus csoportok osztályozása). *Ha* $(G, \cdot)$ *csoport és* $x \in G$*, akkor vagy* $\langle x \rangle \simeq \mathbb{Z}$ *vagy létezik* $n \in \mathbb{N}^*$ *úgy, hogy* $\langle x \rangle \simeq \mathbb{Z}_n$*. (Tehát minden ciklikus csoport izomorf* $\mathbb{Z}$*-vel vagy* $\mathbb{Z}_n$*-nel.)*

Bizonyítás. Legyen $f : \mathbb{Z} \longrightarrow G$, $f(k) = x^k$. Akkor f morfizmus, mert

$$f(k+l) = x^{k+l} = x^k x^l = f(k)f(l).$$

Továbbá $\operatorname{Im} f = \{x^k \mid k \in \mathbb{Z}\} = \langle x \rangle$ és $\operatorname{Ker} f = \{k \in \mathbb{Z} \mid f(k) = e\} \leq (\mathbb{Z}, +)$, ezért létezik $n \in \mathbb{N}$ úgy, hogy $\operatorname{Ker} f = n\mathbb{Z}$.

Ha $n = 0$, akkor $\operatorname{Ker} f = \{0\}$, azaz f injektív függvény és

$$(\mathbb{Z}, +) \simeq \operatorname{Im} f = \langle x \rangle = \{\ldots, x^{-1}, e, x, \ldots\}.$$

Ha $n > 0$, akkor $\operatorname{Ker} f = n\mathbb{Z} \neq \{0\}$. Az I. izomorfizmus tételből következik, hogy

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} \simeq \operatorname{Im} f = \langle x \rangle = \{e, x, \ldots, x^{n-1}\}. \qquad ■$$

3.3.7. megjegyzés (Faktorcsoport részcsoportjai). Mivel a $p_N : G \longrightarrow G/N$ kanonikus projekció szürjektív morfizmus és $\operatorname{Ker} p_N = N$, ezért $\mathcal{S}(G/N) = \{p_N(H) \mid H \leq G, N \subseteq H\}$. Mivel

$$p_N(H) = \{p_N(x) \mid x \in H\} = \{xN \mid x \in H\} = H/N,$$

következik, hogy

$$\mathcal{S}(G/N) = \{H/N \mid H \leq G, N \subseteq H\} \quad \text{és} \quad \mathcal{S}_n(G/N) = \{H/N \mid H \trianglelefteq G, N \subseteq H\}.$$

Például: $\mathcal{S}(\mathbb{Z}_n) = \{H/n\mathbb{Z} \mid H \leq \mathbb{Z}, n\mathbb{Z} \subseteq H\} = \{m\mathbb{Z}/n\mathbb{Z} \mid m \in \mathbb{N}, m|n\}$.

3.3.8. tétel (A II. izomorfizmustétel). *Ha* $(G, \cdot)$ *csoport,* N *normális részcsoportja* G*-nek és* H *részcsoportja* G*-nek, akkor*

$$H/H \cap N \simeq HN/N.$$

Bizonyítás. Legyen $f : H \longrightarrow G/N$, $f(h) = hN$. Akkor f morfizmus, mert minden $h_1, h_2 \in H$ esetén

$$f(h_1h_2) = h_1h_2N = h_1Nh_2N = f(h_1)f(h_2).$$

Továbbá, meghatározuk $\operatorname{Ker} f$-et és $\operatorname{Im} f$-et:

$$\begin{aligned}\operatorname{Ker} f &= \{h \in H \mid f(h) = N\} = \{h \in H \mid hN = N\} = \\ &= \{h \in H \mid h \in N\} = H \cap N; \\ \operatorname{Im} f &= \{f(h) \mid h \in H\} = \{hN \mid h \in H\} = \\ &= \{hnN \mid n \in N, h \in H\} = HN/N.\end{aligned}$$

Az I. izomorfizmustételből, következik, hogy $H/H \cap N \simeq HN/N$. ■

3.3.9. megjegyzés. A fenti jelöléseket alkalmazva $HN = NH = \sup_{S(G)}\{H, N\}$.

Valóban, $HN \neq \emptyset$, és $HN = NH$ mert $hN = Nh$ minden $h \in H$ esetén; ha $x_1 = h_1n_1$, $x_2 = h_2n_2 \in HN$, akkor $x_1x_2 = h_1n_1h_2n_2 = h_1h_2h_2^{-1}n_1h_2n_2 \in HN$, (ahol $h_2^{-1}n_1h_2 \in N$) és $x_1^{-1} = n_1^{-1}h_1^{-1} = h_1^{-1}h_1n_1^{-1}h_1^{-1} \in HN$ (mert $h_1n_1^{-1}h_1^{-1} \in N$), tehát $HN \leq (G, \cdot)$.

Továbbá $h = he \in HN$ és $n = en \in HN$ minden $h \in H$ és $n \in N$ esetén, vagyis $H \subseteq HN$ és $N \subseteq HN$.

Feltételezzük, hogy $H' \leq (G, \cdot)$ úgy, hogy $H, N \subseteq H'$. Ha $h \in H$, $n \in N$, akkor $h, n \in H'$ és $hn \in H'$, azaz $HN \subseteq H'$.

3.3.10. példa. Ha $G = (\mathbb{Z}, +)$, $H = m\mathbb{Z}$ és $N = n\mathbb{Z}$, akkor $\mathbb{Z}/m\mathbb{Z} \cap n\mathbb{Z} \simeq m\mathbb{Z} + n\mathbb{Z}/n\mathbb{Z}$, vagyis

$$(\mathbb{Z}/[m, n]\mathbb{Z}, +) \simeq ((m, n)\mathbb{Z}/n\mathbb{Z}, +).$$

3.3.11. tétel (A III. izomorfizmustétel). *Ha* $(G, \cdot)$ *egy csoport, és* N_1, N_2 *normális részcsoportjai* G*-nek úgy, hogy* $N_1 \subseteq N_2$*, akkor*

$$(G/N_1)/(N_2/N_1) \simeq G/N_2.$$

Bizonyítás. Legyen $g : G/N_1 \longrightarrow G/N_2$, $g(xN_1) = xN_2$; g jól értelmezett, mert $x' = xn_1$, (ahol $n_1 \in N_1$) esetén $g(x'N) = g(xn_1N_1) = xn_1N_2 = xN_2$.

Igazoljuk, hogy g morfizmus. Minden $x, y \in G$ esetén fennáll:

$$g(xN_1yN_1) = g(xyN_1) = xyN_2 = xN_2yN_2 = g(xN_1)g(yN_1).$$

Evidens, hogy g szürjektív függvény. Meghatározzuk a g magját:

$$\begin{aligned}\operatorname{Ker} g &= \{xN_1 \in G/H_1 \mid g(xN_1) = N_2\} = \\ &= \{xN_1 \in G/H_1 \mid xN_2) = N_2\} = \\ &= \{xN_1 \in G/H_1 \mid x \in N_2\} = N_2/N_1.\end{aligned}$$

Az I. izomorfizmustételből következik, hogy $(G/N_1)/(N_2/N_1) \simeq G/N_2$. ■

3.3.12. példa. Ha $G = (\mathbb{Z}, +)$ az egész számok csoportja, és $N_1 = n\mathbb{Z}$, $N_2 = m\mathbb{Z}$ normális részcsoportjai G-nek úgy, hogy $N_1 \subseteq N_2$ (tehát $m|n$), akkor következik, hogy $G/N_1 = \mathbb{Z}_n$, $G/N_2 = \mathbb{Z}_m$ és $N_2/N_1 = m\mathbb{Z}/n\mathbb{Z} = \hat{m}\mathbb{Z}_n$, tehát

$$\mathbb{Z}_n/\hat{m}\mathbb{Z}_n \simeq \mathbb{Z}_m.$$

3.18. feladat. a) Határozzuk meg a $(\mathbb{Z}, +)$ és $(\mathbb{Z}_n, +)$ faktorcsoportjait. Alkalmazás: $n = 10, 12$.

3.19. feladat. Határozzuk meg a következő csoportok faktorcsoportjait:
a) $(S_3, \circ)$;
b) $(Q, \cdot)$
c) $(A_4, \circ)$
d) $(D_n, \cdot)$, ahol $n = 4, 5, 6$.

3.20. feladat. Legyen $f : G \to G'$ egy morfizmus. Bizonyítsuk be, hogy:

a) f akkor és csak akkor injektív, ha minden $\alpha, \beta : H \to G$ morfizmusok esetén, az $f \circ \alpha = f \circ \beta$ egyenlőséhből következik, hogy $\alpha = \beta$.

b) Tételezzük fel, hogy $\operatorname{Im} f \trianglelefteq G'$. f akkor és csak akkor szürjektív, ha minden $\alpha, \beta : G' \to H$ morfizmusok esetén, $\alpha \circ f = \beta \circ f \Rightarrow \alpha = \beta$.

3.21. feladat. Legyen $H = \{z \in \mathbb{C} \mid |z| = 1\}$ és $U = \{z \in \mathbb{C} \mid (\exists)n \in \mathbb{N}^* \ \ z^n = 1\}$. Bizonyítsuk be, hogy:
a) $(\mathbb{C}/\mathbb{R}, +) \simeq (\mathbb{R}, +)$.
b) $(\mathbb{C}^*/H, \cdot) \simeq (\mathbb{R}^*_+, \cdot)$.
c) $(\mathbb{C}^*/\mathbb{R}^*_+, \cdot) \simeq (H, \cdot)$.
d) $(\mathbb{R}/\mathbb{Z}, +) \simeq (H, \cdot)$.
e) $(\mathbb{Q}/\mathbb{Z}, +) \simeq (U, \cdot)$.
f) $(\mathbb{Q}^*/U_2, \cdot) \simeq (\mathbb{Q}^*_+, \cdot)$.
g) $(\mathbb{R}^*/U_2, \cdot) \simeq (\mathbb{R}^*_+, \cdot)$.
h) $(\mathbb{C}/\mathbb{Z}, +) \simeq (\mathbb{C}^*, \cdot)$.
i) $(\mathbb{C}^*/U, \cdot) \simeq (\mathbb{R}^*_+, \cdot) \times (\mathbb{R}/\mathbb{Q}, +)$.

3.22. feladat. Legyen $f_{a,b} : \mathbb{R} \to \mathbb{R}$, $f_{a,b}(x) = ax + b$, ahol $a, b \in \mathbb{R}$, $G = \{f_{a,b} \mid a \in \mathbb{R}^*, \ b \in \mathbb{R}\}$, $H = \{f_{a,0} \mid a \in \mathbb{R}^*\}$ és $N = \{f_{1,b} \mid b \in \mathbb{R}\}$. Igazoljuk, hogy $G, H \leq (S_{\mathbb{R}}, \circ)$, H nem normális részcsoportja G-nek és $(G/N, \circ) \simeq (\mathbb{R}^*, \cdot)$.

3.23. feladat. Legyen $n \in \mathbb{N}^*$, $(K, +, \cdot)$ egy kommutatív test, $SL_n(K) = \{A \in M_n(K) \mid \det(A) = 1\}$, $SO(n) = O(n) \cap SL_n(\mathbb{R})$, $SU(n) = U(n) \cap SL_n(\mathbb{C})$ és $H = \{z \in \mathbb{C} \mid |z| = 1\}$. Igazoljuk, hogy:
a) $GL_n(K)/SL_n(K) \simeq (K^*, \cdot)$.
b) $O(n)/SO(n) \simeq (U_2, \cdot)$.
c) $U(n)/SU(n) \simeq (H, \cdot)$.
d) $SO(2) \simeq H$.

3.24. feladat. Legyen K egy kommutatív test, $T_n(K) = \{(a_{ij}) \in GL_n(K) \mid a_{ij} = 0 \text{ ha } n \geq i > j \geq 1\}$ és $UT_n(K) = \{(a_{ij}) \in T_n(K) \mid a_{ii} = 1 \ (\forall)i, \ 1 \leq i \leq n\}$. Igazoljuk, hogy:
a) $T_n(K) \leq GL_n(K)$;
b) $T_n(K)/UT_n(K) \simeq ((K^*)^n, \cdot)$.

3.25. feladat. Legyen $n \in \mathbb{Z}$ és feltételezzük, hogy $f : G \to G$, $f(x) = x^n$ homomorfizmus. Továbbá, legyen $G_n = \{x \in G \mid x^n = e\}$ és $G^n = \{x^n \mid x \in G\}$. Bizonyítsuk be, hogy:
a) $G_n, G^n \trianglelefteq G$.
b) $G/G_n \simeq G^n$.

3.4. Elem rendje

Legyen $(G, \cdot)$ egy csoport és $x \in G$. Ha $f : \mathbb{Z} \to G$, $f(k) = x^k$, akkor f morfizmus, és $\operatorname{Im} f = \langle x \rangle$.

Ha f injektív morfizmus, akkor azt mondjuk, hogy x *végtelen rendű* (jelölés: $\operatorname{ord}(x) = \infty$), ellenkező esetben (ha f nem injektív) x-et *véges rendűnek* nevezzük.

Ezek szerint, ha x egy véges rendű elem, akkor létezik $k, l \in \mathbb{N}$, $k < l$ úgy, hogy $x^k = x^l$, vagyis $x^{l-k} = e$. Következik, hogy $M = \{k \mid a^k = e, k > 0\} \neq \emptyset$; mivel $M \subseteq \mathbb{N}$, és $\mathbb{N}$ jólrendezett halmaz, M-nek van legkisebb eleme.

3.4.1. definíció. Azt az n legkisebb pozitív számot, amelyre $x^n = e$ az x elem **rend**jének nevezzük. (Jelölés: $\operatorname{ord}(x) = n = \min\{k \in \mathbb{N}^* \mid x^k = e\}$).

3.4.2. példa. a) A $(\mathbb{C}^*, \cdot)$ csoportban $\operatorname{ord}(-1) = 2$, $\operatorname{ord}(i) = 4$ és $\operatorname{ord}(3) = \infty$.
b) Általában ha $x \in G$, akkor $\operatorname{ord}(x) = 1 \Longleftrightarrow x = e$.
c) S_3-ban $\operatorname{ord}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\right) = 2$ és $\operatorname{ord}\left(\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\right) = 3$.

3.4.3. megjegyzés. 1) $\operatorname{ord}(x) = \infty$ akkor és csak akkor, ha minden $n \in \mathbb{N}^*$ esetén $x^n \neq e$. Ebben az esetben, $\langle x \rangle = \operatorname{Im} f \simeq (\mathbb{Z}, +)$.
2) $\operatorname{ord}(x) = n \in \mathbb{N}^*$ akkor és csak akkor, ha teljesül az, hogy $x^n = e$ és ha $x^k = e$, ahol $k \in \mathbb{N}^*$, akkor $n \leq k$.

3.4.4. lemma (Az elem rendjének jellemzése). *Legyen $(G, \cdot)$ egy csoport, $x \in G$ egy véges rendű elem és $n \in \mathbb{N}^*$. A következő állítások egyenértékűek:*
1) Az x elem rendje n.
2) $x^n = e$ és, ha $k \in \mathbb{Z}$ esetén $x^k = e$, akkor $n|k$.

Bizonyítás. 1) $\Longrightarrow$ 2) Mivel $\operatorname{ord}(x) = n$ ezért $x^n = e$.

Feltételezzük, hogy $k \in \mathbb{Z}$ és $x^k = e$. A maradékos osztás tételéből következik, hogy létezik $q, r \in \mathbb{Z}$ úgy, hogy $k = nq + r$ és $0 \leq r < n$. Ekkor $e = x^k = x^{nq+r} = (x^n)^q \cdot x^r = x^r$ és $0 \leq r < n$, vagyis $e = x^r$. Az n minimalitásából következik, hogy $r = 0$, azaz $n|k$.

2) $\Longrightarrow$ 1) Feltételezzük, hogy $k \in \mathbb{N}^*$ és $x^k = e$; következik, hogy $n|k$, ahol $n, k \in \mathbb{N}^*$, ezért $n \leq k$. ■

3.4.5. tétel. *Legyen* $(G, \cdot)$ *egy csoport és* $x \in G$.
1) *Ha* $\mathrm{ord}(x) = n \in \mathbb{N}^*$, *akkor* $\langle x \rangle = \{e, x, \dots, x^{n-1}\}$ *és* $|\langle x \rangle| = n$, *tehát* $\langle x \rangle \simeq (\mathbb{Z}_n, +)$.
2) *Ha* G *véges csoport, akkor az* x *elem rendje osztja a* G *csoport rendjét. Partikulárisan,* $x^{|G|} = e$.

Bizonyítás. 1) Tudjuk, hogy $\langle x \rangle = \{x^k \mid k \in \mathbb{Z}\}$. Alkalmazva a maradékos osztás tételét k-ra, létezik $q, r \in \mathbb{Z}$ úgy, hogy $k = nq + r$ és $0 \le r < n$; következik, hogy $x^k = x^{nq+r} = (x^n)^q x^r = x^r \in \{e, x, \dots, x^{n-1}\}$. Ha $0 \le k < l \le n-1$ és $x^k = x^l$, akkor $x^{l-k} = e$, ahol $0 < l - k < n$, ami ellentmond az n minimalitásának, tehát $|\langle x \rangle| = n$.
2) Alkalmazva Lagrange tételét $|G| = |\langle x \rangle| \cdot [G : \langle x \rangle]$, tehát $|\langle x \rangle|$ osztja $|G|$-t. ■

3.4.6. következmény. 1) **(A p-ed rendű csoportok osztályozása)** *Ha* $|G| = p$, *akkor*

$$(G, \cdot) \simeq (\mathbb{Z}_p, +).$$

2) **(Euler-tétel)** *Ha* $n \in \mathbb{Z}$, $n \ge 2$ *és* $a \in \mathbb{Z}$ *úgy, hogy* $(a, n) = 1$, *akkor* $a^{\varphi(n)} \equiv 1 \pmod{n}$, *ahol*

$$\varphi(n) = |\{a \in \mathbb{Z} \mid 0 \le a \le n, (a, n) = 1\}|$$

az Euler-függvény.
3) **(Fermat-tétel)** *Ha* $p \in \mathbb{Z}$ *prímszám és* $a \in \mathbb{Z}$, *akkor* $a^p \equiv a \pmod{p}$.

Bizonyítás. 1) Mivel $|G| > 1$ következik, hogy létezik $x \in G$ úgy, hogy $x \ne e$, tehát $|\langle x \rangle| > 1$. Az 3.4.5.2) tételből következik, hogy $|\langle x \rangle|$ osztja $|G|$-t, de p prímszám, tehát $G = \langle x \rangle$ p-ed rendű ciklikus csoport. Az 3.4.5.1) tételből következik, hogy $G \simeq (\mathbb{Z}_p, +)$.
2) Tudjuk, hogy $U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n \mid \hat{a} \text{ invertálható}\} = \{\hat{a} \in \mathbb{Z}_n \mid (a, n) = 1\}$ $\varphi(n)$-ed rendű csoport. Ha $\hat{a} \in U(\mathbb{Z}_n)$, akkor $\mathrm{ord}(\hat{a})$ osztja $\varphi(n)$-et, tehát $\hat{a}^{\varphi(n)} = \hat{1}$, vagyis $a^{\varphi(n)} \equiv 1 \pmod{n}$.
3) Ha p osztja a-t, akkor p osztja $a^p - a$-t is, ezért $a^p \equiv a \pmod{p}$.
Ha p nem osztja a-t, akkor $(a, p) = 1$ és $\varphi(p) = p - 1$. Az Euler-tételből következik, hogy $a^{p-1} \equiv 1 \pmod{p}$, vagyis $a^p \equiv 1 \pmod{p}$. ■

3.26. feladat. Legyen $(G, \cdot)$ egy csoport és $x \in G$. Igazoljuk, hogy:
a) $\mathrm{ord}(x) = 1 \Leftrightarrow x = e$; $\mathrm{ord}(x) = 2 \Leftrightarrow x^2 = e,\ x \ne e$.
b) $\mathrm{ord}(x) = \mathrm{ord}(x^{-1})$.
c) Ha $\mathrm{ord}(x) = n \in \mathbb{N}^*$ és $k \in \mathbb{Z}$, akkor $\mathrm{ord}(x^k) = \frac{n}{(k,n)}$; ha $n = km$, akkor $\mathrm{ord}(x^k) = m$.
d) Ha $\mathrm{ord}(x) = n$ és $(n, k) = d$, akkor $\langle x^k \rangle = \langle x^d \rangle$;
Partikulárisan $\langle x \rangle = \langle x^k \rangle \Leftrightarrow (n, k) = 1$. Következik, hogy $\langle x \rangle$-nek pontosan $\varphi(n)$ generáló eleme van.
Alkalmazás: határozzuk meg a 8-ad rendű primitív egységgyököket.
e) Ha $\mathrm{ord}(x) = 2n + 1$, akkor $(\forall) y \in \langle x \rangle$ $(\exists) z \in \langle x \rangle$ úgy, hogy $y = z^2$.

3.27. feladat. Legyen $f : G \to G'$ egy homomorfizmus, és $x \in G$. Igazoljuk, hogy:
a) $\mathrm{ord}(f(x)) | \mathrm{ord}(x)$.
b) Ha f injektív, akkor $\mathrm{ord}(f(x)) = \mathrm{ord}(x)$.
c) Ha f izomorfizmus, akkor $|\{g \in G \mid \mathrm{ord}(g) = n\}| = |\{g' \in G' \mid \mathrm{ord}(g') = n\}|$.
Alkalmazás: Bizonyítsuk be, hogy
a) $(\mathbb{Q}, +) \not\simeq (\mathbb{Q}^*, \cdot)$;
b) $(\mathbb{R}, +) \not\simeq (\mathbb{R}^*, \cdot)$;
c) $(\mathbb{C}, +) \not\simeq (\mathbb{C}^*, \cdot)$;
d) $(\mathbb{R}^*, \cdot) \not\simeq (\mathbb{C}^*, \cdot)$;

3.28. feladat. Ha $(G, \cdot)$ egy csoport és $x, y \in G$, akkor $\mathrm{ord}(xy) = \mathrm{ord}(yx)$.

3.29. feladat. Legyen $(G, \cdot)$ egy csoport, $x, y \in G$ úgy, hogy $xy = yx$, $\mathrm{ord}(x) = m$ és $\mathrm{ord}(y) = n$. Igazoljuk, hogy:
a) $\mathrm{ord}(xy) | [\mathrm{ord}(x), \mathrm{ord}(y)]$.
b) Ha $\langle x \rangle \cap \langle y \rangle = \{e\}$, akkor $\mathrm{ord}(xy) = [m, n]$.
c) Ha $(m, n) = 1$, akkor $\mathrm{ord}(xy) = mn$ és $\langle xy \rangle = \langle x, y \rangle$.
d) Létezik $g \in G$ úgy, hogy $\mathrm{ord}(g) = [m, n]$.
e) Ha $(m, n) = 1$ és $g \in G$, akkor léteznek az egyértelműen meghatározott $x, y \in G$ elemek úgy, hogy $\mathrm{ord}(x) = m$, $\mathrm{ord}(y) = n$ és $xy = g$.

3.30. feladat. Legyen $(G, \cdot)$ egy csoport, $x_1, x_2, \dots, x_r \in G$ úgy, hogy $x_i x_j = x_j x_i$, $1 \le i, j \le r$, $\mathrm{ord}(x_i) = m_i \in \mathbb{N}^*$.
a) $\mathrm{ord}(x_1 \dots x_r) \mid [\mathrm{ord}(x_1), \dots, \mathrm{ord}(x_r)]$.
b) Ha $\langle x_i \rangle \cap \langle x_1, \dots, x_{i-1}, x_{i+1} \dots x_r \rangle = \{e\}$ minden i esetén, akkor $\mathrm{ord}(xy) = [m_1, \dots, m_r]$.
c) Ha $(m_i, m_j) = 1$, $i \ne j$, akkor $\mathrm{ord}(x_1 x_2 \dots x_n) = m_1 m_2 \cdots m_r$.

3.31. feladat (Permutáció rendje). Legyen $\gamma = (i_1 \dots i_l) \in S_n$ egy l-hosszúságú ciklus, és legyen $\sigma = \gamma_1 \circ \dots \circ \gamma_m \in S_n$, ahol $\gamma_1, \dots, \gamma_m$ diszjunkt ciklusok. Igazoljuk, hogy:

a) Ha $0 \le m \le l$, akkor $\gamma^m(i_j) = \begin{cases} i_{j+m}, & \text{ha } j+m \le l \\ i_{j+m-l}, & \text{ha } j+m > l \end{cases}$.

b) $\gamma^{-1} = (i_l\ i_{l-1} \dots i_2\ i_1) = \gamma^{l-1}$.

c) $\mathrm{ord}(\gamma) = l$.

d) Ha $\sigma \in S_n$, akkor létezik egy γ ciklus úgy, hogy $\sigma = \gamma^k \Leftrightarrow \sigma$ azonos hosszúságú ciklusok szorzata.

e) Ha a γ_i hossza l_i, akkor $\mathrm{ord}(\sigma) = [l_1, \dots, l_k]$.

f) Ha $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\ 4 & 6 & 2 & 7 & 8 & 3 & 10 & 9 & 5 & 1 \end{pmatrix}$, határozzuk meg σ^{101}-t.

3.32. feladat. (**Torziórészcsoport**) Legyen $(A, +)$ egy Abel-csoport és

$$T(A) = \{a \in A \mid (\exists) n \in \mathbb{N}^* : \ na = 0\}$$

az A *torziórészcsoportja.* Bizonyítsuk be, hogy:

a) $T(A) \le (A, +)$, és $T(A/T(A)) = \{T(A)\}$.

b) Ha $f : (A, +) \to (B, +)$ egy morfizmus, akkor $f(T(A)) \subseteq T(B)$.

c) Legyen $G = GL_2(\mathbb{Q})$, $X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $Y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$. Számítsuk ki az X, Y, XY elemek rendjét, és igazoljuk, hogy $T(G)$ nem részcsoport.

3.33. feladat. Legyen $U = T(\mathbb{C}^*, \cdot)$ és $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Bizonyítsuk be, hogy:

a) $U = \bigcup_{n \ge 1} U_n$.

b) $U_n \cap U_m = U_{(m,n)}$ és $U_m U_n = U_{[m,n]}$.

c) U_n $\mathbb{C}^*$-nak az egyetlen n-ed rendű részcsoportja.

3.34. feladat. Legyen $(G, \cdot)$ egy csoport, és $\varnothing \ne H \subseteq G$ egy zárt részhalmaz. Ha $(\forall) x \in H$ $\mathrm{ord}(x) < \infty$, akkor H részcsoport.

3.35. feladat. Legyen $(G, \cdot)$ egy véges csoport. Igazoljuk, hogy:

a) $\prod_{x \in G} x = \prod \{x \in G \mid \mathrm{ord}(x) = 2\}$.

Következmény (Wilson tétele). Ha p egy prímszám, akkor $(p-1)! \equiv -1 \pmod p$.

b) Ha $|G|$ páros, akkor $(\exists) x \in G, x \ne e$ úgy, hogy $\mathrm{ord}(x) = 2$.

3.36. feladat. Egy végtelen csoportnak végtelen sok részcsoportja van.

3.37. feladat. Legyen $(G, \cdot)$ egy csoport, $N \le G$ egy ciklikus normális részcsoport, és $H \le N$. Igazoljuk, hogy $H \trianglelefteq G$.

3.38. feladat. Legyen G egy csoport, $m, n \in \mathbb{N}^*$, $(m, n) = 1$, és $N \trianglelefteq G$.

a) Feltételezzük, hogy $[G : N] = n$. Igazoljuk, hogy $(\forall) x \in G$, $x^n \in N$, és ha $x^m \in N$, akkor $x \in N$.

b) Feltételezzük, hogy $|N| = m$. Ha $\mathrm{ord}(x) = n$, akkor $\mathrm{ord}(xN) = n$; fordítva, ha $\mathrm{ord}(xN) = n$, akkor létezik $y \in xN$ úgy, hogy $\mathrm{ord}(y) = n$.

3.39. feladat. Ha p egy prím szám és G egy Abel-csoport, melynek rendje osztható p-vel, akkor G-ben léteznek p-ed rendű elemek.

3.40. feladat. Legyen n egy páratlan szám és G egy $2n$-ed rendű csoport. Igazoljuk, hogy G-nek van egy n-ed rendű normális részcsoportja.

3.41. feladat. Azt mondjuk, hogy G **metaciklikus** csoport, ha létezik $N \trianglelefteq G$ úgy, hogy N és G/N ciklikus csoportok. Igazoljuk, hogy G minden részcsoportja és minden faktorcsoportja metaciklikus.

3.42. feladat (Kváziciklikus csoport). Legyen p egy prímszám és

$$\mathbb{C}_{p^\infty} = \{z \in \mathbb{C} \mid (\exists) n \in \mathbb{N} : z^{p^n} = 1\} = \bigcup_{n \in \mathbb{N}} U_{p^n}.$$

Igazoljuk, hogy: a) $\mathbb{C}_{p^\infty} \le (\mathbb{C}^*, \cdot)$.

b) $\mathbb{C}_{p^\infty}$ bármely valódi részcsoportja U_{p^n} alakú.

c) $\mathbb{C}_{p^\infty}/U_{p^n} \simeq \mathbb{C}_{p^\infty}$.

d) $(\mathbb{Q}_p/\mathbb{Z}, +) \simeq (\mathbb{C}_{p^\infty}, \cdot)$, ahol $\mathbb{Q}_p = \{\frac{k}{p^n} \mid k \in \mathbb{Z},\ n \in \mathbb{N}\}$.

3.5. Csoportok és részcsoportok direkt szorzata

Legyenek H, K csoportok, és tekintsuk a

$$G = H \times K = \{(h, k) \mid h \in H, k \in K\}$$

halmazt és a

$$(h, k) \cdot (h', k') = (hh', kk')$$

műveletet. Akkor $(G, \cdot)$ csoport, amelyet a H és K **direkt szorzat**ának nevezünk. Legyenek $p_H : H \times K \to H$, $p_H(h, k) = h$ és $p_K : H \times K \to K$, $p_K(h, k) = k$ a *kanonikus projekciók.*

3.43. feladat. Legyen $H_1 := H \times \{e\}$, $K_1 := \{e\} \times K \subseteq H \times K$. Bizonyítsuk be, hogy:
a) $H \simeq H_1$ és $K \simeq K_1$. (Tehát H és K beágyazhatók $H \times K$-ba.)
b) A p_H, p_K kanonikus projekciók szürjektív morfizmusok.
c) $H \times K/H_1 \simeq K$, $H \times K/K_1 \simeq H$.
d) $\mathrm{ord}(h, k) = [\mathrm{ord}(h), \mathrm{ord}(k)$.
e) $Z(H \times K) = Z(H) \times Z(K)$.
f) Ha $H \simeq H'$ és $K \simeq K'$, akkor $H \times K \simeq H' \times K'$.

A továbbiakban a fordított problémával foglalkozunk: ha G egy csoport, $H, K \leq G$, mikor lesz G izomorf $H \times K$-val.

3.5.1. tétel. *Legyen* $(G, \cdot)$ *egy csoport,* H, K *részcsoportjai* G*-nek és* $f : H \times K \longrightarrow G$, $f((h, k)) = hk$.
1) *Az* f *függvény akkor és csak akkor injektív, ha* $H \cap K = \{e\}$.
2) *Az* f *függvény akkor és csak akkor szürjektív, ha* $HK = G$ (ahol $HK = \{hk \mid h \in$ $\in H, k \in K\}$).
3) *Az* f *függvény akkor és csak akkor morfizmus, ha* $hk = kh$ *minden* $h \in H$ *és* $k \in K$ *esetén.*

Bizonyítás. 1) Feltételezzük, hogy f injektív és $x \in H \cap K$. Mivel $f((x, e)) = xe = x$ és $f((e, x)) = ex = x$ következik, hogy $f((x, e)) = f((e, x))$, tehát $(x, e) = (e, x)$ és $x = e$.

Fordítva, feltételezzük, hogy $H \cap K = \{e\}$, és legyen $(h_1, k_1), (h_2, k_2) \in H \times K$ úgy, hogy $f((h_1, k_1)) = f((h_2, k_2))$. Ekkor $h_1k_1 = h_2k_2$, vagyis $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{e\}$, tehát $h_1 = h_2$ és $k_1 = k_2$. Ezzel igazoltuk, hogy $(h_1, k_1) = (h_2, k_2)$, vagyis f injektív függvény.

2) Feltételezzük, hogy f szürjektív; akkor

$$G = \mathrm{Im}\, f = \{f((h, k)) \mid (h, k) \in H \times K\} = \{hk \mid h \in H, k \in K\} = HK.$$

A fordított állítás evidens.

3) Feltételezzük, hogy $hk = kh$ minden $h \in H, k \in K$ esetén és igazoljuk, hogy f morfizmus.

$$\begin{aligned} f((h_1, k_1) \cdot (h_2, k_2)) &= f((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = \\ &= h_1k_1h_2k_2 = f((h_1, k_1)) \cdot f((h_2, k_2)) \end{aligned}$$

minden $(h_1, k_1), (h_2, k_2) \in H \times K$ esetén. Fordítva, feltételezzük, hogy f morfizmus. Ekkor $f((e, k) \cdot (h, e)) = f((e, k)) \cdot f((h, e))$ minden $h \in H$, $k \in K$ esetén, de $f((e, k) \cdot (h, e)) = f((h, k)) = hk$ és $f((e, k)) \cdot f((h, e)) = (ek)(he) = kh$, tehát $hk = kh$. ■

3.5.2. definíció. Legyen $(G, \cdot)$ egy csoport, H, K részcsoportjai G-nek és

$$f : H \times K \longrightarrow G, \quad f((h, k)) = hk.$$

Ha f izomorfizmus, akkor azt mondjuk, hogy G a H és K részcsoportok *belső direkt szorzata* (Jelölés: $G = H \times K$).

3.5.3. tétel (A belső direkt szorzat jellemzése). *Legyen* $(G, \cdot)$ *egy csoport és* H, K *részcsoportjai* G*-nek. A következő állítások ekvivalensek:*

(i) $G = H \times K$ (G a H és K belső direkt szorzata).

(ii) $H \cap K = \{e\}$, $G = HK$ *és* $H, K \trianglelefteq G$.

(iii) $H \cap K = \{e\}$, $G = HK$ *és* $hk = kh$ *minden* $h \in H$ *és* $k \in K$ *esetén.*

Bizonyítás. A 3.5.1. Tételből következik, hogy az (i) és (iii) egyenértékűek.

Feltételezzük most, hogy $G = H \times K$. Elég igazolni, hogy $H, K \trianglelefteq G$. Tudjuk, hogy $H, K \leq G$, és igazoljuk, hogy $ghg^{-1} \in H$ minden $h \in H, g \in G$ esetén. Valóban, mivel $g \in G = HK$ következik, hogy létezik $h_1 \in H, k_1 \in K$ úgy, hogy $g = h_1k_1$; ekkor

$$ghg^{-1} = h_1k_1hk_1^{-1}h_1^{-1} = h_1hk_1k_1^{-1}h_1^{-1} = h_1hh_1^{-1} \in H.$$

Hasonlóan igazoljuk, hogy $gkg^{-1} \in K$.

Fordítva, feltételezzük, hogy $H \cap K = \{e\}$, $HK = G$ és $H, K \trianglelefteq G$ és igazoljuk, hogy $hk = kh$ minden $h \in H$ és $k \in K$ esetén. Tudjuk, hogy $khk^{-1}h^{-1} \in H$ (ugyanis $khk^{-1} \in H$, mert $H \trianglelefteq G$) és $khk^{-1}h^{-1} \in K$ (ugyanis $hk^{-1}h^{-1} \in K$, mert $K \trianglelefteq G$), de $H \cap K = \{e\}$, tehát $khk^{-1}h^{-1} = e$, vagyis $kh = hk$. ■

3.5.4. megjegyzés. A 3.5.3. tétel (iii)-beli hipotézisek teljesülnek, ha $|G| = mn$, $|H| = m$, $|K| = n$, $(m, n) = 1$.

Valóban, igazoljuk, hogy $H \cap K = \{e\}$. Ha $x \in H \cap K$, akkor $\mathrm{ord}(x) \mid |H| = m$ és $\mathrm{ord}(x) \mid |K| = n$, tehát $\mathrm{ord}(x) \mid (m, n) = 1$, azaz $x = e$. Következik, hogy az a)-beli $f : H \times K \to G$ morfizmus injektív, mert $\mathrm{Ker}\, f = \{(e, e)\}$. Továbbá $H \times K \simeq \mathrm{Im}\, f \subseteq G \Rightarrow |\mathrm{Im}\, f| = mn = |G| \Rightarrow \mathrm{Im}\, f = G$, tehát f szürjektív.

3.5.5. példa. 1) (Multiplikatív eset) Legyen $G = U(\mathbb{Z}_8) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}\} = \{\hat{1}, \hat{5}, -\hat{1}, -\hat{5}\} = \{\hat{1}, \hat{5}\} \times \{\hat{1}, -\hat{1}\}$. $\mathrm{ord}(\hat{1}) = 1$, $\mathrm{ord}(\hat{3}) = 2$, $\mathrm{ord}(\hat{5}) = 2$, $\mathrm{ord}(\hat{7}) = 2$; $K \cap H = \{\hat{1}\}$, $H \cdot K = G$. G nem ciklikus, mert nem tartalmaz 4-ed rendű elemeket.

2) Legyen $G = U(\mathbb{Z}_{16}) = \{\hat{1}, \hat{3}, \hat{5}, \hat{9}, -\hat{1}, -\hat{3}, -\hat{5}, -\hat{9}\}$. Ekkor $\langle -\hat{1} \rangle = \{\hat{1}, -\hat{1}\} = H$, $\langle 5 \rangle = \{\hat{1}, \hat{9}, \hat{5}, \widehat{13}\} =: K$. Tehát $G = H \times K$. Itt $\mathrm{ord}(\hat{5}) = 4 = 2^{4-2}$, $\mathrm{ord}(\widehat{-1}) = 2$.

3) (Additív eset) Tekintsük a $(\mathbb{Z}_6, +)$ aditív csoportot, $\mathbb{Z}_6 = \{\hat{0}, \hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}\}$ Legyen $H := \langle \hat{2} \rangle = \{\hat{0}, \hat{2}, \hat{4}\}$, $K := \langle \hat{3} \rangle = \{\hat{0}, \hat{3}\}$. Ekkor $|H| = 3$, $|K| = 2$, $3 \cdot 2 = 6 = |\mathbb{Z}_6|$. Tehát b) $\Rightarrow \mathbb{Z}_6 = H \times K$.

3.5.6. megjegyzés. A fenti eredményeket lehet általánosítani:

Ha G egy csoport, $H_1, \ldots, H_n \leq G$ és

$$f : H_1 \times \ldots \times H_n \longrightarrow G, \quad f(h_1, \ldots, h_n) = h_1 \ldots h_n,$$

akkor azt mondjuk, hogy $G = H_1 \times \ldots \times H_n$, ha f izomorfizmus.

A következő állítások ekvivalensek:

(i) $G = H_1 \times \ldots \times H_n$.

(ii) $H_i \cap \langle \bigcup_{j \neq i} H_j \rangle = \{e\}$ minden $i \in \{1, \ldots, n\}$ esetén, $H_1 \ldots H_n = G$ és $h_ih_j = h_jh_i$ minden $h_i \in H_i, h_j \in H_j, i \neq j$ esetén.

(iii) $H_i \cap \langle \bigcup_{j \neq i} H_j \rangle = \{e\}$ minden $i \in \{1, \ldots, n\}$ esetén, $H_1 \ldots H_n = G$ és $H_i \trianglelefteq G$ minden $i \in \{1, \ldots, n\}$ esetén.

3.44. feladat. *Ha* $G_i \simeq H_i$, $i = 1, \ldots, n$ *izomorf csoportok, akkor* $G_1 \times \cdots \times G_n \simeq H_1 \times \cdots \times H_n$.

3.5.7. tétel (ciklikus direkt szorzat). *Legyen* $G = G_1 \times \cdots \times G_r$ *véges csoportok direkt szorzata. Akkor* G *ciklikus csoport* $\Leftrightarrow G_i$ *ciklikus minden* $i = 1, \ldots, r$ *esetén és* $(|G_i|, |G_j|) = 1$ *ha* $i \neq j$.

Bizonyítás. Legyen $|G_i| =: n_i$.

„$\Rightarrow$" Ha G ciklikus, akkor G_i is ciklikus, mivel G_i izomorf G-nek egy részcsoportjával. Feltételezzük, hogy $\exists\ i \neq j$ úgy, hogy $(|G_i|, |G_j|) \neq 1$. Legyen $(n_i, n_j) = d > 1$. Elég igazolni, hogy ekkor G nem tartalmaz $|G| = n_1 \cdot \cdots \cdot n_r$-edrendű elemet. Legyen $x = (x_1, \ldots, x_r) \in G$.

$$x^{\frac{n_1 \cdot \cdots \cdot n_r}{d}} = (x_1, \ldots, x_r)^{\frac{n_1 \cdot \cdots \cdot n_r}{d}} = \left(x_1^{\frac{n_1 \cdots n_r}{d}}, \ldots, x_i^{\frac{n_1 \cdots n_r}{d}}\right) = (e, \ldots, e) = e \in G,$$

mert $x_k^{n_k} = e$ G_k-ban. Ezzel igazoltuk, hogy minden $x \in G$ esetén, $\mathrm{ord}(x) \mid \frac{n_1 \cdot \cdots \cdot n_r}{d}$, tehát $\mathrm{ord}(x) < |G|$.

„$\Leftarrow$" Mivel G_i ciklikus, $(G_i, \cdot) \simeq (\mathbb{Z}_{n_i}, +)$. A kínai maradéktételből (általánosítsuk a 3.3.5. tételt!) következik, hogy

$$G \simeq (\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}, +) \simeq (\mathbb{Z}_{n_1 \cdot \cdots \cdot n_r}, +). \qquad ■$$

3.45. feladat (diagonális részcsoport). Legyen $(G, \cdot)$ egy csoport és $\Delta(G) = \{(g, g) \mid g \in G\}$. Igazoljuk, hogy

a) $\Delta(G) \leq G \times G$, és $G \simeq \Delta(G)$.

b) $\Delta(G)$ akkor és csak akkor normális, ha G kommutatív.

c) Ha G kommutatív, akkor $G \times G/\Delta(G) \simeq G$.

3.46. feladat. Legyen $(G, \cdot)$ egy tetszőleges csoport és $H, K \trianglelefteq G$.

a) Igazoljuk, hogy létezik egy $G/H \cap K \to G/H \times G/K$ injektív morfizmus;

b) ha $G = HK$, akkor $G/H \cap K \simeq G/H \times G/K$.

3.47. feladat. Legyenek G és H véges Abel-csoportok és $f : G \to H$ egy szürjektív morfizmus. Ha $(|\operatorname{Ker} f|, |H|) = 1$, akkor $G \simeq H \times \operatorname{Ker} f$.

3.48. feladat. Legyenek G_i csoportok és $x_i \in G_i$ véges rendű elemek, $i = 1, \dots, r$. Bizonyítsuk be, hogy:
a) $\operatorname{ord}(x_1, \dots, x_n) = [\operatorname{ord}(x_1), \dots, \operatorname{ord}(x_r)]$.
Alkalmazás: Bizonyítsuk be, hogy $(\mathbb{R}^* \times \mathbb{R}^*, \cdot) \not\simeq (\mathbb{C}^*, \cdot)$.
b) Ha $(n_i, n_j) = 1$, $1 \le i, j \le r$, $i \ne j$, akkor $(\mathbb{Z}_{n_1 \dots n_r}, +) \simeq (\mathbb{Z}_{n_1} \times \dots \times \mathbb{Z}_{n_r}, +)$.
c) Ha G_i véges ciklikus csoportok, akkor $\prod_{i=}^{r} G_i$ akkor és csak akkor ciklikus, ha $(|G_i|, |G_j|) = 1$ minden $i \ne j$ esetén.

3.49. feladat. Legyenek $G_1, \dots, G_r$ csoportok és $(A, +)$ egy Abel-csoport. Igazoljuk, hogy

$$(\operatorname{Hom}(G_1 \times \dots \times G_r, A), +) \simeq (\operatorname{Hom}(G_1, A) \times \dots \times \operatorname{Hom}(G_r, A), +). \tag{3.1}$$

3.50. feladat. Ha n páratlan, akkor $D_{2n} \simeq D_n \times D_1$.

3.6. Belső automorfizmus. Konjugáltsági reláció

Legyen $(G, \cdot)$ egy csoport, $i_g : G \to G$, $i_g(x) = gxg^{-1}$, (ahol $g \in G$) és legyen

$$\operatorname{Int}(G) = \{i_g \mid g \in G\}.$$

3.6.1. tétel. a) *Minden* $g \in G$ *esetén* i_g *automorfizmusa* G*-nek, azaz* $\operatorname{Int}(G)$ *részhalmaza* $\operatorname{Aut}(G)$*-nek.*
(i_g-t a g-hez rendelt **belső automorfizmus**nak nevezzük, az $\operatorname{Int}(G)$ halmazt pedig a belső automorfizmusok halmazának.)
b) $\operatorname{Int}(G) \trianglelefteq (\operatorname{Aut}(G), \circ)$.
c) $G/Z(G) \simeq (\operatorname{Int}(G), \circ)$.

Bizonyítás. a) Azonnal belátható, hogy i_g endomorfizmus, és létezik

$$i_g^{-1} : G \to G,\ i_g^{-1}(x) = g^{-1}xg.$$

b) Nyilvánvalóan $i_e = 1_G$, $i_g \circ i_h = i_{gh}$ és $i_g^{-1} = i_{g^{-1}}$ tehát $\operatorname{Int}(G) \le (\operatorname{Aut}(G), \circ)$. Mivel minden $f \in \operatorname{Aut}(G)$ és $i_a \in \operatorname{Int}(G)$ esetén $f \circ i_a \circ f^{-1} = i_{f(a)} \in \operatorname{Int}(G)$, következik, hogy $\operatorname{Int}(G) \trianglelefteq \operatorname{Aut}(G)$.
c) Tekintsük az

$$f : G \to \operatorname{Int}(G),\quad f(a) = i_a$$

függvényt, ahol $i_a : G \to G$, $i_a(x) = axa^{-1}$ a G csoport egy belső automorfizmusa. Könnyen belátható, hogy f szürjektív csoportmorfizmus és

$$\begin{aligned}\operatorname{Ker} f &= \{a \in G \mid i_a = 1_G\} = \\ &= \{a \in G \mid axa^{-1} = x,\ (\forall) x \in G\} = \\ &= \{a \in G \mid ax = xa,\ (\forall) x \in G\} = Z(G).\end{aligned}$$

Alkalmazva az I. izomorfizmustételt következik, hogy $G/Z(G) \simeq \operatorname{Int}(G)$. ■

3.6.2. definíció. 1) Legyen $x, y \in G$. Azt mondjuk, hogy az x **konjugált** y-nal (jelölés: $x \sim y$), ha létezik $g \in G$ úgy, hogy $y = gxg^{-1}$.
2) Ha $x \in G$, akkor a $C_G(x) = \{g \in G \mid gx = xg\}$ halmazt az x *centralizátorának* nevezzük.

3.6.3. tétel. 1) *„$\sim$" ekvivalenciareláció* G*-n, és* $\tilde{x}$*-szel jelöljük az* x *konjugáltsági osztályát:*

$$\tilde{x} = \{y \in G \mid x \sim y\} = \{gxg^{-1} \mid g \in G\}.$$

2) $\tilde{x} = \{x\} \iff x \in Z(G) \iff C_G(x) = G$.
(Ebben az esetben az $\tilde{x}$ osztályt *triviális osztálynak* nevezzük.)
3) $C_G(x)$ *részcsoportja* G*-nek és* $|\tilde{x}| = [G : C_G(x)]$.
4) (**A konjugáltsági osztályokra vonatkozó egyenlőség**)

$$|G| = |Z(G)| + \sum_{a \in A} [G : C_G(a)],$$

ahol $A \subseteq G$ *a nemtriviális osztályok egy teljes reprezentáns rendszere.*

Bizonyítás. 1) Igazoljuk, hogy „$\sim$" ekvivalenciareláció:

Reflexivitás: $x \sim x$ minden $x \in G$ esetén, $x = exe^{-1}$.

Tranzitivitás: $x \sim y$ és $y \sim z$, akkor létezik $g, h \in G$ úgy, hogy $y = gxg^{-1}$ és $z = hyh^{-1}$; következik, hogy $z = hyh^{-1} = h(gxg^{-1})h^{-1} = (hg)x(hg)^{-1}$, tehát $x \sim z$.

Szimmetria: ha $x \sim y$, akkor létezik $g \in G$ úgy, hogy $y = gxg^{-1}$; következik, hogy $g^{-1}y(g^{-1})^{-1} = x$, tehát $y \sim x$.

(„$\sim$" nem kongruenciareláció, azaz nem kompatibilis a művelettel.)

2) $\tilde{x} = \{x\} \Longleftrightarrow \forall g \in G \;\; gxg^{-1} = x \Longleftrightarrow \forall g \in G \;\; xg = gx \Longleftrightarrow x \in Z(G)$.

3) Legyen $x \in G$, és igazoljuk, hogy $C_G(x) \leq G$. $C_G(x) \neq \emptyset$, mert $ex = xe$, tehát $e \in C_G(x)$; ha $g, h \in C_G(x)$, akkor $(gh)x = g(hx) = g(xh) = (gx)h = (xg)h = x(gh)$, tehát $gh \in C_G(x)$; ha $g \in C_G(x)$, akkor $gx = xg$ tehát $xg^{-1} = g^{-1}x$, azaz $g^{-1} \in C_G(x)$.

Igazoljuk, hogy $|\tilde{x}| = [G : C_G(x)]$. Legyen

$$\varphi : G/C_G(x) \longrightarrow \tilde{x}, \;\; \varphi(gC_G(x)) = gxg^{-1}.$$

φ jól értelmezett, mert ha $h \in gC_G(x)$ (azaz $hC_G(x) = gC_G(x)$), akkor $h = gy$, ahol $y \in C_G(x)$ (azaz $xy = yx$); következik, hogy

$$\varphi(hC_G(x)) = hxh^{-1} = (gy)x(gy)^{-1} = gyxy^{-1}g^{-1} = gxg^{-1},$$

mert $yxy^{-1} = x$.

Végül, igazoljuk, hogy φ bijektív. Mivel $\operatorname{Im}\varphi = \{gxg^{-1} \mid g \in G\} = \tilde{x}$, következik, hogy φ szürjektív. Legyen $g, h \in G$ és feltételezzük, hogy $\varphi(gC_G(x)) = \varphi(hC_G(x))$. Értelmezés szerint $gxg^{-1} = hxh^{-1}$, azaz $x(g^{-1}h) = g^{-1}h)x$, tehát $g^{-1}h \in C_G(x)$; következik, hogy $h \in gC_G(x)$, azaz $hC_G(x) = gC_G(x)$, vagyis φ injektív. Mivel φ bijektív következik, hogy $|G/C_G(x)| = |\tilde{x}|$.

4) Mivel $G/\sim = \{\tilde{x} \mid x \in G\}$ G-nek osztályfelbontása, következik, hogy $G = \bigcup_{x \in G} \tilde{x}$ és ha $x \nsim y$, akkor $\tilde{x} \cap \tilde{y} = \emptyset$. Következik, hogy

$$G = Z(G) \cup (\bigcup_{a \in A} \tilde{a}),$$

ahol $Z(G)$ a triviális osztályok egyesítése, és mivel $|\tilde{a}| = [G : C_G(a)]$, következik, hogy

$$|G| = |Z(G)| + \sum_{a \in A} [G : C_G(a)]. \qquad \blacksquare$$

3.51. feladat. Bizonyítsuk be, hogy:

a) $Z(Q) = \{1, -1\}$.

b) $Z(GL_n(K)) = \{aI_n \mid a \in K^*\}$.

c) $Z(UT_3(K)) \simeq (K, +)$ és $UT_3(K)/Z(UT_3(K)) \simeq (K \times K, +)$.

d) $Z(D_n) = \begin{cases} \{e\}, & \text{ha } n \text{ páratlan, } n \geq 3 \\ \{e, x^{n/2}\}, & \text{ha } n \text{ páros, } n \geq 4 \end{cases}$.

3.52. feladat. a) Határozzuk meg a $(Q, \cdot)$ konjugáltsági osztályait.

b) Ha $n = 2k$ páros, akkor a D_n konjugáltsági osztályai

$$\{\{e\}, \{x, x^{n-1}\}, \ldots, \{x^{k-1}, x^{k+1}\}, \{x^k\}, \{y, x^2y, \ldots, x^{n-2}y\}, \{xy, x^3y, \ldots, x^{n-1}y\}\},$$

és ha $n = 2k + 1$ páratlan, akkor a D_n konjugáltsági osztályai

$$\{\{e\}, \{x, x^{n-1}\}, \ldots, \{x^k, x^{k+1}\}, \{y, xy, \ldots, x^{n-1}y\}\}.$$

c) Ha $0 \leq i < n$, akkor:

$$C_{D_n}(x^i) = \begin{cases} \{e, x, \ldots, x^{n-1}\}, & \text{ha } i \neq \frac{n}{2},\ i \neq 0 \\ D_n, & \text{ha } (n \text{ páros, } i = \frac{n}{2}) \text{ vagy } (i = 0) \end{cases}$$

$$C_{D_n}(x^iy) = \begin{cases} \{e, x^{n/2}, x^iy, x^{n-i}y\}, & \text{ha } n \text{ páros, } i \neq 0, \frac{n}{2} \\ \{e, x^{n/2}, y, x^{n/2}y\}, & \text{ha } n \text{ páros, } (i = 0 \text{ vagy } i = \frac{n}{2}) \\ \{e, x^iy\}, & \text{ha } n \text{ páratlan} \end{cases}$$

3.53. feladat. Legyen $(G, \cdot)$ egy csoport és $N \leq G$. Bizonyítsuk be, hogy:

a) Ha $|N| = 2$ és $N \trianglelefteq G$, akkor $N \leq Z(G)$.

b) Ha $N \leq Z(G)$, akkor $N \trianglelefteq G$.

Konjugáltsági reláció S_n-ben

Az alábbi eredmények meghatározzák az $(S_n, \circ)$ szimmetrikus csoport konjugáltsági osztályait.

Megemlítjük hogy $\sigma \in S_n$ **típusa** a $(k_1, \ldots, k_n)$ rendszer, ha a σ diszjunkt ciklusokra való felbontásában szerepel k_1 1-hosszúságú ciklus, k_2 2-hosszúságú ciklus, ..., k_n n-hosszúságú ciklus.

3.6.4. tétel. *Legyen $\sigma, \tau \in S_n$. $\sigma \sim \tau$ akkor és csak akkor, ha σ és τ ugyanolyan típusú.*

Bizonyítás. Legyen $\sigma, \tau \in S_n$ úgy, hogy $\sigma \sim \tau$, és legyen $\sigma = \gamma_1 \circ \ldots \circ \gamma_m$ diszjunkt ciklusok szorzata. Létezik $\rho \in S_n$ úgy, hogy $\tau = \rho \circ \sigma \circ \rho^{-1}$, és mivel

$$\tau = (\rho \circ \gamma_1 \circ \rho^{-1}) \circ (\rho \circ \gamma_2 \circ \rho^{-1}) \circ \ldots \circ (\rho \circ \gamma_m \circ \rho^{-1}),$$

következik, hogy elég igazolni, hogy ha $\gamma = (i_1 \ldots i_l)$ egy l-hosszúságú ciklus, akkor

$$\rho\gamma\rho^{-1} = (\rho(i_1) \ldots \rho(i_l)).$$

Legyen $(\rho(i_1) \ldots \rho(i_l)) = \theta$. Minden $i \in \{1, \ldots, n\}$ esetén

$$\theta(i) = \begin{cases} \rho(i_{k+1}), & \text{ha } i = \rho(i_k), 1 \le k < l \\ \rho(i_k), & \text{ha } i = \rho(i_l) \\ i, & \text{ha } i \ne \{\rho(i_1), \ldots, \rho(i_l)\} \end{cases},$$

$$(\gamma \circ \rho^{-1})(i) = \gamma(\rho^{-1}(i)) = \begin{cases} i_{k+1}, & \text{ha } \rho^{-1}(i) = i_k, 1 \le k < l \\ i_1, & \text{ha } \rho^{-1}(i) = i_l \\ \rho^{-1}(i), & \text{ha } \rho^{-1}(i) \ne \{i_1, \ldots, i_l\}, \end{cases}$$

és végűl

$$\rho(\gamma(\rho^{-1}(i)) = \begin{cases} \rho(i_{k+1}), & \text{ha } i = \rho(i_k), 1 \le k < l \\ \rho(i_1), & \text{ha } i = \rho(i_l) \\ i, & \text{ha } i \ne \{\rho(i_1), \ldots, \rho(i_n)\} \end{cases} = \theta(i)$$

Mivel ρ bijektív következik, hogy $\tau = (\rho \circ \gamma_1 \circ \rho^{-1}) \circ (\rho \circ \gamma_2 \circ \rho^{-1}) \circ \ldots \circ (\rho \circ \gamma_m \circ \rho^{-1})$ diszjunkt ciklusok szorzata, tehát σ és τ azonos típusúak.

Fordítva, legyenek

$$\theta = (i_{11} i_{12} \ldots i_{1l_1})(i_{21} i_{22} \ldots i_{2l_2}) \ldots (i_{m1} i_{m2} \ldots i_{ml_m})$$

és

$$\tau = (j_{11} j_{12} \ldots j_{1l_1})(j_{21} j_{22} \ldots j_{2l_2}) \ldots (j_{m1} j_{m2} \ldots j_{ml_m})$$

azonos típusú permutációk, ahol $l_1 + l_2 + \ldots + l_m = n$ és

$$\{i_{11}, \ldots, i_{ml_m}\} = \{j_{11}, \ldots, j_{ml_m}\} = \{1, \ldots, n\}.$$

Továbbá, legyen

$$\rho = \begin{pmatrix} i_{11} & \ldots & i_{1l_1} & i_{21} & \ldots & i_{2l_2} & \ldots & i_{m1} & \ldots & i_{ml_m} \\ j_{11} & \ldots & j_{1l_1} & j_{21} & \ldots & j_{2l_2} & \ldots & j_{m1} & \ldots & j_{ml_m} \end{pmatrix},$$

$\rho\sigma\rho^{-1} = \theta$, és igazoljuk, hogy $\tau = \rho\sigma\rho^{-1}$. Valóban, ha $1 \le r \le m$ és $1 \le s \le l_r$, akkor

$$\sigma(i_{rs}) = \begin{cases} i_{r,s+1}, & \text{ha } 1 \le s < l_r \\ i_{r1}, & \text{ha } s = l_r \end{cases},$$

és

$$\theta(j_{rs}) = \rho(\sigma(\rho^{-1}(j_{rs}))) = \rho(\sigma(i_{rs})) = \begin{cases} j_{r,s+1}, & \text{ha } 1 \le s < l_r \\ j_{r1}, & \text{has} = l_r \end{cases}$$

következik, hogy $\theta(j_{rs}) = \tau(j_{rs})$, minden $1 \le r \le m$ és $1 \le s \le l_r$ esetén, tehát $\theta = \tau$. ■

3.54. feladat. Bizonyítsuk be, hogy:

a) $Z(S_n) = \{e\}$, ha $n \ge 3$, és $Z(A_n) = \{e\}$, ha $n \ge 4$.

b) Határozzuk meg az $(S_n, \circ)$ konjugáltsági osztályait, ahol $n = 1, 2, 3, 4$.

3.7. Struktúratételek: p-, 2p- és p^2-ed rendű csoportok

A következő tételt az 3.4. paragrafusban bizonyítottuk.

3.7.1. tétel. (A p-ed rendű csoportok osztályozása) *Ha* $(G, \cdot)$ *egy csoport,* p *egy prím- szám és* $|G| = p$*, akkor* $G \simeq (\mathbb{Z}_p, +)$.

Az alábbiakban egy lépessel tovább megyünk és a $2p$ és p^2 rendű csoportoka fogjuk osztályozni.

3.7.2. lemma. *Ha minden* $x \in G$ *esetén* $\mathrm{ord}(x) = 2$*, akkor* G *kommutatív csoport. Ha* G *véges, akkor létezik* $n \in \mathbb{N}^*$ *úgy, hogy* $|G| = 2^n$.

Bizonyítás. Minden $x, y \in G$ esetén $e = xxyy = xyxy$, tehát $xy = yx$.

Matematikai indukciót alkalmazunk. Ha $G = \{e\}$, akkor $|G| = 2^0$. Legyen $|G| = m > 1$ és feltételezzük, hogy az állítás igaz az m-nél kisebb rendű csoportok esetén. Ha $x \in G \setminus \{e\}$, akkor $\langle x \rangle = \{e, x\} \trianglelefteq G$, $|G/\langle x \rangle| = m/2$ és $(\forall) y \in G$ $(y\langle x \rangle)^2 = \langle x \rangle$; következik, hogy $(\exists) n \in \mathbb{N}$ úgy, hogy $m/2 = 2^n$, tehát $|G| = 2^{n+1}$. ■

3.7.3. tétel. (A 2p-ed rendű csoportok osztályozása) *Ha* $(G, \cdot)$ *egy csoport,* p *egy prím szám és* $|G| = 2p$*, akkor* $G \simeq (\mathbb{Z}_{2p}, +)$ *vagy* $G \simeq (D_p, \cdot)$*, ahol*

$$D_p = \langle x, y \mid x^p = y^2 = e,\ yx = x^{p-1}y \rangle = \{x^i y^j \mid 0 \le i < p,\ 0 \le j < 2\}$$

a p*-ed fokú diédercsoport.*

Bizonyítás. Ha $x \in G$, akkor a Lagrange-tételből következik, hogy $\mathrm{ord}(x)$ osztja a $|G| = 2p$ számot, tehát $\mathrm{ord}(x) \in \{1, 2, p, 2p\}$.

Ha létezik $x \in G$ úgy, hogy $\mathrm{ord}(x) = 2p$, akkor, mivel $|\langle x \rangle| = \mathrm{ord}(x) = 2p, \langle x \rangle \le G$ és $|G| = 2p$ következik, hogy $G = \langle x \rangle$, azaz $G \simeq (\mathbb{Z}_{2p}, +)$.

Feltételezzük, hogy $\mathrm{ord}(x) \ne 2p$ minden $x \in G$ esetén.

Ha $x^2 = e$ minden $x \in G$ esetén, akkor a 3.7.2.-ből következik, hogy G kommutatív és $|G| = 2^n$, azaz $2^n = 2p$, vagyis $p = 2$, tehát $|G| = 4$. Ebben az esetben, ha $y \in G \setminus \{e, x\}$, akkor

$$G = \{e, x, y, xy\} \simeq D_2.$$

Feltételezzük, hogy $p > 2$ és létezik $x \in G$ úgy, hogy $\mathrm{ord}(x) = p$. Legyen

$$N = \langle x \rangle = \{e, x, \ldots, x^{p-1}\}.$$

Alkalmazzuk a Lagrange-tételt és kapjuk, hogy $2p = |G| = |N| \cdot [G : N]$, azaz $[G : N] = 2$, tehát $N \trianglelefteq G$. Mivel $[G : N] = 2$ következik, hogy $G/N = \{N, yN\} = \{N, Ny\}$.

Legyen $y \in G \setminus N$, és vegyük észre, hogy $(yN)^2 = N$, mert G/N másodrendű csoport. Mivel p páratlan következik, hogy $(yN)^p = yN \ne N$, azaz $(yN)^p = y^pN \ne N$, tehát $y^p \ne N$; következik, hogy $y^p \ne e$, ezért $\mathrm{ord}(y) = 2$.

Mivel $G = N \cup Ny$ és $N \cap Ny = \emptyset$, tehát

$$G = \{e, x, x^2, \ldots, x^{p-1}, y, xy, x^2y, \ldots, x^{p-1}y\}.$$

Mivel $yx \in yN = Ny$ következik, hogy létezik $k \in \{1, \ldots, p-1\}$ úgy, hogy $yx = x^ky$. Ekkor $e = (yx)^2 = (yx)(yx) = (x^ky)(yx) = x^{k+1}$, ahol $k + 1 \le p$. Mivel $\mathrm{ord}(x) = p$ következik, hogy $k + 1 = p$, vagyis $yx = x^{p-1}y$, tehát $G \simeq D_p$. ■

3.7.4. megjegyzés. $(\mathbb{Z}_{2p}, +) \not\simeq (D_p, \cdot)$, mert $\mathbb{Z}_{2p}$ tartalmaz $2p$-ed rendű elemet és minden $g \in D_{2p}$ esetén $\mathrm{ord}(g) < 2p$.

3.7.5. lemma. *Ha* G p*-csoport* (azaz $|G| = p^n$, ahol $n > 0$)*, akkor* $Z(G) \ne \{e\}$.

Bizonyítás. Alkalmazzuk a konjugáltsági osztályokra vonatkozó egyenlőséget:

$$|G| = |Z(G)| + \sum_{x \in A} [G : C_G(x)],$$

ahol A a nemtriviális osztályoknak egy teljes reprezentáns rendszere, $C_G(x) = \{g \in G \mid gx = xg\} \le G$ az x elem centralizátora és $|\tilde{x}| = [G : C_G(x)]$.

Mivel $|G| = p^n, n > 0$ és $[G : C_G(x)] > 1$ (mert x osztálya nem triviális) Lagrange tételéből következik, hogy

$$[G : C_G(x)] = p^n / |C_G(x)|,$$

azaz p osztja $|Z(G)|$-t, vagyis $|Z(G)| > 1$. ■

3.7.6. lemma. *Ha* $G/Z(G)$ *ciklikus csoport, akkor* G *kommutatív.*

Bizonyítás. Feltételezzük, hogy $G/Z(G) = \langle xZ(G)\rangle$, tehát $G = \bigcup_{k\in\mathbb{Z}} x^k Z(G)$. Ha $y, z \in G$, akkor $y = x^k g$, $z = x^l h$, ahol $k, l \in \mathbb{Z}$, $g, h \in \mathbb{Z}(G)$; innen következik, hogy $yz = x^{k+l}gh = zy$. ■

3.7.7. tétel (A p^2-ed rendű csoportok osztályozása). *Ha* $(G, \cdot)$ *egy csoport,* p *egy prím szám és* $|G| = p^2$, *akkor* $G \simeq (\mathbb{Z}_{p^2}, +)$ *vagy* $G \simeq (\mathbb{Z}_p \times \mathbb{Z}_p, +)$.

Bizonyítás. Igazoljuk, hogy G kommutatív csoport.

A 8.5.-ből következik, hogy $Z(G) \neq \{e\}$, de $|G| = |Z(G)| \cdot [G : Z(G)]$, ezért $|Z(G)| = p^2$ vagy $|Z(G)| = p$.

Ha $|Z(G)| = p^2 = |G|$, akkor $Z(G) = G$, azaz G kommutatív.

Ha $|Z(G)| = p$, akkor $|G/Z(G)| = p^2/p = p$. 3.7.1.-ből következik, hogy $G/Z(G)$ ciklikus, ezért a 3.7.6. lemma szerint G kommutatív, azaz $G = Z(G)$; következik, hogy $|Z(G)| = p^2$ ami ellentmond a feltevésnek.

Ha $x \in G \setminus \{e\}$, akkor $\mathrm{ord}(x) \in \{p, p^2\}$. Ha létezik $x \in G$ úgy, hogy $\mathrm{ord}(x) = p^2$, akkor $|\langle x\rangle| = |G| = p^2$, azaz $G = \langle x\rangle$ ciklikus és $G \simeq (\mathbb{Z}_{p^2}, +)$.

Ellenkező esetben, $\mathrm{ord}(x) = p$ minden $x \in G \setminus \{e\}$. Rögzítünk egy $x \neq e$ elemet és legyen

$$H = \langle x\rangle = \{e, x, \ldots, x^{p-1}\} \simeq (\mathbb{Z}_p, +).$$

Legyen $y \in G \setminus H$, tehát $\mathrm{ord}(y) = p$, és legyen

$$K = \langle y\rangle = \{e, y, \ldots, y^{p-1}\} \simeq (\mathbb{Z}_p, +).$$

Igazoljuk, hogy $H \cap K = \{e\}$. Feltételezzük, hogy létezik k, l úgy, hogy $1 \leq k, l < p$ és $x^k = y^l$. Mivel $(l, p) = 1$ következik, hogy létezik $u, v \in \mathbb{Z}$ úgy, hogy $1 = lu + pv$; ekkor $y = y^1 = y^{lu+pv} = (y^l)^u \cdot (y^p)^v = x^{ku} \in \langle x\rangle = H$ ami ellentmond a feltevésnek.

Legyen $f : H \times K \to G$, $f((h, k)) = hk$. Mivel G kommutatív következik, hogy f morfizmus. Továbbá, a 3.5.3. tétel szerint f injektív, mert $H \cap K = \{e\}$ és szürjektív, mert $|H \times K| = p^2 = |G|$. Következik, hogy

$$G \simeq H \times K \simeq (\mathbb{Z}_p \times \mathbb{Z}_p, +). \qquad ■$$

3.7.8. megjegyzés. $(\mathbb{Z}_{p^2}, +) \not\simeq (\mathbb{Z}_p \times \mathbb{Z}_p, +)$, mert $\mathbb{Z}_{p^2}$ tartalmaz p^2-ed rendű elemet és minden $g = (\hat{a}, \hat{b}) \in \mathbb{Z}_p \times \mathbb{Z}_p$ esetén $\mathrm{ord}(g) \mid p$, mert $pg = (\hat{0}, \hat{0})$.

3.55. feladat. Határozzuk meg a $(Z_p \times \mathbb{Z}_p, +)$ részcsoportjait. Igazoljuk, hogy a részcsoportok száma $p + 3$.

3.56. feladat. a) Határozzuk meg a $(Z_p \times \mathbb{Z}_p, +)$ automorfizmusait.

b) Igazoljuk, hogy $(\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2, +), \circ) \simeq (S_3, \circ)$.

3.57. feladat (D_n részcsoportjai). a) Igazoljuk, hogy minden $n \geq 3$ esetén

$$\mathcal{S}(D_n) = \{\langle x^d\rangle\langle x^i y\rangle, \langle x^d, x^i y\rangle \mid 0 \leq i < d,\ d|n\}.$$

b) Bármely $H \leq D_n$ esetén, határozzuk meg a H rendjét és indexét.

c) Igazoljuk, hogy

$$\mathcal{S}_n(D_n) = \{\langle x^d\rangle \mid 0 < d \leq n,\ d|n\},$$

ha n páratlan, és

$$\mathcal{S}_n(D_n) = \{\langle x^d\rangle, \langle x^2, x^i y\rangle \mid i = 0, 1\},$$

ha $n = 2m$ páros. Bármely $N \trianglelefteq D_n$ esetén, határozzuk meg a D_n/N faktorcsoportot.

3.58. feladat (D_n automorfizmusai). a) Legyen $n \geq 3$, $0 \leq l, m < n$, $(l, n) = 1$ és

$$f_{m,l} : D_n \to D_n, \quad f_{m,l}(x^i) = x^{li}, \quad f_{m,l}(x^j y) = x^{lj+m} y.$$

Igazoljuk, hogy $f_{m,l} \in \mathrm{Aut}(D_n)$.

b) A $\mathbb{Z}_n \times \mathbb{Z}_n^*$ halmazon értelmezzük a $(v, u)(m, l) = (um + v, ul)$ műveletet. Igazoljuk, hogy $\mathbb{Z}_n \times \mathbb{Z}_n^*$ csoport.

c) Legyen $\phi : (\mathbb{Z}_n \times \mathbb{Z}_n^*, \cdot) \to (\mathrm{Aut}(D_n), \circ)$, $\phi(m, l) = f_{m,l}$. Bizonyítsuk be, hogy ϕ izomorfizmus.

3.8. Karakterisztikus és teljesen invariáns részcsoportok

3.8.1. definíció. Legyen G egy csoport és H részcsoportja G-nek.

a) H-t **karakterisztikus részcsoport**nak nevezzük, ha minden $f \in \mathrm{Aut}(G)$ esetén $f(H) \subseteq H$.

Jelölés: $H \leq_c G$.

b) H-t **teljesen invariáns** vagy **teljesen karakterisztikus** részcsoportnak nevezzük, ha minden $f \in \mathrm{End}(G)$ esetén $f(H) \subseteq H$.

Jelölés: $H \leq_t G$.

3.8.2. megjegyzés. a) Mivel $\mathrm{Int}(G) \subseteq \mathrm{Aut}(G) \subseteq \mathrm{End}(G)$, $H \leq_t G \Rightarrow H \leq_c G \Rightarrow H \trianglelefteq G$.

b) A $H \leq G$ részcsoport karakterisztikus akkor és csak akkor, ha minden $f \in \mathrm{Aut}(G)$ esetén $f(H) = H$.

Valóban, abból, hogy $f(H) \subseteq H$ $\forall f \in \mathrm{Aut}(G)$ következik, hogy $H \subseteq f^{-1}(H)$ $\forall f \in \mathrm{Aut}(G)$. De $f^{-1} \in \mathrm{Aut}(G)$, tehát $H \subseteq (f^{-1})^{-1}(H) = f(H)$.

c) Legyen $H_1 \leq H_2 \leq G$ részcsoportjai G-nek. Ha $H_1 \leq_c H_2$ és $H_2 \leq_c G$, akkor $H_1 \leq_c G$.

Valóban, mivel $H_2 \leq_c G$, akkor a G-n értelmezett automorfizmus leszukítése H_2-re szintén automorfizmus.

d) Legyenek $H_1 \leq H_2$ részcsoportjai G-nek. Ha $H_1 \leq_c G$ és $H_2 \trianglelefteq G$, akkor $H_1 \trianglelefteq G$.

e) Legyen G egy csoport és $H_1 \leq H_2 \leq G$-nek. Ha $H_1 \leq_t H_2$ és $H_2 \leq_t G$, akkor $H_1 \leq_t G$.

Valóban, mivel $H_2 \leq_t G$, G-n értelmezett endomorfizmus leszukítése H_2-re endomorfizmusa H_2-nek.

3.8.3. tétel. *Egy csoport centruma karakterisztikus részcsoport.*

Bizonyítás. Tudjuk, hogy $Z(G)$ részcsoportja G-nek. Legyen $f \in \mathrm{Aut}(G)$. Ha $g \in G$, akkor létezik $g' \in G$ melyre $f(g') = g$. Tehát minden $x \in Z(G)$ esetén $f(x)g = f(x)f(g') = f(xg') = f(g'x) = f(g')f(x) = gf(x)$. Következik hogy $f(x) \in Z(G)$ vagyis $f(Z(G)) \subseteq Z(G)$.

Ahhoz, hogy példát tudjunk adni teljesen invariáns részcsoportra, egy új fogalmat kell bevezetnünk.

3.8.1. Kommutátorok. A derivált részcsoport

3.8.4. definíció. Legyen G egy csoport, $x, y \in G$, $X, Y \subseteq G$.

a) Az $[x, y] = x^{-1}y^{-1}xy$ elemet az (x, y) elempár *kommutátor*ának nevezzük. (Vegyük észre, hogy egy kommutátor inverze szintén kommutátor: $[x, y]^{-1} = [y, x]$.)

b) $[X, Y]$-al jelöljük az $[x, y]$ kommutátorok által generált réscsoportot, ahol $x \in X$ és $y \in Y$ vagyis

$$\begin{aligned}[X, Y] &= \langle\{[x, y] \mid x \in X,\ y \in Y\}\rangle \\ &= \{[a_1, b_1][a_2, b_2]\dots[a_n, b_n] \mid (a_i, b_i) \in X \times Y \ \text{ vagy } (a_i, b_i) \in Y \times X\}.\end{aligned}$$

Ezt a részcsoportot az X és Y halmazok kommutátorának nevezzük.

c) G'-et a G **kommutator részcsoport**jának vagy **derivált részcsoport**jának nevezzük, ahol

$$G' := [G, G] = \langle\{[x, y] \mid x, y \in G\}\rangle = \{[x_1, y_1][x_2, y_2]\dots[x_n, y_n] \mid a_i, b_i \in G,\ n \in \mathbb{N}\}.$$

3.8.5. megjegyzés. a) $xy = yx[x, y]$, tehát ha $xy = yx$, akkor $[x, y] = e$. A G csoport akkor és csak akkor kommutativ, ha $\forall x, y \in G$ $[x, y] = 1$, vagyis ha $[G, G] = \{e\}$.

b) Ha $X_1 \subseteq X_2$ és $Y_1 \subseteq Y_2$, akkor $[X_1, Y_1] \leq [X_2, Y_2]$, ahol $X_i, Y_i \subseteq G$, $i = 1, 2$.

3.8.6. tétel. 1) *Legyen* $N \leq G$. *Akkor* N *normális részcsoport* $\Leftrightarrow$ $[N, G] \subseteq N$.

2) *Ha* $N_1 \trianglelefteq G$ *és* $N_2 \trianglelefteq G$, *akkor* $[N_1, N_2] \leq N_1 \cap N_2$.

Bizonyítás. 1) Ha $N \trianglelefteq G$, akkor $\forall n \in N$, $\forall g \in G$ esetén $g^{-1}ng \in N \Rightarrow [n, g] = n^{-1}(g^{-1}ng) \in N$, azaz $[N, G] \subseteq N$.

Fordítva feltételezzük, hogy $[N, G] \subseteq N$. Minden $n \in N$, $g \in G$ esetén $n^{-1}g^{-1}ng \in N$-ből következik, hogy $g^{-1}ng \in N$, tehát $N \trianglelefteq G$.

2) $[N_1, N_2] \leq [N_1, G] \leq N_1$ és $[N_1, N_2] \leq [G, N_2] \leq N_2]$. ■

3.8.7. tétel. 1) *Ha* $f : G \to G'$ *egy morfizmus,* $x_i \in G$, $X_i \subseteq G$, $i = 1, 2$, *akkor*

$$f([x_1, x_2]) = [f(x_1), f(x_2)], \qquad f([X_1, X_2]) = [f(X_1), f(X_2)].$$

2) *Ha* H *teljesen invariáns részcsoportja* G*-nek, akkor* $[H, H]$ *teljesen invariáns részcsoport. Partikulárisan,* $G'[G, G]$ *teljesen invariáns részcsoport.*

3) *Ha* $N_1 \trianglelefteq G$ *és* $N_2 \trianglelefteq G$, *akkor* $[N_1, N_2] \trianglelefteq G$.

4) *Legyen* $\{G_i \mid i = 1, \dots, n\}$ *egy csoportrendszer és legyenek* H_i, H_i' *részcsoportjai* G_i*-nek. Akkor* $H := \prod_{i=1}^n H_i$, $H' := \prod_{i=1}^n H_i'$ *részcsoportjai* $\prod_{i=1}^n G_i$*-nek, és* $[H, H'] = \prod_{i=1}^n [H_i, H_i']$.

Bizonyítás. a) $f([x_1, x_2]) = f(x_1^{-1}x_2^{-1}x_1x_2) = (f(x_1))^{-1}(f(x2))^{-1}f(x_1)f(x_2) = [f(x_1), f(x_2)]$.

Tudjuk, hogy ha $X \subseteq G$, akkor $f(\langle X\rangle) = \langle f(X)\rangle$. Következik, hogy $f([X_1, X_2]) = \langle\{f([x_1, x_2]) \mid x_1 \in X_1,\ x_2 \in X_2\}\rangle = \langle\{[f(x_1), f(x_2)] \mid x_1 \in X_1,\ x_2 \in X_2\}\rangle = [f(X_1), f(X_2)]$.

b) következik a)-ból.

c) Ha $g \in G$ és $i_g : G \to G$ egy belso automorfizmus, akkor $i_g([N_1, N_2]) = [i_g(N_1), i_g(N_2)] = [N_1, N_2]$. Tehát $[N_1, N_2] \trianglelefteq G$.

d)-t az olvasóra bizzuk. ■

3.8.8. tétel. *Legyen* G *egy csoport,* $N \leq H \leq G$ *és* $N \trianglelefteq G$. *Ekkor* $H/N \leq Z(G/N) \Leftrightarrow [H, G] \leq N$.

Bizonyítás. Ha $H/N \leq Z(G/N)$, akkor $\forall h \in H$, $\forall g \in G$ $hNgN = gNhN$, tehát $[h, g]N = h^{-1}g^{-1}hgN = h^{-1}Ng^{-1}NhNgN = N$. Tehát $[h, g] \in N$ azaz $[H, G] \leq N$.

Fordítva, $[h, g]N = N \Rightarrow h^{-1}Ng^{-1}NhNgN = N$, vagyis $hNgN = gNhN$ $\forall h \in H$, $\forall g \in G$; következik, hogy $H/N \leq Z(G/N)$. ■

3.8.9. tétel. *Legyen* $H \leq G$. *Ha* $G' \leq H$, *akkor* $H \trianglelefteq G$ *és* G/H *Abel-csoport. Fordítva, ha* $H \trianglelefteq G$ *és* G/H *Abel-csoport, akkor* $G' \leq H$ *(azaz* G' *a legkisebb normális részcsoport amelyre* G/H *Abel-csoport).*

Bizonyítás. Feltételezzük, hogy $G' \leq H$. Ekkor $[H, G] \leq [G, G] = G' \leq H$. Innen következik, hogy $H \trianglelefteq G$. Továbbá $\forall x, y \in G$, $[xH, yH] = x^{-1}Hy^{-1}HxHyH = x^{-1}y^{-1}xyH = [x, y]H = H$, mivel $[x, y] \in H$. Tehát az (xH, yH) elempár kommutátora semleges elem G/H-ban, következésképpen G/H Abel-csoport.

Fordítva, feltételezzük, hogy $H \trianglelefteq G$ és G/H Abel-csoport. Akkor minden $x, y \in G$ esetén $[xH, yH] = H$, tehát $[x, y]H = H$, azaz $[x, y] \in H$ és $G' \leq H$. ■

3.59. feladat. Legyen G egy Abel-csoport, p egy prím szám, és $T_p(G) := \{g \in G \mid \exists k \in \mathbb{N} :\ \mathrm{ord}(g) = p^k\}$. Igazoljuk, hogy $T_p(G)$ teljesen invaráns részcsoportja G-nek.

Útmutatás: Ha $g \in G$ és $f \in \mathrm{End}(G)$, akkor az $f(g)$ rendje osztja a g rendjét.

3.60. feladat. Legyen $(A, +)$ egy Abel-csoport, B részcsoportja A-nak, $n \in \mathbb{N}^*$ és $nB := \{nb \mid b \in B\}$, $B[n] := \{b \in B \mid nb = 0\}$.

a) Mutassuk meg, hogy nB és $B[n]$ részcsoportjai A-nak.

b) Ha B karakterisztikus részcsoport, akkor nB és $B[n]$ is karakterisztikus részcsoportok.

c) Ha B teljesen invariáns részcsoport akkor nB és $B[n]$ is teljesen invariáns részcsoportok.

3.61. feladat. Legyen $A = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$, $C = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix} \in GL_n(\mathbb{Z})$. Számítsuk ki az $[A, B]$, $[B, C]$, $[C, A]$ kommutátorokat.

3.62. feladat. Igazoljuk, hogy az S_n szimmetrikus csoportban:

a) $(i\ j\ k) = (i\ k)(i\ j) = [(i\ j), (i\ k)]$, ha $n \geq 3$;

b) $(i\ j)(k\ l) = (i\ k\ j)(i\ k\ l) = [(i\ j\ k), (i\ j\ l)]$, ha $n \geq 4$;

c) $(i\ j\ k) = [(i\ l\ j), (i\ m\ k)]$, ha $n \geq 5$.

3.63. feladat. Tekintsük a $D_n = \langle x, y \mid x^n = y^2 = e,\ yx = x^{n-1}y\rangle$ diédercsoportot. Igazoljuk, hogy:

a) $[x^k y^l, x^m y^j] = \begin{cases} e, & \text{ha } l = j = 0 \\ x^{2i}, & \text{ha } l = 1,\ j = 0 \\ x^{-2k}, & \text{ha } l = 0,\ j = 1 \\ x^{2(k-i)}, & \text{ha } l = j = 1 \end{cases}$

b) $D_n' = \begin{cases} \langle x\rangle = \{e, x, \ldots, x^{n-1}\}, & \text{ha } n \text{ páratlan} \\ \langle x^2\rangle = \{e, x^2, \ldots, x^{2n-2}\}, & \text{ha } n \text{ páros} \end{cases}$

c) $D_n/D_n' = \begin{cases} \{\langle x\rangle, y\langle x\rangle\} \simeq C_2, & \text{ha } n \text{ páratlan} \\ \{\langle x^2\rangle, \langle x^2\rangle, y\langle x^2\rangle, xy\langle x^2\rangle\} \simeq C_2 \times C_2, & \text{pentru } n \text{ páros} \end{cases}$.

3.64. feladat. Egy tetszőleges G csoportban legyen $x^y = y^{-1}xy$ és $[x, y, z] = [[x, y], z]$. Igazoljuk, hogy:

a) $[x, y^{-1}] = y[y, x]y^{-1}$; $[x^{-1}, y] = x[y, x]x^{-1}$;

b) $[xy, z] = [x, z]^y[y, z]$; $[x, yz] = [x, z][x, y]^z$.

c) $[x, y^{-1}, z]^y[z, z^{-1}, x]^z[z, x^{-1}, y]^x = e$ **(Hall–Witt-azonosság)**.

3.65. feladat. Mutassuk ki, hogy ha $[G, G] \leq Z(G)$, akkor minden $x, y, z \in G$ esetén:

a) $[x, [y, z]] = [[x, y], z]$;

b) $[xy, z] = [x, z][y, z]$; $[x, yz] = [x, y][x, z]$;

c) $[x^n, y] = [x, y^n] = [x, y]^n$ $\forall n \in \mathbb{N}$;

d) $(xy)^n = x^n y^n [y, x]^{n(n-1)/2}$ $\forall n \in \mathbb{N}^*$;

e) $[x, [y, z]][y, [z, x]][z, [x, y]] = 1$.

3.66. feladat. Mutassuk meg, hogy ha H és K karakterisztikus részcsoportjai G-nek, akkor $[H, K]$ szintén karakterisztikus részcsoport.

3.67. feladat. Mutassuk meg, hogy $[D_n, D_n]$ n-ed rendű, illetve $n/2$-ed rendű ciklikus csoport attól függően, hogy n páratlan vagy páros.

3.68. feladat. Legyen G egy csoport, $G^{ab} := G/G'$, és legyen $(A, +)$ egy Abel-csoport.
a) Ha $f\ G \to A$ egy morfizmus, akkor $G' \subseteq \operatorname{Ker} f$.
b) $(\operatorname{Hom}(G, A), +) \simeq (\operatorname{Hom}(G^{ab}, A), +)$.

3.69. feladat. Legyen G egy csoport, $X \subseteq G$ egy generátorrendszer, és $N \trianglelefteq G$. Mutassuk ki, hogy ha $[x, y] \in N$ $\forall x, y \in X$, akkor $[G, G] \leq N$.

3.70. feladat. Legyen $G \subset GL_3(\mathbb{Z})$, $G = \left\{ \begin{pmatrix} 1 & a & b \\ 0 & 1 & c \\ 0 & 0 & 1 \end{pmatrix} \mid a, b, c \in \mathbb{Z} \right\}$. Igazoljuk, hogy:
a) $G \leq GL_3(\mathbb{Z})$;
b) $[G, G] = Z(G)$.

3.71. feladat. Legyen $\Phi(G) := \bigcap\{M \mid M < G$ maximális részcsoport$\}$ a G csoport **Frattini-részcsoportja**. Igazoljuk, hogy:
a) $\Phi(G) = \{g \in G \mid \forall\ X \subseteq G \ \ \langle X \cup \{g\}\rangle = G \Rightarrow \langle X\rangle = G\}$ (a nem-generáló elemek halmaza).
b) $\Phi(G)$ karakterisztikus részcsoportja G-nek.

3.72. feladat. Egy G csoportot *karakterisztikus egyszerű* csoportnak nevezünk, ha $G \neq \{e\}$, és G-nek nincs valódi karakterisztikus részcsoportja. Igazoljuk, hogy:
a) Egy G csoport bármely főfaktora egyszerű karakterisztikus csoport. (G-nek egy *főfaktora* H/K alakú ahol H és K normális részcsoportjai G-nek, $K \leq H$ és H/K minimális normális részcsoportja G/K-nak.)
b) Egy nem triviális véges G Abel-csoport karakterisztikus egyszerű csoport akkor, és csak akkor, ha G elementáris Abel-csoport.

Megoldás. a) Feltételezhetjük, hogy $K = \{e\}$, vagyis H a minimális normális részcsoportja G-nek. Ekkor bármely H' karakterisztikus részcsoportja H-nak, G-nek normális részcsoportja. Mivel H minimális normális részcsoportja G-nek következik, hogy $H' = 1$, vagyis $H' = H$.

b) Feltételezzük, hogy G egyszerű Abel csoport és legyen p a G rendjének egy prím osztója. Legyen $H = \{x \in G \mid x^p = 1\}$. Mivel G Abel csoport következik, hogy $\forall x, y \in H$ $(xy)^p = x^p y^p = 1$, tehát $xy \in H$. Ez azt mutatja, hogy H részcsoportja G-nek. Cauchy-tétel szerint létezik olyan $x \in G$ amelynek rendje p. Ekkor $1 \neq x \in H$ tehát H nem triviális részcsoport. Hasonlóan H karakterisztikus részcsoportja G-nek mert $\sigma \in \operatorname{Aut}(G)$ esetén:

$$x \in H \Rightarrow x^p = 1 \Rightarrow \sigma(x)^p = \sigma(x^p) = 1 \Rightarrow \sigma(x) \in H.$$

Következik, hogy $H = G$, tehát $x^p = 1$ $\forall x \in G$.

Fordítva, feltételezzük, hogy G elementáris Abel-csoport és legyen p egy prímszám úgy, hogy $x^p = 1$ $\forall x \in G$. Tételezzük fel, hogy $|G| = p^d$, és legyen $x_1 \in G$, $x_1 \neq 1$. Válasszunk egy $x_2 \in G$-t, úgy, hogy $x_2 \notin \langle x_1\rangle$, egy $x_3 \in G$-t úgy, hogy $x_3 \notin \langle x_1, x_2\rangle$ ... stb. Mivel G véges, létezik egy $n \geq 1$ természetes szám úgy, hogy $\langle x_1, x_2, \ldots, x_n\rangle = G$ és $x_{i+1} \notin \langle x_1, x_2, \ldots, x_i\rangle$ bármely $i \in \{1, 2, \ldots, n-1\}$ esetén. Ekkor $\{x_1, x_2, \ldots, x_n\}$ G-nek egy minimális generátorrendszere. Valóban, $x_n \notin \langle x_1, x_2, \ldots, x_n\rangle$, és bebizonyítható, hogy $x_1 \notin \langle x_2, x_3, \ldots, x_n\rangle$, $x_2 \notin \langle x_1, x_3, \ldots, x_n\rangle$ stb. Például feltételezzük, hogy $x_1 \in \langle x_2, x_3, \ldots, x_n\rangle$. Ekkor $x_1 = x_2^{a_2} \ldots x_n^{a_n}$ ahol $a_2, a_3, \ldots, a_n \in \mathbb{Z}$. Ha $p \mid a_n$, akkor $x_n^{a_n} = 1$. Így feltételezhetjük, hogy $x_1 = x_2^{a_2} \ldots x_k^{a_k}$, $k \leq n$ és $p \nmid a_k$. Ekkor $x_k^{a_k} \in \langle x_1, x_2, \ldots, x_k\rangle$; mivel p nem osztja a_k-t, következik, hogy $\langle x_k\rangle = \langle x_k^{a_k}\rangle \leq \langle x_1, x_2, \ldots, x_{k-1}\rangle$, tehát $x_k \in \langle x_1, x_2, \ldots, x_{k-1}\rangle$, ami ellentmond az x_k választásának. Mivel $\{x_1, x2, \ldots, x_n\}$ minimális generátorrendszer, következik, hogy $n = d$.

Tételezzük fel, hogy H a G csoport valódi részcsoportja. Válasszuk meg $x_1 \in H$, $x_1 \neq 1$ és $y_1 \notin H$. A fentiek alapján léteznek $x_1, x_2, \ldots, x_d, y_2, y_3, \ldots, y_d \in G$ úgy, hogy $\{x_1, x_2, \ldots, x_d\}$és $\{y_1, y_2, \ldots, y_d\}$ minimális generátorrendszerek G-ben. Következik, hogy létezik $\sigma : G \to G$, $\sigma(x_1^{r_1}, x_2^{r_2}, \ldots, x_d^{r_d} = y_1^{r_1}, y_2^{r_2}, \ldots, y_d^{r_d}$ $\forall r_1, \ldots r_n \in \mathbb{Z}$, $0 \leq r_i \leq p$, $\forall i \in \{1, 2, \ldots, d\}$. Akkor σ automorfizmusa G-nek. Mivel $x_1 \in H$ és $\sigma(x_1) = y_1 \notin H$, következik, hogy H nem karakterisztikus részcsoportja G-nek. Tehát G karakterisztikus egyszerű csoport.

3.9. Csoportok láncai

3.9.1. definíció. Legyen G egy csoport, $L = (H_0, H_1, \ldots, H_n)$ egy részcsoport rendszer. Ezt a rendszert **lánc**nak nevezzük, ha

$$\{e\} = H_n \leq H_{n-1} \leq \cdots \leq H_1 \leq H_0 = G.$$

Ha a sorozat szigorúan csökkenő, akkor n a lánc **hossza**.

Legyen L egy lánc. Azt mondjuk, hogy:

- L **szubnormállánc**, ha $H_i \trianglelefteq H_{i-1}$, $0 \le i \le n$. Ekkor H_i/H_{i-1} az L **faktorai**.
- L **Abel-lánc**, ha a faktorai Abel-csoportok.
- L **normállánc**, ha $H_i \trianglelefteq G$ minden $i \in \{1, 2, \dots, n\}$ esetén. A *triviális* $\{e\} \trianglelefteq G$ lánc normálánc.
- L **kompozíciólánc**, ha H_i/H_{i+1} egyszerű csoport (vagyis H_{i+1} maximális normális részcsoportja H_i-nek) minden $i \in \{1, 2, \dots, n\}$ esetén.
- L **centrális lánc**, ha L normállánc és $H_i/H_{i+1} \le Z(G/H_{i+1})$.
- L **főnormállánc**, ha L normállánc és H_i/H_{i+1} minimális részcsoportja G/H_{i+1}-nek.

3.9.1. A felső centrális lánc

Definiáljuk a $Z_n(G)$, $n \in \mathbb{N}$ növekvő láncot. Értelmezés szerint $Z_0(G) = \{e\}$ és $Z_1(G) = Z(G)$. Legyen

$$Z(G/Z_1(G)) =: Z_2(G)/Z_1(G).$$

Mivel $Z(G/Z_1(G)) \trianglelefteq G/Z_1(G)$, következik, hogy $Z_2(G) \trianglelefteq G$. Általában, legyen

$$Z_{n+1}(G)/Z_n(G) := Z(G/Z_n(G)).$$

Ekkor következik, hogy $Z_{n+1}(G) \trianglelefteq G$ és $Z_n(G) \le Z_{n+1}(G)$.

3.9.2. definíció. Az $\{e\} = Z_0(G) \le Z_1(G) \le Z_2(G) \le \dots \le Z_n(G) \le \dots$ láncot a G csoport **felső centrális lánc**anak nevezzük.

3.9.3. tétel. *A felso centrális lánc tagjai karakterisztikus részcsoportok.*

Bizonyítás. Evidens, hogy $Z_0(G) \le_c G$ és már láttuk, hogy $Z_1(G) \le_c G$. Feltételezzük, hogy az állítás igaz $Z_n(G)$-re, és igazoljuk $Z_{n+1}(G)$-re. Ekkor minden $f \in \mathrm{Aut}(G)$ esetén $f(Z_n(G)) = Z_n(G)$. Legyen $p_n : G \to G/Z_n(G)$ a kanonikus projekció; következik, hogy $p_n \circ f$ szürjektív morfizmus és $\mathrm{Ker}(p_n \circ f) = Z_n(G)$. Ekkor létezik egy $g : G/Z_n(G) \to G/Z_n(G)$ izomorfizmus úgy, hogy $g \circ p_n = g \circ f$. Mivel $Z(G/Z_n(G))$ karakterisztikus részcsoport, következik, hogy $Z_{n+1}(G)/Z_n(G) = g(Z_{n+1}(G)/Z_n(G))$. Így $Z_{n+1}(G)/Z_n(G) = g(Z_{n+1}(G)/Z_n(G)) = (g \circ p_n)(Z_{n+1}(G)) = (p_n \circ f)(Z_{n+1}(G)) = f(Z_{n+1}(G))/Z_n(G)$. A 3.1.3 tételbol következik, hogy $Z_{n+1}(G) = f(Z_n(G))$, vagyis $Z_{n+1}(G) \le_c G$. ■

3.9.4. példa. Tekintsük a D_n diédercsoportot. Ha n páratlan, akkor $Z_m(D_n) = \{e\}$, $(\forall) m \ge 0$. Feltételezzük, hogy n páros. Akkor $Z(D_n) = \{e, x^{n/2}\}$, és

$$D_n/Z(D_n) = \{x^i Z(D_n), x^l y Z(D_n) \mid 0 \le i, l < \frac{n}{2}\}.$$

Itt $\mathrm{ord}(xZ(D_n)) = \frac{n}{2}$, $\mathrm{ord}(yZ(D_n)) = 2$ és $(yZ(D_n))(xZ(D_n)) = (xZ(D_n))^{\frac{n}{2}-1}(yZ(D_n))$. Következik, hogy $D_n/Z(D_n) \simeq D_{n/2}$. Legyen $n = 2^k l$, ahol l páratlan, $k \ge 1$. Akkor $Z_1(D_n) = \{e, x^{2^{k-1}l}$, $Z_2(D_n)/Z_1(D_n) = \{Z(D_n), x^{2^{k-2}l} D_n\}$, tehát $Z_2(D_n) = \{x^{(2^{k-2}l)t} \mid 0 \le t < 4\}$. Indukcióval kapjuk, hogy

$$Z_r(D_n) = \{x^{2^{k-r}lt} \mid 0 \le t < 2^r\},$$

minden $1 \le r \le k$ esetén, és $Z_{k+1}(D_n) = Z_k(D_n)$.

3.9.2. A derivált lánc és az alsó centrális lánc

Legyen G egy csoport. A kommutátor segítségével értelmezünk két csökkenő láncot: $G^{(n)}$ és $\Gamma_n(G)$, $n \in \mathbb{N}$.
Értelmezés szerint:
$G^{(0)} = G$, $G' = [G, G]$, $\dots G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$ a **derivált lánc**;
$\Gamma_0(G) = G$, $\Gamma_1(G) = [G, G]$, $\dots \Gamma_n(G) = [\Gamma_{n-1}(G), \Gamma_{n-1}(G)]$ az **alsó centrális lánc**.
Következik, hogy: $G^{(0)} \ge G' \ge \dots \ge G^{(n)} \ge \dots$
$\Gamma_0(G) \ge \Gamma_1(G) \ge \dots \ge \Gamma_n(G) \ge \dots$

3.9.5. tétel. 1) *Ha* $f : G \to H$ *szürjektív morfizmus, akkor* $H^{(n)} = f(G^{(n)})$ *és* $\Gamma_n(H) = f(\Gamma_n(G))$, $n \in \mathbb{N}$.
2) *A derivált illetve alsó centrális lánc tagjai teljesen invariáns részcsoportok.*

Bizonyítás. 1) Mivel f szürjektív, $H^{(0)} = f(G^{(0)})$, és $\Gamma_0(H) = f(\Gamma_0(G))$. Feltételezzük, hogy az állítások igazak $n-1$ re: $H^{(n-1)} = f(G^{(n-1)})$, és $\Gamma_{n-1}(H) = f(\Gamma_{n-1}(G))$. Innen

$$H^{(n)} = [H^{(n-1)}, H^{(n-1)}] = [f(G^{(n-1)}), f(G^{(n-1)})] = f([G^{(n-1)}, G^{(n-1)}]) = f(G^n),$$
$$\Gamma_n(H) = [\Gamma_{n-1}(H), \Gamma_{n-1}(H)] = [f(\Gamma_{n-1}(G)), f(\Gamma_{n-1}(G))] = f([\Gamma_{n-1}(G), \Gamma_{n-1}(G)]) = f(\Gamma_n(G)).$$

2) Minden $f \in \mathrm{End}(G)$ esetén $f(G^{(0)}) = f(G) \leq G = G^{(0)}$, és $f(G_0) = f(G) \leq G = G_0$. Feltételezzük, hogy az állítás igaz n-re: $f(G^{(n)}) \leq f(G^{(n)})$ és $f(G_n) \leq f(G_n)$. Akkor $f(G^{(n+1)}) = f([G^{(n)}, G^{(n)}]) = [f(G^{(n)}), f(G^{(n)})] \leq [G^{(n)}, G^{(n)}] = G^{(n+1)}$. Hasonlóan: $f(\Gamma_{n+1}(G)) \leq \Gamma_{n+1}(G)$. ■

3.9.6. megjegyzés. A fenti tételbol következik, hogy $G^{(n)}$ és $\Gamma_n(G)$ normális részcsoportok. A 3.8.8. tétel alapján $\Gamma_{n-1}(G)/\Gamma_n(G) \leq Z(G/\Gamma_n(G))$, azaz $\Gamma_n(G)$ valóban centrális lánc.

3.9.7. példa. Tekintsük a D_n diédercsoportot. Nem nehéz belátni, hogy

$$\Gamma_2(D_n) = \begin{cases} \Gamma_1(D_n) = D_n, & \text{ha } n \text{ páratlan} \\ \langle x^4 \rangle, & \text{ha } n \text{ páros.} \end{cases}$$

Pontosabban, a második esetben

$$\langle x^4 \rangle = \begin{cases} \langle x^2 \rangle, & \text{ha } 4 \nmid n \\ \{e, x^4, x^8, \ldots, x^{\frac{n}{4}-1}\}, & \text{ha } 4 \mid n. \end{cases}$$

Feltételezzük, hogy $n = 2^k l$, ahol l páratlan. Indukcióval kapjuk, hogy:

$$\Gamma_0(D_n) = D_n \supset \Gamma_1(D_n) = \langle x^2 \rangle \supset \cdots \supset \Gamma_k(D_n) = \langle x^{2^k} \rangle = \Gamma_{k+1}(D_n).$$

3.9.3. Kompozícióláncok

3.9.8. definíció. Legyen $L = (G = H_0 \trianglerighteq H_1 \trianglerighteq \cdots \trianglerighteq H_n = \{e\})$ és $L' = (G = K_0 \trianglerighteq K_1 \trianglerighteq \cdots \trianglerighteq K_m = \{e\})$ két szubnormálánc. Azt mondjuk, hogy:

a) L **finomítása** L'-nek (vagy L' **részsorozata** L-nek) ha L' minden tagja szerepel az L tagjai között.

b) L és L' **izomorfak**, ha $m = n$, és létezik a $\{0, 1, \ldots, n-1\}$ halmaznak olyan ϕ permutációja, melyre $K_i/K_{i+1} \simeq H_{\phi(i)}/H_{\phi(i)+1}$.

c) Egy H részcsoportot **szubnormális részcsoport**nak nevezzük, ha G-nek van egy normállánca amely tartalmazza H. Jelölés: $H \trianglelefteq\trianglelefteq G$.

3.9.9. példa. Tekintsük a $(\mathbb{Z}_6, +)$ csoportot. Legyen $H_0 = K_0 = \mathbb{Z}_6$, $H_2 = K_2 = \{\hat{0}\}$, $H_1 = \langle \hat{2} \rangle$ és $K_1 = \langle \hat{3} \rangle$. Ezek a láncok izomorfak, mert $K_0/K_1 \simeq H_1/H_2$ és $K_1/K_2 \simeq H_0/H_1$. A ϕ permutáció a következoképpen van értelmezve: $\phi(0) = 1$, $\phi(1) = 0$, $\phi(2) = 2$.

A következő tétel a II. izomorfizmus tételt általánosítja.

3.9.10. tétel (Zassenhaus-lemma). *Legyen* G *egy csoport és* $H, K \leq G$ *két részcsoport. Ha* $H' \trianglelefteq H$ *és* $K' \trianglelefteq K$, *akkor* $H'(H \cap K') \trianglelefteq H'(H \cap K)$, $K'(K \cap H') \trianglelefteq K'(K \cap H)$, *és*

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq \frac{K'(K \cap H)}{K'(K \cap H')}.$$

Bizonyítás. Legyen $M = K \cap H$. Mivel $K' \trianglelefteq K$ és $M \leq K$, alkalmazva a II. izomorfizmus tételt következik, hogy $M \cap K' = K \cap H \cap K' = K' \cap H$ normális részcsoportja M-nek. Hasonlóan lehet igazolni, hogy $K \cap H' \trianglelefteq M$.

Következik, hogy $M' := (K' \cap H)(K \cap H') \trianglelefteq M$. Legyen

$$f : K'M \to M/M', \quad f(k'm) = mM',$$

ahol $k' \in K'$ és $m \in M$. Bebizonyítjuk, hogy az f definíciója nem függ a $k'm$ elem megválasztásától. Valóban, ha $k'm = k_1'm_1$, $k_1' \in K'$, $m_1 \in M$, akkor $k_1'k' = m_1m^{-1} \in K_1 \cap M \subseteq K' \cap H \subseteq M'$. Innen következik, hogy $m_1M' = mM'$. Tehát, f jól értelmezett függvény.

Mivel $K' \trianglelefteq K$, minden $k'm, k_1'm_1 \in K'M$ esetén

$$f(k'mk_1'm_1) = f(k'k_2'mm_1) = mm_1M' = mM'm_1M' = f(k'm)f(k_1'm_1),$$

tehát f morfizmus.

Igazoljuk, hogy $\operatorname{Ker} f = K'(K \cap H')$. Valóban, mivel $K \cap H' \leq M'$, következik, hogy $K'(K \cap H') \leq \operatorname{Ker} f$. Fordítva, ha $k'm \in \operatorname{Ker} f$, akkor $f(k'm) = mM' = M'$; innen következik, hogy $m \in M'$, tehát m felírható $m = uv$ alakban, ahol $u \in K' \cap H$, $v \in K \cap H'$. Tehát $k'm = (k'u)v \in K'(K \cap H')$; ebből következik, hogy $\operatorname{Ker} f \leq K'(K \cap H')$. Az f morfizmus szürjektív. Alkalmazva az első izomorfizmus tételt,

$$\frac{K'(K \cap H)}{K'(K \cap H')} \simeq M/M'.$$

A szimmetria alapján

$$\frac{H'(H \cap K)}{H'(H \cap K')} \simeq M/M'. \qquad ■$$

3.9.11. megjegyzés. Zassenhaus lemmájából megkapható a II. izomorfizmus tétel, ha $K \leq H$ és $K' = 1$.

3.9.12. tétel (Schreier). *Egy* G *csoport két szubnormáláncának van izomorf finomítása.*

Bizonyítás. Legyenek L és L' a G csoport két normálánca. L-ből és K_{i-1}-ből kapjuk a következő láncot:

$$K_{i-1} = K_{i-1} \cap H_0 \geq K_{i-1} \cap H_1 \geq \cdots \geq K_{i-1} \cap H_n = \{e\}.$$

Beszorozva a sorozat tagjait K_i-vel kapjuk:

$$K_{i-1} = K_i(K_{i-1} \cap H_0) \geq K_I(K_{i-1} \cap H_1) \geq \cdots \geq K_I(K_{i-1} \cap H_n) = K_i.$$

Jelölve $K_{ij} := K_i(K_{i-1} \cap H_j)$, a fenti sorozat a következő alakú lesz:

$$K_{i-1} = K_{i0} \geq K_{i1} \geq \cdots \geq K_{in} = K_i.$$

Zassenhauss lemmájából következik, hogy a fenti sorozat mindegyik tagja normális részcsoportja az előzőnek. Következésképpen, ha L'-ben behatároljuk K_{i-1} és K_i $(1 \leq i \leq m)$ közé a $K_{i-1} = K_{i0} \geq K_{i1} \geq \cdots \geq K_{i,n-1}$ sorozatot, akkor a következő szubnormáláncot kapjuk, amely L'-nek egy finomítása:

$$K_0 \geq K_{11} \geq K_{12} \geq \cdots \geq K_{1n-1} \geq K_1 \geq \cdots \geq K_{m-1} \geq K_{m1} \geq K_{m2} \geq \cdots \geq K_{m,n-1} \geq K_m.$$

Jelölve $H_{ji} := H_j(H_{j-1} \cap K_i)$, a fenti módszerekkel hasonlóan megkapjuk L-nek egy finomítását:

$$H_0 \geq H_{11} \geq H_{12} \geq \cdots \geq H_{1m-1} \geq H_1 \geq \cdots \geq H_{n-1} \geq H_{n1} \geq H_{n2} \geq \cdots \geq H_{nm-1} \geq H_n.$$

Zassenhaus lemmájából következik, hogy

$$K_{i,j-1}/K_{ij} \simeq H_{j,i-1}/H_{ji},$$

és innen következik, hogy a finomítások izomorfak. ■

3.9.13. következmény. *Ha a* G *csoportnak van két szigorúan csökkenő szubnormállánca, akkor ennek a két láncnak van szigorúan csökkenő finomítása, amelyek izomorfak.*

Bizonyítás. Valóban, mivel ha $K_{i,j-1} = K_{ij}$, akkor $H_{j,i-1} = H_{ji}$, a fenti finomításokból elhagyva az ismétlődő tagokat szigorúan csökkenő izomorf finomításokat kapunk. ■

3.9.14. tétel (Jordan–Hölder). *Ha egy* G *csoportnak vannak kompozicióláncai, akkor két ilyen lánc izomorf.*

Bizonyítás. Valóban, ha L és L' két kompoziciólánc, akkor szigorúan csökkenő izomorf finomításaik vannak. Mivel egy kompozicióláncnak nincs valódi finomítása, ezen finomítások megegyeznek L és L'-tel. Tehát L' és L' izomorf láncok. ■

3.9.15. következmény. a) *Ha a* G *csoportnak vannak kompozíció láncai, akkor az összes ilyen lánc ugyanolyan hosszúságú.*

b) *Ha a* G *csoportnak vannak kompozíció láncai, akkor bármely szigorúan csökkenő szubnormálánc kompozicióláncc á finomítható.*

A következőkben a kompozicióláncok létezését jellemezzük.

3.9.16. tétel. *Egy* G *csoportnak akkor és csak akkor van kompozíció lánca, ha a szubnormális részcsoportok halmaza teljesíti a következő feltételeket:*

(1) *csökkenő láncok feltétele: bármely szigorúan csökkenő szubnormális részcsoport sorozat véges.*

(2) *növekvő láncok feltétele: bármely szigorúan növekvő szubnormális részcsoport sorozat véges.*

Bizonyítás. Feltételezzük, hogy a G csoportban létezik egy szigorúan csökkenő

$$H_1 > H_2 > \cdots > H_n > \ldots$$

szubnormális részcsoport sorozat.

Ha H_1 szubnormális részcsoport akkor létezik egy szigorúan csökkenő normál sorozat, amely tartalmazza H_1-et. Legyen

$$G = H'_0 > H'_1 > \cdots > \{e\}$$

egy ilyen sorozat. Feltételezzük, hogy

$$G = H'_0 > H'_1 > \cdots > H_1 > H_2 > \cdots > H_n > \ldots$$

szigorúan csökkenő szubnormális részcsoportok sorozata. Tehát G tartalmaz bármilyen hosszúságú szigorúan csökkenő szubnormáláncot. Akkor G-nek nincs kompozició lánca.

Feltételezzük, hogy G csoportban létezik egy szigorúan növekvő

$$K_1 < K_2 < \cdots < K_n < \ldots$$

szubnormális részcsoport sorozat. Ha K_n szubnormális részcsoport, akkor létezik egy szigorúan csökkenő szubnormállánc, amely tartalmazza K_n-et. Legyen

$$G = K'_0 > K'_1 > \cdots > K'_j > K_n > K'_{j+2} > \cdots > \{e\}$$

egy ilyen lánc. Következik, hogy

$$G = K'_0 > K'_1 > \ldots K'_j > K_n > K_{n-1} > \ldots K_1 > \{e\}$$

egy szigorúan csökkenő szubnormálánc melynek a hossza legkevesebb n. Tehát G tartalmaz bármilyen hosszúságú szigorúan csökkenő szubnormálláncot. Akkor G-nek nincs kompozició lánca.

Fordítva, feltételezzük G teljesíti (1)-gyet és (2)-t. Akkor b)-ből következik, hogy G bármely nem egyszerű szubnormál részcsoportja, maximális normális részcsoporttal rendelkezik. Induktívan megszerkesztünk egy szigorúan csökkenő

$$G = H_0 > H_1 > H_2 > \cdots > H_m > \ldots$$

szubnormális részcsoport sorozatot úgy, hogy H_m maximális normális részcsoportja H_{m-1}-nek, ha H_{m-1} nem egyszerű, és $H_m = \{e\}$ ellenkező esetben; a)-ból következik, hogy létezik n úgy, hogy $H_n = \{e\}$. Tehát

$$G = H_0 > H_1 > \cdots > H_{n-1} > \{e\}$$

G-nek egy kompozició lánca. ■

3.9.17. következmény. a) *Bármely véges csoportnak van kompozició lánca.*

b) *Egy Abel csoportnak van kompozició lánca akkor és csak akkor ha véges.*

Bizonyítás. a) azonnali.

b) Ha

$$G = H_0 > H_1 > \cdots > H_n = \{e\}$$

kompoziciólánc, akkor H_{i-1}/H_i $(i = 1, \ldots, n)$ egyszerű Abel-csoport, tehát véges és prímszám rendű. Következik, hogy

$$|G| = |H_0/H_1| \cdot |H_2/H_1| \cdot \ldots \cdot |H_{n-1}/H_n|,$$

tehát G véges. ■

3.9.18. definíció. Legyen G egy csoport. Ha G-nek vannak kompozició láncai, akkor ezen sorozatok hosszát a G *hosszának* nevezzük. Ha G-nek nincs kompozició lánca, akkor G-t *végtelen hosszúságú*nak nevezzük. Jelölés: $l(G)$ = a G hossza.

3.9.19. tétel. *Legyen* G *egy csoport.*

1) *Ha* N *normális részcsoportja a* G *csoportnak, akkor* $l(G) = l(N) + l(G/N)$.

2) *Legyen* $H, N \leq G$, N *normális részcsoport. Akkor* $l(HN) + l(H \cap N) = l(H) + l(N)$.

3) *Ha* $G = H_0 > H_1 > \cdots > H_n = \{e\}$ *egy szubnormállánc, akkor* $l(G) = \sum_{i=1}^{n} l(H_{i-1}/H_i)$.

Bizonyítás. 1) Feltételezzük, hogy $G > N > \{e\}$. Ez a sorozat kompozicióláncc á finomítható:

$$G = H_0 > H_1 > \cdots > H_k > N > H_{k+2} > \cdots > H_n = \{e\}.$$

Következik, hogy a H_{i-1}/H_i $i = 1, 2, \ldots, k$ csoportok egyszerűek. A III. izomorfizmustétel alapján

$$(H_{i-1}/N)/H_i/N \simeq H_{i-1}/H_i.$$

Tehát a

$$G/N > H_1/N > \cdots > H_k/N > \{N\}$$

szubnormállánc faktorai egyszerű csoportok, tehát kompozicióllánca G/N-nek. Végül, vegyük észre, hogy az

$$N > H_{k+1} > \cdots > H_n > \{e\}$$

lánc H-nak egy kompozició lánca.

2) Alkalmazzuk az 1) pontot és a II. izomorfizmus tételt.

3) Alkalmazzuk az 1) pontot és indukciót. ■

3.73. feladat. Mutassuk meg, hogy a prímhatvány rendű ciklikus csoportnak egyetlen kompozíciólánca van.

3.74. feladat. Igazoljuk, hogy ha a G Abel-csoport rendje $n = p_1 p_2 \dots p_k$, ahol $p_1, p_2, \dots, p_k$ nem feltétlenül különböző prímek, akkor tetszoleges S_k-beli π permutációhoz létezik G-nek olyan kompozíciólánca, amelynek faktorai rendre $C_{p_{\pi(1)}}$, $C_{p_{\pi(2)}}$, $\dots$, $C_{p_{\pi(k)}}$.

3.75. feladat. Keressük meg a következő csoportok összes kompozícióláncait és ezen láncok faktorait:
a) C_{30};
b) D_4;
c) D_5;
d) D_6
e) A_4;
f) S_4;

3.76. feladat. Legyen G egy véges p-csoportok. Bizonyítsuk be, hogy:
a) G minden kompozíciófaktora p-ed rendű ciklikus csoport.
b) Ha $H \leq G$ egy valódi részcsoport, akkor G-nek van H-t tartalmazó kompozíciósorozata.
c) Ha N minimális normális részcsoportja G-nek, akkor $N \leq Z(G)$ és $|N| = p$.
d) G-nek van olyan főnormálńca, amelynek faktorai p-ed rendű ciklikus csoportok.
e) Ha $N \trianglelefteq G$, $|N| = p^i$, akkor $N \leq Z_i(G)$.

Útmutatás. a) Alkalmazzunk teljes indukciót. Így elegendő igazolni, hogy a G véges p-csoport tartalmaz p-indexu normálosztót. Tudjuk, hogy G minden M maximális részcsoportja normális, tehát G/M p-edrendű ciklikus csoport.

c) $N \cap Z(G)$ nemtriviális normális részcsoportja G-nek, amely benne van N-ben. Így $N \leq Z(G)$. Mutassuk meg ennek alapján, hogy N-nek nincs nemtriviális részcsoportja.

d) Alkalmazzunk teljes indukciót c) felhasználásával. Legyen $N_0 = \{e\}$, és N_{i+1} G-nek egy N_i-t tartalmazó olyan normális részcsoportja, hogy N_{i+1}/N_i a G/N_i faktorcsoportban minimális normális részcsoport.

e) A d) ponthoz hasonlóan, G-nek van olyan $\{e\} = N_0 < N_1 < N_2 < \dots < N_m = G$ főnormállánca, hogy $N_i = N$ és $N_{k+1}/N_k \leq Z(G/N_k)$, $k = 0, 1, 2, \dots, n-1$. Ennek alapján teljes indukcióval bizonyítható, hogy minden k-ra $N_k \leq Z_k(G)$.

3.10. Nilpotens csoportok

Ebben a fejezetben az Abel-csoportok egy fontos általánosítását mutatjuk be.

3.10.1. definíció. A G csoportot **nilpotens**nek nevezzük, ha létezik egy

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_r = G$$

centrális lánc.

A következokben a nilpotens csoportokat a felso és az alsó centrális láncokkal jellemezzük.

3.10.2. tétel. *Legyen G egy csoport. A következő állítások ekvivalensek:*
a) *G nilpotens csoport.*
b) *Létezik egy n természetes szám, úgy hogy $\Gamma_n(G) = \{e\}$*
c) *Létezik egy n természetes szám úgy, hogy $Z_n(G) = G$.*
Mi több, ha feltételezzük, hogy G nilpotens, és

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \dots \trianglelefteq H_r = G$$

a G-nek egy centrális lánca, akkor $\Gamma_{r-i}(G) \leq H_i \leq Z_i(G)$ minden $i \in \{0, 1, \dots, r\}$ esetén. Az a legkisebb k természetes szám amelyre $\Gamma_k(G) = \{e\}$ egyenlo azzal a legkisebb k természetes számmal amelyre $Z_k(G) = G$. Azt mondjuk, hogy k a G csoport **nilpotencia osztály***ának nevezzük.*

Bizonyítás. b)⇒a) Feltételezzük, hogy $\Gamma_n(G) = \{e\}$ egy n természetes számra. Ekkor G nilpotens, mivel

$$G = \Gamma_0(G) \geq \Gamma_1(G) \geq \dots \geq \Gamma_n(G) = \{e\}$$

G-nek egy centrális lánca.

c)⇒a) Feltételezzük, hogy létezik n természetes szám, úgy, hogy $Z_n(G) = G$. Ekkor

$$\{e\} = Z_0(G) \leq Z_1(G) \dots Z_n(G) = G$$

G-nek egy centrális lánca, tehát G nilpotens.

a)⇒b), c) Feltételezzük, hogy G nilpotens csoport és legyen

$$\{e\} = H_0 \trianglelefteq H_1 \trianglelefteq \cdots \trianglelefteq H_r = G$$

G-nek egy centrális lánca. Ekkor $H_0 = \{e\} \leq Z_0(G)$, és ha feltételezzük, hogy $H_i \leq Z_i(G)$, akkor minden $x \in H_{i+1}$, $y \in G$ esetén $[x, y] = x^{-1}y^{-1}xy \in H_i$ mivel $H_{i+1}/H_i \leq Z(G/Hi)$. Tehát $[x, y] \in Z_i(G)$, ez azt mutatja, hogy $H_{i+1}Z_i(G)/Z_i(G) \leq Z(G/Z_i(G)) = Z_{i+1}(G)/Z_i(G)$. Innen következik, hogy $H_{i+1} \leq H_{i+1}Z_i(G) \leq Z_{i+1}(G)$. Így $H_i \leq Z_i(G)$ minden $i \in \{0, 1, \ldots, r\}$ esetén. Partikulárisan $G = H_r \leq Z_r(G)$, tehát $Z_r(G) = G$.

Hasonlóan, $\Gamma_0(G) = G \leq H_r$, és ha feltételezzük, hogy $\Gamma_j(G) \leq H_{r-j}$, akkor $\Gamma_{j+1}(G) = [\Gamma_j(G), G] \leq [H_{r-j}, G] \leq H_{r-(j+1)}$. Következésképpen $\Gamma_j(G) \leq H_{r-j}$ minden $j \in \{0, 1, \ldots, r\}$ esetén. Partikulárisan, $\Gamma_r(G) \leq H_0 = \{e\}$, tehát $\Gamma_r(G) = \{e\}$.

Legyen k az a legkisebb természetes szám, amelyre $Z_k(G) = G$. Alkalmazva a fenti eredményeket az $\{e\} = Z_0(G) \leq Z_1(G) \leq \cdots \leq Z_k(G) = G$ centrális láncra kapjuk, hogy $\Gamma_j(G) \leq Z_{k-j}(G)$ minden $j \in \{0, 1, \ldots, k\}$ esetén. Így $\Gamma_k(G) = \{e\}$. Még be kell bizonyítani, hogy ha $k > 1$, akkor $\Gamma_{k-1}(G) \neq \{e\}$. Redukció ad abszurdum módszerét használva, ha feltételezzük, hogy $\Gamma_{k-1}(G) = \{e\}$, és alkalmazzuk a fenti eredményeket a $G = \Gamma_0(G) \geq \Gamma_1(G) \geq \cdots \geq \Gamma_{k-1}(G) = \{e\}$ centrális láncra akkor, következik, hogy $\Gamma_{k-(j+1)}(G) \leq Z_j(G)$. Partikulárisan, $G = \Gamma_0(G) \leq Z_{k-1}(G)$, tehát $G = Z_{k-1}(G)$, de ez ellentmond a k megválasztásának. ■

3.10.3. példa. a) Bármely Abel-csoport 1. osztályú nilpotens csoport.

b) A Q_8 kvaterniócsoport 2. osztályú nilpotens csoport.

c) Ha $n \geq 3$, akkor $Z(S_n) = \{e\}$, tehát S_n nem nilpotens.

d) A D_n dieder csoport nilpotens akkor és csak akkor ha ahol $n = 2^k$ alakú. A D_{2^k} a nilpotencia osztálya k.

3.10.4. tétel. 1) *Nilpotens csoport részcsoportjai nilpotensek.*

2) *Nilpotens csoport homomorf képei nilpotensek.*

3) *Véges számú nilpotens csoportok direkt szorzata nilpotens.*

Bizonyítás. 1) Legyen G egy k osztályú nilpotens csoport és H részcsoportja G-nek. Akkor $\Gamma_0(H) = H \leq G = \Gamma_0(G)$. Feltételezzük, hogy $\Gamma_m(H) \leq \Gamma_m(G)$; abból, hogy $\Gamma_{m+1}(H) = [\Gamma_m(H), H]$, $\Gamma_{m+1}(G) = [\Gamma_m(G), G]$, következik, $\Gamma_{m+1}(H) \leq \Gamma_{m+1}(G)$. Tehát $\Gamma_n(H) \leq \Gamma_n(G)$ minden $n \in \mathbb{N}$ esetén. Következésképpen $\Gamma_k(H) = \{e\}$, azaz, H legfennebb k osztályú nilpotens csoport.

2) Legyen G egy k-osztályú nilpotens csoport és $f : G \to K$ egy szürjektív morfizmus. Ekkor $\Gamma_k(K) = f(\Gamma_k(G)) = f(\{e\}) = e$, azaz K legfennebb k-osztályú nilpotens csoport.

3) Igazoljuk, hogy két nilpotens csoport direkt szorzata nilpotens. Legyen G és K két k illetve l-osztályú nilpotens csoport, és $L := G \times K$. Ekkor $\Gamma_0(L) = L = G \times K = \Gamma_0(G) \times \Gamma_0(K)$. Feltételezzük, hogy $\Gamma_m(L) = \Gamma_m(G) \times \Gamma_m(K)$; innen

$$\Gamma_{m+1}(L) = [\Gamma_m(L), L] = [\Gamma_m(G) \times \Gamma_m(K), G \times K] = [\Gamma_m(G), G] \times [\Gamma_m(K), K] = \Gamma_{m+1}(G) \times \Gamma_{m+1}(K).$$

Következésképpen, ha $k > l$, akkor $\Gamma_k(L) = \Gamma_k(G) \times \Gamma_k(K) = \{(e, e)\}$. Tehát L legfennebb k-osztályú nilpotens csoport. ■

3.10.5. tétel. *Minden véges p-csoport nilpotens és ha $|G| = p^n$, ahol $n \geq 2$, akkor a G nilpotencia osztálya legfennebb $n - 1$.*

Bizonyítás. Tudjuk, hogy $Z_1(G) = Z(G) \neq \{e\}$. Így $|Z_1(G)| = p^{n_1}$, ahol $0 < n_1 < n$. De $Z_1(G) \neq G$, tehát $Z_2(G)/Z_1(G) = Z(G/Z_1(G)) \neq \{e\}$. Innen $|Z_2(G)| = p^{n_2}$, ahol $0 < n_1 < n_2 < n$. Általánosan, ha $Z_{i-1}(G) \neq G$, akkor $Z_i(G)/Z_{i-1}(G) = Z(G/Z_{i-1}(G)) \neq \{e\}$. Innen $|Z_i(G)| = p^{n_i}$, ahol $0 < n_1 < \cdots < n_{i-1} < n_i \leq n$. Létezik egy k természetes szám, úgy, hogy $0 < n_1 < \cdots < n_k = n$, és ekkor G nilpotens és a nilpotencia osztálya k, ahol $k \leq n$. Feltételezzük, hogy $n \geq 2$ és $k = n$; ekkor $n_i = i$, és $|Z_i(G)| = p^i$ minden $i \in \{1, 2, \ldots, n\}$ esetén. Mivel $|G/Z_{n-2}(G)| = p^2$, $G/Z_{n-2}(G)$ Abel-csoport. Kapjuk, hogy $Z_{n-1}(G)/Z_{n-2}(G) = Z(G/Z_{n-2}(G)) = G/Z_{n-2}(G)$, azaz $Z_{n-1}(G) = G$. Ez természetesen nem lehetséges. Következésképpen G nilpotens és a nilpotencia osztálya $k \leq n - 1$. ■

3.10.6. tétel. *Legyen G egy véges csoport. A következő állítások ekvivalensek:*

a) *G nilpotens.*

b) *G bármely részcsoportja szubnormális.*

c) *G bármely valódi H részcsoportja esetén $H < N_G(H)$.*

d) *G bármely maximális részcsoportja normális részcsoport.*

e) *$G' := [G, G] \leq \Phi(G)$, ahol $\Phi(G) := \bigcap\{M \mid M < G$ maximális részcsoport$\}$ a G csoport Frattini-részcsoportja.*

f) *G bármely Sylow-részcsoportja normális részcsoport.*

g) *G izomorf prímszám rendű csoportok direkt szorzatával.*

Bizonyítás. a)⇒b) Legyen k a G csoport nilpotencia osztálya és legyen $Z_i := Z_i(G)$. Akkor $H = HZ_0 \trianglelefteq HZ_1 \trianglelefteq \cdots \trianglelefteq HZ_k = G$. Mivel $Z_{i+1}/Z_i = Z(G/Z_i)$, következik, hogy $HZ_i \trianglelefteq HZ_{i+1}$ bármely $i \in \{0, 1, \ldots, k\}$

esetén. Valóban, ha $h, h' \in H$, $z_i \in Z_i$, $z_{i+1} \in Z_{i+1}$, akkor $(h'z_{i+1})(hz_i)(h'z_{i+1})^{-1} = h'z_{i+1}(hz_i)z_{i+1}h'^{-1}$. De $z_{i+1}(hz_i)z_{i+1}(hz_i)^{-1} \in Z_i$. Tehát $z_{i+1}(hz_i)z_{i+1} = z_i'(hz_i)$ ahol $z_i' \in Z_i$. Következésképpen

$$(h'z_{i+1})(hz_i)(h'z_{i+1})^{-1} = h'z_i'hz_ih'^{-1} \in HZ_i.$$

b)⇒c) Legyen $H < G$. Mivel H szubnormális, létezik G-nek egy olyan H_1 részcsoportja, amelyre $H \trianglelefteq H_1$. Ekkor $H < H_1 \leq N_G(H)$.

c)⇒d) Legyen M maximális részcsoportja G-nek. Mivel $M < G$, következik, hogy $M < N_G(M) \leq G$; de M maximális, tehát $N_G(M) = G$, azaz $M \trianglelefteq G$.

d)⇒e) Legyen M maximális részcsoportja G-nek. Ekkor $M \trianglelefteq G$ és G/M prímszám rendű ciklikus csoport. Partikulárisan, G/M Abel-csoport, tehát $G' \leq M$. Következésképpen $G' \leq F(G)$.

e)⇒d) Legyen M maximális részcsoportja G-nek. Ekkor $G' \leq F(G) \leq M$, tehát M/G' részcsoportja a G/G' Abel-csoportnak. Következik, hogy $M/G' \trianglelefteq G/G'$, tehát $M \trianglelefteq G$.

d)⇒f) Legyen P egy Sylow p-részcsoportja G-nek. Feltételezzük, hogy $N_G(P) < G$. Ekkor létezik M maximális részcsoportja G-nek úgy, hogy $N_G(P) \leq M$. Következik, hogy $N_G(M) = M$ és ez ellentmond annak, hogy $M \trianglelefteq G$. Következésképpen $N_G(P) = G$, tehát $P \trianglelefteq G$.

f)⇒g) Legyenek $p_1, p_2, \ldots, p_s$ a $|G|$ prím osztói. Minden $i \in \{1, 2, \ldots, s\}$ esetén legyen P_i Sylow p_i-részcsoportja G-nek. Ekkor $P_i \trianglelefteq G$, $|P_i| = p_i^{n_i}$ és $|G| = p_1^{n_1} \ldots p_s^{n_s}$. Minden $m \in \{1, 2, \ldots, s\}$ esetén legyen $I_m = P_1P_2 \ldots P_m \leq G$. m szerinti indukcióval bebizonyítjuk, hogy $|I_m| = p_1^{n_1} \ldots p_m^{n_m}$. Ha $m = 1$, $I_1 = P_1$, tehát $|I_1| = p_1^{n_1}$. Feltételezzük, hogy $m > 1$ és hogy $|I_{m-1}| = p_1^{n_1} \ldots p_{m-1}^{n_{m-1}}$. Lagrange tételből $P_m \cap I_{m-1} = \{e\}$, és mivel $I_m = I_{m-1}P_m$, következik, hogy

$$|I_m| = |I_{m-1}P_m| = \frac{|I_{m-1}| \cdot |P_m|}{|I_{m-1} \cap P_m|} = p_1^{n_1} \ldots p_m^{n_m}.$$

Partikulárisan $|I_s| = p_1^{n_1} \ldots p_s^{n_s} = |G|$, tehát $I_s = G$. Mivel $I_{m-1} \cap P_m = \{e\}$ bármely $m \in \{2, \ldots, s\}$, következik a 3.5.6. megjegyzés alapján, hogy $G = P_1 \times P_2 \times \cdots \times P_s$.

g)⇒f) Alkalmazzuk a 3.10.4 tételt. ■

3.10.7. tétel. *Legyen* G *egy csoport és* $H \leq Z(G)$. *Ha* G/H *nilpotens, akkor* G *nilpotens.*

Bizonyítás. Tudjuk, hogy $\Gamma_n(G/H) = \Gamma_n(G)H/H$. Ha k a G/H csoport nilpotencia osztálya, akkor $\Gamma_k(G)H/H = \{H\}$, ahonnan következik, hogy $\Gamma_k(G)H = H$, azaz $\Gamma_k(G) \leq H \leq Z(G)$. Tehát $\Gamma_{k+1}(G) = [\Gamma_k(G), G] = \{e\}$, vagyis G legfennebb $k+1$ osztályú nilpotens csoport. ■

3.10.8. példa. Általában nilpotens csoportok bovítései nem nilpotensek. Például az S_3 szimmetrikus csoport nem nilpotens, mivel a centruma triviális. De A_3 és S_3/A_3 Abel-csoportok tehát nilpotensek.

3.10.9. lemma. *Legyen* $\{e\} < N \trianglelefteq G$. *Akkor* $N \cap Z(G) \neq \{e\}$.

Bizonyítás. Feltételezzük, hogy $Z_k(G) = G$. Akkor létezik egy i természetes szám úgy, hogy $N \cap Z_i(G) = \{e\}$ és $N \cap Z_{i+1}(G) \neq \{e\}$.

Mivel $N \trianglelefteq G$ és $Z_{i+1}(G) \trianglelefteq G$, következik, hogy $N \cap Z_{i+1} \trianglelefteq G$. Tehát $[N \cap Z_{i+1}(G), G] \leq N \cap Z_{i+1}(G) \leq N$, és $[N \cap Z_{i+1}(G), G] \leq [Z_{i+1}(G), G] \leq Z_i(G)$. Következik, hogy $[N \cap Z_{i+1}(G), G] \leq N \cap Z_i(G) = \{e\}$, azaz $\{e\} \neq N \cap Z_{i+1}(G) \leq N \cap Z(G)$.

3.10.10. tétel. *Legyen* G *egy véges csoport és* $H \trianglelefteq G$, $K \trianglelefteq G$. *Ha* H *és* K *nilpotensek, akkor* HK *is nilpotens.*

Bizonyítás. $|G|$ szerinti indukcióval bizonyítunk. Feltételezzük az állítás igaz bármely véges csoportja, amelynek a rendje kisebb, mint $|G|$. Ha $HK < G$, akkor a tétel következik az indukció feltételébol. Feltételezzük, hogy $HK = G$. Eloször igazoljuk, hogy $Z(G) \neq \{e\}$. Mivel $K \trianglelefteq G$, $Z(K) \trianglelefteq G$. Következik, hogy $N := [H, Z(K)] \trianglelefteq G$. Két esetet különböztetünk meg: $N = \{e\}$ és $N \neq \{e\}$. Az elso esetben $Z(K) \leq Z(HK) = Z(G)$, és mivel K nilpotens következik, hogy $Z(K) \neq \{e\}$. Tehát $Z(G) \neq \{e\}$. A második esetben, mivel $N \trianglelefteq H$, következik (az előző lemma alapján), hogy $L := N \cap Z(H) \neq \{e\}$. Abból, hogy $N \leq Z(K)$ következik, hogy $\{e\} \neq Z(H) \cap Z(K) \leq Z(G)$. Tehát mindkét esetben $Z(G) \neq \{e\}$.

Következik, hogy $|G : Z(G)| < |G|$. Tudjuk, hogy

$$G/Z(G) = HK/Z(G) = (HZ(G)/Z(G))(KZ(G)/Z(G).$$

Abból, hogy $HZ(G)/Z(G) \simeq H/H \cap Z(G)$ és $KZ(G)/Z(G) \simeq K/K \cap Z(G)$ kapjuk, hogy $HZ(G)/Z(G)$ és $KZ(G)/Z(G)$ nilpotens csoportok. Tehát az indukció feltétele alapján $G/Z(G)$ nilpotens, azaz G nilpotens. ■

3.10.11. definíció. Legyen G egy véges csoport. A G összes normális és nilpotens részcsoportja által generált $F(G)$ részcsoportot a G **nilpotens radikál**jának vagy **Fitting-radikál**jának nevezzük.

3.77. feladat. Tanulmányozzuk a D_n diédercsoport nilpotenciáját, $n \geq 1$.

3.78. feladat. Legyen

$$G = \left\{ \begin{pmatrix} 1 & a_{12} & a_{13} & \dots & a_n \\ 0 & 1 & a_{23} & \dots & a_{2n} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \dots & 1 \end{pmatrix} \mid a_{ij} \in \mathbb{Z} \right\} \leq \mathrm{GL}(\mathbb{Z}),$$

és $G_k \leq G$ (ahol $1 \leq k < n$) részcsoport álljon azokból a G-beli mátrixokból, amelyekre $j - i \leq k$ esetén $a_{ij} = 0$. Bizonyítsuk be, hogy minden $1 \leq k < n$ esetén $\Gamma_k(G) = Z_{n-1-k}(G) = G_k$.

3.79. feladat. Legyen G egy n-ed rendű nilpotens csoport. Igazoljuk, hogy ha $d \mid n$, akkor G-nek van d-ed rendű részcsoportja.

3.11. Feloldható csoportok

3.11.1. definíció. Legyen G egy csoport, és $G^{(0)} \geq G^{(1)} \geq \dots \geq G^{(n)} \geq \dots$ a G derivált lánca, azaz $G^{(0)} = G$, $G^{(n+1)} = [G^{(n)}, G^{(n)}]$. A G csoportot **feloldható csoport**nak nevezzük, ha létezik $m \in \mathbb{N}$, úgy, hogy $G^{(m)} = \{e\}$. A legkisebb k természetes számot, amelyre $G^{(k)} = \{e\}$ a G **feloldhatóság osztály**ának nevezzük.

3.11.2. megjegyzés. a) Minden Abel csoport 1. osztályú feloldható csoport.

b) Minden nilpotens csoport feloldható.

Valóban, indukcióval könnyen belátható, hogy $G^{(m)} \leq \Gamma_m(G)$ minden m esetén. Tehát ha G k-ad osztályú nilpotens csoport, akkor $G^{(k)} \leq \Gamma_k(G) = \{e\}$. Tehát G legfennebb k-ad osztályú feloldható csoport.

3.11.3. tétel. 1) *Feloldható csoport részcsoportjai feloldhatók.*

2) *Feloldható csoport homomorf képei feloldhatók.*

3) *Legyen* $K \trianglelefteq G$ *és* $H := G/K$. *Ekkor* G *feloldható akkor és csak akkor, ha* K *és* H *feloldható csoportok.*

4) *Véges számú feloldható csoport direkt szorzata is feloldható csoport.*

5) *Legyen* $K \trianglelefteq G$ *és* $H \trianglelefteq G$. *Ha* K *és* H *feloldhatók, akkor* KH *is feloldható.*

Bizonyítás. 1) Legyen G egy k-ad osztályú feloldható csoport, és $H \leq G$. Ekkor $H^{(0)} = H \leq G = G^{(0)}$. Feltételezzük, hogy $H^{(m)} \leq G^{(m)}$; innen $H^{(m+1)} = [H^{(m)}, H^{(m)}] \leq [G^{(m)}, G^{(m)}] = G^{(m+1)}$. Tehát $H(n) \leq G(n)$, minden n esetén, így $H^{(k)} = \{e\}$, azaz H legfennebb k-ad osztályú feloldható csoport.

2) Indukcióval igazoljuk, hogy $f(G)^{(k)} = f(G^{(k)})$.

3) Legyen K egy k-ad osztályú feloldható csoport, H pedig l-ed osztályu feloldható csoport, és legyen $pG \to H$ a kanonikus projekció. Akkor $p(G^{(k)}) = H^{(l)} = \{e\}$, ahonnan következik, hogy $G^{(l)} \leq K$. Innen $G^{(l+k)} = (G^{(l)})^{(k)} \leq K^{(l)} = \{e\}$. Tehát G legfennebb $l + k$-ad osztályú feloldható csoport.

4) következik 3)-ból.

5) $H/K \cap H$ feloldható mert H-nak homomorf képe. A 2. izomorfizmus tételbol $HK/K \simeq H/H \cap K$, tehát HK/K feloldható. Mivel K feloldható, következik, hogy KH is feloldható. ■

A következő tétel fontos szerepet játszik a Galois-elméletben.

3.11.4. tétel. *Egy* G *csoport feloldható akkor és csak akkor, ha van egy* $G = H_0 \geq H_1 \geq \dots \geq H_n = \{e\}$ *szubnormállánca, amelynek a* H_{i-1}/H_i *faktorai,* $i \geq 1$, *Abel-csoportok.*

Bizonyítás. Ha G n-ed osztályú feloldható csoport akkor a $G = G^{(0)} \geq G' \geq G'' \geq \dots \geq G^{(n)} = \{e\}$ derivált lánc normállánc, és a faktorai Abel-csoportok.

Fordítva, feltételezzük G-nek van egy szubnormállánca, amelynek faktorai Abel-csoportok. Mivel G/H_1 Abel-csoport, $G' \leq H_1$. Feltételezzük, hogy $G^{(i-1)} \leq H_{i-1}$, és mivel H_{i-1}/H_i Abel-csoport, következik, hogy $G^{(i)} = [G^{(i-1)}, G^{(i-1)}] \leq [H^{(i-1)}, H^{(i-1)}] \leq H_i$. Következik, hogy $G^{(n)} = \{e\}$, azaz G legfenebb n-ed osztályú feloldható csoport. ■

3.11.5. következmény. *Egy véges csoport feloldható akkor és csak akkor, ha egy kompozíció láncának a faktorai prímszám rendű ciklikus csoportok.*

3.11.6. példa. Az S_n szimmetrikus csoport feloldható akkor és csak akkor, ha $n \leq 4$.

Valóban, az állítás igaz, ha $n = 1, 2$ mivel S_1 és S_2 Ábel-csoportok. S_3 nem kommutatív és a rendje 6, $A_3 \trianglelefteq S_3$ rendje pedig 3. Következésképpen A_3 ciklikus csoport, tehát Abel-csoport, és S_3/A_3 szintén ciklikus és a rendje 2. Így $\{e\} \leq A_3 \leq S_3$ Abel-lánc.

Általában, minden $n \geq 3$ esetén $S_n' = A_n$. Valóban, mivel S_n/A_n kommutatív, $S_n' \leq A_n$; fordítva, tudjuk, hogy minden páros permutáció 3 hosszúságú ciklusok szorzata, de a 3.62. a) feladat szerint minden hosszúságú ciklus kommutátor, tehát $A_n \leq S_n'$.

S_4-re megszerkesztjük a következő normálláncot, amelynek faktorai Abel-csoportok: $\{e\} \leq K \leq A_4 \leq S_4$, ahol $K = \{e, (1\ 2)(3\ 4), (1\ 3)(2\ 4), (1\ 4)(2\ 3)\}$ Klein-csoport. Pontosabban, a 3.62. feladat a) és b) pontjaiból azonnal következik, hogy $K = A_4'$, tehát a fenti lánc az S_4 derivált lánca. Tehát S_4-is feloldható csoport.

Végűl, ha $n \geq 5$, akkor S_n feloldhatatlan, mivel $S_n'' = A_5' = A_5$ az 3.62. c) feladat szerint.

3.11.7. definíció. Legyen G véges csoport.

a) A G összes normális és feloldható részcsoportjai által generált $W(G)$ részcsoport normális és feloldható. $W(G)$-t a G **feloldható radikál**jának, vagy a G **Wendt-részcsoport**jának nevezzük.

b) Ha $W(G) = 1$, akkor G-t **félig egyszerű csoport**nak nevezzük.

3.11.8. tétel. $G/W(G)$ *félig egyszerű csoport.*

Bizonyítás. A G feloldható és normális részcsoportjai között $W(G)$ maximális. Következik, hogy $G/W(G)$-nek nincs $\{W(G)\}$-től különböző normális és feloldható részcsoportja. Innen következik, hogy $W(G/W(G)) = \{W(G)\}$. Tehát $G/W(G)$ félig egyszerű. ■

3.11.9. tétel. *Legyen* G *egy véges csoport. Ekkor* $W(G) = \{e\} \Leftrightarrow F(G) = \{e\}$.

Bizonyítás. Mivel minden nilpotens csoport feloldható, következik, hogy $F(G) \leq W(G)$. Tehát ha $W(G) = \{e\}$, akkor $F(G) = \{e\}$.

Fordítva, legyen $W(G) \neq \{e\}$. Mivel $W(G)$ feloldható, létezik egy k természetes szám, úgy, hogy $W(G)^{(k)} = \{e\}$ és $W(G)^{(k-1)} \neq \{e\}$. Mivel $[W(G)^{(k-1)}, W(G)^{(k-1)}] = W(G)^{(k)} = \{e\}$, következik, hogy $W(G)^{(k-1)}$ Abel-csoport, tehát nilpotens is. Tehát $W(G)^{(k-1)} \leq F(G)$, azaz $F(G) \neq \{e\}$. ■

3.80. feladat. Feloldható-e a D_n diéder csoport?

3.81. feladat. Igazoljuk, hogy minden pq, p^2q, illetve p^2q^2 rendű csoport feloldható (ahol p, q prímszámok).

4. fejezet

Gyűrűk, testek, polinomok

4.1. Ideálok

4.1.1. definíció. Legyen R egy gyűrű, és I egy nemüres részhalmaza. Azt mondjuk, hogy I **balideál**ja (**jobbideál**ja) R-nek (jelölés: $I \underset{b}{\trianglelefteq} R$, $(I \underset{j}{\trianglelefteq} R)$), ha:

1. minden $x, y \in I$ esetén $x - y \in I$;
2. minden $x \in I$ és $r \in R$ esetén $rx \in I$ (illetve $xr \in I$).

Ha I egyidőben balideál és jobbideál, akkor I-t **ideálnak** nevezzük (jelölés: $I \trianglelefteq R$).

4.1.2. megjegyzés. 1) Ha I ideálja R-nek, akkor I részgyűrűje R-nek.

2) A $\{0\}$ és R ideáljai R-nek. Ezeket *triviális* ideáloknak nevezzük. Ha $I \neq 0$ és $I \neq R$, akkor I-t *valódi* ideálnak nevezzük.

Ha az R gyűrűnek nincs valódi ideálja, akkor R-et **egyszerű gyűrű**nek nevezzük.

4.1.3. példa. 1) Ha R egy gyűrű, $a \in R$, akkor $Ra = \{ra \mid r \in R\}$ bal oldali ideálja R-nek, $aR = \{ar \mid r \in R\}$ jobb oldali ideálja R-nek és aRa ideálja R-nek.

2) Ha $(\mathbb{Z}, +, \cdot)$ gyűrű, akkor $n\mathbb{Z}$ ideálja $\mathbb{Z}$-nek minden $n \in \mathbb{Z}$ esetén (tehát $\mathbb{Z}$-nek minden ideálja $n\mathbb{Z}$ alakú).

3) Ha R kommutatív gyűrű, akkor a balideál, a jobbideál és az ideál fogalmai ekvivalensek.

4) Legyen $I = \{\begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}\} \subseteq M_2(\mathbb{Z})$ és $J = \{\begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in \mathbb{Z}\} \subseteq M_2(\mathbb{Z})$. Akkor I jobb oldali ideál, de nem bal oldali ideál és J bal oldali ideál, de nem jobb oldali ideál.

5) Ha $f : R \to S$ gyűrűmorfizmus, akkor $\operatorname{Ker} f$ ideálja R-nek.

Valóban, $\operatorname{Ker} f$ részcsoportja az $(R, +)$-nak és minden $x \in \operatorname{Ker} f$, $r \in R$ esetén $f(rx) = f(r)f(x) = f(r)0 = 0$, tehát $rx, xr \in \operatorname{Ker} f$.

6) Adott az R gyűrű és $X \subseteq R$. Tekintsük a következő halmazokat (bal oldali és jobb oldali **anulátorideál**):

$\operatorname{Ann}_b(X) = \{r \in R \mid rx = 0, \text{ minden } x \in X\}$;

$\operatorname{Ann}_j(X) = \{r \in R \mid xr = 0, \text{ minden } x \in X\}$;

$\operatorname{Ann}(X) = \{r \in R \mid rx = xr = 0, \text{ minden } x \in X\}$.

Ekkor $\operatorname{Ann}_b(X)$ bal oldali ideálja R-nek, $\operatorname{Ann}_j(X)$ jobb oldali ideálja R-nek és $\operatorname{Ann}(X)$ ideálja R-nek.

7) Feltételezzük, hogy I bal oldali ideálja R-nek (I jobb oldali ideálja R-nek) és létezik $a \in I$ úgy, hogy a invertálható elem, akkor $I = R$.

Valóban, mivel a invertálható elem, létezik a^{-1} úgy, hogy $aa^{-1} = a^{-1}a = 1$. Mivel I bal oldali ideálja R-nek (I jobb oldali ideálja R-nek), következik, hogy minden $r \in R$ esetén $ra^{-1} \in R$ ($a^{-1}r \in R$). Végül $(ra^{-1})a = r \in I$ ($a(a^{-1}r) = r \in I$), tehát $I = R$.

Innen következik, hogy egy testnek nincsenek valódi ideáljai, azaz minden test egyszerű gyűrű.

4.1.4. tétel (Testek jellemzése ideálokkal). *Legyen R egy gyűrű. A következő állítások ekvivalensek:*

(i) R *test;*

(ii) $RR \neq \{0\}$, R*-nek nincsenek valódi balideáljai és* R*-nek nincsenek valódi jobbideáljai.*

Bizonyítás. 1) $\Longrightarrow$ 2) Ha R test, akkor R-nek nincsenek valódi balideáljai és jobbideáljai. Továbbá $0 \neq 1 = 1 \cdot 1 \in RR$, tehát $RR \neq \{0\}$.

2) $\Longrightarrow$ 1) Igazolni kell, hogy $R \neq \{0\}$ és minden nemnulla eleme invertálható. Valóban, ha $R = \{0\}$, akkor $RR = \{0\}$ ami ellentmond a 2)-es feltevésnek. Továbbá, tekintsük az $\operatorname{Ann}_j(R) = \{r \in R \mid xr = 0, \ \forall x \in R\}$ jobb oldali ideált. A 2)-es feltevés szerint $\operatorname{Ann}_j(R) = \{0\}$ vagy $\operatorname{Ann}_j(R) = R$ (az utolsó nem lehetséges, mert $RR \neq \{0\}$);

következik, hogy $\mathrm{Ann}_j(R) = \{0\}$, tehát minden $a \in R^*$ esetén $Ra \neq \{0\}$. Mivel Ra bal oldali ideálja R-nek, a 2)-es feltevés szerint $Ra = R$, tehát minden $y \in R$ esetén létezik $x \in R$ úgy, hogy $y = xa$. Hasonlóan $aR = R$, tehát minden $y' \in R$-re létezik $x' \in R$ úgy, hogy $y' = ax'$. Igazoltuk, hogy $(R^*, \cdot)$ csoport, tehát R test. ■

4.1. feladat. Legyen R egy egységelemes gyűrű, $I = \left\{ \begin{pmatrix} a & b \\ 0 & 0 \end{pmatrix} \mid a, b \in R \right\}$ és $J = \left\{ \begin{pmatrix} a & 0 \\ b & 0 \end{pmatrix} \mid a, b \in R \right\}$. Igazoljuk, hogy:

a) I jobbideálja $M_2(R)$-nek, J balideál és $I \cap J$ részgyűrű, de nem ideál.

b) Az $M_2(R)$ nilpotens elemei, illetve zérusosztói, nem alkotnak ideált.

4.2. feladat. Ha R egy gyűrű és I, J két ideál, legyen $I : J = \{r \in R \mid (\forall) b \in J \ rb \in I\}$. Igazoljuk, hogy:

a) $I : J \trianglelefteq R$; $I : I = R$.

b) $(I_1 \cap \cdots \cap I_n) : J = (I_1 : J) \cap \cdots \cap (I_n : J)$.

c) $I : (J_1 + \cdots + J_n) = (I : J_1) \cap \cdots \cap (I : J_n)$.

d) $n\mathbb{Z} : m\mathbb{Z} = \frac{[m,n]}{m}\mathbb{Z}$.

4.3. feladat. Ha A egy kommutatív gyűrű és $I \trianglelefteq A$, legyen $\sqrt{I} = \{a \in A \mid (\exists) n \in \mathbb{N} \ a^n \in I\}$. Igazoljuk, hogy:

a) $I \subseteq \sqrt{I} \trianglelefteq A$; $I \subseteq J \Rightarrow \sqrt{I} \subseteq \sqrt{J}$.

b) $\sqrt{IJ} = \sqrt{I \cap J} = \sqrt{I} \cap \sqrt{I}$.

c) $\sqrt{I + J} = \sqrt{\sqrt{I} + \sqrt{J}}$.

d) $\sqrt{\sqrt{I}} = \sqrt{I}$.

4.2. Részgyűrűk és ideálok hálója

Legyen $(R, +, \cdot)$ egy gyűrű. Bevezetjük a következő jelöléseket:

- $\mathcal{S}(R) = \{S \mid S \leq R\}$ az R gyűrű részgyűrűinek halmaza;
- $\mathcal{I}_b(R) = \{A \mid A \underset{b}{\trianglelefteq} R\}$ az R gyűrű balideáljainak halmaza;
- $\mathcal{I}_j(R) = \{A \mid A \underset{j}{\trianglelefteq} R\}$ az R gyűrű jobbideáljainak halmaza;
- $\mathcal{I}(R) = \{A \mid A \trianglelefteq R\}$ az R gyűrű ideáljainak halmaza.

4.2.1. tétel. *Az* $(\mathcal{S}(R), \subseteq)$, $(\mathcal{I}_b(R), \subseteq)$, $(\mathcal{I}_j(R), \subseteq)$, $(\mathcal{I}(R), \subseteq)$ *rendezett halmazok teljes hálók.*

Bizonyítás. Ideálok esetén bizonyítunk. A többi esetekben hasonlóan járunk el.

Alkalmazzuk a teljes hálók jellemzési tételét. Igazolnunk kell, hogy minden $(A_i)_{i \in I}$ ideálrendszernek van infimuma, azaz $\bigcap_{i \in I} A_i \trianglelefteq R$. A részcsoportokra vonatkozó megfelelő tulajdonságból következik, hogy $(\bigcap_{i \in I} A_i, +)$ részcsoportja $(R, +)$. Legyen $r \in \bigcap_{i \in I} A_i$ és $x \in R$; következik, hogy $r \in A_i$ minden $i \in I$-re. Mivel az A_i-k ideálok R-ben, $rx, xr \in A_i$ minden $i \in I$ esetén, vagyis $rx, xr \in \bigcap_{i \in I} A_i$. ■

4.2.2. definíció. Legyen R egy gyűrű.

a) Az $\langle X \rangle = \bigcap_{S \leq R, X \subseteq S} S$ részgyűrűt az X *által generált részgyűrűnek* nevezzük.

b) Az $(X) = \bigcap_{U \trianglelefteq R, X \subseteq U} U$ ideált az X *által generált ideálnak* nevezzük.

Ha $X = \{x\}$, akkor $(\{x\}) = (x)$ az x *által generált főideál.*

4.2.3. tétel. *Legyen* R *egy gyűrű és* $\emptyset \neq X \subseteq R$, *akkor:*

1) $\langle X \rangle = \{\sum_{\text{véges}} \pm x_1 \ldots x_n \mid n \in \mathbb{N}^*, x_i \in X, 1 \leq i \leq n\}$.

2) $(X) = RX + XR + RXR + X + (-X)$
$$= \{\textstyle\sum_{i=1}^{k} a_i x_i + \sum_{i=1}^{l} x_i' b_i + \sum_{i=1}^{m} a_i' x_i'' b_i' + \sum_{i=1}^{n} y_i \mid \\ a_i, b_i, a_i', b_i' \in R, \ x_i, \ x_i', \ x_i'' \in X, \ y_i \in X \bigcup (-X)\}.$$

3) *Ha* R *kommutatív gyűrű, akkor* $(X) = RX + X + (-X)$.

4) *Ha* R *kommutatív és egységelemes gyűrű, akkor* $(X) = RX$.

Bizonyítás. 1) Jelöljük S-sel az egyenlőségben szereplő jobb oldali halmazt. Igazolnunk kell, hogy $\langle X \rangle = S$. Ez azt jelenti, hogy S-nek teljesítenie kell a következőket: S részgyűrűje R-nek, X részhalmaza S-nek és R minden olyan S' részgyűrűje esetén, amelynek X részhalmaza, tartalmaznia kell S-et.

Bármely két S-beli összeg különbsége és szorzata S-ben van, tehát S részgyűrűje R-nek. Az S értelmezéséből következik, hogy $X \subseteq S$-nek. Ha S' egy, az S-től különböző részgyűrűje R-nek és $X \subseteq S'$-nek, akkor $S \subseteq S'$. Tehát S az R-nek azon legkisebb részgyűrűje, amely tartalmazza X-et.

2) Jelöljük T-vel az egyenlőségben szereplő jobb oldali halmazt. Igazolnunk kell, hogy $(X) = T$. Ez azt jelenti, hogy T-nek teljesítenie kell a következőket: T ideálja R-nek, X részhalmaza T-nek és R minden olyan T' ideálja esetén, amelynek X részhalmaza, tartalmaznia kell T-t. Az igazolás hasonló az 1)-es pontban végzett igazoláshoz.

3) Következik a 2)-es pontból.

4) Következik a 3)-as pontból. ■

4.2.4. következmény. 1) *Ha* $x \in R$, *akkor* $(x) = Rx + xR + RxR + \mathbb{Z}x$.
2) *Ha* R *kommutatív, akkor* $(x) = Rx + \mathbb{Z}x$.
3) *Ha* R *kommutatív és egységelemes, akkor* $(x) = Rx = \{rx \mid r \in R\}$.
4) *Ha* $U_i \trianglelefteq R$ *minden* $i \in I$ *esetén, akkor*

$$\inf\{U_i \mid i \in I\} = \bigcap_{i\in I} U_i;$$
$$\sup\{U_i \mid i \in I\} = (\bigcup_{i\in I} U_i) =: \sum_{i\in I} U_i$$
$$= \{a_{i_1} + a_{i_2} + \ldots + a_{i_n} \mid n \in \mathbb{N}^*;\ i_1, \ldots, i_n \in I,\ a_{i_k} \in U_{i_k}\}.$$

Két ideál esetén: ha $I, J \trianglelefteq R$, *akkor*

$$\inf(I, J) = I \cap J;$$
$$\sup(I, J) = I + J = \{a + b \mid a \in I, b \in J\}.$$

4.2.5. megjegyzés (Ideálok szorzata). Legyen I és J két ideál, és tekintsük a következő halmazt:

$$I \cdot J = \{ab \mid a \in I, b \in J\} \subseteq R.$$

Ez általában nem ideálja R-nek. Például, legyen $R = \mathbb{C}[X]$ és

$$I = (2, X) = \{2f + Xg \mid f, g \in \mathbb{C}[X]\} = \{2a_0 + a_1X + \ldots \mid a_i \in \mathbb{C}\} \trianglelefteq \mathbb{C}[X]$$
$$J = (3, X) = \{3f + Xg \mid f, g \in \mathbb{C}[X]\} = \{3a_0 + a_1X + \ldots \mid a_i \in \mathbb{C}\} \trianglelefteq \mathbb{C}[X].$$

Vegyük észre, hogy $2X, 3X \in I \cdot J$, de $5X = 2X + 3X \neq I \cdot J$.

Értelmezés szerint, legyen

$$IJ = \{\sum_{i=1}^{n} a_i b_i \mid n \in \mathbb{N}^*, a_i \in I, b_i \in J, i = 1, \ldots, n\};$$

ekkor IJ ideálja R-nek.

Valóban minden $a = \sum_{i=1}^{n} a_i b_i$ és $b = \sum_{j=1}^{n} a'_i b'_j \in IJ$ esetén $a - b \in IJ$. Ha $r \in R$, akkor $ra = \sum_{i=1}^{n} ra_i b_j \in IJ$ (mert $ra_i \in I$, mivel I ideál), hasonlóan $ar \in IJ$.

Fennáll az is, hogy $IJ \subseteq I \cap J$, mert $\sum_{i=1}^{n} a_i b_i \in I, J$.

4.2.6. tétel (Részgyűrűk és ideálok megfeleltetése). *Legyen* $f : R \to R'$ *gyűrűmorfizmus, és* $I := \operatorname{Ker} f$.
a) *Ha* A *részgyűrűje* $(R, +, \cdot)$*-nak, akkor* $f(A)$ *részgyűrűje* $(R', +, \cdot)$*-nak és*

$$f^{-1}(f(A)) = A + I.$$

Ha $A \trianglelefteq R$, *akkor* $f(A) \trianglelefteq f(R)$.
b) *Ha* A' *részgyűrűje* $(R', +, \cdot)$, *akkor* $f^{-1}(A')$ *részgyüje* $(R, +, \cdot)$*-nak. Ha* A' *ideálja* R*-nek, akkor* $f^{-1}(A')$ *ideálja* R*-nek.*
c) *Feltételezzük, hogy* f *szürjektív és legyen* $\mathcal{I} = \{A \trianglelefteq R \mid I \subseteq A\} \subseteq \mathcal{I}(R)$. *Továbbá, legyen*

$$\varphi : \mathcal{I} \longrightarrow \mathcal{I}(R'), \qquad \varphi(A) = f(A),$$

$$\psi : \mathcal{I}(R') \longrightarrow \mathcal{I}, \qquad \psi(A') = f^{-1}(A').$$

Ekkor φ *és* ψ *hálóizomorfizmusok, és* $\psi = \varphi^{-1}$.

Bizonyítás. a) Legyen A az $(R, +, \cdot)$-nak egy részgyűrűje. A csoportelméletből tudjuk, hogy $f(A)$ részcsoportja az $(R', +)$-nak és $f^{-1}(f(A)) = A + \operatorname{Ker} f$.

Minden $a' = f(a)$, $b' = f(b) \in f(A)$ esetén $a'b' = f(a)f(b) = f(ab)$ (mert f gyűrűmorfizmus). Feltevés szerint A részgyűrűje $(R, +, \cdot)$-nak, ezért minden $a, b \in A$ esetén $ab \in A$. Következik, hogy $a'b' = f(ab) \in f(A)$-nak.

Abban az esetben, ha A ideálja R-nek, minden $a' = f(a) \in f(A)$ és $r' = f(r) \in f(R)$ esetén $r'a' = f(r)f(a) = f(ra)$, $r'a' = f(r)f(a) = f(ra) \in f(A)$, mert $ra, ar \in A$.

b) Legyen A' részgyűrűje az $(R', +, \cdot)$-nak. A csoportelméletből következik, hogy $f^{-1}(A') = \{a \in R \mid f(a) \in A'\}$ részcsoportja $(R, +)$-nak.

Minden $a, b \in f^{-1}(A')$ esetén $ab \in f^{-1}(A')$-nek, mert $f(ab) = f(a)f(b) \in A'$.

Abban az esetben, ha A' ideálja R'-nek, minden $a \in f^{-1}(A')$ és $r \in R$ esetén $ra, ar \in f^{-1}(A')$, mert $f(ra) = f(r)f(a)$, $f(ar) = f(a)f(r) \in A'$.

c) Az a) és b) pontokból következik, hogy φ és ψ jól értelmezettek. A csoportelméletből következik, hogy φ és ψ bijektívek és növekvőek, vagyis $\psi = \varphi^{-1}$. ■

4.4. feladat (Mátrixgyűrű ideáljai). Legyen R egy egységelemes gyűrű, és

$$\phi : \mathcal{I}(R) \to \mathcal{I}(M_n(R)), \quad \phi(I) = M_n(I) = \{A = [a_{ij}] \mid a_{ij} \in I\}.$$

Igazoljuk, hogy ϕ hálóizomorfizmus.

Következmény: ha K test és $n \geq 2$, akkor $M_n(K)$ egyszerű gyűrű és nem test.

4.5. feladat. (X, n) főideálja $\mathbb{Z}[X]$-nek akkor és csak akkor, ha $n = 0, 1, -1$.

4.6. feladat. Ha K test, akkor $\mathcal{I}(K[[X]]) = \{(0), (X^n) \mid n \in \mathbb{N}\}$.

4.7. feladat. Legyen R egy gyűrű és $I, J, L \in \mathcal{I}(R)$. Igazoljuk, hogy:

a) $I \cup J$ ideál $\Leftrightarrow$ $I \subseteq J$ vagy $J \subseteq I$.

b) Ha R egységelemes gyűrű, $I + J = R$ és $I \supseteq JL$, akkor $I \supseteq L$; ha R kommutatív és $I + J = R$, akkor $IJ = I \cap J$.

c) $(I + J)(I \cap J) \subseteq IJ$.

4.3. Faktorgyűrű

4.3.1. Kongruenciarelációk

4.3.1. definíció. Legyen $(R, +, \cdot)$ egy gyűrű és ρ egy ekvivalenciareláció az R-en (jelölés: $\rho \in \mathcal{E}(R)$). Azt mondjuk, hogy ρ **kongruencia** R-en (jelölés: $\rho \in \mathcal{C}(R, +, \cdot)$), ha kompatibilis a műveletekkel, vagyis minden $a_1, a_2, b_1, b_2 \in R$ esetén

$$a_1 \rho\, b_1, \quad a_2 \rho\, b_2 \implies a_1 a_2 \rho\, b_1 b_1, \quad (a_1 + a_2) \rho\, (b_1 + b_2).$$

4.3.2. tétel (Ideálok és kongruenciák kapcsolata). a) *Legyen* I *egy ideálja* R*-nek és* $\rho_I \subseteq R \times R$*, amely a következőképpen van értelmezve: minden* $a, b \in R$ *esetén*

$$a \rho_I b \iff a - b \in I \overset{\text{jel.}}{\iff} a \equiv b \pmod{I}.$$

Akkor ρ_I *kongruencia* R*-en.*

b) *Legyen* ρ *az* R*-nek egy kongruenciarelációja. Akkor* $\rho\langle 0\rangle = \{a \in R \mid 0 \rho a\} \trianglelefteq R$.

c) *Legyen* $\varphi : \mathcal{I}(R) \longrightarrow \mathcal{C}(R)$, $\varphi(I) = \rho_I$ *és* $\psi : \mathcal{C}(R) \longrightarrow \mathcal{I}(R)$, $\psi(\rho) = \rho\langle 0\rangle$. *Akkor* φ *és* ψ *hálóizomorfizmusok, mitöbb* $\psi = \varphi^{-1}$.

Bizonyítás. a) Mivel $(R, +)$ Abel-csoport, következik, hogy I normális részcsoport, és csoportelméletből tudjuk, hogy $\rho_I \in \mathcal{C}(R, +)$.

Ha $a_1, a_2, b_1, b_2 \in R$ úgy, hogy $a_1 \rho_I b_1$ és $a_2 \rho_I b_2$, akkor a ρ_I reláció értelmezése szerint $b_1 - a_1 \in I$ és $b_2 - a_2 \in I$, vagyis $b_1 = a_1 + u_1$ és $b_2 = a_2 + u_2$, ahol $u_1, u_2 \in I$. Akkor $b_1 b_2 = (a_1 + u_1)(a_2 + u_2) = a_1 a_2 + a_1 u_2 + u_1 a_2 + u_1 u_2$ következik, hogy $b_1 b_2 - a_1 a_2 \in I$, mert $a_1 u_2 + u_1 a_2 + u_1 u_2 \in I$. A ρ_I értelmezése szerint $a_1 a_2 \rho_I b_1 b_2$.

b) Csoportelméletből tudjuk, hogy $\rho\langle 0\rangle$ részcsoportja $(R, +)$-nak. Minden $a \in \rho\langle 0\rangle$ és $r \in R$ esetén, $0 \rho a$ és $r \rho r$ (mert a reláció reflexív). Mivel ρ kongruencia R-en, $0 \rho r a$ és $0 \rho a r$, tehát $ra, ar \in \rho\langle 0\rangle$. A fentiekből következik, hogy $\rho\langle 0\rangle$ ideálja R-nek.

c) Az a) és b) pontokból következik, hogy φ és ψ jól értelmezettek. Csoportelméletből tudjuk, hogy φ és ψ növekvő, bijektív függvények és $\psi = \varphi^{-1}$. ■

Ha I ideálja R-nek, azt mondjuk, hogy ρ_I a *modulo* I *kongruenciareláció* .

4.3.3. példa. Ha $f : R \longrightarrow S$ egy gyűrűmorfizmus, akkor $\operatorname{Ker} f = \{r \in R \mid f(r) = 0\}$ ideálja R-nek. Minden $a, b \in R$ esetén

$$a \;\rho_{\operatorname{Ker} f}\; b \iff b - a \in \operatorname{Ker} f \iff a \;\ker f\; b,$$

mert f morfizmus. Ezért

$$(\ker f)\langle 0\rangle = \{a \in R \mid 0 \ker f a\} = \{a \in R \mid f(0) = 0 = f(a)\} = \operatorname{Ker} f.$$

4.3.2. Faktorgyűrű szerkesztése

Legyen I ideálja $(R, +, \cdot)$-nak, és tekintsük az $R/I = R/\rho_I = \{\rho_I\langle r\rangle \mid r \in R\}$ faktorhalmazt, ahol

$$\rho\langle r\rangle = r + I = \{r + a \mid a \in I\} =: [a]_I$$

az a osztálya modulo I.

Tudjuk, hogy $(R/I, +)$ Abel-csoport, ahol a művelet a következőképpen van értelmezve: $(r+I)+(s+I) = r+s+I$, és a $p_I : R \longrightarrow R/I$, $p_I(r) = r + I$ kanonikus projekció szürjektív csoportmorfizmus.

Értelmezés szerint, legyen $(r + I)(s + I) = rs + I$. Az értelmezés nem függ a reprezentánsoktól. Valóban, ha $r' = r+a \in r+I$ és $s' = s+b \in s+I$, akkor $(r'+I)(s'+I) = r's'+I = (r+a)(s+b)+I = rs+rb+as+ab+I = rs+I$.

A fenti szorzás asszociatív. Ha R-nek van egységeleme ($1 \in R$), akkor $1 + I$ egységelem az R/I-ben. Ha létezik $r^{-1} \in R$-ben, akkor $(r + I)^{-1} = r^{-1} + I$. Következik, hogy $(R/I, +, \cdot)$ gyűrű és $p_I : R \longrightarrow R/I$ szürjektív gyűrűmorfizmus. Vegyük észre, hogy

$$\begin{aligned}\operatorname{Ker} p_I &= \{r \in R \mid p_I(r) = I\} = \\ &= \{r \in R \mid r + I = 0 + I\} = \\ &= \{r \in R \mid r \in I\} = I.\end{aligned}$$

Az R/I gyűrűt R-nek az I szerinti **faktorgyűrű**jének nevezzük.

4.3.4. következmény (A faktorgyűrű részgyűrűi és ideáljai). *Ha* I *egy ideálja* R*-nek, akkor:*

$$\mathcal{S}(R/I, +, \cdot) = \{A/I \mid A \leq (R, +, \cdot), I \subseteq A\},$$

$$\mathcal{I}(R/I, +, \cdot) = \{J/I \mid J \trianglelefteq R, I \subseteq J\}.$$

Bizonyítás. Következik a 4.2.6. tételből. ■

4.3.3. Izomorfizmustételek

4.3.5. tétel (I. izomorfizmustétel). *Ha* $f : R \to S$ *gyűrűmorfizmus, akkor*

$$R/\operatorname{Ker} f \simeq \operatorname{Im} f.$$

Bizonyítás. Láttuk, hogy $\operatorname{Ker} f \trianglelefteq R$-nek és $\operatorname{Im} f = f(R) \leqslant S$. Csoportelméletből tudjuk, hogy

$$f^* : R/\operatorname{Ker} f \longrightarrow \operatorname{Im} f, \quad f^*(r + \operatorname{Ker} f) = f(r)$$

jól értelmezett, bijektív függvény, és csoportizomorfizmus (az „+”-ra nézve). Továbbá, minden $r, r' \in R$ esetén

$$\begin{aligned}f^*((r + \operatorname{Ker} f)(r' + \operatorname{Ker} f)) &= f^*(rr' + \operatorname{Ker} f) = \\ &= f(rr') = \\ &= f(r)f(r') = \\ &= f^*(r + \operatorname{Ker} f)f^*(r' + \operatorname{Ker} f),\end{aligned}$$

tehát f^* gyűrűizomorfizmus. ■

4.3.6. tétel (II. izomorfizmustétel). *Ha* R *egy gyűrű,* $A \leqslant (R, +, \cdot)$ *és* $I \trianglelefteq R$*, akkor*

$$(A + I)/I \simeq A/A \cap I.$$

Bizonyítás. Csoportelméletből tudjuk, hogy $A, I \leqslant (R, +)$, és g csoportmorfizmus, ahol

$$g : A/A \cap I \longrightarrow (A + I)/I, \quad g(a + A \cap I) = a + I.$$

Igazolni kell, hogy $A + I \leqslant (R, +, \cdot)$, $A \cap I \trianglelefteq A$, és g gyűrűmorfizmus.

Minden $a + u, b + v \in A + I$ esetén $(a + u)(b + v) = ab + av + ub + uv \in A + I$, tehát $A + I \leqslant R$. Minden $u \in I$ és $b + v \in A + I$ esetén $u(b + v) = ub + uv \in I$, tehát $I \trianglelefteq A + I$.

Mivel $A, I \leqslant (R, +)$ következik, hogy $A \cap I \leqslant (R, +)$. De $I \subseteq A$, ezért $A \cap I \trianglelefteq A$. Minden $a \in A$ és $w \in A \cap I$ esetén $aw, wa \in A \cap I$.

Végűl, minden $a_1 + A \cap I, a_2 + A \cap I \in A/A \cap I$ esetén

$$\begin{aligned}g((a_1 + A \cap I)(a_2 + A \cap I)) &= g(a_1a_2 + A \cap I) = \\ &= a_1a_2 + A \cap I = \\ &= (a_1 + I)(a_2 + I) = \\ &= g(a_1 + A \cap I)g(a_2 + A \cap I). \qquad ■\end{aligned}$$

4.3.7. tétel (III. izomorfizmustétel). *Ha* R *egy gyűrű,* $I, J \trianglelefteq R$ *és* $I \subseteq J$*, akkor*

$$(R/I)/(J/I) \simeq R/J.$$

Bizonyítás. Mivel $J/I \trianglelefteq (R/I, +, \cdot)$, létezik az $(R/I)/(J/I)$ faktorgyűrű. A csoportelmélet III. izomorfizmustételéből tudjuk, hogy

$$\varphi : R/I \longrightarrow R/J, \qquad \varphi(r + I) = r + J$$

szürjektív csoportmorfizmus és $\operatorname{Ker} f = J/I$, tehát $((R/I)/(J/I), +) \simeq (R/J, +)$.

Igazoljuk, hogy φ gyűrűmorfizmus. Valóban, minden $r_1 + I, r_2 + I \in R/I$ esetén

$$\begin{aligned}
\varphi((r_1 + I) + (r_2 + I)) &= \varphi(r_1 + r_2 + I) = \\
&= r_1 + r_2 + J = \\
&= r_1 + J + r_2 + J = \\
&= \varphi(r_1 + I) + \varphi(r_2 + I), \\
\varphi((r_1 + I)(r_2 + I)) &= \varphi(r_1 r_2 + I) = \\
&= r_1 r_2 + J = \\
&= (r_1 + J)(r_2 + J) = \\
&= \varphi(r_1 + I)\varphi(r_2 + I). \qquad \blacksquare
\end{aligned}$$

4.8. feladat. Alkalmazva az I. izomorfizmustételt, bizonyítsuk be, hogy:
a) $\mathbb{C} \simeq \mathbb{R}[X]/(X^2 + 1)$.
b) $\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}[X]/(X^2 - d)$.
c) $\mathbb{Q}(\sqrt[3]{p}) \simeq \mathbb{Q}[X]/(X^3 - p)$.
d) $\mathbb{Z}[X]/(n, X) \simeq \mathbb{Z}_n$.

4.3.4. Modulo n maradékosztályok gyűrűje

Legyen $(\mathbb{Z}, +, \cdot)$ az egész számok gyűrűje. Láttuk, hogy $\mathcal{I}(\mathbb{Z}) = \{n\mathbb{Z} \mid n \in \mathbb{N}\}$, ahol $n\mathbb{Z} = \{nk \mid k \in \mathbb{Z}\} = (n)$ az n által generált főideál. Vegyük észre, hogy

$$a + n\mathbb{Z} = b + n\mathbb{Z} \Longleftrightarrow b - a \in n\mathbb{Z} \Longleftrightarrow a \equiv b \pmod{n}$$

Következik, hogy a $\mathbb{Z}_n$ modulo n maradékosztályok gyűrűje megegyezik a $\mathbb{Z}/n\mathbb{Z}$ faktorgyűrűvel, tehát

$$\mathbb{Z}_n = \mathbb{Z}/n\mathbb{Z} = \{\hat{a} \mid a \in \mathbb{Z}\},$$

ahol $\hat{a} = a + n\mathbb{Z} = \{a + nk \mid a \in \mathbb{Z}\}$ az a osztálya modulo n. Az $[a]_n := a + n\mathbb{Z}$ jelölést is fogjuk használni.

Partikulárisan, ha $n = 0$, akkor $\hat{a} = \{a\}$ és $\mathbb{Z}_0 = \{\{a\} \mid a \in \mathbb{Z}\} \simeq \mathbb{Z}$, és ha $n = 1$, akkor $\hat{a} = a + \mathbb{Z} = \mathbb{Z}$ és $\mathbb{Z}_1 = \{\mathbb{Z}\} = \{\hat{0}\}$.

A továbbiakban legyen $n \geq 2$. Ekkor

$$a \equiv b \pmod{n} \Leftrightarrow a \mod n = b \mod n,$$

tehát

$$\mathbb{Z}_n = \{\hat{0}, \hat{1}, \ldots, \widehat{n-1}\}$$

egy n elemű halmaz.

A $\mathbb{Z}_n$ halmazon értelmezzük a következő műveleteket:

$$\hat{a} + \hat{b} = \widehat{a + b}, \qquad \hat{a}\hat{b} = \widehat{ab},$$

minden $a, b \in \mathbb{Z}$ esetén. Az előző paragrafusok eredményeiből következik, hogy a fenti definiciók nem függnek a reprezentánsoktól és $(\mathbb{Z}_n, +, \cdot)$ kommutatív egységelemes gyűrű.

Könnyen belátható, hogy ha $(a, n) = 1$, akkor $\hat{a}$ invertálható $\mathbb{Z}_n$-ben, és ha $(a, n) = d > 1$, akkor $\hat{a}$ zérusosztó; következik, hogy ha p prímszám, akkor $\mathbb{Z}_p$ test, és ha n nem prímszám, akkor $\mathbb{Z}_n$ nem integritástartomány.

A $\varphi : \mathbb{N}^* \longrightarrow \mathbb{N}$, $\varphi(n) = |\{a \in \mathbb{N} \mid 0 \leq a < n, (a, n) = 1\}| = |U(\mathbb{Z}_n)|$ függvényt **Euler-függvény**nek nevezzük.

4.9. feladat. a) Készítsük el az $\mathcal{I}(\mathbb{Z}_{12})$, $\mathcal{I}(\mathbb{Z}_{30})$, $\mathcal{I}(\mathbb{Z}_{24})$ hálók Hasse-diagramját.
b) Határozzuk meg n-et, ha $(\mathcal{I}(\mathbb{Z}_n), \subseteq)$ teljesen rendezett halmaz.

4.10. feladat. Legyen $n = p_1^{a_1} \cdots p_r^{a_r}$ egy természetes szám és $A = \{p_1, \dots, p_r\}$. Igazoljuk, hogy létezik egy $\phi : \mathrm{Idemp}(\mathbb{Z}_n) \to \mathcal{P}(A)$ bijektív függvény.

Alkalmazás: Határozzuk meg a $\mathbb{Z}_{12}$ és $\mathbb{Z}_{360}$ idempotenseit.

4.11. feladat. a) Hány $f : \mathbb{Z} \to \mathbb{Z}_n$ gyűrűmorfizmus létezik? Határozzuk meg az $f : \mathbb{Z} \to \mathbb{Z}_{360}$ morfizmusokat.

b) Határozzuk meg az $f : \mathbb{Z}_n \to \mathbb{Z}_m$ morfizmusokat.

c) Határozzuk meg a $(\mathbb{Z}_n, +, \cdot)$ endomorfizmusait és automorfizmusait.

4.12. feladat. Igazoljuk, hogy $\mathbb{Z}_n$-ben akkor és csak akkor léteznek nemnulla nilpotens elemek, ha n négyzetmentes. Határozzuk meg az $r(\mathbb{Z}_n)$ számosságát.

4.4. Gyűrűk direkt szorzata

Legyenek $R_1, \dots, R_n$ gyűrűk, és tekintsük az $R := R_1 \times \cdots \times R_n$ gyűrűt, ahol ha $r = (r_1, \dots, r_n)$, $r' = (r'_1, \dots, r'_n) \in R$, akkor értelmezés szerint,

$$r + r' = (r_1 + r'_1, \dots, r_n + r'_n), \qquad rr' = (r_1 r'_1, \dots, r_n r'_n).$$

Legyen $p_i : R \to R_j$, $p_i(r_1, \dots, r_n) = r_i$ a **kanonikus projekció**, $1 \le i \le n$.

Az $(R, (p_i)_{1 \le i \le n})$ párt az $R_1, \dots, R_n$ gyűrűk **direkt szorzatának** nevezük.

Könnyen igazolható, hogy:

- p_i szürjektív gyűrűmorfizmus.
- minden i esetén R_i beágyazható R-be, azaz

$$R_i \simeq \{0\} \times \cdots \times \{0\} \times R_i \times \{0\} \times \cdots \times \{0\} \le R.$$

- R egységelemes gyűrű $\Leftrightarrow$ R_i egységelemes gyűrűk, $i = 1, \dots, n$.
- Ha R egységelemes, akkor $U(R) = U(R_1) \times \cdots \times U(R_n)$, azaz $r = (r_1, \dots, r_n)$ invertálható R-ben $\Leftrightarrow$ r_i invertálható R_i-ben, $i = 1, \dots, n$.

4.13. feladat. Ha $R_i \simeq S_i$ izomorf gyűrűk, $i = 1, \dots, n$, akkor $R_1 \times \cdots \times R_n \simeq S_1 \times \cdots \times S_n$.

4.14. feladat. Legyenek $R_1, \dots, R_n$ gyűrűk, és $R = R_1 \times \cdots \times R_n$. Igazoljuk, hogy:

a) Ha R_i egységelemes gyűrű, $i = 1, \dots, n$, akkor

$$\mathcal{I}(R) = \{I_1 \times \cdots \times I_n \mid I_i \trianglelefteq R_i,\ i = 1, \dots, n\}.$$

b) $\mathbb{Z} \times \mathbb{Z}$-nek van olyan részgyűrűje amely nem ideál.

c) Ha $I_i \trianglelefteq R_i$ és $I = I_1 \times \cdots \times I_n$, akkor $R/I = R_1/I_1 \times \cdots \times R_n/I_n$.

4.15. feladat (A kínai maradéktétel általánosítása). Legyen R egy gyűrű és $I_1, \dots, I_n \trianglelefteq R$ úgy, hogy $I_i + I_j = R$ ha $i \ne j$. Igazoljuk, hogy

$$R/I_1 \cap \cdots \cap I_n \simeq R/I_1 \times \cdots \times R/I_n.$$

4.16. feladat. Legyen R egy egységelemes gyűrű, $e_1, \dots, e_n \in Z(R)$ idempotens elemek úgy, hogy $e_1 + \cdots + e_n = 1$ és $e_i e_j = 0$ ha $i \ne j$. Bizonyítsuk be, hogy:

a) $e_i R \trianglelefteq R$ és $(e_i R, +, \cdot)$ egységelemes gyűrű.

b) $R \simeq e_1 R \times \cdots \times e_n R$.

c) Ha $R \simeq R_1 \times \cdots \times R_n$, akkor léteznek $e_i \in Z(R)$ idempotensek, $\sum e_i = 1$, $e_i e_j = 0$ ha $i \ne j$, úgy, hogy $R_i \simeq e_i R$.

Alkalmazás: Szerkesszük meg a $\mathbb{Z}_6$ és Z_{15} felbontásait idempotensek segítségével.

4.5. Prímtest. Test karakterisztikája

Legyen $(K, +, \cdot)$ egy test. Ha K_i részteste $(K, +, \cdot)$-nak minden $i \in I$ esetén, akkor könnyen belátható, hogy $\bigcap_{i \in I} K_i$ is részteste K-nak. Következik, hogy létezik K-nak egy legkisebb részteste: $P(K) = \bigcap_{L \le K} L$.

4.5.1. definíció. a) A $P(K)$ résztestet a K test **prímrésztest**ének nevezzük.

b) Ha $P(K) = K$, akkor a K testet **prímtest**nek nevezzük.

4.5.2. tétel (Prímrésztest jellemzése). *Ha* $(K, +, \cdot)$ *egy test, akkor*

$$P(K) = \langle 1 \rangle = \{(m \cdot 1)(n \cdot 1)^{-1} \mid m, n \in \mathbb{Z},\ n \cdot 1 \neq 0 \ \ K\text{-ban}\},$$

(*ahol* $\langle 1 \rangle$ K*-nak az* 1*-es által generált részteste*).

Bizonyítás. Jelöljük L-lel az $\{(m \cdot 1)(n \cdot 1)^{-1} \mid m, n \in \mathbb{Z},\ n \cdot 1 \neq 0 \ \ K\text{-ban}\}$ halmazt. Igazolnunk kell, hogy $1 \in L$, L részteste K-nak és L a legkisebb részteste K-nak; $1 \in L$ evidens, mert $1 = 1 \cdot 1^{-1}$. Igazoljuk, hogy $L \leq K$-nak, alkalmazva a résztestek jellemzési tételét: $L \neq \emptyset$, mert $0, 1 \in L$ és minden $a = (m \cdot 1)(n \cdot 1)^{-1}, b = (p \cdot 1)(q \cdot 1)^{-1} \in L$ esetén (ahol $m, n, p, q \in \mathbb{Z}$), $a - b = ((mq - np) \cdot 1)((nq) \cdot 1)^{-1} \in L$, $ab = ((mp) \cdot 1)((nq) \cdot 1)^{-1} \in L$ és, ha $a \neq 0$, akkor $a^{-1} = (n \cdot 1)(m \cdot 1)^{-1} \in L$.

Ha $L' \leq K$, akkor $1 \in L'$ és minden $m, n \in \mathbb{Z}$ esetén $m \cdot 1, n \cdot 1 \in L'$. De L' test, tehát $(m \cdot 1)(n \cdot 1)^{-1} \in L'$. Ha $n \cdot 1 \neq 0$ K-ban, akkor $L \leq L'$. ■

4.5.3. példa. a) A $(\mathbb{Q}, +, \cdot)$ test prímtest, mert $\mathbb{Q} = \{mn^{-1} \mid m, n \in \mathbb{Z}, n \neq 0\} = P(\mathbb{Q})$.

b) Ha p prímszám, akkor $(\mathbb{Z}_p, +, \cdot)$ prímtest, mert $\mathbb{Z}_p = \{n\hat{1} \mid n = 0, 1, \ldots, p-1\} = P(\mathbb{Z}_p)$.

4.5.4. definíció. Legyen $(R, +, \cdot)$ egységelemes gyűrű. Tekintsük az $(R, +)$ additív csoportban az $1 \in R$ elem rendjét (jelölés: $\mathrm{ord}(1)$).

Ha $\mathrm{ord}(1) = n \in \mathbb{N}^*$, akkor azt mondjuk, hogy az R gyűrű **karakterisztikája** n (jelölés: $\mathrm{char}(R) = n$).

Ha $\mathrm{ord}(1) = \infty$, akkor azt mondjuk, hogy az R gyűrű **karakterisztikája** 0 (jelölés: $\mathrm{char}(R) = 0$)).

4.5.5. lemma. *Ha* R *egy zérusosztómentes gyűrű, akkor az* R *karakterisztikája* 0 *vagy* p*, ahol* p *egy prímszám.*

Bizonyítás. Feltételezzük, hogy $\mathrm{char}(R) \neq 0$. Következik, hogy létezik $n \in \mathbb{N}^*$ úgy, hogy $\mathrm{char}(R) = n$. Ha $n = rs$ úgy, hogy $r, s \geq 2$, akkor $0 = n1 = (r1)(s1)$, de $r1 \neq 0$ és $s1 \neq 0$, vagyis R-ben vannak zérusosztók. ■

4.5.6. tétel (Prímtestek osztályozása). *Legyen* K *egy test.*

a) *Ha a* K *karakterisztikája* p*,* $p > 0$ *prímszám, akkor* $P(K)$ *izomorf* $\mathbb{Z}_p$*-vel.*

b) *Ha a* K *karakterisztikája* 0*, akkor* $P(K)$ *izomorf* $\mathbb{Q}$*-val.*

Bizonyítás. a) Mivel $\mathrm{char}(K) = p$ következik, hogy $\mathrm{ord}(1) = p$ a $(K, +)$ csoportban. Legyen $\varphi : \mathbb{Z} \longrightarrow K$, $\varphi(n) = n1$, ahol $1 \in K$, és igazoljuk, hogy φ unitér gyűrűmorfizmus:

$$\begin{aligned} \varphi(n + m) &= (n + m)1 = n1 + m1 = \varphi(n) + \varphi(m); \\ \varphi(nm) &= (nm)1 = (n1)(m1) = \varphi(n)\varphi(m); \\ \varphi(1) &= 1. \end{aligned}$$

Mivel $\mathrm{ord}(1) = p$, következik, hogy $\mathrm{Ker}\, f = \{n \in \mathbb{Z} \mid n1 = 0\} = \{n \in \mathbb{Z} \mid p|n\} = p\mathbb{Z}$, tehát $\mathbb{Z}/\mathrm{Ker}\, f = \mathbb{Z}_p$. Létezik $\varphi^* : \mathbb{Z}_p \longrightarrow K$, $\varphi^*(\hat{n}) = n1$ unitér morfizmus, következik, hogy φ^* injektív morfizmus. De $\mathrm{Im}\, \varphi^* = \{n1 \mid n \in \mathbb{Z}\} = P(K)$, tehát $\mathbb{Z}_p$ izomorf $P(K)$-val.

b) Legyen $\varphi : \mathbb{Q} \longrightarrow K$ úgy, hogy $\varphi(m/n) = \{(m1)(n1)^{-1} \mid m, n \in \mathbb{Z}\}$. Igazoljuk, hogy φ jól értelmezett függvény. Feltételezzük, hogy $m/n = r/s$, vagyis $ms = rn$. Felírjuk úgy, hogy $(m1)(s1) = (n1)(r1)$, szorzunk jobbról $(s1)^{-1}$-gyel és balról $(n1)^{-1}$-gyel; következik, hogy $(m1)(n1)^{-1} = (r1)(s1)^{-1}$, vagyis $\varphi(m/n) = \varphi(r/s)$.

Igazoljuk, hogy φ injektív testmorfizmus. Valóban, minden $m/n, r/s \in \mathbb{Q}$ esetén

$$\begin{aligned} \varphi(m/n + r/s) &= \varphi((ms + rn)/(ns)) = \\ &= ((ms + rn)1)((ns)1)^{-1} = \\ &= (ms1 + rn1)(ns1)^{-1} = \\ &= (ms1)(ns1)^{-1} + (rn1)(ns1)^{-1} = \\ &= (m1)(n1)^{-1} + (r1)(s1)^{-1} = \\ &= \varphi(m/n) + \varphi(r/s) \\ \varphi(m/n \cdot r/s) &= \varphi((mr)/(ns)) = \\ &= ((mr)1)((ns)1)^{-1} = \\ &= ((m1)(r1))((n1)(s1))^{-1} = \\ &= \varphi(m/n) \cdot \varphi(r/s) \end{aligned}$$

Ha $\varphi(m/n) = 0$ következik, hogy $m/n = 0$, vagyis φ injektív.

Mivel $\mathrm{Im}\, f = \{(m1)(n1)^{-1} \mid m, n \in \mathbb{Z}, n \neq 0\} = P(K)$, következik, hogy $\mathbb{Q}$ izomorf $P(K)$-val. ■

4.5.7. tétel (Frobenius-endomorfizmus). *Legyen* K *egy test, és legyen* $\varphi : K \to K$, $\varphi(x) = x^p$, *ahol* $p = \operatorname{char} K$, *ha* $\operatorname{char} K > 0$, *vagy* $p = 1$ *ha* $\operatorname{char} K = 0$.

Akkor ϕ *injektív testmorfizmus.*

Bizonyítás. Ha $\operatorname{char} K = 0$, akkor $\varphi = 1_k$, ahonnan következik, hogy φ automorfizmus.

Ha $\operatorname{char} K = p \neq 0$, akkor p prím, ahonnan következik, hogy $C_p^k = \frac{p!}{k!(p-k)!}$ $(1 < k < p)$ osztható p-vel. Tehát alkalmazva a Newton binomiális formulát, kapjuk: $(x_1 + x_2)^p = x_1^p + x_2^p$ vagyis $\varphi(x_1 + x_2) = \varphi(x_1) + \varphi(x_2)$ minden $x_1, x_2 \in K$ elemre.

Ezenkivül, mivel $x_1x_2 = x_2x_1$ kapjuk, hogy $\varphi(x_1x_2) = (x_1x_2)^p = x_1^px_2^p = \varphi(x_1)\varphi(x_2)$. Tehát φ endomorfizmus.

Mivel $\varphi(1) = 1$ következik, hogy $\operatorname{Ker}\varphi \neq k$, ahonnan kapjuk, hogy $\operatorname{Ker}\varphi = 0$. Tehát a φ endomorfizmus injektív. ■

4.17. feladat. Legyen R egy egységelemes gyűrű. Igazoljuk, hogy létezik egyetlen olyan $n \in \mathbb{N}$ amelyre létezik $f : \mathbb{Z}_n \to R$ injektív unitér morfizmus.

4.6. Hányadosgyűrűk

Tekintsük a következő feladatokat:

A. Ha $(G, \cdot)$ egy kommutatív félcsoport, szerkesszünk egy $(G', \cdot)$ csoportot úgy, hogy G részfélcsoportja legyen G'-nek.

B. Ha $(A, +, \cdot)$ egy kommutatív gyűrű, szerkesszünk egy $(K, +, \cdot)$ testet úgy, hogy az A részgyűrűje legyen K-nak.

Például $(\mathbb{N}, +)$ részfélcsoportja $(\mathbb{Z}, +)$-nak és $(\mathbb{Z}, +, \cdot)$ részfélcsoportja $(\mathbb{Q}, +, \cdot)$-nak.

A. Hányadosfélcsoport

4.6.1. megjegyzés. Legyen G' egy kommutatív csoport és G egy részfélcsoportja G'-nek. Ekkor tudjuk, hogy minden $h \in G, g_1, g_2 \in G'$ esetén $hg_1 = hg_2$-ből következik, hogy $g_1 = g_2$.

Általában, ha G egy kommutatív félcsoport és $h \in H$ úgy, hogy minden $g_1, g_2 \in G$ esetén

$$hg_1 = hg_2 \Longrightarrow g_1 = g_2,$$

akkor a h elemet *reguláris*nak nevezzük.

4.6.2. tétel (A hányadosfélcsoport szerkesztése). *Ha* $(G, \cdot)$ *egy kommutatív félcsoport és* $H \neq \emptyset$ *részfélcsoportja* G*-nek úgy, hogy a* H *elemei regulárisak, akkor létezik egy* $(G_H, \cdot)$ *kommutatív monoid és egy* $i_H : G \longrightarrow G_H$ *injektív morfizmus úgy, hogy minden* $h \in H$ *esetén* $i_H(h)$ *invertálható* G_H*-ban.*

Bizonyítás. $(G \times H, \cdot)$ félcsoport, ahol

$$(g, h)(g', h') = (gg', hh')$$

minden $(g, h), (g'h') \in G \times H$ esetén. $G \times H$-n értelmezzük a következő relációt:

$$(g_1, h_1) \sim (g_2, h_2) \Longleftrightarrow g_1h_2 = g_2h_1,$$

és igazoljuk, hogy $\sim$ ekvivalenciareláció.

Reflexivitás: $(g, h) \sim (g, h)$, mert $gh = gh$.

Tranzitivitás: Ha $(g_1, h_1) \sim (g_2, h_2)$ és $(g_2, h_2) \sim (g_3, h_3)$, akkor $g_1h_2 = g_2h_1$ és $g_2h_3 = g_3h_2$; következik, hogy $g_1h_2h_3 = g_2h_1h_3 = g_3h_2h_3$. De a H elemei regulárisak, ezért $g_1h_3 = g_3h_1$, vagyis $(g_1, h_1) \sim (g_3, h_3)$.

Szimmetria: Ha $(g_1, h_1) \sim (g_2, h_2)$, akkor $g_1h_2 = g_2h_1$, $g_2h_1 = g_1h_2$, tehát $(g_2, h_2) \sim (g_1, h_1)$.

Továbbá, igazoljuk, hogy $\sim$ kongruenciareláció (azaz kompatibilis a „$\cdot$”-tal) a $G \times H$ félcsoporton. Valóban, ha $(g_1, h_1) \sim (g_2, h_2)$ és $(g_1', h_1') \sim (g_2', h_2')$, akkor $g_1h_2 = g_2h_1$ és $g_1'h_2' = g_2'h_1'$, tehát $g_1g_1'h_2h_2' = g_2g_2'h_1h_1'$ vagyis $(g_1g_1', h_1h_1') \sim (g_2g_2', h_2h_2')$.

Tekintsük a

$$G_H = G \times H/\sim = \{\widetilde{(g, h)} \mid (g, h) \in G \times H\}$$

faktorhalmazt, ahol

$$\widetilde{(g, h)} = \{(g', h') \mid (g, h) \sim (g', h')\},$$

és értelmezzük a következő szorzatot:

$$(\widetilde{g_1, h_1})(\widetilde{g_2, h_2}) = (\widetilde{g_1g_2, h_1h_2}).$$

A fenti értelmezés nem függ a reprezentánsoktól, mert „$\sim$” kongruencia reláció, és $(G_H, \cdot)$ kommutatív félcsoport, mert $(G \times H)$ kommutatív félcsoport. Minden $h \in H$ esetén $\widetilde{(h,h)} \in G_H$ és

$$\widetilde{(g,h')}\widetilde{(h,h)} = \widetilde{(gh,hh')} = \widetilde{(g,h')},$$

tehát $\widetilde{(h,h)}$ semleges elem és G_H monoid.

Legyen

$$i_H : G \longrightarrow G_H, \quad i_H(g) = \widetilde{(gh,h)}$$

és igazoljuk, hogy i_H injektív morfizmus:

$$i_H(g_1g_2) = \widetilde{(g_1g_2h,h)} = \widetilde{(g_1hg_2h,h^2)} = \widetilde{(g_1h,h)}\widetilde{(g_2h,h)} = i_H(g_1)i_H(g_2);$$

i_H injektív, mert minden $g_1, g_2 \in G$ esetén, ha $i_H(g_1) = i_H(g_2)$, akkor $\widetilde{(g_1h,h)} = \widetilde{(g_2h,h)}$, $g_1hh = g_2hh$, tehát $g_1 = g_2$.

Igazolnunk kell még, hogy minden $h \in H$ esetén $i_H(h)$ invertálható. Valóban, mivel $i_H(h) = \widetilde{(h^2,h)}$, fennáll, hogy

$$\widetilde{(h^2,h)}\widetilde{(h,h^2)} = \widetilde{(h^3,h^3)} = \widetilde{(h,h)},$$

tehát $i_H(h)^{-1} = \widetilde{(h,h^2)}$. ■

4.6.3. megjegyzés. a) Minden $\widetilde{(g,h)} \in G_H$ esetén

$$\widetilde{(g,h)} = i_H(G) \cdot i_H(h)^{-1}.$$

Valóban, alkalmazzuk az i_H értelmezését:

$$i_H(g) \cdot i_H(g)^{-1} = \widetilde{(gh,h)}\widetilde{(h,h^2)} = \widetilde{(gh^2,h^3)} = \widetilde{(g,h)}.$$

b) Ha G-nek minden eleme reguláris és $H = G$, akkor $(G_G, \cdot)$ kommutatív csoport.

c) Értelmezés szerint, az egész számok csoportja $(\mathbb{Z}, +) = (\mathbb{N}_{\mathbb{N}}, +)$.

4.6.4. definíció. a) G_H-t G-*nek a* H *szerinti hányadosfélcsoportjának* nevezzük, G_G pedig G-nek a **hányadoscsoportja**.

b) Az $i_H : G \longrightarrow G_H$ injektív morfizmust *kanonikus injekciónak* nevezzük.

B. Hányadosgyűrű

4.6.5. definíció. Ha $(A, +, \cdot)$ egy kommutatív gyűrű és $\emptyset \neq S \subseteq A$ úgy, hogy S részfélcsoportja az $(A, \cdot)$ félcsoportnak, akkor S-et **multiplikatív zárt rendszer**nek nevezzük.

Vegyük észre, hogy az $s \in S$ elem akkor és csak akkor reguláris, ha nem zérusosztó.

Feltételezzük, hogy S egy multiplikatív zárt rendszer, amelynek elemei regulárisak. Ekkor létezik az $(A_S, \cdot)$ monoid, ahol

$$A_S = \{\widetilde{(a,s)} \mid (a,s) \in A \times S\}$$

és az

$$i_S : A \to A_S, \quad i_S(a) = \widetilde{(as,s)}$$

függvény injekív félcsoportmorfizmus.

4.6.6. tétel (A hányadosgyűrű szerkesztése). *Az* $(A_S, \cdot)$ *kommutatív monoidon értelmezhető egyetlen „+” művelet úgy, hogy* $(A_S, +, \cdot)$ *egysgelemes kommutatív gyűrű, és* $i_S : A \longrightarrow A_S$ *injektív gyűrűmorfizmus legyen.*

Bizonyítás. Egyértelműség: Feltételezzük, hogy létezik a “ + " művelet úgy, hogy i_S gyűrűmorfizmus. Ekkor

$$\begin{aligned}\widetilde{(a_1,s_1)} + \widetilde{(a_2,s_2)} &= i_S(a_1)i_s(s_1)^{-1} + i_S(a_2)i_S(s_2)^{-1} = \\ &= i_S(a_1)i_S(s_2)i_s(s_1)^{-1}i_S(s_2)^{-1} + i_S(a_2)i_S(s_1)i_S(s_1)^{-1}i_S(s_2)^{-1} = \\ &= i_S(a_1s_2 + a_2s - 1)i_S(s_1s_2)^{-1} = \\ &= \widetilde{(a_1s_2 + a_2s_1, s_1s_2)}\end{aligned}$$

egyértelműen meghatározott, minden $\widetilde{(a_1, s_1)}, \widetilde{(a_2, s_2)} \in A_S$ esetén.

Létezés: definíció szerint, legyen

$$\widetilde{(a_1, s_1)} + \widetilde{(a_2, s_2)} = \widetilde{(a_1 s_2 + a_2 s_1, s_1 s_2)}.$$

Igazoljuk, hogy „+" jól értelmezett: valóban, ha $(a_1, s_1) \sim (a_1', s_1')$ (azaz $a_1 s_1' = a_1' s_1$) és $(a_2, s_2) \sim (a_2', s_2')$ (azaz $a_2 s_2' = a_2' s_2$) akkor könnyen belátható hogy $(a_1 s_2 + a_2 s_1, s_1 s_2) \sim (a_1' s_2' + a_2' s_1', s_1' s_2')$.

Tudjuk, hogy $(A_S, \cdot)$ kommutatív monoid és igazoljuk, hogy $(A_S, +, \cdot)$ gyűrű.

Asszociativitás: minden $\widetilde{(a_1, s_1)}, \widetilde{(a_2, s_2)}, \widetilde{(a_3, s_3)} \in A_S$ esetén

$$\begin{aligned}
(\widetilde{(a_1, s_1)} + \widetilde{(a_2, s_2)}) + \widetilde{(a_3, s_3)} &= (\widetilde{(a_1 s_2 + a_2 s_1, s_1 s_2)}) + \widetilde{(a_3, s_3)} = \\
&= \widetilde{((a_1 s_2 + a_2 s_1, s_1 s_2) s_3 + a_3 (s_1 s_2), (s_1 s_2) s_3)} = \\
&= \widetilde{((a_1 s_2 s_3 + a_2 s_1 s_3 + a_3 s_1 s_2, s_1 s_2 s_3)};\\
\widetilde{(a_1, s_1)} + (\widetilde{(a_2, s_2)} + \widetilde{(a_3, s_3)}) &= \widetilde{(a_1, s_1)} + \widetilde{(a_2 s_3 + a_3 s_2, s_2 s_3)} = \\
&= \widetilde{(a_1 (s_1 s_3) + s_1 (a_2 s_3 + a_3 s_2), s_1 (s_2 s_3)} = \\
&= \widetilde{(a_1 s_1 s_3 + s_1 a_2 s_3 + s_1 a_3 s_2, s_1 s_2 s_3)}.
\end{aligned}$$

Kommutativitás: minden $\widetilde{(a_1, s_1)}, \widetilde{(a_2 s_2)} \in A_S$ esetén

$$\begin{aligned}
\widetilde{(a_1, s_1)} + \widetilde{(a_2, s_2)} &= \widetilde{(a_1 s_2 + a_2 s_1, s_1 s_2)} = \\
&= \widetilde{(a_2 s_1 + a_1 s_2, s_2 s_1)} = \\
&= \widetilde{(a_2, s_2)} + \widetilde{(a_1, s_1)}.
\end{aligned}$$

Semleges elem: vegyük észre, hogy $\widetilde{(0, s)} = \{(0, t) \mid t \in S\} \in A_S$ és minden $\widetilde{(a, t)}$ esetén

$$\widetilde{(a, t)} + \widetilde{(0, s)} = \widetilde{(a, t)}.$$

Ellentett elem: Minden $\widetilde{(a, s)} \in A_S$ esetén létezik $-\widetilde{(a, s)} = \widetilde{(-a, s)} \in A_S$ úgy, hogy

$$\widetilde{(a, s)} + \widetilde{(-a, s)} = \widetilde{(0, s)}.$$

Disztributivitás: minden $(\widetilde{(a_1, s_1)}, \widetilde{(a_2, s_2)}$ és $\widetilde{(b, t)} \in A_S$ esetén

$$\begin{aligned}
(\widetilde{(a_1, s_1)} + \widetilde{(a_2, s_2)})\widetilde{(b, t)} &= \widetilde{(a_1 s_2 + a_2 s_1, s_1 s_2)}\widetilde{(b, t)} = \\
&= \widetilde{(a_1 s_2 b + a_2 s_1 b, s_1 s_2 t)};\\
\widetilde{(a_1, s_1)}\widetilde{(b, t)} + \widetilde{(a_2, s_2)}\widetilde{(b, t)} &= \widetilde{(a_1 b s_2 t + s_2 t a_2 b, s_1 t s_2 t)}.
\end{aligned}$$

Végűl, tudjuk, hogy $i_S : A \to A_S$ injektív félcsoportmorfizmus igazolni kell, hogy i_S additív:

$$\begin{aligned}
i_S(a_1 + a_2) &= \widetilde{((a_1 + a_2) s, s)},\\
i_S(a_1) + i_S(a_2) &= \widetilde{(a_1 s, s)} + \widetilde{(a_2 s, s)} = \\
&= \widetilde{(a_1 s^2 + a_2 s^2, s^2)} = \\
&= \widetilde{((a_1 + a_2) s^2, s^2)} = \\
&= \widetilde{((a_1 + a_2) s, s)}. \qquad \blacksquare
\end{aligned}$$

4.6.7. megjegyzés. a) Gyakran a következő jelöléseket használjuk:

$$\frac{a}{s} = \widetilde{(a, s)}, \quad S^{-1}A = A_S = \{\frac{a}{s} \mid a \in A,\ s \in S\}.$$

Vegyük észre, hogy $\frac{a}{s} + \frac{b}{t} = \frac{at+bs}{st}$, $\frac{a}{s} \cdot \frac{b}{t} = \frac{ab}{st}$ és $i_S(a) = \frac{as}{s}$.

b) Ha A integritástartomány és $S = A^*$, akkor S multiplikatív zárt rendszer és $A_S = S^{-1}A$ kommutatív test. Ebben az esetben $S^{-1}A$-t az A **hányadostest**ének nevezzük. Jelölés: $S^{-1}A = K(A) = \mathrm{frac}(A)$.

c) Értelmezés szerint, a *racionális számok teste*

$$(\mathbb{Q}, +, \cdot) = (\mathbb{Z}_{\mathbb{Z}^*}, +, \cdot) = \{a/b \mid a, b \in \mathbb{Z}, b \neq 0\}.$$

d) Ha K kommutatív test, akkor $K[X_1, \ldots, X_n]$ integritástartomány, és

$$K(X_1, \ldots, X_n) := \mathrm{frac}(K[X_1, \ldots, X_n]) = \{f/g \mid f, g \in A[X_1, \ldots, X_n]\}$$

a racionális törtek teste.

4.6.8. tétel. (A hányadosgyűrű univerzális tulajdonsága) *Az* $(S^{-1}A, i_S)$ *elempár rendelkezik a következő univerzális tulajdonsággal: minden* B *kommutatív egységelemes gyűrű esetén, és minden* $f : A \to B$ *unitér gyűrűmorfizmus esetén, amelyre minden* $s \in S$ *esetén* $f(s)$ *invertálható* B*-ben létezik egyetlen* $\bar{f} : S^{-1}A \longrightarrow B$ *unitér morfizmus úgy, hogy* $f = \bar{f} \circ i_S$ *(azaz az* f *meghosszabbítása létezik és egyértelmű, és a következő diagram kommutatív).*

$$\begin{tikzcd} A \arrow[r, "f"] \arrow[d, "i_S"'] & B \\ S^{-1}A \arrow[ur, dotted, "\bar{f}"'] & \end{tikzcd}$$

Bizonyítás. Egyértelműség: Feltételezzük, hogy $\bar{f}$ létezik, és legyen $a/b \in S^{-1}A$. Ekkor

$$\begin{aligned} \bar{f}(a/b) &= \bar{f}(i_S(a)i_S(s)^{-1}) = \\ &= \bar{f}(i_S(a))\bar{f}(i'_S(s))^{-1} = \\ &= (\bar{f} \circ i_S)(a)\bar{f} \circ i_S)(s)^{-1} = \\ &= f(a)f(s)^{-1} \end{aligned}$$

egyértelműen meghatározott.

Létezés: értelmezés szerint, legyen $\bar{f} : S^{-1}A \longrightarrow B$, $\bar{f}(a/b) = f(a)f(s)^{-1}$.

Először igazoljuk, hogy $\bar{f}$ jól értelmezett. Valóban, legyen $a/s = b/t$, vagyis $at = bs$. Mivel f morfizmus következik, hogy $f(a)f(t) = f(b)f(s)$, de $f(t), f(s)$ invertálhatók B-ben, ezért $f(a)f(s)^{-1} = f(b)f(t)^{-1}$, vagyis $\bar{f}(a/s) = \bar{f}(b/t)$.

Igazoljuk, hogy $\bar{f}$ morfizmus. Minden $a/s, b/t \in S^{-1}A$ esetén

$$\begin{aligned} \bar{f}(a/s + b/t) &= \bar{f}((at + bs)/(st)) = \\ &= f(at + bs)f(st)^{-1} = \\ &= [f(a)f(t) + f(b)f(s)]f(s)^{-1}f(t)^{-1} = \\ &= f(a)f(s)^{-1} + f(b)f(t)^{-1} = \\ &= \bar{f}(a/s)\bar{f}(b/t); \\ \bar{f}((a/s)(b/t)) &= \bar{f}((ab)/(st)) = f(ab)f(st)^{-1} = \\ &= f(ab)f((st)^{-1}) = f(ab)f(t^{-1}s^{-1}) = \\ &= f(a)f(b)f(t^{-1})f(s^{-1}) = \\ &= \bar{f}(a/s)\bar{f}(b/t). \end{aligned}$$

Végűl, igazoljuk, hogy a diagramm kommutatív: minden $a \in A$ esetén fennáll

$$\begin{aligned} (\bar{f} \circ i_S)(a) &= \bar{f}(i_S(a)) = \bar{f}((as)/s) = \\ &= f(as)f(s)^{-1} = \\ &= f(a)f(s)f(s)^{-1} = f(a). \qquad \blacksquare \end{aligned}$$

4.6.9. következmény. *Legyen* K *egy kommutatív test és* A *részgyűrűje* K*-nak* (tehát A integritástartomány). *Legyen* $\mathrm{frac}(A) := S^{-1}A$ *az* A *hányadosteste, ahol* $S = A^*$. *Akkor*

$$\mathrm{frac}(A) \simeq \{ab^{-1} \mid a, b \in A, b \neq 0\}.$$

Bizonyítás. Jelöljük L-el az $\{ab^{-1} \mid a, b \in A, b \neq 0\}$ halmazt és vegyük észre, hogy L az A-t tartalmazó legkisebb résztest (vagyis az A által generált résztest).

Valóban, L részteste K-nak, mert $0, 1 \in L$ és minden $x, y \in L$, ahol $y \neq 0$ esetén $x - y, xy^{-1} \in L$. Igazolnunk kell, hogy ha H részteste K-nak úgy, hogy $A \subseteq H$, akkor $L \subseteq H$. Mivel $A \subseteq H$ és H résztest, minden $a, b \in A$ ($b \neq 0$) esetén az $ab^{-1} \in H$, vagyis $L \subseteq H$.

Legyen $f : A \longrightarrow K$, $f(a) = a$. Ekkor f unitér gyűrűmorfizmus és minden $b \in S^*$ esetén $f(b) = b$ invertálható K-ban. A hányadosgyűrű univerzális tulajdonsága szerint létezik az

$$\bar{f} : S^{-1}A \longrightarrow K, \quad \bar{f}(a/b) = f(a)f(b)^{-1} = ab^{-1}$$

gyűrűmorfizmus.

$\bar{f}(1) = 1 \neq 0$, ezért $\bar{f}$ injektív; $\bar{f}$ szürjektív, mert $\operatorname{Im} \bar{f} = \{ab^{-1} \mid a, b \in A\} = L$. A fentiekből következik, hogy $S^{-1}A \simeq L$. ■

4.18. feladat. a) Legyen $d \in \mathbb{Z}$ négyzetmentes. Igazoljuk, hogy a $\mathbb{Z}[\sqrt{d}]$ hányadosteste $\mathbb{Q}(\sqrt{d})$.

b) Legyen p egy prímszám és $\mathbb{Q}_{(p)} = \{\frac{m}{n} \mid (n, p) = 1\}$. Igazoljuk, hogy $\mathbb{Q}_{(p)}$ részgyűrűje $\mathbb{Q}$-nak, és $\mathbb{Q}_{(p)}$ hányadosteste $\mathbb{Q}$.

4.19. feladat (Az egész számok gyűrűje). Legyen $(\mathbb{Z}, +)$ az $(\mathbb{N}, +)$ monoid hányadoscsoportja és értelmezzük a „$\cdot$” műveletet:

$$\widetilde{(m, n)} \cdot \widetilde{(p, q)} = \widetilde{(mp + nq, nq + mp)}.$$

Továbbá, legyen

$$\mathbb{Z}_+^* = \{\widetilde{(m, n)} \mid m > n\}, \quad \mathbb{Z}_-^* = \{\widetilde{(m, n)} \mid m < n\},$$

és értelmezzük a “$<$” relációt:

$$\widetilde{(m, n)} < \widetilde{(p, q)} \Longleftrightarrow \widetilde{(p, q)} - \widetilde{(m, n)} \in \mathbb{Z}_+^*.$$

Igazoljuk, hogy:

a) $\widetilde{(m, n)} = \begin{cases} \{(m - n + y, y) \mid y \in \mathbb{N}\}, & \text{ha } m \geq n \\ \{(y, n - m + y) \mid y \in \mathbb{N}\}, & \text{ha } n \geq m \end{cases}$; a fenti értelmezések nem függnek a reprezentánsoktól.

b) $(\mathbb{Z}_+, \cdot)$ integritástartomány.

c) $\{\mathbb{Z}_-^*, \{0\}, \mathbb{Z}_+^*\}$ osztályfelbontása $\mathbb{Z}$-nek.

d) $(\mathbb{Z}, +)$ teljesen rendezett, és az $i_{\mathbb{N}} : \mathbb{N} \to \mathbb{Z}_+$ kanonikus injekció szigorúan növekvő izomorfizmus.

e) Ha $a, b, c, d \in \mathbb{Z}$, akkor $a < b,\ c \leq d \ \Rightarrow\ a + c < b + d$; $a < b,\ c > 0 \ \Rightarrow\ ac < bc$.

4.20. feladat (A racionális számok teste). Legyen $(\mathbb{Q}, +, \cdot)$ a $(\mathbb{Z}, +, \cdot)$ hányadosteste,

$$0 = \overline{(0, 1)}, \quad \mathbb{Q}_+^* = \{\frac{m}{n} \mid m, n \in \mathbb{Z}_+^*\}, \quad \mathbb{Q}_-^* = \{\frac{m}{n} \mid m \in \mathbb{Z}_-^*,\ n \in \mathbb{Z}_+^*\},$$

és értelmezés szerint,

$$a < b \Longleftrightarrow b - a \in \mathbb{Q}_+^*.$$

Igazoljuk, hogy:

a) $\overline{(a, b)} = \{(a'x, b'x) \mid x \in \mathbb{Z}^*\}$, ahol $d = (a, b)$, $a = a'd$, $b = b'd$, $(a', b') = 1$, és a fenti értelmezések nem függnek a reprezentánsoktól.

b) $\{\mathbb{Q}_-, \{0\}, \mathbb{Q}_+\}$ osztályfelbontása $\mathbb{Q}$-nak.

c) $(\mathbb{Q}, \leq)$ teljesen rendezett, és az $i_{\mathbb{Z}^*} : \mathbb{Z} \to \mathbb{Q}$ kanonikus injekció szigorúan növekvő.

d) $a < b,\ c \leq d \ \Rightarrow\ a + c < b + d$; $a < b,\ c > 0 \ \Rightarrow\ ac < bc$.

e) (*Arkhimedesz axiómája*) $a \in \mathbb{Q},\ b \in \mathbb{Q}_+ \ \Rightarrow\ (\exists) n \in \mathbb{N}$ úgy, hogy $a \leq bn$.

4.21. feladat. Igazoljuk, hogy:

a) $\mathbb{Z}[X]$ hányadosteste $\mathbb{Q}(X)$.

b) $(S^{-1}A)[X] \simeq S^{-1}(A[X])$.

c) Ha $S = \{b^n \mid n \geq 0\}$, akkor $S^{-1}A \simeq A[X]/(Xb - 1)$.

d) Legyen $A = K[X]$ és $S = A \setminus (X)$. Akkor $S^{-1}A = K[X, \frac{1}{X}]$.

e) A $K[[X]]$ hányadosteste a

$$K\{X\} = \{\sum_{i=-n}^{\infty} a_i X^i \mid n \in \mathbb{N}\}$$

Laurent-féle formális sorok teste.

A következő feladatokban A egy kommutatív egységelemes gyűrű és $S \subseteq A$ egy multiplikatív zárt rendszer.

4.22. feladat. a) Ha $S \subseteq U(A)$, akkor $S^{-1}A \simeq A$.
b) $U(S^{-1}A) = \{\frac{a}{s} \mid (\exists)b \in A$ úgy, hogy $ab \in S\}$.
c) $r(S^{-1}A) = S^{-1}r(A)$.
d) Az $i_S : A \to S^{-1}A$ kanonikus injekció monomorfizmus, epimorfizmus, és általában nem szürjektív.

4.23. feladat. Ha $I \trianglelefteq A$, legyen $S^{-1}I = \{\frac{a}{s} \mid a \in I,\ s \in S\}$. Igazoljuk, hogy

$$\phi : \mathcal{I}(A) \to \mathcal{I}(S^{-1}A),\ \phi(I) = S^{-1}I$$

hálómorfizmus.

4.24. feladat. Legyenek $S \subset A$, $T \subset B$ és $U \subset C$ multiplikatív zárt rendszerek, $f : A \to B$ és $g : g \to C$ morfizmusok úgy, hogy $f(S) \subseteq T$ es $g(T) \subseteq U$. Bizonyítsuk be, hogy:
a) Létezik egyetlen $f_S : S^{-1}A \to T^{-1}B$ morfizmus, úgy, hogy $f_S \circ i_S = i_T \circ f$.
b) $(1_A)_S = 1_{S^{-1}A}$ és $(g \circ f)_S = g_T \circ f_S$.

4.25. feladat. Legyenek $S, T \subset A$ multiplikatív rendszerek, és legyen $ST = \{st \mid s \in S,\ t \in T\}$.
a) $(ST)^{-1}A \simeq \bar{S}^{-1}(T^{-1}A)$, ahol $\bar{S} = i_T(S) \subset T^{-1}A$.
b) Ha $S \subseteq T$, akkor a következő állítások ekvivalensek:

(i) $i_{TS} : S^{-1}A \to T^{-1}A$ izomorfizmus.

(ii) $(\forall)t \in T\ (\exists)a \in A$ úgy, hogy $at \in S$.

(iii) $(\forall)U \subset A$ multiplikatív rendszer esetén, $T \subseteq U \Rightarrow S \subseteq U$.

4.7. Polinomok és algebrai egyenletek

4.7.1. Polinom deriváltja. Többszörös gyökök

Legyen K egy kommutatív test.

Az $(1, X, X^2, \dots)$ bázis a $K[X]$ K-feletti vektortérben. A vektorterek univerzális tulajdonságából következik, hogy létezik egyetlen olyan $D : K[X] \to K[X]$ lineáris függvény, amelyre $D(X^k) = kX^{k-1}$ minden $k \in \mathbb{N}$ esetén. Általában, ha $f = \sum_{k=0}^{n} a_k X^k$, akkor

$$D(f) = f' = f^{(1)} = \sum_{k=1}^{n} k a_k X^{k-1}.$$

A $D(f) = f'$ polinomot az f **formális deriváltj**ának nevezzük.

4.7.1. lemma. 1) $D(f+g) = D(f) + D(g)$, $D(af) = aD(f)$;
2) $D(fg) = D(f)g + fD(g)$; $D(f_1 \dots f_n) = \sum_{i=1}^{n} f_1 \dots f_{i-1} D(f_i) f_{i+1} \dots f_n$;
3) $D(g \circ f) = (D(g) \circ f)D(f)$.

Bizonyítás. 1) Ha $f = \sum_{k \geq 0} a_k X^k$, $g = \sum_{k \geq 0} b_k X^k$, akkor

$$\begin{aligned} D(f+g) &= D(\sum_{k \geq 0} (a_k + b_k) X^k) = \\ &= \sum_{k \geq 0} k(a_k + b_k) X^{k-1} = \\ &= \sum_{k \geq 0} k a_k X^{k-1} + \sum_{k \geq 0} k b_k X^{k-1} = \\ &= D(f) + D(g), \end{aligned}$$

$$\begin{aligned} D(af) &= D(a \sum_{k \geq 0} a_k X^k) = D(\sum_{k \geq 0} a a_k X^k) = \\ &= \sum_{k \geq 0} k a a_k X^{k-1} = a \sum_{k \geq 0} k a_k X^{k-1} = \\ &= aD(f). \end{aligned}$$

2) Ha $f = X^i$ és $g = X^j$, akkor $fg = X^{i+j}$ és

$$D(fg) = (i+j)X^{i+j-1} = X^i jX^{j-1} + iX^{i-1}X^j = (i+j)X^{i+j-1} = fD(g) + D(f)g.$$

Ha $f = \sum_{i=0}^{n} a_i X^i$ és $g = \sum_{j=0}^{m} b_j X^j$, akkor $fg = \sum_{k=0}^{n+m} \sum_{i+j=k} a_i b_j X^i X^j$.

$$\begin{aligned} D(fg) &= \sum_{k=1}^{n+m} \sum_{i+j=k} a_i b_j D(X^i X^j) = \\ &= \sum_{k=1}^{n+m} \sum_{i+j=k} (a_i b_j X^i D(X^j) + a_i b_j D(X^i) X^j) = \\ &= \sum_{k=1}^{n+m} \sum_{i+j=k} a_i b_j X^i D(X^j) + \sum_{k=1}^{n+m} \sum_{i+j=k} a_i b_j D(X^i) X^j = \\ &= fD(g) + D(f)g. \end{aligned}$$

Az általános állítást igazoljuk indukcióval n-szerint. Ha $n = 1$, akkor $D(f_1) = D(f_1)$.
Feltételezzük, hogy fennáll n-re, és igazoljuk $n+1$-re:

$$\begin{aligned} D(f_1 \dots f_n f_{n+1}) &= D(f_1 \dots f_n) f_{n+1} + f_1 \dots f_n D(f_{n+1}) = \\ &= (\sum_{i=1}^{n} f_1 \dots D(f_i) \dots f_n) f_{n+1} + f_1 \dots f_n D(f_{n+1}) = \\ &= \sum_{i=1}^{n+1} f_1 \dots D(f_i) \dots f_n f_{n+1}. \end{aligned}$$

3) Ha $g = X^k$, akkor $g \circ f = f^k$ és $D(g) = kX^{k-1}$, és b)-ből következik, hogy $D(g \circ f) = D(f^k) = kf^{k-1}D(f) = (D(g) \circ f)D(f)$.
Általában, ha $g = \sum_{k=0}^{n} b_k X^k$, akkor

$$\begin{aligned} D(g \circ f) &= \sum_{k=1}^{n} b_k D(f^k) = \sum_{k=1}^{n} b_k k f^{k-1} D(f) = \\ &= ((D(g)) \circ f) D(f). \qquad \blacksquare \end{aligned}$$

A **többszörös deriválta**t rekurzióval definiáljuk:

$$f^{(0)} = f, \quad f^{(1)} = D(f), \quad f^{(k+1)} = D^{k+1}(f) = D(f^{(k)}).$$

4.7.2. lemma (Taylor-képlet). *Ha* $f \in K[X]$, $\deg(f) = n$ *és* $a \in K$, *akkor léteznek a* $b_0, \dots, b_n \in K$ *elemek úgy, hogy*

$$f = \sum_{k=0}^{n} b_k (X - a)^k.$$

Ha $\mathrm{char} K = 0$, *akkor a* b_k *együtthatók egyértelműen meghatározottak:*

$$b_k = \frac{f^{(k)}(a)}{k!}$$

minden $k \in \mathbb{N}$ *esetén.*

Bizonyítás. $\deg f$-szerinti indukciót alkalmazunk. Ha $\deg f < 1$, akkor $f = a_0 \in K$. Ha $\deg f = 1$, akkor $f = a_0 + a_1 X = a_1(X - a) + a_1 a + a_0$. Feltételezzük, hogy $n > 1$, és az állítás igaz n-nél kisebb fokú polinomok esetén. Legyen $f = (X - a)f_1 + f(a)$, ahol $\deg f_1 = n - 1$. Az indukció feltevéséből következik, hogy

$$f_1 = \sum_{k=0}^{n-1} b_k (X - a)^k,$$

tehát

$$f = f(a) + \sum_{k=0}^{n-1} b_k (X - a)^{k+1}.$$

Ha $\mathrm{char}\, K = 0$ és $f = \sum_{k=0}^{n} b_k (X - a)^k$, akkor $f(a) = b_0 = (f^{(0)}(a))/(0!)$, és deriválással kapjuk, hogy $f^{(k)}(a) = k! b_k, \quad k = 0, \dots, n.$ $\blacksquare$

4.7.3. megjegyzés. 1) Ha $K = \mathbb{Z}_p$, p prímszám, akkor char $= p$. Ezért minden $k \geq p$ esetén $k!b_k = 0$.

2) Ha a K test karakterisztikája 0 és $f \in K[X]$, akkor $f' = 0$ akkor és csakis akkor áll fenn, ha $f \in K$.

3) Legyen a K test karakterisztikája $p \neq 0$ és $f \in K[X]$; $f' = 0$ akkor és csak akkor áll fenn, ha f a következő alakú:

$$f = a_0 + a_1X^p + a_2X^{2p} + \cdots + a_nX^{np}$$

vagyis $f \in K[X^p]$.

4.7.4. tétel. *Legyenek* $f \in K[X], a \in K, k \in \mathbb{N}^*$ *és* char $K = 0$.

1) *Ha* a k*-szoros gyöke* f*-nek, akkor* a $(k-1)$*-szeres gyöke a deriváltjának (D(f)-nek) és* $f^{(0)}(a) = f^{(1)}(a) = \cdots = f^{(k-1)}(a) = 0$ *és* $f^{(k)}(a) \neq 0$.

2) *Ha* $f^{(0)}(a) = f^{(1)}(a) = \cdots = f^{(k-1)}(a) = 0$ *és* $f^{(k)}(a) \neq 0$*, akkor* f*-nek az* a k*-szoros gyöke.*

Bizonyítás. 1) Feltételezzük, hogy $f = (X-a)^k g$ és $g(a) \neq 0$. Deriváljuk az f-et:

$$D(f) = k(X-a)^{k-1}g + (X-a)^kD(g) = (X-a)^{k-1}[kg + (X-a)D(g)].$$

Következik, hogy $(X-a)^{k-1}|D(f)$ és $g_1(a) = kg(a) \neq 0$, ahol $g_1 = kg + (X-a)D(g)$. Ezzel igazoltuk, hogy ha a k-szoros gyöke f-nek, akkor a $(k-1)$-szeres gyöke a deriváltjának ($D(f)$-nek). Indukcióval igazolható, hogy a $(k-i)$-szeres gyöke $f^{(i)}$-nek,$i = 1, \ldots, k$, tehát a 1-szeres gyöke $f^{(k-1)}$-nek, (0)-szoros gyöke $f^{(k)}$-nak, azaz $f^{(k)}(a) \neq 0$.

2) Alkalmazva a Taylor képletet következik, hogy

$$\begin{aligned} f &= \sum_{j=0}^{n} (f^{(j)}(a))/(j!)(X-a)^j = \\ &= \sum_{i=k}^{n} (f^{(i)}(a))/(i!)(X-a)^i = \\ &= (X-a)^k((f^{(k)}(a))/(k!) + (X-a)f^{(k+1)}(a))/((k+1)!) + \ldots). \end{aligned}$$

Jelöljük g-vel az $(f^{(k)}(a))/(k!) + (X-a)f^{(k+1)}(a))/((k+1)!) + \ldots$ polinomot; következik, hogy $(X-a)^k|f$ és $g(a) \neq 0$, mert $f^{(k)} \neq 0$. ■

4.7.2. Többhatározatlanú polinomok

4.7.5. definíció. 1) Legyen A egy kommutatív gyűrű, $1 \neq 0$ és tekintsük az $A[X_1]$ egyhatározatlanú polinomalgebrát. Az $A[X_1, X_2] = (A[X_1])[X_2]$ algebrát *kéthatározatlanú polinomalgebrának* nevezzük.

2) Általában rekurzióval definiáljuk az $A[X_1, \ldots, X_n]$ n*-határozatlanú polinomalgebrát*:

$$A[X_1, \ldots, X_n] = (A[X_1, \ldots, X_{n-1}])[X_n].$$

Ha $f \in A[X_1, \ldots, X_n]$, akkor f egyértelműen írható az

$$\begin{aligned} f &= \sum_{k=0}^{n} f_k X_n^k \\ &= \sum_{(k_1,\ldots,k_n), k_i \geq 0} a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n}, \end{aligned}$$

alakban, ahol a nemnulla $f_k \in A[X_1, \ldots, X_{n-1}]$ és $a_{k_1,\ldots,k_n} \in A$ száma véges.

3) Az $a_{k_1,\ldots,k_n} X_1^{k_1} \ldots X_n^{k_n}$ tagot **monom**nak nevezzük. E monom **foka** $k_1 + \cdots + k_n$.

4) Az f *polinom foka* $\deg f = \max\{k_1 + \cdots + k_n \mid a_{k_1,\ldots,k_n} \neq 0\}$.

5) Ha $k_1 + \cdots + k_n$ konstans minden $a_{k_1,\ldots,k_n}$ esetén akkor azt mondjuk, hogy f **homogén polinom**.

6) Az f polinom egyértelműen írható

$$f = h_0 + h_1 + \cdots + h_m$$

alakban, ahol $h_i \in A[X_1, \ldots, X_n]$ homogén polinomok és $\deg(h_i) = i$. Azt mondjuk, hogy $h_0, h_1, \ldots, h_m$ *az* f *homogén komponensei.*

Az alábbi állítások általánosítják az $A[X]$ esetén ismert tételeket.

4.7.6. megjegyzés. 1) Ha $f, g \in A[X_1, \dots, X_n]$, akkor

$$\deg(f+g) \le \max\{\deg(f), \deg(g)\};$$

$$\deg(fg) \le \deg(f) + \deg(g).$$

2) Ha A integritástartomány, akkor $\deg(fg) = \deg(f) + \deg(g)$ és az $A[X_1, \dots, X_n]$ is integritástartomány.

4.7.7. tétel (A polinomalgebra univerzális tulajdonsága). *Legyen* B *egy kommutatív egységelemes gyűrű,* $\varphi : A \to B$ *egy uniér gyűrűmorfizmus és* $b_1, \dots, b_n \in B$. *Ekkor létezik és egyértelműen meghatározott a* $\bar{\varphi}_{b_1 \dots b_n} : A[X_1, \dots, X_n] \to B$ A*-algebramorfizmus úgy, hogy* $\bar{\varphi}_{b_1 \dots b_n} \circ i = \varphi$ *és* $\bar{\varphi}_{b_1 \dots b_n}(X_i) = b_i$, *tehát az*

$$\begin{tikzcd} A \arrow[r, "\varphi"] \arrow[d, "\iota_A"'] & B \\ A[X_1, \dots, X_n] \arrow[ur, dotted, "\bar{\varphi}_{b_1, \dots, b_n}"'] & \end{tikzcd}$$

diagram kommutatív, és általában

$$\bar{\varphi}_{k_1 \dots k_n}(f) = \sum_{(b_1, \dots, b_n)} \varphi(a_{k_1, \dots, k_n}) b_1^{k_1} \dots b_n^{k_n}.$$

Bizonyítás. n-szerinti indukciót alkalmazunk. Ha $n = 1$, akkor az állítás igaz a 1.4.3. tétel alapján. Feltételezzük, hogy fennáll $n-1$-re és alkalmazva az indukció feltevését következik, hogy fennáll n-re is. A bizonyítás részletes elvégzését az olvasóra bizzuk. ■

4.7.8. definíció. A fenti tételben legyen $A = B$ és $\phi = 1_A$. Ekkor az

$$\tilde{f} : A^n \to A, \quad \tilde{f}(a_1, \dots, a_n) = \phi_{a_1, \dots, a_n}(f)$$

függvényt n változós **polinomfüggvény**nek nevezzük.

4.26. feladat. a) Ha A integritástartomány és $f, g \in A[X_1, \dots, X_n]$, akkor $\deg(fg) = \deg(f) + \deg(g)$.
b) A k-ad fokú n-változós monomok száma C_{n+k-1}^k.

4.27. feladat (Polinomiális képlet). Igazoljuk, hogy

$$(X_1 + \dots + X_n)^k = \sum_{k_1 + \dots + k_n = k} \frac{k!}{k_1! \dots k_n!} X_1^{k_1} \dots X_n^{k_n}.$$

4.28. feladat. a) Ha $a_1, \dots, a_n \in A$, akkor $A[X_1, \dots, X_n]/(X_1 - a_1, \dots, X_n - a_n) \simeq A$.
b) Ha $I \trianglelefteq A$, akkor $A[X_1, \dots, X_n]/I[X_1, \dots, X_n] \simeq (A/I)[X_1, \dots, X_n]$.

4.29. feladat. Legyenek $\phi : A \to B$ és $\psi : B \to C$ unitér homomorfizmusok. Bizonyítsuk be, hogy:
a) Létezik egyetlen $\phi[X_1, \dots, X_n] : A[X_1, \dots, X_n] \to B[X_1, \dots, X_n]$ morfizmus úgy, hogy $i_B \circ \phi = \phi[X_1, \dots, X_n] \circ i_A$, ahol $i_A : A \to A[X_1, \dots, X_n]$ a kanonikus injekció.
b) $1_A[X_1, \dots, X_n] = 1_{A[X_1, \dots, X_n]}$ és $(\psi \circ \phi)[X_1, \dots, X_n] = \psi[X_1, \dots, X_n] \circ \phi[X_1, \dots, X_n]$.

4.7.3. Szimmetrikus polinomok

Ha $\sigma \in S_n$ egy n-ed fokú permutáció, akkor a polinomalgebra univerzális tulajdonságából következik, hogy az $X_i \mapsto X_{\sigma(i)}$, $1 = 1, \dots, n$ megfeleltetések meghatároznak egy

$$\sigma^* : A[X_1, \dots, X_n] \to A[X_1, \dots, X_n]$$

A-algebramorfizmust.

4.7.9. példa. a) Ha $f = aX_1X_2X_3 + X^2X_3 + X_1X_2X_3^2 \in A[X_1, X_2, X_3]$, $a \neq 0$ és $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, akkor $\sigma^*(f) = aX_3X_1X_2 + X_3^2X_2 + X_3X_1X_2^2$.
b) Általában, ha $f = \sum a_{i_1 \cdots n} X_1^{i_1} \cdots X_n^{i_n} \in A[X_1, \dots, X_n]$, akkor

$$\sigma^*(f) = \sum a_{i_1 \dots i_n} X_{\sigma(1)}^{i_1} \cdots X_{\sigma(n)}^{i_n}.$$

4.7.10. definíció. Azt mondjuk, hogy $f \in A[X_1, \dots, X_n]$ **szimmetrikus polinom**, ha $\sigma^*(f) = f$ bármely $\sigma \in S_n$ esetén.

4.7.11. példa. 1) Ha $n = 2$, $f = X_1^2 + X_2^2 + X_1X_2$, akkor f szimmetrikus polinom, mert $\sigma^*(f) = f$ minden $\sigma \in S_2$ esetén.

2) Legyen $g = X_1^2X_2$, $\sigma = (12)$. Mivel $\sigma^*(g) = X_1X_2^2 \neq g$, következik, hogy g nem szimmetrikus polinom.

3) Ha $P_n = X_1^n + X_2^n + \dots + X_n^n \in A[X_1, \dots, X_n]$, akkor P_n szimmetrikus polinom.

4) Legyen

$$s_1 = X_1 + X_2 + \dots + X_n = \sum_{i=1}^{n} X_i$$

$$s_2 = X_1X_2 + X_1X_3 + \dots + X_1X_n + \dots + X_{n-1}X_n = \sum_{1 \le i < j \le n} X_iX_j$$

$$s_3 = X_1X_2X_3 + \dots + X_{n-2}X_{n-1}X_n = \sum_{1 \le i_1 < i_2 < i_3 \le n} X_{i_1}X_{i_2}X_{i_3}$$

$$\dots$$

$$s_k = X_1X_2 \dots X_k + \dots + X_{n-k+1} \dots X_n = \sum_{1 \le i_1 < \dots < i_k \le n} X_{i_1} \dots X_{i_k}$$

$$\dots$$

$$s_n = X_1X_2 \dots X_n.$$

Az $s_1, s_2, \dots, s_n$ polinomokat **elemi szimmetrikus polinomok**nak nevezzük.

Legyenek $M = aX_1^{k_1} \dots X_n^{k_n}$, $M' = a'X_1^{k'_1} \dots X_n^{k'_n} \in A[X_1, \dots, X_n]$ monomok.

Értelmezés szerint, $M > M'$, ha létezik olyan $j \in \{1, \dots, n\}$ amelyre $k_1 = k'_1$, $k_2 = k'_2, \dots, k_{j-1} = k'_{j-1}$ és $k_j > k'_j$. A „$<$” reláció tranzitív, es a monomok **lexikografikus rendezés**ének nevezzük.

Könnyen belátható, hogy *a monomok halmazában minden szigorúan csökkenő sorozat véges.*

Azt mondjuk, hogy az $f \in A[X_1, \dots, X_n]$ polinomnak a *főtagja* M, ha M az f legnagyobb tagja a lexikografikus rendezésben.

4.7.12. példa. 1) $X_1^2X_2^5 > X_1^2X_2^4X_3^7$.

2) Az $f = X_1^2X_2 + X_1X_2^2 + X_3^2 + X_2^4 + X_1^2X_2^2$ polinom főtagja $X_1^2X_2^2$.

3) Az s_k elemi szimmetrikus polinom főtagja $X_1 \dots X_k$.

4.7.13. lemma. *Ha* $M_1, M_2, N_1, N_2 \in A[X_1, \dots, X_n]$ *monomok úgy, hogy* $M_1 > M_2$, *akkor:*

1) $M_1N_1 > M_2N_1$.

2) *Ha* $N_1 > N_2$, *akkor* $M_1N_1 > M_2N_2$.

3) *Ha* $f, g \in A[X_1, \dots, X_n]$, M *az* f *főtagja és* N *a* g *főtagja, akkor* fg *főtagja az* MN *szorzat.*

Bizonyítás. Legyen $M_1 = aX_1^{k_1} \dots X_n^{k_n}$, $M_2 = bX_1^{l_1} \dots X_n^{l_n}$, $N_1 = cX_1^{m_1} \dots X_n^{m_n}$. Mivel $M_1 > M_2$, következik, hogy $k_1 = l_1, \dots, k_{s-1} = l_{s-1}, k_s > l_s$, ezért $k_1 + m_1 = l_1 + m_1, \dots, k_{s-1} + m_{s-1} = l_{s-1} = m_{s-1}, k_s + m_s > l_s + m_s$, azaz $M_1N_1 > M_2N_1$.

2) alkalmazva kétszer egymás után az 1) pontot következik, hogy $M_1N_1 > M_2N_1 > M_2N_2$.

3) következik 2)-ből. ■

4.7.14. lemma. *Ha* $f \in A[X_1, \dots, X_n]$ *egy szimmetrikus polinom,* $M_1 = aX_1^{k_1} \dots X_n^{k_n}$ *az* f *főtagja, akkor* $k_1 \ge k_2 \ge \dots \ge k_n$.

Bizonyítás. Feltételezzük, hogy létezik olyan i amelyre $k_i < k_{i+1}$, és legyen

$$M' = aX_1^{k_1} \dots X_{i-1}^{k_{i-1}} X_i^{k_{i+1}} X_{i+1}^{k_i} X_{i+2}^{k_{i+2}} \dots X_n^{k_n};$$

következik, hogy $M' = \sigma^*(M)$, ahol $\sigma^* = (i, i+1) \in S_n$. Mivel f szimmetrikus polinom, következik, hogy M' tagja f-nek és $M' > M$ ellentmondás. ■

4.7.15. tétel (A szimmetrikus polinomok alaptétele). *Ha* $f \in A[X_1, \dots, X_n]$ *egy szimmetrikus polinom, akkor létezik az egyértelműen meghatározott* $g \in A[Y_1, \dots, Y_n]$ *polinom úgy, hogy* $f = g(s_1, \dots, s_n)$, *ahol* s_i, $i = 1, \dots, n$ *az elemi szimmetrikus polinomok.*

Bizonyítás. *Létezés*: feltételezzük, hogy $f \neq 0$, és legyen $aX_1^{k_1} \dots X_n^{k_n}$ az f főtagja; láttuk, hogy $k_1 \ge \dots \ge k_n \ge 0$. Vegyük észre, hogy az $s_1^{l_1} \dots s_n^{l_n}$ polinom főtagja

$$X_1^{l_1+l_2+\dots+l_n} X_2^{l_2+\dots+l_n} \dots X_i^{l_i+\dots+l_n} \dots X_n^{l_n},$$

azaz $X_1^{k_1}\dots X_n^{k_n}$, ahol $k_i = i_i + \dots + l_n$. Következik, hogy az $as_1^{k_1-k_2}s_2^{k_2-k_3}\dots s_n^{k_n}$ polinom főtagja $aX_1^{k_1}\dots X_n^{k_n}$.

Legyen $f_1 = f - as_1^{k_1-k_2}s_2^{k_2-k_3}\dots s_n^{k_n}$ és $g_1 = aY_1^{k_1-k_2}\dots Y_n^{k_n} \in A[Y_1,\dots,Y_n]$; következik, hogy f_1 szimmetrikus polinom, melynek főtagja kisebb mint az f főtagja.

Folytatva az eljárást f_1-re, létezik $g_2 \in A[Y_1,\dots,Y_n]$ úgy, hogy $f_2 = f_1 - g_2(s_1,\dots,s_n)$ szimmetrikus polinom, és az f_2 főtagja kisebb az f_1 főtagjánál.

$n-1$ lépés után kapjuk, hogy $f_{n-1} = f_{n-2} - g_{n-1}(s_1,\dots,s_n)$, ahol az f_{n-1} főtagja kisebb az f főtagjánál, és létezik olyan $n \in \mathbb{N}$ amelyre $f_n = f_{n-1} - g_n(s_1,\dots,s_n) = 0$; következik, hogy $f = g_1(s_1,\dots,s_n) + \dots + g_n(s_1,\dots,s_n)$.

Legyen $g = g_1 + \dots + g_n \in A[Y_1,\dots,Y_n]$; akkor $f = g(s_1,\dots,s_n)$.

Egyértelműség: legyen $f = g_1(s_1,\dots,s_n) = g_2(s_1,\dots,s_n)$, azaz $(g_1 - g_2)(s_1,\dots,s_n) = 0$, és igazoljuk, hogy $g_1 = g_2$. Elég igazolni hogy, ha $h \in A[Y_1,\dots,Y_n]$ és $h(s_1,\dots,s_n) = 0$, akkor $h = 0$.

Feltételezzük, hogy $h \neq 0$, $h = \sum a_{l_1\dots l_n}Y_1^{l_1}\dots Y_n^{l_n}$, ahol $a_{l_1\dots l_n} \neq 0$; a $a_{l_1\dots l_n}s_1^{l_1}\dots s_n^{l_n}$ polinom főtagja $a_{l_1\dots l_n}X_1^{k_1}\dots X_n^{k_n}$, ahol $k_i = l_i + \dots + l_n$, és az $a_{l'_1\dots l'_n}s_1^{k'_1}\dots s_n^{k'_n}$ a főtagja $a_{l'_1\dots l'_n}X_1^{k'_1}\dots X_n^{k'_n}$, ahol $k'_i = l'_i + \dots + l'_n, i \in \{1,\dots,n\}$.

Vegyük észre, hogy ha $(l_1,\dots,l_n) \neq (l'_1,\dots,l'_n)$ akkor $(k_1,\dots,k_n) \neq (k'_1,\dots,k'_n)$; következik, hogy ha $M = aX_1^{k_1}\dots X_n^{k_n}$ a h főtagja, akkor M nem egyszerűsödik, azaz $h(s_1,\dots,s_n) \neq 0$ ellentmondás. ■

4.30. feladat. Igazoljuk, hogy:

a) $(\tau\circ\sigma)^* = \sigma^*\circ\tau^*$ és $e^*(f) = f$ $(\forall) f \in A[X_1,\dots,X_n]$.

b) A szimmetrikus polinomok halmaza részgyűrűje $A[X_1,\dots,X_n]$-nek.

c) $f \in A[X_1,\dots,X_n]$ akkor és csak akkor szimmetrikus, ha az f homogén komponensei szimmetrikusak.

4.31. feladat. Alkalmazzuk a szimmetrikus polinomok alaptételét a következő esetekben:

a) $f = (X_1 - X_2)^2(X_2 - X_3)^2(X_3 - X_1)^2$.

b) $f = \sum_{i\neq j} X_i^3X_j = S(X_1^3X_2)$.

c) $f = \sum_{i,j,k} X_i^5X_j^2X_k = S(X_1^5X_2^2X_3)$.

d) $f = (-X_1 + X_2 + \dots + X_n)(X_1 - X_2 + \dots + X_n)\dots(X_1 + X_2 + \dots - X_n)$.

Newton–Waring-képletek

Tekintsük a

$$P_k = X_1^k + \dots + X_n^k$$

szimmetrikus polinomot. A szimmetrikus polinomok alaptétele szerint létezik egy olyan $g_k \in \mathbb{Z}[Y_1,\dots,Y_n]$ polinom, amelyre $P_k = g_k(s_1,\dots,s_n)$. A g_k polinomokat nehéz lenne kiszámítani, ezért keresünk egy összefüggést a P_k és az $s_1,\dots,s_n$ szimmetrikus polinomok között.

Ha $k_1 \geq \dots \geq k_n$, legyen $\mathrm{Orb}(X_1^{k_1}\dots X_n^{k_n}) = \{X_{\sigma(1)}^{k_1}\dots X_{\sigma(n)}^{k_n} \mid \sigma \in S_n\}$, és legyen

$$S(X_1^{k_1}\dots X_n^{k_n}) = \sum_{M\in\mathrm{Orb}(X_1^{k_1}\dots X_n^{k_n})} M$$

a „legkisebb” szimmetrikus polinom, amelynek főtagja $X_1^{k_1}\dots X_n^{k_n}$.

1. eset. Feltételezzük, hogy $k \leq n$.

$$\begin{aligned}
P_1 &= s_1\\
P_{k-1}s_1 &= (X_1^{k-1} + \dots + X_n^{k-1})(X_1 + \dots + X_n) =\\
&= P_k + S(X_1^{k-1}X_2)\\
P_{k-2}s_2 &= (X_1^{k-2} + \dots + X_n^{k-2})(X_1X_2 + \dots + X_{n-1}X_n) =\\
&= S(X_1^{k-1}X_2) + S(X_1^{k-2}X_2X_3)\\
P_{k-3}s_3 &= (X_1^{k-3} + \dots + X_n^{k-3})(X_1X_2X_3 + \dots + X_{n-2}X_{n-1}X_n) =\\
&= S(X_1^{k-2}X_2X_3) + S(X_1^{k-3}X_2X_3X_4)\\
&\dots\\
P_{k-i}s_i &= (X_1^{k-i} + \dots + X_n^{k-i})(X_1X_2\dots X_i + \dots + X_{n-i+1}\dots X_n) =\\
&= S(X_1^{k-i+1}X_2\dots X_i) + S(X_1^{k-i}X_2\dots X_{i+1})\\
&\dots\\
P_1s_{k-1} &= (X_1 + \dots + X_n)(X_1\dots X_{k-1} + \dots + X_{n-k}\dots X_n) =\\
&= S(X_1^2X_2\dots X_{k-1}) + kS(X_1\dots X_k).
\end{aligned}$$

Az I. egyenlőséget beszorozzuk (-1)-gyel, a II. egyenlőséget $(-1)^2$-nel, a III. egyenlőséget $(-1)^3$-nal, ... , az i-ediket $(-1)^i$-nel, ..., és az (n-1)-ediket $(-1)^{k-1}$-nel. Ezután összegezve őket kapjuk:

$$P_k - P_{k-1}s_1 + P_{k-2}s_2 - \cdots + (-1)^i P_{k-i}s_i + \cdots + (-1)^{k-1}P_1 s_{k-1} + (-1)^k k s_k = 0.$$

2. eset. Feltételezzük, hogy $k > n$.

$$\begin{aligned}
P_{k-1}s_1 &= (X_1^{k-1} + \cdots + X_n^{k-1})(X_1 + \cdots + X_n) = \\
&= P_k + S(X_1^{k-1}X_2) \\
P_{k-2}s_2 &= (X_1^{k-2} + \cdots + X_n^{k-2})(X_1X_2 + \cdots + X_{n-1}X_n) = \\
&= S(X_1^{k-1}X_2) + S(X_1^{k-2}X_2X_3) \\
P_{k-3}s_3 &= (X_1^{k-3} + \cdots + X_n^{k-3})(X_1X_2X_3 + \cdots + X_{n-2}X_{n-1}X_n) = \\
&= S(X_1^{k-2}X_2X_3) + S(X_1^{k-3}X_2X_3X_4) \\
&\ldots \\
P_{k-i}s_i &= (X_1^{k-i} + \cdots + X_n^{k-i})(X_1X_2\ldots X_i + \cdots + X_{n-i+1}\ldots X_n) = \\
&= S(X_1^{k-i+1}X_2\ldots X_i) + S(X_1^{k-i}X_2\ldots X_{i+1}) \\
&\ldots \\
P_{k-n}s_n &= S(X_1^{k-n+1}X_2\ldots X_n).
\end{aligned}$$

Hasonlóan szorzunk, összegezünk és kapjuk, hogy

$$P_k - P_{k-1}s_1 + P_{k-2}s_2 - \cdots + (-1)^i P_{k-i}s_i + \cdots + (-1)^n P_{k-n}s_n = 0.$$

4.32. feladat (Newton–Waring-képletek). Legyen $P_k = X_1^k + \cdots + X_n^k$.
a) Fejezzük ki P_2, P_3 és P_4-et s_1, s_2, s_3 és s_4 függvényében, ha $n = 2, 3$ és ha $n \geq 4$.
b) Ha $n = 4$, fejezzük ki s_1, s_2, s_3 és s_4-et P_1, P_2, P_3 és P_4 függvényében.

4.7.4. Diszkrimináns és rezultáns

A. Diszkrimináns. Tekintsük a következő n határozatlanú polinomot:

$$\Delta_n = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{vmatrix} = \prod_{1 \leq i < j \leq n} (X_j - X_i) \in \mathbb{Z}[X_1, \ldots, X_n].$$

Ha $\sigma \in S_n$, akkor $\sigma^*(\Delta_n) = \operatorname{sgn}(\sigma)\Delta_n$, vagyis Δ_n nem szimmetrikus polinom, de Δ_n^2 szimmetrikus polinom.

4.7.16. definíció. Δ_n^2-et az $(X_1, \ldots, X_n)$ rendszer **diszkriminánsa**nak nevezzük.

$$\Delta_n^2 = \begin{vmatrix} 1 & 1 & \ldots & 1 \\ X_1 & X_2 & \ldots & X_n \\ \vdots & \vdots & \ddots & \vdots \\ X_1^{n-1} & X_2^{n-1} & \ldots & X_n^{n-1} \end{vmatrix} \cdot \begin{vmatrix} 1 & X_1 & \ldots & X_1^{n-1} \\ 1 & X_2 & \ldots & X_2^{n-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & X_n & \ldots & X_n^{n-1} \end{vmatrix} =$$

$$= \begin{vmatrix} n & P_1 & P_2 & \ldots & P_{n-1} \\ P_1 & P_2 & P_3 & \ldots & P_n \\ P_2 & P_3 & P_4 & \ldots & P_{n+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ P_{n-1} & P_n & P_{n+1} & \ldots & P_{2n-2} \end{vmatrix}$$

Legyen $f = a_0X^n + a_1X^{n-1} + \cdots + a_{n-1}X + a_n \in \mathbb{C}[X]$, $a_0 \neq 0$. Feltételezzük, hogy $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$ az f gyökei.

4.7.17. definíció.

$$\Delta(f) = a_0^{2n-2}\Delta_n^2(\alpha_1, \ldots, \alpha_n) \in \mathbb{C}$$

elemet az f polinom **diszkriminánsa**nak nevezzük.

4.7.18. megjegyzés. a) $\Delta(f) = 0 \iff f$-nek van többszörös gyöke.

b) A szimmetrikus polinomok alaptételéből és Viete-képleteiből következik, hogy a $\Delta(f)$ diszkriminánsa kifejezhető az $a_1, \dots, a_n$ együtthatók segítségével.

4.7.19. példa. Legyen $n = 2$, $f = X^2 + aX + b$ és α_1, α_2 az f gyökei. Határozzuk meg $\Delta(f)$-et a polinom együtthatóinak függvényében:

$$P_1(\alpha_1, \alpha_2) = \alpha_1 + \alpha_2 = -a, \quad P_2(\alpha_1, \alpha_2) = \alpha_1^2 + \alpha_2^2 = s_1^2 - 2s_2 = a^2 - 2b,$$

tehát ebben az esetben

$$\Delta(f) = \begin{vmatrix} 2 & -a \\ -a & a^2 - 2b \end{vmatrix} = 2a^2 - 4b - a^2 = a^2 - 4b$$

megeggyezik az eddig is ismert diszkriminánssal.

B. Rezultáns.

Legyenek

$$f = a_0X^n + a_1X^{n-1} + \dots + a_{n-1}X + a_n,$$
$$g = b_0X^m + b_1X^{m-1} + \dots + a_{m-1}X + b_m,$$

komplex együtthatós polinomok, ahol $n, m > 0$, de nincs kizárva az, hogy $a_0 = 0$ vagy $b_0 = 0$.

4.7.20. definíció. Az f és g polinomok **rezultáns**ának nevezzük a következő $n + m$-ed rendű determinánst:

$$\mathrm{Res}(f, g) = \begin{vmatrix} a_0 & a_1 & a_2 & . & & . & . & a_n & 0 & . & \dots & . \\ 0 & a_0 & a_1 & a_2 & & . & . & . & a_n & 0 & \dots & . \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & 0 \\ . & . & . & 0 & a_0 & a_1 & a_2 & . & . & . & \dots & a_n \\ b_0 & b_1 & b_2 & . & . & b_m & 0 & . & . & . & \dots & . \\ 0 & b_0 & b_1 & b_2 & . & . & b_m & 0 & . & . & \dots & . \\ . & . & . & . & . & . & . & . & . & . & . & . \\ . & . & . & . & . & . & . & . & . & . & . & 0 \\ . & . & . & 0 & b_0 & b_1 & b_2 & . & . & . & \dots & b_m \end{vmatrix}$$

ahol az első m sor tartalmazza az f együtthatóit, és az utolsó n sor tartalmazza a g együtthatóit.

4.7.21. tétel. *Legyen* $f, g \in \mathbb{C}[X]$. *A következő állítások ekvivalensek:*

(i) $\mathrm{Res}(f, g) = 0$.

(ii) *Léteznek olyan* $f_1, g_1 \in \mathbb{C}[X]$, *amelyre* $fg_1 + f_1g = 0$, $\deg f_1 < n$, $\deg g_1 < m$.

(iii) $a_0 = b_0 = 0$ *vagy létezik olyan* $h \in \mathbb{C}[X]$ *amelyre* $h \mid f$, $h \mid g$ *és* $\deg h \geq 1$.

Bizonyítás. (iii)$\iff$(ii). Feltételezzük, hogy $h \in \mathbb{C}[X]$, $h \mid f$, $h \mid g$ és $\deg h \geq 1$. Ekkor léteznek az $f_1, g_1 \in \mathbb{C}[X]$ polinomok úgy, hogy $f = hf_1$ és $g = -hg_1$; következik, hogy $fg_1 + f_1g = 0$, $\deg f_1 < n$, $\deg g_1 < m$. Ha pedig $a_0 = b_0 = 0$, akkor legyen $f_1 = f$ és $g_1 = -g$.

Fordítva, ha f-nek és g-nek nincs valódi közös tényezője, akkor az $fg_1 = -f_1g$ egyenlőségből következik, hogy $f \mid f_1$ és $g \mid g_1$, tehát $\deg f < n$, $\deg g < m$ és $a_0 = b_0 = 0$.

(ii)$\iff$(i). Akkor és csak akkor léteznek olyan

$$f_1 = c_0X^{n-1} + c_1X^{n-2} + \dots + c_{n-1},$$
$$g_1 = d_0X^{m-1} + d_1X^{m-2} + \dots + d_{m-1}$$

polinomok amelyre $fg_1 + f_1g = 0$, ha az

$$\begin{array}{lll} a_0d_0 + & b_0c_0 & = 0 \\ a_1d_0 + a_0d_1 + & b_1c_0 + b_0c_1 & = 0 \\ a_2d_0 + a_1d_1 + a_0d_2 + & b_2c_0 + b_1c_1 + b_0c_2 & = 0 \\ \dots\dots\dots\dots & & \end{array}$$

homogén egyenletrendszernek van egy $(d_0, \dots, d_{m-1}, c_0, \dots, c_{n-1})$ nemtriviális megoldása. Egy ilyen megoldás akkor és csak akkor létezik, ha $\mathrm{Res}(f, g)^t = 0$, azaz ha $\mathrm{Res}(f, g) = 0$. ■

4.7.22. tétel. *Feltételezzük, hogy*

$$f = a_0(X - \alpha_1)\dots(X - \alpha_n),$$
$$g = b_0(X - \beta_1)\dots(X - \beta_m).$$

Ekkor

$$\operatorname{Res}(f, g) = a_0^m \prod_{i=1}^{n} g(\alpha_i) = (-1)^{mn} b_0^m \prod_{j=1}^{m} f(\beta_j) = a_0^m b_0^n \prod_{i=1}^{n}\prod_{j=1}^{m}(\alpha_i - \beta_j).$$

Bizonyítás. Mivel $\operatorname{Res}(f, g) = (-1)^{mn}\operatorname{Res}(g, f)$, elég igazolni az első egyenlőséget. Továbbá, elég tanulmányozni az „általános esetet": feltételezhetjük, hogy $g(\alpha_1), \dots, g(\alpha_n)$ páronként különböző számok.

Tekintsük az $f,\ g - Y \in \mathbb{C}[Y][X]$ polinomokat; ekkor

$$\operatorname{Res}(f, g - Y) = (-1)^m a_0 Y^n + \dots + \operatorname{Res}(f, g).$$

Vegyük észre, hogy α_i közös gyöke az f és $g - g(\alpha_i)$ polinomoknak, tehát mindkettő osztható $(X - \alpha_i)$-vel. Az előző tételből következik, hogy $\operatorname{Res}(f, g - g(\alpha_i) = 0$, tehát Bézout tétele szerint a $\operatorname{Res}(f, g - Y) \in \mathbb{C}[Y]$ polinom osztható $(g(\alpha_i) - Y)$-nal, $i = 1, \dots, n$. Mivel $g(\alpha_1), \dots, g(\alpha_n)$ páronként különböző számok, következik, hogy $\operatorname{Res}(f, g) = a_0^m \prod_{i=1}^{n}(g(\alpha_i) - Y)$, és végül, Y-t behelyetesítjük 0-val. ■

4.7.23. tétel. $\Delta(f) = (-1)^{\frac{n(n-1)}{2}} \frac{1}{a_0} \operatorname{Res}(f, f')$.

Bizonyítás. A 4.7.22. tétel szerint $\operatorname{Res}(f, f') = a_0^{n-1} \prod_{i=1}^{n} f'(\alpha_i)$. Mivel

$$f' = a_0 \sum_{i=1}^{n} \prod_{j \neq i}(X - \alpha_i),$$

következik, hogy $f'(\alpha_i) = a_0 \prod_{j \neq i}(\alpha_i - \alpha_j)$, tehát

$$\begin{aligned}\operatorname{Res}(f, f') &= a_0^{2n-1} \prod_{i=1}^{n}\prod_{j \neq i}(\alpha_i - \alpha_j)\\ &= a_0(-1)^{\frac{n(n-1)}{2}} a_0^{2n-2} \prod_{j<i}(\alpha_i - \alpha_j)^2\\ &= a_0(-1)^{\frac{n(n-1)}{2}} \Delta(f). \qquad ■\end{aligned}$$

4.33. feladat. Számítsuk ki a következő komplex együtthatós polinomok diszkriminánsát:
a) $f = aX^2 + bX + c$.
b) $f = X^3 + aX + b$.
c) $f = X^3 + aX^2 + bX + c$.
d) $f = X^n + a$.
e) $f = X^n + X^{n-1} + \dots + X + 1$.

4.34. feladat. Számítsuk ki az $\operatorname{Res}(f, g)$ rezultánst, ahol
a) $f = a_0X^2 + a_1X + a_2$ és $g = b_0X^2 + b_1X + b_2$.
b) $f \in \mathbb{C}[X]$ és $g = X - a$.

4.35. feladat. Legyenek $f, g, h \in \mathbb{C}[X]$, és igazoljuk, hogy:
a) $\operatorname{Res}(fg, h) = \operatorname{Res}(f, h)\operatorname{Res}(g, h)$.
b) $\Delta(fg) = \Delta(f)\Delta(g)\operatorname{Res}(f, g)$.

4.7.5. Algebrai egyenletek

A XIX. századig az algebra fő célja a valós együtthatós algebrai egyenletek gyökeinek meghatározása volt, azaz módszereket kerestek a gyökök kifejezésére racionális függvények segítségével.

A Galois-elmélet bebizonyítja, hogy ennek a poblémának nincs mindig megoldása, vagyis léteznek algebrai egyenletek melyeknek gyökei nem fejezhetők ki racionális gyökfüggvények segítségével. Ugyanebből az elméletből következik, hogy az ötnél kisebb fokú algebrai egyenletek mindig megoldhatók gyökök segítségével.

A. A binom egyenlet: $x^n = z$, ahol $z = r(\cos t + i \sin t) \in \mathbb{C}$.
Megoldásai $x_k = \sqrt[n]{r}(\cos(t + 2k\pi)/n + i \sin(t + 2k\pi)/n)$, ahol $k \in \{0, \dots, n-1\}$.

A továbbiakban bemutatjuk a másod-, harmad- és negyedfokú egyenletek megoldását $\mathbb{C}$-ben.

B. másodfokú egyenlet: $y^2 + ay + b = 0$.
Helyettesítjük y-t $x - a/2$-vel; ekkor $x^2 = a^2/4 - b$, $x_{1,2} = \pm\sqrt{a^2/4 - b}$; következik, hogy $y_{1,2} = x_{1,2} - a/2$.

C. harmadfokú egyenlet: $y^3 + ay^2 + by + c = 0$.
Helyettesítjük y-t $x - a/3$-mal. Azt kapjuk, hogy

$$x^3 + x(b - a^2/3) + (2a^3/27 - ab/3 + c) = 0,$$

tehát elég vizsgálni az $x^3 + px + q = 0$ egyenletet.

Az x megoldást $x = u + v$ alakban keressük. Az $(u + v)^3 = u^3 + v^3 + 3uv(u + v)$-ből következik, hogy $(u + v)^3 - 3uv(u + v) - (u^3 + v^3) = 0$, azaz $x^3 - 3uvx - (u^3 + v^3) = 0$. Ekkor

$$\begin{cases} -3uv & = p \\ -(u^3 + v^3) & = q \end{cases} \iff \begin{cases} uv & = -p/3 \\ u^3 + v^3 & = -q \end{cases} \implies \begin{cases} u^3v^3 & = -p^3/27 \\ u^3 + v^3 & = -q; \end{cases}$$

következik, hogy u^3 és v^3 gyökei a következő másodfokú egyenletnek: $z^2 + qz - p^3/27 = 0$, melyeket kifejezhetünk mint: $z_{1,2} = -q/2 \pm \sqrt{p^3/27 + q^2/4}$.

Legyenek $u, v \in \mathbb{C}$ úgy, hogy $u^3 = z_1$ és $v^3 = z_2$ és $uv = -p/3$; ekkor a keresett megoldások: $x_1 = u + v$, $x_2 = \varepsilon u + \varepsilon^2 v$, $x_3 = \varepsilon^2 u + \varepsilon v$, ahol ε egy harmadrendű primitív egységgyök.

D. negyedfokú egyenlet: $y^4 + ay^3 + cy^2 + dy + e = 0$.
Helyettesítjük y-t $x - a/4$-gyel; következik, hogy elég tárgyalni az $x^4 + px^2 + qx + r = 0$ egyenletet.

Az x megoldást $x = u + v + w$ alakban keressük. Észrevesszük, hogy $(u + v + w)^2 = u^2 + v^2 + w^2 + 2(uw + vw + uv)$, azaz $(u + v + w)^2 - (u^2 + v^2 + w^2) = 2(uw + vw + uv)$. Ezt négyzetre emelve kapjuk, hogy $(u + v + w)^4 - 2(u + v + w)^2(u^2 + v^2 + w^2) + (u^2 + v^2 + w^2)^2 = 4(u^2w^2 + v^2w^2 + u^2v^2) + 8uvw(u + v + w)$. Következik, hogy

$$x^4 - 2(u^2 + v^2 + w^2)x^2 - 8uvwx - 2(u^2v^2 + u^2w^2 + v^2w^2) + u^4 + v^4 + w^4 = 0,$$

tehát

$$\begin{cases} u^2 + v^2 + w^2 & = -p/2 \\ u^2v^2 + u^2w^2 + v^2w^2 & = (p^2 - 4r)/16\,; \\ u^2v^2w^2 & = q^2/64 \end{cases}$$

következik, hogy u^2, v^2, w^2 megoldásai a

$$z^3 + (p/2)z^2 + ((p^2 - 4r)/16)z - q^2/64 = 0.$$

harmadfokú egyenletnek. Legyenek z_1, z_2, z_3 a gyökök, és legyen

$$u = \pm\sqrt{z_1},\ v = \pm\sqrt{z_2},\ w = \pm\sqrt{z_3}$$

úgy, hogy $uvw = -q/8$. Ekkor

$$x_1 = u + v + w,\ x_2 = u - v - w,\ x_3 = -u + v - w,\ x_4 = -u - v + w.$$

2. Módszer: Az $x^4 + px^2 + qx + r = 0$ egyenletet felírjuk az

$$(x^2 + (p/2) + \alpha)^2 - (2\alpha x^2 - qx + (\alpha^2 + p\alpha - r + (p^2/4)) = 0$$

alakban, ahol a második tag teljes négyzet, ha α teljesíti a $q^2 - 8\alpha(\alpha^2 + p\alpha - r + p^2/4) = 0$ egyenlőséget (vagyis α egy harmadfokú egyenlet gyöke).

Az így meghatározott α-ra felírható az $(x^2 + p/2 + \alpha)^2 - 2\alpha(x - q/(4\alpha))^2 = 0$ egyenlet, tehát elég megoldani az $x^2 - \theta x + (p/2 + \alpha + q/(2\theta)) = 0$ és $x^2 + \theta x + (p/2 + \alpha - q/(2\theta)) = 0$, másodfokú egyenleteket, ahol $\theta^2 - 2\alpha = 0$.

(A fentiekben feltételeztük, hogy $q \neq 0$. Ha $q = 0$, akkor $x^4 + px^2 + qx + r = 0$ bikvadratikus egyenlet.)

4.36. feladat (Harmadfokú egyenlet). a) Igazoljuk, hogy x_1, x_2, x_3 valóban az $x^3 + px + q = 0$ egyenlet gyökei, vagyis telyesülnek a Viete-képletek: $x_1 + x_2 + x_3 = 0$, $x_1x_2 + x_2x_3 + x_1x_3 = p$, $x_1x_2x_3 = -q$.

b) Oldjuk meg a következő egyenleteket:

1. $y^3 + 6y^2 + 21y + 52 = 0$.
2. $y^3 + 3y^2 - 3y - 14 = 0$.

c) (*Valós együtthatós egyenlet tárgyalása*) Feltételezzük, hogy $p, q \in \mathbb{R}$. Tudjuk, hogy az $f = X^3 + pX + q$ polinom diszkriminánsa $\Delta(f) = -4p^3 - 27q^2 = -108(\frac{q^2}{4} + \frac{p^3}{27})$. Igazoljuk, hogy:

1. Ha $\Delta(f) < 0$ akkor $x_1 \in \mathbb{R}$ és $x_2, x_3 \in \mathbb{C}$ konjugáltak.

2. Ha $\Delta(f) = 0$, akkor $x_1 = 2\alpha,\ x_2 = x_3 = -\alpha \in \mathbb{R}$.

3. Ha $\Delta(f) > 0$, akkor x_1, x_2, x_3 páronként különböző gyökök (*casus irreducibilis*).

4.37. feladat (Negyedfokú egyenlet). a) Igazoljuk, hogy x_1, x_2, x_3, x_4 valóban az $x^3+px^2+qx+r = 0$ egyenlet gyökei, vagyis teljesülnek a Viete-képletek: $x_1 + x_2 + x_3 + x_4 = 0$, $x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4 = p$, $x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_3 = -q$, $x_1x_2x_3x_4 = r$.

b) Oldjuk meg az $y^4 - 4y^3 - 6y^2 - 92y - 91 = 0$ egyenletet.

4.8. Integritástartományok aritmetikája

Ebben az alfejezetben A-val jelölünk egy integritástartományt és K-val az A hányadostestét, tehát

$$K = \{a/b \mid a, b \in A,\ b \neq 0\}.$$

Például, ha $A = \mathbb{Z}$, akkor $K = \mathbb{Q}$; ha $A = \mathbb{Z}[\sqrt{d}]$, akkor $K = \mathbb{Q}(\sqrt{d})$; ha $A = k[X]$ (ahol k test), akkor $K = k(X) = \{f/g \mid f, g \in k[X]\}$.

4.8.1. Oszthatóság. Prímelem és irreducibilis elem

4.8.1. definíció. Legyenek $a, b \in A$. Azt mondjuk, hogy a *osztja* b-*t* (jelölés: $a|b$), ha létezik olyan $c \in A$ amelyre $b = ac$.

4.8.2. megjegyzés. 1) A fent értelmezett „|" reláció előrendezési reláció, és általában nem szimmetrikus és nem antiszimmetrikus.

2) Ha $a|b$ és $a|c$, akkor $a|b + c$; ha $a|b$ és $a|b + c$, akkor $a|c$.

3) Ha $a|b$ és $c|d$, akkor $ac|bd$, azaz „|" kompatibilis a „·"-sal.

4.8.3. definíció. Azt mondjuk, hogy a **asszociált** b-vel (jelölés: $a \sim b$), ha $a|b$ és $b|a$.

4.8.4. megjegyzés. 1) Mivel „|" előrendezés, következik, hogy a „∼" reláció ekvivalenciareláció A-n. Jelöljük $\tilde{a}$-val az a elem asszociáltsági osztályát, azaz

$$\tilde{a} = \{b \in a \mid a \sim b\},$$

és legyen $A/_\sim = \{\tilde{a} \mid a \in A\}$ a „$\sim$" szerinti faktorhalmaz.

2) Könnyen belátható, hogy $a \sim 1 \iff a \in U(A)$; továbbá minden $a, b \in A$ esetén $a \sim b$ akkor és csak akkor, ha $b = au$, ahol $u \in U(A)$; következik, hogy $\tilde{1} = U(A)$ és

$$\tilde{a} = \{au \mid u \in U(A)\} = aU(A) = a\tilde{1}$$

minden $a \in A$ esetén.

Például: $U(\mathbb{Z}) = \{1, -1\}$ és ha $a \in \mathbb{Z}$, akkor $\tilde{a} = \{a, -a\}$.

3) Ha $a \sim b$ és $c \sim d$, akkor $ac \sim bd$, azaz „$\sim$" kompatibilis a „·"-sal; következik, hogy $(A/_\sim, \cdot)$ monoid, ahol $\tilde{a}\tilde{b} = \widetilde{ab}$.

4) Ha A test, akkor $U(A) = A^*$ és $A/_\sim = \{\{0\}, U(A)\}$.

5) Az $(A/_\sim, \cdot)$ monoidon definiáljuk a következő relációt:

$$\tilde{a} \leq \tilde{b} \iff a|b.$$

Mivel „|" előrendezés, következik, hogy a definíció nem függ a reprezentánsoktól, es a „$\leq$" reláció rendezési reláció $A/_\sim$-n. Mivel „|" kompatibilis a szorzással, következik, hogy „$\leq$" is kompatibilis. Azt mondjuk, hogy $(A/_\sim, \cdot, \leq)$ rendezett monoid. Vegyük észre, hogy

$$\min(A/_\sim, \leq) = \tilde{1}, \quad \max(A/_\sim, \leq) = \tilde{0}.$$

4.8.5. definíció. 1) Legyen $p \in A$, $p \neq 0$. Azt mondjuk, hogy p *irreducibilis elem*, ha nem invertálható és nincs valódi osztója, azaz, ha teljesíti a következő feltételeket:

1. $p \not\sim 1$.

2. Minden $a, b \in A$ esetén, ha $p = ab$, akkor $a \sim 1$ vagy $b \sim 1$ (Másképpen, $a \sim p$ vagy $b \sim p$).

2) Legyen $p \in A$, $p \neq 0$. Azt mondjuk, hogy p *prímelem*, ha teljesíti a következő feltételeket:

1. $p \not\sim 1$.

2. Minden $a, b \in A$ esetén, ha $p|ab$, akkor $p|a$ vagy $p|b$.

4.8.6. tétel. *Ha $p \in A$ egy prímelem, akkor p irreducibilis elem.*

Bizonyítás. Mivel p prímelem következik, hogy $p \not\sim 1$.
Feltételezzük, hogy $p = ab$. Akkor $a|p$ és $b|p$, de mivel $p|ab$, következik, hogy $p|a$ vagy $p|b$; következik, hogy $p \sim a$ vagy $p \sim b$, tehát p irreducibilis. ■

4.8.7. definíció. Legyenek $x_1, \ldots, x_n \in A$ és $d, m \in A$.
a) d *legnagyobb közös osztója* $x_1, \ldots, x_n$*-nek* , ha $\tilde{d} = \inf_{A/\sim}\{\tilde{x}_1, \ldots, \tilde{x}_n\}$.
Jelölés: $d = \text{ln.k.o.}(x_1, \ldots, x_n) = (x_1, \ldots, x_n)$.
b) m *legkisebb közös többszöröse* $x_1, \ldots, x_n$*-nek*, ha $\tilde{m} = \sup_{A/\sim}\{\tilde{x}_1, \ldots, \tilde{x}_n\}$.
Jelölés: $m = \text{lk.k.o.}(x_1, \ldots, x_n) = [x_1, \ldots, x_n]$.

4.8.8. megjegyzés. 1) $d = (x_1, \ldots, x_n) \iff \begin{cases} d|x_1, \ldots, d|x_n, \\ \text{ha } d'|x_1, \ldots, d'|x_n, \text{ akkor } d'|d. \end{cases}$

2) $m = [x_1, \ldots, x_n] \iff \begin{cases} x_1|m, \ldots, x_n|m, \\ \text{ha } x_1|m', \ldots, x_n|m', \text{ akkor } m|m'. \end{cases}$

Vegyük észre, hogy d és m, ha léteznek, csak asszociáltság erejéig vannak meghatározva, azaz a $\tilde{d}$ és $\tilde{m}$ osztályok egyértelműen meghatározottak.

4.8.9. tétel. *Legyenek $x, y, x_1, x_2, x_3 \in A$, és feltételezzük, hogy az alábbi l.n.k.o-k léteznek.*
1) $(x_1, x_2, x_3) = ((x_1, x_2), x_3) = (x_1, (x_2, x_3))$.
1') $[x_1, x_2, x_3] = [[x_1, x_2], x_3] = [x_1, [x_2, x_3]]$.
2) $x|y \iff (x, y) = x \iff [x, y] = y$.
3) $(x_1x_3, x_2x_3) \sim (x_1, x_2)x_3$.
Partikulárisan, ha $d = (x_1, x_2), x_1 = dx_1', x_2 = dx_2'$, *akkor* $(x_1', x_2') = 1$.
4) *Ha* $(x_1, x_2) = 1$, *akkor* $(x_1, x_2x_3) = (x_1, x_3)$.
Partikulárisan, feltételezzük, hogy $(x_1, x_2) = 1$. *Ekkor*

a) *Ha* $(x_1, x_3) = 1$, *akkor* $(x_1, x_2x_3) = 1$.

b) *Ha* $x_1|x_2x_3$, *akkor* $x_1|x_3$.

5) $x_1x_2 \sim [x_1, x_2](x_1, x_2)$.

Bizonyítás. 1) Legyen $d = (x_1, x_2, x_3)$ és $d' = ((x_1, x_2), x_3)$.
Akkor $d|x_1, x_2, x_3 \iff d|x_1x_2$ és $d|x_3 \iff d|(x_1, x_2)$ és $d|x_3 \iff d|((x_1, x_2), x_3)$, azaz $d|d'$.
Fordítva következik, hogy $d'|(x_1, x_2)$ és $d'|x_3 \iff d'|x_1, d'|x_2$ és $d'|x_3 \implies d'|(x_1, x_2, x_3)$, azaz $d'|d$.
2) $x|y \iff \tilde{x} \leq \tilde{y} \iff \inf\{\tilde{x}, \tilde{y}\} = \tilde{x} \iff (x, y) = x \iff \sup\{\tilde{x}, \tilde{y}\} = \tilde{y} \iff [x, y] = y$.
3) Mivel $(x_1, x_2)|x_1$ és $(x_1, x_2)|x_2$, következik, hogy $(x_1, x_2)x_3|x_1x_3$ és $(x_1, x_2)x_3|x_2x_3$; innen kapjuk, hogy $(x_1, x_2)x_3|(x_1x_3, x_2x_3)$, tehát $(x_1x_3, x_2x_3) = (x_1, x_2)x_3y$, ahol $y \in A$.
Továbbá

$$x_1x_3 = (x_1x_3, x_2x_3)y' = (x_1, x_2)x_3yy',$$

vagyis $x_1 = (x_1, x_2)yy'$, és

$$x_2x_3 = (x_1x_3, x_2x_3)y'' = (x_1, x_2)x_3yy'',$$

vagyis $x_2 = (x_1, x_2)yy''$; következik, hogy $(x_1, x_2)y \mid x_1, x_2$, azaz $(x_1, x_2)y \mid (x_1, x_2)$. Kapjuk, hogy $y \sim 1$, vagyis $(x_1x_3, x_2x_3) \sim (x_1, x_2)$.
Partikulárisan, ha $d = (x_1, x_2) = (x_1'd, x_2'd) = d(x_1', x_2')$, akkor $(x_1', x_2') = 1$.
4) Alkalmazva a fenti tulajdonságokat

$$\begin{aligned}(x_1, x_3) &= (x_1, 1 \cdot x_3) = (x_1, (x_1, x_2)x_3) = \\ &= (x_1, (x_1x_3, x_2x_3)) = \\ &= ((x_1, x_1x_3), x_2x_3)) = \\ &= (x_1, x_2x_3).\end{aligned}$$

5) Legyen $d = (x_1, x_2), x_1 = dx_1', x_2 = dx_2'$ és $m = dx_1'x_2'$. Mivel

$$m = dx_1'x_2' = x_1x_2' = x_1'x_2,$$

következik, hogy $x_1, x_2|m$, azaz m közös többszörös.

Feltételezzük, hogy $x_1, x_2|m'$; következik, hogy $m' = x_1u = x_2v$, azaz $m' = dx_1'u = dx_2'v$. Akkor $m'x_2' = dx_1'x_2'u = mu$ és $m'x_1' = dx_1'x_2'v = mv$, vagyis $m|m'x_1'$, $m|m'x_2'$; következik, hogy $m|(m'x_1', m'x_2')$, de $(m'x_1', m'x_2') = m'(x_1', x_2') = m'$, tehát $m|m'$.

Igazoltuk, hogy $m = [x_1, x_2]$ és $x_1x_2 = ddx_1'x_2' = dm = (x_1, x_2)[x_1, x_2]$. ■

4.38. feladat. Legyenek $x_i \in A$, és feltételezzük, hogy az alábbi l.n.k.o-k léteznek.

a) $(x_1, \dots, x_n, x_{n+1}) = ((x_1, \dots, x_n), x_{n+1})$; $[x_1, \dots, x_n, x_{n+1}] = [[x_1, \dots, x_n], x_{n+1}]$.

b) $(x_1x, \dots, x_nx) \sim (x_1, \dots, x_n)x$.

c) Ha $(x, x_i) = 1$, $i = 1, \dots, n$, akkor $(x, x_1 \dots x_n) = 1$.

d) Ha $(x_i, x_j) = 1$ minden $i, j = 1, \dots, n$, $i \neq j$ esetén, akkor $[x_1, \dots, x_n] = x_1 \dots x_n$.

4.8.2. Faktoriális gyűrűk

4.8.10. definíció. Azt mondjuk, hogy A **faktoriális (Gauss-)gyűrű**, ha minden $a \in A$, $a \neq 0$ és $a \not\sim 1$ esetén az a elem felbontható irreducibilis tényezőkre és egy asszociáltságtól eltekintve a felbontás egyértelmű, azaz

1. Léteznek a $p_1, \dots, p_k$ irreducibilis tényezők úgy, hogy $a = p_1 \dots p_k$.
2. Ha $a = q_1 \dots q_l$, ahol q_i irreducibilis tényezők, akkor $k = l$ és létezik $\sigma \in S_k$ úgy, hogy $p_i \sim q_{\sigma(i)}$.

Jelölje $l(a) = k$ az a *elem hosszát.*

4.8.11. megjegyzés. Legyen A eg faktoriális gyűrű, és legyenek $a = up_1^{s_1} \dots p_m^{s_m}$, $b = vp_1^{t_1} \dots p_m^{t_m}$, ahol $s_i, t_i \geq 0$, $u, v \in U(A)$, p_i prím elemek és $p_i \not\sim p_j$, ha $i \neq j$. Ekkor

$$a|b \iff s_i \leq t_i \text{ minden } i \in \{1, \dots, m\} \text{ esetén}$$
$$a \sim b \iff s_i = t_i \text{ minden } i \in \{1, \dots, m\} \text{ esetén.}$$
$$(a, b) \sim p_1^{\min\{s_1, t_1\}} \dots p_r^{\min\{s_r, t_r\}}$$
$$[a, b] \sim p_1^{\max\{s_1, t_1\}} \dots p_r^{\max\{s_r, t_r\}}.$$

4.8.12. tétel (Faktoriális gyűrűk jellemzése). *Legyen A egy integritási tartomány. A következő állítások ekvivalensek:*

1) *A faktoriális gyűrű.*

2) *Az A gyűrű teljesíti a következő feltételeket:*

(a) *Az $(A/_\sim, \leq)$ rendezett halmazban minden szigorúan csökkenő sorozat véges (azaz ha $(a_i)_{i\geq 1}, a_i \in A$ úy, hogy $a_{i+1}|a_i$ minden $i \geq 1$ esetén, akkor létezik n úgy, hogy $\tilde{a}_i = \tilde{a}_{i+1}$ minden $i \geq n$ esetén).*

(b) *Minden $a, b \in A$ esetén létezik $(a, b) \in A$.*

3) *Az A gyűrű teljesíti a következő feltételeket:*

(a) *Az $(A/_\sim, \leq)$ rendezett halmazban minden szigorúan csökkenő sorozat véges.*

(b) *Ha $p \in A$ irreducibilis elem, akkor p prím.*

Bizonyítás. 1) $\Longrightarrow$ 2) a) Mivel $(a_i)_{i\geq 1}, a_i \in A$ úgy, hogy $a_{i+1}|a_i$ minden $i \geq 1$ esetén következik, hogy $l(a_{i+1}) \leq l(a_i)$. De $l(a_i) \in \mathbb{N}$ ezért az $l(a_i)_{i\geq 1}$ szigorúan csökkenő sorozat véges, azaz létezik $n \in \mathbb{N}$ úgy, hogy $l(a_{i+1}) = l(a_i)$ minden $i \geq n$ esetén.

b) Legyenek $a, b \in A$. Ha $a = 0$, akkor $(a, b) = b$. Ha $a \sim 1$, akkor $(a, b) = a$.

Feltételezzük, hogy $a \not\sim 1$, $b \not\sim 1$ és $a = up_1^{s_1} \dots p_m^{s_m}$, $b = vp_1^{t_1} \dots p_m^{t_m}$, ahol $s_i, t_i \geq 0$, $u, v \in U(A)$ és p_i irreducibilis elemek.

Ha $c|a$ és $c|b$, akkor, a felbontás egyértelmüségéből következik, hogy $c = wp_1^{r_1} \dots p_m^{r_m}$ alakú, ahol $r_i \leq s_i, t_i$; következik, hogy

$$(a, b) \sim p_1^{\min\{s_1, t_1\}} \dots p_m^{\min\{s_m, t_m\}}.$$

2) $\Longrightarrow$ 3) Legyen $p \in A$ egy irreducibilis elem. Akkor $p \neq 0$, $p \not\sim 1$, és feltételezzük, hogy $p|ab$, $p \nmid a$. Igazolni kell, hogy $p|b$.

Mivel $p|ab$, következik, hogy $(ab, p) = p$, de $p \nmid a$ ezért $(a, p) = 1$. Továbbá

$$(p, b) = (p, (a, p)b) = (p, (ab, pb)) = ((p, ap), ab) = (p, ab) = p,$$

tehát $p|b$.

3) $\Longrightarrow$ 1) A felbontás létezése: Legyen $a \in A,\ a \neq 0,\ a \not\sim 1$.

Ha a irreducibilis, akkor $a = a$. Ha a nem irreducibilis, akkor $a = a_1 a_1'$ következik, hogy $a_1 | a$ és $a_1 \not\sim a$ (azaz $\tilde{a_1} < \tilde{a}$). Ha a_1 nem irreducibilis, akkor $a_1 = a_2 a_2'$ következik, hogy $a_2 | a_1$ és $a_2 \not\sim a_1$ (azaz $\tilde{a_2} < \tilde{a_1}$).

Folytatva az eljárást kapunk egy $\tilde{a} > \tilde{a_1} > \tilde{a_2} > \tilde{a_3} > \dots$ végtelen csökkenő sorozatot, ellentmondás a feltevéssel.

Egyértelműség: feltételezzük, hogy $a = p_1 \dots p_n = q_1 \dots q_m$. Mivel p_i, q_i irreducibilis elemek, a feltevés szerint prímek is.

Mivel $p_1 | q_1 \dots q_m$ és p_1 prím, feltételezhetjük, hogy $p_1 | q_1$, de q_1 irreducibilis tehát $p_1 \sim q_1$; következik, hogy $p_1 \dots p_n = u_1 q_1 \dots q_m$, ahol $u_1 \sim 1$, vagyis $p_2 \dots p_n \sim q_2 \dots q_m$.

Indukcióval folytatva, kapjuk hogy $n = m$ és $p_i \sim q_i$ minden $i \in \{1, \dots, n\}$ esetén. ■

4.39. feladat. Legyen A egy faktoriális gyűrű és $a, b, c \in A$. Igazoljuk, hogy:

a) $(a, [b, c]) = [(a, b), (a, c)]$ és $[a, (b, c)] = ([a, b], [a, c])$.

b) $(a, b) = (a, c)$, $[a, b] = [a, c] \Rightarrow b \sim c$.

c) $[a, b, c][a, b][b, c][c, a] \sim abc(a, b, c)$.

4.40. feladat. Legyen A egy faktoriális gyűrű, $a, b \in A$, $m, n \in \mathbb{N}$ és $d = (m, n)$. Igazoljuk, hogy

a) Ha $a = bq + r$, akkor $(a, b) = (b, r)$.

b) Ha $(a, b) = 1$, akkor $(a^m - b^m, a^n - b^n) = a^d - b^d$.

4.41. feladat. Az A faktoriális gyűrű nek véges számú invertálható eleme van (A nem test). Igazoljuk, hogy A-ban végtelen sok nemasszociált irreducibilis elem létezik.

Alkalmazás:

a) $A = \mathbb{Z}_p[X]$;

b) $A = \mathbb{Z}[i\sqrt{d}]$, ahol $d \geq 1$.

4.42. feladat. Ha A faktoriális gyűrű és $S \subset A$ egy multiplikatív zárt rendszer, akkor $S^{-1}A$ is faktoriális.

4.8.3. Főideálgyűrűk

Ha $a \in A$ akkor $(a) = aA = \{ax \mid x \in A\}$ az a elem által generált főideál. Tekíntsük az $(\mathcal{I}(A), \subseteq)$ teljes hálót és az $(\mathcal{I}_f(A) = \{(a) \mid a \in A\}, \subseteq)$ főideálok rendezett halmazát.

4.8.13. lemma. *Ha* $\varphi : A/_\sim \to \mathcal{I}_f(A)$, $\varphi(\tilde{a}) = (a)$ *és* $\psi : \mathcal{I}_f(A) \to A/_\sim$, $\psi((a)) = (\tilde{a})$, *akkor* φ, ψ *csökkenő függvények és* $\psi = \varphi^{-1}$.

Bizonyítás. Ha $a|b$, akkor létezik $c \in A$ úgy, hogy $b = ca \in (a)$, tehát $(b) \subseteq (a)$. Fordítva, ha $(b) \subseteq (a)$, akkor $b \in (a)$, tehát $a|b$. Következik, hogy

$$a \sim b \iff a|b,\ b|a \iff (a) = (b).$$

Azonnal következik, hogy φ és ψ jól értelmezett csökkenő függvények és $\psi = \varphi^{-1}$. ■

4.8.14. definíció. Az A integritástartományt, melynek minden ideálja főideál *főideálgyűrűnek* nevezzük.

4.8.15. tétel. *Ha* A *főideálgyűrű, akkor* A *faktoriális gyűrű. Ebben az esetben minden* $a, b \in A$ *esetén*

$$d = (a, b) \iff (a) + (b) = (d),$$

$$m = [a, b] \iff (a) \cap (b) = (m).$$

Bizonyítás. Mivel A főideálgyűrű, következik, hogy $\mathcal{I}(A) = \mathcal{I}_f(A)$, tehát $(\mathcal{I}(A), \subseteq)$ és $(A/_\sim, \leq)$ antiizomorf hálók.

Ha $a, b \in A$, akkor létezik $d \in A$ úgy, hogy $(d) = \sup\{(a), (b)\} = (a) + (b)$; következik, hogy $\tilde{d} = \inf\{\tilde{a}, \tilde{b}\}$, tehát $d = (a, b)$.

Ha $a, b \in A$, akkor létezik $m \in A$ úgy, hogy $(m) = \inf\{(a), (b)\} = (a) \cap (b)$; következik, hogy $\tilde{d} = \sup\{\tilde{a}, \tilde{b}\}$, tehát $m = [a, b]$.

Igazolni kell még, hogy $A/_\sim$-ben minden szigorúan csökkenő sorozat véges. Ha $a_i \in A$, $i \in I$ egy sorozat úgy, hogy $a_{i+1} | a_i$, akkor $(a_i) \subseteq (a_{i+1})$ minden $i \geq 1$ esetén. Legyen $I = \bigcup_{i \geq 1} (a_i)$ és igazoljuk, hogy $I \trianglelefteq A$. Valóban, $I \neq \emptyset$; ha $x, y \in I$, akkor létezik i, j úgy, hogy $x \in (a_i)$ és $y \in (b_j)$; feltételezjetjük, hogy $i \leq j$, tehát $x, y \in (a_j)$, és $x - y \in (a_i) \subseteq I$. Ha $x \in I$ és $r \in A$, akkor létezik i úgy, hogy $x \in (a_i)$, tehát $rx \in (a_i) \subseteq I$.

Mivel I főideál létezik $a \in A$ úgy, hogy $I = (a)$; de $a = a \cdot 1 \in I$, tehát létezik n úgy, hogy $a \in (a_n)$; következik, hogy $I = (a_n)$ tehát $I = (a_i)$ és $a_i \sim a$ minden $i \geq n$ esetén, vagyis tehát $a_i \sim a_{i+1}$ minden $i \geq n$ esetén. ■

4.8.16. megjegyzés. 1) Ha $a, b \in A$ és $d = (a, b)$, akkor létezik $u, v \in A$ úgy, hogy

$$d = au + bv.$$

2) $(a, b) = 1 \iff$ létezik olyan $u, v \in A$ amelyre $1 = au + bv$.

Valóban ha u, v létezik és $d = (a, b)$, akkor $d|a$ és $d|b$; következik, hogy $d|au + bv = 1$, tehát $d \sim 1$, és $(a, b) = 1$. Fordítva következik a)-ből.

4.8.17. következmény. *Legyen A egy főideálgyűrű. $p \in A$ irreducibilis elem akkor és csak akkor, ha $A/(p)$ test.*

Bizonyítás. Feltételezzuk, hogy p irreducibilis. Igazolni kell, hogy $A/(p)$-ben minden nemnulla elem invertálható. Legyen $a \in A \setminus (p)$; akkor $(a, p) = 1$, tehát léteznek $u, v \in A$ úgy, hogy $au + pv = 1$. Következik, hogy $A/(p)$-ben $(a + (p))(u + (p)) = 1 + (p)$, azaz $(a + (p))^{-1} = u + (p)$.

Fordítva feltételezzuk, hogy p nem irreducibilis. Ha $p \sim 1$ akkor $(p) = A$ és $A/(p) = \{0\}$ nem test; ha $p = ab$ egy valódi felbontás A-ban, akkor $A/(p)$-ben $a + (p) \neq (p)$, $b + (p) \neq (p)$ és $(p) = (a + (p))(b + (p))$, tehát $A/(p)$ nem test, mert léteznek zérusosztók. ■

4.8.18. tétel (A kínai maradéktétel). *Legyen A egy főideálgyűrű, legyenek $a_1, \dots, a_r \in A$, $(a_i, a_j) = 1$, $1 \leq i, j \leq r$, $i \neq j$. Akkor*

$$A/(a_1) \times \cdots \times A/(a_r) \simeq A/(a_1 \cdots a_r).$$

Bizonyítás. Legyen $f : A \to A/(a_1) \times \cdots \times A/(a_r)$ $f(x) = (x + (a_1), \dots, x + (a_r))$. Igazoljuk, hogy f gyűrűmorfizmus:

$$\begin{aligned} f(x + y) &= (x + y + (a_1), \dots, x + y + (a_r)) = (x + (a_1) + y + (a_1), \dots, x + (a_r) + y + (a_r)) = \\ &= (x + (a_1), \dots, x + (a_r)) + (y + (a_1), \dots, y + (a_1)) = f(x) + f(y); \\ f(xy) &= (xy + (a_1), \dots, xy + (a_r)) = ((x + (a_1))(y + (a_1)), \dots, (x + (a_r))(y + (a_r))) = \\ &= (x + (a_1), \dots, x + (a_r))(y + (a_1), \dots, y + (a_1)) = f(x)f(y). \end{aligned}$$

Meghatározzuk $\operatorname{Ker} f$-et:

$$\begin{aligned} \operatorname{Ker} f &= \{x \in A \mid f(x) = (x + (a_1), \dots, x + (a_r)) = ((a_1), \dots, (a_r))\} = \\ &= \{x \in A \mid a_i|x,\ i = 1, \dots, r\} = \\ &= \{x \in A \mid a_1 \dots a_r|x\} = (a_1 \dots a_r). \end{aligned}$$

Az I. izomorfizmustételből, következik, hogy létezik az

$$\bar{f} : A/\operatorname{Ker} f \to \operatorname{Im} f, \quad \bar{f}(x + (a_1 \dots a_r)) = f(a) = (x + (a_1), \dots, x + (a_1))$$

izomorfizmus, ahol $A/\operatorname{Ker} f = A/(a_1 \dots a_r)$.

Végül, igazoljuk az $\bar{f}$ szürjektívitását. Pontosabban, az $\bar{f}$ morfizmus bijektivítása ekvivalens azzal, hogy bármely $b_1, \dots, b_r \in A$ esetén az

$$\begin{cases} x & \equiv b_1 \pmod{a_1} \\ & \vdots \\ x & \equiv b_r \pmod{a_r} \end{cases}$$

kongruenciarendszernek van megoldása A-ben és bármely két megoldás kongruens modulo $a_1 \cdots a_r$.

A kongruenciarendszer megoldása. A következő jelöléseket vezetjük be: $M := a_1 \cdots a_r$, $M_i := \frac{M}{a_i}$. Itt $(M_i, a_i) = 1$ mert $(a_i, a_j) = 1$ minden $i \neq j$ esetén. Következik, hogy léteznek $u_i, v_i \in A$ úgy, hogy $M_i u_i + a_i v_i = 1$, tehát $M_i u_i \equiv 1 \pmod{a_i}$.

Legyen $x := \sum_{i=1}^{r} b_i M_i u_i$. Ekkor $x \equiv b_i \pmod{a_i}$, mert $M_j \equiv 0 \pmod{a_i}$, ha $j \neq i$. Tehát x az egyetlen megoldás $\bmod M$. ■

4.8.4. Euklideszi gyűrűk

4.8.19. definíció. Legyen A egy integritástartomány, és $\varphi : A^* \to \mathbb{N}$ egy függvény úgy, hogy minden $a, b \in A, b \neq 0$ esetén létezik $q, r \in A$ úgy, hogy $a = bq + r$ és $r = 0$ vagy $\varphi(r) < \varphi(b)$. Akkor (A, φ)-t *euklideszi gyűrűnek* nevezzük, és φ neve pedig *euklideszi norma.*

4.8.20. példa. 1) A $(\mathbb{Z}, |\cdot|)$, ahol $\varphi(a) = |a| \in \mathbb{N}, a \in A$, euklideszi gyűrű (lásd az 1.1.1. tételt).
2) Ha K egy kommutatív test, akkor $(K[X], \deg)$, ahol $\varphi(f) = \deg f \in \mathbb{N}$, euklideszi gyűrű.
3) Legyen $d \in \mathbb{Z}$ négyzetmentes szám, $\mathbb{Z}[\sqrt{d}] = \{z \mid z = a + b\sqrt{d},\ a, b \in \mathbb{Z}\}$ és

$$N:\ \mathbb{Z}[\sqrt{d}] \to \mathbb{N},\quad N(z) = |z\bar{z}| = |a^2 - b^2 d|.$$

Ha $d \in \{\pm 1, \pm 2, 3\}$, akkor $(\mathbb{Z}[\sqrt{d}], N)\}$ euklideszi gyűrű. Ha $d \in \{-3, -5\}$, akkor $(\mathbb{Z}[\sqrt{d}], N)\}$ nem euklideszi gyűrű.
4) Ha K egy kommutatív test, $A = K[[X]]$, $f = \sum_{i \geq 0} a_i X^i$ egy formális sor, és

$$o(f) = \min\{i \geq 0 \mid a_i \neq 0\} \in \mathbb{N},$$

akkor $(K[[X]], o)$ euklideszi gyűrű.

4.8.21. tétel. *Ha A euklideszi gyűrű, akkor A főideálgyűrű.*

Bizonyítás. Legyen $I \trianglelefteq A$. Ha $I = \{0\}$, akkor $I = (0)$. Feltételezzük, hogy $I \neq \{0\}$ és igazoljuk, hogy létezik $a \in I$ úgy, hogy $(a) = I$.

Legyen $n = \min\{\varphi(x) \mid x \in I, x \neq 0\}$, és $a \in I$ úgy, hogy $\varphi(a) = n$. Mivel $a \in I$ következik, hogy $(a) \subseteq I$. Fordítva, legyen $b \in I$; akkor $b = aq + r$, ahol $q, r \in A$, és $r = 0$ vagy $\varphi(r) < \varphi(a)$. Mivel $r = b - aq \in I$, a $\varphi(a)$ minimalitásából következik, hogy $r = 0$, azaz $b \in (a)$, tehát $I \subseteq (a)$. ■

4.8.22. következmény (Az aritmetika alaptétele). *Minden $a \in \mathbb{Z}$, $a \notin \{-1, 0, 1\}$ esetén léteznek és jól meghatározottak a $p_1, \ldots, p_n \in \mathbb{N}$ prímszámok úgy, hogy $a = \pm p_1 \ldots p_n$.*

4.8.23. megjegyzés. a) Ha (A, φ) egy euklideszi gyűrű és $a, b \in A$, akkor létezik $(a, b) = d \in A$. A d elem meghatározható az euklideszi algoritmus segítségével: ha $b \neq 0$, akkor

$$\begin{aligned}
a &= bq_1 + r_1, & \varphi(r_1) &< \varphi(b)\\
b &= r_1 q_2 + r_2, & \varphi(r_2) &< \varphi(r_1)\\
r_1 &= r_2 q_3 + r_3, & \varphi(r_3) &< \varphi(r_2)\\
&\ldots\\
r_{n-1} &= r_n q_{n+1} + r_{n+1}, & \varphi(r_{n+1}) &< \varphi(r_n)\\
r_n &= r_{n+1} q_{n+2} + 0,
\end{aligned}$$

akkor $(a, b) = r_{n+1}$, azaz (a, b) egyenlő az utolsó nem nulla maradékkal.

Valóban, ha $a = bq + r$, akkor $(a, b) = (b, r)$; következik, hogy

$$(a, b) = (b, r_1) = (r_1, r_2) = \ldots = (r_{n-1}, r_n) = (r_n, r_{n+1}) = r_{n+1}.$$

b) Ha $d = (a, b)$, akkor léteznek $u, v \in A$ úgy, hogy $d = au + bv$. Az u és v elemek is kiszámíthatók az euklideszi algoritmusból. Valóban,

$$\begin{aligned}
(a, b) &= r_{n+1} = r_{n-1} - r_n q_{n+1} =\\
&= r_{n-1} - (r_{n-2} - r_{n-1} q_n) q_{n+1} =\\
&= r_{n-1}(1 + q_n q_{n+1}) - r_{n-2} g_{n-1} =\\
&= r_{n-1} u_{n-1} + r_{n-2} v_{n-1},
\end{aligned}$$

és indukcióval folytatjuk.

4.8.24. tétel. *Legyen R euklideszi gyűrű és a, b, $c \in R$. Az*

$$ax + by = c$$

egyenlet akkor és csak akkor oldható meg, ha $(a, b) \mid c$. Ha az egyenletben a, b közzül legalább az egyik nem nulla, továbba az egyenlet megodható és x_0, y_0 egy megodása, akkor bármely megoldás a következő alakban áll elő:

$$x = x_0 + \frac{b}{(a, b)} t, \qquad y = y_0 - \frac{a}{(a, b)} t, \quad t \in \mathbb{R}.$$

Bizonyítás. Ha az $ax + by = c$ egyenletnek van megoldása, akkor az egyenlet bal oldalának osztója az a, b elemek legnagyobb közös osztója, ezért osztója a jobb oldalnak is, azaz $(a, b) \mid c$. Tegyük fel, hogy $(a, b) \mid c$ teljesül és $(a, b)u = c$. Ekkor a fentiek szerint az $ax = by = (a, b)$ egyenletnek van megoldása; legyen ez x_1, y_1, azaz $ax_1 + by_1 = (a, b)$. Beszorozva az egyenlőséget u-val, kapjuk: $ax_1 u + by_1 u = (a, b) = c$. Tehát $x_1 u$

és y_1u megoldása az eredeti $ax = by = c$ egyenletnek. Tegyük fel, hogy x_0, y_0 egy megoldása az $ax = by = c$ egyenletnek, és legyen x, y tetszőleges megoldás, azaz $ax_0 + by_0 = c$, $ax + by = c$, tehát

$$a(x - x_0) + b(y - y_0) = 0.$$

A feltevés szerint a, b közül legalább egyik nem 0, így $(a, b) \neq 0$. Tehát $\frac{a}{(a,b)}(x - x_0) = -\frac{b}{(a,b)}(y - y_0)$. Mivel $(\frac{a}{(a,b)}, \frac{b}{(a,b)}) = 1$, $\frac{b}{(a,b)} \mid x - x_0$ és $\frac{a}{(a,b)} \mid y - y_0$. Következik, hogy $\exists t, s \in R$ úgy, hogy

$$x = x_0 + \frac{b}{(a, b)}t, \qquad y = y_0 - \frac{a}{(a, b)}s.$$

Ha behelyettesítjük az eredeti egyenletbe, kapjuk, x, y megoldás akkor és csak akkor, ha $t = -s$. ■

4.43. feladat. Legyen $d \in \mathbb{Z}$ négyzetmentes és $N : \mathbb{Z}[\sqrt{d}] \to \mathbb{N}$, $N(z) = |z\bar{z}|$. Igazoljuk, hogy:

a) A $(\mathbb{Z}[\sqrt{d}]/\sim, \leq)$ rendezett halmaz teljesíti a minimum követelményt.

b) Ha $N(z)$ prímszám, akkor z irreducibilis.

c) A $\mathbb{Z}[i\sqrt{3}]$ gyűrűben $4 = 2 \cdot 2 = (1 - i\sqrt{3})(1 + i\sqrt{3})$ nemasszociált felbontások irreducibilis tényezőkre. (Következtessük, hogy a 2, $1 - i\sqrt{3}$, $1 + i\sqrt{3}$ irreducibilisek de nem prímek.)

d) A $\mathbb{Z}[i\sqrt{5}]$ gyűrűben $6 = 2 \cdot 3 = (1 - i\sqrt{5})(1 + i\sqrt{5})$, és $21 = 3 \cdot 7 = (4 - i\sqrt{5})(4 + i\sqrt{5})$ nemasszociált felbontások irreducibilis tényezőkre. (Következtessük, hogy a 2, 3, $1 - i\sqrt{5}$, $1 + i\sqrt{5}$, 3, 7, $4 - i\sqrt{5}$, $4 + i\sqrt{5}$ elemek irreducibilisek de nem prímek.)

Igazoljuk, hogy nem létezik l.n.k.o$(6, 2(1 + i\sqrt{5}))$.

e) A $\mathbb{Z}[i\sqrt{6}]$ gyűrűben $6 = 2 \cdot 3 = (-i\sqrt{6})(i\sqrt{6})$ nemasszociált felbontások irreducibilis tényezőkre. (Következtessük, hogy 2, 3, $-i\sqrt{6}$, $i\sqrt{6}$ irreducibilisek de nem prímek.)

f) Ha $d \leq -3$ páratlan, akkor 2 irreducibilis és nem prím $\mathbb{Z}[\sqrt{d}]$-ben.

g) Ha $d \equiv 1 \pmod 4$, akkor $\mathbb{Z}[\sqrt{d}]$ nem faktoriális.

h) Ha $d = -1, \pm 2, 3$, akkor $(\mathbb{Z}[\sqrt{d}], N)$ euklideszi gyűrű.

4.44. feladat. a)* Ha A egy főideálgyűrű, akkor $A[[X]]$ faktoriális.

b) $(K[[X]], o)$ euklideszi gyűrű, ahol $o(f)$ az f rendje.

c) $K[[X, Y]] = K[[X]][[Y]]$ faktoriális.

4.45. feladat. Az A faktoriális gyűrűben az irreducibilis elemek száma véges. Igazoljuk, hogy A euklideszi gyűrű. *Alkalmazás*: Igazoljuk, hogy az alábbi gyűrűk teljesítik a feltételt:

a) $A = \mathbb{Z}_{(p)} = \{\frac{a}{b} \mid p \nmid b\}$;

b) $A = K[[X]]$.

4.8.5. Polinomgyűrűk aritmetikája

Ebben a paragrafusban részletesen vizsgáljuk a polinomgyűrűk aritmetikai tulajdonságait. Mivel $K[X]$-ben érvényes a maradékos osztás tétele, az első eredményünk a következő:

4.8.25. tétel. $(K[X], \deg)$ *euklideszi gyűrű.*

4.8.26. példa. 1) Ha $f \in K[X]$ és $\deg f = 1$, akkor f irreducibilis polinom.

2) Ha $\deg f = 2$ vagy $\deg f = 3$, akkor f irreducibilis akkor és csak akkor, ha f-nek nincs gyöke K-ban.

Valóban, ha $f(a) = 0$, akkor Bezout-tétel szerint $f = (X - a)g$, vagyis f nem irreducibilis. Fordítva, feltételezzük, hogy f-nek nincs gyöke K-ban és legyen $f = gh$, ahol $\deg g$, $\deg h \geq 1$. Ha $\deg g = 1$, akkor $g = aX + b$ és $-b/a$ gyöke g-nek; következik, hogy $f(-b/a) = 0$, vagyis f-nek van gyöke K-ban, ellentmondás.

3) Az $f = X^4 + 1 \in \mathbb{R}[X]$ polinomnak nincs gyöke $\mathbb{R}$-ben, de

$$f = X^4 + 2X^2 + 1 - 2X^2 = (X^2 + \sqrt{2}X + 1)(X^2 - \sqrt{2}X + 1)$$

reducíbilis.

4) A K testet algebrailag zártnak nevezzük, ha minden $f \in K[X]$, $\deg f \geq 1$ esetén f-nek van gyöke K-ban (például $\mathbb{C}$ algebrailag zárt); következik, hogy az $f \in K[X]$ polinom akkor és csak akkor irreducibilis, ha $\deg f = 1$.

5) Az $f \in \mathbb{R}$ polinom akkor és csak akkor irreducibilis, ha $\deg f = 1$ vagy ha $\deg f = 2$ és $\Delta(f) < 0$.

4.8.27. megjegyzés. 1) Az $A[X]$ gyűrűben $f \sim 1 \iff f \in U(A)$, és

$$f \sim g \iff (\exists) a \in U(A) : g = af.$$

2) A $K[X]$ gyűrűben $f \sim 1 \iff f \in K^*$, és

$$f \sim g \iff (\exists) a \in K^* : g = af.$$

4.8.28. tétel. *Ha* A *nem test, akkor* $A[X]$ *nem főideálgyűrű.*

Bizonyítás. Igazoljuk, hogy létezik $I \trianglelefteq A[X]$ úgy, hogy I nem főideál.

Mivel A nem test, létezik $a \in A$, $a \neq 0$ nem invertálható elem. Legyen

$$I = (a, X) = \{ag + Xh \mid g, h \in A[X]\} \trianglelefteq A[X].$$

Feltételezzük, hogy létezik $f \in A[X]$ úgy, hogy $(a, X) = f$. Ekkor léteznek $g \in A[X]$ úgy, hogy $a = fg$ és $h \in A[X]$ úgy, hogy $X = fh$; következik, hogy $\deg f = 0$, azaz $f \in A$, és f invertálható mert $fh = X$. Akkor $(f) = A[X] = (a, X)$, tehát léteznek $u, v \in A[X]$ úgy, hogy $1 = au + vX$; következik, hogy $v = 0$, tehát $au = 1$, azaz $a \in U(A)$, ellentmondás. ■

Kijelenthetjük a paragrafus főeredményét:

4.8.29. tétel. *Ha* A *faktoriális gyűrű, akkor* $A[X]$ *is faktoriálisgyűrű.*

A tétel bizonyításához szükségünk van néhány fogalomra és segédtételre.

4.8.30. tétel. *Ha* $p \in A$ *prímelem az* A *integrítástartományban, akkor* p *prím* $A[X]$*-ben is.*

Bizonyítás. Mivel $p \in A$ prímelem következik, hogy p nem invertálható. Feltételezzük, hogy $f, g \in A[X]$ és $p|fg$, és igazoljuk, hogy $p|f$ vagy $p|g$. Legyen $f = \sum_{i=0}^{n} a_i X^i$ és $g = \sum_{j=0}^{m} b_j X^j$, ahol $a_i, b_j \in A$, és feltételezzük, hogy $p \nmid f$ és $p \nmid g$.

Ekkor létezik $k = \min\{i \geq 0 \mid p \nmid a_i\}$, $0 \leq k \leq n$ és $l = \min\{j \geq 0 \mid p \nmid b_j\}$, $0 \leq l \leq m$. Mivel $fg = \sum_{r=0}^{m+n} c_r X^r$, a fentiek alapján következik, hogy

$$p|c_{k+l} = a_0 b_{k+l} + a_1 b_{k+l-1} + \cdots + a_k b_l + \cdots + a_{k+l-1} b_1 + a_{k+l} b_0.$$

Mivel p osztja az $a_0, \ldots, a_{k-1}, b_0, \ldots, b_{l-1}$ elemeket, következik, hogy $p|a_k b_l$; de p prím, tehát $p|a_k$ vagy $p|b_l$, ellentmondás. ■

4.8.31. definíció. Legyen A egy faktoriális gyűrű, $f \in A[X]$, $f = \sum_{i=0}^{n} a_i X^i$, és

$$c(f) = (a_0, \ldots, a_n)$$

az f *tartalma.* Az f polinomot *primitív polinomnak* nevezzük, ha $c(f) \sim 1$.

4.8.32. megjegyzés. $f = c(f) \cdot f'$, ahol $c(f) \in A$ és $f' \in A[X]$ primitív polinom. Ez a felírás egyértlmű, azaz ha $f = af' = bf''$, ahol $f', f'' \in A[X]$ primitív polinomok, akkor $a \sim b$ és $f' \sim f''$.

4.8.33. lemma (Gauss). *Legyen* A *egy faktoriális gyűrű. Ha* $f, g \in A[X]$ *primitív polinomok, akkor* fg *is primitív polinom. Általában*

$$c(fg) = c(f)c(g).$$

Bizonyítás. Feltételezzük, hogy fg nem primitív, azaz $c(fg) \nsim 1$. Ekkor létezik $p \in A$ prímelem úgy, hogy $p|c(fg)$, tehát $p|fg$. Mivel p prím $A[X]$-ben is, következik, hogy $p|f$ vagy $p|g$ ami ellentmond az f és g primitívitásának.

Általános esetben: $fg = c(f)f'c(g)g'$, ahol $f', g' \in A[X]$ és primitív polinomok, tehát $f'g'$ is primitív; ugyanakkor $fg = c(fg)h$, ahol $h \in A[X]$ primitív polinom; következik, hogy $f'g' \sim h$ és $c(f)c(g) \sim c(fg)$. ■

4.8.34. lemma. *Legyen* A *egy faktoriális gyűrű,* $K = \mathrm{frac}(A) = \{a/b \mid a, b \in A,\ b \neq 0\}$ *és* $f \in A[X]$. *Az* f $A[X]$*-ben akkor és csak akkor irreducibilis, ha* f *primitív és irreducibilis polinom* $K[X]$*-ben.*

Bizonyítás. Igazoljuk, hogy ha f primitív és irreducibilis $K[X]$-ben, akkor az f polinom irreducibilis $A[X]$-ben. Valóban, feltételezzük, hogy f nem irreducibilis az $A[X]$-ben, azaz $f = gh$, $g, h \in A[X]$ és $g, h \not\sim 1$. Mivel f primitív következik, hogy $\deg g, \deg h \geq 1$, azaz f reducíbilis $K[X]$-ben, ellentmondás.

Fordítva, feltételezzük, hogy f irreducibilis $A[X]$-ben és reducibilis $K[X]$-ben, azaz $f = gh$, ahol $g, h \in K[X]$, $\deg g$, $\deg h \geq 1$. Legyen $g = (a/b)g_1$ és $h = (c/d)h_1$, ahol $a/b, c/d \in K$ és $g_1, h_1 \in A[X]$ primitívek; következik, hogy $f = (a/b)(c/d)g_1h_1$, azaz $bdf = acg_1h_1$.

Mivel f irreducibilis $A[X]$-ben következik, hogy f primitív; de g_1h_1 is primitív (mert g_1, h_1 primitívek), tehát $bd \sim ac$ és $f \sim g_1h_1$ $A[X]$-ben, vagyis f reducibilis $A[X]$-ben, ami ellentmondás. ■

A 4.8.29. tétel bizonyítása. a) Igazoljuk, hogy $A[X]/\sim$-ben minden szigorúan csökkenő lánc véges.

Legyen $f_i \in A[X]$, $i \in \mathbb{N}$ úgy, hogy $f_{i+1}|f_i$, és igazoljuk, hogy létezik $n \in \mathbb{N}$ úgy, hogy $f_{i+1} \sim f_i$ minden $i \geq n$ esetén. Legyen $f_i = a_i g_i$, ahol $a_i \in A$ és $g_i \in A[X]$ primitív polinomok. Mivel $f_{i+1}|f_i$ következik, hogy $a_{i+1}g_{i+1}|a_i g_i$; de $(a_{i+1}, g_i) = 1$, tehát $a_{i+1}|a_i$ és $g_{i+1}|g_i$.

Az A gyűrű faktoriális, ezért létezik $n_1 \in \mathbb{N}$ úgy, hogy $a_{i+1} \sim a_i$ minden $i \geq n_1$ esetén. Mivel $g_{i+1}|g_i$ következik, hogy $\deg g_{i+1} \leq \deg g_i$, azaz létezik $n_2 \in \mathbb{N}$ úgy, hogy $\deg g_{i+1} = \deg g_i$ minden $i \geq n_2$ esetén; következik, hogy létezik $h \in A$ úgy, hogy $g_i = g_{i+1}h$, de g_i, g_{i+1} primitívek, ezért $h \sim 1$ és $g_i \sim g_{i+1}$ minden $i \geq n_2$ esetén.

Legyen $n = \max\{n_1, n_2\}$; akkor $f_i = a_i g_i \sim a_{i+1}g_{i+1} = f_{i+1}$ minden $i \geq n$ esetén.

b) Igazoljuk, hogy ha f irreducibilis $A[X]$-ben, akkor f prím.

Ha $\deg f = 0$, akkor $f \in A$ és f irreducibilis A-ban. Mivel A faktoriális következik, hogy f prím A-ban, tehát f prím $A[X]$-ben.

Feltételezzük, hogy $\deg f \geq 1$. Az 4.8.34. lemmából következik, hogy f primitív és irreducibilis $K[X]$-ben. Mivel $K[X]$ euklideszi gyűrű, faktoriális gyűrű is, ezért f prím $K[X]$-ben.

Feltételezzük, hogy $f|gh$ $A[X]$-ben; következik, hogy $f|gh$ $K[X]$-ben, tehát $f|g$ vagy $f|h$. Ha $f|g$ $K[X]$-ben akkor létezik $q \in K[X]$ úgy, hogy $g = fq$. Legyen $g = ag_1$, $q = (b/c)q_1$, ahol $a, b.c \in A$ és $g_1, q_1 \in A[X]$ primitív polinomok; ekkor $ag_1 = (b/c)fq_1$, azaz $acg_1 = bfq_1$. Alkalmazva a 4.8.33. Gauss-lemmát következik, hogy $ac \sim b$ és $g_1 \sim fq_1$. Mivel $f|g_1$ $A[X]$-ben és $(a, f) = 1$, következik, hogy $f|g$ $A[X]$-ben. ■

Végül bebizonyítunk két irreducibilitási kritériumot.

4.8.35. tétel (Eisenstein-kritérium). *Legyen A egy faktoriális gyűrű, $K = K(A)$ az A hányadosteste, $p \in A$ egy irreduciblis elem és $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$.*

Ha $p \nmid a_n$, $p|a_i$ minden $i < n$ esetén, és $p^2 \nmid a_0$, akkor f irreducibilis $K[X]$-ben (tehát $A[X]$-ben is, ha f primitív.)

Bizonyítás. Feltételezzük, hogy az f polinom primitív és reducibilis, azaz $f = gh$, ahol $g, h \in A[X]$ és $\deg g, \deg h \geq 1$.

Legyenek $g = \sum_{i=0}^{m} b_iX^i$, $h = \sum_{j=0}^{l} c_jX^j$, $m+l = n$ $(m, l \geq 1)$. Ekkor $a_n = b_mc_l$, és mivel $p \nmid a_n$ következik, hogy $p \nmid b_m$ és $p \nmid c_l$.

Mivel $a_0 = b_0c_0$, és feltevés szerint $p|a_0$, de $p^2 \nmid a_0$, feltételezhetjük, hogy $p|b_0$ és $p \nmid c_0$.

Legyen $k = \min\{j \geq 0 \mid p \nmid b_j\}$; következik, hogy $0 < k \leq m < n$, tehát $p|a_k$.

Tudjuk, hogy $a_k = b_0c_k + b_1c_{k-1} + \ldots + b_{k-1}c_1 + b_kc_0$; k minimalitásából következik, hogy $p|b_0, b_1, \ldots, b_{k-1}$ de $p \nmid b_k$ és $p \nmid c_0$, azaz $p \nmid b_kc_0$, ami ellentmondás. ■

4.8.36. tétel. *Legyenek A, B faktoriális gyűrűk, és $\varphi : A \to B$ egy szürjektív morfizmus. Létezik a*

$$\bar{\varphi} : A[X] \to B[X], \quad \bar{\varphi}(f) = \sum_{i=0}^{n} \varphi(a_i)X^i$$

szürjektív morfizmus.

Legyen $f = \sum_{i=0}^{n} a_iX^i \in A[X]$ és feltételezzük, hogy $\deg(f) = \deg(\bar{\varphi}(f)) \geq 1$ és f primitív.

Ha $\bar{\varphi}(f)$ irreducibilis $B[X]$-ben, akkor f irreducibilis $A[X]$-ben.

Bizonyítás. A $\bar{\varphi}$ morfizmus létezését és szürjektivitását a polinomgyűrű univerzális tulajdonsága biztosítja.

Feltételezzük, hogy f reducibilis $A[X]$-ben, azaz $f = gh$, ahol $g, h \in A[X]$, és $\deg g$, $\deg h \geq 1$; következik, hogy $\bar{\varphi}(f) = \bar{\varphi}(g)\bar{\varphi}(h)$. Mivel $\deg(f) = \deg(\bar{\varphi}(f))$ következik, hogy $\deg(g) = \deg(\bar{\varphi}(g)) \geq 1$ és $\deg(h) = \deg(\bar{\varphi}(h)) \geq 1$, azaz $\bar{\varphi}(f)$ reducibilis, ellentmondás. ■

4.46. feladat. a) $f \in \mathbb{C}[X]$ irreducibilis $\Leftrightarrow$ $\deg f = 1$.

b) $f \in \mathbb{R}[X]$ irreducibilis $\Leftrightarrow$ $\deg f = 1$ vagy $\deg f = 1$ és $\Delta(f) < 0$.

4.47. feladat. a) Határozzuk meg az $f \in \mathbb{Z}_2[X]$ irreducibilis polinomokat, ha $\deg f \leq 6$.

b) Határozzuk meg az $f \in \mathbb{Z}_3[X]$ irreducibilis polinomokat, ha $\deg f \leq 3$.

4.48. feladat. Legyen A egy faktoriális gyűrű, $K = K(A)$ az A hányadosteste, $\frac{r}{s} \in K$ egy irreducibilis tört, és $f = a_0 + a_1X + \cdots + a_nX^n \in A[X]$.

Ha $f(\frac{r}{s}) = 0$, akkor $r|a_0$ és $s|a_n$.

4.49. feladat. Legyen p egy prímszám és $n \neq 1$. Alkalmazva az Eisenstein-kritériumot, igazoljuk, hogy a következő polinomok irreducibilisek $\mathbb{Z}[X]$-ben:

a) $f = X^n \pm p$.

b) $f = X^{p^n} + p - 1$.

c) $f = X^{p-1} + \cdots + X + 1$.

4.50. feladat. Legyen $f = a_0 + a_1X + \cdots + a_nX^n \in \mathbb{Z}[X]$, p egy prímszám, és

$$\hat{f} = \hat{a}_0 + \hat{a}_1X + \cdots + \hat{a}_nX^n \in \mathbb{Z}_p[X].$$

Feltételezzük, hogy $p \not| a_n$. Igazoljuk, hogy, ha $\hat{f}$ irreducibilis, akkor f irreducibilis.
Alkalmazás. a) $f = X^4 - 3X^3 + 10X^2 - 6X + 1$, $p = 2$.
b) $f = X^5 - 5X^4 - 6X + 1$, $p = 5$.
c) $f = X^p - X + a$, $(a, p) = 1$.

4.9. Prímideálok és maximális ideálok

Ebben a paragrafusban A egy kommutatív egységelemes gyűrű.

4.9.1. definíció. a) A $P \trianglelefteq A$ ideált **prímideál**nak nevezzük, ha $P \neq A$ és minden $a, b \in A$ esetén, ha $ab \in P$, akkor $a \in P$ vagy $b \in P$.

b) Legyen R egy egységelemes gyűrű (nem feltétlenül kommutatív). Ha az M ideál maximális eleme az $\mathcal{I}(R) \setminus \{R\}$ rendezett halmaznak, akkor M-et **maximális ideál**nak nevezzük. (Tehát M maximális $\Leftrightarrow$ $M \neq R$ és ha $M \subseteq I \trianglelefteq R$, akkor $M = I$ vagy $I = R$.)

Jelölés:

$$\mathrm{Spec}(A) = \{P \trianglelefteq A \mid P \text{ prím}\}$$

az A *spektruma*, és

$$\mathrm{Max}(A) = \{M \trianglelefteq A \mid M \text{ maximális}\}$$

az A *maximális spektruma.*

Vegyük észre, hogy R akkor és csak akkor egyszerű gyűrű, ha $\{0\}$ maximális ideál.

4.9.2. tétel (Prímideálok jellemzése). *A következő állítások ekvivalensek:*

1. P *prímideál.*
2. *Az* A/P *faktorgyűrű integritástartomány.*
3. $S := A \setminus P$ *multiplikatív zárt rendszer.*

Bizonyítás. 1) $\Longrightarrow$ 2) Mivel P prímideál következik, hogy $P \neq A$, azaz $A/P \neq \{0\}$, tehát A/P egységelemes, nem triviális és kommutatív gyűrű.

Legyen $a + P, b + P \in A/P$ úgy, hogy $(a + P)(b + P) = P$; következik, hogy $ab + P = P$, vagyis $ab \in P$. Feltevés szerint P prímideál, ezért $a \in P$ vagy $b \in P$, azaz $a + P = P$ vagy $b + P = P$. Tehát A/P zérusosztómentes.

2) $\Longrightarrow$ 1) Mivel A/P integritástartomány következik, hogy A/P-ben $1 + P \neq 0 + P$, azaz $P \neq A$.

Legyen $a, b \in A$, és feltételezzük, hogy $ab \in P$; következik, hogy $ab + P = P$, azaz $(a + P)(b + P) = P$. Mivel A/P integritástartomány $a + P = P$ vagy $b + P = P$, azaz $a \in P$ vagy $b \in P$, tehát P prímideál.

1) $\Longleftrightarrow$ 3) Akkor és csak akkor $P \neq A$, ha $1 \notin P$. Mivel S a P komplementuma, $1 \notin P$ akkor és csak akkor, ha $1 \in S$.

Legyen $a, b \in A$. Akkor ($ab \in P \Longrightarrow a \in P$ vagy $b \in P$) $\Longleftrightarrow$ ($a \notin P$ és $b \notin P \Longrightarrow ab \notin P$) $\Longleftrightarrow$ ($a \in S$ és $b \in S \Longrightarrow ab \in S$). ■

4.9.3. tétel (Maximális ideálok jellemzése). *Legyen* R *egy egységelemes gyűrű.*

a) M *akkor és csak akkor maximális ideál, ha* R/M *egyszerű gyűrű.*

b) *Ha* R *kommutatív, akkor* M *maximális* $\Leftrightarrow$ R/M *test.*

c) *Minden* $I \in \mathcal{I}(R) \setminus \{R\}$ *esetén létezik egy olyan* M *maximális ideál amelyre* $I \subseteq M$.

Bizonyítás. a) R/M nem egyszerű $\Leftrightarrow$ $(\exists)\bar{I} = I/M \trianglelefteq R/M$ nem triviális $\Leftrightarrow$ $(\exists)M \subseteq I \trianglelefteq R$ úgy, hogy $M \neq I$ és $I \neq R \Leftrightarrow (\exists)I \in \mathcal{I}(R) \setminus R:\ M \subset I \Leftrightarrow M$ nem maximális ideál.

b) Ha R kommutatív, egységelemes és $1 \neq 0$ következik, hogy egy $I \in \mathcal{I}(R) \setminus R$ esetén R/I kommutatív, egységeleme $1 + I$ és $1 + I \neq I$, hiszen ellenkező esetben következne, hogy $1 \in I \Rightarrow I = R$, ellentmondás.

Az a) pont és a fentiek alapján: M maximális ideál$\Leftrightarrow$ R/M egyszerű, kommutatív, egységelemes és $1 + M \neq M \Leftrightarrow R/M$ test.

c) Igazoljuk, hogy az $\mathcal{I}(R) \setminus \{R\}$ rendezett halmaz induktív. Valóban, legyen $\mathcal{L} = \{I_i \mid i \in \Lambda\} \subseteq \mathcal{I}(R) \setminus R$ egy lánc. Belátható akkor, hogy $T = \bigcup_{i \in \Lambda} I_i \in \mathcal{I}(R) \setminus R$, hiszen: $0 \in T$ nyilvánvalóan; $a, b \in T$ esetén $a - b \in T$, mivel $a, b \in T \Rightarrow a \in I_i,\ b \in I_j$, ahol $I_i, I_j \in \mathcal{L}$; de $\mathcal{L}$ lánc, tehát $I_i \subseteq I_j$ vagy $I_j \subseteq I_i \Rightarrow a, b \in I_i \trianglelefteq R$ vagy $a, b \in I_j \trianglelefteq R \Rightarrow a - b \in I_i$ vagy $a, b \in I_j \Rightarrow a - b \in T$; $a \in T, x \in R$ esetén $ax, xa \in T$, mivel $a \in T \Rightarrow a \in I_i$, ahol $I_i \in \mathcal{L} \Rightarrow ax, xa \in I_i \Rightarrow ax, xa \in T$; végül, $T \neq R$, mivel ellenkező esetben létezne $i \in \Lambda$ úgy, hogy $1 \in I_i \neq R$.

A Zorn-lemmából következik, hogy $\mathcal{I}(R) \setminus \{R\}$-ben léteznek maximális elemek. ■

4.9.4. következmény. *Ha* M *maximális ideálja* A*-nak, akkor* M *prímideál.*

4.9.5. tétel. *Legyen* A *integritástartomány és* $p \in A,\ p \neq 0$.
a) p *akkor és csak akkor prímelem, ha* (p) *prímideál.*
b) *Feltételezzük, hogy* A *főideálgyűrű.* p *irreducibilis elem akkor és csak akkor, ha* (p) *maximális ideál.*

Bizonyítás. a) Feltételezzük, hogy p prímelem, akkor $p \not\sim 1$, azaz $(p) \neq A$. Ha $a, b \in A$ úgy, hogy $ab \in (p)$, akkor $p|ab$. Mivel p prímelem, $p|a$ vagy $p|b$, azaz $a \in (p)$ vagy $b \in (p)$, tehát (p) prímideál.

Fordítva, feltételezzük, hogy $(p) \neq A$, akkor $p \not\sim 1$.

Legyen $a, b \in A$ úgy, hogy $p|ab$, azaz $ab \in (p)$. Mivel (p) prímideál $a \in (p)$ vagy $b \in (p)$, azaz $p|a$ vagy $p|b$, tehát p prímelem.

b) $p \in A$ irreducibilis $\Longleftrightarrow \tilde{p}$ minimális elem $(A/_\sim \setminus \{\tilde{1}\}, \leq)$-ban $\Longleftrightarrow (p)$ maximális elem $\mathcal{I}(A) \setminus \{A\}, \subseteq)$-ban. ■

4.9.6. következmény. *Ha* A *főideálgyűrű, és nem test, akkor*

$$\mathrm{Spec}(A) = \{(p) \mid p \in A,\ p \text{ irreducibilis elem}\} \cup \{(0)\},$$

$$\mathrm{Max}(A) = \{(p) \mid p \in A,\ p \text{ irreducibilis elem}\}.$$

4.51. feladat. a) $(n, X) \subseteq \mathbb{Z}[X]$ prímideál $\Leftrightarrow n$ prímszám.
b) Ha A egy integritástartomány és $a \in A$, akkor $(a, X) \subseteq A[X]$ prímideál (maximális ideál) $\Leftrightarrow (a) \subseteq A$ prím (maximális).
c) $(X),\ (X, Y) \subset \mathbb{Z}[X, Y]$ prímideálok, nem maximálisak.
d) $(X^2),\ (X^2 - 1) \subset \mathbb{Q}[X, Y]$ nem prímideálok.
e) $(X - 3),\ (X^2 + 1) \subset \mathbb{Q}[X, Y]$ prímek, nem maximálisak.
f) $(X - 3, Y - 5),\ ((X^2 + 1, Y - 5),\ (X, Y) \subset \mathbb{Q}[X, Y]$ maximális ideálok.

4.52. feladat. Ha $P \subset A$ prímideál, akkor $P[X_1, \ldots, X_n] \subset A[X_1, \ldots, X_n]$ prímideál.

4.53. feladat. Legyen $f : A \to B$ egy szürjektív morfizmus.
a) Ha $P \in \mathrm{Spec}(A)$ és $\mathrm{Ker}\, f \subseteq P$, akkor $f(P) \in \mathrm{Spec}(B)$.
b) Ha $Q \in \mathrm{Spec}(B)$, akkor $f^{-1}(Q) \in \mathrm{Spec}(A)$.

4.54. feladat. Legyen A egy kommutatív gyűrű és $r(A) = \sqrt{(0)}$ a nilpotens elemek ideálja. Igazoljuk, hogy $r(A/r(A)) = \{r(A)\}$.

4.55. feladat. Igazoljuk, hogy ha K test és $n \geq 2$, akkor $M_n(K)$ egyszerű gyűrű, és nem test.

4.56. feladat. Az A kommutatív egységelemes gyűrűt **lokális**nak nevezzük ha A-nak pontosan egy maximális ideálja van. Igazoljuk, hogy:
a) A lokális akkor és csak akkor ha az A neminvertálható elemei ideált alkotnak.
b) Ha K egy kommutatív test, akkor $K[[X]]$ lokális gyűrű.

4.57. feladat. Legyen $P \trianglelefteq A$ egy prímideál, $S = A \setminus P$ és $A_P := S^{-1}A$. Igazoljuk, hogy

$$\mathrm{Max}(A_P) = \{PA_P\}$$

(tehát A_P lokális gyűrű).

4.58. feladat. Legyen A egy kommutatív egységelemes gyűrű és $\mathfrak{m}$ egy ideálja. Azt mondjuk, hogy $\mathfrak{m}$ *minimális ideál*, ha $\mathfrak{m}$ minimális eleme az $\mathcal{I}(A) \setminus \{(0)\}$ rendezett halmaznak. Igazoljuk, hogy:
a) $\mathfrak{m}$ főideál és $\mathfrak{m}^2 = \mathfrak{m}$ vagy $\mathfrak{m} = (0)$.
b) Ha $r(A) = (0)$, akkor $(\exists) e \in A$ idempotens elem úgy, hogy $\mathfrak{m} = (e)$.

4.59. feladat. Legyen R egy egységelemes gyűrű és $I \subseteq \sqrt{(0)}$ egy ideál. Igazoljuk, hogy minden $r + I \in R/I$ idempotens elem esetén, létezik $e \in R$ idempotens úgy, hogy $e + I = r + I$.

5. fejezet

Testbővítések és Galois-elmélet

A XIV.-XVIII. századi matematika egyik legfontosabb problémája az algebrai egyenletek megoldhatósága és partikulárisan a gyökképlettel való megoldhatósága volt.

Algebrai egyenlet alatt egy $f(x) = 0$ alakú egyenletet értünk, ahol f egy valós vagy komplex együtthatójú polinom. Ennek az egyenletnek egy megoldását olyan x komplex szám jelenti, amelyre igaz a fenti egyenlőség. Az egyenlet megoldása az összes ilyen szám megkeresése, tehát az f polinom gyökeinek a meghatározása. Ez a feladat több mint 2000 éve foglalkoztatja a matematikusokat. A másodfokú egyenletek megoldására szolgáló képletek már a babilóniaknál ismert volt, a harmadfokú és negyedfokú egyenletek megoldśa pedig a reneszánsz korszakból ismert.

Niels Henrik Abel volt az első, aki megmutatta, hogy nem minden ötödfokú egyenlet oldható meg gyökképlettel. Ez a probléma a Galois-elmélet megjelenésével oldódott meg, amely kritériumokat ad a magasabb fokú egyenletek tárgyalására.

Évariste Galois (1811-1832) a XIX. század elején élt francia matematikus. Már 17 évesen olyan felfedezéseket tett, melyek új korszakot nyítottak az algebrai egyenletek elméletében. Miután több dolgozat beadásával is próbálkozott az Akadémiánál, de ezek vagy elvesztek, vagy senki nem értette meg, Galois minden energiáját a forradalmi politikának szentelte. Valószínű ez lett halálának oka is, pisztolypárbajban kapott halálos sebet. A párbaly előtti éjszakán, sietősen írta egész éjszaka a felfedezéseit. Ezek a lapok a csoportelmélet megalapozását foglalnak magukba. Írása csak akkor került nyilvánosságra, amikor Liouville 1846-ban közzétette folyóiratában. Fontosságát teljesen csak később értették meg.

Galois szükséges és elégséges feltételeket adott ahhoz, hogy egy algebrai egyenlet gyökképlettel megoldható legyen. Ennek eléréséhez Galois a testbővítésekhez hozzárendelt egy csoportot, ami ma a Galois csoport nevet viseli. Az elmélet alaptétel jelentősége abban áll, hogy általa lehetővé válik a közbülső testek tanulmányozása a Galois csoport részcsoportjain. A közbülső testnek végtelen sok, míg a Galois csoportnak csak véges sok eleme van, tehát a részcsoportok sokkal jobban kezelhetők.

Bemutatunk néhány nevezetes szerkesztési feladatot is. Megemlítjük itt a következőket: Déloszi probléma (adott kockához olyan kocka szerkesztése, melynek térfogata az eredetinek a duplája), szögharmadolás (triszekció), kör négyszögesítése (adott körrel egyenlő területű négyzet szerkesztése). Ezek nem oldható meg körzővel és vonalzóval. A kör négyszögesítésére negatív választ először F. Lindemann adott 1882-ben. Lindemann igazolta, hogy π nem algebrai szám, azaz π nem gyöke egyetlen egy racionális együtthatós (nem nulla) polinomnak sem, tehát π transzcendens szám.

A szabályos sokszögek szerkesztésével már az ókorban foglalkoztak. Euklidesz idejében ismert volt a szerkesztés 2^k, $3 \cdot 2^k$, $5 \cdot 2^k$ és $15 \cdot 2^k$ esetekben. Gauss volt az első, aki megszerkesztette az 17 oldalú szabályos sokszöget. A *„Disquisitiones arithmeticae”* című munkájában megadta, hogy melyek azok a sokszögek, amelyek szerkeszthetőek a körző és a vonalzó segítségével. Több matematikus, köztük Euler is igazolta, hogy egy szabályos n oldalú sokszög megszerkeszthető a körző és vonalzó segítségével akkor és csak akkor, ha $n = 2^k p_1 p_2 \dots p_l$, ahol $p_1, p_2, \dots, p_l$ egymástól különböző Fermat-féle prímszámok, azaz $2^{2^n} + 1$ alakúak.

A Galois-elméletnek igen sok alkalmazása van az algebra, számelmélet és geometria terén is. Egy az alaptétellel analóg tétel bizonyítható a végtelen algebrai bővítésekre is, felhasználva a topológikus csoportokat. Létezik differenciálegyenletekre vonatkozó Galois-tétel. Ezen kivül a Galois-tétel egyike a legelső és legjellemzőbb tételeknek, amelyek egy matematikai struktúrát, jelen esetben a testbővítéseket, egy másik struktúrával, itt a csoportokkal tanulmányoznak. Ma a matematikában sok irány létezik, amely hasonló célkitűzésekkel rendelkezik.

5.1. Véges bővítések

Ha egy K test részteste az L testnek, akkor L-et a K **bővítésének** nevezzük. Azt, hogy L test a K test bővítése a következő képpen jelöljük: $K \leq L$ vagy L/K. Ha $K \leq L$, akkor L K-algebra, tehát K-feletti vektortér is.

5.1.1. definíció. Legyen L/K egy testbővítés. A L dimenzióját K felett $[L : K]$-val jelöljük, és a **bővítés fokának** nevezzük:

$$[L : K] = \dim_K L$$

Azt mondjuk, hogy L **véges bővítése** K-nak, ha $[L : K]$ véges, vagyis $[L : K] < \infty$.

5.1.2. tétel (Véges bővítések tranzitivitása). *Ha $K \leq L \leq L'$ testbővítések, akkor*

$$[L' : K] = [L : K][L' : L].$$

Partikulárisan, ha $K \leq L \leq L'$ és ha a $K \leq L$, $K \leq L'$, $L \leq L'$ bővítések közül kettő véges, akkor a harmadik is véges bővítés.

Bizonyítás. Legyen $\{x_i \mid i \in I\}$ bázisa L-nek K-felett és legyen $\{y_j \mid j \in J\}$ bázisa L'-nek L-felett. Elegendő kimutatni, hogy $x_i y_j$, ahol $(i, j) \in I \times J$ bázisát alkotja a L'-nek K-felett. Ha $a \in L'$, akkor létezik $b_j \in L$, úgy, hogy $a = \sum_{j \in J} b_j y_j$, ahol az összeg véges. Minden b_j esetén létezik $\alpha_{ij} \in K$ úgy hogy $b_j = \sum_{i \in I} \alpha_{ij} x_i$. Következik, hogy

$$a = \sum_{i \in I,\ j \in J} \alpha_{ij} x_i y_j,$$

azaz a az $\{x_i y_j \mid (i, j) \in I \times J\}$ halmaz elemeinek egy lineáris kombinációja, melynek együtthatói a K testből vannak. Tehát, L' egy K-feletti vektortér melyet az $\{x_i y_j \mid (i, j) \in I \times J\}$ halmaz generál.

Feltételezzük, hogy $\sum \alpha_{ij} x_i y_j = 0$ ahol $\alpha_{ij} \in K$ és $(i, j) \in I \times J$. Kiemelve közös tényezőként, az egyenlet a következő képpen írható fel:

$$\sum_{j \in J} (\sum_{i \in I} \alpha_{ij} x_i) y_j = 0$$

ahonnan következik, hogy $\sum_{i \in I} \alpha_{ij} x_i = 0$ bármely j értékre, ahonnan következik, hogy $\alpha_{ij} = 0$, bármely $i \in I$ és bármely j-re. Tehát, a kifejezés minden együtthatója nulla. Ezzel kimutattuk, hogy az $x_i y_j$ elemek, ahol $(i, j) \in I \times J$ lineárisan függetlenek K-felett. ■

5.2. Algebrai bővítések

A továbbiakban, a test alatt kommutatív testet értünk. Legyen L a K test egy bővítése.

5.2.1. definíció. a) Azt mondjuk, hogy $a \in L$ **algebrai elem K-felett,** ha létezik $f \in K[X]$, $f \neq 0$ úgy hogy $f(a) = 0$.

Egy $a \in L$ elemet, amely nem algebrai elem K-felett **transzcendens elemnek** nevezzük K-felett.

b) Ha egy elem a $\mathbb{C}$ komplex számtestből algebrai a $\mathbb{Q}$ racionális számtest felett akkor azt az elemet **algebrai számnak** nevezzük.

Egy $\mathbb{C}$-beli elemet amely transzcendens $\mathbb{Q}$ felett, **transzcendens számnak** nevezzük.

c) A $K \leq L$ testbővítést **algebrai bővítésnek** nevezzük, ha minden $a \in L$ algebrai elem K felett.

Például, $\sqrt{2} \in \mathbb{R}$ algebrai szám, mert gyöke az $X^2 - 2 \in \mathbb{Q}[X]$ polinomnak; $i \in \mathbb{C}$ algebrai szám, mert gyöke az $X^2 + 1 \in \mathbb{Q}[X]$ polinomnak; $\pi = 3,1415\ldots$ transzcendens szám (F. Lindemann); $e = 2,71\ldots$ transzcendens szám (Ch. Hermite).

5.2.2. tétel. *Bármely véges bővítés, algebrai bővítés.*

Bizonyítás. Ha $K \leq L$ véges bővítés és $[L : K] = \dim_K L = n$, akkor minden $a \in L$ esetén az $1, a, a^2, \ldots, a^n$ elemek lineárisan függőek a L-ben. Következik, hogy léteznek K-ban az α_i, $i = 0, \ldots, n$ nem mind nulla elemek, úgy hogy

$$\alpha_0 + \alpha_1 a + \alpha_2 a^2 + \cdots + \alpha_n a^n = 0.$$

Legyen $f = \alpha_0 + \alpha_1 X + \alpha_2 X^2 + \cdots + \alpha_n X^n \in K[X]$, és $f \neq 0$. Ebből következik, hogy $f(a) = 0$, tehát a algebrai elem K felett. ■

5.2.3. definíció. a) Legyen $K \leq L$ és $A \subseteq L$. Jelöljük $K[A]$-val a K *és* A által generált részgyűrűt; $K(A)$-val jelöljük a $K \cup A$ által generált L résztestet ($K \cup A$-t tartalmazó legkisebb résztestet), és azt mondjuk, hogy K-hoz **adjunkcionáltuk** az A elemeit.

b) Sajátos esetben, ha $A = \{a_1, \ldots, a_n\}$ akkor jelöljuk $K(A) = K(a_1, \ldots, a_n)$. Egy $K \leq L$ bővítést **véges típusú bővítésnek** nevezzük, ha létezik $a_i \in L$, $(i = 1, \ldots, n)$ úgy hogy $L = K(a_1, \ldots, a_n)$.

c) Egy $K \leq L$ bővítést **egyszerű bővítésnek** nevezzük, ha létezik $a \in L$ úgy hogy $L = K(a)$. Ebben az esetben, azt mondjuk, hogy a **primitív** eleme a $K \leq L$ bővítésnek.

5.2.4. megjegyzés. 1) Bármely véges bővítés véges típusú.

Valóban, ha $K \leq L$ egy véges bővítés akkor a L-nek van egy véges $\{a_1, \dots, a_n\}$ bázisa. Következik, hogy $L = K(a_1, \dots, a_n)$.

2) $K[A] \subseteq K(A)$.

3) Ha $K \leq L$ és $A \subseteq L$, akkor $K(A) = K$ akkor és csak akkor ha $A \subseteq K$.

4) $K[a] = \{f(a) \mid f \in K[X]\} = \{\alpha_0 + \alpha_1 a + \dots + \alpha_n a^n \mid \alpha_i \in K\ ,\ n \in \mathbb{N}\}$.

5) $K(a) = \{\frac{f(a)}{g(a)} \mid f, g \in K[X], g(a) \neq 0\}$.

6) $K[A] = \{f(a_1, \dots, a_n) \mid f \in K[X_1, \dots, X_n], n \in \mathbb{N},\ a_1, \dots, a_n \in A\}$.

7) $K(A) = \{\frac{f(a_1,\dots,a_n)}{g(a_1,\dots,a_n)} \mid f, g \in K[X_1, \dots, X_n], a_1, \dots, a_n \in A, g(a_1, \dots, a_n) \neq 0,\ n \in \mathbb{N}\}$.

5.2.5. tétel. *Ha $a \in L$ algebrai elem K felett, akkor létezik egyetlen $f \in K[X]$ nemnulla polinom, úgy hogy:*

(1) $f(a) = 0$;

(2) f *főpolinom* (az f főegyütthatója 1);

(3) *ha* $g \in K[X]$, $g \neq 0$ *és* $g(a) = 0$, *akkor* $f \mid g$.

(Tehát f a legkisebb fokú nemnulla polinom, melynek a gyöke.)

Bizonyítás. Legyen $\phi : K \to L$, $\phi(\alpha) = \alpha$, és legyen $\bar{\phi}_a : K[X] \to L$, $\bar{\phi}_a(g) = \alpha_0 + \alpha_1 a + \dots + \alpha_m a^m$, ahol $g = \alpha_0 + \alpha_1 X + \dots + \alpha_m X^m \in K[X]$. A polinomgyűrű univerzális tulajdonságból következik, hogy $\bar{\phi}_a$ unitér gyűrűmorfizmus. Tehát, $\operatorname{Ker} \bar{\phi}_a = \{g \in K[X] \mid g(a) = 0\}$ ideálja, tehát főideálja, $K[X]$-nek. Mivel a algebrai következik hogy $\operatorname{Ker} \bar{\phi}_a \neq 0$, vagyis létezik $0 \neq f \in K[X]$ úgy hogy $\operatorname{Ker} \bar{\phi}_a = (f)$. Tehát, f kielégíti a tételbeli (1) és (3) feltételeket.

Mivel, hogy $(f) = (f')$ akkor és csak akkor, ha f és f' asszociáltak $K[X]$-ben következik, hogy egyetlen egy $f \in K[X]$ létezik melynek a főegyütthatója 1, úgy hogy $\operatorname{Ker} \bar{\phi}_a = (f)$. Eszerint a polinom minden feltételt kielégít a tételből. ■

5.2.6. definíció. a) Legyen $a \in L$ egy algebrai elem K felett. A fenti tételnek megfelelő f polinom neve az a elem **minimálpolinomja** K felett, és jelöljük $m_{K,a}$-val. Az a **foka** alatt $m_{K,a}$ fokát értjük.

b) Legyenek $a, b \in L$ algebrai elemek K felett. Ha a és b-nek ugyanaz a minimál polinomja K felett, akkor a és b-t **konjugáltnak** nevezzük K felett.

5.2.7. tétel (Egyszerű algebrai bővítés jellemzése). *Legyen $K \leq L$ egy testbővítés, és $a \in L$ egy algebrai elem K felett. Legyen $0 \neq f \in K[X]$.*

1) $f = m_{K,a}$ *akkor és csak akkor, ha*

(1) $f(a) = 0$;

(2) *az f főegyütthatója 1;*

(3) f *irreducibilis $K[X]$-ben.*

2) *Feltételezzük, hogy $f = \alpha_0 + \alpha_1 X + \dots + \alpha_{n-1} X^{n-1} + X^n$ az a minimálpolinomja. Akkor:*

(a) $K(a) = K[a] \simeq K[X]/(f)$;

(b) $[K(a) : K] = n = \deg f$ *és* $\{1, a, a^2, \dots, a^{n-1}\}$ *bázis $K(a)$-ban;*

(c) *A $K(a)$ K-algebra szorzásra vonatkozó művelettáblája az $1, a, a^2, \dots, a^{n-1}$ bázisban az*

$$a^n = -\alpha_0 - \alpha_1 a - \dots - \alpha_{n-1} a^{n-1}$$

egyenlőséggel van meghatározva:

(c) *Ha $b \in L$ gyöke f-nek, akkor létezik egyetlen $\phi : K(a) \to K(b)$ K-algebra izomorfizmus, úgy, hogy $\phi(a) = b$.*

Bizonyítás. 1) „$\Longrightarrow$” Felteételezzük, hogy $f = gh$, ahol $g.h \in K[X]$. Akkor $0 = f(a) = g(a)h(a)$, és mivel L test, következik, hogy $g(a) = 0$ vagy $h(a) = 0$, tehát $f \mid g$ vagy $f \mid h$; következik, hogy $f \sim g$ vagy $f \sim h$, tehát f irreducibilis.

„$\Longleftarrow$” Mivel $f(a) = 0$, következik, hogy $m_{K,a} \mid f$; de f irreducibilis, tehát $f \sim m_{K,a}$. Mivel mindkettő főpolinom, következik, hogy $f = m_{K,a}$.

2) (a) Ha $\bar{\phi}_a : K[X] \longrightarrow L$, $\bar{\phi}_a(g) = g(a)$ gyűrűmorfizmus, akkor $\operatorname{Im} \bar{\phi}_a = K[a]$ és $\operatorname{Ker} \bar{\phi}_a = (f)$. Tehát, az 1. izomorfizmustétel alapján a $K[X]/(f) \simeq K[a]$ gyűrűk izomorfak. Mivel f irreducibilis $K[X]$-ben következik, hogy f maximális ideálja $K[X]$-nek. Tehát, $K[X]/(f)$ test. Ennek következtében, $K[a]$ is test, és mivel $K[a] \subseteq K(a)$, következik, hogy $K(a) = K[a]$.

(b) Mivel a-nak a K-feletti foka n, következik, hogy az $1, a, a^2, \dots, a^{n-1}$ elemek lineárisan függetlenek K felett.

Ha $b \in K(a) = K[a]$, akkor a $K[a] = \operatorname{Im} \bar{\phi}_a$ egyenlőségből következik hogy létezik $g \in K[X]$, úgy hogy $b = g(a)$. Elosztva a g-t f-el egy q hányadost, és egy r maradékot kapunk úgy hogy: $g = fq + r$, $\deg r < \deg f$, ahonnan kapjuk:

$$b = g(a) = f(a)q(a) + r(a) = r(a)$$

és ez igazolja, hogy a $K(a)$ K-lineáris tér az $1, a, a^2, \dots, a^{n-1}$ elemek által van generálva. Tehát, $1, a, a^2, \dots, a^{n-1}$ elemek egy bázisát alkotják $K(a)$-nak K-felett.

(c) Az $f(a) = 0$ egyenlőségből következik, hogy

$$\begin{aligned} a^{n+1} &= -\alpha_0 a - \alpha_1 a^2 - \dots - \alpha_{n-1} a^n = \\ &= \alpha_{n-1}\alpha_0 - (\alpha_0 - \alpha_{n-1}\alpha_1)a - (\alpha_1 - \alpha_{n-1}\alpha_2)a^2 - \dots - (\alpha_{n-2} - \alpha_{n-1}^2)a^{n-1} \end{aligned}$$

Lépésről, lépésre haladva megkapjuk az $a^{n+2}, \dots, a^{2n-2}$-et az $1, a, a^2, \dots, a^{n-1}$ lineáris kombinációjaként.

(d) Az 1) pontól következik, hogy f minimálpolnomja b-nek is, tehát a fenti (a), (b), (c) állítások érvényesek b-re is. Tekintsük a fenti $\bar{\phi}_a : K[X] \to K(a)$ és $\bar{\phi}_b : K[X] \to K(b)$ K-algebraizomorfizmusokat. Legyen

$$\varphi : K(a) \to K(b), \quad \varphi = \bar{\phi}_b \circ \bar{\phi}_a^{-1}.$$

Akkor φ K-algebraizomorfizmus, és $\varphi(\beta_0 + \beta_1 a + \dots + \beta_{n-1}a^{n-1}) = \beta_0 + \beta_1 b + \dots + \beta_{n-1}b^{n-1}$ minden $\beta_0, \dots, \beta_{n-1} \in K$ esetén.

Mivel K és a generálja $K(a)$-t, egyetlen ilyen izomorfizmus létezik. ■

5.2.8. megjegyzés. 1) A fenti tétel alapján következik, hogy minden $b \in K(a)$ esetén létezik egy polinomiális kifejezés amely a következő alakú:

$$b = g(a) = \beta_0 + \beta_1 a + \dots + \beta_{n-1}a^{n-1} \in K(a),$$

ahol $g \in K[X]$.

2) Ha $b \in K(a)$, $b \neq 0$, akkor b a fenti alakba írható és ekkor a b^{-1} polinomiális kifejezését megkapjuk a következő képpen:

Abból a tényből, hogy f prím a $K[X]$-ben, illetve $\deg g \leq \deg f$ következik, hogy f és g relatív prímek a $K[X]$-ben, tehát, létezik $u, v \in K[X]$ úgy hogy $ug + vf = 1$, amiből következik, hogy $u(a)g(a) = 1$, mivel $f(a) = 0$. Tehát, $b^{-1} = u(a)$.

3) Ha $a \in L$ algebrai elem K felett, akkor a $K \leq K(a)$ bővítés véges, tehát algebrai is.

4) Ha a $K \leq L$ bővítés véges, akkor minden $a \in L$ algebrai K felett és az a foka osztja $[L : K]$-t.

Valóban, a 5.2.2. tételből következik hogy a algebrai K felett. Az 5.1.2. tételből pedig következik, hogy $[L : K] = [L : K(a)][K(a) : K]$. Tehát, a 5.2.7. tétel 2) pont alapján, az a foka osztja a $[L : K]$.

5) Ha $K \leq L$ és $a_1, a_2 \in L$ két algebrai elem K felett, amelynek ugyanaz a minimálpolinomja, vagyis konjugált elemek, akkor a $K(a_1)$ és $K(a_2)$ testek izomorfak.

Valóban, $K(a_1) \simeq K[X]/(f) \simeq K(a_2)$, ahol f az a_1 és a_2 minimálpolinomja.

6) Legyenek $a_1, \dots, a_n \in L$ algebrai elemek K felett. Ekkor, $K(a_1, \dots, a_n) = K[a_1, \dots, a_n]$, vagyis minden $b \in K(a_1, \dots, a_n)$ esetén létezik $g \in K[X_1, \dots, X_n]$ úgy, hogy $b = g(a_1, \dots, a_n)$.

7) Ha $K \leq L$, $L = K(a_1, \dots, a_n)$ és mindegyik a_i elem algebrai $K(a_1, \dots, a_{i-1})$ felett, ahol $(i = 1, \dots, n)$ akkor a $K \leq L$ bővítés véges, tehát algebrai is. Partikulárisan, ha $a_1, \dots a_n$ algebrai elemek K felett, akkor a $K \leq L$ bővítés véges, tehát algebrai.

Valóban, minden $m_i = [K(a_1, \dots, a_{i-1}, a_i) : K(a_1, \dots, a_{i-1})]$, $i = 1, \dots, n$ véges, és következik, hogy $[L : K] = m_1 m_2 \dots m_n$.

8) Ha $K \leq L$ és A azon elemek halmaza a L-ből melyek algebraiak a K felett, akkor $K \subseteq A$ és A egy részteste a L-nek.

Valóban, ha $a \in K$, akkor a az $X - a \in K[X]$ polinom gyöke, vagyis a algebrai K felett. Tehát, $K \subseteq A$. Ha $a_1, a_2 \in A$ akkor a 7) pontból következik, hogy a $K \leq K(a_1, a_2)$ bővítés algebrai, amiből következik, hogy $K(a_1, a_2) \subseteq A$. Mivel $a_1, a_2 \in K(a_1, a_2)$ és $K(a_1, a_2)$ egy test következik, hogy $a_1 - a_2 \in K(a_1, a_2) \subseteq A$. Ha $a_2 \neq 0$, akkor $a_1 a_2^{-1} \in K(a_1, a_2) \subseteq A$. Tehát, A részteste a L-nek.

9) Az $\mathbb{A} := \{z \in \mathbb{C} \mid z \text{ algebrai szám}\} \leq \mathbb{C}$ algebrai számok halmaza részteste $\mathbb{C}$-nek.

10) Nem minden algebrai bővítés véges, például $\mathbb{Q} \leq \mathbb{A}$ algebrai de nem véges.

5.2.9. tétel (Algebrai bővítések tranzitivitása). *Ha a $K \leq L$ és $L \leq L'$ algebrai bővítések, akkor a $K \leq L'$ bővítés is algebrai.*

Bizonyítás. Ha $a \in L'$ akkor létezik $g \in L[X]$, $0 \neq g = \beta_0 + \beta_1 X + \dots + \beta_n X^n$ úgy hogy $g(a) = 0$. Legyen $L'' := K(\beta_0, \beta_1, \dots, \beta_n)$; akkor a algebrai L felett és a 5.2.8. 7) megjegyzésből következik hogy a a $K \leq L''$ és $L'' \leq L(a)$ bővítések végesek. Tehát, a $K \leq L(a)$ bővítés véges, és $K \leq L(a)$ algebrai. Tehát, a algebrai elem K felett. ■

5.2.10. példa. 1) Ha $a \in \mathbb{R}_+$ algebrai szám, akkor $\sqrt[n]{a}$ is algebrai. Valóban, ha $f(a) = 0$, ahol $0 \neq f \in \mathbb{Q}[X]$, akkor $\sqrt[n]{a}$ gyöke az $f(X^n)$ polinomnak.

2) Az $a = \sqrt{8+\sqrt{5}} - \sqrt[7]{\sqrt{2}-\sqrt{3}}$ szám algebrai $\mathbb{Q}$ felett, hiszen az algebrai számok résztestet alkotnak.

3) $a = \pi^2 - 3\pi + 2$ nem algebrai, mert ha például $g \in \mathbb{Q}[X]$, $g \neq 0$ polinomra ha $g(a) = 0$ lenne, akkor π gyöke lenne a $g(X^2 - 3X + 2)$ polinomnak, holott π nem algebrai.

5.1. feladat. Algebraiak-e a következő számok?

a) $a = \sqrt{1+\pi^2}$

b) $b = \pi - \sqrt{\pi}$

c) $c = \pi^2 + \pi + \sqrt{1+2\pi}$.

Megoldás. a) Ha a algebrai, akkor $\pi^2 = a^2 - 1$ is algebrai, tehát π^2 gyöke egy $g \in \mathbb{Q}[X]$, $g \neq 0$ polinomnak. Tehát π gyöke a $g(X^2)$ polinomnak, ellentmondás.

b) Kifejezzük π-t: $\pi = \frac{1}{2}(2b - 1 \pm \sqrt{1-4b})$. Ha b algebrai, akkor könnyen belátható, hogy $\sqrt{1-4b}$ is algebrai, tehát π is algebrai, ellentmondás.

c) Feltételezzük, hogy c algebrai szám. Mivel $1 + 2\pi = (c - \pi^2 - \pi)^2$, következik, hogy π algebrai $\mathbb{Q}(c)$ felett, tehát $\mathbb{Q}$ felett is, a 5.2.8. 7) megjegyzés szerint.

5.2. feladat. Legyen $f = X^3 - X + 1 \in \mathbb{Q}[X]$ és legyen $a \in \mathbb{C}$ gyöke f-nek. Igazoljuk, hogy:

a) f irreducibilis és határozzuk meg $\frac{1}{a}$ értékét $\{1, a, a^2\}$ függvényében.

b) Legyen $b = 1 - 2a + 3a^2 \in \mathbb{Q}(a)$. Számítsuk ki $\frac{1}{b}$-t $\{1, a, a^2\}$ lineáris kombinációjaként.

Megoldás. a) f-nek nincs gyöke $\mathbb{Q}$-ban és $\deg f \leq 3$, ezért f irreducibilis. Továbbá $f(a) = 0$; $a^3 - a + 1 = 0$; $a^2 - 1 + \frac{1}{a} = 0$, tehát $\frac{1}{a} = -a^2 + 1$.

b) $b = 1 - 2a = 3a^2$, $\frac{1}{b} = \alpha + \beta a + \gamma a^2$, és keressük α, β, γ értékeit: $b \cdot \frac{1}{b} = 1$; $(1 - 2a + 3a^2)(\alpha + \beta a + \gamma a^2) = 1$. Felhasználva, hogy $a^3 = a - 1$ illetve $a^4 = a^2 - a$, felállítható a következő egyenletrendszer:

$$\begin{cases} \alpha - 3\beta + 2\gamma = 1 \\ -2\alpha + 4\beta - 5\gamma = 0 \\ 3\alpha - 2\beta + 4\gamma = 0 \end{cases}$$

Innen $\alpha = \frac{6}{11}$, $\beta = -\frac{7}{11}$, $\gamma = -\frac{8}{11}$, tehát, $\frac{1}{b} = \frac{6}{11} - \frac{7}{11}a - \frac{8}{11}a^2$.

5.3. feladat. a) Legyen $f = X^4 - 6X - 2 \in \mathbb{Q}[X]$. Igazoljuk, hogy f irreducibilis $\mathbb{Q}$ fölött; ha $a \in \mathbb{C}$ gyöke f-nek, számítsuk ki az $a^3 - 2a^5$, $\frac{1}{a}$ számokat az $\{1; a; a^2; a^3\}$ bázisban.

b) Legyen $f = X^4 + 6X - 2 \in \mathbb{Q}[X]$. Igazoljuk, hogy f irreducibilis $\mathbb{Q}$ fölött; ha $a \in \mathbb{C}$ gyöke f-nek, adjuk meg az $u^6 - 2u^3$ és $\frac{1}{u}$ elemeket az $\{1, u, u^2, u^3\}$ bázisban.

c) Legyen $u \in \mathbb{C}$ az $X^3 - 2X + 2$ ($\mathbb{Q}$ felett irreducibilis) polinom egyik gyöke. Adjuk meg az u^7, u^{-1} és $u^4 + u^{-2}$ elemeket az $\{1, u, u^2\}$ bázisban,

d) Legyen $u \in \mathbb{C}$ az $X^4 - 3X + 3$ ($\mathbb{Q}$ felett irreducibilis) polinom egyik gyöke. Adjuk meg az $(u^3 - 3)^{-1}(u^2 + 2)$ számot az u legfeljebb harmadfokú, racionális együtthatós polinomjaként.

e) Bizonyítsuk be, hogy ha $u \in \mathbb{C}$, az $f(x) = X^3 - 12X + 8$ polinom gyöke, akkor $\frac{u^2}{2} - 4$ is gyöke.

5.4. feladat. Határozzuk meg $K/\mathbb{Q}$ testbővítés fokát az alábbi testekre:

a) $\mathbb{Q}(\sqrt{7})$; b) $\mathbb{Q}(i\sqrt{5})$; c) $\mathbb{Q}(1 + i\sqrt{3})$;

d) $\mathbb{Q}(u + iv)$; e) $\mathbb{Q}(\sqrt{5}, \sqrt{6})$; f) $\mathbb{Q}(\sqrt{2}, \sqrt{3})$;

g) $\mathbb{Q}(i + \sqrt{5})$; h) $\mathbb{Q}(\sqrt{6} - i\sqrt{5})$; i) $\mathbb{Q}(\sqrt{3} + \sqrt{5})$.

Megoldás. a) $K = \mathbb{Q}(\sqrt{7})$; $[K : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{7}}$; $m_{\mathbb{Q},\sqrt{7}} = f = (X - \sqrt{7})(X + \sqrt{7}) = X^2 - 7 \in \mathbb{Q}[X]$ irreducibilis, mert nincs gyöke $\mathbb{Q}$-ban. Tehát, $\deg m_{\mathbb{Q},\sqrt{7}} = [K : \mathbb{Q}] = 2$; bázis: $\{1, \sqrt{7}\}$ és $K = \{\alpha + \beta\sqrt{7} \mid \alpha, \beta \in \mathbb{Q}\}$.

b) $K = \mathbb{Q}(i\sqrt{5})$; $[K : \mathbb{Q}] = \deg m_{\mathbb{Q},i\sqrt{5}}$; $m_{\mathbb{Q},i\sqrt{5}} = f = (X - i\sqrt{5})(X + i\sqrt{5}) = X^2 + 5$ irreducibilis, mert nincs gyöke $\mathbb{Q}$-ban. Tehát, $\deg m_{\mathbb{Q},i\sqrt{5}} = 2$; bázis: $\{1, i\sqrt{5}\}$ és $K = \{\alpha + \beta i\sqrt{5} \mid \alpha, \beta \in \mathbb{Q}\}$.

c) $K = \mathbb{Q}(1 + i\sqrt{3})$; $[K : \mathbb{Q}] = \deg m_{\mathbb{Q},1+i\sqrt{3}}$; $m_{\mathbb{Q},1+i\sqrt{3}} = (X - 1 - i\sqrt{3})(X - 1 + i\sqrt{3}) = X^2 - (1 + i\sqrt{3})X - (1 - i\sqrt{3})X + 4 = X^2 - 2X + 4$ irreducibilis, mert nincs gyöke $\mathbb{Q}$-ban. Tehát, $\deg m_{\mathbb{Q},1+i\sqrt{3}} = 2$; bázis: $\{1, 1 + i\sqrt{3}\}$; $K = \{\alpha + \beta + i\sqrt{3}\beta \mid \alpha, \beta \in \mathbb{Q}\}$.

d) $K = \mathbb{Q}(u + iv)$; $[K : \mathbb{Q}] = \deg m_{\mathbb{Q}}(u + iv))$; $m_{\mathbb{Q},u+i\sqrt{v}} = (X - u - i\sqrt{v})(X - u + i\sqrt{v}) = X^2 - 2uX + u^2 + v^2 \in \mathbb{Q}[X]$ irreducibilis, mert nincs gyöke $\mathbb{Q}$-ban. Tehát, $[K : \mathbb{Q}] = 2$.

e) $\mathbb{Q} \leq \mathbb{Q}(\sqrt{5}) \leq \mathbb{Q}(\sqrt{5})(\sqrt{6})$; $[K : \mathbb{Q}] = [\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}(\sqrt{5})][\mathbb{Q}(\sqrt{5}) : \mathbb{Q}]$; $[\mathbb{Q}(\sqrt{5}) : \mathbb{Q}] = 2$, mert $m_{\mathbb{Q},\sqrt{5}} = (X - \sqrt{5})(X + \sqrt{5}) = X^2 - 5 \in \mathbb{Q}[x]$ irreducibilis; $[\mathbb{Q}(\sqrt{5}, \sqrt{6}) : \mathbb{Q}(\sqrt{5})] = 2$, mert $m_{\mathbb{Q}(\sqrt{5}),\sqrt{6}} = X^2 - 6 \in \mathbb{Q}(\sqrt{5})[X]$ irreducibilis; valóban, reductio ad absurdum: feltételezzük, hogy $\sqrt{6} \in \mathbb{Q}(\sqrt{5})$; $\sqrt{6} = \alpha + \sqrt{5}\beta$, $\alpha, \beta \in \mathbb{Q}$; $\beta \neq 0$, $6 = \alpha^2 + 5\beta^2 + 2\sqrt{5}\beta\alpha$, vagyis $\begin{cases} \alpha^2 + 5\beta^2 = 6 \\ 2\beta\alpha = 0 \end{cases}$. Innen, $\alpha = 0$ és $\beta = \pm\sqrt{\frac{6}{5}}$. Legyen $\beta = \frac{m}{n}$ irreducibilis

tört, vagyis $(m,n)=1$; $\beta^2=\frac{6}{5}$, $5m^2=6n^2$; következik, hogy $5\mid 6n^2$, $5\mid n^2$, $5\mid n$ vagyis $n=5k$, $k\in\mathbb{N}$; $5m^2=6\cdot 5^2\cdot k^2$, $m^2=6\cdot 5\cdot k^2$; innen $5\mid m^2$, $5\mid m$, tehát, $m=5l$, $l\in\mathbb{N}$. $n=5k$, $m=5l$ ellentmondás azzal, hogy $(m,n)=1$. Tehát, $[K:\mathbb{Q}]=2\cdot 2=4$.

f) $\mathbb{Q}\le\mathbb{Q}(\sqrt{2})\le\mathbb{Q}(\sqrt{2})(\sqrt{3})$; $[K:\mathbb{Q}]=[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})][\mathbb{Q}(\sqrt{2}):\mathbb{Q}]$; $[\mathbb{Q}(\sqrt{2}):\mathbb{Q}]=2$, mert $m_{\mathbb{Q},\sqrt{2}}=(X-\sqrt{2})(X+\sqrt{2})=X^2-2\in\mathbb{Q}[X]$ irreducibilis $[\mathbb{Q}(\sqrt{2},\sqrt{3}):\mathbb{Q}(\sqrt{2})]=2$, mert $m_{\mathbb{Q}(\sqrt{2}),\sqrt{3}}=X^2-3\in\mathbb{Q}(\sqrt{2})[X]$ irreducibilis. Tehát, $[K:\mathbb{Q}]=4$.

g) $K=\mathbb{Q}(i+\sqrt{5})$; $[K:\mathbb{Q}]=\deg m_{\mathbb{Q},i+\sqrt{5}}$;

$$\begin{aligned}m_{\mathbb{Q},i+\sqrt{5}}&=(X-i+\sqrt{5})(X+i+\sqrt{5})(X+i-\sqrt{5})(X-i-\sqrt{5})=\\&=X^4-8X^2+36\in\mathbb{Q}[X]\end{aligned}$$

irreducibilis, mert nincs racionális gyöke és nincs másodfokú tényezője $\mathbb{Q}$-felett. Tehát, $[K:\mathbb{Q}]=4$.

h) $K=\mathbb{Q}(\sqrt{6}-i\sqrt{5})$, $[K:\mathbb{Q}]=\deg m_{\mathbb{Q},\sqrt{6}-i\sqrt{5}}$

$$\begin{aligned}m_{\mathbb{Q},\sqrt{6}-i\sqrt{5}}&=(X-\sqrt{6}-i\sqrt{5})(X-\sqrt{6}+i\sqrt{5})(X+\sqrt{6}-i\sqrt{5})(X+\sqrt{6}+i\sqrt{5})=\\&=X^4-2X^2+121\in\mathbb{Q}[X]\end{aligned}$$

irreducibilis, mert nincs racionális gyöke és nincs másodfokú tényezője $\mathbb{Q}$-felett. Tehát, $[K:\mathbb{Q}]=4$.

5.5. feladat. Igazoljuk, hogy bármilyen $n\ge 1$ esetén létezik $\mathbb{Q}$-ban egy n-ed fokú irreducibilis polinom. Következtessük, hogy minden $n\ge 1$ esetén $\mathbb{Q}$-nak van egy n-ed fokú véges bővítése.

Megoldás. Felhasználva az Eisenstein kritériumot észrevesszük, hogy minden $n\ge 1$ esetén az $f=X^n-2$ polinom irreducibilis $\mathbb{Q}$-felett.

Tehát, $\mathbb{Q}(\sqrt[n]{2})$ bővítése $\mathbb{Q}$-nak, $[\mathbb{Q}(\sqrt[n]{2}):\mathbb{Q}]=n$, minden $n\ge 1$ esetén.

5.6. feladat. Legyen $k\subseteq K$ egy testbővítés.

a) $[K:k]=1$ akkor és csak akkor, ha $k=K$.

b) Ha $[K:k]$ egy prímszám igazoljuk, hogy nem létezik olyan L test amelyen $k\subseteq L\subseteq K$, és bármely K-beli elem, amely nem szerepel a k-ban egy primitív elemét képezi a $k\subseteq K$ bővítésnek.

Megoldás. a) Ha $k\ne K$ akkor $\{1,x\}$ lineárisan független rendszer, ahol $x\in K\setminus k$. Tehát, $[K:k]\ge 2$.

b) Tekintsük a $k\subseteq L\subseteq K$ bővítések, ahol $[K:k]$ prímszám. Ekkor, $[K:L]$ osztja a $[K:k]$. Tehát, $[K:L]=1$ vagy $[K:k]=[K:L]$. Ha $[K:L]=1$ akkor $K=L$; ha $[K:k]=[K:L]$ akkor $[L:k]=1$, vagyis $L=k$.

Legyen $x\in K\setminus k$. Ekkor, $k(x)$ részteste K-nak, és tartalmazza k-t; következik, hogy $k(x)=K$.

5.7. feladat. Határozzuk meg az alábbi komplex számok minimálpolinomjait $\mathbb{Q}$ és $\mathbb{R}$ felett:

a) $\sqrt[3]{3}$; b) $1-i\sqrt{3}$; c) $2+i$; $i\sqrt[3]{3}$.

Megoldás. a) $m_{\mathbb{Q},\sqrt[3]{3}}=X^3-3$; $m_{\mathbb{R},\sqrt[3]{3}}=X-\sqrt[3]{3}$.

b) $m_{\mathbb{Q},1-i\sqrt{3}}=(X-1+i\sqrt{3})(X-1-i\sqrt{3})=X^2-2X+4$, tehát az $1-i\sqrt{3}$ minimálpolinomja $\mathbb{Q}$ felett azonos az $\mathbb{R}$ feletti minimálpolinommal.

c) $m_{\mathbb{Q},2+i}=(X+2-i)(X-2+i)=X^2-4X+5$, tehát a $2+i$ szám minimálpolinomja $\mathbb{R}$ felett azonos a $\mathbb{Q}$ feletti minimálpolinommal.

d) $m_{\mathbb{Q},i\sqrt[3]{3}}=X^6+9$; $m_{\mathbb{R},i\sqrt[3]{3}}=X^2+\sqrt[3]{9}$.

5.8. feladat. a) Ha $K\le L$ egy algebrai bővítés és K végtelen akkor K és L-nek ugyanaz a kardinálisuk, vagyis $|K|=|L|$.

b) Ha $K\le L$ egy algebrai bővítés és K véges, akkor L véges vagy megszámlálható.

Megoldás. a) Legyen $P=K[X]\setminus K$ és $P_n=\{f\in K[X]\mid \deg f\le n\}$; akkor $|P_n|=|K^n|=|K|$, és mivel $P=\bigcup_{n=1}^{\infty}P_n$, kapjuk, hogy $|P|=|K|$. Legyen $f\in P$ és $K_f:=\{a\in L\mid f(a)=0\}$. Ekkor, $L=\bigcup_{f\in P}K_f$ ahol mindegyik K_f véges; mivel $|P|=|K|$ végtelen, következik, hogy $|L|\le|K|$.

b) Az a) pontból, következik, hogy P megszámlálható, ahonnan következik, hogy L véges vagy megszámlálható.

5.9. feladat. Ha $K\le L$ és $A,B\subseteq L$, akkor $(K(A))(B)=K(A\cup B)=(K(B))(A)$.

Megoldás. A részhalmaz által generált résztest definíciójából következik, hogy:

$$K(A\cup B)=\bigcap\{L'\mid L'\le L, K\cup A\cup B\subseteq L'\}$$

$$(K(A))(B)=\bigcap\{L'\mid L'\le L, K(A)\cup B\subseteq L'\},$$

és ha $L'\le L$, akkor $K(A)\cup B\subseteq L'$ akkor és csak akkor, ha $K\cup A\cup B\subseteq L'$

5.3. Egy gyök adjunkciója. Polinom felbontási teste

Az előbbi paragrafusban, kiindulva abból hogy $K \leq L$ bővítés és az $a \in L$ algebrai elem K felett, felépítettük az L test $K(a)$ résztestét. Ehhez felhasználtuk az a minimálpolinomját, amely mint láttuk irreducibilis a K felett. A továbbiakban, kiindulunk egy K testből és egy $f \in K[X]$ irreducibilis polinomból, és fel fogunk építeni egy $K(a)/K$ bővítést, amelyet az f polinom a gyökének az adjunkciójával kapunk K-ból.

5.3.1. tétel. *Ha K egy test és $f \in K[X]$ egy irreducibilis főpolinom, akkor létezik egy L test amely a következő tulajdonságokkal rendelkezik:*

(1) *K izomorf az L test egy résztestével, vagyis K tekinthető az L test egy résztestének.*

(2) *L tartalmazza f-nek egy a gyökét úgy, hogy $L = K(a)$ és $f = m_{K,a}$.*

Bizonyítás. Mivel f irreducibilis $K[X]$-ben következik, hogy $f \notin K$ és $L = K[X]/(f)$ test. Tehát ha $\alpha \in K^*$, akkor $p(\alpha) \notin (f)$, igazolja, hogy a $p : K[X] \to L$ kanonikus projekció injektív morfizmus, vagyis L-nek a $p(K)$ részteste izomorf a K-val. Ez megengedi, hogy azonosítsuk a K-t a $p(K)$-val, és ezután L bővítése K-nak és $f \in L[x]$.

Legyen $a := X + (f) \in L$ és $f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n$. Akkor

$$f(a) = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n + (f) = f + (f) = (f),$$

amiből következik, hogy $f(a) = 0$ L-ben. Tehát, a gyöke f-nek. Mivel $K \cup \{X\}$ generálja a $K[X]$ gyűrűt és $p : K[X] \to L$ szürjektív morfizmus, következik, hogy $p(K \cup \{X\}) = K \cup \{a\}$ generálja L-et. Tehát, $L = K[a] = K(a)$. Mivel f irreducibilis, következik, hogy az α minimálpolinomja f. ■

5.3.2. példa. 1) Láttuk, hogy $X^2+1 \in \mathbb{R}[X]$ irreducibilis és $\mathbb{C} \simeq \mathbb{R}[x]/(X^2+1)$; $\mathbb{R}$ részteste $\mathbb{C}$-nek, $i := X+(X^2+1)$ gyöke az X^2+1 polinomnak, vagyis $i^2 = -1$. Így a $\mathbb{C}$ testet megkaptuk az i adjunkciójával, vagyis $\mathbb{C} = \mathbb{R}(i)$.

2) Az eddig ismert véges testek $\mathbb{Z}_p$ alakúak, ahol p egy prímszám. A fenti tételt felhasználva, más véges testeket is szerkeszthetünk. Az $f = X^2 - X - \hat{1} \in \mathbb{Z}_3[X]$ irreducibilis $\mathbb{Z}_3$ felett, mert a $\mathbb{Z}_3$ egyetlen eleme sem gyöke az f-nek. Tehát, $K := \mathbb{Z}_3[x]/(f)$ test, $a := X + (f)$ gyöke f-nek és $K = \mathbb{Z}_3(a)$. A K test elemei a következő alakúak: $u = \alpha + \beta a$, ahol $\alpha, \beta \in \mathbb{Z}_3$. Tehát $|K| = 9$.

Ha $u' = \alpha' + \beta' a \in K$ akkor $u + u' = (\alpha + \alpha') + (\beta + \beta')a$. Az uu' szorzatot megkapjuk, ha felhasználjuk, hogy $a^2 = a + \hat{1}$: $uu' = \alpha\alpha' + \beta\beta' + (\alpha\beta' + \alpha'\beta + \beta\beta')a$.

Például, abból hogy $a^2 = a + \hat{1}$ következik, hogy $a(a - \hat{1}) = \hat{1}$ ami igazolja, hogy $a^{-1} = a - \hat{1} = a + \hat{2}$. Kiszámítjuk az $\hat{1} + \hat{2}a$ inverzét, ami $\alpha + \beta a$ alakú. Az $(\alpha + \beta a)(\hat{1} + \hat{2}a) = \hat{1}$ egyenlőségből következik az $\alpha + \hat{2}\beta = \hat{1}$, $\hat{2}\alpha = \hat{0}$ egyenletrendszer, tehát $\alpha = \hat{0}$ és $\beta = \hat{2}$. Innen, $(\hat{1} + \hat{2}a)^{-1} = \hat{2}a$.

5.3.3. tétel. *Legyen K_1 és K_2 két test és*

$$f = \alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n \in K_1[X], \qquad g = \beta_0 + \beta_1 X + \cdots + \beta_n X^n \in K_2[X]$$

két n-ed fokú polinom. Legyenek $K_1(a_1)$ illetve $K_2(a_2)$ olyan testek melyeket a K_1 illetve a K_2-testbeli f illetve g polinomok egy gyökének adjunkciójából kaptunk a 5.3.1. tétel alkalmazásával. Feltételezzük, hogy f irreducibilis $K_1[X]$-ben és $\phi : K_1 \to K_2$ egy olyan izomorfizmus, mely az f-et g-be transzformálja, vagyis $\phi(\alpha_i) = \beta_i$, $i = 0, 1, \ldots, n$.

Akkor g irreducibilis $K_2[X]$-ben, és a ϕ izomorfizmus meghosszabítható egyértelműen a $\bar{\phi} : K_1(a_1) \to K_2(a_2)$ izomorfizmusig, úgy hogy $\bar{\phi}(a_1) = a_2$, ahol $a_1 = X + (f)$ és $a_2 = X + (g)$.

$$\begin{tikzcd}
K_1[X] \arrow[r, "\phi'"] \arrow[d, "p_1"'] & K_2[X] \arrow[d, "p_2"] \\
K_1(a_1) \arrow[r, dotted, "\bar{\phi}"'] & K_2(a_2)
\end{tikzcd}$$

Bizonyítás. A polinomgyűrű univerzális tulajdonsága alapján, következik hogy a ϕ izomorfizmus meghosszabítható egyértelműen egy $\phi' := \bar{\phi}_X : K_1[X] \to K_2[X]$ izomorfizmusra, úgy hogy

$$\phi'(\alpha_0 + \alpha_1 X + \cdots + \alpha_n X^n) = \phi(\alpha_0) + \phi(\alpha_1)X + \cdots + \phi(\alpha_n)X^n$$

ahonnan következik, hogy $\phi'(f) = g$. Tehát, g irreducibilis $K_2[X]$-ben. Láttuk, hogy $K_1(a_1) = K_1[X]/(f)$ és $K_2(a_2) = K_2[X]/(g)$. Ha $p_i : K_i[X] \to K_i(a_i)$, $i = 1, 2$ a kanonikus homomorfizmus, akkor $p_2 \circ \phi'$ szürjektív morfizmus.

Mivel $\phi'(f) = g$, következik, hogy φ' izomorfizmus leképezi az (f) ideált a (g) ideálra, és ebből következik hogy $\mathrm{Ker}(p_2 \circ \phi') = (f) = \mathrm{Ker}\, p_1$. Tehát, létezik egy $\bar{\phi} : K_1(a_1) \to K_2(a_2)$ izomorfizmus, úgy hogy a fennti diagramm kommutatív legyen. A diagramm kommutatívitásából, következik hogy $\bar{\phi}$ a következő képpen van meghatározva:

$$\bar{\phi}(\alpha_0 + \alpha_1 a_1 + \cdots + \alpha_{n-1} a_1^{n-1}) = \phi(\alpha_0) + \phi(\alpha_1)a_2 + \cdots + \phi(\alpha_{n-1})a_2^{n-1}$$

ahol $\alpha_i \in K$, $i = 0, 1, \ldots, n-1$, ami igazolja, hogy $\bar{\phi}$ az egyetlen ilyen izomorfizmus. ■

5.3.4. tétel. *Ha* $f \in K[X]$ *és* $\deg f = n \geq 1$, *akkor létezik egy* F/K *bővítés úgy hogy teljesüljenek a következő feltételek:*

1. f *felbontható* $F[X]$*-ben a következő képpen:* $f = a(X - x_1)\dots(X - x_n)$, *ahol* a *az* X^n *együtthatója az* f*-ben és* $x_1, \dots, x_n \in F$ *nem feltétlenül különbözőek;*
2. $F = K(x_1, \dots, x_n)$.

Bizonyítás. n szerinti indukciót alkalmazunk. Ha $n = 1$ akkor evidens, hogy $F = K$. Feltételezzük, hogy $n > 1$ és hogy a tétel igaz bármilyen K test esetén, és bármilyen $(n-1)$-ed fokú polinom esetén a $K[X]$-ből.

Mivel $K[X]$ faktoriális gyűrű, következik, hogy f-nek van egy g irreducibilis tényezője $K[X]$-ben. Tehát, $g \notin K$, és a 3.1. Tétel alapján következik, hogy létezik egy $K_1 = K(x_1)$ bővítése K-nak úgy, hogy x_1 gyöke g-nek.

Tehát, $K_1[X]$-ben $f = (X - x_1)h$, ahol $\deg h = n - 1$. Alkalmazzuk a $h \in K_1[X]$-re az indukció hipotézisét, amiből megkapjuk F-t. ■

A következő tétel azt állítja, hogy egyetlen olyan test létezik, amely eleget tesz az előbbi állításainak.

5.3.5. tétel. *Legyen* K *és* K' *két izomorf test, melyek kielégítik a 5.3.4. tétel feltételeit.*

Ha $\varphi : K \to K'$ *egy olyan izomorfizmus, mely az* f*-et* g*-be transzformálja át (vagyis* $\varphi'(f) = g$, *ahol* $\varphi' : K[X] \to K'[X]$ *izomorfizmus,* $\varphi'(a) = \varphi(a)$, *minden* $a \in K$*-ra és* $\varphi'(X) = X$*), akkor* φ *meghosszabítható a* $\bar{\varphi} : F \to F'$ *izomorfizmushoz.*

Bizonyítás. A bizonyítást $r = [F : K]$ szerinti indukcióval végezzük. Ha $r = 1$ akkor $F = K$ és $F' = L$. Tehát, ebben az esetben $\bar{\varphi} = \varphi$.

Ha $r > 1$ és a tétel igaz K bármely bővítésére mely eleget tesz a 5.3.4. tétel feltételeinek, és a K feletti fokuk kisebb mint r. Mivel $r > 1$ következik, hogy f-nek van egy irreducibilis $u \in K[X]$ osztója, $\deg u = m > 1$. Akkor $v := \varphi(u)$ g-nek irreducibilis osztója $K'[X]$-ben. Az u polinomnak van F-ben egy x_1 gyöke és v-nek F'-ben van egy x_1' gyöke. Mivel $m > 1$ és u és v irreducibilisek következik, hogy $x_1 \notin K$ és $x_1' \notin K'$ és a 5.3.3. tételből következik, hogy φ meghosszabbítható a $\varphi_1 : K(x_1) \to K'(x_1')$ izomorfizmushoz. Az 5.1.2. és 5.2.7 tételekből következik, hogy

$$[F : K] = [F : K(x_1)] \cdot m$$

ami igazolja, hogy $[F : K(x_1)] < r$. Tehát, az indukció hipotéziséből következik, hogy φ_1 meghosszabbítható a $\bar{\varphi} : F \to F'$ izomorfizmushoz. ■

5.3.6. definíció. Legyen K egy test és $f \in K[X]$, $\deg f = n \geq 1$. A 5.3.4. és 5.3.5. tételekben izomorfizmusig meghatározott F testet az f polinom K feletti **felbontási test**ének nevezzük. Jelölés: $F = F_{f,K}$.

5.3.7. megjegyzés. 1) Az $f \in K[X]$ felbontási teste (K felett) nem csak az f-től függ, hanem a K-tól is. Például, az $X^2 + 1 \in \mathbb{R}[X]$ felbontási teste $\mathbb{C}$, az $X^2 + 1 \in \mathbb{Q}[X]$ felbontási teste $\mathbb{Q}(i) = \{a + bi \mid a, b \in \mathbb{Q}\}$.

2) Legyen $f = \alpha_0 X^n + \alpha_1 X^{n-1} + \dots + \alpha_{n-1} X + \alpha_n \in K[X]$, $\deg f = n > 0$ és $x_1, \dots, x_n$ az f gyökei. Ha $u = g/h \in K(X_1, \dots, X_n)$ szimmetrikus racionális tört és $h(x_1, \dots, x_n) \neq 0$, akkor $u(x_1, \dots, x_n) \in K$.

Valóban, a szimmetrikus polinomok alaptételéből következik, hogy u felírható

$$u = g'(s_1, \dots, s_n)/h'(s_1, \dots, s_n)$$

alakban, ahol $g', h' \in K[Y_1, \dots, Y_n]$ és $s_1, \dots, s_n$ az n határozatlanú elemi szimmetrikus polinomok. Viéte képleteiből következik, hogy

$$s_i(x_1, \dots, x_n) = (-1)^i \alpha_i / \alpha_0 \in K,$$

minden $i = 1, \dots, n$ esetén.

3) Ha F az $f \in K[X]$ polinom felbontási teste, akkor 5.2.8. 7)-ből következik, hogy a $K \leq F$ bővítés algebrai.

5.10. feladat. Legyen $a = \sqrt[3]{2}$ és $K = \mathbb{Q}(a) \leq \mathbb{C}$. Számítsuk ki K-ban:
a) $a^4 - a$; b) $\frac{1}{a}$; c) $\frac{a-2}{a+2}$.

Megoldás. $f = X^3 - 2 \in \mathbb{Q}[X]$ irreducibilis, a gyöke f-nek.
a) $a^3 - 2 = 0$, $a^4 = 2a$, $a^4 - a = 2a - a = a = \sqrt[3]{2}$.
b) $a^3 - 2 = 0$, $a^2 = \frac{2}{a}$, $\frac{1}{a} = \frac{a^2}{2} = \frac{(\sqrt[3]{2})^2}{2} = \frac{1}{\sqrt[3]{2}}$.

5.11. feladat. Legyen $a = \sqrt[4]{2}$ és $K = \mathbb{Q}(a) \leq \mathbb{C}$. Számítsuk ki K-ban:
a) $\frac{1}{a}$; b) $(a^3 + 2a^2 - a + 3)(2a^3 - 4a^2 + 5a - 1)$.

5.12. feladat. Igazoljuk, hogy bármely $a, b \in \mathbb{Q}$, $a \neq b$ esetén $\mathbb{Q}(\sqrt{a}, \sqrt{b}) = \mathbb{Q}(\sqrt{a} + \sqrt{b})$

Megoldás. „$\supseteq$" $\sqrt{a} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$, $\sqrt{b} \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$, tehát $(\sqrt{a} + \sqrt{b}) \in \mathbb{Q}(\sqrt{a}, \sqrt{b})$.

„$\subseteq$" $\frac{1}{\sqrt{a}+\sqrt{b}} = \frac{\sqrt{a}-\sqrt{b}}{a-b}$ Tudva, hogy $\frac{\sqrt{a}-\sqrt{b}}{a-b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ következik, hogy $\sqrt{a} - \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$ és $\sqrt{a} + \sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$. Összeadva, illetve kivonva egymásból kapjuk, hogy $2\sqrt{a}, 2\sqrt{b} \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$, vagyis $(\sqrt{a}, \sqrt{b}) \in \mathbb{Q}(\sqrt{a} + \sqrt{b})$.

5.13. feladat. Legyen $a = \sqrt[3]{1 + \sqrt{3}}$, $K = \mathbb{Q}(\sqrt{3})$, $L = \mathbb{Q}(a)$. Igazoljuk, hogy:

a) $\mathbb{Q} \leq K \leq L$ és $L = K(a)$;
b) $[L : \mathbb{Q}] = 6$;
c) $[K : \mathbb{Q}] = 2$;
d) $[L : K] = 3$ és határozzuk meg $m_{K,a}$ minimálpolinomot.

Megoldás. a) Mivel $\sqrt[3]{1 + \sqrt{3}} \in L$ következik, hogy $a^3 = 1 + \sqrt{3} \in L$, ahonnan $\sqrt{3} = a^3 - 1 \in L$, vagyis $\mathbb{Q}(\sqrt{3}) \leq L$. Mivel $\mathbb{Q} \leq \mathbb{Q}(\sqrt{3})$ következik, hogy $\mathbb{Q} \leq K \leq L$.

b) $a = \sqrt[3]{1 + \sqrt{3}}$, $a^3 = 1 + \sqrt{3}$ ahonnan $a^3 - 1 = \sqrt{3}$. Négyzetreemelve, $a^6 - 2a^3 - 2 = 0$. Legyen $f = X^6 - 2X^3 - 2$; f irreducibilis $\mathbb{Q}$ fölött az Eisenstein kritérium alapján és $f(a) = 0$; következik, hogy $m_{\mathbb{Q},a} = f$, és vagyis $[L : \mathbb{Q}] = 6$.

c) $[K : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{3}} = 2$, mivel $m_{\mathbb{Q},\sqrt{3}} = X^2 - 3$.

d) $a = \sqrt[3]{1 + \sqrt{3}}$, $a^3 = 1 + \sqrt{3}$, $a^3 - 1 - \sqrt{3} = 0$. Legyen $g = X^3 - 1 - \sqrt{3} \in K[X]$, ami irreducibilis, $g(a) = 0$, tehát $m_{K,a} = g$. Mivel $[L : \mathbb{Q}] = [L : K][K : \mathbb{Q}]$ következik, hogy $[L : K] = 3$.

5.14. feladat. Legyen $a = \sqrt{1 + \sqrt{3}} \in K$ ahol $K = \mathbb{Q}(\sqrt{1 + \sqrt{3}})$ és legyen $L = \mathbb{Q}(\sqrt{3})$.

a) Határozzuk meg az $m_{\mathbb{Q},a}$ minimálpolinomot;
b) Igazoljuk, hogy $[K : \mathbb{Q}] = 4$;
c) Igazoljuk, hogy $\mathbb{Q} \leq L \leq K$ és $[L : \mathbb{Q}] = 2$;
d) Határozzuk meg az $m_{L,a}$ minimálpolinomot.

Megoldás. a) $a = \sqrt{1 + \sqrt{3}}$, $a^2 = 1 + \sqrt{3}$, $a^4 - 2a^2 - 2 = 0$, tehát $m_{\mathbb{Q},a} = X^4 - 2X^2 - 2$ (irreducibilis az Eisenstein kritérium alapján).

b) $[K : \mathbb{Q}] = \deg m_{\mathbb{Q},a} = 4$;

c) Igazolni kell, hogy $\sqrt{3} \in K$: $a = \sqrt{1 + \sqrt{3}} \in K$, $a^2 = 1 + \sqrt{3} \in K$, tehát $\sqrt{3} = a^2 - 1 \in K$. $[L : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{3}} = 2$, mert $m_{\mathbb{Q},\sqrt{3}} = X^2 - 3$.

d) $[K : L] = [K : \mathbb{Q}]/[L : \mathbb{Q}] = 4/2 = 2$, vagyis $K = \mathbb{Q}(a) = L(a)$. $\deg m_{L,a} = 2$, $m_{L,a} = X^2 - 1 - \sqrt{3} \in L[X]$.

5.15. feladat. Legyen $a = i\sqrt{\sqrt[3]{2} - 1}$, $L = \mathbb{Q}(a)$ és $K = \mathbb{Q}(\sqrt[3]{2})$. Igazoljuk, hogy:

a) $\mathbb{Q} \leq K \leq L$ és $L = K(a)$;
b) a gyöke az $f = X^6 - 3X^4 + 3X^2 + 1 \in \mathbb{Q}[X]$ polinomnak;
c) $a \notin K$;
d) $[L : \mathbb{Q}] = 6$ és f irreducibilis $\mathbb{Q}$ felett.

5.16. feladat. Határozzuk meg a következő polinomok felbontási testét $\mathbb{Q}$ felett, ahol $f \in \mathbb{Q}[X]$, $F = F_{f,\mathbb{Q}}$. Határozzuk meg az $F/\mathbb{Q}$ bővítés fokát es egy bázisát.

a) $f = X^3 - 3$; b) $f = X^4 + 1$; c) $f = X^4 + X^2 + 1$;
d) $f = X^4 - X^2 - 2$; e) $f = (X^2 - 6)(X^2 + 2)$; f) $f = X^4 + 9$.

Megoldás. a) $f = X^3 - 3$, f gyökei $z_k = \sqrt[3]{3} \cdot \varepsilon_k$, ahol $\varepsilon_k = \cos\frac{2k\pi}{3} + i\sin\frac{2k\pi}{3}$, $k \in \{0, 1, 2\}$ vagyis: $\varepsilon_0 = 1$, $\varepsilon_1 = \cos\frac{2\pi}{3} + i\sin\frac{2\pi}{3} = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$, $\varepsilon_2 = \cos\frac{4\pi}{3} + i\sin\frac{4\pi}{3} = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$; következik, hogy:

$$F = \mathbb{Q}(z_0, z_1, z_2) = \mathbb{Q}(\sqrt[3]{3}, \sqrt[3]{3}(-\frac{1}{2} + i\frac{\sqrt{3}}{2}), \sqrt[3]{3}(-\frac{1}{2} - i\frac{\sqrt{3}}{2}))$$

Igazoljuk, hogy $F = \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$.

„$\subseteq$" $z_0 = \sqrt[3]{3} \in \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$; $z_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2} \in \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$, és $z_2 \in \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3})$.

„$\supseteq$" $\sqrt[3]{3} \in F$, mert $z_0 = \sqrt[3]{3}$; $i\sqrt{3} \in F$, mert $i\sqrt{3} = \frac{z_1}{z_0} - \frac{z_2}{z_0} \in F$.

Kapjuk a $\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{3}) \leq \mathbb{Q}(\sqrt[3]{3}, i\sqrt{3}) = F$ összetett bővítést.

$[\mathbb{Q}(\sqrt[3]{3}) : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt[3]{3}} = 3$ mert $m_{\mathbb{Q},\sqrt[3]{3}} = X^3 - 3$; bázisa: $\{1, \sqrt[3]{3}, \sqrt[3]{9}\}$.

$[F : \mathbb{Q}(\sqrt[3]{3})] = \deg m_{\mathbb{Q}(\sqrt[3]{3})}(i\sqrt{3})) = 2$, mert $m_{\mathbb{Q}(\sqrt[3]{3}),i\sqrt{3}} = X^2 + 3$, bázis: $\{1, i\sqrt{3}\}$.

Tehát, $[F : \mathbb{Q}] = 2 \cdot 3 = 6$, bázis: $\{1, \sqrt[3]{3}, \sqrt[3]{9}, i\sqrt[3]{3} \cdot \sqrt{3}, i\sqrt[3]{9} \cdot \sqrt{3}, i\sqrt{3}\}$.

b) $f = X^4 + 1$, f gyökei: $z_k = \varepsilon_k$, $k \in \{0, 1, 2, 3\}$, ahol $z_0 = \cos\frac{\pi}{4} + i\sin\frac{\pi}{4} = \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $z_1 = \cos\frac{3\pi}{4} + i\sin\frac{3\pi}{4} = -\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}$, $z_2 = \cos\frac{5\pi}{4} + i\sin\frac{5\pi}{4} = \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$, $z_3 = \cos\frac{7\pi}{4} + i\sin\frac{7\pi}{4} = -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}$.

$F = \mathbb{Q}(-\frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} + i\frac{\sqrt{2}}{2}, -\frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2}, \frac{\sqrt{2}}{2} - i\frac{\sqrt{2}}{2})$. Igazoljuk, hogy $F = \mathbb{Q}(\sqrt{2}, i)$.
„$\subseteq$" $z_0, z_1, z_2, z_3 \in \mathbb{Q}(\sqrt{2}, i)$, mert zárt a műveletekre nézve.
„$\supseteq$" $\sqrt{2} = x_0 + x_2 \in F$, $i = \frac{z_0 - z_2}{z_0 - z_1}$.
Tehát $[F : \mathbb{Q}] = [\mathbb{Q}(\sqrt{2}) : \mathbb{Q}][\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})]$.
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{2}} = 2$, mert $m_{\mathbb{Q},\sqrt{2}} = X^2 - 2$, bázis: $\{1, \sqrt{2}\}$.
$[\mathbb{Q}(\sqrt{2}, i) : \mathbb{Q}(\sqrt{2})] = \deg m_{\mathbb{Q}(\sqrt{2},(i)} = 2$, mert $m_{\mathbb{Q}(\sqrt{2}),i} = X^2 + 1$, bázis: $\{1, i\}$.
Tehát, $[F : \mathbb{Q}] = 2 \cdot 2 = 4$, bázis: $\{1, i, \sqrt{2}, i\sqrt{2}\}$.

c) $f = X^4 + X^2 + 1 = (X^2 - X + 1)(X^2 + X + 1)$; az f gyökei: $x_1 = \frac{1+i\sqrt{3}}{2}$, $x_2 = \frac{1-i\sqrt{3}}{2}$, $x_3 = \frac{-1+i\sqrt{3}}{2}$, $x_4 = \frac{-1-i\sqrt{3}}{2}$.
$F = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(i\sqrt{3})$. Tehát, $[F : \mathbb{Q}] = 2$, bázis: $\{1, i\sqrt{3}\}$.
d) Az $f = X^4 - 2X^2 - 2$ gyökei $x_1 = \sqrt{1 + \sqrt{3}}$, $x_2 = -\sqrt{1 + \sqrt{3}}$, $x_3 = i\sqrt{\sqrt{3} - 1}$, $x_4 = -i\sqrt{\sqrt{3} - 1}$.
$F = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\sqrt{1 + \sqrt{3}}, i\sqrt{\sqrt{3} - 1})$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt{1 + \sqrt{3}}) \leq \mathbb{Q}(\sqrt{1 + \sqrt{3}}, i\sqrt{\sqrt{3} - 1}) = F$
$[\mathbb{Q}(\sqrt{1 + \sqrt{3}}) : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{1+\sqrt{3}}} = 4$, mert $m_{\mathbb{Q},\sqrt{1+\sqrt{3}}} = X^4 - 2X^2 - 2$ irreducibilis; bázis: $\{1, \sqrt{1 + \sqrt{3}}, 1 + \sqrt{3}, (1 + \sqrt{3})(\sqrt{1 + \sqrt{3}})\}$.
$[F : \mathbb{Q}(\sqrt{1 + \sqrt{3}})] = \deg m_{\mathbb{Q}(\sqrt{1+\sqrt{3}}),i\sqrt{\sqrt{3}-1}} = 2$, mert $m_{\mathbb{Q}(\sqrt{1+\sqrt{3}}),i\sqrt{\sqrt{3}-1}} = X^2 - 1 + \sqrt{3}$ ami irreducibilis, mert nincs gyöke $\mathbb{Q}(\sqrt{1 + \sqrt{3}})$-ban. $\sqrt{3} \in \mathbb{Q}(1 + \sqrt{3})$; bázis: $\{1, i\sqrt{\sqrt{3} - 1}\}$; következik, hogy $[F : \mathbb{Q}] = 8$.
e) $f = (X^2 - 6)(X^2 - 2) = (X - \sqrt{6})(X + \sqrt{6})(X - \sqrt{2})(X + \sqrt{2})$; az f gyökei: $x_1 = \sqrt{6}$, $x_2 = -\sqrt{6}$, $x_3 = \sqrt{2}$, $x_4 = -\sqrt{2}$.
$F = \mathbb{Q}(x_1, x_2, x_3, x_4) = \mathbb{Q}(\sqrt{6}, \sqrt{2}) = \mathbb{Q}(\sqrt{3}, \sqrt{2})$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}) \leq \mathbb{Q}(\sqrt{3}, \sqrt{2}) = F$.
$[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{2})} = 2$, mert $m_{\mathbb{Q},\sqrt{2}} = X^2 - 2$, $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$. Tehát, F bázisa: $\{1, \sqrt{3}, \sqrt{2}, \sqrt{6}\}$.
f) Az $f = X^4 - 9$, gyökei $z_0 = \sqrt{3}$, $z_1 = i\sqrt{3}$, $z_2 = -\sqrt{3} = (-1)z_0$, $z_3 = -i\sqrt{3}$.
$F = \mathbb{Q}(z_0, z_1, z_2, z_3) = \mathbb{Q}(\sqrt{3}, i\sqrt{3}) = \mathbb{Q}(\sqrt{3}, i)$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt{3}) \leq \mathbb{Q}(\sqrt{3}, i) = F$
$[\mathbb{Q}(\sqrt{3}) : \mathbb{Q}] = \deg m_{\mathbb{Q},\sqrt{3}} = 2$, mert $m_{\mathbb{Q}}(\sqrt{3}) = X^2 - 3$; bázis: $\{1, \sqrt{3}\}$
$[F : \mathbb{Q}(\sqrt{3})] = \deg m_{\mathbb{Q}(\sqrt{3}),i} = 2$, mert $m_{\mathbb{Q}(\sqrt{3}),i} = X^2 + 1$; bázis: $\{1, i\}$.
Tehát, $[F : \mathbb{Q}] = 2 \cdot 2 = 4$, bázis $\{1, \sqrt{3}, i, i\sqrt{3}\}$.

5.17. feladat. Határozzuk meg az $f = X^4 + X^3 + X + \hat{1}$ felbontási testét $\mathbb{Z}_2$ felett.

Megoldás. Keressük f gyökeit: $f(-1) = 1 - 1 - 1 + 1 = 0$, tehát $f = (X+1)f_1$, ahol $f_1 = X^3 + 1$. $f_1(-1) = -1 + 1 = 0$, tehát $f = (X+1)^2(X^2 - X + 1)$; $X^2 - X + 1$ irreducibilis $\mathbb{Z}_2$ fölött. Tehát, az f felbontási teste $\mathbb{Z}_2$ felett a $\mathbb{Z}_2/(X^2 - X + 1)$ négy elemű test.

5.18. feladat. Legyen $L = K(a, b)$, $f = m_{K,a}$, $g = m_{K,b}$, $\deg f = m$, és $\deg g = n$. Feltételezzük, hogy $(m, n) = 1$. Igazoljuk, hogy:
a) $[L : K] = mn$;
b) g irreducibilis $K(a)$-fölott (tehát $m_{K(a),b} = g$).

5.19. feladat. Legyen u és v két tetszőleges természetes szám. Igazoljuk, hogy $\mathbb{Q}(\sqrt{u}) = \mathbb{Q}(\sqrt{v})$ akkor és csak akkor, ha uv négyzetszám.

Megoldás. Legyen $\mathbb{Q}(\sqrt{u}) = \mathbb{Q}(\sqrt{v})$ és tegyük fel, hogy u nem négyzetszám. Mivel $\mathbb{Q}(\sqrt{u})$-ban $\{1, \sqrt{u}\}$ bázis, $\sqrt{v} \in \mathbb{Q}(\sqrt{u})$, ezért $\sqrt{v} = s + t\sqrt{u}$, ahol $s, t \in \mathbb{Q}$. Így $\exists a, b, c \in Z$, úgy hogy $a + b\sqrt{u} = c\sqrt{v}$. Akkor $a^2 + 2ab\sqrt{u} + b^2u = c^2v$, ezért $2ab = 0$ és $a^2 + b^2u = c^2v$ egyenletek egyszerre kell teljesüljenek.
1. eset: ha $a = 0$ akkor $b^2u = c^2v \Leftrightarrow b^2u^2 = c^2uv \Rightarrow uv$ négyzetszám.
2. eset: ha $b = 0$, akkor $a^2 = c^2v \Rightarrow v$ négyzetszám, de $\sqrt{u} \in \mathbb{Q}(\sqrt{v}) = \mathbb{Q}$ akkor u is négyzetszám.
Most bizonyítsuk be a fordított irányt feltéve hogy uv négyzetszám. Akkor $\sqrt{u}\sqrt{v} \in \mathbb{N}$ és tetszőleges $L/\mathbb{Q}$ testbővítésre $\sqrt{u} \in L \Leftrightarrow \sqrt{v} \in L$. Ekkor $\mathbb{Q}(\sqrt{u}) = \mathbb{Q}(\sqrt{v})$.

5.20. feladat. Bizonyítsuk be, hogy minden $q \in \mathbb{Q}$ esetén létezik ε egységgyök, amelyre $\sqrt{q} \in \mathbb{Q}(\varepsilon)$.

Megoldás. Ha $\varepsilon^{(1)}$ m_1-edik és $\varepsilon^{(2)}$ m_2-edik egységgyök, akkor $m_3 = [m_1, m_2]$ és tetszőleges $\varepsilon^{(3)}$ primitív m_3-adik egységgyökre fennáll: $\mathbb{Q}(\varepsilon^{(1)}, \varepsilon^{(2)}) \subseteq \mathbb{Q}(\varepsilon^{(3)})$, ezért elégséges prímekre számolni, azaz legyen q egy prímszám.

Mivel $\sqrt{2} \in \mathbb{Q}(\frac{\sqrt{2}+i\sqrt{2}}{2}) = \mathbb{Q}(\varepsilon)$, ahol ε primitív 8-ik egységgyök. A továbbiakban legyen q páratlan prímszám, ε primitív q-ik egységgyök. Jelöljük $\varepsilon_i = \varepsilon^i$, ahol $i = 1, \ldots, q$, és legyen $f = \frac{X^q - 1}{X - 1} = X^{q-1} + X^{q-2} + \cdots + X + 1$, illetve $t = \frac{5q^2 + q - 2}{2}$. Most számítsuk ki $D(f)$-et az f diszkriminánsát. Az $X^q - 1$ polinom diszkriminánsát, mint

determinánst az utolsó q számú sora szerint kifejtve adódik $D(X^q-1)=(-1)^t q^q$. Másrészt az f gyöktényezős felbontását felhasználva

$$\prod_{i=1}^{q-1}(\varepsilon_i-\varepsilon_q)^2=((1-\varepsilon_1)\cdots(1-\varepsilon_{q-1}))^2=(f(1))^2=q^2.$$

$$D(f)=\prod_{1\le i<j<q}(\varepsilon_i-\varepsilon_j)^2=\frac{\prod_{1\le i<j\le q}(\varepsilon_i-\varepsilon_j)^2}{\prod_{1\le i<q}(\varepsilon_i-\varepsilon_q)^2}=\frac{D(X^q-1)}{q^2}=(-1)^t q^{q-2}.$$

$$\sqrt{(-1)^t q}\cdot q^{\frac{q-3}{2}}=\sqrt{D(f)}=\prod_{1\le i<j<q}(\varepsilon_i-\varepsilon_j)\in\mathbb{Q}(\varepsilon_1,\dots,\varepsilon_n)=\mathbb{Q}(\varepsilon).$$

Innen $\sqrt{(-1)^t q}\in\mathbb{Q}(\varepsilon)$, ezért a $\sqrt{q}\in\mathbb{Q}(\varepsilon,i)\subset\mathbb{Q}(\eta)$, ahol η egy $4q$-adik primitív egységgyök.

5.4. Véges testek

Ebben a paragrafusban Wedderburn híres tételét fogjuk bebizonyítani, amely tétel igazolja, hogy bármely véges test kommutatív és meghatározzuk a véges testek struktúráját.

5.4.1. tétel. *Ha K véges test, akkor létezik p prímszám és létezik $n\in\mathbb{N}^*$ úgy, hogy $|K|=p^n$.*

Bizonyítás. Mivel K véges, következik, hogy $\operatorname{char}K=p$ prímszám, és legyen $L=P(K)\simeq\mathbb{Z}_p$ a K prímrészteste. Ekkor K L-feletti vektortér, tehát létezik egy véges bázisa. Ha $\dim_L K=n$, akkor $K\simeq L^n$, tehát $|K|=|L|^n=p^n$. ■

A továbbiakban az $X^n-1\in\mathbb{Z}[X]$ polinom néhány tulajdonságát soroljuk fel, melyek fontosak a Wedderburn tétel bizonyításánál.

Ha $n\in\mathbb{N}^*$, akkor az X^n-1 polinom gyökei $\varepsilon_k=\cos(2k\pi/n)+i\sin(2k\pi/n)=\varepsilon_1^k$, ahol $k\in\{0,\dots,n-1\}$; az ε_k számokat *n-ed rendű egységgyököknek* nevezzük. Tudjuk, hogy

$$U_n=\{\varepsilon_k\mid k\in\{0,\dots,n-1\}\}=\langle\varepsilon_1\rangle\simeq(\mathbb{Z}_n,+)$$

n-ed rendű ciklikus csoport, és $\varepsilon_k=\varepsilon_1^k$ akkor és csak akkor generálja U_n-et, ha $(n,k)=1$; ebben az esetben azt mondjuk, hogy ε_k *primitív n-ed rendű egységgyök.*

Legyen

$$\Phi_n=\prod_{0\le k<n,(k,n)=1}(X-\varepsilon_k).$$

Φ_n-et az n-ed rendű **ciklotomikus polinomnak** nevezzük; értelmezéséből következik, hogy $\deg(\Phi_n)=\varphi(n)$, ahol $\varphi(n)$ az Euler-szám. Ha P_m jelöli az m-ed rendű primitív egységgyökeinek a halmazát, akkor $U_n=\bigcup_{m|n}P_m$ particiója U_n-nek; következik, hogy

$$X^n-1=\prod_{0\le k<n}(X-\varepsilon_k)=\prod_{m|n}\Phi_m.$$

5.4.2. lemma. 1) *$\Phi_n\in\mathbb{Z}[X]$ és $\Phi_n|(X^n-1)$ $\mathbb{Z}[X]$-ben.*
2) *Ha $m|n$, akkor $(X^m-1)|(X^n-1)$ $\mathbb{Z}[X]$-ben.*
3) *Ha $m|n$ és $1\le m<n$, akkor $\Phi_n|((X^n-1)/(X^m-1))$.*
4) *Ha $q\in\mathbb{N}$ és $q\ge 2$, akkor $\Phi_n(q)\nmid(q-1)$.*

Bizonyítás. 1) A bizonyítást n szerinti indukcióval végezzük. $n=1$ esetén $\Phi_1=X-1\in\mathbb{Z}[X]$. Feltételezzük, hogy az állítás igaz Φ_m-re, ahol $m<n$. Ekkor $X^n-1=f\Phi_n$, ahol $f\in\mathbb{Z}[X]$ és az f főegyütthatója 1. Tehát, $\Phi_n\in\mathbb{Z}[X]$.

2) Ha $m\mid n$ akkor az X^m-1 polinom bármely gyöke az $X^n-1=0$ polinomnak is gyöke.

4) Ábrázolva az 1 és ϵ számokat a komplex számsíkban, észreveszük, hogy $|q-\epsilon|>(q-1)$ minden $\epsilon\in P_n$, $\epsilon\ne 1$ esetén. ■

5.4.3. tétel (Wedderburn). *Ha K véges test, akkor K kommutatív.*

Bizonyítás. Legyen $Z=Z(K)=\{a\in K\mid ax=xa,\forall x\in K\}$, a K test centruma; elég igazolni, hogy $Z=K$.

Tudjuk, hogy Z részteste K-nak, és ha $x\in K$, akkor $C_K(x)=\{a\in K\mid ax=xa\}$ is részteste K-nak; következik, hogy K és $C_K(x)$ Z-feletti véges dimenziós vektorterek. Ha $|Z|=q$, akkor $|K|=q^n$ és $|C_K(x)|=q^{n_x}$, ahol $n=\dim_Z K$ és $n_x=\dim_Z C_K(x)$.

Továbbá $|K^*|=q^n-1$, $Z(K^*)=Z^*$ és $|C_K(x)^*|=g^{n_x}-1$, ahol $C_K(x)^*=C_{K^*}(x)$ minden $x\in K^*$ esetén.

A $(K^*, \cdot)$ csoport konjugáltsági osztályaira vonatkozó egyenlet:

$$|K^*| = |Z^*| + \sum_{x \in A} [K^* : C_K(x)^*]$$

ahol A a nemtriviális osztályok egy teljes reprezentánsrendszere; következik, hogy

$$q^n - 1 = q - 1 + \sum_{x \in A} (q^n - 1)/(q^{n_x} - 1),$$

ahol $n_x \mid n$ és $n_x \neq n$ ha $x \in A$. A 5.4.2. lemmából következik, hogy $\Phi_n(q) | (q^n - 1)$ és $\Phi_n(q) | (q^n - 1)/(q^{n_x} - 1)$, ami ellentmondás, mert $\Phi_n(q) \nmid (q - 1)$. ■

5.4.4. tétel (kommutatív test multiplikatív részcsoportjai). *Legyen* K *egy kommutatív test és* $G \leq (K^*, \cdot)$ *egy véges részcsoport. Akkor* $(G, \cdot)$ *ciklikus.*

Partikulárisan, ha K *véges test, akkor* K^* *ciklikus csoport.*

5.4.5. példa. a) $\mathbb{R}$-ben: az $(\mathbb{R}^*, \cdot)$ véges részcsoportjai: ha G n-ed rendű, akkor bármely $x \in G$ esetén $x^n = 1$, tehát $x = 1$ vagy $x = -1$, így $G = \{1\}$ vagy $G = \{-1, 1\}$.

b) $\mathbb{C}$−ben: ha G n-edrendű részcsoportja $(\mathbb{C}, \cdot)$-nak , akkor

$$G = U_n = \{z \in \mathbb{C} \mid z^n = 1\} = \left\{ \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n} \mid k \in \mathbb{Z}, k = \{0, 1, 2, \ldots, n-1\} \right\}.$$

c) Legyen

$$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\},$$

a kvaterniók (nem kommutatív) teste, ahol

$$ij = -ji = k,\ jk = -kj = i,\ ki = -ik = j,\ i^2 = j^2 = k^2 = ijk = -1$$

Ekkor $Q = \{\pm 1, \pm i, \pm j, \pm k\} \leq (\mathbb{H}^*, \cdot)$ a kvaterniók csoportja nem ciklikus és nem kommutatív.

d) A Wedderburn-tétel szerint minden véges test kommutatív. A 5.4.4. tétel alapján ha K véges test, akkor $(K^*, \cdot)$ ciklikus csoport.

Partikulárisan, ha p prímszám, akkor $\left(\mathbb{Z}_p^*, \cdot\right)$ ciklikus csoport.

e) Tekintsünk néhány esetet:

$m = 2$ $\quad U(\mathbb{Z}_2) = \{\hat{1}\} = \langle \hat{1} \rangle$
$m = 3$ $\quad U(\mathbb{Z}_3) = \{\hat{1}, \hat{2}\} = \langle \hat{2} \rangle$
$m = 4$ $\quad U(\mathbb{Z}_4) = \{\hat{1}, \hat{3}\} = \langle \hat{3} \rangle$
$m = 5$ $\quad U(\mathbb{Z}_5) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}\} = \langle \hat{2} \rangle$
$m = 6$ $\quad U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$
$m = 7$ $\quad U(\mathbb{Z}_7) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\} = \langle \hat{3} \rangle$

5.4.6. lemma. *Egy* $(G, \cdot)$ *tetszőleges csoport esetén*

a) *ha* $x,\ y \in G,\ xy = yx$, $\operatorname{ord}(x) = m$, $\operatorname{ord}(y) = n$ *és* $(m, n) = 1$, *akkor* $\operatorname{ord}(xy) = mn$;

b) *ha* $x_1,\ x_2,\ \ldots,\ x_r \in G$ *úgy, hogy* $x_i x_j = x_j x_i,\ 1 \leq i, j \leq r$, $\operatorname{ord}(x_i) = m_i \in \mathbb{N}^*$ *és* $(m_i, m_j) = 1,\ i \neq j$, *akkor* $\operatorname{ord}(x_1 x_2 \ldots x_n) = m_1 m_2 \cdots m_r$.

Az 5.4.4 tétel bizonyítása. Legyen $|G| = p_1^{n_1} \ldots p_r^{n_r}$, $r \geq 2$, $p_1,\ p_2,\ \ldots,\ p_r$ prímszámok, $n_i \geq 1$. Igazoljuk hogy létezik $x \in G$, úgy, hogy $\operatorname{ord}(x) = n$.

Az $X^{\frac{n}{p_i}} - 1 \in K[X]$ polinomnak legfenebb n/p_i gyöke van K-ban, minden $i = 1, \ldots, r$ esetén. Mivel $n > \frac{n}{p_i}$, létezik $g_i \in G$ úgy, hogy $g_i^{\frac{n}{p_i}} \neq 1$. Legyen $x_i = g_i^{n/p_i^{m_i}} \in G$ és igazoljuk, hogy $\operatorname{ord}(x_i) = p_i^{m_i}$. Valóban $(x_i)^{p_i^{m_i}} = (g_i^{\frac{n}{p_i^{m_i}}})^{p_i^{m_i}} = g_i^n = 1$, mert $|G| = n$ és $\operatorname{ord}(g_i) \mid |G|$ (Lagrange tétel). Tehát $\operatorname{ord}(x_i) \mid p_i^{m_i}$, ahonnan $\operatorname{ord}(x_i) = p_i^m$, ahol $m \leq m_i$. Feltételezve, hogy $m < m_i$,

$$1 = (x_i)^{p_i^{m_i}} = (g_i^{n/p_i})^{p_i^m} = g_i^{n/p_i^{m_i - m}},$$

tehát $g_i^{n/p_i} = 1$, ellentmond g_i megválasztásának.

Legyen $x = x_1 \cdots x_r \in G$. Mivel G kommutatív, alkalmazhatjuk az előző lemmát. Mivel $\operatorname{ord}(x_i) = p_i^{n_i}$ és $(p_i, p_j) = 1$ ha $i \neq j$, a lemma b) alpontjából következik, hogy $\operatorname{ord}(x) = p_1^{m_1} \ldots p_r^{m_r} = n$. Tehát $G = \langle x \rangle$ ciklikus. ■

5.4.7. tétel (Véges testek létezése). 1) *Két, azonos elemszámú véges test izomorf egymással.*

2) *Bármely* $p > 0$ *prímszám esetén és bármely* $n > 0$ *esetén, létezik egy* p^n *elemű test, az* $X^{p^n} - X \in \mathbb{Z}_p[X]$ *polinom felbontási teste* $\mathbb{Z}_p$ *felett.*

Bizonyítás. 1) Legyen $q := p^n$, $K = \{a_1 = 0, a_2, \dots, a_q\}$ és $K^* = K \setminus \{0\}$.

Minden $a_i \in K^*$ elem rendje a $(K^*, \cdot)$ csoportban osztja $|K^*| = q-1$-gyet, amiből következik, hogy $a_i^{q-1} - a_i = 1$, minden $a_i \in K^*$ esetén; következik, hogy $a_i^q - a_i = 0$, minden $a_i \in K$ esetén. Tehát K minden eleme gyöke az $f := X^q - X \in \mathbb{Z}_p[x]$ polinomnak, és f-nek nincs több gyöke a $\mathbb{Z}_p$ feletti felbontási testében. Következik, hogy a K test az f polinom felbontási teste $\mathbb{Z}_p$ felett.

Ha L egy másik $q = p^n$ elemű test, akkor $P(L) \simeq \mathbb{Z}_p$, L pedig a felbontási teste $P(L)$ felett a $g = X^q - X \in P(L)[X]$. Tehát a 5.3.5. tétel alapján következik, hogy $K \simeq L$.

2) Az $f = X^q - X \in \mathbb{Z}_p[X]$ polinom formális deriváltja, $f' = qX^{q-1} - 1 = -1$, ami azt igazolja, hogy f-nak q különböző gyöke van az $F = F_{f,\mathbb{Z}_p}$ felbontási testben. A $\psi : F \to F$, $\psi(a) = a^q$ testautomorfizmus, mivel ψ az n-edik hatványa a Frobenius automorfizmusnak. Az f polinom gyökei azonosak a ψ fix-pontjaival. Tehát, az f gyökei egy q elemű $F_0 \leq F$ résztestet alkotnak; következik, hogy $F_0 = F_{f,\mathbb{Z}_p}$, tehát $|F| = p^n$. ■

A fenti tételből következik, hogy bármilyen p prí mszám esetén létezik, izomorfizmustól eltekintve, egyetlen egy p^n elemű test, melyet $GF(p^n)$-el, vagy $\mathbb{F}_{p^n}$-el jelölünk és a p^n elemű **Galois test**nek nevezzük. A 5.4.7. és 5.4.1. tételek azt bizonyítják, hogy bármely véges test izomorf egy $GF(p^n)$ alakú testtel, vagyis a $\mathbb{F}_{p^n}$ alakú testek kimerítik az összes véges testeket.

5.4.8. megjegyzés. Ha $K \leq L$ egy véges bővítés és K egy véges test, akkor létezik $a \in L$ úgy hogy $L = K(a)$, vagyis L-ben létezik egy primitív elem.

Valóban, L is véges, tehát az $(L^*, \cdot)$ csoport ciklikus. Ha a ennek a csoportnak egy generáló eleme, akkor $L = K(a)$.

5.4.9. tétel (Véges test résztestei). *Legyen* K *egy véges test,* $|K| = p^n$.

1) *A* K *test egy résztestének a számossága* p^m *alakú, ahol* $m \mid n$.

2) *Ha* $m \in \mathbb{N}^*$ *és* $m \mid n$, *akkor* K*-nak egyetlen* p^m *elemű részteste van.*

Bizonyítás. 1) Ha $L \leq K$, akkor az L prím részteste $\mathbb{Z}_p$. Tehát, a 4.1 tételből, $|L| = p^m$, ahol $m = [L : \mathbb{Z}_p]$. Mivel $\mathbb{Z}_p \leq L \leq K$, következik, hogy $n = m[K : L]$.

2) Ha $q := p^m$, akkor láttuk fennebb, hogy az $f := X^q - X \in \mathbb{Z}_p[X]$ polinom K-beli gyökei egybeesnek a $\varphi : K \to K$, $\varphi(x) = x^p$ Frobenius automorfizmus m-ad hatványú fixpontjaival. Tehát, ezek a gyökök K-nak egy L résztestét alkotják és $|L| \leq q$.

Ha $k := n/m$, akkor $|K| = q^k$ és $|K^*| = q^k - 1$, ahol $K^* = K \setminus \{0\}$. Mivel $(K^*, \cdot)$ ciklikus csoport, következik, hogy K^*-nak van egy a generátor eleme. Ha $s := (q^k - 1)/(q - 1)$, akkor $o(a^s) = q - 1$ a $(K^*, \cdot)$ csoportban; következik, hogy

$$0, a^s, a^{2s}, \dots, a^{(q-1)s} \tag{5.1}$$

q darab különböző elem és $(a^{is})^{(q-1)} = 1$, $i = 1, \dots, q-1$, amiből következik, hogy $(a^{is})^q = a^{is}$, $i = 0, 1, \dots, q-1$). Tehát, a 5.1-beli elemek f-nek gyökei, vagyis L-hez tartoznak. Következik, hogy $|L| \geq q$, tehát $|L| = q$.

A továbbiakban igazoljuk, hogy L az egyedüli q elemű részteste K-nak. Valóban, ha L' egy q elemű részteste K-nak, akkor L^* $q - 1$ elemű csoport, amiből következik hogy $x^{q-1} = 1$, minden $x \in L'^*$ esetén. Ebből az következik, hogy az L' elemei az f polinom gyökei. Tehát, L' a 5.1-beli elemekből áll, vagyis $L' = L$. ■

5.21. feladat. Számítsuk ki Φ_n-et, ha $n = 1, 2, 3, 4, 5, 6$ és ha $n = p$ prímszám.

5.22. feladat. a) Igazoljuk, hogy

$$\Phi_{p^n} = \Phi_p(X^{p^{n-1}}), \quad \Phi_{p^n q^m} = \Phi_{pq}(X^{p^{n-1} q^{m-1}}), \quad \Phi_{p^n q^m r^l} = \Phi_{pqr}(X^{p^{n-1} q^{m-1} r^{l-1}}).$$

b) Számítsuk ki Φ_n-et, ha $n = 8, 9, 10, 12, 72, 180$.

5.23. feladat. Igazoljuk, hogy Φ_n irreducibilis $\mathbb{Z}[X]$ felett (tehát $\mathbb{Q}[X]$ felett is.)

Megoldás. Legyen $\varepsilon_n = \varepsilon$ egy n-edrendű primitív egységgyök és $f = m_{\mathbb{Q},\varepsilon}$. Mivel $\Phi_n(\varepsilon) = 0$ következik, hogy $\Phi_n = fg$ ahol $f, g \in \mathbb{Q}[X]$. A Gauss-lemmából következik, hogy $f, g \in \mathbb{Z}[X]$.

Legyen $p > 1$ prímszám, úgy hogy $(p, n) = 1 \Longrightarrow \varepsilon^p$ n-edrendű primitív egységgyök azaz az ε^p n-edrendű az $(U_n, \cdot)$ csoportban. Ekkor $\Phi_n(\varepsilon^p) = 0$, tehát $f(\varepsilon^p) = 0$ vagy $g(\varepsilon^p) = 0$. *Reductio ad absurdum*: feltételezzük, hogy $f(\varepsilon^p) \neq 0$. Akkor $g(\varepsilon^p) = 0$.

Legyen $h = g(X^p) \in \mathbb{Z}[X]$. Ekkor ε gyöke lesz a h polinomnak, mert $h(\varepsilon) = g(\varepsilon^p) = 0$. Ekkor $f = m_{\mathbb{Q},\varepsilon} \mid h$, és a Gauss-lemmából $h = fq$, ahol $q \in \mathbb{Z}[X]$. Tekintsük a

$$\mathbb{Z}[X] \to \mathbb{Z}_p[X], \qquad f = a_0 + a_1 X + \dots + a_n X^n \longmapsto \overline{f} = \overline{a}_0 + \overline{a}_1 X + \dots + \overline{a}_m X^m$$

morfizmust. Ekkor $\overline{h} = \overline{f} \cdot \overline{q}$, de $\overline{h} = \overline{g}(X^p) = \overline{g}^p$, mert $\overline{a}^p = \overline{a}$ $\mathbb{Z}_p$-ben a kis-Fermat tételből, tehát $\overline{g}^p = \overline{f} \cdot \overline{g}$.

Ha $\psi \in \mathbb{Z}_p[X]$ irreducibilis tényezője f-nek, akkor $\psi \mid \overline{g}^p$, és mivel ψ prím $Z_p[X]$-ben kapjuk, hogy $\psi \mid \overline{g}$. Mivel $\overline{\Phi}_n = \overline{f}\overline{g}$, következik, hogy $\psi^2 \mid \Phi_n$, és ekkor ψ dupla gyöke Φ_n-nek. De ez ellentmondás, mert Φ_n-nek csak egyszeres gyökei vannak. Ezért $f(\varepsilon^p) = 0$ kell legyen minden $p > 1$ prímszám esetén. Tehát $(p, n) = 1$ esetén ε^p gyöke f-nek.

Legyen ξ egy gyöke Φ_n-nek, azaz ξ n-edrendű primitív egységgyök, tehát léetzik $m \in \{1, \dots, n\}$, úgy hogy $(m, n) = 1$ és $\xi = \varepsilon^m$.

Legyen $m = p_1 p_2 \dots p_s$, ahol p_i prímek, $(p_i, n) = 1$ minden $1 \le i \le s$ esetén, és $f(\varepsilon^{p_i}) = 0$. Tehát $\Phi_n(\varepsilon^{p_i}) = 0$. A fenti eljárással ε helyett ε^{p_1}-t véve i szerinti indukcióval kapjuk, hogy $f((\varepsilon^{p_1})^{p_2}) = f(\varepsilon^{p_1 p_2}) = 0$, tehát $\Phi(\varepsilon^{p_1 p_2}) = 0$.

Tehát $f(\xi) = f(\varepsilon^{p_1 \cdots p_s}) = 0$. Mivel minden ξ primitív egységgyökre fennáll, kaptuk, hogy Φ_n bármely gyöke, gyöke f-nek is, tehát $\Phi_n = f = m_{\mathbb{Q},\varepsilon}$ irreducibilis $\mathbb{Q}$ felett.

5.24. feladat. Határozzuk meg $\mathbb{Z}_{13}^*$ generáló elemeit.

Megoldás. $\mathbb{Z}_{13}^* = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}, \hat{7}, \hat{8}, \hat{9}, \hat{10}, \hat{11}, \hat{12}\}$; $\hat{2}^0 = 1$, $\hat{2}^1 = 2$, $\hat{2}^2 = \hat{4}$, $\hat{2}^3 = \hat{8}$, $\hat{2}^4 = 3$, $\hat{2}^5 = \hat{6}$, $\hat{2}^6 = \hat{12}$, $\hat{2}^7 = \hat{11}$, $\hat{2}^8 = \hat{9}$, $\hat{2}^9 = 5$, $\hat{2}^{10} = \hat{10}$, $\hat{2}^{11} = \hat{7}$.

Tehát, $\mathbb{Z}_{13}^* = \langle 2 \rangle$. $\langle 2^k \rangle = \mathbb{Z}_{13}^*$ akkor és csakis akkor, ha $(k, 12) = 1$, vagyis $k \in \{1, 5, 7, 11\}$. Tehát, a generáló elemek: $\hat{2}, \hat{6}, \hat{11}, \hat{7}$.

5.25. feladat. Határozzuk meg $\mathbb{Z}_{17}^*$ generáló elemeit.

Megoldás. $\mathbb{Z}_{17}^* = \{\hat{1}, \hat{2}, \dots, \hat{16}\}$.

Generáló elemek: $\hat{3}^1, \hat{3}^3, \hat{3}^5, \hat{3}^7, \hat{3}^9, \hat{3}^{11}, \hat{3}^{15}$, vagyis $\hat{3}, \hat{9}, \hat{5}, \hat{11}, \hat{14}, \hat{7}, \hat{12}, \hat{6}$.

5.26. feladat. Szerkesszük meg a 4 elemű $\mathbb{F}_4$ testet.

Megoldás. $4 = 2^2$, esetünkben $p = 2$, $n = 2$; $f = X^2 + X + 1$ irreducibilis $\mathbb{Z}_2$ felett (nincs gyöke $\mathbb{Z}_2$-ben). Következik, hogy

$$\begin{aligned}\mathbb{F}_4 &= \mathbb{F}_2/(f) = \{\alpha_0 + \alpha_1 a \mid \alpha_0, \alpha_1 \in \mathbb{F}_2,\ a = x + (f),\ a^2 + a + 1 = 0\} = \\ &= \{\hat{0}, \hat{1}, a, \hat{1} + a\}\end{aligned}$$

Művelettáblák:

$+$	$\hat{0}$	$\hat{1}$	a	$\hat{1}+a$
$\hat{0}$	$\hat{0}$	$\hat{1}$	a	$\hat{1}+a$
$\hat{1}$	$\hat{1}$	$\hat{0}$	$\hat{1}+a$	a
a	a	$\hat{1}+a$	$\hat{0}$	$\hat{1}$
$\hat{1}+a$	$\hat{1}+a$	a	$\hat{1}$	$\hat{0}$

$\cdot$	$\hat{0}$	$\hat{1}$	a	$\hat{1}+a$
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	a	$\hat{1}+a$
a	$\hat{0}$	a	$\hat{1}+a$	$\hat{1}$
$\hat{1}+a$	$\hat{0}$	$\hat{1}+a$	$\hat{1}$	a

5.27. feladat. Szerkesszük meg az $\mathbb{F}_8$ testet.

Megoldás. $8 = 2^3$, esetünkben $p = 2$, $n = 3$; $f = X^3 + X + 1 \in \mathbb{Z}_2[X]$ irreducibilis polinom.

$$\begin{aligned}\mathbb{F}_8 &= \mathbb{F}_2/(f) = \{\alpha_0 + \alpha_1 a + \alpha_2 a^2 \mid \alpha_i \in \mathbb{Z}_2,\ a^3 + a + \hat{1} = \hat{0},\ a = X + (f)\} = \\ &= \{\hat{0}, \hat{1}, a, 1 + a, a^2, \hat{1} + a^2, a + a^2, 1 + a + a^2\}\end{aligned}$$

Tudjuk, hogy $a^3 = a + 1$ és $a^4 = a^2 + a$. Bevezetjük a következő jelöléseket: $\hat{1} + a := x$, $\hat{1} + a^2 := y$, $a + a^2 := z$, $\hat{1} + a + a^2 := t$. Művelettáblák:

$+$	$\hat{0}$	$\hat{1}$	a	x	a^2	y	z	t
$\hat{0}$	$\hat{0}$	$\hat{1}$	a	x	a^2	y	z	t
$\hat{1}$	$\hat{1}$	$\hat{0}$	x	a	y	a^2	t	z
a	a	x	$\hat{0}$	$\hat{1}$	z	t	a^2	y
x	x	a	$\hat{1}$	$\hat{0}$	t	z	y	a^2
a^2	a^2	y	z	t	$\hat{0}$	$\hat{1}$	a	x
y	y	a^2	t	z	$\hat{1}$	$\hat{0}$	x	a
z	z	t	a^2	y	a	x	$\hat{0}$	$\hat{1}$
t	t	z	y	a^2	x	a	$\hat{1}$	$\hat{0}$

$\cdot$	$\hat{0}$	$\hat{1}$	a	x	a^2	y	z	t
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	a	x	a^2	y	z	t
a	$\hat{0}$	a	a^2	z	x	$\hat{1}$	t	y
x	$\hat{0}$	x	z	y	t	a^2	$\hat{1}$	a
a^2	$\hat{0}$	a^2	x	t	z	a	y	$\hat{1}$
y	$\hat{0}$	y	$\hat{1}$	a^2	a	t	x	z
z	$\hat{0}$	z	t	$\hat{1}$	y	x	a	a^2
t	$\hat{0}$	t	y	a	$\hat{1}$	z	a^2	x

5.28. feladat. Határozzuk meg az $\mathbb{F}_8^*$ generáló elemeit.
$\mathbb{F}_8 = \{\hat{0}, \hat{1}, a, \hat{1}+a, a^2, \hat{1}+a^2, a+a^2, 1+a+a^2\}$.

Megoldás. $(k,7) = 1$ akkor és csakis akkor, ha $k \in \{1,2,3,4,5,6\}$.
$a^0 = 1$, $a^1 = a$, $a^2 = a^2$, $a^3 = \hat{1}+a$, $a^4 = a^2+a$, $a^5 = \hat{1}+a+a^2$, $a^6 = a+a^2+a^3 = a^2+1$, vagyis $\mathbb{F}_8{}^* = \langle a^k \rangle$, minden $k = 1,2,3,4,5,6$ esetén.

5.29. feladat. Szerkesszünk 9 elemű testet.

Megoldás. $9 = 3^2$, esetünkben $p = 3$, $n = 2$; $f = x^2+1 \in \mathbb{Z}_3[X]$ irreducibilis polinom (mert nincs gyöke $\mathbb{Z}_3$-ban.

$$\mathbb{F}_9 = GF(3)/(f) = \{\alpha_0 + \alpha_1 a \mid \alpha_i \in \mathbb{Z}_3;\ a = x + (f);\ a^2+1 = 0\} =$$
$$= \{\hat{0}, \hat{1}, \hat{2}, a, \hat{2}a, a+\hat{1}, \hat{2}a+\hat{1}, a+\hat{2}, \hat{2}+\hat{2}a\}$$

Tudjuk, hogy $a^2 = \hat{2}$. Bevezetjük a következő jelöléseket: $a+\hat{1} =: u$, $\hat{2}a+\hat{1} =: v$, $a+\hat{2} =: x$, $\hat{2}a+\hat{2} =: y$. Művelettáblák:

$+$	$\hat{0}$	$\hat{1}$	$\hat{2}$	a	$\hat{2}a$	u	v	x	y
$\hat{0}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	a	$\hat{2}a$	u	v	x	y
$\hat{1}$	$\hat{1}$	$\hat{2}$	$\hat{0}$	u	v	x	y	a	$\hat{2}a$
$\hat{2}$	$\hat{2}$	$\hat{0}$	$\hat{1}$	x	y	a	$\hat{2}a$	u	v
a	a	u	x	$\hat{2}a$	$\hat{0}$	v	$\hat{1}$	y	$\hat{2}$
$\hat{2}a$	$\hat{2}a$	v	y	$\hat{0}$	a	$\hat{1}$	u	$\hat{2}$	x
u	u	x	a	v	$\hat{1}$	y	$\hat{2}$	$\hat{2}a$	$\hat{0}$
v	v	y	$\hat{2}a$	$\hat{1}$	u	$\hat{2}$	x	$\hat{0}$	a
x	x	a	u	y	$\hat{2}$	$\hat{2}a$	$\hat{0}$	v	$\hat{1}$
y	y	$\hat{2}a$	v	$\hat{2}$	x	$\hat{0}$	a	$\hat{1}$	u

$\cdot$	$\hat{0}$	$\hat{1}$	$\hat{2}$	a	$\hat{2}a$	u	v	x	y
$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$	$\hat{0}$
$\hat{1}$	$\hat{0}$	$\hat{1}$	$\hat{2}$	a	$\hat{2}a$	u	v	x	y
$\hat{2}$	$\hat{0}$	$\hat{2}$	$\hat{1}$	$\hat{2}a$	a	y	x	v	u
a	$\hat{0}$	a	$\hat{2}a$	$\hat{2}$	$\hat{1}$	x	u	y	v
$\hat{2}a$	$\hat{0}$	$\hat{2}a$	a	$\hat{1}$	$\hat{2}$	v	y	u	x
u	$\hat{0}$	u	y	x	v	$\hat{2}a$	$\hat{2}$	$\hat{1}$	a
v	$\hat{0}$	v	x	u	y	$\hat{2}$	a	$\hat{2}a$	$\hat{1}$
x	$\hat{0}$	x	v	y	u	$\hat{1}$	$\hat{2}a$	a	$\hat{2}$
y	$\hat{0}$	y	u	v	x	a	$\hat{1}$	$\hat{2}$	$\hat{2}a$

5.30. feladat. Határozzuk meg az $\mathbb{F}_9^*$ generáló elemeit.

Megoldás. $\mathbb{F}_9 = \{\hat{0}, \hat{1}, \hat{2}, a, \hat{1}+a, \hat{2}+a, \hat{2}a, \hat{1}+\hat{2}a, \hat{2}+\hat{2}a\}$;
$(\hat{1}+\hat{2}a)^2 = a$, $(\hat{1}+\hat{2}a)^3 = a(\hat{1}+\hat{2}a) = a+\hat{1}$, $(\hat{1}+\hat{2}a)^4 = (\hat{1}+\hat{2}a)(a+\hat{1}) = \hat{2}$, $(\hat{1}+\hat{2}a)^5 = (\hat{1}+\hat{2}a)\hat{2} = \hat{2}+a$, $(\hat{1}+\hat{2}a)^6 = (\hat{1}+\hat{2}a)(\hat{2}+a) = \hat{2}+\hat{2}a$, tehát $\langle \hat{1}+\hat{2}a \rangle = \mathbb{F}_9{}^*$;
$(k,8) = 1$ akkor és csakis akkor, ha $k \in \{1,3,5,7\}$, vagyis a generáló elemek $\hat{1}+\hat{2}a, 1 \hat{+} a, \hat{2}+a, \hat{2}+a$.

5.31. feladat. Legyen $f = X^4 + \hat{1} \in \mathbb{Z}_3[X]$. Határozzuk meg az f gyökeit.

Megoldás. $f(\hat{0}) = \hat{1}$, $f(\hat{1}) = \hat{1}$, $f(\hat{2}) = \hat{2}$, vagyis f-nek nincs gyöke $\mathbb{Z}_3$-ban.
$f = X^4 + \hat{1} = X^4 - \hat{2}X^2 + 1 - X^2 = (X^2-\hat{1})^2 - X^2 = (X^2 - X - \hat{1})(X^2 + X - \hat{1}) = f_1 f_2$;
$K := \mathbb{Z}_3[x]/(X^2 - X - \hat{1})$ test mert $f_1 = X^2 - X - \hat{1}$ irreducibilis $\mathbb{Z}_3$ felett. Legyen $a = X + (f_1) \in K$; következik, hogy $K = \mathbb{Z}_3(a) = \{\alpha + \beta a \mid \alpha, \beta \in \mathbb{Z}_3\} = \{\hat{0}, \hat{1}, \hat{2}, a, a+\hat{1}, a+\hat{2}, \hat{2}a, \hat{2}a+\hat{1}, \hat{2}a+\hat{2}\}$.
$(X^2 - X - 1) : (X - a) = X + (a-1)$, ahol a maradék $a^2 - a - 1 = 0$, mert a gyöke f_1-nek. Tehát, f_1 gyökei: $x_1 = a$, $x_2 = -a + \hat{1} = \hat{2}a + \hat{1}$. Kiszámítjuk, hogy $f_2(\hat{2}a) = f_2(a+2) = 0$, tehát $f = (X-a)(X-\hat{2}a)(X-\hat{2}a-\hat{1})(X-a-\hat{2})$.

5.32. feladat. Határozzuk meg az $\mathbb{F}_{16}^*$ generáló elemeit.

Megoldás. $16 = 2^4$; $f = X^4 + X^3 + X^2 + X + \hat{1} \in \mathbb{Z}_2[X]$ irreducibilis.

$$\mathbb{F}_{16} = \mathbb{Z}_2[x]/(f) = \{\hat{0}, \hat{1}, a, \hat{1}+a, \hat{1}+a^2, \hat{1}+a+a^2, a+a^2, a^3,$$
$$\hat{1}+a^3, a+a^3, \hat{1}+a+a^3, a^2+a^3, \hat{1}+a^2+a^3, \hat{1}+a+a^2+a^3, a+a^2+a^3\}$$

ahol $a^4 + a^3 + a^2 + a + \hat{1} = 0$, vagy $a^4 = a^3 + a^2 + a + \hat{1}$.

$(a+\hat{1})^0 = \hat{1}$, $(a+\hat{1})^1 = a+\hat{1}$, $(a+\hat{1})^2 = a^2+\hat{1}$, $(a+\hat{1})^3 = a^3+a^2+a+\hat{1}$, $(a+\hat{1})^4 = a^4+1 = a^3+a^2+a$, $(a+\hat{1})^5 = a^3+a^2+\hat{1}$, $(a+\hat{1})^6 = a^3$, $(a+\hat{1})^7 = a^2+a+\hat{1}$, $(a+\hat{1})^8 = a^3+\hat{1}$, $(a+\hat{1})^9 = a^2$, $(a+\hat{1})^{10} = a^3+a^2$, $(a+\hat{1})^{11} = a^3+a+\hat{1}$, $(a+\hat{1})^{12} = a$, $(a+\hat{1})^{13} = a^2+a$, $(a+\hat{1})^{14} = a^3+a$,

Tehát, ${\mathbb{F}_{16}}^* = \langle (a+\hat{1})^k \rangle$, ahol $(k, 15) = 1$, $k \in \{1, 2, 4, 6, 7, 8, 11, 13, 14\}$.

5.33. feladat. Határozzuk meg az $\mathbb{F}_{16}$ résztesteit.

5.5. Algebrailag zárt testek. Egy test algebrai lezártja

5.5.1. definíció. a) Egy K (kommutatív) testet **algebrailag zártnak** nevezzük, ha minden $f \in K[X]$, $f \neq 0$ esetén az f gyökei a K-ban vannak, vagyis az f polinom K feletti felbontási teste megegyezik (azonos) K-val.

b) Egy K test algebrailag zárt egy L bővítésében, ha minden $f \in K[X]$, $f \neq 0$ esetben az f L-beli gyökei a K-ban vannak.

5.5.2. megjegyzés. 1) Ha $K \leq L$, akkor K algebrailag zárt L-ben, akkor és csak akkor, ha az L-beli K feletti algebrai elemek K-ban vannak.

2) Ha K egy test akkor a következő állítások ekvivalensek:

1. K algebrailag zárt;
2. K-nak bármely algebrai bővítése a K-nak azonos K-val;
3. K algebrailag zárt bármely L bővítésében;
4. Ha $f \in K[X]$ és $\deg f \geq 1$, akkor f-nek van egy gyöke K-ban;
5. A $K[X]$-beli irreducibilis polinomok azonosak az elsőfokú polinomokkal.

3) A véges testek algebrailag nem zártak.

Valóban, ha $K = \{a_1, \ldots, a_n\}$ akkor az $f = 1 + (X - a_1) \ldots (X - a_n) \in K[X]$ polinomnak nincs gyöke K-ban.

A következő tételt a klasszikus *algebra alaptételének* is szokták nevezni.

5.5.3. tétel (Gauss-d'Alambert). *A $\mathbb{C}$ komplex számtest algebrailag zárt.*

Bizonyítás. *I. eset.* Feltételezzük, hogy $f \in \mathbb{R}[X]$, és legyen $\deg(f) = n = 2^k m$, ahol $2 \nmid m$.

k-szerinti indukcióval igazoljuk, hogy f-nek van gyöke $\mathbb{C}$-ben.

Ha $k = 0$, akkor $\deg(f)$ páratlan szám és $\lim_{x\to\infty} f(x) = -\lim_{x\to-\infty} f(x)$; de f folytonos függvény, tehát létezik $\alpha \in \mathbb{R}$ úgy, hogy $f(\alpha) = 0$.

Legyen $k > 0$. Létezik egy L test, $\mathbb{C} \leq L$ úgy, hogy $f = a_n(X - x_1) \ldots (X - x_n)$, ahol $x_i \in L$ minden $i \in \{1, \ldots, n\}$ esetén.

Ha $\alpha \in \mathbb{R}$, legyen $z_{ij}^\alpha = x_i x_j + \alpha(x_i + x_j)$, ahol $1 \leq i < j \leq n$ és legyen

$$g = \prod_{1 \leq i < j \leq n} (X - z_{ij}^\alpha) \in L[X].$$

Ha $\sigma \in S_n$, $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$ bijektív függvény, akkor σ indukál egy $\sigma' : \{(i,j) \mid i < j\} \to \{(i,j) \mid i < j\}$, $\sigma'(i,j) = \sigma(i)\sigma(j)$ bijektív függvényt; következik, hogy a g együtthatói szimmetrikusak az $x_1, \ldots, x_n$-ben, tehát $g \in \mathbb{R}[X]$. Mivel

$$\deg(g) = C_n^2 = n(n-1)/2 = 2^k m(2^k m - 1)/2 = 2^{k-1} m(2^k m - 1),$$

az indukció feltevéséből következik, hogy g-nek van gyöke $\mathbb{C}$-ben.

Igazoltuk, hogy minden $\alpha \in \mathbb{R}$ esetén létezik (i_α, j_α) úgy, hogy $z_{i_\alpha j_\alpha}^\alpha \in \mathbb{C}$. Mivel $\mathbb{R}$ végtelen halmaz, következik, hogy létezik $\alpha \neq \beta$ és (i,j) úgy, hogy z_{ij}^α, $z_{ij}^\beta \in \mathbb{C}$; ekkor $x_i x_j + \alpha(x_i + x_j) \in \mathbb{C}$ és $x_i x_j + \beta(x_i + x_j) \in \mathbb{C}$, és mivel $\alpha \neq \beta$, következik, hogy $x_i + x_j \in \mathbb{C}$ és $x_i x_j \in \mathbb{C}$. Mivel x_i, x_j gyökei az $X^2 - (x_i + x_j)X + x_i x_j \in \mathbb{C}[X]$ polinomnak, következik, hogy $x_i, x_j \in \mathbb{C}$.

II. eset. Legyen $f \in \mathbb{C}[X]$; mivel $f\bar{f} \in \mathbb{R}[X]$, az I. esetből következik, hogy létezik $x \in \mathbb{C}$ úgy, hogy $f(x)\bar{f}(x) = 0$.

Ha $f(x) = 0$, akkor f-nek van komplex gyöke. Ha $\bar{f}(x) = 0$, akkor $\overline{f(x)} = 0$, vagyis $f(\bar{x}) = 0$, tehát f-nek van komplex gyöke. ■

5.5.4. tétel. *Legyen* $K \leq L$ *és* $A = \{a \in L \mid a$ *algebrai* K*-felett*$\}$.
1) A *algebrailag zárt* L*-ben;*
2) *Ha* L *algebrailag zárt, akkor* A *is algebrailag zárt.*

Bizonyítás. 1) Valóban, a $K \leq A$ bővítés algebrai és ha $b \in L$ algebrai elem A felett akkor a 5.2.8. 3) értelmében az $A \leq A(b)$ bővítés algebrai. A 5.2.9. tételből következik, hogy a $K \leq A(b)$ bővítés algebrai, ahonnan következik, hogy b algebrai elem K felett, vagyis $b \in A$.

2) Ha $f \in A[X]$, $f \neq 0$ akkor $f \in L[X]$ és mivel L algebrailag zárt, következik hogy az f gyökei L-ben vannak. Tehát, 1)-ből következik, hogy az f gyökei az A-ban vannak, tehát A algebrailag zárt. ■

5.5.5. megjegyzés. Az $\mathbb{A}$ algebrai számok teste algebrailag zárt.

5.5.6. definíció. Egy $\overline{K}$ testet a K test *algebrai lezártjának* nevezzük, ha $\overline{K}$ algebrailag zárt, és $\overline{K}$ egy algebrai bővítése a K-nak.

A továbbiakban igazolni fogjuk, hogy bármely testnek van egy algebrai lezártja mely egyértelmű izomorfizmustól eltekintve. A következő tételt az egyértelműség bizonyításánál fogjuk felhasználni.

5.5.7. tétel. *Ha* $K_1 \leq K_2$ *egy algebrai bővítés és* K *egy algebrailag zárt test. Akkor bármely nem nulla* $\varphi : K_1 \to K$ *morfizmus meghosszabítható egy* $\overline{\varphi} : K_2 \to K$ *morfizmushoz.*

Ha a $\varphi(K_1) \leq K$ *bővítés algebrai és* K_2 *algebrailag zárt akkor minden* $\overline{\varphi} : K_2 \to K$ *morfizmus mely meghosszabítja a* φ*-t egy izomorfizmus.*

Bizonyítás. Legyen

$$\mathcal{M} := \{(L_1, \varphi') \mid K_1 \leq K_1' \leq K_2,\ \varphi' : K_1' \to K \text{ morfizmus},\ \varphi'_{|K_1} = \varphi\}.$$

A $\mathcal{M}$ halmazonn értelmezzük a „$\leq$" relációt: $(K_1', \varphi') \leq (K_1'', \varphi'')$ akkor és csak akkor, ha $K_1' \subseteq K_1''$ és $\varphi' = \varphi''_{|K_1'}$. Akkor „$\leq$" rendezési reláció. Az $\mathcal{M}, \leq)$ rendezett halmaz teljesíti a Zorn-lemma feltételeit. Tehát, létezik egy $(\overline{K}_1, \varphi) \in \mathcal{M}$ maximális elem. Igazoljuk, hogy $\overline{K}_1 = K_2$.

Valóban, ha $\overline{K}_1 \neq K_2$, akkor létezik egy $b \in K_2 \setminus \overline{K}_1$ elem, ahonnan következik, hogy $\overline{K}_1 \subseteq \overline{K}_1(b)$. Ha $f = \sum_{i=0}^{n} a_i X^i \in \overline{K}_1[X]$ a b minimálpolinomja és $f' = \sum_{i=0}^{n} \overline{\varphi}(a_i) X^i$, illetve b' az f' egyik gyöke a K-ban, akkor a 5.3.3. tétel alapján $\overline{\varphi}$ meghosszabítható egy $\overline{\varphi'} : \overline{K}_1(b) \to \overline{\varphi}(\overline{K}_1)(b') \subseteq K$ morfizmushoz. Tehát, $(\overline{K}_1, \overline{\varphi}) < (\overline{K}_1(b), \overline{\varphi'})$ ami ellentmond a $(\overline{K}_1, \overline{\varphi})$ elempár maximalitásának. Ezek szerint, igazoltuk, hogy $\overline{K}_1 = K_2$, vagyis φ meghosszabítható egy $\overline{\varphi} : K_2 \longrightarrow K$ morfizmushoz.

Ha $\varphi(K_1) \leq K$ algebrai bővítés és $\overline{\varphi} : K_2 \to K$ egy morfizmus, mely meghosszabítja φ-t, akkor a $\overline{\varphi}(K_2) \leq K$ bővítés algebrai és mivel K_2 algebrailag zárt, $\overline{\varphi}(K_2)$ is algebrailag zárt. Tehát, $\overline{\varphi}(K_2) = K$, vagyis $\overline{\varphi}$ izomorfizmus. ■

5.5.8. tétel. *Bármely testnek van egy algebrai lezártja amely egyértelmű izomorfiától eltekintve.*

Bizonyítás. *Létezés.* Legyen $(K, +, \cdot)$ egy test és M egy olyan halmaz, mely tartalmazza a K-t és amely megszámlálhatatlan (vagyis $|M| > |\mathbb{N}|$) ha K véges és ha K végtelen akkor az M kardinálisa nagyobb mint a K kardinálisa. Jelöljük $\mathcal{M}$-mel a $(L, +, \cdot)$ testek halmazát melyek algebrai bővítései a K-nak és $L \subseteq M$. Az $\mathcal{M}$ halmazon értelmezük a „$\leq$" relációt: $(L_1, +, \cdot) \leq (L_2, +, \cdot)$ akkor és csak akkor, ha $(L_2, +, \cdot)$ algebrai bővítése a $(L_1, +, \cdot)$-nek. Akkor „$\leq$" rendezési reláció, és az $(\mathcal{M}, \leq)$ rendezett halmaz eleget tesz a Zorn-lemma feltételeinek. Tehát, létezik egy $(\overline{K}, +, \cdot) \in \mathcal{M}$ maximális elem.

Igazoljuk, hogy $(\overline{K}, +, \cdot)$ algebrailag zárt. Feltételezzük az ellenkezőjét, azaz, hogy létezik egy $(L, +, \cdot)$ algebrai bővítése a $(\overline{K}, +, \cdot)$-nak, úgy hogy $\overline{K} < L$. A 5.2.9. tételből következik, hogy $(L, +, \cdot)$ algebrai bővítése K-nak; az M megválasztásából és a 5.8. feladatból következik, hogy $|L| < |M|$. Tehát, létezik egy injektív $\alpha : L \to M$ függvény úgy hogy $\alpha(x) = x$, minden $x \in \overline{K}$. Az $\alpha(L)$ halmaz test a következő műveletekkel: $\alpha(x_1) + \alpha(x_2) = \alpha(x_1 + x_2)$ és $\alpha(x_1)\alpha(x_2) = \alpha(x_1 x_2)$ (tehát $\alpha(L)$ izomorf az $(L, +, \cdot)$ testtel. Következik, hogy $(\alpha(L), +, \cdot) \in \mathcal{M}$ és $(\overline{K}, +, \cdot) < (\alpha(L), +, \cdot)$ ami ellentmond a $(\overline{K}, +, \cdot)$ maximalitásával.

Igazoltuk, hogy $(\overline{K}, +, \cdot)$ algebrailag zárt, de mivel $(\overline{K}, +, \cdot)$ algebrai bővítése K-nak következik, hogy $(\overline{K}, +, \cdot)$ algebrai lezártja a $(K, +, \cdot)$-nak.

Egyértelműség. Ha $\overline{K}$ és L két algebrai lezártja a K-nak, akkor az előző tételből következik, hogy 1_K meghosszabítható a $\overline{K} \simeq L$ izomorfizmusig. ■

5.5.9. példa. 1) Az $\mathbb{R}$ test algebrai lezártja $\mathbb{C}$ és a $\mathbb{Q}$ algebrai lezártja az $\mathbb{A}$ algebrai számok teste.

2) Ha $0 < m < n$, akkor $m! \mid n!$, és kapjuk a következő növekvő láncot:

$$\mathbb{F}_p \subset \mathbb{F}_{p^{2!}} \subset \mathbb{F}_{p^{3!}} \subset \cdots$$

Legyen

$$\mathbb{F}_{p^\infty} := \bigcup_{n \in \mathbb{N}^*} \mathbb{F}_{p^{n!}}.$$

Ekkor $\mathbb{F}_{p^\infty}$ egy test mely tartalmazza $\mathbb{F}_{p^n}$-t mint résztest minden $n \in \mathbb{N}^*$-re. Az $\mathbb{F}_{p^\infty}$ test minden eleme véges multiplikatív rendű, $\mathbb{F}_{p^\infty}$ végtelen és p karakterisztikájú. Kimutatható, hogy $\mathbb{F}_{p^\infty}$ algebrailag zárt, az $\mathbb{F}_p$ test algebrai lezártja.

5.34. feladat. Igazoljuk, hogy az 5.5.7. tétel bizonyításában értelmezett $(\mathcal{M}, \leq)$ rendezett halmaz eleget tesz a Zorn-lemma feltételeinek.

5.35. feladat. Igazoljuk, hogy az 5.5.8. tétel bizonyításaban értelmezett $(\mathcal{M}, \leq)$ rendezett halmaz eleget tesz a Zorn-lemma feltételeinek.

5.6. Szeparábilis algebrai bővítések

Legyen K egy kommutatív test.

5.6.1. definíció. a) Egy $f \in K[X]$ n-edfokú polinomot **szeparábilis polinom**nak nevezünk (a K test felett), ha n különböző gyöke van a felbontási testében.

b) $K \leq L$ **szeparábilis bővítés**, ha minden elem az L-ból egy K feletti szeparábilis polinomnak a gyöke (azaz, ha L minden elemének a minimálpolinomja szeparábilis).

5.6.2. tétel. $f \in K[X]$ *szeparábilis* K *felett, akkor és csak akkor, ha* f *és* f' *legnagyobb közös osztója* 1.

Bizonyítás. Legyen F az f felbontási teste. $F[X]$-ben kapjuk:

$$f = a(X - x_1)^{m_1} \dots (X - x_k)^{m_k},$$

ahol a az X^n együtthatója f-ben (f n-ed fokú) és $x_1, \dots, x_k$ különböző elemek F-ből, az $m_1, \dots, m_k$ számok pedig pozitív egészek. Következik, hogy

$$\begin{aligned} f' &= am_1(X - x_1)^{m_1 - 1}(X - x_2)^{m_2} \dots (X - x_k)^{m_k} + \dots \\ &\quad + am_k(X - x_1)_1^m \dots (X - x_{k-1})^{m_{k-1}}(X - x_k)^{m_k - 1} \end{aligned}$$

Következik, hogy az f és f' polinomok d legnagyobb közös az $X - x_1, \dots, X - x_k$ hatványainak szorzata. Tehát $d = 1$ akkor és csakis akkor, ha az $X - x_1, \dots, X - x_k$ polinomok közül egyik sem osztja f'-et, és ez csak akkor állhat fenn, ha $m_1 = \dots = m_k = 1$, vagyis f szeparábilis.

(Megjegyezzük, hogy f és f' legnagyobb közös osztója nem változik a $K[X]$-ról $F[X]$-re való áttéréskor. Ez onnan következik, hogy a legnagyobb közös osztó meghatározható az Euklidesz-algoritmussal.) ■

5.6.3. következmény. a) *Legyen* $f \in K[X]$ *irreducibilis polinom.* f *szeparábilis akkor és csakis akkor, ha* $f' \neq 0$.

b) *Ha* $\operatorname{char} K = 0$ *és* $f \in K[X]$ *irreducibilis polinom, akkor* f *szeparábilis.*

c) *Legyen* $\operatorname{char} K = p$ *prímszám. Az* $f \in K[X]$ *irreducibilis polinomnak akkor és csakis akkor van többszörös gyöke, ha* $f \in K[X^p]$.

Bizonyítás. a) Valóban, mivel $\deg f' < \deg f$ és mivel f irreducibilis, következik, hogy ha $f' \neq 0$, akkor az f és f'-nek d legnagyobb közös osztója egyenlő 1-el, ahonnan következik, hogy f szeparábilis.

Ha $f' = 0$, akkor $d = f \notin k$, ami az előző tétel alapján azt jelenti, hogy f nem szeparábilis.

b) Ha f irreducibilis $K[X]$-ben, akkor $f \notin K$, ami implikálja, hogy $f' \neq 0$. Tehát a)-ból következik, hogy f szeparábilis.

c) Alkalmazzuk a)-t és azt, hogy $f' = 0$ akkor és csak akkor, ha $f \in K[X^p]$. ■

5.6.4. definíció. Egy K testet **tökéletes**nek nevezünk, ha a $\varphi : K \to K$ Frobenius-endomorfizmus automorfizmus.

5.6.5. példa. 1) Azonnal belátható, hogy a 0 karakterisztikájú testek, az algebrailag zárt testek és a véges testek tökéletesek.

2) Legyen $K = \mathbb{Z}_p(X) = \{\frac{f}{g} \mid f, g \in \mathbb{Z}_p[X]\}$ a $\mathbb{Z}_p[X]$ hányadosteste. Ebben az esetben φ nem szürkektív, tehát K nem tökéletes.

5.6.6. tétel. *Egy* K *test tökéletes akkor és csakis akkor, ha bármely algebrai bővítése szeparábilis.*

Bizonyítás. Elegendő a bizonyítást abban az esetben elvégezni, ha $\operatorname{char} K = p \neq 0$. Ha létezne olyan x elem a K test egy bővítéséből, amelyik nem szeparábilis K felett, akkor az $m_{x,K} \in K[X^p]$. Tehát

$$f = \sum_{i=0}^{n} a_i X^{pi}$$

Ha a k test tökéletes, akkor létezik $b_i \in K$ úgy hogy $b_i^p = a_i$. Akkor

$$f = \sum_{i=0}^{n} b_i^p X^{pi} = (\sum_{i=0}^{n} b_i X^i)^p$$

tehát f reducibilis lenne $k[X]$-ben, ami ellentmondás!

Fordítva, kimutatjuk, hogy ha a K test nem tökéletes, akkor létezik egy algebrai elem a K felett, amely nem szeparábilis. Mivel a K test nem tökéletes, következik, hogy létezik egy $X^p - a$ alakú polinom ($a \in K$), amelynek egyetlen gyöke sincs K-ban. Elég igazolni, hogy $X^p - a \in K[X^p]$ irreducibilis $K[X]$-ben (mert akkor az $F_{f,K}$ felbontási test nem szepárábilis bővítése K-nak).

Valóban, legyen x és y az $X^p - a$ polinom gyökei a k egy algebrai lezártjában. Innen kapjuk, hogy $x^p = y^p$, ahonnan következik, hogy $x = y$. Így tehát az $X^p - a$ egyetlen x gyöke van a k-ban, amelynek a multiplicitása p. Ha $g := m_{x,k}$, kapjuk, hogy

$$X^p - a = g^s.$$

Legyen b a g-nek a nulladfokú tagja. Kapjuk, hogy $a = b^s$, ahol $p = s \deg g$. Mivel az $X^p - a$ polinomnak nincs gyöke a k-ban, következik, hogy $s = 1$ és következésképp a $X^p - a$ polinom irreducibilis $K[X]$-ben. ■

5.6.7. tétel. *Legyen K egy végtelen test és $K \leq L$ véges, szeparábilis bővítés, ekkor a $K \leq L$ bővítés egyszerű (van primitív eleme).*

Bizonyítás. Mivel $K \leq L$ véges bővítés, következik, hogy léteznek $u_1, \ldots, u_k \in L$ úgy, hogy $L = K(u_1, \ldots, u_k)$. Bebizonyítjuk a tételt $k = 2$ esetre, ahonnan indukcióval levezethető az általános eset.

Feltételezzük, hogy $L = K(a, b)$. Legyen $f = m_{a,K}$, $g = m_{b,K}$, $n = \deg f$, $m = \deg g$, $F = F_{fg,K}$ pedig az $fg \in K[x]$ felbontási teste.

Mivel a $K \leq L$ bővítés szeparábilis, kapjuk, hogy f-nek van n darab $a_1 = a, a_2, \ldots, a_n$ különböző gyöke, g-nek pedig m darab különböző $b_1 = b, b_2, \ldots, b_m$ gyöke.

Abból, hogy K végtelen, következik, hogy létezik $c \in K$ úgy hogy

$$a_i + cb_j \neq a + bc$$

ha $(i, j) \neq (1, 1)$ és $1 \leq i \leq n$, $1 \leq j \leq m$. Jelölje $d = a + bc$ és megmutatjuk, hogy $L = K(d)$.

Evidens, hogy $K(d) \subseteq K(a, b) = L$.

Az $f_1 = f(d - cx)$ polinom együtthatói a $K(d)$-ből vannak. Vegyük észre, hogy

$$f_1(b) = f(d - bc) = f(a) = 0$$

vagyis $b_1 = b$ közös gyöke az f_1-nek és g-nek. A c elem kiválasztásából következik, hogy f_1 és g-nek nincsen több közös gyöke. Tehát $X - b$ a legnagyobb közös osztója az f_1 és g-nek, amelyek együtthatói $K(d)$-ben vannak, ahonnan következik, hogy $X - b$ együtthatói $K(d)$-ben vannak. Tehát $b \in K(d)$, és mivel $d = a + bc$ és $c \in K$ következik, hogy $a \in K(d)$. Kapjuk, hogy $k(a, b) \subseteq K(d)$. Így kimutattuk, hogy $L = K(a, b) = K(d)$. ■

5.6.8. tétel. *Legyen $k \leq K$, $p > 0$ karakterisztikájú testek algebrai bővítése.*

1) *Ha K szeparábilis bővítése a k-nak, akkor $K = k(K^p)$.*

2) *Ha $[K : k] < \infty$ és $K = k(K^p)$ akkor K szeparábilis bővítése a k-nak.*

3) *Az $x \in K$ elem szeparábilis a k felett akkor és csakis akkor, ha $k(x) = k(x^p)$. Ha x szeparábilis k felett akkor $k(x)/k$ szeparábilis bővítés.*

Bizonyítás. 1) Mivel K szeparábilis bővítése a k-nak, következik, hogy K szeparábilis bővítése a $k(K^p)$-nek. Ha $k(K^p) = K' \neq K$, akkor létezne egy $x \in K$ elem, amelyikre fennáll, hogy $x \notin K'$. Akkor láttuk, hogy az $X^p - x^p$ polinom irreducibilis $K'[X]$-ben. Mivel $X^p - x^p \in K'[X^p]$ következne, hogy x nem szeparábilis K' felett, ami ellentmondás.

2) Feltételezzük, hogy létezik egy $x \in K$ elem, amely nem szeparábilis k felett. Ekkor az x minimálpolinomja k felett a következő alakú:

$$f = \sum_{i=0}^{n} a_i (X^p)^i, \qquad a_i \in k, \qquad n > 0.$$

Tehát x-re igaz:

$$\sum_{i=0}^{n} a_i (x^p)^i = 0 \tag{5.2}$$

Az $1, x, \ldots, x^n$ elemek azonban lineárisan függetlenek k felett, tehát kiegészíthetőek a K egy k feletti bázisává. Legyen tehát $1, x, \ldots, x^n, y_1, \ldots, y_k$ a K egy k feletti bázisa. Így abból, hogy, hogy $k(K^p) = K$, következik, hogy az

$$1, x^p, \ldots, (x^p)^n, y_1^p, \ldots, y_k^p \tag{5.3}$$

elemek szintén a K egy generátorrendszerét adják. Valóban a hipotézisből következik, hogy a K-beli elemek lineáris kombinációi a K^p-beli elemek k-beli együtthatóinak amelyek lineáris kombinációi a (5.3) rendszer elemei k^p-beli együtthatóinak.

Így a (5.3) elemrendszer a K k feletti bázisa lenne. Viszont a (5.2) összefüggés alapján a (5.3) rendszer első $n+1$ eleme lineárisan függőek.

3) Ha x szeparábilis k felett, akkor x szeparábilis $k(x^p)$ felett is. Ha pedig $x \notin k(x^p)$, akkor következne, hogy x nem szeparábilis $k(x^p)$ felett sem. Tehát $x \in k(x^p)$ és $k(x) = k(x^p)$.

Fordítva, ha $k(x) = k(x^p)$, akkor következik, hogy $k(x) = k((k(x))^p)$ és az előző állításból kapjuk, hogy bármely elem a $k(x)$-ből szeparábilis k felett. ■

5.6.9. következmény (a szeparábilitás tranzitívitása). *Ha $k \leq K$ és $K \leq L$ szeparábilis algebrai testbővítések, akkor a $k \leq L$ bővítés is szeparábilis.*

Bizonyítás. Feltételezhetjük, hogy a testek karakterisztikája $p \neq 0$. Legyen $x \in L$. Ekkor x szeparábilis a K' test felett, amely testet a k felett az x K feletti minimálpolinomának az együtthatói generálják. A 5.6.8. c) alapján $K'(x^p) = K'(x)$, a 5.6.8. b) állítás miatt pedig $k(K'^p) = K'$, mivel $k \leq K'$ szeparábilis. Tehát

$$k((K'(x))^p) = K'(x^p) = K'(x)$$

és ismét alkalmazva a 5.6.8. b)-t kapjuk, hogy x szeparábilis k felett. ■

5.36. feladat. Ha K tökéletes test és $f \in K[X]$ irreducibilis polinom, akkor f szeparábilis.

5.37. feladat. Legyenek $k \leq K \leq L$ algebrai testbővítések.

a) Ha $x \in L$ szeparábilis elem a k felett, akkor x szeparábilis a K felett is. Sajátos esetben, ha L szeparábilis bővítése a k-nak, akkor L szeparábilis bővítése a K-nak.

b) Egy tökéletes test bármely algebrai bővítése tökéletes test.

Megoldás. a) Ha L/k szeparábilis bővítés, akkor tetszőleges L-beli a elemre az $f = m_k(a)$ polinomnak nincs többszörös gyöke az L testben. Legyen $g = m_{K,a} \in K[X]$.

Mivel $k \leqslant K$, $k[X] \leqslant K[X]$. Ez azt jelenti, hogy $f \in K[X]$, és mivel $f(a) = 0$, $K[X]$-ben kapjuk, hogy $g \mid f$. Felhasználva, hogy f-nek nincs többszörös gyöke, így a szeparábilis K felett. Mivel a tetszőleges L-beli elem volt, kapjuk, hogy L/K szeparábilis.

b) Legyen egy L/K tetszőleges algebrai bővítés és mivel K/k algebrai - az algebrai bővítések tranzitivitását felhasználva - L/k is algebrai bővítés lesz. Ez utóbbi eredményből és a feltételekből adódik, hogy L/k szeparábilis. De ekkor az a) pont értelmében L/K is szeparábilis bővítés. Mivel L/K tetszőleges volt, következik, hogy K tökéletes test.

5.38. feladat. Keressünk egy primitív elemet a $\mathbb{Q} \leq \mathbb{Q}(\sqrt{2}, \sqrt{5})$ bővítés esetén.

5.7. Normális algebrai bővítések

5.7.1. definíció. Ha a $k \leq K$ algebrai bővítés teljesíti a következő tétek ekvivalens állí tásait, akkor azt mondjuk, hogy $k \leq K$ **normális bővítés**.

5.7.2. tétel. *Legyen $k \leq K$ egy algebrai bővítése és $\overline{k}$ a k-nak algebrai lezártja, amely tartalmazza a K-t. A kövekező állítások ekvivalensek:*

(i) *$\overline{k}$ minden k-automorfizmusa indukál egy K-nak egy k-automorfizmusát.*

(i') *Ha $u \in \mathrm{Aut}_k(K)$, akkor $u(K) \subseteq K$.*

(ii) *Ha egy $k[X]$-beli irreducibilis polinomnak van egy gyöke K-ban, akkor minden gyöke K-ban van.*

(iii) *Bármely L/K algebrai bővítés esetén, L minden k-automorfizmusa indukál K-nak egy automorfizmusát.*

Bizonyítás. (i)$\Rightarrow$ (i') evidens.

(i')$\Rightarrow$(i) Elég igazolni, hogy u szürjektív. Legyen $y \in K$ és $f \in k[X]$ az y minimálpolinomja. Akkor u az f bármely K-beli gyökét az f egy másik K-beli gyökébe viszi. Mivel u injektív leképezés és az f K-beli gyökeinek a halmaza véges, következik, hogy u szürjektív az f K-beli gyökeinek halmazán. Innen következik, hogy u szürjektív.

(i)⇒(ii) Legyen $f \in k[X]$ egy irreducibilis polinom a és $x \in K$ gyöke f-nek. Ha $y \in \overline{k}$ egy másik gyöke f-nek, tudjuk, hogy létezik $u : k(x) \to k(y) \subseteq \overline{k}$ k-automorfizmus úgy, hogy $u(x) = y$, amely kiterjeszthető egy $\overline{u} : \overline{k} \to \overline{k}$ k-automorfizmussá, az 5.5.7. tétel alapján. Akkor (i)-ból következik, hogy $\overline{u}(K) = K$, tehát $u(x) = y \in K$.

(ii)⇒(iii) Legyen $u : L \to L$ egy k-automorfizmus, x egy K-beli elem és $f \in k[X]$ az x k feletti minimálpolinomja. Ekkor $u(x)$ gyöke f-nek, vagyis $u(x) \in K$, tehát $u(K) \subseteq K$. Innen következik, hogy $u(K) = K$ (lásd az (i')⇒(i) bozonyítását).

A (iii)⇒(i) implikáció nyilvánvaló. ■

5.7.3. tétel. 1) *Egy* $k \leq K$ *véges bővítés akkor és csakis akkor normális, ha létezik egy* $f \in k[X]$ *polinom, aminek a felbontási teste* K.

2) *Ha* $k \leq K$ *egy véges, normális és szeparábilis bővítés, akkor létezik egy* $f \in k[X]$ *szeparábilis polinom, amelynek a felbontási teste* K.

Bizonyítás. Először is kimutatjuk hogy egy $f \in k[X]$ polinom felbontási teste normális bővítése k-ak, vagyis igazoljuk az 1) állítás egyik irányú implikációját. Feltételezzük, hogy K az $f \in k[X]$ felbontási teste és hogy a $k \subseteq K$ bővítés nem normális. Következik, hogy létezik egy $g \in k[X]$ polinom, amelynek van egy $x_1 \in K$ gyöke és egy $x_2 \notin K$ gyöke is. Az 1_K izomorfizmus meghosszabbítható egy

$$\varphi : k(x_1) \to k(x_2)$$

izomorfizmussá, amelyre igaz, hogy $\varphi(x_1) = x_2$.

A K test az f $k(x_1)$ feletti gyökeinek a teste, a $K(x_2)$ pedig az f $k(x_2)$ feletti gyökeinek teste. Tehát a φ izomorfizmus meghosszabbítható egy

$$\overline{\varphi} : K \to K(x_2)$$

izomorfizmussá. Mivel $\overline{\varphi}$ az 1_K meghosszabbítás, következik, hogy $\overline{\varphi}$ egy lineáris k-tér izomorfizmus is. Másrészt mivel $x_2 \notin K$ kapjuk, hogy $\dim_k K < \dim_k K(x_2)$, ami ellentmond annak, hogy $\overline{\varphi}$ egy lineáris k-tér izomorfizmus.

Bebizonyítjuk az 1) állítás másik irányú implikációját és a 2) állítást.

Feltételezzük, hogy $k \subseteq K$ egy véges normális bővítés. Ha $K = k$, akkor K bármely elsőfokú polinom felbontási testének tekinthető. Ha $K \neq k$, akkor létezik $x_1 \in K/k$, ha pedig $f_1 \in k[X]$ az x_1 minimálpolinomja, akkor mivel f_1 irreducibilis k felett és a $k \subseteq K$ normális, következik, hogy az f_1 minden gyöke K-ban van. Tehát a K_1 felbontási teste az f_1-nek részteste K-nak és $k \neq K_1$. Ha a $k \leq K$ bővítés szeparábilis is, akkor igaz, hogy f_1 polinom szeparábilis, vagyis K_1 test egy szeparábilis polinom felbontási teste.

Ha $K_1 \neq K$, akkor létezik $x_2 \in K \setminus K_1$, ha pedig $f_2 \in k[X]$ az x_2 minimálpolinomja, akkor az $f_1 f_2$ polinom K_2 felbontási teste részteste a K-nak és fennáll $K_1 < K_2$. Ha a $k \subset K$ bővítés szeparábilis is, akkor az f_2 szeparábilis is; az $f_1 \neq f_2$-ből és mivel f_1 és f_2 prímek következik, hogy f_1 és f_2 relatív prímek. Tehát f_1 és f_2-nek nincsenek közös gyökei. Következik, hogy $f_1 f_2$ szeparábilis.

Ha $K_2 \neq K$ az előbbi mintára megszerkeszthető K_3 és kapunk egy szigorúan növekvő sorozatot:

$$k \subset K_1 \subset K_2 \subset K_3 \subset \dots$$

amely a K olyan résztesteiből áll, amelyek k[X]-beli polinomok felbontási testei, ha pedig $k \subset K$ bővítés szeparábilis is, akkor ezek a polinomok szeparábilisak is.

Abból a feltevésből, hogy a $k \leq K$ bővítés véges, kapjuk, hogy létezik $n > 0$, úgy hogy $K = K_n$. ■

5.7.4. példa. 1) Bármely testbővítés, amelynek a foka 2, normális bővítés.

Valóban, legyen k egy test és K a k test egy másodfokú bővítése. Ha $x \in K$ és $x \neq k$, akkor $1, x$ egy bázisa a K-nak a k felett, tehát $K = k(x)$. Ha $f = X^2 + aX + b$ az x minimálpolinomja, akkor az f foka 2. Mivel f-nek létezik egy gyöke K-ban, következik, hogy a második gyöke is K-ban van (mert a gyökök összege $-a \in K$). Így K az f felbontási teste, s ennek következménye, hogy K a k-nak normális bővítése.

2) Bármely véges K test normális bővítése minden résztestének.

Valóban, ha K-nak van p^r eleme, ahol p a K test karakterisztikája, akkor K a felbontási teste $X^{p^r} - X$ polinomnak, minden részteste esetén.

3) Legyen $K = \mathbb{Q}(\sqrt[3]{4})$, amelyet a $\mathbb{Q}$ egy bővítésének tekintünk. Ez egy nem normális bővítés.

Valóban $\sqrt[3]{4}$-nak a minimálpolinomja $X^4 - 3$ és ennek nincsen mindegyik gyöke K-ban. Ennek a polinomnak nem minden gyöke valós.

4) A normális algebrai bővítések nem rendelkeznek a tranzitivitás tulajdonságával.

Valóban, például $\mathbb{Q}(\sqrt[3]{4})$ nem normális bővítése $\mathbb{Q}$-nak, habár $\mathbb{Q}(\sqrt{3})$ normális bővítése $\mathbb{Q}$-nak, $\mathbb{Q}(\sqrt[3]{4})$ pedig normális bővítése $\mathbb{Q}(\sqrt{3})$-nak.

5.7.5. tétel. *Legyenek* $L \supseteq K \supseteq k$ *algebrai testbővítések. Ha* L *normális bővítése* k*-nak, akkor* L *normális bővítése* K*-nak is.*

Bizonyítás. Legyen $\overline{k}$ a k-nak egy algebrai lezártja, amely tartalmazza L-et. A feltevésből következik, hogy bármely $u \in \mathrm{Aut}_k(\overline{k})$ elem indukálja egy k-automorfizmusát az L-nek és abból, hogy $\mathrm{Aut}_K(\overline{k})$ részcsoportja $\mathrm{Aut}_k(\overline{k})$-nak következik, hogy L normális bővítése K-nak. ■

5.7.6. tétel. *Legyen* k *egy test és* K *egy véges bővítése. Ekkor létezik egy normális véges bővítése* k*-nak, amely tartalmazza* K*-t.*

Bizonyítás. Legyen $K = k(x_1, x_2, \dots, x_n)$ és $f_i \in k[X]$ az x_i minimálpolinomja, $i = 1, \dots, n$. Akkor L az $f = \prod_{i=1}^{n} f_i$ polinomnak a felbontási teste, amely benne van egy $\overline{k}$ algebrai lezártjában a k-nak, amely tartalmazza K-t. Ez egy véges és normális bővítése k-nak, amely tartalmazza K-t. ■

5.39. feladat. Legyen $k \leq L$ egy testbővítés és $K_1 \leq L$ valamint $K_2 \leq L$ két algebrai bővítése a k-nak. Jelölje $K_1K_2 = k(K_1, K_2)$ az L-nek azon résztestét, amelyet K_1 és K_2 generál.

a) Ha K_1 a K-nak normális bővítése, akkor K_1K_2 normális bővítése K_2-nek.

b) Ha K_1/k és K_2/k normális bővítések, akkor K_1K_2 és $K_1 \cap K_2$ normális bővítései k-nak.

Megoldás. a) Legyen $\overline{k}$ a k-nak egy olyan algebrai lezártja, amely tartalmazza K_1K_2-t. Észrevesszük, hogy létezik ilyen lezárás, tehát K_1K_2 algebrai bővítése k-nak. Abból a tényből, hogy $\mathrm{Aut}_{K_2}(\overline{k}) \subseteq \mathrm{Aut}_k(\overline{k})$ és K_1 normális bővítése k-nak következik, hogy $u(K_1) \subseteq K_1$ minden $u \in G(\overline{k}/K_2)$ esetén.

Hasonlóan $u(K_2) \subseteq K_2$ és következik, hogy $u(K_1K_2) \subseteq K_1K_2$.

b) Legyen $u \in \mathrm{Aut}_k(\overline{k})$. Mivel K_1 és K_2 testek normális bővítései k-nak, következik, hogy $u(K_1) \subseteq K_1$, és $u(K_2) \subseteq K_2$. Tehát $u(K_1K_2) \subseteq K_1K_2$ és $u(K_1 \cap K_2) \subseteq K_1 \cap K_2$.

5.8. Galois-csoport

Legyen K egy test, és $\mathrm{Aut}(K)$ a K automorfizmusainak a halmaza. Legyen a $k \leqslant K$ testbővítés és

$$\begin{aligned} G(K/k) &= \mathrm{Aut}_k(K) = \{\sigma \in \mathrm{Aut}(K) \mid \sigma(\alpha) = \alpha \ , \forall \alpha \in k\} \\ &= \{\sigma : K \to K \mid \sigma \text{ } k\text{-algebraizomorfizmus}\}. \end{aligned}$$

5.8.1. definíció. A $(G(K/k), \circ)$ csoport neve a K/k bővítés **Galois-csoportja**.

Ha $K = F_{f/k}$ az $f \in k[x]$ polinom felbontási teste a k felett, akkor

$$G(f/k) := G(F_{f/k}/k)$$

az f polinom k feletti Galois-csoportja vagy az $f(x) = 0$ egyenlet k feletti Galois-csoportja.

5.8.2. definíció. A K/k bővítést **Galois-bővítés**nek nevezzük, ha K/k véges, normális és szeparábilis.

5.8.3. megjegyzés. 1) Legyenek a $k \leqslant K \leqslant L$ testbővítések. Ha L/k Galois-bővítés, akkor L/K is az.

2) Ha k a K test részprímteste, akkor $G(K/k) = \mathrm{Aut}(K)$.

Valóban, mivel minden $a \in K$ esetén $a = (m \cdot 1)(n \cdot 1)^{-1}$ alakú, ahol $m, n \in Z$, $1 \in K$ és $n \cdot 1 \neq 0$. Ugyanakkor, ha $\sigma \in \mathrm{Aut}(K)$ akkor $\sigma(1) = 1$. Minden $a \in K$-ra fennáll, hogy: $\sigma(a) = \sigma(m \cdot 1)\sigma(n \cdot 1)^{-1} = \sigma(m)\sigma(1)\sigma(n^{-1})\sigma(1) = (m1)(n1)^{-1} = a$, tehát $\sigma \in G(K/k)$, azaz $\mathrm{Aut}(K) \subseteq G(K/k)$. Tehát $\mathrm{Aut}(K) = G(K/k)$.

3) Legyen $k \leqslant K$ testbővítés, $f \in k[X]$ egy polinom és $u \in K$ az f-nek egy gyöke. Ha $\sigma \in G(K/k)$, akkor $\sigma(u)$ szintén gyöke lesz az f-nek.

Valóban, legyen $f = a_0 + a_1x + \dots + a_nx^n$. Akkor $a_0 + a_1u + \dots + a_nu^n = 0$; mivel $\sigma(a_i) = a_i$, $i = 1, 2, \dots, n$ és σ morfizmus, következik, hogy $a_0 + a_1\sigma(u) + \dots + a_n[\sigma(u)]^n = 0$, vagyis a $\sigma(u)$ gyöke f-nek.

5.8.4. tétel (Galois-bővítés Galois-csoportja). *Legyen* K/k *egy Galois-bővítés.*

1) *Létezik* $x \in K$ *úgy, hogy* $K = k(x)$*, és* $K = F_{f/k}$*, ahol* $f := m_{k,x}$.

2) $|G(K/k)| = [K : k] = \deg m_{k,x}$.

3) *Feltételezzük, hogy* $\deg m_{k,x} = n$*. Ekkor létezik* $\varphi : G(K/k) \hookrightarrow S_n$ *injektív csoportmorfizmus.*

Bizonyítás. 1) Mivel K/k véges és szeparábilis, létezik primitív eleme, azaz létezik $x \in K$ szeparábilis elem ($m_{k,x}$-nek nincs többszörös gyöke) úgy, hogy

$$K = k(x) = \{\alpha_0 + \alpha_1x + \dots + \alpha_{n-1}x^{n-1} \mid \alpha_i \in k\}.$$

Mivel K/k normális, $m_{k,x}$ minden gyöke K-ban van, tehát $K = F_{f/k}$.

2) Legyen $n := [K : k] = \deg f$. Legyenek $x = x_1, x_2, \dots, x_n \in K$ az f (különböző) gyökei.

Ha $\sigma \in G(K/k)$, akkor $\sigma(x)$ is gyöke f-nek, tehát $\sigma(x) \in \{x_1, x_2, \dots, x_n\}$. Mivel $K = k(x)$, a $\sigma(x)$ elem meghatározza σ-t. Tehát $|G(K/k)| \leqslant n$.

Igazoljuk, hogy $|G(K/k)| \geq n$. Mivel x, x_i konjugált elemek, létezik $\sigma_i : k(x) \to k(x_i)$ k-automorfizmus úgy, hogy $\sigma_i(x) = x_i$. Mivel $k \leqslant k(x_i) \leqslant K$ és $[K : k] = [k(x_i) : k] = \deg f$, következik, hogy $k(x_i) = K$, tehát $\sigma_1, \dots, \sigma_n \in G(K/k)$ különböző automorfizmusok.

3) Ha $\sigma \in G(K/k)$ akkor tetszőleges $i = 1, 2, \dots, n$ esetén $\sigma(x_i)$ gyöke f-nek vagyis $\sigma(x_i) \in \{x_1, x_2, \dots, x_n\}$. Láttuk, hogy a gyökök képe meghatározza σ-t. Legyen $\varphi : G(K/k) \to S_n$ úgy, hogy

$$\varphi(\sigma) = \begin{pmatrix} x_1 & x_2 & \dots & x_n \\ \sigma(x_1) & \sigma(x_2) & \dots & \sigma(x_n) \end{pmatrix}$$

Akkor $\varphi(\sigma \circ \tau) = \varphi(\sigma) \circ \varphi(\tau)$, mert $(\sigma \circ \tau)(x_i) = \sigma(\tau(x_i))$, tehát φ csoportmorfizmus. Mivel a gyökök képe meghatározza σ-t, következik, hogy φ injektív. ■

A 5.8.4. tétel alapján a Galois csoport megegyezik az S_n egy megfelelő részcsoportjával. Feltevődik a kérdés, hogy a Galois-csoport mikor egyezik meg S_n-el.

5.8.5. tétel. 1) *Bármely $n > 0$ egész szám és bármely K_0 test esetén létezik egy K bővítése a K_0-nak és egy $f \in K[X]$ n-edfokú polinom, amelynek a Galois csoportja a K felett izomorf az S_n-el.*

2) *Minden $n > 0$ egész számra létezik az $\mathbb{R}$ test egy egy K részteste és egy $f \in K[X]$ n-ed fokú polinom, amelynek a Galois csoportja K felett izomorf S_n-nel.*

Bizonyítás. 1) Legyen $K' = K_0(X_1, \ldots, X_n)$ a $K_0[X_1, \ldots, X_n]$ polinom hányadosteste K_0 felett. Jelölje $K = K_0(s_1, \ldots, s_n)$ a K'-nek K_0 és az $s_1, \ldots, s_n$ elemi szimmetrikus polinomok által generált résztestét. Az

$$f = (X - X_1) \ldots (X - X_n) = X^n - s_1 X^{n-1} + \cdots + (-1)^n s_n \in K[X]$$

polinom felbontási teste K'. Megmutatjuk, hogy ebben az esetben

$$G(K/K') \to S_k, \qquad \sigma \to \varphi$$

injektív homomorfizmus szürjektív is. Ha φ az $\{1, \ldots, n\}$ halmaz egy permutációja, akkor következik, hogy létezik egy $\sigma : K_0[X_1, \ldots X_n] \to K_0[X_1, \ldots, X_n]$, amelyikre fennáll, hogy $\sigma(a) = a$ és $\sigma(x_i) = \sigma_{\varphi(i)}$, minden $a \in K_0$ és $i = 1, \ldots, n$ esetén.

A σ kiterjeszthető egy $\sigma' : K' \to K'$ automorfizmusra, tehát $\sigma' \in G(K/K')$ és az előbbi összefüggések alapján következik, hogy a $G(K/K') \to S_k$ homomorfizmus leképezi a σ'-et φ-re.

2) Az 1)-nek megfelelően elegendő megmutatni, hogy $\mathbb{R}$-nek van egy $\mathbb{Q}(s_1, \ldots, s_n)$-el izomorf részteste, ami ekvivalens avval az állítással, hogy $\mathbb{R}$-nek van egy részgyűrűje, ami izomorf a $\mathbb{Q}[X_1, \ldots, X_n]$-el.

Ezt n-szerinti indukcióval igazoljuk. Ha $n = 0$, az állítás visszavezetődik arra, hogy $\mathbb{Q}$ részteste $\mathbb{R}$-nek. Feltételezzük, hogy létezik egy $\sigma : \mathbb{Q}[X_1, \ldots, X_n] \to \mathbb{R}$ injektív homomorfizmus és jelölje $a_i = \sigma(X_i)$, $i = 1, \ldots, n$. A polinomgyűrű univerzális tulajdonságából következik, hogy minden $a \in \mathbb{R}$-re létezik egy

$$\sigma_a : \mathbb{Q}[X_1, \ldots, X_{n+1}] \to \mathbb{R}$$

homomorfizmus, amelyik meghosszabbítja a σ-t és $\sigma_a(n + 1) = a$. Következik, hogy ha felírunk egy $f \in \mathbb{Q}[X_1, \ldots, X_{n+1}]$ elemet a következő alakban

$$f = f_0 + f_1 X_{n+1} + \ldots + f_m X_{m+1} \qquad \text{ahol } f_j \in \mathbb{Q}[X_1, \ldots, X_n],\ j = 0, \ldots, m$$

akkor

$$\sigma_a(f) = \sigma(f_0) + \sigma(f_1)a + \ldots + \sigma(f_m)a^m$$

és $\sigma(f_j) \in \mathbb{Q}[a_1, \ldots, a_n] \subseteq \mathbb{Q}(a_1, \ldots, a_n)$.

Következésképp, ha σ_a nem injektív, akkor a algebrai $\mathbb{Q}(a_1, \ldots, a_n)$ felett. Ha egyetlen σ_a, ahol a valós szám, sem lenne injektív, akkor következne, hogy $\mathbb{R}$ algebrai bővítése a $\mathbb{Q}(a_1, \ldots, a_n)$-nek, ami ahhoz a hibás következtetéshez vezetne hogy $\mathbb{R}$ megszámlálható. Tehát létezik a valós szám, úgy hogy σ_a injektív legyen. ■

5.8.6. tétel. 1) *Legyen $f \in \mathbb{Q}[X]$ irreducibilis polinom, amelynek foka p prímszám. Feltételezzük, hogy f-nek pontosan $p - 2$ valós gyöke van. Akkor az f Galois csoportja izomorf S_p-vel.*

2) *Bármely $p \geqslant 5$ prímszám esetén létezik egy p-ed fokú $f \in \mathbb{Q}[X]$ polinom, amelynek Galois csoportja izomorf σ_p-vel.*

Bizonyítás. 1) Legyen $K = F_{f,\mathbb{Q}}$ és legyenek x_1, x_2 az f azon gyökei, amelyek nem valósak. Mivel $[\mathbb{Q}(x_1) : \mathbb{Q}] = p$ és $K \supseteq \mathbb{Q}(x_1)$ következik, hogy $p \mid [K : \mathbb{Q}]$; de mivel f irreducibilis és 0 karakterisztikájú, következik, hogy szeparábilis is és emiatt

$$[K : \mathbb{Q}] = |G(K/\mathbb{Q})|.$$

Tehát létezik egy u p-edrendű k-automorfizmusa a K-nak. Azonosítva $G = G(K/\mathbb{Q})$-t az f gyökeinek egy permutációcsoportjával, u-nak megfelel egy p hosszúságú ciklus. Másrészt ez a hozzárendelés indukálja egy v $\mathbb{Q}$-automorfizusát a K-nak, amely felcseréli x_1-et x_2-vel és fixen hagyja az f összes többi gyökét, vagyis v-nek megfelel az S_p egy transzpozíciója. Tudjuk, hogy egy l hosszuságú ciklus rendje l és két diszjunkt ciklus szorzatának rendje a két rend legnagyobb közös osztója.

Tehát G tartalmaz egy p-edrendű ciklust, $\sigma = (i_1\ \ldots\ i_p)$, ahol $i_k \in \{1, \ldots, p\}$, $1 \leq k \leq p$. Az általánosság leszükítése nélkül feltételezhetjük, hogy G az $(1, 2)$ transzpozíciót tartalmazza, és mivel σ-nak egy hatványa $(1\ 2\ \ldots\ p)$, feltételezzük, hogy $(1\ 2 \ldots\ p)$-t is tartalmazza G. Így $\sigma(1\ 2)\sigma^{-1} = (2\ 3)$, ..., $\sigma(p-2\ p-1)\sigma^{-1} = (p-1\ p)$. Ezek a transzpozíciók generálják G-t, tehát $G = S_p$.

2) Legyen m egy páros egész szám, $m > 0$. Legyen $n_1 < n_2 < \cdots < n_{k-2}$, $k-2$ páros egész szám, ahol k páratlan egész szám, $k > 3$. Tekintsük az

$$f = (X^2 + m)(X - n_1)(X - n_2)\dots(X - n_{k-2})$$

polinomot. Az $\tilde{f}$ polinomfüggvénynek $k-2$ valós gyöke van éspedig $n_1, n_2, \dots, n_{k-2}$. Rolle tételéből következik, hogy $\tilde{f}$-nek van legalább $k-3$ szélsőértéke, amelyből $\frac{k-3}{2}$ maximális és $\frac{k-3}{2}$ minimális. Mivel $m \geqslant 2$ és $n_1, n_2, \dots, n_{k-2}$ páros számok, akkor $|f(h)| > 2$ bármely h páratlan egész szám esetén. Következik, hogy az f értékei a maximum pontokban nagyobbak, mint 2.

Legyen $g = f - 2 \in \mathbb{Q}[X]$; akkor $\tilde{g}$-nek van legalább $\frac{k-3}{2}$ maximuma és $\frac{k-3}{2}$ minimuma. A $\tilde{g} : \mathbb{R} \to \mathbb{R}$ függvény értékei a maximum pontokban nagyobbak mint 0. Mivel van $\frac{k-3}{2}$ maximum és $\frac{k-3}{2}$ minimum következik, hogy g-nek van legalább $k-3$ valós gyöke. Mivel $g(n_{k-2}) = -f(n_{k-2}) - 2 = -2$ és $g(+\infty) = +\infty$ következik, hogy g-nek van még egy valós gyöke, amely nagyobb, mint n_{k-2}. Tehát g-nek van legalább $k-2$ valós gyöke. Igazolni fogjuk, hogy elég nagy m-re g-nek van két komplex gyöke.

Legyen $g = \prod_{i=1}^{k}(X - x_i)$ felbontása g-nek $\mathbb{C}[X]$-ben. Mivel

$$g = (X^2 + m)(X - n_1)\dots(X - n_{k-2}) - 2$$

az együtthatók azonosításából kapjuk, hogy

$$\sum_{i=1}^{k} x_i = \sum_{j=1}^{k-2} n_j \quad ; \quad \sum_{i<j} x_i x_j = \sum_{\alpha<\beta} n_\alpha n_\beta + m,$$

és

$$\sum_{i=1}^{k} x_i^2 = \left(\sum_{i=1}^{k} x_i\right)^2 - 2\sum_{i<j} x_i x_j = \sum_{\alpha=1}^{k-2} n_\alpha^2 - 2m.$$

Elég nagy m-re $\sum_{\alpha=1}^{k-2} n_\alpha^2 - 2m < 0$, vagyis $\sum_{i=1}^{k} x_i^2 < 0$. Azt jelenti, hogy g-nek legalább egy gyöke komplex. Mivel g együtthatói valószak, van legalább két komplex gyöke. Mivel $\deg g = k$ és g-nek van legalább $k-2$ valós gyöke, elég nagy m-re, g-nek van $k-2$ valós gyöke és két komplex gyöke.

A g polinom irreducibilis. Valóban $f(X) = X^k + a_1 X^{k-2} + \cdots + a_k$, ahol $a_1, a_2, \dots, a_k$ páros számok. Mivel $a_k = -mn_1n_2\dots n_{k-2}$ és $k > 3$, következik, hogy $4|a_k$. Akkor

$$g(X) = f(X) - 2 = X^k + a_1 X^{k-2} + \cdots + (a_k - 2)$$

összes együtthatója $a_1, a_2, \dots, a_{k-1}, a_{k-2}$ páros szám. Mivel 4 nem osztja $a_k - 2$-t alkalmazhatjuk Eisenstein irreducibilitási kritériumát és következik, hogy g k-adfokú irreducibilis polinom.

Ha $k = p$ prímszám, $p \geqslant 5$, akkor az 1) pont alapján következik, hogy a g polinom Galois csoportja izomorf σ_p-vel. ■

5.8.7. tétel (Véges testek automorfizmusai). *Legyen* $K = \mathbb{F}_{p^n}$ *egy véges test és* $k = \mathbb{F}_{p^m}$ *egy részteste. Ekkor* $G(K/k) = \langle \varphi^m \rangle$ *egy* $d = n/m$*-ed rendű ciklikus csoport, ahol* $\varphi : K \to K$, $\varphi(x) = x^p$ *a Frobenius-endomorfizmus.*

Bizonyítás. A véges testek tulajdonságaiból következik, hogy d egy természetes szám, é $k = \{x \in K \mid x^{p^m} = x\}$. Mivel $\varphi^m(x) = x^{p^m}$, következik, hogy $\varphi^{mi} \in G(K/k)$, $i = 1, 2, \dots, d$. Továbbá, ezek az automorfizmusok különbözőek, mivel, ha $\varphi^{si}(x) = \varphi^{mj}(x)$ minden $x \in K$ esetén, ahol $1 \leq i < j \leq d$, akkor

$$\begin{aligned} x^{n-m(j-i)} &= \varphi^{n-m(j-i)}(x) = \varphi^{n-mj}(\varphi^{mi}(x)) = \\ &= (\varphi^{n-mj}(\varphi^{mj}(x)) = \varphi^n(x) = x \end{aligned}$$

minden $x \in K$ elemre. Innen következik, hogy a K minden eleme gyöke lenne egy polinomnak, aminek a fokszáma kisebb, mint p^n, de ez ellentmondás.

Másrészt K/k egyszerű Galois-bővítés, $K = k(x)$, ahol x a K nemnulla elemei multiplikatív csoportjának egy generátora. Kapjuk, hogy $|G(K/k)| = [K : k] = d$, tehát $G(K/k) = \{\varphi^{mi} \mid i = 1, 2, \dots, d\}$. ■

5.40. feladat. Legyen $\mathbb{Q}(i\sqrt{2})$ a $\mathbb{Q}$ bővítése. Határozzuk meg a $G(\mathbb{Q}(i\sqrt{2})/\mathbb{Q})$ csoportot.

Megoldás. Legyen $u \in G(\mathbb{Q}(i\sqrt{2})/\mathbb{Q})$. Akkor $u(r+si\sqrt{2}) = u(r)+u(s)u(i\sqrt{2}) = r+su(i\sqrt{2})$. Mivel $(i\sqrt{2})^2+2 = 0$ kapjuk, hogy $0 = u((i\sqrt{2})^2) + 2 = (u(i\sqrt{2}))^2 + 2$. Innen levezethetjük, hogy $u(i\sqrt{2}) = i\sqrt{2}$ vagy $u(i\sqrt{2}) = -i\sqrt{2}$. Első esetben u az identikus automorfizmus, az utóbbiban pedig az $u(r + si\sqrt{2}) = r - si\sqrt{2}$ által értelmezett automorfizmus. Tehát a $G(\mathbb{Q}(i\sqrt{2})/\mathbb{Q})$ két elemet tartalmaz és emiatt izomorf $\mathbb{Z}_2$-vel.

5.41. feladat. Meghatározzuk az $f = X^4 - 3 \in \mathbb{Q}[X]$ polinom Galois-csoportját. Mivel f komplex gyökei: $\pm\sqrt[4]{3}$, $\pm i\sqrt[4]{3}$, ezért

$$F = F_{f,\mathbb{Q}} = \mathbb{Q}(\sqrt[4]{3}, -\sqrt[4]{3}, i\sqrt[4]{3}, -i\sqrt[4]{3}) = \mathbb{Q}(\sqrt[4]{3}, i).$$

Az $F/\mathbb{Q}$ bővítés foka 8, mert f irreducibilis a racionális számtest felett, tehát $\sqrt[4]{3}$ adjungálása negyedfokú bővítést jelent, és még a $\mathbb{Q}(\sqrt[4]{3})$ testhez i-t kell adjungálni, ami másodfokú bővítés; a fokszámok pedig összeszorzódnak.

Ha mármost az $F/\mathbb{Q}$ bővítés automorfizmusait akarjuk leírni, akkor először is világos, hogy elegendő megadni, hogy egy σ relatív automorfizmus miként hat $\sqrt[4]{3}$-on és i-n; hiszen F elemei $\sqrt[4]{3}$ és i-nek $\mathbb{Q}$-ból vett együtthatókkal képzett polinomjai, és σ művelettartó volta miatt elegendő σ hatását $\mathbb{Q}$-n (itt minden elem fix) és $\sqrt[4]{3}$-on valamint i-n ismerni. Mivel $\sqrt[4]{3}$ az $X^4 - 3$, i pedig az $X^2 + 1$ racionális együtthatójú irreducibilis polinom gyöke, az előbb mondottak szerint $\sqrt[4]{3}$ csak $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $i\sqrt[4]{3}$, $-i\sqrt[4]{3}$ valamelyikébe, i pedig csak i, $-i$-be mehet át tetszőleges relatív automorfizmusnál. Ennélfogva nyolc automorfizmusokról lehet szó.

Ha e az identikus leképezést, σ a $\sqrt[4]{3} \to i\sqrt[4]{3}$ $i \to i$, és τ a $\sqrt[4]{3} \to \sqrt[4]{3}$, $i \to -i$ leképezésekhez tartozó $\mathbb{Q}$-automorfizmust jelöli, akkor a fenti automorfizmusok rendre

$$e, \tau, \sigma^2, \sigma^2\tau, \sigma, \sigma\tau, \sigma^3, \sigma^3\tau$$

σ és τ között a következő relációk teljesülnek:

$$\sigma^4 = e, \tau^2 = e, \tau\sigma = \sigma^3\tau,$$

vagyis a $G(F/\mathbb{Q})$ Galois csoport most a D_4 diédercsoporttal izomorf.

Mivel az f polinom Galois csoportja az f permutációiból álló csoportnak is tekinthető, meghatározzuk a gyököknek azokat a permutációit, amelyeknek Galois csoport eleme felel meg. Az f polinomnak 4 gyöke van, ezeknek összesen $4! = 24$ permutációja van, de a Galois csoportnak csak 8 eleme van. Az hogy nem minden gyökpermutáció vezet relatív automorfizmushoz, onnan van, hogy a gyökök közt fennállhatnak olyan összefüggések, amelyek minden relatív automorfizmusnál helyes összefüggésbe kell hogy átmenjenek. Ebben a példában az első két gyök összege 0, és a második két gyök összege 0 és 0 minden automorfizmusnál fix elem. Ezért nem jelenthet automorfizmust az a permutáció, amelynél $-\sqrt[4]{3}$ és $-i\sqrt[4]{3}$ fix és $\sqrt[4]{3}$, $i\sqrt[4]{3}$ helyet cserél, mert ennél a helyes

$$\sqrt[4]{3} + (-\sqrt[4]{3}) = 0 \qquad i\sqrt[4]{3} + (-i\sqrt[4]{3}) = 0$$

összefüggések a helytelen

$$i\sqrt[4]{3} + (-\sqrt[4]{3}) = 0 \qquad \sqrt[4]{3} + (-i\sqrt[4]{3}) = 0$$

relációkba mennek át. A $\sqrt[4]{3}$, $-\sqrt[4]{3}$, $i\sqrt[4]{3}$, $-i\sqrt[4]{3}$ gyököket az $1, 2, 3, 4$ sorszámmal látva el, csak oly permutáció jelenthet relatív automorfizmust, amelynél az $1, 2$ pár az $1, 2$ párba vagy a $3, 4$ párba megy át, vagyis:

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

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

Számuk 8, tehát annyi, mint $G(F/\mathbb{Q})$ elemeinek a száma, így mindannyian előfordulnak. Valóban ezek rendre az

$$e, \sigma^2\tau, \tau, \sigma^2, \sigma\tau, \sigma^3, \sigma, \sigma^3\tau$$

$\mathbb{Q}$-automorfizmusoknak felelnek meg.

5.42. feladat. Bizonyítsuk be, hogy az $f = X^n - 1$ polinom és a Φ_n ciklotomikus polinom Galois csoportja $\mathbb{Q}$ felett izomorf az $(U(\mathbb{Z}_n), \cdot)$ csoporttal.

Megoldás. Meghatározzuk az f felbontási testét. Az f gyökei az n-edrendű egységgyökök a következő alakúak:

$$\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$$

ahol $k \in \{1, \ldots, n\}$. Sajátosan

$$\varepsilon_1 = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

Tudjuk, hogy $\varepsilon := \varepsilon_1$ generálja az összes többi gyököt, tehát az f $\mathbb{Q}$ feletti felbontási teste: $\mathbb{Q}(\varepsilon_1)$. Mivel Φ_n irreducibilis $\mathbb{Q}$ felett, következik, hogy $m_{\mathbb{Q},\varepsilon} = \Phi_n$. A $G = G(f/\mathbb{Q})$ Galois csoportot azok a σ_k automorfizmusok származtatják, amelyek a következő alakúak:

$$\sigma_k(\varepsilon_1) = \varepsilon_1^k = \varepsilon_k \qquad (k, n) = 1$$

ε_k szintén egységgyök lesz és a rendje megegyezik a ε_1 rendjével, tehát ε_k primitív egységgyök.

$$G = G(\mathbb{Q}(\varepsilon_1)/\mathbb{Q}) = \{\sigma_k \mid (k, n) = 1\}$$

Ezen σ_k-k száma megegyezik $\varphi(n)$-el, ami ugyanannyi, mint a $\mathbb{Z}_n$ egységeinek a száma, mert k egysége $\mathbb{Z}_n$-nek. Keressünk egy megfeleltetést G és $(U(\mathbb{Z}_n), \cdot)$ csoportok között. Minden σ_k-nak G-ből megfeleltetjük a $\hat{k}$ elemet $U(\mathbb{Z}_n)$-ből. Könnyen belátható, hogy ez a megfeleltetés izomorfizmus.

5.43. feladat. Legyen $2 \leq n \in \mathbb{N}$, és $f = X^n - a \in \mathbb{Q}[X]$. Ekkor $|G(f/\mathbb{Q})| = [F_{f,\mathbb{Q}} : \mathbb{Q}] \leq n(n-1)$.

Megoldás. Az f gyökei $x_k = \sqrt[n]{a}\varepsilon_k$, ahol $\varepsilon_k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n}$ és $k = 0, \ldots, n-1$; $\varepsilon := \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$ n-edik primitív egységgyök és $x_k = \sqrt[n]{a}\varepsilon^k$. Akkor $F_{f/\mathbb{Q}} = \mathbb{Q}(x_0, \ldots, x_{n-1}) = \mathbb{Q}(\sqrt[n]{a}, \varepsilon) = \mathbb{Q}(\sqrt[n]{a})(\varepsilon)$.

Az $F/\mathbb{Q}$ bővítés foka $[\mathbb{Q}(\sqrt[n]{a}, \varepsilon) : \mathbb{Q}] = [\mathbb{Q}(\sqrt[n]{a})(\varepsilon) : \mathbb{Q}(\varepsilon)] \cdot [\mathbb{Q}(\varepsilon) : \mathbb{Q}]$. De $[\mathbb{Q}(\sqrt[n]{a})(\varepsilon) : \mathbb{Q}(\varepsilon)] \leq n$ mert $\sqrt[n]{a}$ gyöke az $X^n - a \in \mathbb{Q}(\varepsilon)$ polinomnak, és $[\mathbb{Q}(\varepsilon) : \mathbb{Q}] \leq n-1$, mert $m_{\mathbb{Q}}(\varepsilon)$ osztja az $X^{n-1} + X^{n-2} + \cdots + 1$ polinomot, és így $[\mathbb{Q}(\sqrt[n]{a}, \varepsilon) : \mathbb{Q}] \leq n(n-1)$.

5.44. feladat. Legyen az $f = X^n - a \in K[x]$, ahol K egy 0-karakterisztikájú test. Feltételezzük hogy K tartalmazza az n-edrendű egységgyököket. Igazoljuk, hogy $G(f/\mathbb{Q})$ ciklikus csoport és $|G(f/\mathbb{Q})| \mid n$.

Megoldás. Legyen u f-nek egy gyöke és ε egy primitív n-edik egységgyök (Feltételezhetjük, hogy $K \leq \mathbb{C}$ és $\varepsilon = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$). Ekkor az $u, \varepsilon u, \varepsilon^2 u, \ldots, \varepsilon^{n-1}u$ gyökei f-nek, így az f polinom $\mathbb{Q}$ feletti felbontási teste $F_{f,\mathbb{Q}} = K(u, \varepsilon u, \varepsilon^2 u, \ldots, \varepsilon^{n-1}u) = K(u)$. Mivel minden $\varphi \in \mathrm{Aut}_K(F)$ esetén $\varphi(u)$ is gyöke f-nek, $\varphi(u) = u\varepsilon^{k(\varphi)}$, ahol $0 \leq k(\varphi) \leq n-1$. Mivel $F = K(u)$ következik, hogy $k(\varphi)$ meghatározza φ-t.

Legyen $(U_n, \cdot)$ az n-edrendű egységyökök csoportja. Tudjuk, hogy $U_n = \langle\varepsilon\rangle$ ciklikus. Legyen $\phi : G(F/K) \to U_n$, $\phi(\varphi) = \varepsilon^{k(\varphi)}$. ϕ csoportmorfizmus mert $\phi(\varphi_1 \circ \varphi_2) = \varepsilon^{k(\varphi_1 \circ \varphi_2)} = \varepsilon^{k(\varphi_1)} \cdot \varepsilon^{k(\varphi_2)} = \phi(\varphi_1)\phi(\varphi_2)$. ϕ injektív, mert $k(\varphi)$ meghatározza φ-t. Akkor $G(F/K) \cong \mathrm{Im}\,\phi \subseteq U_n$, de $\mathrm{Im}\,\phi$ mint ciklikus csoport részcsoportja ciklikus, tehát $G(F/K)$ is ciklikus, és mivel $|U_n| = n$ következik, hogy $|G(F/K)| \mid n$.

5.45. feladat. Legyen $f = X^n - 1 \in K[X]$. Igazoljuk, hogy $G(F/K)$ Abel-csoport.

Megoldás. $F_{f/K} = K(1, \varepsilon, \varepsilon^2, \ldots, \varepsilon^{n-1}) = K(\varepsilon)$, ahol ε primitív n-edik egységgyök. Legyen $\varphi \in G(K(\varepsilon)/K)$; akkor $\varphi(\varepsilon)$ gyöke az $f = X^n - 1$ polinomnak, tehát $\varphi(\varepsilon) = \varepsilon^{k(\varphi)}$, ahol $0 \leq k(\varphi) \leq n-1$.

Legyen $\varphi, \varphi' \in G(K(\varepsilon)/K)$ a Galois-csoport két eleme. Felhasználva, hogy φ és φ' morfizmusok, egyszerű számolással kapjuk, hogy $(\varphi' \circ \varphi)(\varepsilon) = \varphi'(\varphi(\varepsilon)) = \varphi'(\varepsilon^{k(\varphi)}) = (\varepsilon^{k(\varphi)})^{k(\varphi')} = \varepsilon^{k(\varphi)k(\varphi')} = (\varepsilon^{k(\varphi')})^{k(\varphi)} = (\varphi'(\varepsilon))^{k(\varphi)} = \varphi(\varphi'(\varepsilon)) = (\varphi \circ \varphi')(\varepsilon)$. Tehát $\varphi' \circ \varphi = \varphi \circ \varphi'$.

5.9. A Galois-elmélet alaptétele

Legyen K/k egy bővítés, $G = G(K/k)$ és legyen

$$K^H = \{x \in K \mid \sigma(x) = x,\ \forall\sigma \in H\}$$

a $H \leq G$ részcsoport invariansainak a halmaza.

5.9.1. lemma. 1) $k \leqslant K^H \leqslant K$.
2) *Ha* $H_1 \subseteq H_2$ *akkor* $K^{H_1} \supseteq K^{H_2}$.

Bizonyítás. 1) Legyen $x \in k$ és $\sigma \in G$ tetszőleges. Ekkor $\sigma(x) = x$. Mivel $H \leqslant G$ és $x \in k \leqslant K$, tetszőleges $\sigma \in H$-ra $\sigma(x) = x$, ami azt jelenti, hogy $x \in K^H$, tehát $k \subseteq K^H$. A $K^H \subseteq K$ állítás evidens.

Mivel $k \leqslant K^H$, következik, hogy $\left|K^H\right| \geqslant 2$ és legyen $x, y \in K^H$. Ekkor $\sigma(x-y) = \sigma(x) - \sigma(y) = x - y$ azaz $x - y \in K^H$; $\sigma(xy^{-1}) = \sigma(x)\sigma(y^{-1}) = xy^{-1}$ azaz $xy^{-1} \in K^H$, tehát K^H részteste K-nak.

2) Legyen $x \in K^{H_2}$ és $\sigma \in H_1$; mivel $H_1 \subseteq H_2$, $\sigma(x) = x$, tehát az értelmezés szerint $x \in K^{H_1}$. ■

5.9.2. tétel. *Legyen* $k \leqslant L \leqslant K$.
1) $G(K/L) \leqslant (G, \circ)$, *ahol* $G = G(K, k)$.
2) *ha* $k \leqslant L_1 \leqslant L_2 \leqslant K$, *akkor* $G(K/L_1) \supseteq G(K/L_2)$.

Bizonyítás. 1) Legyen σ és ψ két tetszőleges automorfizmus $G(K/L)$-ből és $x \in L$ tetszőleges elem. Ekkor $(\sigma \circ \psi)(x) = \sigma(\psi(x)) = \sigma(x) = x$, tehát $\sigma \circ \psi \in G(K/L)$. Legyen $\sigma \in G(K/L)$ és $x \in L$ tetszőleges, tehát $\sigma(x) = x$; akkor $x = 1_K(x) = (\sigma^{-1} \circ \sigma)(x) = \sigma^{-1}(\sigma(x)) = \sigma^{-1}(x)$, tehát $\sigma^{-1} \in G(K/L)$.

2) Legyen $\sigma \in G(K/L_2)$. Ez azt jelenti, hogy $\forall x \in L_2$-re $\sigma(x) = x$. Mivel $L_1 \subseteq L_2$, akkor $\forall x \in L_1$-re is igaz, hogy $\sigma(x) = x$, ami ekvivalens azzal, hogy $\sigma \in G(K/L_1)$. ■

Az olyan L testeket, amelyikre $k \subseteq L \subseteq K$, közbülső testnek hívjuk. A következő alaptétel a közbülső testek és $G(K/k)$ részcsoportjai között állapít meg egy egyételmű megfeleltetést.

5.9.3. tétel (A Galois-elmélet alaptétele). *Legyen* K/k *Galois-bővítés,* $G = G(K/k)$ *és* $\mathcal{K} = \{L \mid k \leqslant L \leqslant K\}$ *a közbülső testek hálója. Legyen*

$$\Phi : \mathcal{S}(G) \to \mathcal{K}, \qquad \Phi(H) = K^H,$$

$$\Psi : \mathcal{K} \to \mathcal{S}(G), \qquad \Psi(L) = G(K/L).$$

1) Φ, Ψ *hálóantiizomorfizmusok, és* $\Psi = \Phi^{-1}$.

2) *Ha* $k \leqslant L \leqslant K$, *akkor* L/k *normális bővítés* $\Leftrightarrow H = G(K/L) \trianglelefteq G$; *ebben az esetben* $G(L/k) \simeq \frac{G(K/k)}{G(K/L)} = G/H$.

Bizonyítás. 1) Az előző lemmákból tudjuk, hogy Φ, Ψ jól értelemezett, csökkenő függvények.

Igazoljuk, hogy minden $H \leqslant G$ esetén $G(K/K^H) = H$. Vegyük észre, hogy $H \subseteq G(K/K^H)$, mert ha $\sigma \in H$, akkor minden $x \in K^H$ esetén $\sigma(x) = x$, azaz $\sigma \in G(K/K^H)$. Jelöljük $m = |H|$. Ekkor elég igazolni, hogy $|G(K/K^H)| \leq m$. Mivel K/K^H Galois-bővítés, $\left|G(K/K^H)\right| = [K : K^H]$ és létezik $x \in K$ úgy, hogy $K = K^H(x)$. Legyen

$$g := \prod_{\sigma \in H} (X - \sigma(x)) = (X - \sigma_1(x))(X - \sigma_2(x)) \dots (X - \sigma_m(x)),$$

ahol $H = \{\sigma_1, \dots, \sigma_m\}$; következik, hogy $g = X^m + \beta_{m-1}X^{m-1} + \dots + \beta_1 X + \beta_0$, ahol $\beta_i \in K$. A Viète képleteiből következik, hogy minden $\sigma \in H$ esetén $\sigma(\beta_i) = \beta_i$, tehát $g \in K^H[X]$. (Például: $-\beta_{n-1} = \sigma_1(x) + \dots + \sigma_n(x) \Longrightarrow -\sigma(\beta_{n-1}) = \sigma_1(x) + \dots + \sigma_n(x)$.) Tehát $[K : K^H] = \deg m_{K^H,x} \leqslant m$, vagyis $\left|G(K/K^H)\right| \leqslant m$, amit igazolni akartunk.

Igazoljuk, hogy minden L, $k \leqslant L \leqslant K$ esetén $K^{G(K/L)} = L$. Vegyük észre, hogy $L \subseteq K^{G(K/L)}$, mert minden $x \in L$ és minden $\sigma \in G(K/L)$ esetén $\sigma(x) = x$, és ekkor $k \leqslant L \leqslant K^{G(K/L)} \leqslant K$. Mivel K/L és $K/K^{G(K/L)}$ Galois-bővítések, következik, hogy $[K : L] = |G(K/L)|$ és felhasználva a fentieket,

$$[K : K^{G(K/L)}] = |G(K/K^{G(K/L)})| = |G(K/L)|.$$

Mivel $[K : L] = [G(K/L)][K^{G(K/L)} : L]$, kapjuk, hogy $L = K^{G(K/L)}$.

2) ekvivalens a következő állítással: $H \trianglelefteq G$ *akkor és csak akkor, ha* K^H/k *normális bővítés; ebben az esetben* $G(K^H/k) \simeq G/H$.

Feltételezzük, hogy $H = G(K/K^H) \trianglelefteq G$ és igazoljuk, hogy K^H/k normális bővítés. Legyen $x \in K^H = L$ és legyen x' az x-nek egy konjugáltja. Mivel K/k Galois-bővítés kapjuk, hogy $x' \in K$. Igazoljuk, hogy $x' \in L$, azaz minden $\tau \in H$ esetén $\tau(x') = x'$. Tudjuk, hogy létezik $\sigma' : k(x) \to k(x')$ k-automorfizmus úgy, hogy $\sigma'(x) = x'$. Ekkor létezik $\bar{\sigma} : \bar{k} \to \bar{k}$ k-automorfizmus úgy, hogy $\bar{\sigma}_{|k(x)} = \sigma$. Mivel K/k normális, $\sigma = \bar{\sigma}_{|K} \in \mathrm{Aut}(K)$. Tehát létezik $\sigma \in G(K/k)$ úgy, hogy $\sigma(x) = x'$. Mivel $\sigma H \sigma^{-1} = H$, következik, hogy $H = \{\sigma\tau\sigma^{-1} \mid \tau \in H\}$, és egy tetszőleges $\tau \in H$ elemre $(\sigma\tau\sigma^{-1})(x') = \sigma(\tau(\sigma^{-1}(x'))) = \sigma(\tau(x)) = \sigma(x) = x'$, azaz $x' \in L$.

Fordítva, feltételezzük, hogy $k \leq L = K^H$ normális, és igazoljuk, hogy $G(K/L) = H \trianglelefteq G$. Legyen $\sigma \in G = G(K/k)$; mivel L/k normális, $\sigma_{|L} \in \mathrm{Aut}(L)$. Ekkor $\varphi : G(K/k) \to G(L/k)$, $\varphi(\sigma) = \sigma_{|L}$ csoportmorfizmus, és

$$\mathrm{Ker}\,\varphi = \{\sigma \in G \mid \sigma_{|L} = 1_L\} = \{\sigma \in G \mid \sigma(x) = x,\ \forall x \in L\} = G(K/L).$$

Tehát $G(K/L) \trianglelefteq G$. Igazoljuk, hogy φ szürjektív. Legyen $\tau \in G(L/k)$ azaz $\tau : L \to L$ egy k-automorfizmus; ekkor létezik $\bar{\tau} : \bar{L} \to \bar{L}$ automorfizmus úgy, hogy $\bar{\tau}_{|L} = \tau$. Mivel K/k normális, $\sigma := \bar{\tau}_{|K} : K \to K$ esetén $\sigma \in G(K/k)$. Ekkor $\varphi(\sigma) = \sigma_{|L} = \bar{\tau}_{|L} = \tau$, tehát φ szürjektív. Az 1. izomorfizmus tételből következik, hogy $\frac{G(K/k)}{G(K/L)} \simeq G(L/k)$. ■

5.9.4. tétel. *Tekintsük* $k \leq K_1 \leq L$ *és* $k \leq K_2 \leq L$ *testbővítéseket, és feltételezzük, hogy* $k \leq K_1$ *Galois-bővítés. Legyen* $G_1 := G(K_1/k)$, $G_2 := G(K_2/k)$ *és* $G := G(K_1K_2/k)$.

1) *Ekkor a* $K_2 \subseteq K_1K_2$ *bővítés is Galois, a* $G(K_1K_2/K_2)$ *csoport pedig izomorf a* $G_1 = G(K_1/k)$ *csoport egy részcsoportjával.*

2) *Ha* $K_1 \cap K_2 = k$, *akkor* $G(K_1K_2/K_2) \simeq G_1 = G(K_1/k)$.

3) *Ha* K_2/k *normális bővítés, akkor* K_1K_2 *normális bővítése* k*-nak, és ha* $K_1 \cap K_2 = k$, *akkor*

$$G(K_1K_2/k) \simeq G_1 \times G_2.$$

Bizonyítás. 1) A K_1 test egy $f \in k[X]$ széparábilis polinom felbontási teste. Tehát ha $x_1, \dots, x_r$ az f különböző gyökei, akkor $K_1 = K(x_1, \dots, x_r)$, ami mivel a hipotézis szerint $K_1 \bigcup K_2$ generálja K_1K_2-t, implikálja azt, hogy $K_1K_2 = K_2(x_1, \dots, x_r)$.

Tehát K_1K_2 az f polinom K_2 feletti felbontási teste és innen következik, hogy a $K_2 \subseteq K_1K_2$ bővítés véges, normális és szeparábilis.

Ha $\sigma \in G(K_1K_2/K_2)$, akkor onnan, hogy $K \subseteq K_2$ következik, hogy $\sigma(a) = a$ minden $a \in K$-ra. Továbbá $\sigma(\{x_1, \dots, x_r\}) = \{x_1, \dots, x_r\}$. Ez azt mutatja, hogy $\sigma(K_1) = K_1$ és értelmezhetjük a $\sigma_{|K_1} : K_1 \to K_1$ k-automorfizmust. A

$$\rho : G(K_1K_2/K_2) \to G(K_1/k), \qquad \sigma \to \sigma_{|K_1}$$

leképezés morfizmus.

Mivel σ az $x_1, \dots, x_n$-re való leszükítése által meghatározott, következik, hogy ρ injektív. Valóban, ha $\sigma \in \operatorname{Ker}\rho$, akkor $u_{|K_1} = 1_{K_1}$, vagyis $\sigma(x) = x$ bármely $x \in K_1$ esetén. Legyen $z \in K_1K_2$ tetszőleges elem. Akkor $z = \frac{\sum_{i=1}^m z_i y_i}{\sum_{j=1}^n z'_j y'_j}$, ahol $z_i,\ z'_j \in K_1$ és $y_i,\ y'_j \in K_2$. Mivel $\sigma \in G(K_1K_2/K_2)$ következik, hogy σ K_2-morfizmus. Tehát $\sigma(z) = z$, bármely $z \in K_1K_2$, és $\sigma = 1_{K_1K_2}$. Következésképpen $\operatorname{Ker}\rho = \{1_{K_1K_2}\}$, tehát ρ injektív.

2) Igazoljuk, hogy ρ szürjektív. Legyen $G'_1 = \operatorname{Im}\rho$. A Galois elmélet alaptételéből $G'_1 = G_1$ akkor és csak akkor ha $K_1^{G'_1} = K_1^{G_1} = k$. Ellenőrizni kell a $K_1^{G'_1} = k$ egyenlőséget. Ha $a \in K_1^{G'}$, akkor $\tau(a) = a$, bármely $\tau \in G'_1$ esetén. Legyen $\sigma \in G(K_1K_2/K_2)$, és legyen $\tau = \rho(\sigma) = \sigma_{|K_1}$. Tehát $\sigma(a) = \tau(a) = a$, bármely $\sigma \in G(K_1K_2/K_2)$, vagyis $a \in (K_1K_2)^{G(K_1K_2/K_2)} = K_2$. Mivel $a \in K_1$, következik, hogy $a \in K_1 \cap K_2 = k$, tehát $K_1^{G'} = k$. Következésképpen $G'_1 = G_1$, tehát ρ szürjektív.

3) Könnyen belátható, hogy K_1K_2 normális bővítése k-nak. Definiáljuk a

$$\rho : G \to G_1 \times G_2, \quad \rho(\sigma) = (\sigma_{|K_1},\ \sigma_{|K_2})$$

leképezést. ρ csoportmorfizmus, és igazoljuk, hogy ρ izomorfizmus.

Igazoljuk először, hogy φ injektív. Legyen $\sigma \in \operatorname{Ker}\rho$. Akkor $(\sigma_{|K_1},\ \sigma_{|K_2}) = (1_{K_1},\ 1_{K_2})$ azaz $\sigma(x) = x$ bármely $x \in K_1$ és $\sigma(y) = y$ bármely $y \in K_2$ esetén. Legyen $z \in K_1K_2$; akkor $z = \frac{\sum_{i=1}^m z_i y_i}{\sum_{j=1}^n z'_j y'_j}$, ahol $z_i,\ z'_j \in K_1$ és $y_i,\ y'_j \in K_2$. Tehát $\sigma(z) = z$; következik, hogy $\sigma = 1_{K_1K_2}$, és ρ injektív.

Igazoljuk, hogy φ szürjektív. Legyen $(\tau_1, \tau_2) = G_1 \times G_2$. Az előző pont alapján τ_1-re létezik $\sigma_1 : K_1K_2 \to K_1K_2$, amely egy K_2-morfizmus úgy, hogy $\sigma_{1|K_1} = \tau_1$. Akkor $\varphi(\sigma_1) = (\tau_1,\ 1_{K_1})$. Hasonlóan τ_2-re létezik $\sigma_2 : K_1K_2 \to K_1K_2$, amely egy K_1-morfizmus úgy, hogy $\sigma_{2|K_2} = \tau_2$, akkor $\rho(\sigma_2) = (1_{K_2}, \tau_2)$. Ha $\sigma = \sigma_1\sigma_2$, akkor $\rho(\sigma) = \rho(\sigma_1\sigma_2) = \rho(\sigma_1)\rho(\sigma_2) = (\tau_1, 1_{K_1})(1_{K_2}, \tau_2) = (\tau_1, \tau_2)$, tehát ρ szürjektív. ■

5.9.5. következmény. *Legyen* k *egy test és* $K_1, K_2, \dots, K_n$ *normális bővítései* k*-nak úgy, hogy*

$$K_i \cap (K_{i-1}K_{i+1} \dots K_n) = k$$

bármely $i = 1, 2, \dots, n$ *esetén. Ha* G_i *az* K_i *bővítés Galois csoportja* k *felett* $(1 \leqslant i \leqslant n)$ *és* G *az* $K_1, K_2, \dots, K_n$ *bővítés Galois csoportja, akkor* $G \simeq G_1 \times G_2 \times \dots \times G_n$.

Bizonyítás. Bizonyítsuk n szerinti indukcióval. Ha $n = 2$, a bizonyítás következik az előző tétel alapján. Mivel $K_n \cap (K_1 \dots K_{n-1}) = k$ az előző tétel alapján $G \simeq G(K_1 \dots K_{n-1}/k) \times G_n$. Az indukció hipotéziséből következik, hogy $G(K_1 \dots K_{n-1}/k) \simeq G_1 \times G_2 \times \dots \times G_{n-1}$, ahonnan kapjuk, hogy $G \simeq G_1 \times G_2 \times \dots \times G_n$. ■

5.9.6. példa. Legyen $p_1, p_2, \dots, p_n$ egymástól különböző prímszámok. Tekintsük az $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, \dots, \sqrt{p_n})$ testet. Ha $K_i = \mathbb{Q}(\sqrt{p_i})$, akkor $K = K_1K_2 \dots K_n$. Könnyen belátható, hogy $K_i \cap K_1 \dots K_{i-1}K_{i+1} \dots K_n) = \mathbb{Q}$, bármely $i = 1, 2, \dots, n$. Jelöljük $G_i = G(K_i/\mathbb{Q})$, tehát $G_i \simeq (\mathbb{Z}_2, +)$. Alkalmazva az előbbi tételt következik, hogy $G(K/\mathbb{Q}) \simeq G_1 \times G_2 \times \dots \times G_n \simeq \mathbb{Z}_2^n$.

5.9.7. tétel. *Legyen* K *egy test,* $G \leqslant \operatorname{Aut}(K)$ *véges részcsoport, és legyen*

$$F = K^G = \{a \in K \mid \sigma(a) = a,\ \forall \sigma \in G\}.$$

Akkor K/F *Galois-bővítés és* $G(K/F) = G$.

Bizonyítás. Legyen $G = \{u_1, \dots, u_n\}$, $x \in K$ tetszőleges, és legyenek $x_1 = x, x_2, \dots x_n$ az $\{u_i(x) \mid i = 1, \dots, n\}$ halmaz különböző elemei. A Viéte képleteiből következik, hogy $f := \prod_{i=1}^r (X - x_r) \in F[X]$. Mivel $f(x) = 0$, következik, hogy x algebrai elem F-felett. Legyen $g := m_{x,F}$. Mivel $x_1, \dots, x_r$ konjugált elemek, következik, hogy $g(x_i) = 0$, $i = 1, \dots, n$, tehát $\deg g \geq r$; de $g \mid f$, tehát $g = f$. Tehát x szeparábilis F felett és K tertalmazza az x összes kunjugáltjait. Mivel x tetszőleges volt, következik, hogy K/F algebrai normális és szeparábilis.

Igazoljuk, hogy K/F véges, pontosabban $[K : F] \leq n$. Feltételezzük, hogy $[K : F] \geq n$ (esetleg végtelen). Legyen $F \leq K' \leq K$ úgy, hogy $n < [K' : F] < \infty$. Akkor K'/F Galois bővítés, tehát létezik $x \in K'$ úgy, hogy $K' = F(x)$. Akkor $n \geq \deg m_{x,F} = [K' : F] > n$, ellentmondás. Kapjuk, hogy K/F Galois bővítés, és a Galois-elmélet alaptételéből következik, hogy $G(K/F) = G$. ■

5.46. feladat. Legyen $f \in \mathbb{Q}[X]$, $K = F_{f,\mathbb{Q}}$, $G = G(K/\mathbb{Q}) = G(f/\mathbb{Q})$. Határozzuk meg K-t, G-t, $\mathcal{S}(G)$-t és, alkalmazva a Galois-elmélet alaptételét, a K résztesteit, a következő esetekben:

a) $f = X^2 - d$ polinom, $d \in \mathbb{Z}$ négyzetmentes szám;
b) $f = X^4 - 3$;
c) $f = (X^2 + 3)(X^2 - 5)$;
d) $f = X^3 + 2$.

Megoldás. a) Legyenek az f gyökei: $x_1 = \sqrt{d}, x_2 = -\sqrt{d}$. Ekkor $K = F_{f/\mathbb{Q}} = \mathbb{Q}(x_1, x_2) = \mathbb{Q}(\sqrt{d})$. A $\sqrt{d}$ -nek $\mathbb{Q}$ feletti minimálpolinomja $m_{\mathbb{Q}}(\sqrt{d}) = x^2 - d \Rightarrow [K : \mathbb{Q}] = 2$, bázis lesz K-ban $\{1, \sqrt{d}\}$ és $K = \{\alpha + \beta\sqrt{d} \mid \alpha, \beta \in \mathbb{Q}\}$.

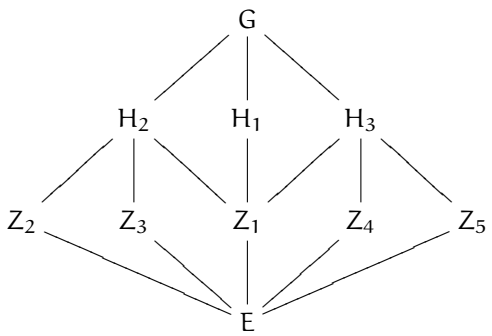
Mivel $K = \mathbb{Q}(\sqrt{d})$, ha $\sigma \in G(K/\mathbb{Q})$ tudjuk, hogy $\sigma(\sqrt{d})$ meghatározza σ-t. Mivel $\sqrt{d}$ gyöke $m_{\mathbb{Q},\sqrt{d}}$-nek $\Rightarrow \sigma(\sqrt{d})$ is gyöke az $X^2 - d$ polinomnak. Akkor $\sigma(\sqrt{d}) = \pm\sqrt{d}$. Legyen $\sigma_1(\sqrt{d}) = \sqrt{d}$ tehát $\sigma_1 = 1_K$ és jelöljük σ_2-t σ-val, ahol $\sigma_2(\sqrt{d}) = -\sqrt{d}$. Tehát $G = \{\sigma_1, \sigma_2\} = \{1_K, \sigma\}$. Mivel $(\sigma \circ \sigma)(\sqrt{d}) = \sigma(-\sqrt{d}) = -(-\sqrt{d}) = \sqrt{d}$, ezért $\sigma^2 = 1_K$.

Akkor $G \simeq (C_2, \cdot) \simeq (\mathbb{Z}_2, +)$ másodrendű ciklikus csoport.

$$\mathcal{S}(G) = \{\{1_K\}, G\} = \mathcal{S}_n(G) = \{H \mid H \trianglelefteq G\} = \{H_1, H_2\}.$$

A $K/\mathbb{Q}$ bővítés két közbülső teste: $K^{H_1} = \{x \in K \mid 1_K(x) = x\} = K$ és $K^{H_2} = \{x \in K \mid 1_K(x) = x, \sigma(x) = x\} = \mathbb{Q}$.

b) Az előző paragrafus **2.** feladatában láttuk, hogy $G = \{\varepsilon, \sigma, \sigma^2, \sigma^3, \tau, \sigma\tau, \sigma^2\tau, \sigma^3\tau\}$. Ennek részcsoport-hálója:



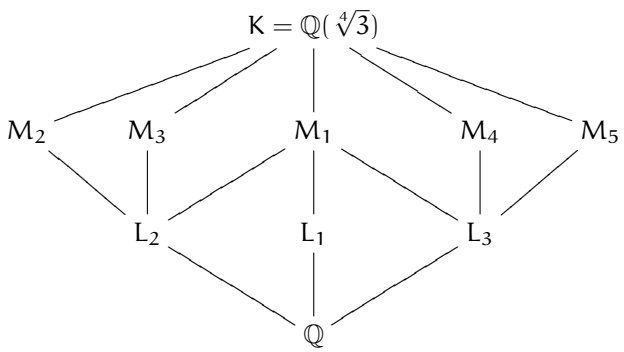
ahol: $H_1 = \{\varepsilon, \sigma, \sigma^2, \sigma^3\}$; $H_2 = \{\varepsilon, \sigma^2, \tau, \sigma^2\tau\}$, $H_3 = \{\varepsilon, \sigma^2, \sigma\tau, \sigma^3\tau\}$; $Z_1 = \{\varepsilon, \sigma^2\}$, $Z_2 = \{\varepsilon, \tau\}$, $Z_3 = \{\varepsilon, \sigma^2\tau\}$, $Z_4 = \{\varepsilon, \sigma\tau\}$, $Z_5 = \{\varepsilon, \sigma^3\tau\}$, $E = \{\varepsilon\}$. A Galois elmélet alaptétele alapján a H csoportnak megfelel K-ban a K^H test. Emlékeztetőül:

$$\begin{array}{ccccccccc} & & \varepsilon & \tau & \sigma^2 & \sigma^2\tau & \sigma & \sigma\tau & \sigma^3 & \sigma^3\tau \\ \sqrt[4]{3} & \to & \sqrt[4]{3} & \sqrt[4]{3} & -\sqrt[4]{3} & -\sqrt[4]{3} & i\sqrt[4]{3} & i\sqrt[4]{3} & -i\sqrt[4]{3} & -i\sqrt[4]{3} \\ i & \to & i & -i & i & -i & i & -i & i & -i \end{array}$$

Az K^{H_1}, K^{H_2} és K^{H_3} testbővítések foka a $\mathbb{Q}$ felett 2, az K^{Z_i}-eké, $i = 1 \ldots 5$ pedig 4.

Mivel ε az identikus megfeleltetés, ez minden elemet fixen hagy. $L_1 = K^{H_1} = \{x \in K | \sigma(x) = x\} = \mathbb{Q}(i)$. $L_2 = K^{H_2} = \{x \in K \mid \sigma^2(x) = x,\ \tau(x) = x\} = \mathbb{Q}(\sqrt{3})$, $L_3 = K^{H_3} = \{x \in K \mid \sigma^2(x) = x,\ \sigma\tau(x) = x\} = \mathbb{Q}(i\sqrt{3})$, $M_1 = K^{Z_1} = \{x \in K \mid \sigma^2(x) = x\} = \mathbb{Q}(i, \sqrt{3})$, $M_2 = K^{Z_2} = \{x \in K \mid \tau(x) = x\} = \mathbb{Q}(\sqrt[4]{3})$, $M_3 = K^{Z_3} = \{x \in K \mid \sigma^2\tau(x) = x\} = \mathbb{Q}(i\sqrt[4]{3})$, $M_4 = K^{Z_4} = \{x \in K \mid \sigma\tau(x) = x\} = \mathbb{Q}(\sqrt[4]{3} + i\sqrt[4]{3})$, $M_5 = K^{Z_5} = \{x \in K \mid \sigma^3\tau(x) = x\} = \mathbb{Q}(\sqrt[4]{3} - i\sqrt[4]{3})$. A G Galois csoportnak a $\mathbb{Q}$ test felel meg, az ε által generált E csoportnak pedig maga az $K = \mathbb{Q}(\sqrt[4]{3}, i)$.

Az $K/\mathbb{Q}$ bővítés közbülső testeinek hálója az előbbivel duálisan izomorf (ugyanaz a diagramm a fejetetejére álllítva):



c) Az f polinomnak négy komplex gyöke van: $\pm i\sqrt{3}$, $\pm\sqrt{5}$. Tehát az f felbontási teste

$$K = \mathbb{Q}(i\sqrt{3}, -i\sqrt{3}, \sqrt{5}, -\sqrt{5}) = \mathbb{Q}(i\sqrt{3}, \sqrt{5}).$$

Vizsgáljuk az $K/\mathbb{Q}$ bővítés automorfizmusainak hatását az $i\sqrt{3}$ és $\sqrt{5}$ elemekre:

$$\begin{array}{ccccc} & \varepsilon & \sigma & \tau & \sigma\tau \\ i\sqrt{3} \to & i\sqrt{3} & -i\sqrt{3} & i\sqrt{3} & -i\sqrt{3} \\ \sqrt{5} \to & \sqrt{5} & \sqrt{5} & -\sqrt{5} & -\sqrt{5} \end{array}$$

Tehát $\sigma^2 = \varepsilon$ és $\tau^2 = \varepsilon$. A $G = G(K/\mathbb{Q})$ Galois csoport izomorf a Klein féle csoporttal, amelynek három valódi részcsoportja van, így G-nek is három valódi részcsoportja van, a következőek: $H_1 = \{\varepsilon, \sigma\}$; $H_2 = \{\varepsilon, \tau\}$,

$H_3 = \{\varepsilon, \sigma\tau\}$. Jelölje E a csak ε-t tartalmazó részcsoportot. Ekkor a G Galois csoport részcsoport-hálója a következő:

$$\begin{tikzcd}
 & G \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
H_2 \arrow[dr, dash] & H_1 \arrow[d, dash] & H_3 \arrow[dl, dash] \\
 & E &
\end{tikzcd}$$

Meghatározzuk az ezeknek megfelelő L_1, L_2, L_3 résztesteket: $L_1 = K^{H_1} = \{x \in K \mid \sigma(x) = x\} = \mathbb{Q}(\sqrt{5})$, $L_2 = K^{H_2} = \{x \in K \mid \tau(x) = x\} = \mathbb{Q}(i\sqrt{3})$, $L_3 = K^{H_3} = \{x \in K \mid \sigma\tau(x) = x\} = \mathbb{Q}(i\sqrt{15})$, $K^G = \mathbb{Q}$, $K^E = K = \mathbb{Q}(i\sqrt{3}, \sqrt{5})$. Tehát az $K/\mathbb{Q}$ bővítés közbülső testeinek a hálója:

$$\begin{tikzcd}
 & \mathbb{Q}(i\sqrt{3}, \sqrt{5}) \arrow[dl, dash] \arrow[d, dash] \arrow[dr, dash] & \\
L_2 \arrow[dr, dash] & L_1 \arrow[d, dash] & L_3 \arrow[dl, dash] \\
 & \mathbb{Q} &
\end{tikzcd}$$

d) Az f polinomnak három gyöke van a komplex számtest felett: $x_1 = -\sqrt[3]{2}$, $x_2 = -\sqrt[3]{2}\varepsilon_1$, $x_3 = -\sqrt[3]{2}\varepsilon_2$, ahol $\varepsilon_1 = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ és $\varepsilon_2 = \varepsilon_1^2 = -\frac{1}{2} - i\frac{\sqrt{3}}{2}$ Mivel egyik sem racionális szám az f $\mathbb{Q}$ feletti felbontási teste $K = \mathbb{Q}(x_1, x_2, x_3) = \mathbb{Q}(\sqrt[3]{2}, \varepsilon_1)$ A bővítés foka $[K : \mathbb{Q}] = 6$. Tehát az $N/\mathbb{Q}$ Galois csoportjának 6 eleme van. Vizsgáljuk, ezek, hogyan hatnak $\sqrt[3]{2}$ és ε_1 elemekre. A $\sqrt[3]{2}$ elem átmehet $\sqrt[3]{2}$-ba, $\varepsilon_1\sqrt[3]{2}$-ba, vagy $\varepsilon_1^2\sqrt[3]{2}$-ba. Az ε_1-ból ε_1 vagy ε_1^2 lesz. Tehát $G(K/\mathbb{Q})$ a következő morfizmusokat tartalmazza:

$$\begin{array}{ccccccccc}
 & & \varepsilon & \sigma & \tau & \tau\sigma & \tau^2 & \tau^2\sigma \\
\sqrt[3]{2} & \to & \sqrt[3]{2} & \sqrt[3]{2} & \varepsilon_1\sqrt[3]{2} & \varepsilon_1\sqrt[3]{2} & \varepsilon_1^2\sqrt[3]{2} & \varepsilon_1^2\sqrt[3]{2}. \\
\varepsilon_1 & \to & \varepsilon_1 & \varepsilon_1^2 & \varepsilon_1 & \varepsilon_1^2 & \varepsilon_1 & \varepsilon_1^2
\end{array}$$

Tehát $G = G(K/\mathbb{Q}) = \{\varepsilon, \sigma, \tau, \tau^2, \tau\sigma, \tau^2\sigma\}$. Észrevesszük, hogy $G(K/\mathbb{Q})$ izomorf az S_3 szimmetrikus csoporttal, és négy valódi részcsoportja van: $H_1 = \{\varepsilon, \sigma\}$, $H_2 = \{\varepsilon, \tau\sigma\}$, $H_3 = \{\varepsilon, \tau^2\sigma\}$ másodrendű részcsoportok és $H_4 = \{\varepsilon, \tau, \tau^2\}$ harmadrendű részcsoport. Meghatározzuk a bővítés közbülső testeit: $L_1 = K^{H_1} = \mathbb{Q}(\sqrt[3]{2})$, $L_2 = K^{H_2} = \{x \in K \mid \tau\sigma(x) = x\} = \mathbb{Q}(\varepsilon_1^2\sqrt[3]{2})$, $L_3 = K^{H_3} = \{x \in K \mid \tau^2\sigma(x) = x\}$, $\tau^2\sigma(\varepsilon_1\sqrt[3]{2}) = \varepsilon_1^2\varepsilon_1^2\sqrt[3]{2} = \varepsilon_1\sqrt[3]{2}$, $L_3 = \mathbb{Q}(\varepsilon_1\sqrt[3]{2})$. A τ automorfizmus csak ε_1 elemet hagyja fixen, tehát a H_4-nek megfelelő résztest $L_4 = \mathbb{Q}(\varepsilon_1)$.

5.47. feladat. Legyen $f \in K[X]$ egy szeparábilis polinom és $L := F_{f,K}$ az f felbontási teste. Igazoljuk, hogy f akkor és csak akkor irreducibilis, ha $G(f/K)$ tranzitív csoport.

Megoldás. Tegyük fel, hogy $\deg f = n$ és f a K test felett irreducibilis. Ekkor ha $x_1, \dots, x_n$ gyökei f-nek, akkor $x_i \in L \setminus K$ minden $i = 1, \dots, n$ esetén. Legyen $G = G(f/K) = G(L/K)$ az f Galois-csoportja. Minden x_i esetén $m_K(x_i) = \prod_{i=1}^{n}(x - x_i) = f$. Tudjuk, hogy minden i, h esetén létezik $\psi \in G$ úgy hogy $\psi(x_i) = x_j$; következik, hogy $G(f/K)$ tranzitív csoport.

Most bizonyítsuk be a fordított állítást, feltéve, hogy f nem irreducibilis. Akkor léteznek $f_1, \dots, f_k$ irreducibilis polinomok $K[X]$-ben, úgy hogy $f = f_1 \dots f_k$ és $2 \le k \le n$.

Legyen x_1 gyöke f_1-nek és x_2 gyöke f_2-nek. Ekkor $x_1, x_2 \in L \setminus K$, $x_1 \neq x_2$ és $m_{K,x_1} = f_1$ illetve $m_{K,x_2} = f_2$. Tudjuk, hogy minden $\sigma \in G$ automorfizmus esetén $\sigma(x_1)$ az x_1 elem konjugáltja, ezért σ az x_1-et az f_1 gyökeibe viheti csak; mivel x_2 nem gyöke f_1-nek, $G(f/K)$ nem lehet tranzitív, ami ellentmond a feltételeknek. Ezért f irreducibilis.

5.48. feladat. Legyen K egy 0-karakterisztikájú test és $f = X^n + a_1X^{n-1} + \dots + a_n \in K[X]$ szeparábilis polinom. Igazoljuk, hogy az f diszkriminánsa egy K-beli elem négyzete akkor és csak akkor ha $G(f/K) \le A_n$.

Megoldás. Legyen L az f felbontási teste K felett. Tudjuk, hogy az f diszkriminánsa d^2, ahol $d := \prod_{1 \le i < j \le n}(x_i - x_j) \in L$. A Galois-elmélet alaptétele szerint, d fixen marad a $G(L/K)$ hatása alatt $\Leftrightarrow d \in K$.

Tegyük fel, hogy az f diszkriminánsa egy K-beli elem négyzete, vagyis $d \in K$. Ekkor minden $\alpha \in G(f/K)$ esetén α páros permutációja az $\{x_1, \dots, x_n\}$ halmaznak, azaz $\alpha \in A_n$, mivel ha $\alpha \notin A_n$, akkor d nem fixpont. Kaptuk, hogy $G(f/K) \le A_n$.

Most igazoljuk a fordított állítást. Vegyük észre, hogy az $\{x_1, \dots, x_n\}$ halmaz páros permutációi fixen hadják d-t. Tegyük fel hogy $d \notin K$. Akkor létezik $\sigma \in G(f/K)$ úgy hogy $\sigma(d) \neq d$; ekkor α páratlan permutációt határoz meg a gyökök halmazán, azaz $G \not\le A_n$, ellentmondás. Tehát $d \in K$.

5.10. Gyökképlettel megoldható algebrai egyenletek

Legyen k egy 0 karakterisztikájú test. Ebben a paragrafusban a $\overline{k}$ a k test egy olyan algebrai lezártját jelöli, amely a k minden alábbi algebrai bővítését tartalmazza.

5.10.1. definíció. a) Egy $x \in k$ elemről azt mondjuk, hogy **gyök** a k test felett, ha x egy $X^n - a \in k[X]$ alakú polinomnak a gyöke.

b) A k test **egyszerű gyökökkel való bővítés**ének nevezzük egy $X^n - a \in k[X]$ alakú polinom felbontási testét.

c) A $k \leq L$ algebrai bővítését **gyökökkel való bővítés**nek nevezzük, ha létezik a

$$k = K_0 \subseteq K_1 \subseteq K_2 \subseteq \cdots \subseteq K_s = L$$

résztest sorozat, úgyhogy K_{i+1} egyszerű gyökökkel való bővítése a K_i-nek minden $i = 0, 1, \ldots, s-1$-re.

d) Legyen $f \in k[X]$, $\deg f > 0$. Azt mondjuk, hogy az $f(x) = 0$ egyenlet **gyökképlettel megoldható**, ha létezik egy K gyökökkel való bővítése a k-nak amelyik tartalmazza az f összes gyökét (azaz $F_{f,k} \leq K$).

5.10.2. megjegyzés. 1) Tudjuk, hogy ha b az $X^n - a$ polinom egy gyöke és ξ egy n-edrendű primitív egységgyök, akkor az $X^n - a$ összes gyökei $\xi^i b$ alakúak, $0 \leq i \leq n-1$ és különbözőek. Tehát ha K/k egyszerű gyökökkel való normális bővítés, akkor $K = k(\xi, b)$.

2) Az értelmezésből egyből következik, hogy hogy ha K egy gyökökkel való bővítése a k-nak és L egy gyökökkel való bővítése a K-nak, akkor L egy gyökökkel való bővítése a k-nak, tehát a gyökökkel való bővítés tranzitív és mindig véges bővítés. Mivel a normális bővítések nem tranzitívak, következik, hogy a gyökökkel való bővítések nem feltétlenül normálisak. Így például a $\mathbb{Q}(\sqrt[4]{3})$ gyökökkel való bővítése a $\mathbb{Q}$-nak, de nem normális.

5.10.3. tétel. *Minden L gyökökkel való bővítése a k-nak benne van egy normális gyökökkel való bővítésben.*

Bizonyítás. Legyen

$$k = k_0 \subseteq k_1 \subseteq \cdots \subseteq k_s = L,$$

ahol k_{i+1} egyszerű gyökökkel való bővítése a k_i-nek, $i = 0, 1, \ldots, s-1$. Indukciót alkalmazunk s szerint.

Ha $s = 1$, L egyszerű gyökökkel való bővítés, tehát normális. Legyen $s > 1$. Az indukció hipotéziséből következik, hogy létezik egy K normális gyökökkel való bővítése a k-nak, amely tartalmazza k_{s-1}-et. Viszont $L = k_{s-1}(\xi, b)$, ahol ξ egy n-edrendű primitív egységgyök és b egy $X^n - \beta \in k_{s-1}[X]$ alakú polinom gyöke. Legyen $g \in k[X]$ a β minimálpolinomja k felett és $\beta_1 = \beta, \beta_2, \ldots, \beta_r$ ennek a polinomnak a gyökei. Minden i-re, ahol $1 \leq i \leq r$ legyen α_i az $X^n - \beta_i \in K[X]$ polinom egy gyöke; $i = 1$-re $\alpha_1 = b$. Ekkor

$$L' = K(\xi, \alpha_1, \ldots, \alpha_r)$$

egy normális gyökökkel való bővítése a k-nak, ami tartalmazza L-et. Valóban, abból, hogy $\xi, b \in L'$ következik, hogy L' tartalmazza L-et. Ahhoz, hogy megmutassuk, hogy L' gyökökkel való bővítése a k-nak elegendő igazolni, hogy gyökökkel való bővítése a K-nek. Ez a

$$K = L'_0 \subseteq L'_1 \subseteq \ldots \subseteq L'_r$$

résztest sorozatból következik, ahol $L'_i = K(\xi, \alpha_1, \ldots, \alpha_i)$, $\quad i = 1, 2, \ldots, r$. Még be kell bizonyítanunk, hogy L'/k normális bővítés. Valóban, $L' = Kk(\xi, \alpha_1, \ldots, \alpha_r)$, a K és $k(\xi, \alpha_1, \ldots, \alpha_r)$ testek pedig normális bővítései k-nak, mivel $k(\xi, \alpha_1, \ldots, \alpha_r)$ a $g(X^n)$-nek k felett felbontási teste. ■

5.10.4. tétel. *Legyen k egy 0 karakterisztikájú test és K/k egy véges és normális bővítés. A K test akkor és csakis akkor beágyazható egy K'/k gyökökkel való bővítésbe, ha a $G(K/k)$ Galois csoportja feloldható.*

Bizonítás. Feltételezzük hogy létezik egy K' gyökökkel való bővítése a k-nak, amely tartalmazza a K-t. Az 5.10.3. tételnek megfelelően feltételezhetjük, hogy K' normális is.

Mivel a $G(K/k)$ csoport faktorcsoportja a $G(K'/k)$ csoportnak, elegendő megmutatni, hogy $G(K'/k)$ feloldható csoport. Legyen

$$K' = K'_0 \supseteq K'_1 \supseteq \ldots \supseteq K'_n = k$$

ahol K'_{i-1} egyszerű gyökökkel való bővítése a K'_i-nek, $i = 1, 2, \ldots, n$ és $G_i = G(K'/K'_i)$. Így kapjuk az

$$\{e\} = G_0 \subseteq G_1 \subseteq \ldots \subseteq G_n = G(K'/k)$$

sorozatot.

Mivel K'_{i-1} egyszerű gyökökkel való bővítése a K'_i-nek, következik, hogy normális bővítés is, a Galois elmélet alaptételéből pedig kapjuk, hogy G_{i-1} normális részcsoportja G_i-nek és, hogy

$$G_i/G_{i-1} \simeq G(K'_{i-1}/K'_i).$$

Felhasználva azt az állítást, hogy ha egy csoportnak van egy normális, véges részcsoport lánca, amelynek a faktorai feloldható csoportok, akkor maga a csoport is felolható, elegendő igazolni, hogy egy egyszerű gyökökkel való bővítés Galois csoportja feloldható.

Legyen tehát $L = k(\xi, b)$ egy egyszerű gyökökkel való bővítése a k-nak, ahol b az $X^n - a \in k[X]$ polinom egy gyöke, a ξ pedig n-edrendű primitív egységgyök. Tekintsük az $L \geq k(\xi) \geq k$ bővítéseket. Észrevesszük, hogy a $k \leq k(\xi)$ és $k(\xi) \leq L$ bővítések normálisak.

A fenti érveléssel elegendő kimutatni, hogy $G(L/k(\xi))$ és $G(k(\xi)/k)$ feloldható csoportok. Észrevesszük, hogy $G(L/k(\xi))$ izomorf a $(\mathbb{Z}_n, +)$ csoportnak egy részcsoportjával, mivel az L azon automorfizmusai, amelyek a $k(\xi)$ elemeit fixen hagyják, avval a tulajdonsággal rendelkeznek, hogy a b képe egy $\xi^s b$ elem ahol s egész szám és $0 \leq s \leq n-1$. A második csoport izomorf az $(U(\mathbb{Z}_n), \cdot)$ csoportnak egy részcsoportjával, mert a $k(\xi)$ bármely k feletti automorfizmusa egy n-edrendű primitív gyököt, n-edrendű primitív gyökbe visz át. Ezek a csoportok Abel-csoportok és feloldhatóak.

Fordítva, feltételezzük, hogy $G := G(K/k)$ Galois csoport feloldható. Tudjuk azt, hogy egy G csoport véges és feloldhatósága egyenértékű avval, hogy van egy ciklikus faktorokból álló normális lánca. Legyen

$$G = G_s \supseteq G_{s-1} \supseteq \cdots \supseteq G_0 = \{e\}$$

G-nek egy normális lánca ciklikus csoport faktorokkal és legyen $K_i = K^{G_i}$, $i = 0, 1, \ldots, s$. Innen kapjuk a

$$K = K_0 \supseteq K_1 \supseteq \cdots \supseteq K_s = k$$

testbővítés sorozatot. A Galois elmélet alaptételéből következik, hogy K_{i-1}/K_i normális bővítés, és

$$G(K_{i-1}/K_i) \simeq G_i/G_{i-1}.$$

Annak kimutatásához, hogy a K test be van ágyazva egy gyökökkel való bővítésébe a k-nak elegendő, hogy a fenti állítást bebizonyítsuk abban az esetben, ha a $G(K/k)$ Galois csoport ciklikus. Valóban, a fent értelmezett s szerinti indukciót alkalmazva, feltételezzük, hogy az állítás igaz $s-1$-re. Ekkor létezik egy L gyökökkel való bővítés, amely tartalmazza a K_1-et. Ha kimutattuk, hogy a KL test benne van a L-nek egy gyökökkel való bővítésében, akkor bebizonyítottuk az állítást K-ra. Tudjuk, hogy a KL test normális bővítése L-nek. Másrészt a $G(KL/L)$ csoport részcsoportja a $G(K/K_1)$ csoportnak és $G(K/K_1) \simeq G/G_{s-1}$, tehát $G(KL/L)$ ciklikus csoport.

Felételezhetjük tehát, hogy $G(K/k)$ ciklikus csoport. Legyen $m = [K : k] = |G(K/k)|$, ε egy primitív m-edrendű egységgyök és $L := K(\varepsilon)$. Észrevesszük, hogy L/k normális bővítés. Elegendő kimutatni, hogy L gyökökkel való bővítése $k(\varepsilon)$-nak, így tehát a k-nak is. Tudjuk, hogy $G(L/k(\varepsilon)) \subseteq G(K/k)$. Tehát $G(L/k(\varepsilon))$ n-edrendű ciklikus csoport, ahol n osztója m-nek. Az állítást a következő lemmaból következik.

5.10.5. lemma. *Ha $k \leq K$ egy n-edfokú normális testbővítés, amelynek a Galois csoportja ciklikus és a k test tartalmazza az n-edrendű egységgyököket, akkor K/k egyszerű gyökökkel való bővítés.*

Valóban, legyen σ a $G := G(K/k)$ csoport egy generátora, ξ egy n-edrendű primitív egységgyök és $x \in K$. Jelölje

$$(\xi^q, x) = \sum_{i=0}^{n-1} \xi^{qi}\sigma^i(x).$$

Az $(\xi^q, x) \in K$ elemet az x elem **Lagrange-féle rezolvens**ének nevezzük.

Észrevesszük, hogy ha $(\xi, x) \neq 0$, akkor következik, hogy $k(x) = K$. Valóban legyen $H := G(K/k(x))$ és $d := [G : H]$. Ha $k(x) \neq K$ kapjuk, hogy $d \neq n$ és $n = dm$. Ekkor $\sigma^d \in H$ és

$$\begin{aligned}(\xi, x) &= \sum_{i=0}^{n-1} \xi^i\sigma^i(x) = \sum_{i=0}^{m-1}\sum_{j=0}^{d-1} \xi^{id+j}\sigma^{id+j}(x) = \\ &= \sum_{i=0}^{m-1}\sum_{j=0}^{d-1} \xi^{id+j}\sigma^j(x) = \sum_{j=0}^{d-1} \sigma^j(x)\xi^j \sum_{i=0}^{m-1} \xi^{id} = \\ &= \sum_{j=0}^{d-1} \sigma^j(x)\xi^j \frac{1-\xi^n}{1-\xi^d} = 0,\end{aligned}$$

ami ellentmond a hipotézisnek.

Bebizonyítjuk, hogy létezik $x \in K$ elem, avval a tulajdonsággal, hogy $(\xi, x) \neq 0$. Valóban legyen a egy primitív eleme a K-nak, tehát $K = k(a)$. Létezik egy r egész szám, $1 \leq r \leq n$, úgy, hogy $(\xi, a^r) \neq 0$, mert ellenkező esetben a következő lineáris egyenletrendszert kapjuk:

$$\sum_{i=0}^{n-1} \xi^i \sigma^i(a^j) = 0, \qquad j = 1, 2, \ldots, n,$$

amiből következne, hogy $\xi^i = 0$, $i = 0, 1, \ldots, n-1$, mivel $\det(\sigma^i(a^i)) \neq 0$ (ez a $\sigma^0(a), \ldots, \sigma^{n-1}(a)$ egymástól különböző elemek Vandermonde-determinánsa).

Legyen most $b \in K$ úgyhogy $(\xi, b) \neq 0$ és $k(b) = K$. Bármely q egész számra, $0 \leq q \leq n-1$ kapjuk, hogy

$$\sigma(\xi^q, b) = \sum_{i=0}^{n-1} \xi^{qi} \sigma^{i+1}(b) = \xi^{-q} \sum_{i=1}^{n} \xi^{qi} \sigma^i(b) = \xi^{-q}(\xi^q, b), \tag{5.4}$$

ahonnan sajátos esetben kapjuk, hogy

$$\sigma(\xi, b) = \xi^{-1}(\xi, b) \tag{5.5}$$

és tehát

$$\sigma((\xi, b)^q) = \xi^{-q}(\xi, b)^q. \tag{5.6}$$

Az (1) és (3)-ból levezethetjük, hogy

$$\sigma\Big(\frac{(\xi^q, b)}{(\xi, b)^q}\Big) = \frac{(\xi^q, b)}{(\xi, b)^q} = c(q) \tag{5.7}$$

ahonnan következik, hogy $c(q) \in k$. Legyen $\overline{b} = (\xi, b)$. Akkor (5.7)-ből következik, hogy $(\xi^q, b) \in k(\overline{b})$, minden $q = 0, 1, \ldots, n-1$ esetén. Tudjuk ugyanakkor, hogy:

$$\sum_{q=0}^{n-1} (\xi^q, b) = \sum_{q=0}^{n-1} \sum_{i=0}^{n-1} \xi^{qi} \sigma^i(b) = \sum_{i=0}^{n-1} \sigma^i(b) \sum_{q=0}^{n-1} \xi^{qi} =$$
$$= nb + \sum_{i=1}^{n-1} \sigma^i(b) \frac{1 - \xi^{in}}{1 - \xi^i} = nb$$

ahonnan kapjuk, hogy $b \in k(\overline{b})$ tehát $k(\overline{b}) = k(b) = K$. Az (5.5) összefüggésből levezethető, hogy $\sigma(\overline{b}^n) = \overline{b}^n$, vagyis $\overline{b}^n \in k$. Tehát $\overline{b}$ gyöke az $X^n - \overline{b}^n \in k[X]$ polinomnak. ■

5.10.6. következmény. *Legyen k egy 0 karakterisztikájú test és $f \in k[X]$, $\deg f > 0$. Az $f(x) = 0$ egyenlet akkor és csak akkor oldható meg gyökképlettel, ha az f Galois csoportja feloldható.*

5.49. feladat. Bizonyítsuk be, hogy az $x(x^2-4)(x^2+2) = 2$ egyenlet nem oldható meg gyökképlettel a $\mathbb{Q}$ felett.

Megoldás. Legyen $f = X^5 - 2X^3 - 8X - 2$. Az Eisenstein kritérium alapján f polinom irreducibilis $\mathbb{Q}$ felett. $f' = 5X^4 - 6X^2 - 8$; $f'(x) = 0 \Leftrightarrow 5y^2 - 6y - 8 = 0$, ahol $y = x^2$; $y_{1,2} = \frac{3 \pm \sqrt{9+40}}{5}$; $y_1 = 2$ és $y_2 = -\frac{4}{5}$.

Az f'-nek két valós gyöke van: $x_{1,2} = \pm\sqrt{2}$. Vizsgálva f' előjelét és f monotonitását, kapjuk, hogy $f(-\sqrt{2}) = 8\sqrt{2} - 2 > 0$, $f(\sqrt{2}) = -8\sqrt{2} - 2 < 0$.

Tehát az f polinomnak pontosan 3 gyöke van, alkalmazhatjuk az 5.8.6. 1) tételt $p = 5$ esetében, így az f Galois csoportja izomorf S_5-el, ami nem feloldható.

5.11. Geometriai szerkeszthetőség

5.11.1. Körzővel és vonalzóval szerkeszthető komplex számok

Legyen $\mathcal{S}$ egy sík és $S = \{P_1, P_2, \ldots, P_n\}$ véges halmaz $\mathcal{S}$-ből. Rekurzívan meghatározhatók az $S_1, S_2, \ldots, S_n, \ldots$ ponthalmazok. Legyen $S_1 = S$ és feltételezzük, hogy az S_r halmaz értelmezett. Akkor S_{r+1} egyenlő S_r-el és ehhez hozzájárulnak a következőképpen kapott pontok:

1: két adott vagy már megszerkesztett egyenes, illetve kör metszéspontjának kijelölése;

2: két adott vagy már megszerkesztett át, egyenes húzása;

3: két adott vagy már megszerkesztett pont távolságának körzőbe vétele, és ezzel mint sugárral kör rajzolása egy adott vagy már megszerkesztett pontból, mint középpontból.
A fent említett módon kapunk egy véges, növekvő halmazsorozatot: $S_1 \subseteq \cdots \subseteq S_r \subseteq \ldots$ Jelöljük

$$C(P_1, P_2, \ldots, P_n) = \bigcup_{r \geqslant 1} S_r.$$

Egy P pont amely eleme a $C(P_1, P_2, \ldots, P_n)$ halmaznak, megszerkeszthető a körző és vonalzó segítségével a $P_1, P_2, \ldots, P_n$ pontokból. Ha $S = \{P_1\}$, akkor $C(P_1) = \{P_1\}$.

Tekintjük a $\mathcal{S}$ síkban az xOy koordináta rendszert, melynek kezdőpontja $O = P_1$, és a P_2 pont koordinátái $(1, 0)$

Tekintsük a $\Theta : \mathcal{S} \to \mathbb{C}$, $\Theta(P) = x + iy$ leképezést, ahol P-nek a koordinátái (x, y), Θ bijektív leképezés. Az $x + iy$ komplex szám affixuma $P(x, y)$. Jelöljük $\Theta(P_i) = \alpha_i$ $(1 \leqslant i \leqslant n)$. Tehát $\alpha_1 = 0$ és $\alpha_2 = 1$. Jelöljük

$$\Theta(C(P_1, P_2, \ldots, P_n)) = C(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Egy $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ komplex szám megszerkeszthető az $\alpha_1, \alpha_2, \ldots, \alpha_n$ számokból a körző és vonalzó segítségével.

5.11.1. tétel. $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *részteste* $\mathbb{C}$*-nek, és rendelkezik a következő tulajdonságokkal:*
1) *Ha* $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$*, akkor* $\bar{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$*;*
2) *Ha* $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$*, akkor* $\sqrt{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$*;*
3) $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ *a legkisebb részteste* $\mathbb{C}$*-nek, amely tartalmazza az* $\alpha_1, \alpha_2, \ldots, \alpha_n$ *komplex számokat és rendelkezik az* 1), 2) *tulajdonságokkal.*

Bizonyítás. Legyen $\alpha, \alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Jelöljük $\Theta(P) = \alpha$ és $\Theta(P') = \alpha'$, ahol $P, P' \in w$. Tehát $P, P' \in C(P_1, P_2, \ldots, P_n)$.

A paralelogramma szabály által kapott Q pontnak megfelel az $\alpha + \alpha'$ komplex szám. Belátható, hogy Q megszerkeszthető a körző és vonalzó segítségével, vagyis $\alpha + \alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Felírjuk α és α'-t trigonometrikus alakban: $\alpha = r(\cos\varphi + i\sin\varphi)$, $\alpha' = r'(\cos\varphi' + i\sin\varphi')$; akkor

$$\alpha\alpha' = rr'[\cos(\varphi + \varphi') + i\sin(\varphi + \varphi')].$$

Mivel $\varphi + \varphi'$ könnyen megszerkeszthető körző és vonalzó segítségével, szerkesszük meg rr'-t is a a körző és vonalzó segítségével. A derékszögű háromszögek hasonlósága alapján kapjuk $\frac{x}{r} = \frac{r'}{1}$, ahonnan $x = rr'$. Belátható, hogy x megszerkeszthető körző és vonalzó segítségével. Tehát $\alpha\alpha' \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Ha $\alpha = r(\cos\varphi + i\sin\varphi) \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, $\alpha \neq 0$, akkor $\alpha^{-1} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Valóban, $\alpha^{-1} = \frac{1}{r}[\cos(-\varphi) + i\sin(-\varphi)]$. Akkor $\frac{x}{1} = \frac{1}{r}$, tehát $x = \frac{1}{r}$. Mivel x megszerkeszthető körzővel és vonalzó segítségével következik, hogy $\alpha^{-1} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Tehát $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ részteste $\mathbb{C}$-nek.

1) Legyen $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Azonnal következik, hogy $\bar{\alpha} \in C(\alpha_1, \ldots, \alpha_n)$.

2) Legyen $\alpha = r(\cos\varphi + i\sin\varphi) \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Akkor

$$\sqrt{\alpha} = \sqrt{r}(\cos\frac{\varphi}{2} + i\sin\frac{\varphi}{2}).$$

Mivel $\sqrt{r}$ és $\dfrac{\varphi}{2}$ megszerkeszthetők körző és vonalzó segítségével, következik, hogy $\sqrt{\alpha} \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

3) Legyen K részteste $\mathbb{C}$-nek, amely tartalmazza $\alpha_1, \alpha_2, \ldots, \alpha_n$-et és rendelkezik az 1), 2) tulajdonságokkal. Mivel $-1 \in K$, az 1) tulajdonságból következik, hogy $i = \sqrt{-1} \in K$. Ha $\alpha = x + iy$, akkor az 1) pontból kapjuk, hogy $\bar{\alpha} = x - iy \in K$; következik, hogy $x, y \in K$. Tehát

$$\alpha = x + iy \in K \Longleftrightarrow x, y \in K.$$

Jelöljük $\mathcal{S}' = \Theta^{-1}(K)$. Igazoljuk, hogy $\mathcal{S}'$ rendelkezik a következő tulajdonságokkal:

1° Két $\mathcal{S}'$-beli pontok által meghatározott egyenes metszéspontja $\mathcal{S}'$-beli pont.

2° Egy $\mathcal{S}'$-beli pontok által meghatározott egyenes és egy $\mathcal{S}'$-beli középpontú, $\mathcal{S}'$-beli pontok által meghatározott sugarú kör metszéspontja $\mathcal{S}'$-beli pont.

3° Két $\mathcal{S}'$-beli pont által meghatározott középpontú, illetve sugarú kör metszéspontja $\mathcal{S}'$ beli pont.

Ellenőrizzük az 1° tulajdonságot. Valóban, az

$$\begin{cases} ax + by + c = 0 \\ a'x + b'y + c' = 0 \end{cases}, \quad a, b, a', b', c, c' \in K$$

egyenletrendszer megoldásai K-beli elemek.

Ellenőrizzük a 2° tulajdonságot. Az 1° tulajdonsághoz hasonlóan

$$\begin{cases} ax + by + c = 0 \\ x^2 + y^2 + mx + ny + p = 0 \end{cases}, \quad a, b, c, m, n, p \in K,$$

egyenletrendszer megoldásai K-beli elemek.

A 3° tulajdonság következik a 2°-ból mivel két kör metszéspontjának meghatározása egyenértékű az egyik kör és a hatványtengely metszéspontjainak meghatározásával.

Mivel $P_1, P_2, \ldots, P_n \in \mathcal{S}'$, az 1°, 2° és 3°-ból következik, hogy $C(P_1, P_2, \ldots P_n) \subseteq \mathcal{S}'$, tehát

$$C(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K,$$

ami azt jelenti, hogy $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ a legkisebb részteste $\mathbb{C}$-nek, amely tartalmazza $\alpha_1, \alpha_2, \ldots, \alpha_n$ számokat és rendelkezik az 1) és 2) tulajdonságokkal. ■

5.11.2. Körzővel és vonalzóval való szerkeszthetőség első kritériuma

Tekintsük az $S = \{P_1, P_2, \ldots, P_n\}$ halmazt a $\mathcal{S}$ síkból, $C(P_1, P_2, \ldots P_n)$ a körzővel és vonalzóval megszerkeszthető pontokhalmaza. Legyen $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ részteste $\mathbb{C}$-nek amely asszociált a $C(P_1, P_2, \ldots, P_n)$ halmazzal. Mivel $\mathbb{Q} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, kapjuk, hogy

$$F := \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Ha $n = 2$, akkor $C(\alpha_1, \alpha_2) = C(0, 1)$ és $F = \mathbb{Q}(\alpha_1, \alpha_2, \bar{\alpha}_1, \bar{\alpha}_2) = \mathbb{Q}$. A $C(0, 1)$ halmazt a körzővel és vonalzóval szerkeszthető komplex számok halmazának nevezzük. Egy komplex szám akkor és csak akkor szerkeszthető, ha a valós és az imaginárius része is szerkeszthető.

5.11.2. tétel (Szerkeszthetőség első kritériuma). *Az α komplex szám szerkeszthető körzővel és vonalzóval az $\alpha_1, \alpha_2, \ldots, \alpha_n$ számokból, akkor és csak akkor, ha léteznek az*

$$F = F_0 \subset F_1 \subset F_2 \subset \ldots \subset F_r$$

véges testbővítések úgy, hogy $\alpha \in F_r$ és $[F_i : F_{i-1}] \leqslant 2$ bármely $1 \leqslant i \leqslant r$ esetén.

Bizonyítás. Jelöljük

$$K := \{\alpha \in \mathbb{C} \mid \exists\, F = F_0 < F_1 < F_2 < \ldots < F_r \text{ bővítések: } \alpha \in F_r,\ [F_i : F_{i-1}] \leqslant 2,\ \forall i\}.$$

Legyen $\alpha, \beta \in K$; léteznek $F = F_0 < F_1 < F_2 < \ldots < F_r$ véges testbővítések, ahol $\alpha \in F_r$ és $[F_i : F_{i-1}] \leqslant 2$, $1 \leqslant i \leqslant r$, illetve $F' = F'_0 < F'_1 < F'_2 < \ldots < F'_r$, ahol $\beta \in F'_r$ és $[F'_j : F'_{j-1}] \leqslant 2$, $(1 \leqslant j \leqslant r')$. Kapjuk a következő tetbővítésekből álló láncot

$$F = F_0 < F_1 < F_2 < \ldots < F_r = F_rF'_0 < F_rF'_1 < \ldots < F_rF'_{r'},$$

ahol $[F_rF'_j : F_rF'_{j-1}] \leqslant 2$, bármely $1 \leqslant j \leqslant r'$. Mivel $\alpha + \beta$, $\alpha\beta \in F_rF'_r$ és $\alpha^{-1} \in F_r$, ha $\alpha \neq 0$ következik, hogy K részteste $\mathbb{C}$-nek. Mivel F zárt a konjugálási műveletre nézve következik, hogy a K test is zárt a konjugálási műveletre nézve. Ha

$$F = F_0 < F_1 < F_2 < \ldots < F_r$$

véges tetbővítésekből álló lánc úgy, hogy $[F_i : F_{i-1}] \leqslant 2$, $(1 \leqslant i \leqslant r)$, akkor F_i zárt a négyzetgyökvonásra nézve. Tehát K zárt a négyzetgyökvonásra nézve műveletre nézve. Mivel $\alpha_1, \alpha_2, \ldots, \alpha_n \in K$, a 11.1. tétel alapján következik, hogy $C(\alpha_1, \alpha_2, \ldots, \alpha_n) \subseteq K$. Legyen $\alpha \in K$ és legyen az

$$F = F_0 < F_1 < F_2 < \ldots < F_r,$$

testbővítésekből álló lánc úgy, hogy $\alpha \in F_r$ és $[F_i : F_{i-1}] \leqslant 2$, bármely $1 \leqslant i \leqslant r$ esetén. Igazoljuk indukcióval, hogy bármely i esetén $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Ha $i = 0$,

$$F_0 = \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n) \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n).$$

Feltételezzük, hogy $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ és igazoljuk, hogy $F_{i+1} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Mivel $[F_{i+1} : F_i] \geqslant 2$, kapjuk, hogy $F_{i+1} = F_i(\beta)$, ahol β algebrai elem F_i felett, β minimál polinomja f, $\deg f \leq 2$. Tehát β gyöke egy másodfokú egyenletnek, melynek együtthatói $F_i \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$-beli elemek. Mivel $C(\alpha_1, \alpha_2, \ldots, \alpha_n)$ rendelkezik a 2) tulajdonsággal, következik, hogy $\beta \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, tehát $F_{i+1} \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. Igazoltuk, hogy $K \subseteq C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, ahonnan $K = C(\alpha_1, \alpha_2, \ldots, \alpha_n)$. ■

5.11.3. következmény. *Ha $\alpha \in C(\alpha_1, \alpha_2, \ldots, \alpha_n)$, akkor az α minimál polinomjának foka az*

$$F := \mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha}_1, \bar{\alpha}_2, \ldots, \bar{\alpha}_n)$$

test felett 2^k alakú.

Bizonyítás. Létezik az $F = F_0 < F_1 < F_2 < \ldots < F_r$, testbővítésekből álló lánc, ahol $\alpha \in F_r$, $[F_i : F_{i-1}] \leq 2$, $1 \leq i \leq r$. Következik, hogy $[F_r : F] = 2^l$, ahol $l > 0$. Mivel $[F_r : F] = [F(\alpha) : F][F_r : F(\alpha)]$, kapjuk, hogy $[F(\alpha) : F] = 2^k$, ahol $l \geqslant 0$. De $[F(\alpha) : F] = \deg m_{\alpha,F}$. Tehát $\deg m_{\alpha,F} = 2^k$. ■

5.11.3. Szögharmadolás

A feladat adott szöget három egyenlő részre osztani. Igazolni fogjuk, hogy nem minden szög osztható fel három egyenlő részre a körző és vonalzó segítségével.

Egy adott φ szöget például a koszinuszával jellemezhetjük, tehát $u = \cos\varphi$ ismeretében akarjuk $x = \cos\frac{\varphi}{3}$-at megszerkeszteni. Mivel

$$\cos\varphi = 4\cos^3\frac{\varphi}{3} - 3\cos\frac{\varphi}{3},$$

ezért x a $4x^3 - 3x - u = 0$ egyenlet gyöke. Legyen

$$f = 4X^3 - 3X - u.$$

Elég igazolni, létezik φ úgy, hogy $u = \cos\varphi \in \mathbb{Q}$ és f irreducibilis $\mathbb{Q}$ felett. Ekkor az $[F_{f,\mathbb{Q}} : \mathbb{Q}]$ fokszáma 3-al osztható, tehát nem lehet 2-hatvány. Következik, hogy, általában, a szögharmadolás nem hajtható végre körzővel és vonalzóval.

Például, legyen $\varphi = 60°$. A $60°$-os szöget meghatározzák a P_1, P_2, P_3 pontok, ahol

$$\alpha_3 = \cos 60° + i\sin 60° = \frac{1}{2} + i\frac{\sqrt{3}}{2}.$$

Ebben az esetben

$$F = \mathbb{Q}(\alpha_1, \alpha_2, \alpha_3, \bar{\alpha}_1, \bar{\alpha}_2, \bar{\alpha}_3) = \mathbb{Q}(i\sqrt{3}).$$

Legyen $\alpha = \cos 20° + i\sin 20°$. A $\cos 3\varphi = 4\cos^3\varphi - 3\cos\varphi$ egyenlőségből $\varphi = 20°$-ra kapjuk, hogy $\frac{1}{2} = 4\cos^3 20° - 3\cos 20°$. Tehát $\cos 20°$ gyöke az

$$f = 4X^3 - 3X - \frac{1}{2} \in \mathbb{Q}[X]$$

irreducibilis polinomnak. Mivel $\deg f = 3$, a $\cos 20°$ minimál polinomának a foka $\mathbb{Q}(i\sqrt{3})$ felett egyenlő 3-al. A 5.11.3. következmény alapján $\cos 20°$ nem eleme a $C(0, 1, i\sqrt{3})$ halmaznak, tehát a $60°$-os szög nem osztható fel három egyenlő részre a körző és a vonalzó segítségével.

5.11.4. A Déloszi probléma (kockakettőzés)

Adott kockához nem szerkeszthető (körző és vonalzó segítségével) olyan kocka, amelynek térfogata az eredeti kocka térfogatának kétszerese. A kocka élét egységnyinek választva a kiindulási test a racionális számok teste. A megszerkesztendő kocka élhossza $\sqrt[3]{2}$. $\sqrt[3]{2}$ az $X^3 - 2$ polinom gyöke. A $\mathbb{Q}$ test felett $X^3 - 2$ irreducibilis, $\sqrt[3]{2}$ tehát $\mathbb{Q}$ felett harmadfokú, a 5.11.3. következmény alapján következik, hogy $\sqrt[3]{2} \notin C(0, 1)$. Tehát a feladat euklideszi szerkesztéssel megoldhatatlan.

5.11.5. Háromszögszerkesztési feladat

Igazolni fogjuk, hogy nem mindíg szerkeszthető körzővel és vonalzóval egy háromszög, amelynek adottak a szögfelezői. Legyenek i_a, i_b, i_c az ABC háromszög szögfelezői, p pedig a háromszög félkerülete. Ismertek a következő kifejezések:

$$i_a = \frac{2p\sin\frac{B}{2}\sin\frac{C}{2}}{\cos\frac{A}{2}\cos\frac{B-C}{2}}, \quad i_b = \frac{2p\sin\frac{C}{2}\sin\frac{A}{2}}{\cos\frac{B}{2}\cos\frac{C-A}{2}}, \quad i_c = \frac{2p\sin\frac{A}{2}\sin\frac{B}{2}}{\cos\frac{C}{2}\cos\frac{A-B}{2}}.$$

Feltételezzük, hogy $i_b = i_c$, tehát $B = C$. Akkor $A + 2B = \pi$,

$$\cos\frac{A}{2} = \sin B, \qquad \sin\frac{A}{2} = \cos B, \qquad \cos\frac{C-A}{2} = \sin\frac{3B}{2}.$$

Következik, hogy

$$k = \frac{i_a}{i_b} = \frac{\sin\frac{3B}{2}}{2\cos B}$$

Jelöljük $\xi = \sin\frac{B}{2}$. Ha kifejezzük a $\sin\frac{3B}{2}$-t és $\cos B$-t a ξ segítségével, kapjuk a következő egyenlőséget:

$$4\xi^3 - 4k\xi^2 - 3\xi + 2k = 0.$$

Választjuk $k = 3$; akkor ξ gyöke az

$$f = 4X^3 - 12X^2 - 3X + 6$$

polinomnak, amely irreducibilis $\mathbb{Q}[X]$-ben. Következik, hogy $\xi \notin C(0,1)$. Tehát nem szerkeszthető a körző és a vonalzó segítségével egy háromszög, amikor ismertek az i_a, i_b szögfelezők, ahol $i_a = 3i_b$.

5.11.6. A kör négyszögesítése

A feladat adott körrel egyenlő területű négyzet szerkesztése. Adottak az $\mathcal{S}$ síkban a következő pontok: P_1-a kör középpontja, P_2-egy pont a körön. Az $\mathcal{S}$ síkban rögzítünk egy koordináta rendszert, úgy, hogy P_1 a koordináta rendszer kezdőpontja, a P_2 koordinátái pedig $(1,0)$. A négyzet oldala legyen $\sqrt{\pi}$. Mint ismeretes, π nem algebrai szám, azaz nem gyöke egyetlen racionális együtthatós polinomnak sem. Tehát π transzcendens a $\mathbb{Q}$ felett, következik, hogy $\sqrt{\pi}$ transzcendens, $\sqrt{\pi} \notin C(0,1)$. Tehát a kör négyszögesí tése körzővel és vonalzóval nem oldható meg.

A kör négyszögesítésének a feladata az úgynevezett quadratrix segítségével már megoldható. A quadratrixot a következő módon határozzuk meg: egy egységnyi sugarú kör sugarát egy rögzített helyzetből kiindulva forgassuk állandó szögsebességgel úgy, hogy egységnyi idő alatt $90°$-al forduljon el. Ezzel egyidőben egységnyi sebességgel toljunk el egy egyenest a sugár kezdőhelyzetéből kiindulva a kezdőhelyzettel párhuzamosan. A mozgó sugár és az egyenes metszéspontja által leírt görbét nevezzük quadratrixnek.

Határozzuk meg a quadratrix polárkoordinátás egyenletét. A kör középpontja legyen a koordináta rendszer kezdőpontja, a sugár kezdeti helyzete a polártengely. t idő múlva a sugár a $\frac{\pi}{2}t$ szöggel fordul el. Ezalatt az egyenes t-vel tolódik el. Ekkor $r \sin \varphi = t$, azaz t-t kiküszöbölve $r = \frac{2/\pi}{\sin \varphi}$. Ha φ-vel tartunk 0-hoz, akkor r $\frac{2}{\pi}$-hez tart. A quadratrix tehát a polártengelytől $\dfrac{2}{\pi}$ hosszúságú szakaszt vág le, és $\frac{2}{\pi}$ birtokában a reciproka $\frac{\pi}{2}$ is szerkeszthető.

5.11.7. Szerkeszthetőség második kritériuma

5.11.4. definíció. A $K \leq E$ testbővítést **pitagorikus**nak nevezzük, ha létezik a

$$K = K_0 < K_1 < K_2 < \ldots < K_r = L$$

testbővítésekből álló lánc úgy, hogy $[K_i : K_{i-1}] \leqslant 2$, bármely $1 \leqslant i \leqslant r$.

Észrevehető, hogy $1 \leqslant i \leqslant r$ esetén K_i egyszerű gyökökkel való bővítése K_{i-1}-nek, és bármely L/K pitagorikus bővítés egy gyökökkel való bővítés.

A 5.10.3. tételhez hasonlóan kapjuk:

5.11.5. tétel. *Ha* L/K *pitagorikus bővítés, akkor létezik egy* F/K *pitagorikus és normális bővítés úgy, hogy* $L \subseteq F$.

5.11.6. tétel. *Legyen* L *normális bővítése a* K *testnek. Akkor* L/K *pitagorikus bővítés akkor és csak akkor, ha* $[L : K]$ *2-nek hatványa.*

Bizonyítás. Feltételezzük, hogy L pitagorikus bővítése K-nak. Létezik a

$$K = K_0 \subset K_1 \subset K_2 \subset \ldots \subset K_r = L$$

testbővítésekből álló lánc, ahol $[K_i : K_{i-1}] \leqslant 2$, bármely $1 \leqslant i \leqslant r$ esetén. Következik, hogy $[L : K] = 2^s$, ahol $s \geq 0$.

Fordítva, feltételezzük, hogy $[E : K] = 2^n$. Jelöljük G-vel a $G(E/K)$ Galois csoportot, melynek rendje $|G| = 2^n$. Jelöljük Z_1-el a G centrumát. Mivel G 2-csoport, $Z_1 \neq \{e\}$. Mivel G/Z_1 is 2-csoport, a centruma Z_2/Z_1 alakú, ahol $Z_2 \leq G$, és tartalmaz legalább két elemet. Így kapjuk G részcsoportjainak egy növekvő láncát:

$$Z_1 \subset Z_2 \subset \ldots \subset Z_{i-1} \subset Z_i \subset \ldots,$$

ahol Z_i/Z_{i-1} centruma a G/Z_{i-1} csoportnak. Mivel G véges csoport és bármely $i \geqslant 1$ esetén Z_i/Z_{i-1} tartalmaz legalább két elemet, létezik egy $r \geqslant 1$ úgy, hogy $G = Z_r$. Mivel Z_i/Z_{i-1} kommutatív és rendje 2-nek hatványa, kapjuk az

$$\{e\} = H_0 \subset H_1 \subset H_2 \subset \ldots \subset H_s = G,$$

láncot úgy, hogy $H_i \trianglelefteq G$, $[H_i : H_{i-1}] = 2$, $1 \leqslant i \leqslant s$. Ha jelöljük $K_i = E^H_{s-i}$, ahol $0 \leqslant i \leqslant s$, kapjuk a

$$K = K_0 < K_1 < \ldots < K_s = L$$

bővítések láncát. A Galois elmélet alaptétele alapján $[K_i : K_{i-1}] = 2$ bármely $1 \leqslant i \leqslant s$ esetén. Tehát L pitagorikus bővítése a K testnek. ■

5.11.7. következmény (Szerkeszthetőség 2. kritériuma). *Tekintsük az $\alpha_1, \alpha_2, \ldots, \alpha_n$ komplex számokat, $n \geq 1$. Az α komplex szám megszerkeszthető a körző és vonalzó segí tségével az $\alpha_1, \alpha_2, \ldots, \alpha_n$ számokból, ha létezik*

$$\mathbb{Q}(\alpha_1, \alpha_2, \ldots, \alpha_n, \bar{\alpha_1}, \bar{\alpha_2}, \ldots, \bar{\alpha_n}) \leq L$$

normális bővítés, amelynek foka 2-nek hatványa, úgy, hogy $\alpha \in L$.

5.11.8. Szabályos n-szög szerkesztése

A feladat a szabályos n-szöget szerkeszteni, azaz egy kört felosztani n egyenlő részre. Adottak az $\mathcal{S}$ síkban a P_1 és P_2 pontok, a kör középpontja illetve egy pont a körön. Az $\mathcal{S}$ síkban rögzítünk egy koordináta rendszert, melynek kezdőpontja legyen a kör középpontja $O = P_1$, a P_2 pont koordinátái pedig $(1, 0)$. Célszerűbb itt a

$$\xi = \cos\frac{2\pi}{n} + i\sin\frac{2\pi}{n}$$

komplex egységgyököt tekinteni, és ennek szerkeszthetőségét vizsgálni. ξ az $x^n - 1 = 0$ egyenlet gyöke. Tehát $\mathbb{Q}(\xi)$ normális bővítése $\mathbb{Q}$-nak mert $\mathbb{Q}(\xi)$ az $X^n - 1 \in \mathbb{Q}[X]$ polinom felbontási teste.

Alkalmazva a szerkeszthetőség második kritériumát, ξ megszerkeszthető a körző és vonalzó segítségével akkor és csak akkor, ha létezik egy $E/\mathbb{Q}$ normál bővítés úgy, hogy $\xi \in L$ és $[L : \mathbb{Q}] = 2^s$. Mivel $\mathbb{Q}(\xi) \subseteq L$, $[\mathbb{Q}(\xi) : \mathbb{Q}] = 2^r$. Tehát ξ szerkeszthető körző és vonalzó segítségével akkor és csak akkor, ha $[\mathbb{Q}(\xi) : \mathbb{Q}]$ 2-nek hatványa.

5.11.8. tétel. *A szabályos n-szög akkor és csak akkor szerkeszthető körző és vonalzó segí tségével, ha*

$$n = 2^s p_1 p_2 \ldots p_r$$

alakú ($s \geqslant 0$, $r \geqslant 0$), ahol p_i páratlan prímszámok úgy, hogy p_{i-1} 2-nek hatványa.

Bizonyítás. A ξ minimál polinomja $\mathbb{Q}$ felett a $\Phi_n = \prod_{(k,n)=1}(X - \xi^k)$ ciklotomikus polinom, amelynek foka $\phi(n)$. Ha $n = 2^s p_1^{n_1} p_2^{n_2} \ldots p_k^{n_k}$, ahol $s \geqslant 0$, $p_1, p_2, \ldots, p_k$ 2-től különböző prí mszámok, akkor

$$\varphi(n) = 2^{a-1} p_1^{n_1-1}(p_1 - 1) \ldots p_k^{n_k-1}(p_k - 1)$$

2-nek hatványa akkor és csak akkor, ha $n_1 = n_2 = \cdots = n_k = 1$ és $p_1 - 1, \ldots, p_k - 1$ 2-nek hatványa. Legyen $p_i - 1 = 2^{m_i}$, $1 \leqslant i \leqslant k$. Ahhoz, hogy p_i prímszám legyen, m_i 2-nek hatványa kell legyen. Valóban, felírhatjuk, hogy $m_i = 2^{t_i} u$, ahol u páratlan szám. Akkor

$$p_i = 2^{m_i} + 1 = \left(2^{2^{t_i}}\right)^u + 1.$$

Mivel u páratlan, $2^{2^{t_i}} + 1$ osztja p-t. Mivel p_i prím, $u = 1$, $m_i = 2^{t_i}$ és $p_i = 2^{2^{t_i}} + 1$. ■

A $p = 2^{2^n} + 1$ alakú prímszámokat **Fermat-prímszám**oknak nevezzük. Megjegyezzük, hogy $n = 1, 2, 3, 4$ esetén $p = 3, 5, 17, 257, 65537$. $n = 5$ esetén Euler igazolta, hogy $2^{32} + 1 = 641 \cdot 6700417$, tehát nem prímszám.

5.11.9. Szabályos ötszög és tízszög szerkesztése

Vizsgáljuk $p = 5$ esetet. Jelöljük l_5 illetve l_{10}-el az ötszög illetve tízszög oldalát és legyen $\varepsilon = \cos\frac{2\pi}{5} + i\sin\frac{2\pi}{5}$ az ötödrendű egységgyök, amelyre $\varepsilon^4 + \varepsilon^3 + \varepsilon^2 + \varepsilon = -1$, ahonnan $\varepsilon^4 = \varepsilon^{-1}$, $\varepsilon^3 = \varepsilon^{-2}t$. Legyen $\varepsilon + \varepsilon^{-1} =: y$, tehát

$$y^2 + y - 1 = 0. \qquad (1)$$

Vegyük ézre, hogy

$$y = \varepsilon + \varepsilon^{-1} = 2\cos\frac{2\pi}{5} = 2\sin\left(\frac{\pi}{2} - \frac{2\pi}{5}\right) = 2\sin\frac{\pi}{10} = l_{10}.$$

Az (1) egyenletnek van két megszerkeszthető gyöke. A pozitív gyöke pontosan a tízszög oldala. A tízszög oldala segítségével könnyen kiszámítható az ötszög oldala, kiindulva az

$$l_{2n} = \sqrt{2 - \sqrt{4 - l_n^2}}$$

összefüggésből. A mi esetünkben $2 - \sqrt{4 - l_5^2} = l_{10}^2$. Következik, hogy

$$l_5^2 = \frac{1}{4}(10 - 2\sqrt{5}) = 1 + l_{10}^2.$$

Ebből következik a szabályos ötszög illetve szabályos tízszög oldalának szerkesztése.

5.50. feladat. Igazoljuk, hogy:

a) A $90°$, $180°$, $\arccos \frac{11}{16}$ szögek harmadolása elvégezhető.

b) Ha $(k, n) = 1$, akkor $[\mathbb{Q}(\cos \frac{2k\pi}{n} : \mathbb{Q}] = \frac{\phi(n)}{2}$.

c) A $\frac{2\pi}{n}$ szög harmadolása lehetséges $\iff \phi(3n) = 2^k$, ahol $k \geq 1$.

d) Az $n°$ szög szerkeszthető $\iff 3 \mid n$.

5.51. feladat. Megszerkeszthető-e az 1 térfogatú szabályos tetraéder élének hosszúsága?

5.52. feladat. Megszerkeszthető-e az egyenlő szárú háromszög, ha adott a szára és a beirt kör sugara?

5.53. feladat. Megszerkeszthető-e az a háromszög, ha adott két oldala és az egyik oldallal szemközti szög felezőjének a hossza?

6. fejezet

Elemi és algebrai számelmélet

6.1. Oszthatósag $\mathbb{Z}$-ben

Jelölje $(\mathbb{Z}, +, \cdot)$ az egész számok gyűrűjét. Tudjuk, hogy $\mathbb{Z}$ integritástartomány.

Minden $x \in \mathbb{R}$ esetén $x = n + \varepsilon$ egyértelműen úgy, hogy $n \in \mathbb{Z}$, $\varepsilon \in [0, 1)$. Jelölés: $n = [x]$ az x **egészrésze**, $\varepsilon = \{x\}$ az x **törtrésze**. Evidens, hogy $\{x\} = x - [x] \in [0, 1)$, és $[x] \leq x < [x] + 1$.

6.1.1. Maradékos osztás

6.1.1. tétel (Maradékos osztás tétele, 1. változat). *Legyen* $a, n \in \mathbb{Z}$, $n \neq 0$. *Akkor létezik egyetlen* $q, r \in \mathbb{Z}$ *úgy, hogy*

$$a = nq + r, \quad 0 \leq r < |n|, \quad q = \left[\frac{a}{n}\right] \in \mathbb{Z}, \quad r = n\left\{\frac{a}{n}\right\}.$$

Azt mondjuk, hogy r a **legkisebb pozitív maradék**.

6.1.2. következmény (Maradékos osztás tétele, 2. változat). *Legyen* $a, n \in \mathbb{Z}$, $n \neq 0$. *Akkor létezik egyetlen* $q, r \in \mathbb{Z}$ *úgy, hogy*

$$a = nq + r, \quad -\frac{|n|}{2} < r \leq \frac{|n|}{2}.$$

Mi több, $r \geq 0 \Leftrightarrow \left\{\frac{a}{n}\right\} \leq \frac{1}{2}$, *és* $r < 0 \Leftrightarrow \left\{\frac{a}{n}\right\} > \frac{1}{2}$.

Azt mondjuk, hogy r az **legkisebb abszolútértékű maradék**. Például, ha $n \geq 3$ páratlan szám, akkor a maradékok $0, \pm 1, \pm 2, \ldots, \pm\frac{n-1}{2}$; ha $n \geq 2$ páros szám, akkor a maradékok $0, \pm 1, \pm 2, \ldots, \pm(\frac{n}{2} - 1), \frac{n}{2}$.

6.1. feladat. Mutassuk meg, hogy
a) minden egész szám négyzete vagy $3k$ alakú vagy $3k + 1$ alakú;
b) minden egész szám négyzete vagy $5k$ vagy $5k + 1$ vagy $5k - 1$ alakú;
c) minden egész szám négyzete vagy $7k$ vagy $7k + 1$ vagy $7k - 1$ alakú.

6.2. feladat. Határozzuk meg az $1! + 2! + \cdots + n!$ szám utolsó két számjegyét, ahol $n \in \mathbb{N}^*$.

6.1.3. következmény (a alapú számrendszer). *Legyen* $a \in \mathbb{N}$, $a > 1$. *Akkor minden* $n \in \mathbb{N}^*$ *szám felírható egyértelműen*

$$n = b_k a^k + b_{k-1} a^{k-1} + \cdots + b_1 a + b_0$$

alakban, ahol $b_i \in \mathbb{N}$, $0 \leq b_i \leq a - 1, i \in \{1, 2, \ldots, k\}, b_k \neq 0$. (A b_i számok az n **számjegyei**.) *A szamjegyek száma* $k = [\log_a n] + 1$.

Bizonyítás. A 6.1.1. tétel szerint

$$\begin{aligned} n &= aq_0 + b_0, \quad 0 \leq b_0 \leq a - 1 \\ q_0 &= aq_1 + b_1, \quad 0 \leq b_1 \leq a - 1, \\ q_1 &= aq_2 + b_2, \quad 0 \leq b_2 \leq a - 1, \\ &\ldots \end{aligned}$$

és q_i, b_i egyértelműen meghatározottak. Itt $q_0 > q_1 > q_2 > \ldots$, és legyen $q_k = 0$ az első nulla hányados, tehát $q_{k-1} = b_k$, $0 < b_k \leq a - 1$. Visszahelyettesítve kapjuk, hogy

$$n = a(aq_1 + b_1) + b_0 = a(a(aq_2 + b_2) + b_1) + b_0 = \cdots = b_k a^k + b_{k-1} a^{k-1} + \cdots + b_1 a + b_0.$$

Végul vegyük észre, hogy mivel $0 < b_k < a$, $a^k \leq n < a^{k+1}$, tehát $k \leq \log_a n < k + 1$. ■

6.3. feladat. Igazoljuk, hogy minden $m > n$ esetén az m alapú számrendszerben felírt

$$123\ldots(n-1)n(n-1)\ldots321$$

szám teljes négyzet.

6.1.4. tétel (Az egészrész tulajdonságai). *Ha* $x, y \in \mathbb{R}$ *és* $n \in \mathbb{N}^*$*, akkor*
1) $[x] + [y] \le [x+y] \le [x] + [y] + 1$;
2) $[x] + [-x] = \begin{cases} 0, & x \in \mathbb{Z} \\ -1, & x \notin \mathbb{Z} \end{cases}$;
3) $\left[\frac{[x]}{n}\right] = \left[\frac{x}{n}\right]$;
4) **(Hermite-képlet)** $[x] + \left[x + \frac{1}{n}\right] + \left[x + \frac{2}{n}\right] + \ldots \left[x + \frac{n-1}{n}\right] = [nx]$.

Bizonyítás. 1) Legyen $x = m + \alpha$, $y = n + \beta, m, n \in \mathbb{Z}$, $0 \le \alpha, \beta < 1$. Akkor $x + y = m + n + \alpha + \beta$, ahol $0 \le \alpha+\beta < 2$. Ha $\alpha+\beta < 1$, akkor $[x+y] = m+n = [x]+[y]$. Ha $\alpha+\beta \ge 1$, akkor $[x+y] = m+n+1 = [x]+[y]+1$.
3) Legyen $[x] = m$, azaz $x = m + \alpha, 0 \le \alpha < 1$. Létezik $q, r \in \mathbb{Z}$ úgy, hogy $m = qn + r$, $0 \le r \le n-1$. Így

$$\left[\frac{[x]}{n}\right] = \left[\frac{m}{n}\right] = \left[q + \frac{r}{n}\right] = q,$$

$$\left[\frac{x}{n}\right] = \left[\frac{m+\alpha}{n}\right] = \left[\frac{qn+r+\alpha}{n}\right] = \left[q + \frac{r+\alpha}{n}\right] = q + \left[\frac{r+\alpha}{n}\right] = q.$$

4) Legyen

$$f(x) = [nx] - [x] - \left[x + \frac{1}{n}\right] - \left[x + \frac{2}{n}\right] - \cdots - \left[x + \frac{n-1}{n}\right].$$

Vegyük észre, hogy $f(x + \frac{1}{n}) = f(x)$ minden $x \in \mathbb{R}$ esetén és ha $0 \le x < \frac{1}{n}$, akkor $f(x) = 0$. Így $f(x) = 0$ minden $x \in \mathbb{R}$ esetén. ■

6.4. feladat. Oldjuk meg $\mathbb{R}$-ben az $[x + \frac{1}{2}] + [x - \frac{1}{2}] = [2x]$ egyenletet.

6.5. feladat. Igazoljuk, hogy $e = \sum_{n=0}^{\infty} \frac{1}{n!}$ irracionális szám.

Megoldás. Vegyük észre, hogy minden $k \in \mathbb{N}^*$ esetén $[k!e] = k! \sum_{n=0}^{k} \frac{1}{n!} < k!e$.

6.6. feladat. Legyen $\alpha, \beta \in \mathbb{R}_+^*$, $A = \{[n\alpha] \mid n \in \mathbb{N}^*\}$ és $B = \{[n\beta] \mid n \in \mathbb{N}^*\}$. Igazoljuk, hogy a következő állítások ekvivalensek:
(i) $A \cup B = \mathbb{N}$ és $A \cap B = \emptyset$.
(ii) $\alpha, \beta \notin \mathbb{Q}$ és $\frac{1}{\alpha} + \frac{1}{\beta} = 1$.

6.1.2. Oszhatóság. Legnagyobb közös osztó

Néhány alaptulajdonságot az 1.1.2 paragrafusban tárgyaltunk. A 4.8 paragrafusban bebizonyítottuk, hogy $\mathbb{Z}$ faktoriális gyűrű.

6.7. feladat. Legyenek $a, b \in \mathbb{Z}$ és $n \in \mathbb{N}^*$. Akkor
1) $a - b \mid a^n - b^n$,
2) ha n páratlan, akkor $a + b \mid a^n + b^n$,
3) ha n páros, akkor $a + b \mid a^n - b^n$.

6.8. feladat. 1) Igazoljuk, hogy teszőleges $n \in \mathbb{N}$ esetén, $n^5 - n$ osztható 30-al.
2) Igazoljuk, hogy $7 \mid 2^n - 1$ akkor és csak akkor, ha $3 \mid n$, ahol $n \in \mathbb{N}$.
3) Igazoljuk, hogy minden $m \in \mathbb{N}^*$ páratlan számra $240 \mid m^5 - m$.
4) Igazoljuk, hogy $(5n^2 + 3)(n^4 + 8)$ osztható 24-gyel minden $n \in \mathbb{N}$ esetén.
5) Igazoljuk, hogy $3 \cdot 5^{2n+1} + 2^{3n+1}$ osztható 17-tel minden $n \in \mathbb{N}$ esetén.
6) Igazoljuk, hogy ha $n \in \mathbb{Z}$ nem osztható 11-gyel, akkor $n^5 + 1$ vagy $n^5 - 1$ osztható 11-gyel.
6) Igazoljuk, hogy $11 \mid a^2 + b^2$ akkor és csak akkor, ha $11 \mid a$ és $11 \mid b$.

6.9. feladat. 1) Határozzuk meg azokat az $n \in \mathbb{N}^*$ számokat, melyekre $20 \mid 1^n + 2^n + 3^n + 4^n$.
2) Határozzuk meg azokat az $m, m \in \mathbb{Z}$ számokat, melyekre $m + n \mid mn$.

6.10. feladat. Ha $x \in \mathbb{R}$, $x > 0$, akkor az $n \in \mathbb{N}^*$ szám x-nél nem nagyobb pozitív többszöröseinek a száma $[x/n]$.

6.11. feladat. 1) Mutassuk meg, hogy minden $n \in \mathbb{N}^*$ esetén $(n^3 + 3n^2 + 5n + 3, n^2 + 2n + 2) = 1$.
2) Határozzuk meg azokat az $n \in \mathbb{N}^*$ számokat, melyekre $(5^n + 1, 39) = 1$.

6.12. feladat. Legyen $a, b, c \in \mathbb{Z}$. Igazoljuk, hogy
1) $(a, [b, c]) = [(a, b), (a, c)]$, $\quad [a, (b, c)] = ([a, b], [a, c])$;
2) ha $(a, b) = (a, c)$ és $[a, b] = [a, c]$, akkor $b = c$.
3) $[a, b, c](a, b)(b, c)(c, a) = abc(a, b, c)$.

6.13. feladat. 1) Legyen $a \in \mathbb{Z}$, $d \in \mathbb{N}^*$. Igazoljuk, hogy létezik $x, y \in \mathbb{Z}$ úgy, hogy $x + y = s$, $(x, y) = d \iff d \mid s$.
2) Legyen $d, m \in \mathbb{N}^*$. Igazoljuk, hogy létezik $x, y \in \mathbb{Z}$ úgy, hogy $[x, y] = m$, $(x, y) = d \iff d \mid m$.
3) Legyen $p \in \mathbb{Z}$ és $d \in \mathbb{N}^*$. Igazoljuk, hogy létezik $x, y \in \mathbb{Z}$ úgy, hogy $xy = p$, $(x, y) = d \iff d \mid p^2$.

6.14. feladat. Legyen $a, m, n \in \mathbb{N}^*$, $a \geq 2$. Igazoljuk, hogy
1) $(a^m - 1, a^n - 1) = a^{(m,n)} - 1$.
2) Ha $m > n$, akkor $a^{2^n} + 1 \mid a^{2^m} - 1$.
3) Ha $m \neq n$, akkor $(a^{2^m} + 1, a^{2^n} + 1) = \begin{cases} 1, & \text{ha } a \text{ páros} \\ 2, & \text{ha } a \text{ páratlan} \end{cases}$.
4) $(\frac{a^m - 1}{a - 1}, a - 1) = (a - 1, m)$.

6.15. feladat. Igazoljuk, hogy n egymásutáni egész szám szorzata osztható $n!$-sal minden $n \in \mathbb{N}^*$ esetén.

6.16. feladat. Igazoljuk, hogy $2^n \mid C_{2n}^n$ és $2^{n+1} \nmid C_{2n}^n$ minden $n \in \mathbb{N}^*$-re.

6.17. feladat (Egyszerű törtek). Legyen $\frac{n}{m} \in \mathbb{Q}$, ahol $n = p_1^{a_1} \dots p_r^{a_r}$. Igazoljuk, hogy a $\frac{m}{n}$ törtrésze felírható a következő alakban:

$$\left\{\frac{m}{n}\right\} = \sum_{i=1}^{r} \sum_{j=1}^{a_i} \frac{m_{ij}}{p_i^j},$$

ahol $0 \leq m_{ij} < p_i$ minden $j = 1, \dots, a_i$ esetén. Alkalmazás: legyen $\frac{m}{n} = \frac{97}{180}$.

6.1.3. Prímszámok

6.1.5. tétel (Euklidesz). *Végtelen sok prímszám létezik.*

Bizonyítás. Tegyük fel, hogy az állítás nem igaz, tehát véges sok prímszám létezik. Legyenek ezek $p_1, p_2, \dots, p_r$. Tekintsük az $N = p_1 p_2 \dots p_r + 1$ számot, mely nem osztható a $p_1, p_2, \dots, p_r$ prímek egyikével sem. De N-nek létezik q prímosztója, tehát a $p_1, p_2, \dots, p_r$ prímeken kívül más prímszám is létezik, ami ellentmondás. ■

6.18. feladat. Igazoljuk, hogy:
a) Végtelen sok $4k - 1$ alakú prímszám létezik. (Útmutatás: legyen $N = 4p_1 \dots p_r - 1$.)
b) Végtelen sok $6k - 1$ alakú prímszám létezik. (Útmutatás: legyen $N = 6p_1 \dots p_r - 1$.)

6.19. feladat. Ha $n \in \mathbb{N}$ összetett szám, akkor legkisebb prímosztója nem nagyobb $\sqrt{n}$-nél.

6.20. feladat. Igazoljuk, hogy ha p prímszám, akkor $p \mid C_p^k$, bármely k esetén, $1 \leq k \leq p - 1$.

6.21. feladat. 1) Lehet-e a $p, p + 2, p + 4$ számok mindegyike prímszám?
2) Határozzuk meg az összes olyan prímet, melyek egyszerre összegei és különbségei két prímszámnak.

6.22. feladat. Igazoljuk, hogy ha $2^n + 1$ prímszám, akkor $n = 2^k$ alakú.

Az $F_n = 2^{2^n} + 1, n \in \mathbb{N}$ számokat **Fermat-számok**nak, az ilyen alakú prímeket pedig **Fermat-prímek**nek nevezzük. Fermat azt sejtette, hogy az F_n számok mind prímek; $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$ valóban prímek; Euler igazolta, hogy F_5 osztható 641-gyel, tehát a fenti állítás fordítottja nem igaz. Ismert, hogy F_n összetett ha $5 \leq n \leq 21, n = 23, n = 25$. Nem tudjuk, hogy léteznek-e további Fermat-prímek.

6.23. feladat. Igazoljuk, hogy ha $2^n - 1$ prímszám, akkor n is prímszám.

Az $M_p = 2^p - 1$ alakú prímszámokat, ahol p prím, **Mersenne-prímek**nek nevezzük. $M_{11} = 2^{11} - 1 = 23 \cdot 89$ nem prím, tehát a fenti állítás fordítottja nem igaz. Nem tudjuk, hogy általában mely M_p számok a prímek és nem tudjuk, hogy van-e végtelen sok Mersenne-féle prímszám.

6.24. feladat. Legyen $a, b, n \in \mathbb{N}^*$, $a > b$ és $a \geq 2$.
a) Ha és $a^n + b^n$ prím, akkor $n = 2^k$ alakú.
b) Ha $a^n - b^n$ prím, akkor $a - b = 1$ és n prím.

Léteznek olyan prímszámok, melyek különbsége 2, például: $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, ...; ezeket **ikerprímek**nek nevezzük. Nem tudjuk, hogy létezik-e végtelen sok ikerprímpár.

6.25. feladat. 1) Határozzuk meg azokat a p prímeket, melyekre $2p - 1$ és $2p + 1$ is prímek.
2) Ha $p, q \geq 5$ ikerprímek, akkor $12 \mid p + q$.
3) Lehetnek-e $2^n - 1$ és $2^n + 1$ ikerprímek, ahol $n \in \mathbb{N}$?

6.26. feladat. Minden $n \in \mathbb{N}^*$ esetén létezik n egymásután következő összetett szám.

Megoldás. Legyen $a_k = (n + 1)! + k + 1$, ahol $k \in \{1, 2, \ldots, n\}$. Akkor $k + 1 \mid a_k$, és $a_k > k + 1$ minden $k \in \{1, 2, \ldots, n\}$ esetén.

6.27. feladat. Igazoljuk, hogy ha $n \geq 3$, akkor n és $n!$ között van legalább egy prímszám.

Megoldás. Legyen $N = n! - 1$; akkor N-nek van legalább egy p prímosztója. Itt $p > n$, mert ha $p \leq n$ lenne, akkor $p \mid n!$, ami ellentmondás. Másrészt $p \leq N$, ahonnan $p < n!$.

Nem ismerünk olyan képletet, mely csak prímszámokat ad, illetve mely megadja az n-edik prímszámot.

6.28. feladat. Igazoljuk, hogy nem létezik $f \in \mathbb{Z}[X]$ úgy, hogy $f(n)$ prímszám legyen, tetszőleges $n \in \mathbb{N}$ esetén.

Megoldás. Ha $f \in \mathbb{Z}[X]$ és $a \in \mathbb{Z}$, akkor $f(= (X - a)q + f(a)$. Legyen $b := f(a) + a$; akkor $f(b)$ osztható $f(a)$-val.

Például legyen $f = X^2 + X + 41$; akkor $f(0), f(1), f(2), \ldots, f(39)$ mind prímszámok, de $f(40)$ nem prím (Euler).

6.29. feladat (Legendre). Igazoljuk, hogy a p prímszám $n!$ kanonikus alakjában éppen a $\sum_{k \geq 1} \left[\frac{n}{p^k}\right]$ hatványon fordul elő.
Alkalmazások. a) Hány 0-ban végződik 1000! ?
b) Bontsuk prímtényezőkre 100!-t.
c) Mely számok faktoriálisa végződik 1000 nullában?
d) Igazoljuk, hogy $a_1!a_2! \ldots a_n! \mid (a_1 + a_2 + \cdots + a_n)!$, minden $n \in \mathbb{N}^*$ és $a_i \in \mathbb{N}^*$ esetén.

6.30. feladat. Ha p prímszám és $1 \leq k \leq p^n - 1$, akkor $C_{p^n}^k$ osztható p-vel.

6.31. feladat. Bizonyítsuk be, hogy minden páratlan prímszám egyértelműen felírható két négyzet különbségeként.

Máig megoldatlan feladat a **Goldbach-sejtés**: minden 2-nél nagyobb páros természetes szám felírható két prímszám összegeként.

6.32. feladat. Bizonyítsuk be, hogy minden $k \in \mathbb{N}^*$ esetén létezik végtelen sok olyan p prímszám, hogy a $p - k, \ldots, p - 2, p - 1, p + 1, p + 2, \ldots p + k$ számok mindegyike összetett szám.

6.33. feladat. Bizonyítsuk be, hogy minden $n \in \mathbb{N}$, $n > 1$ esetén $\sum_{k=1}^{n} \frac{1}{k}$ nem egész szám.

Prímszámokra vonatkozó becslések

Felsorolunk bizonyítás nélkük néhány fontos eredményt.

Jelölje p_n az n-edik prímszámot, és ha $x \in \mathbb{R}$, $x > 0$, jelölje $\pi(x) = \sum_{p \leq x} 1$ az x-nél nem nagyobb prímszámok számát. Így $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, \ldots$, $\pi(10) = 4, \pi(100) = 25$, stb.

A következő tételt J. Hadamard és Ch. de la Vallée Poussin bizonyítottak 1896-ban, egymástól függetlenül, komplex-függvénytani segédeszközökkel. Az első elemi bizonyítást Erdős Pál és A. Selberg adták 1949-ben, szintén egymástól függetlenül.

6.1.6. tétel (nagy prímszámtétel). $\lim_{x \to \infty} \pi(x)/\frac{x}{\log x} = 1$.

6.1.7. tétel (Bertrand-posztulátum, Csebisev-tétel). *Ha $n \in \mathbb{N}, n \geq 2$, akkor létezik olyan p prímszám, melyre $n < p < 2n$.*

Azonnal következik, hogy ha $n \geq 2$, akkor $p_n < 2^n$.

6.1.8. tétel. $\lim_{n \to \infty} \frac{\log p_n}{\log n} = 1$.

6.1.4. Számelméleti függvények

Legyen $\mathcal{A} = \{f \mid f : \mathbb{N}^* \to \mathbb{C}\}$ a **számelméleti függvények** halmaza és

$$\mathcal{M} = \{f \in \mathcal{A} \mid f(1) = 1,\ f(mn) = f(m)f(n) \text{ ha } (m, n) = 1\}$$

a **multiplikatív számelméleti függvények** halmaza. Ha $f, g \in \mathcal{A}$, legyen

$$(f * g)(n) = \sum_{d|n} f(d)g(n/d),\ (\forall)n \in \mathbb{N}^*$$

az f és g **konvolutiója**. Ha $f \in \mathcal{F}$, akkor az

$$F(n) = \sum_{d|n} f(d), \quad n \in \mathbb{N}^*$$

képlettel értelmezett F függvényt az f **Dirichlet-féle összegzési függvény**ének nevezzük.

6.1.9. példa. Számelméleti függvények a következők:

- $\mathbf{1}$, ahol $\mathbf{1}(n) = 1$ minden $n \in \mathbb{N}^*$-ra. Nyilvánvaló, hogy $\mathbf{1}$ multiplikatív;
- ι, ahol $\iota(n) = n$, és általában, ι_s, ahol $\iota_s(n) = n^s$ minden $n \in \mathbb{N}^*$-ra. Nyilvánvaló, hogy ι_s multiplikatív minden $s \in \mathbb{R}$ esetén;
- τ, ahol $\tau(n)$ az n szám osztóinak száma;
- σ, ahol $\sigma(n)$ az n szám osztóinak összege;
- φ, az **Euler-függvény**, ahol $\varphi(n) = |\{a \in \mathbb{Z} \mid 0 < a < n,\ (a, n) = 1\}|$. Később 6.2.13-ban igazoljuk, hogy φ multiplikatív;
- μ, a **Möbius-függvény**, ahol

$$\mu(n) = \begin{cases} 1, & \text{ha } n = 1, \\ 0, & \text{ha létezik } p \text{ prím, melyre } p^2 \mid n, \\ (-1)^r, & \text{ha } n = p_1p_2\dots p_r, p_i \neq p_j \end{cases}$$

6.34. feladat. *Igazoljuk, hogy μ multiplikatív függvény.*

Megoldás. Ha $m = n = 1$, akkor $\mu(mn) = \mu(mn) = \mu(1) = 1 = \mu(m)\mu(n)$. Ha $m = 1$ és $n \neq 1$, akkor $\mu(mn) = \mu(n) = \mu(m)\mu(n)$ (hasonlóan, ha $n = 1$ és $m \neq 1$). Ha $m \neq 1, n \neq 1$ és ha m vagy n nem négyzetmentes, azaz ha létezik p prím úgy, hogy $p^2 \mid m$ vagy $p^2 \mid n$, akkor $p^2 \mid mn$ és $\mu(mn) = 0 = \mu(m)\mu(n)$. Végül ha m is és n is négyzetmentes, akkor legyen $m = p_1p_2\dots p_r$ és $n = q_1q_2\dots q_s, p_i \neq q_j$. Ekkor $\mu(mn) = \mu(p_1p_2\dots p_rq_1q_2\dots q_s) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n)$.

6.1.10. lemma. *Legyen $g : \{p^a \mid p \text{ prím}, a \in \mathbb{N}^*\} \to \mathbb{C}$ egy függvény. Ekkor létezik egyetlen $f \in \mathcal{M}$ úgy, hogy $f(p^a) = g(p^a)$ minden p prím és $a \in \mathbb{N}^*$ esetén.*

Bizonyítás. Ha $n = p_1^{a_1}p_2^{a_2}\dots p_r^{a_r} > 1$, legyen $f(n) = g(p_1^{a_1})g(p_2^{a_2})\dots g(p_r^{a_r})$. ■

6.1.11. tétel. 1) $(\mathcal{F}, +, *)$ *integritástartomány.*
2) $f \in U(\mathcal{F})$ *akkor és csak akkor, ha* $f(1) \neq 0$.
3) $\mathcal{M} \leq (U(\mathcal{F}), *)$

Bizonyítás. 1) Nyilvánvalóan $(\mathcal{F}, +)$ kommutatív csoport, melyben a semleges elem a nullfüggvény. Igazoljuk, hogy $(\mathcal{F}, *)$ kommutatív monoid. Minden $(\forall)f, g, h \in \mathcal{F},\ n \in \mathbb{N}^*$ esetén

$$((f * g) * h)(n) = \sum_{dd_3=n} (f * g)(d)h(d_3) = \sum_{dd_3=n} (\sum_{d_1d_2=d} f(d_1)f(d_2))h(d_3) = \sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3).$$

Analóg módon

$$(f * (g * h))(n) = \sum_{d_1d_2d_3=n} f(d_1)g(d_2)h(d_3),$$

tehát $(f * g) * h = f * (g * h)$, vagyis a $*$ művelet asszociatív. Mivel

$$(f * g)(n) = \sum_{d_1d_2=n} f(d_1)f(d_2) = (g * f)(n),$$

következik, hogy a $*$ művelet kommutatív. Azonnal belátható, hogy az

$$\epsilon : \mathbb{N}^* \to \mathbb{C}, \quad \epsilon(n) = \begin{cases} 1, & \text{ha } n = 1 \\ 0, & \text{ha } n \geq 2 \end{cases}$$

számelméleti függvény az $(\mathcal{F}, *)$ félcsoport semleges eleme, tehát $(\mathcal{F}, *)$ kommutatív monoid. Minden $f, g, h \in \mathcal{F}$, és $n \in \mathbb{N}^*$ esetén

$$\begin{aligned}(f * (g + h))(n) &= \sum_{d|n} f(d)(g + h)(n/d) = \sum_{d|n} f(d)g(n/d) + \sum_{d|n} f(d)h(n/d) = \\ &= (f * g)(n) + (f * h)(n) = (f * g + f * h)(n).\end{aligned}$$

Innen $f * (g + h) = f * g + f * h$, tehát $(\mathcal{F}, +, *)$ egységelemes, kommutatív gyűrű.

Még ki kell mutatni, hogy $(\mathcal{F}, +, *)$-ban nincsenek zérusosztók. Ennek érdekében tekintsünk két f és g nem nulla számelméleti függvényt. Igazolni fogjuk, hogy $f * g \neq 0$. Legyenek n illetve m a legkisebb nem nulla természetes számok, melyekre $f(n) \neq 0$ illetve $g(m) \neq 0$. Akkor $d < n$-re $f(d) = 0$, $d > n$-re $\frac{nm}{d} < m$, tehát $g(\frac{nm}{d}) = 0$, és innen felírható, hogy

$$(f * g)(nm) = \sum_{d|nm} f(d)g(nm/d) = \sum_{d|nm,\ d<n} 0 \cdot g(nm/d) + f(n)g(m) + \sum_{d|nm,\ d>n} f(d) \cdot 0 \neq 0.$$

2) „$\Longrightarrow$" Ha $f \in \mathcal{U}(\mathcal{F})$, akkor létezik $\tilde{f} \in \mathcal{U}(\mathcal{F})$ úgy, hogy $f * \tilde{f} = \tilde{f} * f = e$. Következik, hogy $f(1)\tilde{f}(1) = (f * \tilde{f})(1) = e(1) = 1$, ahonnan $f(1)\tilde{f}(1) = 1$, tehát $f(1) \neq 0$.

„$\Longleftarrow$" Tételezzük fel, hogy $f(1) \neq 0$. Igazolni fogjuk, hogy az

$$\tilde{f} : \mathbb{N}^* \to \mathbb{C}, \quad \tilde{f}(n) = \begin{cases} \frac{1}{f(1)}, & \text{ha } n = 1 \\ -\frac{1}{f(1)} \sum_{d|n,\ d>1} f(d)\tilde{f}\left(\frac{n}{d}\right), & \text{ha } n \geq 2 \end{cases}$$

rekurzív összefüggéssel megadott függvény az f inverze. Valóban $(f * \tilde{f})(1) = f(1)\tilde{f}(1) = f(1) \cdot \frac{1}{f(1)} = 1 = \epsilon(1)$, és $n \geq 2$-re

$$(f * \tilde{f})(n) = \sum_{d|n} f(d)\tilde{f}(n/d) = f(1)\tilde{f}(n) + \sum_{d|n,\ d>1} f(d)\tilde{f}(n/d) = f(1)\tilde{f}(n) - f(1)\tilde{f}(n) = 0 = \epsilon(n).$$

2) Mivel minden $f \in \mathcal{M}$ esetén $f(1) = 1 \neq 0$, az előző pont alapján következik, hogy $f \in \mathcal{U}(\mathcal{F})$. Tehát $\mathcal{M} \subseteq \mathcal{U}(\mathcal{F})$, és vegyük még észre, hogy $e \in \mathcal{M}$. Ahhoz, hogy $\mathcal{M} \leq \mathcal{U}(\mathcal{F})$, még be kell látni, hogy:

(1) $f, g \in \mathcal{M} \Rightarrow f * g \in \mathcal{M}$;

(2) $f \in \mathcal{M} \Rightarrow \tilde{f} \in \mathcal{M}$, ahol $\tilde{f}$ az f inverze a $*$ műveletre vonatkozóan.

Igazoljuk (1)-et. Nyilvánvalóan $(f * g)(1) = f(1)g(1) = 1 \cdot 1 = 1$. Ha $n, m \in \mathbb{N}^*$ és $(m, n) = 1$, akkor az nm osztói $d_1 d_2$ alakúak, ahol $d_1 | n, d_2 | m$, mi több $(d_1, d_2) = \left(\frac{n}{d_1}, \frac{m}{d_2}\right) = 1$. A fentiek alapján

$$\begin{aligned}(f * g)(nm) &= \sum_{d|nm} f(d)g(nm/d) = \sum_{d_1|n,\ d_2|m} f(d_1 d_2)g(nm/d_1 d_2) = \\ &= \sum_{d_1|n,\ d_2|m} f(d_1)f(d_2)g(n/d_1)g(m/d_2) = (\sum_{d_1|n} f(d_1)g(n/d_1))(\sum_{d_2|m} f(d_2)g(m/d_2)) = \\ &= (f * g)(n) \cdot (f * g)(m).\end{aligned}$$

Tehát $f * g \in \mathcal{M}$.

Igazoljuk (2)-őt. Tekintsük a következő segédfüggvényt:

$$g \in \mathcal{F}, \quad g(n) = \begin{cases} 1, & \text{ha } n = 1 \\ \tilde{f}(p_1^{\alpha_1}) \dots \tilde{f}(p_k^{\alpha_k}), & \text{ha } n = p_1^{\alpha_1} \dots p_k^{\alpha_k} \end{cases}.$$

Azonnal belátható, hogy $g \in \mathcal{M}$, és akkor (1) alapján, $f * g \in \mathcal{M}$. Igazolni fogjuk, hogy $f * g = e$. Mivel $f * g$, $\epsilon \in \mathcal{M}$, ehhez elég belátni, hogy $(f * g)(p^\alpha) = \epsilon(p^\alpha)$ minden p prim és $\alpha \in \mathbb{N}$ esetén. Valóban

$$(f * g)(p^\alpha) = \sum_{i=0}^{\alpha} f(p^i)g(p^{\alpha-i}) = \sum_{i=0}^{\alpha} f(p^i)\tilde{f}(p^{\alpha-i}) = (f * \tilde{f})(p^\alpha) = \epsilon(p^\alpha),$$

tehát $f * g = \epsilon$, és mivel az f inverze egyértelmű, $\tilde{f} = g \in \mathcal{M}$. ■

6.1.12. következmény. 1) *Legyen* $n = p_1^{a_1} \dots p_r^{a_r}$, *ahol* p_i *páronként különböző prímszámok és* $a_i \in \mathbb{N}^*$. *Ekkor*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right) \cdots \left(1 - \frac{1}{p_r}\right).$$

2) *Ha* $f \in \mathcal{M}$ *és* F *az* f *összegzési függvénye, akkor* F *is multiplikatív. Mi több,*

$$F(n) = \prod_{i=1}^{r} \left(1 + f(p_i) + f(p_i^2) \cdots + f(p_i^{a_i})\right).$$

3) *A* σ, τ *függvények multiplikatívak és*

$$\sigma(n) = \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdots \frac{p_r^{a_r+1} - 1}{p_r - 1},$$
$$\tau(n) = (a_1 + 1) \dots (a_r + 1).$$

4) **(Möbius-féle inverziós képlet)** $\mu * \mathbf{1} = \epsilon$. *Partikulárisan, minden* $f, g \in \mathcal{F}$ *esetén*

$$g = f * \mathbf{1} \Longleftrightarrow f = g * \mu.$$

5) **(Gauss)** $\sum_{d|n} \varphi(d) = n$.

Bizonyítás. 1) Mivel $\varphi \in \mathcal{M}$, $\varphi(n) = \varphi(p_1^{a_1}) \cdot \dots \cdot \varphi(p_r^{a_r})$. A φ függvény értelmezése alapján $\varphi\left(p^a\right)$ a p^a-nal relatív prímek számát jelenti. Az $1, \dots, p-1, p, p+1, \dots, 2p-1, p, 2p+1, \dots, p^a - 1, p^a$ számok közül minden p-dik osztható p-vel, a többi relatív prím p-vel, így

$$\varphi\left(p^a\right) = p^a - p^{a-1} = p^a\left(1 - \frac{1}{p}\right),$$

és innen következik az állítás.

2) Vegyük észre, hogy $F = f * \mathbf{1}$. Továbbá,

$$\prod_{i=1}^{k} \left(1 + f(p_i) + f(p_i^2) \cdots + f(p_i^{a_i})\right) = \sum_{0 \le b_i \le a_i} f(p_1^{b_1}) \dots f(p_k^{b_k}) = \sum_{d|n} f(n).$$

3) Vegyük észre, hogy $\sigma = \iota * \mathbf{1}$ és $\tau = \mathbf{1} * \mathbf{1}$. Mivel a p^a osztói $1, p, \dots, p^a$, kapjuk, hogy $\tau(p^a) = a + 1$ és $\sigma(p^a) = \frac{p^{a+1}-1}{p-1}$, és alkalmazzuk az előző pontot.

4) Azonnal belátható, hogy $(\mu * \mathbf{1})(p^a) = \epsilon(p^a)$ minden p prím és $a \in \mathbb{N}^*$ esetén.

5) Azonnal belátható, hogy $(\varphi * \mathbf{1})(p^a) = \iota(p^a)$ minden p prím és $a \in \mathbb{N}^*$ esetén. ■

Tökéletes számok

6.1.13. definíció. Az $n \in \mathbb{N}^*$ számot **tökéletes szám**nak nevezzük ha $\sigma(n) = 2n$.

Például $n = 6$ és $n = 28$ tökéletes számok, mert $6 = 1 + 2 + 3$ és $28 = 1 + 2 + 4 + 7 + 14$, illetve $\sigma(6) = 1 + 2 + 3 + 6 = 2.6 = 12$ és $\sigma(28) = 1 + 2 + 4 + 7 + 14 + 28 = 2.28 = 56$.

6.1.14. tétel (Euklidesz). *Ha* $n = 2^k - 1$ *prímszám, akkor* $n = 2^{k-1}(2^k - 1)$ *tökéletes szám.*

Bizonyítás. A σ függvény multiplikativitása alapján $\sigma(n) = \sigma(2^{k-1}(2^k - 1)) = \sigma(2^{k-1})\sigma(2^k - 1) = (2^k - 1)(1 + 2^k - 1) = 2^k(2^k - 1) = 2n$. ■

6.1.15. tétel (Euler). *Ha* n *páros tökéletes szám, akkor* $n = 2^{k-1}(2^k - 1)$ *alakú, ahol* $2^k - 1$ *Mersenne-féle prímszám.*

Bizonyítás. Legyen $n = 2^a m$, ahol $a \ge 1$ és m páratlan. Így $\sigma(n) = \sigma(2^a m) = \sigma(2^a)\sigma(m) = (2^{a+1} - 1)\sigma(m)$ és innen $\sigma(n) = 2n$ alapján $(2^{a+1} - 1)\sigma(m) = 2^{a+1} m$. Következik, hogy $2^{a+1} - 1 | 2^{a+1} m$, s mivel $(2^{a+1} - 1, 2^{a+1}) = 1$ kapjuk, hogy $2^{a+1} - 1 | m$, azaz $m = (2^{a+1} - 1)m_1$, amit visszahelyettesítve: $(2^{a+1} - 1)\sigma(m) = (2^{a+1} - 1)2^{a+1} m_1$, ahonnan $\sigma(m) = 2^{a+1} m_1$. Az m_1 és m osztói m-nek, $m_1 < m$ és $m_1 + m = m_1 + (2^{a+1} - 1)m_1 = 2^{a+1} m_1 = \sigma(m)$. Így m-nek m_1-en és m-en kívül nincs más osztója, s kapjuk, hogy $m_1 = 1$ és $m = 2^{a+1} - 1$ prímszám. Tehát az $a = k - 1$ jelöléssel $n = 2^{k-1}(2^k - 1)$, ahol $2^k - 1$ prímszám. ■

6.1.16. megjegyzés. Nem tudjuk, hogy létezik-e végtelen sok tökéletes szám. Azt sem tudjuk, hogy létezik-e páratlan tökéletes szám.

6.35. feladat. Igazoljuk, hogy minden $m, n \in \mathbb{N}^*$ esetén
a) $\varphi(mn) = \mathrm{frac}\varphi(m)\varphi(n)(m,n)\varphi((m,n))$; b) $\sigma(mn) \le \sigma(m)\sigma(n)$.

6.36. feladat. Igazoljuk, hogy minden $n \in \mathbb{N}^*$ esetén
a) $\prod_{d|n} d = n^{\frac{\tau(n)}{2}}$; b) $\tau(n) \le 2\sqrt{n}$.

6.37. feladat. Határozzuk meg n-et úgy, hogy
a) $\phi(n) = 18$; b) $\phi(n)$ páratlan legyen; c) $\tau(n)$ páros legyen.

6.38. feladat. Igazoljuk, hogy minden $n \in \mathbb{N}^*$-ra
a) $\mu(n^3) = \mu(n^2)$; b) $\varphi(n^2) = n\varphi(n)$.

6.39. feladat. Legyenek $f, g, h \in \mathcal{F}$ égy , hogy minden $n \in \mathbb{N}^*$-ra

$$f(n) = \sum_{k=1}^{n} h(k/n), \qquad g(n) = \sum_{(k,n)=1} h(k/n).$$

Igazoljuk, hogy: a) $f = g * 1$. b) $\mu(n) = \sum_{(k,n)=1} e^{\frac{2\pi i k}{n}}$.

6.2. Kongruenciák

6.2.1. A $\mathbb{Z}_n$ gyűrű

Legyen $n \in \mathbb{N}$. $\mathbb{Z}$-n definiáljuk a modulo n kongruenciarelációt: ha $a, b \in \mathbb{Z}$, akkor

$$a \equiv b \pmod{n} \overset{\text{def}}{\Leftrightarrow} n \mid b - a \Leftrightarrow b - a \in n\mathbb{Z} \Leftrightarrow \exists k \in \mathbb{Z} : b = a + nk \Longleftrightarrow a \bmod n = b \bmod n.$$

Jelölés: $\hat{a} = [a]_n = \{a + nk \mid k \in \mathbb{Z}\} = a + n\mathbb{Z}$ az a osztálya modulo n. Legyen

$$\mathbb{Z}_n := \{\hat{a} \mid a \in \mathbb{Z}\};$$

akkor $\mathbb{Z}_n$ kommutatív egységelemes gyűrű, ahol

$$\hat{a} + \hat{b} \overset{\text{def}}{=} \widehat{a+b}, \qquad \hat{a}\hat{b} \overset{\text{def}}{=} \widehat{ab}.$$

Semleges elemek: $\hat{0} = n\mathbb{Z}$, $\hat{1} = 1 + n\mathbb{Z}$. Partikuláris esetek:

- $n = 0$: $a \equiv b \pmod{0} \Leftrightarrow b - a = 0 \Leftrightarrow b = a$
  $\hat{a} = [a]_n = \{a\}$, $\mathbb{Z}_0 = \{\{a\} \mid a \in \mathbb{Z}\} \simeq \mathbb{Z}$;
- $n = 1$: $a \equiv b \pmod{1}$ igaz $\forall a, b \Rightarrow \hat{a} = \mathbb{Z}$, $\mathbb{Z}_1 = \{\hat{0}\}$;
- $n \ge 2$: $\exists! q, r \in \mathbb{Z}$ úgy, hogy

  $$a = nq + r, \quad 0 \le r < n$$

  Itt $q = \left[\frac{a}{n}\right]$, $r = a - n\left[\frac{a}{n}\right] \equiv a \pmod{n}$; következik, hogy $\hat{a} = \hat{r}$, tehát $|\mathbb{Z}_n| \le n$; ha $0 \le r < s < n - 1$, akkor $n \nmid s - r$, tehát $|\mathbb{Z}_n| = n$.

6.40. feladat. Ha $a \equiv b \pmod{n}$, akkor $(a, n) = (b, n)$.

Megoldás. Legyen $a - b = kn$, ahol $k \in \mathbb{Z}$. Mivel $(a, n)|a$ és $(a, n) \mid m$, következik, hogy $(a, m) \mid b$. Tehát (a, m) közös osztója b-nek és m-nek, ahonnan $(a, m) \mid (b, m)$. Hasonlóképpen kapjuk, hogy $(b, m) \mid (a, m)$, tehát $(a, m) = (b, m)$.

6.41. feladat (alaptulajdonságok). Legyenek $a, b, c, d \in \mathbb{Z}$ és $m, m_1, m_2, k \in \mathbb{N}^*$. Akkor
1) ha $a \equiv b \pmod{m}$ és $c \equiv d \pmod{m}$, akkor $a + c \equiv b + d \pmod{m}$ és $ac \equiv bd \pmod{m}$;
2) ha $f \in \mathbb{Z}[X]$ és $a \equiv b \pmod{m}$), akkor $f(a) \equiv f(b) \pmod{m}$;
3) ha $a \equiv b \pmod{m}$ és $d \mid a, b, m$, akkor $\frac{a}{d} \equiv \frac{b}{d} \pmod{\frac{m}{d}}$;
4) ha $ac \equiv bc \pmod{m}$ és $(c, m) = 1$, akkor $a \equiv b \pmod{m}$;
5) ha $a \equiv b \pmod{m_1}$ és $a \equiv b \pmod{m_2}$, akkor $a \equiv b \pmod{[m_1, m_2]}$).

6.42. feladat (oszthatósági szabályok). Legyen

$$N = \overline{a_k a_{k-1} \dots a_1 a_0} = a_k \cdot 10^k + a_{k-1} \cdot 10^{k-1} + \dots + a_1 \cdot 10 + a_0$$

egy tízes számrendszerbeli szám. Igazoljuk, hogy:
1) $N \equiv a_0 \pmod 2$, $\pmod 5$, $\pmod{10}$.
2) $N \equiv \overline{a_1 a_0} \pmod 4$, $\pmod{25}$.
3) $N \equiv \overline{a_2 a_1 a_0} \pmod 8$, $\pmod{125}$.
4) $N \equiv a_0 + a_1 + \dots + a_k \pmod 3$, $\pmod 9$.
5) $N \equiv \sum_{i=0}^{k} (-1)^i a_i \pmod{11}$.
6) $N \equiv \overline{a_2 a_1 a_0} + \overline{a_k \dots a_3} \pmod{27}$, $\pmod{37}$. (Vegyük észre, hogy $27 \cdot 37 = 999$.)
7) $N \equiv \overline{a_2 a_1 a_0} - \overline{a_k \dots a_3} \pmod 7$, $\pmod{11}$, $\pmod{13}$. (Vegyük észre, hogy $7 \cdot 11 \cdot 37 = 1001$.)

6.2.1. lemma. *Legyen $a \in \mathbb{Z}$. A következő állítások ekivalensek:*
(i) $\hat{a} \in U(\mathbb{Z}_n)$
(ii) a *nem zérusosztó $\mathbb{Z}_n$-ben.* ($\hat{a}\hat{b} = \hat{0} \Rightarrow \hat{b} = \hat{0}$)
(iii) $(a, n) = 1$.

Bizonyítás. „(i)⇒(ii)" $\hat{a}\hat{b} = \hat{0}$. Beszorozva $\hat{a}^{-1}$-gyel kapjuk, hogy $\hat{b} = \hat{0}$.

„(ii)⇒(iii)" ⇔ „(iii) ⇒ (ii)" Feltételezzük, hogy $(a, n) = d > 1$. Legyen $a = a'd$, $n = n'd$, tehát $(a', n') = 1$. Ebben az esetben $\hat{a}$ zérusosztó. Valóban,

$$\widehat{an'} = \widehat{an'} = \widehat{a'dn'} = \widehat{a'n} = \widehat{a'}\hat{n} = \hat{0}.$$

„(iii)⇒(i)" Ha $(a, n) = 1$, akkor $\exists\, u, v \in \mathbb{Z}$ úgy, hogy $au + nv = 1$. Innen $\hat{1} = \hat{a}\hat{u} + \hat{n}\hat{v}$, tehát $\hat{a}^{-1} = \hat{u}$. (u, v meghatározható Euklidészi algoritmussal.) ■

6.2.2. tétel. *A következő állítások ekivalensek:*
(i) $\mathbb{Z}_n$ *test (minden nem nulla elem invertálható);*
(ii) $\mathbb{Z}_n$ *integritástartomány;*
(iii) n *prímszám.*

Bizonyítás. (i) ⇔ (iii) $\mathbb{Z}_n$ test ⇔ $\forall\, 0 < a < n$, $(a, n) = 1$ ⇔ n prím. ■

6.2.3. megjegyzés. Láttuk, hogy $(\mathbb{Z}_n, +, \cdot)$ kommutatív gyűrű.

1) Tekintsük a $(\mathbb{Z}_n, +)$ csoportot. $\mathbb{Z}_n = \langle \hat{1} \rangle$ ciklikus csoport, mert $\operatorname{ord}(\hat{1}) = n$. Láttuk, hogy $\langle \hat{r} \rangle = (\mathbb{Z}_n, +)$ ⇔ $(r, n) = 1$ (tehát a $(\mathbb{Z}_n, +)$-t generáló elemeinek a száma $\varphi(n)$).

2) Tekintsük az $(U(\mathbb{Z}_n, \cdot)$ csoportot. Láttuk, hogy

$$U(\mathbb{Z}_n) = \{\hat{a} \in \mathbb{Z}_n \mid (a, n) = 1\},$$

tehát $|\, U(\mathbb{Z}_n) \,| = \varphi(n)$.

6.2.4. következmény. a) **(Euler-tétel)** *Minden $a \in \mathbb{Z}$, $(a, n) = 1$ esetén*

$$a^{\varphi(n)} \equiv 1 \pmod n$$

(*azaz $a^{\varphi(n)} = 1$ $U(\mathbb{Z}_n)$-ben*).

b) **(kis Fermat-tétel)** $\forall\, a \in \mathbb{Z}$, $\forall\, p$ *prímszám esetén* $a^p \equiv a \pmod p$.

Bizonyítás. a) Következik a Lagrange-tételből.

b) $p \nmid a \Rightarrow (p, a) = 1 \overset{a)}{\Rightarrow} a^{p-1} \equiv 1 \pmod p \Rightarrow a^{p-1} \equiv a \pmod p$. Ha $p \mid a$, akkor $p \mid a^p$, tehát $p \mid a^p - a$, ahonnan $a^p \equiv a \pmod p$. ■

6.2.5. megjegyzés. Az a) állítást be lehet bizonyítani Lagrange-tétel nélkül is, mivel $U(\mathbb{Z}_n)$ kommutatív. Legyen G egy kommutatív csoport, $|G| = n$ és legyen $a \in G$. Igazoljuk, hogy $a^n = e$.

Valóban, feltételezzük, hogy $G = \{x_1, \dots, x_n\}$; ekkor

$$t_a : G \to G,\ t_a(x) = ax$$

bijektív, tehát

$$G = \{ax_1, \dots, ax_n\} \Rightarrow x_1 \cdot \dots \cdot x_n = ax_1 \cdot \dots \cdot ax_n \overset{\text{komm}}{\Rightarrow} x_1 \cdot \dots \cdot x_n = a^n x_1 \cdot \dots \cdot x_n \Rightarrow a^n = e.$$

6.43. feladat. Számítsuk ki a következő legkisebb pozitív maradékokat:
a) $2^{1000000} \mod 77$; b) $3^{400} \mod 100$ c) $3^{100000} \mod 101$.

6.44. feladat. Igazoljuk, hogy $42 \mid n^7 - n$ és $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \mid n^{13} - n$ minden $n \in \mathbb{N}^*$ esetén.

6.45. feladat. Igazoljuk, hogy ha $p > 3$ prím és $a \in \mathbb{Z}$, akkor $a^p \equiv a \pmod{6p}$.

6.46. feladat. Igazoljuk, hogy ha $p > 5$ prím, akkor minden 10-es alapú számrendszerben felírt, $p - 1$ azonos számjegyből álló szám osztható p-vel.

6.47. feladat. Létezik-e $n \in \mathbb{N}^*$, melyre $n \mid 2^n - 1$?

6.2.6. tétel (Wilson-tétel). p *prímszám* $\Leftrightarrow (p-1) \equiv -1 \pmod p$.

Bizonyítás. „$\Rightarrow$" $p = 2$ esetén az állítás igaz, mert $1 \equiv (-1) \pmod 2$.

$p > 2$ esetén képezzük a következő polinomot:

$$P(X) = (X - \hat{1})(X - \hat{2}) \dots (X - \widehat{p-1}) - (X^{p-1} - \hat{1}) = a_{p-2}X^{p-2} + \dots + a_1 X + a_0 \in \mathbb{Z}_p[X],$$

tehát $\deg P \leq p - 1$. Vegyük észre, hogy P-nek van $p - 1$ gyöke: $\hat{1}, \hat{2}, \dots, \widehat{p-1}$ gyökei P-nek mivel $x^{p-1} \equiv 1 \pmod p$. Következik, hogy $P = \hat{0}$, a null-polinom. Innen

$$\hat{0} = P(0) = (-1)^{p-1} \cdot \hat{1} \cdot \hat{2} \cdot \hat{3} \dots (\widehat{p-1}) + \hat{1} = (-1)^{p-1}(\widehat{p-1})! + \hat{1} = (\widehat{p-1})! + \hat{1},$$

mivel $p - 1$ páros.

Második bizonyítás ($p > 2$ esetén):

Vegyük észre, hogy $\hat{1} \cdot \hat{2} \dots \widehat{p-1}$ a $(\mathbb{Z}_p^*, \cdot)$ csoport összes elemeinek a szorzata. Csoportosítjuk x-et x^{-1}-gyel. Evidens, hogy tetszőleges csoportban $x = y \Leftrightarrow x^{-1} = y^{-1}$. Páronként vesszük a $(\mathbb{Z}_p^*, \cdot)$ csoport elemeit. Vegyük észre, hogy $\mathbb{Z}_p^*$-ban $x = x^{-1} \Leftrightarrow x^2 = \hat{1} \Leftrightarrow x = \hat{1}$ vagy $x = -\hat{1}$. Így a keresett szorzat

$$\underbrace{\hat{1}}_{\substack{\downarrow \\ \text{önmagának inverze}}} \cdot \underbrace{\hat{2} \cdot \hat{3} \cdots (\widehat{p-3}) \cdot (\widehat{p-2})}_{\substack{\shortparallel \\ 1}} \cdot \underbrace{\left(\widehat{p-1}\right)}_{\substack{\downarrow \\ \text{önmagának inverze}}} = -\hat{1}$$

„$\Leftarrow$" Feltételezzük, hogy p nem prímszám: $p = ls$, ahol $l, s \geq 2$. Mivel $(p-1)! + 1 = kp$, ahol $k \in \mathbb{Z}$, következik, hogy $1 = kp - (p-1)!$. Mivel $l \mid p$ és $l \mid (p-1)!$, következik, hogy $l \mid 1$, ellentmondás, mert $l \geq 2$. ■

6.48. feladat. Mennyi 100!-nak 109-cel való osztási maradéka?

6.49. feladat. Bizonyítsuk be, hogy a Fermat és Wilson tételei ekvivalensek a következő állítással: minden a egész szám és minden p prím esetén $a^p + (p-1)!a \equiv 0 \pmod p$.

6.50. feladat. Legyen p egy prímszám. Bizonyítsuk be, hogy létezik $x \in \mathbb{Z}$ úgy, hogy $x^2 \equiv -1 \pmod p \Leftrightarrow p \equiv 1 \pmod 4$ vagy $p = 2$.

Megoldás. Ha $p = 2$, akkor legyen $x = 1$ és vegyük észre, hogy $1 \equiv -1 \pmod 2$. Legyen $p = 4k + 1$ alakú. A Wilson-tétel szerint

$$(p-1)! = 1 \cdot 2 \cdot 3 \dots \frac{p-3}{2} \cdot \frac{p-1}{2} \cdot \frac{p+1}{2} \cdot \frac{p+3}{2} \dots (p-1) \equiv -1 \pmod p.$$

Mivel $\frac{p+1}{2} = p - \frac{p-1}{2} \equiv -\frac{p-1}{2} \pmod p$, $\frac{p+3}{2} = p - \frac{p-3}{2} \equiv -\frac{p-3}{2} \pmod p$, $\dots$, $p - 1 \equiv -1 \pmod p$, kapjuk, hogy

$$(-1)^{\frac{p-1}{2}} \left(1 \cdot 2 \cdot 3 \cdots \frac{p-3}{2} \cdot \frac{p-1}{2}\right)^2 \equiv -1 \pmod p.$$

Itt $\frac{p-1}{2} = 2k$ páros szám, tehát az $x = (\frac{p-1}{2})!$ választással teljesül az $x^2 \equiv -1 \pmod p$ kongruencia.

Legyen $p = 4k + 3$ alakú, és tegyük fel, hogy létezik $x \in \mathbb{Z}$ úgy, hogy $x^2 \equiv -1 \pmod p$. Mindkét oldalt $\frac{p-1}{2} = 2k + 1$ hatványra emelve kapjuk, hogy $x^{p-1} \equiv -1 \pmod p$. Itt $p \nmid x$ (ellenkező esetben $p \mid -1$, ami ellentmondás). A Fermat-tétel szerint $x^{p-1} \equiv 1 \pmod p$, tehát $-1 \equiv 1 \pmod p$, ami ellentmondás.

6.51. feladat (Wilson-tétel általánosítása). Legyen $K = \{0, 1, a_3, \dots, a_q\}$ egy véges (tehát kommutatív) test. Igazoljuk, hogy $a_3 \dots a_q = -1$.

Az elsőfokú kongruencia megoldása

Tekintsük az $ax \equiv b \pmod{n}$ (1) kongruenciát, ahol $a, b \in \mathbb{Z}$ adottak, $n \in \mathbb{N}^*$, $n \geq 2$ adott, $x \in \mathbb{Z}$ ismeretlen.
Legyen $d := (a, n)$, $a = a'd$, $n = n'd$, tehát $(a', n') = 1$.

- Ha x megoldás $\Rightarrow b - ax = nk$ alakú $\Rightarrow b = ax + nk$, ami osztható d-vel, mert $a \vdots d$ és $n \vdots d$.
  Tehát ha $d \nmid b$ akkor nincs megoldás.
- Feltételezzük, hogy $d|b$ és legyen $b = b'd$.
  Akkor $ax \equiv b \pmod{n} \Leftrightarrow a'x \equiv b' \pmod{n'}$ (2).

Ez utóbbi kongruencia egyenértékű az $\widehat{a'}\widehat{x} = \widehat{b'}$ $\mathbb{Z}_n$-beli egyenlőséggel.

$(a', n') = 1 \Rightarrow \exists\ \widehat{a'}^{-1} \in U(\mathbb{Z}_{n'})$ ($\widehat{a'}^{-1}$-t az Euklidészi algoritmussal határozzuk meg). Tehát $\mathbb{Z}_{n'}$-ben az egyetlen megoldás $\widehat{x} = \widehat{b'}\widehat{a'}^{-1}$. Legyen x_0 a (2) legkisebb pozitív megoldása ($0 \leq x_0 < n'$). Akkor az (1) megoldásai: $x_0,\ x_0 + n',\ \ldots,\ x_0 + (d-1)n'$. Ezek mind különböző megoldások (nem kongruensek $\bmod n$).

6.52. feladat. Oldjuk meg a következő kongruenciákat:
a) $x \equiv 2 \pmod{3}$; b) $9x \equiv 12 \pmod{21}$; c) $27x \equiv 72 \pmod{900}$; d) $68x \equiv 2 \pmod{72}$;
e) $68x \equiv 16 \pmod{72}$.

6.53. feladat. Oldjuk meg $\mathbb{Z}_{18}$-ban az $\widehat{a}\widehat{x} = \widehat{b}$ egyenletet:
a) $\widehat{7}x = \widehat{15}$; b) $\widehat{8}x = \widehat{11}$; c) $\widehat{10}x = \widehat{16}$.

6.2.2. Pszeudoprímszámok

A Fermat-tétel fordítottja nem igaz, azaz ha $a^n \equiv a \pmod{n}$; ahol $a \in \mathbb{N}$, akkor nem következik, hogy n prímszám.

6.54. feladat. Igazoljuk, hogy $2^n \equiv 2 \pmod{n}$, ahol:
a) $n = 341 = 11 \cdot 31$; $n = 561 = 3 \cdot 11 \cdot 17$; $n = 645 = 3 \cdot 5 \cdot 343$.

6.2.7. definíció. a) Az $n \in \mathbb{N}^*$ számot **pszeudoprímszám**nak nevezzük, ha n összetett és $2^n \equiv 2 \pmod{n}$.
b) Az $n \in \mathbb{N}^*$ számot **Carmichael-szám**nak nevezzük, ha n összetett és ha az $a^n \equiv a \pmod{n}$ kongruencia igaz minden $a \in \mathbb{Z}$ számra.

6.2.8. tétel. *Végtelen sok pszeudoprímszám létezik.*

Bizonyítás. Igazoljuk, hogy ha n pszeudoprím, akkor $2^n - 1$ is pszeudoprím. Valóban, ha n összetett, akkor $2^n - 1$ is összetett; mivel $2^n \equiv 2 \pmod{n}$, legyen $2^n - 2 = nq$, ahonnan

$$2^{2^n-1} - 2 = 2(2^{2^n-2} - 1) = 2(2^{nq} - 1) = 2((2^n)^q - 1)$$

osztható $2^n - 1$-gyel. Tehát az $(a_n)_{n\geq 1}$, $a_1 = 341$, $a_{n+1} = 2^{a_n} - 1$, $n \geq 1$ szigorúan növekvő számsorozat minden tagja pszeudoprímszám. ■

Az első páros pszeudoprím $n = 161038$, ezt D.H. Lehmer találta 1950-ben. N.G.W.H. Beeger igazolta, hogy végtelen sok páros pszeudoprímszám van.

6.2.9. tétel. *Ha* $n = q_1 q_2 \ldots q_k$, *ahol* $k \geq 2$, q_i *különböző prímszámok és* $q_i - 1 \mid n - 1$, $i = 1, 2, \ldots, k$, *akkor* n *Carmichael-szám.*

Bizonyítás. Fermat-tétele szerint, ha $q_i \nmid a$, akkor $a^{q_i - 1} \equiv 1 \pmod{q_i}$, ahonnan $a^{n-1} = a^{k_i(q_i-1)} \equiv 1 \pmod{q_i}$; innen $a^n \equiv a \pmod{q_i}$; ez a kongruencia igaz $q_i \mid a$ esetén is, minden $i \in \{1, 2, \ldots, k\}$-ra. Innen $a^n \equiv a \pmod{n}$ minden $a \in \mathbb{Z}$ esetén. ■

A 341 nem Carmichael-szám, mert $11^{341} \not\equiv 11 \pmod{341}$. (Valóban, könnyen belátható, hogy $11^{341} - 11 \equiv -18 \pmod{31}$.) A legkisebb Carmichael-számok az $561 = 3 \cdot 11 \cdot 17$, $1105 = 5 \cdot 13 \cdot 17$, $1729 = 7 \cdot 13 \cdot 19$, $2465 = 5 \cdot 17 \cdot 29$, $2821 = 7 \cdot 13 \cdot 31$. 1992-ben R. Alford, A. Granville és C. Pomerance bebizonyították, hogy végtelen sok Carmichael-szám létezik.

6.2.10. példa (Fermat-számok). a) Az $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$ sorozat tagjai páronként relatív prímek. Valóban, legyen $n, m \in \mathbb{N}$, $m < n$ és $d \in \mathbb{N}$, $d \mid F_n$, $d \mid F_m$. Akkor

$$F_n - 2 = 2^{2^n} - 1 = (2^{2^{n-1}} + 1)(2^{2^{n-1}} - 1) = \cdots = F_{n-1}F_{n-2}\ldots F_m(2^{2^m} - 1) = kF_m,$$

tehát $d \mid 2$. De az F_n számok páratlanok, így $d = 1$.

b) $641 \mid F_5$. Valóban, $641 = 640 + 1 = 5 \cdot 2^7 + 1$, így $5 \cdot 2^7 \equiv -1 \pmod{641}$; negyedik hatványra emelve: $5^4 \cdot 2^{28} \equiv 1 \pmod{641}$. Másrészt, $641 = 625 + 16 = 5^4 + 2^4$, ahonnan $2^4 \equiv -5^4 \pmod{641}$. Összeszorozva a két kongruenciát következik, hogy $5^4 \cdot 2^{32} \equiv -5^4 \pmod{641}$; mivel $(5^4, 641) = 1$, kapjuk, hogy $2^{32} + 1 = 2^{2^5} + 1 \equiv 0 \pmod{641}$.

c) Minden $F_n, n \in \mathbb{N}$ szám prím vagy pszeudoprím, azaz $2^{F_n} \equiv 2 \pmod{F_n}$. Valóban,

$$2^{F_n} - 2 = 2(2^{F_n - 1} - 1) = 2(2^{2^{2^n}} - 1) = 2(F_{2^n} - 2) = 2kF_n$$

minden $n \in N$-re, ahol $2^n > n$.

6.2.3. A kínai maradéktétel

6.2.11. tétel (A kínai maradéktétel). *Legyenek* $n_1, \dots, n_r \in \mathbb{N}^*$, $(n_i, n_j) = 1$, $1 \le i, j \le r$, $i \ne j$. *Akkor*

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r} \simeq \mathbb{Z}_{n_1 \cdots n_r}.$$

Bizonyítás. Legyen $f : \mathbb{Z} \to \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$ $f(a) = ([a]_{n_1}, \dots, [a]_{n_r})$. Igazoljuk, hogy f gyűrűmorfizmus:

$$\begin{aligned} f(a+b) &= ([a+b]_{n_1}, \dots, [a+b]_{n_r}) = ([a]_{n_1} + [b_{n_1}], \dots, [a]_{n_r} + [b]_{n_r}) = \\ &= ([a]_{n_1}, \dots, [a]_{n_r}) + ([b]_{n_1}, \dots, [b]_{n_r}) = f(a) + f(b) \\ f(ab) &= ([ab]_{n_1}, \dots, [ab]_{n_r}) = ([a]_{n_1}[b_{n_1}], \dots, [a]_{n_r}[b]_{n_r}) = \\ &= ([a]_{n_1}, \dots, [a]_{n_r})([b]_{n_1}, \dots, [b]_{n_r}) = f(a)f(b) \end{aligned}$$

Meghatározzuk a $\operatorname{Ker} f$-et:

$$\begin{aligned} \operatorname{Ker} f &= \{a \in \mathbb{Z} \mid f(a) = ([a]_{n_1}, \dots, [a]_{n_r}) = ([0]_{n_1}, \dots, [0]_{n_r})\} = \\ &= \{a \in \mathbb{Z} \mid n_i | b,\ i = 1, \dots, r\} = \\ &= \{a \in \mathbb{Z} \mid n_1 \dots n_r | a\} = n_1 \dots n_r \mathbb{Z}. \end{aligned}$$

Az I. izomorfizmustételből, következik, hogy létezik az

$$\bar{f} : \mathbb{Z}/\operatorname{Ker} f \longrightarrow \operatorname{Im} f, \quad \bar{f}([a]_{n_1 \cdot \dots \cdot n_r}) = f(a) = ([a]_{n_1}, \dots, [a]_{n_r})$$

izomorfizmus, ahol $\mathbb{Z}/\operatorname{Ker} f = \mathbb{Z}_{n_1 \dots n_r}$ és $\operatorname{Im} f \subseteq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$. Végül, az $\bar{f}$ szürjektívitását igazoljuk két módszerrel.

(1) Mivel $|\mathbb{Z}_{n_1 \dots n_r}| = n_1 \dots n_r$ és $\bar{f}$ bijektív függvény következik, hogy $|\operatorname{Im} f| = n_1 \dots n_r$. De $\operatorname{Im} f \subseteq \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$, és $|\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}| = n_1 \dots n_r$, tehát $\operatorname{Im} f = \mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}$.

(2) A fenti függvény bijektivítása egyenértékű azzal, hogy bármely $a_1, \dots, a_r \in \mathbb{Z}$ esetén az

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \quad\vdots \\ x \equiv a_r \pmod{n_r} \end{cases}$$

kongruenciarendszernek van megoldása $\mathbb{Z}$-ben és bármely két megoldás kongruens modulo $n_1 \cdots n_r$.

A kongruenciarendszer megoldása. A következő jelöléseket vezetjük be: $N := n_1 \cdots n_r$, $M_i := \frac{N}{n_i}$. Itt $(M_i, n_i) = 1$ mert $(n_i, n_j) = 1$ minden $i \ne j$ esetén. Következik, hogy létezik $u_i \in \mathbb{Z}$ úgy, hogy

$$M_i u_i \equiv 1 \pmod{n_i}$$

(u_i meghatározható az Euklidészi algoritmussal). Legyen

$$x := \sum_{i=1}^{r} a_i M_i u_i.$$

Ekkor $x \equiv a_i \pmod{n_i}$, mert $M_j \equiv 0 \pmod{n_i}$, ha $j \ne i$. Tehát x az egyetlen megoldás $\bmod N$. ■

6.2.12. következmény. *Feltételezzük, hogy* $n_1, \dots, n_r \in \mathbb{N}^*$ *páronként relatív prímek. Akkor*

$$U(\mathbb{Z}_{n_1 \cdot \dots \cdot n_r}) \simeq U(\mathbb{Z}_{n_1}) \times \cdots \times U(\mathbb{Z}_{n_r}).$$

Bizonyítás. A kínai maradéktételből következik, hogy

$$(U(\mathbb{Z}_{n_1 \cdot \dots \cdot n_r}), \cdot) \simeq (U(\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r}), \cdot) = (U(\mathbb{Z}_{n_1}) \times \cdots \times U(\mathbb{Z}_{n_r})). \qquad ■$$

6.2.13. következmény. *Ha* $(m,n)=1$, *akkor* $\varphi(mn)=\varphi(m)\varphi(n)$, *azaz* φ *multiplikatív számelméleti függvény. Általánosan, ha* $(n_i,n_j)=1, 1\le i<j\le r$, *akkor* $\varphi(n_1\cdot\dots\cdot n_r)=\varphi(n_1)\cdots\varphi(n_r)$.

6.55. feladat. Oldjuk meg a következő kongruenciarendszereket:

$$\text{a)}\begin{cases} x\equiv 2 \pmod 3\\ x\equiv 3 \pmod 5\\ x\equiv 5 \pmod 7\end{cases};\qquad \text{b)}\begin{cases} x\equiv 3 \pmod 4\\ x\equiv 4 \pmod 5\\ x\equiv 6 \pmod 7\end{cases};\qquad \text{c)}\begin{cases} x\equiv 2 \pmod 3\\ x\equiv 4 \pmod 5\\ x\equiv 6 \pmod 7\\ x\equiv 8 \pmod{16}\end{cases}.$$

6.2.4. Magasabbfokú kongruenciák

Legyen $m=p_1^{a_1}\dots p_r^{a_r}$ egy egész szám és $f\in\mathbb{Z}[X]$ egy n-ed fokú polinom. Tekintsük az

$$f(x)\equiv 0 \pmod m \tag{6.1}$$

kongruenciát. A következő állítás visszavezeti a (6.1) kongruenciát prímhatványmodulusú kongruenciákra.

6.56. feladat. a) $\exists\, x\in\mathbb{Z}$ úgy, hogy $f(x)\equiv 0 \pmod m \Leftrightarrow \exists\, x\in\mathbb{Z}$ úgy, hogy

$$\begin{cases} f(x)\equiv 0 \pmod{p_1^{a_1}}\\ \dots\\ f(x)\equiv 0 \pmod{p_r^{a_r}}\end{cases}.$$

b) Jelöljük N_i-vel az $f(x)\equiv 0 \pmod{p_i^{a_i}}$ kongruencia megoldásainak a számát, és N-el az $f(x)\equiv 0 \pmod m$ kongruencia megoldásainak a számát. Igazoljuk, hogy $N=N_1N_2\dots N_r$.

Ha $m=p$ prímszám, akkor vegyük észre, hogy a Fermat-tétel szerint, a (6.1) kongruencia ekvivalens az $r(x)\equiv 0 \pmod p$ kongruenciával, ahol r az f polinom $g=X^p-X$ polinommal való osztási maradéka. Tehát elég tárgyalni a legfeljebb $(p-1)$-edfokú modulo p kongruenciákat.

6.57. feladat. Oldjuk meg a $3x^{13}+4x^{11}+4x^6+2x^3+3x^2+2x+1\equiv 0 \pmod 5$ kongruenciát.

A következő tétel módszert ad prímhatványmodulusú kongruencia megoldására.

6.2.14. tétel. *Legyenek az* $f(x)\equiv 0 \pmod{p^a}$ *kongruencia megoldásai* $x_1,x_2,\dots,x_k$. *Minden* x_i *megoldás az* $f(x)\equiv 0 \pmod{p^{a+1}}$ *kongruenciának*

a) *egy megoldását származtatja ha* $f'(x_i)\not\equiv 0 \pmod p$, *és ez* $x_i+t_ip^a$, *ahol* t_i *az*

$$f'(x_i)t\equiv -\frac{f(x_i)}{p^a} \pmod p,$$

t*-ben elsőfokú kongruencia egyedüli megoldása,*

b) p *megoldását származtatja ha* $f'(x_i)\equiv -\frac{f(x_i)}{p^a}\equiv 0 \pmod p$, *és ezek* $x_i, x_i+p^a, x_i+2p^a,\dots,x_i+(p-1)p^a$.

Az így nyert megoldások inkongruensek modulo p^{a+1}, *és megadják az* $f(x)\equiv 0 \pmod{p^{a+1}}$ *összes megoldását.*

Bizonyítás. Ha x megoldása az $f(x)\equiv 0 \pmod{p^{a+1}}$ kongruenciának, akkor x megoldása $f(x)\equiv 0 \pmod{p^a}$-nak is, tehát $x=x_i+tp^a$ alakú. A t értékeket kell meghatároznuk úgy, hogy $f(x_i+tp^a)\equiv 0 \pmod{p^{a+1}}$ legyen. Használjuk a Taylor-képletet:

$$f(x+y)=f(x)+\frac{y}{1!}f'(x)+\frac{y^2}{2!}f''(x)+\dots+\frac{y^n}{n!}f^{(n)}(x).$$

Kapjuk, hogy

$$f(x_i+tp^a)\equiv f(x_i)+p^atf'(x_i)\equiv 0 \pmod{p^{a+1}},$$

ahol $p^a\mid f(x_i)$, tehát

$$f'(x_i)t\equiv -\frac{f(x_i)}{p^a} \pmod p,$$

mely t-ben elsőfokú kongruencia. Tekintsük a kővetkező eseteket:

- Ha $f'(x_i)\not\equiv 0 \pmod p$, akkor ennek 1 megoldása van: $t=t_i$,
- Ha $f'(x_i)\equiv 0 \pmod p$, $\frac{f(x_i)}{p^a}\not\equiv 0 \pmod p$, akkor nincs megoldás,

- Ha $f'(x_i) \equiv \frac{f(x_i)}{p^a} \equiv 0 \pmod p$, akkor p megoldás van, s ezek $t_i = 0, 1, 2, \ldots, p-1$, s az adott p^{a+1} modulusú kongruencia megoldásai $x_i, x_i + p^a, x_i + 2p^a, \ldots, x_i + (p-1)p^a$, melyek inkongruensek modulo p^{a+1}.

Végül, két különböző x_i és x_j megoldásból kiindulva különböző megoldások származnak. Valóban, ha $x_i + t_i p^a \equiv x_j + t_j p^a \pmod{p^{a+1}}$ lenne, akkor $x_i \equiv x_j \pmod{p^a}$, ami ellentmondás. ■

6.2.15. példa. 1) Oldjuk meg az $f(x) = x^2 + x + 7 \equiv 0 \pmod{7^3}$ kongruenciát.

Az $f(x) = x^2 + x + 7 \equiv 0 \pmod 7$ kongruencia megoldásai $x_1 = 0$, $x_2 = -1$. $f'(x) = 2x + 1$, $f(0) = 7$, $f'(0) = 1$, $f(-1) = 7$, $f'(-1) = -1$. Képezzük a $t \equiv -1 \pmod 7$ és $-t \equiv -1 \pmod 7$ kongruenciákat, melyek megoldásai $t_1 = -1$ és $t_2 = 1$. Innen az $f(x) \equiv 0 \pmod{7^2}$ megoldásai $x_1 + 7t_1 = -7$ és $x_2 + 7t_2 = 6$.

Hasonlóképpen, $f(-7) = 49$, $f'(-7) = -13$, $f(6) = 49$, $f'(6) = 13$. Képezzük a $-13t \equiv -1 \pmod 7$ és $13t \equiv -1 \pmod 7$ kongruenciákat, melyek megoldásai $t_1' = -1$ és $t_2' = 1$. Kapjuk az $f(x) \equiv 0 \pmod{7^3}$ megoldásait: $x \equiv -56 \pmod{7^3}$ és $x \equiv 55 \pmod{7^3}$.

2) Oldjuk meg az $f(x) = x^2 + x + 7 \equiv 0 \pmod{3087}$ kongruenciát.

Mivel $3087 = 3^2 \cdot 7^3$, először megoldjuk az $f(x) \equiv 0 \pmod{3^2}$ és $f(x) \equiv 0 \pmod{7^3}$ kongruenciákat, melynek megoldásai $x \equiv 1, 4, -2 \pmod{3^2}$ illetve $x \equiv -56, 55 \pmod{7^3}$. Így az eredeti kongruenciának $2 \cdot 3 = 6$ megoldása van, ezek meghatározásához meg kell oldanunk 6 kongruenciarendszert. A megoldások: $x \equiv 55, -56, 973, -974, 1084, -1085 \pmod{3087}$.

6.58. feladat. Oldjuk meg az $f(x) = x^4 + 36X^3 + 16x^2 + 8x - 6 \equiv 0 \pmod{875}$ kongruenciát.

6.2.5. Az $(U(\mathbb{Z}_m), \cdot)$ csoport struktúrája

Tudjuk, hogy ha $m \geq 2$, a $\mathbb{Z}_m = \left\{\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}\right\}$ gyűrű kommutatív. Jelölje $U(\mathbb{Z}_m)$ a $\mathbb{Z}_m$ invertálható elemeinek halmazát; ekkor

$$U(\mathbb{Z}_m) = \{\hat{a} \in \mathbb{Z}_m \mid (a, m) = 1\}$$

és $(U(\mathbb{Z}_m), \cdot)$ Ábel csoport. Az $U(\mathbb{Z}_m)$ rendje $|U(\mathbb{Z}_m)| = \varphi(m)$, ahol $\varphi : \mathbb{N}^* \to \mathbb{N}$ az Euler-függvény.

Tudjuk, hogy a $(\mathbb{Z}_m, +)$ csoport ciklikus: $\mathbb{Z}_m = \langle \hat{1} \rangle = \left\{k \cdot \hat{1} \mid k \in \mathbb{Z}\right\}$. A továbbiakban azt tanulmányozuk, hogy az $(U(\mathbb{Z}_m), \cdot)$ csoport milyen esetben lesz ciklikus.

6.2.16. definíció. Legyen $a \in \mathbb{Z}$, $(a, m) = 1$, tehát $\hat{a} \in U(\mathbb{Z}_m)$. Ekkor

$$o_m(a) := \operatorname{ord}(\hat{a}) \quad (\text{az } U(\mathbb{Z}_m) \text{ csoportban})$$

az a egész szám **multiplikatív rendje** modulo m.

6.2.17. lemma (Az $o_m(a)$ tulajdonságai). a) $o_m(a) \mid \varphi(m)$.

b) $a^j \equiv a^l \pmod m \iff j \equiv l \pmod{o_m(a)}$.

c) *Ha* $o_m(a) = h \in \mathbb{N}^*$, *akkor* $o_m(a^k) = \frac{h}{(h,k)}$, $\forall k \in \mathbb{Z}$.

Bizonyítás. a) következik a Lagrange-tételből és abból, hogy $|U(\mathbb{Z}_m)| = \varphi(m)$.

b) $a^j \equiv a^l \pmod m \Leftrightarrow \hat{a}^j = \hat{a}^k$ $U(\mathbb{Z}_m)$-ben $\Leftrightarrow \hat{a}^{j-k} = \hat{1} \Leftrightarrow o_m(a) \mid j - k \Leftrightarrow j \equiv k \pmod{o_m(a)}$.

c) következik az 3. fejezet 3.26 c) feladatból.

6.2.18. tétel (Főtétel). *Legyen* $m \in \mathbb{N}^*, m = p_1^{n_1} \cdot \cdots \cdot p_r^{n_r}, p_i$ *prímek,* $n_i \in \mathbb{N}^*, r \geq 1$.

a) $(U(\mathbb{Z}_m), \cdot) \simeq (U(\mathbb{Z}_{p_1^{n_1}}) \times \cdots \times U(\mathbb{Z}_{p_r^{n_r}}), \cdot)$.

b) *Ha* $p > 2$ *prímszám,* $n \in \mathbb{N}^*$, *akkor* $U(\mathbb{Z}_{p^n})$ *ciklikus csoport.*

c) *Ha* $n \geq 3$, *akkor*

$$U(\mathbb{Z}_{2^n}) = \langle \hat{5} \rangle \times \langle \widehat{-1} \rangle,$$

ahol $o_{2^n}(5) = 2^{n-2}$, $o_{2^n}(-1) = 2$, $\langle -\hat{1} \rangle = \{\hat{1}, -\hat{1}\}$, $\langle \hat{5} \rangle = \{\hat{1}, \hat{5}, \ldots, \hat{5}^{2^{n-2}-1}\}$ *(tehát a csoport nem ciklikus).*

A 5.4.4 tételben már bebizonyítottuk az egyik esetet:

6.2.19. tétel. *Ha* p *prímszám, akkor* $\left(\mathbb{Z}_p^*, \cdot\right)$ *ciklikus csoport.*

Tekintsünk először néhány példát.

6.2.20. példa. 1) Legyen $m = p$ prímszám:

$m = 2$ $\quad U(\mathbb{Z}_2) = \{\hat{1}\} = \langle\hat{1}\rangle$
$m = 3$ $\quad U(\mathbb{Z}_3) = \{\hat{1}, \hat{2}\} = \langle\hat{2}\rangle$
$m = 4$ $\quad U(\mathbb{Z}_4) = \{\hat{1}, \hat{3}\} = \langle\hat{3}\rangle$
$m = 5$ $\quad U(\mathbb{Z}_5) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}\} = \langle\hat{2}\rangle$
$m = 6$ $\quad U(\mathbb{Z}_6) = \{\hat{1}, \hat{5}\}$
$m = 7$ $\quad U(\mathbb{Z}_7) = \{\hat{1}, \hat{2}, \hat{3}, \hat{4}, \hat{5}, \hat{6}\} = \langle\hat{3}\rangle$

2) Legyen $m = 9 = 3^2$ (tehát a b) esetben vagyunk). $U(\mathbb{Z}_9) = \{\hat{1}, \hat{2}, \hat{4}, \hat{5}, \hat{7}, \hat{8}\}$, $\varphi(9) = 3^2 - 3 = 6$; $\langle\hat{2}\rangle = \{\hat{1}, \hat{2}, \hat{4}, \hat{8}, \hat{7}, \hat{5}\} = U(\mathbb{Z}_9) \Rightarrow o_9(2) = 6 = \varphi(9)$

Láttuk, hogy $\langle\hat{2}^k\rangle = U(\mathbb{Z}_9) \Leftrightarrow (k, \varphi(9)) = 1 \Leftrightarrow k \in \{1, 5\} \Leftrightarrow \hat{2}^k \in \{\hat{2}, \hat{5}\}$.

3) Legyen $m = 8 = 2^3$ (tehát a b) esetben vagyunk). $G = U(\mathbb{Z}_8) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}\} = \{\hat{1}, \hat{5}, -\hat{1}, -\hat{5}\} = \{\hat{1}, \hat{5}\} \times \{\hat{1}, -\hat{1}\} = H \times K$. $\operatorname{ord}(\hat{1}) = 1$, $\operatorname{ord}(\hat{3}) = 2$, $\operatorname{ord}(\hat{5}) = 2$, $\operatorname{ord}(\hat{7}) = 2$; $K \cap H = \{\hat{1}\}$, $H \cdot K = G$. G nem ciklikus, mert nem tartalmaz 4-ed rendű elemeket.

4) Legyen $m = 16 = 2^4$. $U(\mathbb{Z}_{16}) = \{\hat{1}, \hat{3}, \hat{5}, \hat{7}, \hat{9}, \widehat{11}, \widehat{13}, \widehat{15}\}$, $\varphi(16) = 2^4 - 2^3 = 8$; $H := \langle -\hat{1}\rangle = \{\hat{1}, -\hat{1}\} \Rightarrow o_{16}(-1) = 2$; $K := \langle\hat{5}\rangle = \{\hat{1}, \hat{5}, \hat{9}, \widehat{13}\} \Rightarrow o_{16}(5) = 4 = 2^{4-2}$;

$H \cap K = \{\hat{1}\}$; $\forall \hat{x} \in U(\mathbb{Z}_{16})\ \exists!(\hat{y}, \hat{z}) \in H \times K$ úgy, hogy $\hat{x} = \hat{y}\hat{z}$, és így $U(\mathbb{Z}_{16}) = \{\hat{1}, \hat{5}, \hat{9}, \widehat{13}, -\hat{1}, -\hat{5}, -\hat{9}, \widehat{-13}\}$.

6.2.21. lemma (Főlemma). *Legyen* $k \in \mathbb{N}$

a) *Ha* $p > 2$ *prímszám, akkor* $(1+p)^{p^k} \equiv 1 + p^{k+1} \pmod{p^{k+2}}$.

b) $5^{2^k} \equiv 1 + 2^{k+2} \pmod{2^{k+3}}$.

Bizonyítás. k szerinti indukciót alkalmazunk. A $k = 1$ esetet az olvasóra bizzuk.

a) Legyen $k \geq 1$, és feltételezzük, hogy

$$(1+p)^{p^k} = 1 + p^{k+1} + bp^{k+2},$$

ahol $b \in \mathbb{Z}$. Akkor

$$\begin{aligned}(1+p)^{p^{k+1}} = ((1+p)^{p^k})^p = (1 + p^{k+1} + bp^{k+2})^p &\equiv 1 + p^{k+2} + bp^{k+3} \pmod{p^{2k+2}}\\ &\equiv 1 + p^{k+2} \pmod{p^{k+3}},\end{aligned}$$

mert $2k + 2 \geq k + 3$.

b) Legyen $k \geq 1$, és feltételezzük, hogy

$$5^{2^k} = 1 + 2^{k+2} + cp^{k+3},$$

ahol $c \in \mathbb{Z}$. Akkor

$$\begin{aligned}5^{2^{k+1}} = (5^{2^k})^2 = (1 + 2^{k+2} + c2^{k+3})^2 &\equiv 1 + 2^{k+3} + c2^{k+4} \pmod{2^{2k+4}}\\ &\equiv 1 + 2^{k+3} \pmod{2^{k+4}},\end{aligned}$$

mert $k + 4 \leq 2k + 4$. ■

A fötétel bizonyítása

a) Következik a kínai maradéktételből, mert $(p_i^{k_i}, p_j^{k_j}) = 1$, ha $i \neq j$.

b) Tudjuk, hogy $|U(\mathbb{Z}_{p^n})| = \varphi(p^n) = p^n - p^{n-1} = p^{n-1}(p-1)$. Igazoljuk, hogy létezik $\hat{x} \in U(\mathbb{Z}_{p^n})$ úgy, hogy $o_{p^n}(x) = p^n - p^{n-1} = |U(\mathbb{Z}_{p^n})| = \varphi(p^n)$; ekkor $\langle\hat{x}\rangle = U(\mathbb{Z}_{p^n}) = \{\hat{1}, \hat{x}, \hat{x}^2, \ldots, \hat{x}^{\varphi(p^n)-1}\}$.

Vegyük észre, hogy $(p^{n-1}, p-1)$ relatív prímek: $(p^{n-1}, p-1) = 1$. Keressük az $\alpha, \beta \in U(\mathbb{Z}_{p^n})$ elemeket úgy, hogy $\operatorname{ord}(\alpha) = p^{n-1}$, $\operatorname{ord}(\beta) = p - 1$, mert akkor $\operatorname{ord}(\alpha\beta) = p^{n-1}(p-1)$ tehát $\langle\alpha\beta\rangle = U(\mathbb{Z}_{p^n})$.

Legyen $\alpha := \widehat{1+p} \in \mathbb{Z}_{p^n}$. Mivel $(p^n, 1+p) = 1 \Rightarrow \alpha \in U(\mathbb{Z}_{p^n})$. A főlemma a) pontjából következik:

$$(1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^{n+1}} \Rightarrow (1+p)^{p^{n-1}} \equiv 1 + p^n \pmod{p^n} \Rightarrow$$

$$\Rightarrow (1+p)^{p^{n-1}} \equiv 1 \pmod{p^n} \Rightarrow \alpha^{p^{n-1}} \equiv \hat{1} \quad U(\mathbb{Z}_{p^n})\text{-ben} \Rightarrow \operatorname{ord}(\alpha) \mid p^{n-1}.$$

Tehát ha $\operatorname{ord}(\alpha) \neq p^{n-1}$, akkor $\alpha^{p^{n-2}} = \hat{1}$. A főlemma a) pontjából kapjuk, hogy

$$(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \pmod{p^n} \Rightarrow (1+p)^{p^{n-2}} \not\equiv 1 \pmod{p^n},$$

mert $p^n \nmid p^{n-1}$. Tehát $\operatorname{ord}(\alpha) \nmid p^{n-2}$, ahonnan $\operatorname{ord}(\alpha) = p^{n-1}$.

Tudjuk, hogy $(\mathbb{Z}_p^*, \cdot)$ ciklikus csoport. Legyen $\mathbb{Z}_p^* = \langle \bar{b} \rangle$, ahol $1 \le b < p$, $\bar{b} = [b]_p$ és $o_p(b) = p-1$. Legyen $\hat{b} := [b]_{p^n}$. Mivel $p \nmid b$, következik, hogy $(p^n, b) = 1$, tehát $\hat{b} \in U(\mathbb{Z}_{p^n})$.

$$b^{o_{p^n}(b)} \equiv 1 \pmod{p^n} \Rightarrow b^{o_{p^n}(b)} \equiv 1 \pmod{p} \Rightarrow \operatorname{ord}(b) \mid o_{p^n(b)} \Rightarrow p-1 \mid o_{p^n}(b);$$

de $o_{p^n}(b) \mid |U(\mathbb{Z}_{p^n})| = p^{n-1}(p-1) \Rightarrow o_{p^n}(b) = (p-1)N$, ahol $(p-1)N \mid (p-1)p^{n-1}$, tehát $o_{p^n}(b) = (p-1)p^s$, ahol $0 \le s \le n-1$.

Legyen $\beta := \hat{b}^{p^{n-1}} \in U(\mathbb{Z}_{p^n})$. Akkor

$$\operatorname{ord}(\beta) = \frac{\operatorname{ord}(\hat{b})}{(\operatorname{ord}(\hat{b}), p^{n-1})} = \frac{(p-1)p^s}{((p-1)p^s, p^{n-1})} = \frac{(p-1)p^s}{p^s} = (p-1).$$

c) A főlemma b) pontját alkalmazva

$$5^{2^{n-2}} \equiv 1 + 2^n \pmod{2^{n+1}} \Longrightarrow 5^{2^{n-2}} \equiv 1 \pmod{2^n} \Longrightarrow o_{2^n}(5) \mid 2^{n-2}.$$

Ha $o_{2^n}(5) \ne 2^{n-2}$, akkor $5^{2^{n-3}} \equiv 1 \pmod{2^n}$. A főlemmá b) pontjából kapjuk, hogy

$$5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n} \Longrightarrow 5^{2^{n-3}} \not\equiv 1 \pmod{2^n},$$

mert $2^n \nmid 2^{n-1}$. Tehát $\langle \hat{5} \rangle = \{\hat{5}^k \mid 0 \le k < 2^{n-2}\} < U(\mathbb{Z}_{2^n})$, mert $|U(\mathbb{Z}_{2^n})| = \varphi(2^n) = 2^n - 2^{n-1} = 2^{n-1}$. Elég igazolni, hogy

$$\varphi : \langle \hat{5} \rangle \times \langle -\hat{1} \rangle \to U(\mathbb{Z}_{2^n}), \quad \varphi(\hat{y}, \hat{z}) = \hat{y}\hat{z}$$

csoportizomorfizmus. Tudjuk, hogy φ csoportmorfizmus. Továbbá

– φ injektív $\Leftrightarrow \langle \hat{5} \rangle \cap \langle -\hat{1} \rangle = \{\hat{1}\}$;

– ha igazoljuk, hogy φ injektív, akkor φ szürjektív is, mert mindkét halmaznak 2^{n-1} eleme van.

Tehát elég igazolni, hogy $\langle \hat{5} \rangle \cap \langle -\hat{1} \rangle = \{\hat{1}\}$, azaz igazoljuk, hogy $-\hat{1} \notin \{\hat{1}, \hat{5}, \hat{5}^2, \dots, \hat{5}^{2^{n-2}-1}\}$. Tegyük fel, hogy létezik k úgy, hogy $0 \le k < 2^{n-2}$ és $\hat{5}^k = -\hat{1}$, azaz $5^k \equiv -1 \pmod{2^n}$. Négyzetreemeléssel

$$5^{2k} \equiv 1 \pmod{2^n} \Longrightarrow o_{2^n}(5) = 2^{n-2} \mid 2k \Longrightarrow 2^{n-3} \mid k \Longrightarrow k = 2^{n-3}l < 2^{n-2},$$

tehát $l = 1$, ahonnan $k = 2^{n-3}$. Alkalmazva a főlemma b) pontját,

$$-1 \equiv 5^{2^{n-3}} \equiv 1 + 2^{n-1} \pmod{2^n} \Rightarrow 2^n \mid 2 + 2^{n-1},$$

ami lehetetlen, ha $n \ge 3$. ■

6.2.22. következmény. $U(\mathbb{Z}_m)$ *ciklikus csoport* $\Leftrightarrow m = 2, 4, p^n, 2p^n$, *ahol* $p > 2$ *prímszám,* $n \in \mathbb{N}^*$.

Bizonyítás. Legyen $m = 2^k p_1^k \cdot \dots \cdot p_r^{k_r}$, ahol p_i páratlan prímszámok $k_i \in \mathbb{N}^*$, $r \in \mathbb{N}$, $k \in \mathbb{N}$, $m \ge 2$.

„$\Leftarrow$" Az $m = 2$, $m = 4$ eseteket már megvizsgáltuk. Az $m = p^n$ eset a főtétel b) pontjából következik.

Ha $m = 2p^n$, akkor léteznek a következő csoportizomorfizmusok:

$$U(\mathbb{Z}_m) \simeq U(\mathbb{Z}_2) \times U(\mathbb{Z}_{p^n}) = \{[1]_2\} \times U(\mathbb{Z}_{p^n}) \simeq U(\mathbb{Z}_{p^n}), \quad ([1]_2, [x]_{p^n}) \mapsto [x]_{p^n}.$$

Tehát ciklikus. Pontosabban, ha $\langle [x]_{p^n} \rangle = U(\mathbb{Z}_{p^n})$, akkor $\langle [x]_{2p^n} \rangle = U(\mathbb{Z}_{2p^n})$ feltéve, hogy $(x, 2p^n) = 1$, azaz $2 \nmid x$.

„$\Rightarrow$" Láttuk, hogy

$$U(\mathbb{Z}_m) \simeq U(\mathbb{Z}_{2^k}) \times U(\mathbb{Z}_{p_1^{n_1}}) \times \dots \times U(\mathbb{Z}_{p_r^{k_r}}).$$

Ha $k \ge 3$, akkor az 6.2.18 tétel c) alpontjából következik, hogy $U(\mathbb{Z}_{2^k})$ nem ciklikus, mert $(|\langle \hat{5} \rangle|, |\langle -\hat{1} \rangle|) = 2 \ne 1$. Az 3.5.7. tétel alapján $U(\mathbb{Z}_m)$ sem ciklikus. Következik, hogy $k \le 2$.

Ha $k = 2$ és $r \ge 1$, azaz $k_1 \ge 1$, $m = 2^2 p_1^{k_1}$, akkor $(\varphi(2^2), \varphi(p_1^{k_1})) = (2^{2-1}, (p_1 - 1)p_1^{k_1 - 1}) = 2$, tehát az 3.5.7. tételből következik, hogy $U((Z)_m)$ nem ciklikus.

Tehát, ha $r \ge 1$, akkor $k = 0$ vagy $k = 1$, azaz $m = p_1^{k_1} \cdots p_r^{k_r}$ vagy $m = 2p_1^{k_1} \cdots p_r^{k_r}$. Ha $r \ge 2$, azaz $k_1, k_2 \ge 1$, $m = 2^k p_1^{k_1} p_2^{k_2} \cdots$, ahol $k \in \{0, 1\}$, akkor

$$(|U(\mathbb{Z}_{p_1^{k_1}})|, |U(\mathbb{Z}_{p_2^{k_2}})|) = (\varphi(p_1^{k_1}), \varphi(p_2^{k_2})) = ((p_1 - 1)p_1^{k_1 - 1}, (p_2 - 1)p_2^{k_2 - 1}) \vdots 2 \ne 1,$$

mert $p_1 - 1$ és $p_2 - 1$ párosak. Az 3.5.7 lemmából következik, hogy $U(\mathbb{Z}_m)$ nem ciklikus.

Tehát $m \in \{2, 4, p^k, 2p^k\}$. ■

6.2.6. Primitív gyökök és indexek

Célunk megoldani az $x^n \equiv a \pmod{n}$ kongruenciát. Ehhez bevezetjük a **diszkrét logaritmus** (index) fogalmát.

6.2.23. megjegyzés. Valós számok esetén, ha $a \in \mathbb{R}_+^* \setminus \{1\}$, akkor $\exp_a : (\mathbb{R}, +) \to (\mathbb{R}_+^*, \cdot)$, $x \mapsto a^x$, csoportizomorfizmus. E morfizmus inverze $\log_a : (\mathbb{R}_+^*, \cdot) \to (\mathbb{R}, +)$, azaz $a^x = b \Leftrightarrow x = \log_a b$, ahol $a \in \mathbb{R}_+^* \setminus \{1\}$, $b \in \mathbb{R}_+^*$.

6.2.24. definíció. Feltételezzük, hogy $(U(\mathbb{Z}_m), +)$ ciklikus csoport. Ha $g \in \mathbb{Z}$, $(g, m) = 1$ és $(U(\mathbb{Z}_m) = \langle \hat{g} \rangle = \{\hat{1}, \hat{g}, \hat{g}^2, \dots, \hat{g}^{\varphi(m)-1}\}$, akkor azt mondjuk, hogy g **primitív gyök** modulo m.

6.2.25. következmény. *Létezik primitív gyök modulo* m *akkor és csak akkor, ha* $m = 2, 4, p^n, 2p^n$, *ahol* $p > 2$ *prímszám és* $n \in \mathbb{N}^*$.

6.2.26. megjegyzés. Tudjuk, hogy ha létezik primitív gyök modulo m, akkor az (inkongruens) primitív gyökök száma $\varphi(\varphi(m))$ (mert ha $0 \le k \le \varphi(m)$ akkor $\langle \hat{g}^k \rangle = U(\mathbb{Z}_m) \Leftrightarrow (k, \varphi(m)) = 1$).

6.2.27. példa. Keressük a primitív gyököket modulo 11.

$\varphi(11) = 10$, $\varphi(\varphi(11)) = \varphi(10) = \varphi(2)\varphi(5) = (2-1)(5-1) = 4$; $U(\mathbb{Z}_{11}) = \{\hat{1}, \hat{2}, \dots, \widehat{10}\} = \mathbb{Z}_{11}^*$; $\hat{2}^0 = \hat{1}$, $\hat{2}^1 = \hat{2}$, $\hat{2}^2 = \hat{4}$, $\hat{2}^3 = \hat{8}$, $\hat{2}^4 = \hat{5}$, $\hat{2}^5 = \widehat{10}$, $\hat{2}^6 = \hat{9}$, $\hat{2}^7 = \hat{7}$, $\hat{2}^8 = \hat{3}$, $\hat{2}^9 = \hat{6}$, $\hat{2}^{10} = \hat{1}$, tehát $g = 2$ primitiv gyök modulo 11.

A primitív gyökök modulo 11: $2^k \mod 11$, ahol $k \in \{0, 1, 2, \dots, 10 \mid (k, 10) = 1\} = \{1, 3, 5, 7, 9\}$, tehát a primitív gyökök: $2, 8, 7, 6$.

6.59. feladat. Határozzuk meg a primitív gyököket

a) modulo $121 = 11^2$;
b) modulo 13 és modulo 17.
c) modulo $3, 9, 27, 18$.
e) modulo $5, 10, 25, 50$.
f) modulo $7, 14, 49$

6.60. feladat. 1) Keressünk primitív gyököket modulo $p = 41$.
2) Keressünk primitív gyököket modulo $p = 61$.
3) Keressünk primitív gyököket modulo $p = 67$.

Legyen g egy primitív gyök modulo m. Akkor $U(\mathbb{Z}_m) = \{\hat{1}, \hat{g}, \hat{g}^2, \dots, \hat{g}^{\varphi(m)-1}\}$, tehát minden $a \in \mathbb{Z}$ esetén úgy, hogy $(a, m) = 1$, létezik egyetlen olyan $j \in \{0, 1, \dots, \varphi(m) - 1\}$ úgy, hogy $\hat{a} = \hat{g}^j$, azaz $a \equiv g^j \pmod{m}$.

6.2.28. definíció. $j = \operatorname{ind}_a = \log_g a$ az a egész szám g alapú **index**e vagy **diszkrét logaritmus**a.

Tehát ha $i \in \mathbb{Z}$, akkor

$$g^i \equiv a \pmod{m} \Leftrightarrow \operatorname{ind}_a \equiv i \pmod{\varphi(m)},$$

mivel

$$g^i \equiv g^k \pmod{m} \Leftrightarrow i \equiv k \pmod{o_m(g)},$$

ahol $k = \operatorname{ind}_a$.

6.2.29. lemma (Az index tulajdonságai). *Legyen* $a, b \in \mathbb{Z}$, $(a, m) = (b, m) = 1$ *és feltételezzük, hogy* g *primitív gyök modulo* m.

0) $a \equiv b \pmod{m} \Leftrightarrow \operatorname{ind}_g a \equiv \operatorname{ind}_g(b) \pmod{\varphi(m)}$.
1) $\operatorname{ind}_a b \equiv \operatorname{ind}_g a + \operatorname{ind}_g b \pmod{\varphi(m)}$.
2) $\operatorname{ind}_g(a^k) \equiv k \operatorname{ind}_g(a) \pmod{\varphi(m)}$ *minden* $k \in \mathbb{Z}$ *esetén; Partikulárisan* $\operatorname{ind}_g a^{-1} \equiv -\operatorname{ind}_g a \pmod{\varphi(m)}$.
3) $o_m(a) = \frac{\varphi(m)}{(\operatorname{ind}_g a, \varphi(m))}$.

Bizonyítás. 0) Létezik egyetlen $i, j \in \{0, 1, \dots, \varphi(m) - 1\}$ úgy, hogy $a \equiv g^i \pmod{m}$, $b \equiv g^j \pmod{m}$. Akkor $a \equiv b \pmod{m} \Leftrightarrow g^i \equiv g^j \pmod{m} \Longleftrightarrow i \equiv j \pmod{\varphi_m(g)} \Leftrightarrow \operatorname{ind}_g a \equiv \operatorname{ind}_g b \pmod{\varphi(m)}$.

1) Legyen $\operatorname{ind}_g a = i \Leftrightarrow g^i \equiv a \pmod{m}$, $\operatorname{ind}_g b = j \Leftrightarrow g^j \equiv b \pmod{m}$; ekkor $ab \equiv g^{i+j} \pmod{m}$, vagyis $\operatorname{ind}_g(ab) \equiv i + j \mod \varphi(m)$.

2) Legyen $\operatorname{ind}_g a = i$, azaz $g^i \equiv a \pmod{m}$. Ekkor

$$a^k \equiv g^{ik} \pmod{m} \Leftrightarrow k \operatorname{ind}_a = ik \equiv \operatorname{ind}_g(a^k) \pmod{\varphi(m)}.$$

3) $o_m(a) = \operatorname{ord}(\hat{a}) = \operatorname{ord}(g^i) = \frac{\operatorname{ord}(\hat{g})}{(\operatorname{ord}(\hat{g}), i)} = \frac{\varphi(m)}{(\varphi(m), \operatorname{ind}_g a)}$. ■

6.2.30. példa. Indextábla $m = 11$, $g = 2$ esetén:

k	0	1	2	3	4	5	6	7	8	9
2^k	1	2	4	8	5	10	9	7	3	6

a	1	2	3	4	5	6	7	8	9	10
$\mathrm{ind}_2\, a$	0	1	8	2	4	9	7	3	6	5

6.61. feladat. Készítsünk indextáblát modulo 19. Határozzuk meg:
1) $12 \cdot 13$-nak a 19-el való osztási maradékát (index-táblával).
2) 9^{2074}-nek a 19-el való osztási maradékát (index-táblával).

6.62. feladat. Legyen $p > 2$ egy prímszám, $a \in \mathbb{Z}$. Igazoljuk, hogy ha $o_p(a) = 3$, akkor $o_p(a+1) = 6$.

6.63. feladat. Ha a primitív gyök modulo p^n $(n > 1, p > 2)$, akkor a primitív gyök modulo p.

6.2.7. Binom kongruenciák megoldása

Legyen $m \geq 2$, $a \in \mathbb{Z}$, $(a, m) = 1$, $m \in \mathbb{Z}$. tekintsük a következő feladatot: határozzuk meg az $x \in \mathbb{Z}$ számokat úgy

$$x^n \equiv a \pmod{m}$$

azaz

$$\hat{x}^n \equiv \hat{a} \quad U(\mathbb{Z}_m)\text{-ben.}$$

Ha x megoldás, mivel $(a, m) = 1$, következik, hogy $(x, m) = 1$.

6.2.31. definíció. Ha az $x^n \equiv a \pmod{m}$ kongruenciának van megoldása, akkor azt mondjuk, hogy az a szám n-edik **hatványmaradék** modulo m.

Megoldás primitív gyök létezése esetén

6.2.32. tétel. *Feltételezzük, hogy* $\exists\, g \in \mathbb{Z}$ *primitív gyök modulo* m. *Legyen* $a \in \mathbb{Z}$, $(a, m) = 1$, $n \in \mathbb{Z}$.
1) *Az* $x^n \equiv a \pmod{n}$ *kongruencia megoldásainak a száma*

$$\begin{cases} (n, \varphi(m), & \textit{ha } \frac{\varphi(m)}{a^{(n,\varphi(m))}} \equiv 1 \pmod{m} \\ 0, & \textit{ellenkező esetben, azaz ha } a^{\frac{\varphi(m)}{(n,\varphi(m))}} \equiv 1 \pmod{m} \end{cases}$$

2) *Az* n*-edik modulo* m *hatványmaradékok száma*

$$\frac{\varphi(m)}{(n, \varphi(m))} = |\{\hat{a} \in U(\mathbb{Z}_m) \mid \exists \hat{x} \in U(\mathbb{Z}_m) : \hat{x}^n = \hat{a}\}|.$$

Bizonyítás. 1) Feltételezzük, hogy $x \in \mathbb{Z}$ megoldása az $x^n \equiv a \pmod{m}$ kongruenciának; akkor

$$a^{\frac{\varphi(m)}{(n,\varphi(m))}} \equiv x^{n\frac{\varphi(m)}{(n,\varphi(m))}} \equiv (x^{\varphi(m)})^{\frac{n}{(n,\varphi(m))}} \equiv 1 \pmod{m},$$

tehát, ha $a^{\frac{\varphi(m)}{(m,\varphi(m))}} \not\equiv 1 \pmod{m}$ akkor nincs megoldás.

Fordítva, tételezzük fel, hogy $a^{\frac{\varphi(m)}{(m,\varphi(m))}} \equiv 1 \pmod{m}$. Legyen $j = \mathrm{ind}_g\, a$, azaz $j \in \{0, 1, \ldots, \varphi(m)-1\}$, $g^j \equiv a \pmod{m}$; ekkor a feltétel alapján

$$g^{j\frac{\varphi(m)}{(m,\varphi(m))}} \equiv 1 \pmod{m} \overset{o_m(g)=\varphi(m)}{\Longleftrightarrow} \varphi(m) \mid j\frac{\varphi(m)}{(n, \varphi(m))} \Leftrightarrow (n, \varphi(m)) \mid j = \mathrm{ind}_g\, a.$$

Minden x megoldás, ha létezik, $x \equiv g^j \mod m$ alakú, ahol $y \in \{0, 1, \ldots, \varphi(m) - 1\}$. Ekkor

$$x^n \equiv a \pmod{m} \Leftrightarrow g^{ny} \equiv g^j \pmod{m} \Leftrightarrow nj \equiv j \pmod{\varphi(m)},$$

tehát egy elsőfokú kongruenciához jutottunk, y ismeretlennel. Mivel $(n, \varphi(m)) \mid j$, következik, hogy létezik y megoldás, és a modulo $\varphi(m)$ inkongruens megoldások száma $(n, \varphi(m))$.

2) a n-edik hatványmaradék modulo $m \Leftrightarrow \exists\, x \in \mathbb{Z}$ úgy, hogy

$$x^n \equiv a \pmod{m} \Leftrightarrow a^{\frac{\varphi(m)}{(n,\varphi(m))}} \equiv 1 \pmod{m} \overset{\mathrm{ind}}{\Longleftrightarrow} \frac{\varphi(m)}{(n, \varphi(m))} \mathrm{ind}_g\, a \equiv 0 \pmod{\varphi(m)}.$$

j megoldás létezik, mert $(\varphi(m), \frac{\varphi(m)}{(n,\varphi(m))}) \mid 0$, és a modulo $\varphi(m)$ inkongruens j megoldások száma

$$(\varphi(m), \frac{\varphi(m)}{(n, \varphi(m))}) = \frac{\varphi(m)}{(n, \varphi(m))}.$$

6.2.33. példa. Oldjuk meg az $x^{12} \equiv 16 \pmod{17}$ kongruenciát. Keresünk primitív gyököket modulo 17, majd készítünk index-táblát. $\varphi(17) = 16$.

k	3^k
0	1
1	3
2	9
3	10
4	13
5	5
6	15
7	11
8	16
9	14
10	8
11	7
12	4
13	12
14	2
15	6

a	$\operatorname{ind}_3 a$
1	0
2	14
3	1
4	12
5	5
6	15
7	11
8	10
9	2
10	3
11	7
12	13
13	4
14	9
15	6
16	8

$$x^{12} \equiv 16 \pmod{17} \Leftrightarrow 12 \cdot \operatorname{ind}_3 x \equiv 8 \pmod{16}.$$

Legyen $y := \operatorname{ind}_3 x$;

$$12y \equiv 8 \pmod{16} \Leftrightarrow 3y \equiv 2 \pmod{4} \Leftrightarrow y = 2 \pmod{4}.$$

Tehát a $\bmod 16$ inkongruens megoldások: $y_0 = 2$, $y_1 = 6$, $y_2 = 10$, $y_3 = 14$. Innen

$$x_0 \equiv 3^{y_0} \equiv 9 \pmod{17},\ x_1 \equiv 3^{y_1} \equiv 15 \pmod{17},\ x_2 \equiv 3^{y_2} \equiv 8 \pmod{17},\ x_3 \equiv 3^{y_3} \equiv 2 \pmod{17}.$$

6.64. feladat. Oldjuk meg a következő kongruenciákat:
1) $5x^4 \equiv 3 \pmod{11}$;
2) $x^6 \equiv 3 \pmod{11}$;
3) $2x^5 \equiv 5 \pmod{13}$;
4) $8x^{26} \equiv 37 \pmod{41}$;
5) $x^{17} \equiv 37 \pmod{41}$;
6) $20^x \equiv 21 \pmod{41}$.

6.65. feladat. Határozzuk meg az n-edik hatványmaradékokat modulo 41, ha
1) $n = 5$;
2) $n = 3$;
3) $n = 8$.

Sejtés (E. Artin): *Ha* $a \in \mathbb{Z}, a \neq -1,\ a \neq b^2$, *akkor végtelen sok* p *prímszám létezik úgy, hogy* a *primitív gyök modulo* p.

6.66. feladat. Oldjuk meg $1 + x + x^2 + x^3 + x^4 + x^5 + x^6 \equiv 0 \pmod{29}$ kongruenciát.

6.67. feladat. -1 negyedik hatványmaradék modulo $p \Leftrightarrow p \equiv 1 \pmod{8}$.

6.68. feladat. a) Feltételezzük, hogy $p \equiv 1 \pmod{4}$. Igazoljuk, hogy g primitív gyök modulo $p \Leftrightarrow -g$ primitív gyök modulo p.

b) Feltételezzük, hogy $p \equiv -1 \pmod{4}$. Igazoljuk, hogy g primitív gyök modulo $p \Leftrightarrow o_p(-g) = \frac{p-1}{2}$.

6.69. feladat. Legyen p egy prímszám és $K = \left\{ \begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{Z}_p \right\}$. Igazoljuk, hogy $(K, +, \cdot)$ test $\Leftrightarrow p \equiv 3 \pmod{4}$.

Az általános eset

Az általános esetben, legyen $m = 2^p p_1^{e_1} \dots p_r^{e_r}$, ahol $e, e_i \in \mathbb{N}^*$, $p \geq 2$ prímszám.

6.2.34. megjegyzés. Legyen $(a, m) = 1$, $n \in \mathbb{Z}$. A kínai maradéktétel alapján, az $x^n \equiv a \pmod{m}$ binom kongruencia megoldható $\Leftrightarrow$ az

$$\begin{cases} x^n \equiv a \pmod{2^e} \\ x^n \equiv a \pmod{p_1^{e_1}} \\ \quad \vdots \\ x^n \equiv a \pmod{p_r^{e_r}} \end{cases}$$

kongruenciarendszer megoldható. A $2, 2^2, p_i^{e_i}$ esetekben alkalmazzuk az 6.2.32 tételt.

6.2.35. példa. Oldjuk meg az $x^4 \equiv 16 \pmod{36}$ kongruenciát.
$36 = 2^2 \cdot 3^2$, tehát nem létezik primitív gyök modulo 36.

$$\begin{cases} x^4 \equiv 16 \pmod{4} \\ x^4 \equiv 16 \pmod{9} \end{cases} \Leftrightarrow \begin{cases} x^4 \equiv 0 \pmod{4} \\ x^4 \equiv 7 \pmod{9} \end{cases}$$

- mod 4: $x_{01} = 0$, $x_{02} = 2$ megoldások;
- mod 9: $g = 2$ primitív gyök;

$$x^4 \equiv 7 \pmod{9} \Leftrightarrow 4 \operatorname{ind}_2 x \equiv 4 \pmod{6} \Leftrightarrow 4y \equiv 4 \pmod{6} \Leftrightarrow 2y \equiv 2 \pmod{3} \Leftrightarrow y \equiv 1 \pmod{3}.$$

6.70. feladat. Oldjuk meg a következő kongruenciákat:
1) $x^4 \equiv 5 \pmod{36}$;
2) $x^6 \equiv 3 \pmod{100}$
3) $x^3 \equiv 8 \pmod{36}$

Tekintsük a 2e esetet , $e \geq 3$. Tudjuk a főtételből, hogy $U(\mathbb{Z}_{2^e}) \simeq \langle \widehat{-1} \rangle \times \langle \widehat{5} \rangle$, ahol $o_{2^e}(-1) = 2$, $o_{2^e}(5) = 2^{e-2}$, $\varphi(2^e) = 2^{e-1}$.

6.2.36. tétel. *Legyen $e \geq 3$, $a \in \mathbb{Z}$ páratlan, $m = 2^e$, $n \in \mathbb{N}^*$. Tekintsük az $x^n = a \pmod{2^e}$ kongruenciát.*
1) *Ha n páratlan, akkor létezik megoldás.*
2) *Ha n páros, akkor az x megoldások száma*

$$\begin{cases} 2(n, 2^{e-2}), & \textit{ha } a \equiv 1 \pmod{4} \textit{ és } a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}, \textit{ ahol } d := (n, 2^{e-2}); \\ 0\ , & \textit{ellenkező esetben.} \end{cases}$$

Bizonyítás. Legyen $a \equiv (-1)^s 5^t \pmod{2^e}$, $x \equiv (-1)^y 5^z \pmod{2^e}$, ahol $s, y \in \{0, 1\}$, $t, z \in \{0, 1, \dots, 2^{e-2} - 1\}$. A főtételből következik, hogy az y, s, t, z számok egyértelműen meghatározottak.

$$x^n \equiv a \pmod{2^e} \Leftrightarrow (-1)^{yn} 5^{zn} \equiv (-1)^s 5^t \pmod{2^e} \Leftrightarrow \begin{cases} yn \equiv s \pmod{2} \\ zn \equiv t \pmod{2^{e-2}} \end{cases},$$

ahol y, z ismeretlenek, e, n, s, t adottak.

(a) Feltételezzük, hogy n páratlan, azaz $(2, n) = 1$. Mivel $(2, n) \mid s \Rightarrow \exists!\ y$ megoldás modulo 2; mivel $(2^{e-2}, n) \mid t \Rightarrow \exists!\ z$ megoldás modulo 2^{e-2}.

(b) Feltételezzük, hogy n páros és legyen $d = (n, 2^{e-2})$. Létezik y megoldás, akkor és csak akkor, ha

$$(n, 2) \mid s \overset{s \in \{0,1\}}{\Longleftrightarrow} s = 0.$$

Ha $s = 0$, akkor $a \equiv 5^t \pmod{2^e} \Rightarrow a \equiv 1 \pmod{4}$, $(e \geq 3)$; fordítva, ha $a \equiv 1 \pmod{4}$, mivel $a \equiv (-1)^s \pmod{4}$, és $s \in \{0, 1\}$, következik, hogy $s = 0$; tehát létezik y megoldás $\Leftrightarrow a \equiv 1 \pmod{4}$, és pontosan két megoldás létezik, y_0, y_1, mert $(n, 2) = 2$.

Tárgyaljuk most a z-t: $\exists\ z_0, z_1, \dots, z_{d-1}$ megoldás $\Leftrightarrow d \mid t \Leftrightarrow t = du$;

∘ Feltételezzük, hogy $t = du$ alakú. Akkor $a^{\frac{2^{e-2}}{d}} \equiv 5^{du \frac{2^{e-2}}{d}} \equiv 5^{u 2^{e-2}} \equiv 1 \pmod{2^e}$

∘ Fordítva, $1 \equiv a^{\frac{2^{e-2}}{d}} \equiv 5^{t \frac{2^{e-2}}{d}} \overset{\theta_{2^e}(5) = 2^{e-2}}{\Longrightarrow} 2^{e-2} \mid t \frac{2^{e-2}}{d} \Rightarrow t \mid d \in \mathbb{N} \Rightarrow d \mid t$.

Tehát léteznek a $z_0, z_1, \dots, z_{d-1}$ megoldások $\Leftrightarrow a^{\frac{2^{e-2}}{d}} \equiv 1 \pmod{2^e}$ ■

6.71. feladat. Adott a következő kongruencia : $x^5 \equiv 3 \pmod{16}$, azaz $n = 5, e = 4, a = 3$. Számítsuk ki y-t, t-t, x-et.

6.72. feladat. Határozzuk meg a hatodik hatványmaradékokat modulo 16, azaz a páratlan a-kat úgy, hogy $x^6 \equiv a \pmod{16}$ megoldható legyen.

6.2.37. megjegyzés. Legyen $p > 2$, prímszám és tekintsük az $x^n \equiv a \pmod{p^e}$ kongrueniát. A megoldáshoz két módszerünk van:

I. módszer: Legyen g primitív gyök modulo p^e, készítünk index-táblát, és megoldjuk az

$$n \operatorname{ind}_g x = \operatorname{ind}_g a \pmod{\varphi(p^e)}$$

kongrueniát;

II. módszer: a következő tételre alapszik.

6.2.38. tétel. *Legyen $p > 2$ prímszám, $(a, p) = 1$, $(n, p) = 1$. Az $x^n \equiv a \pmod{p}$ kongruencia akkor és csak akkor oldható meg, ha bármely $e \geq 1$ esetén az $x^n \equiv a \pmod{p^e}$ kongruencia megoldható. Minden kongruenciának ugyanannyi megoldása van, azaz a megoldások száma nem függ e-től.*

Bizonyítás. Ha $n = 1$, akkor az állítás evidens. Feltételezzük, hogy $n \geq 2$. Legyen x_0 megoldása az $x^n \equiv a \pmod{p^e}$ kongruenciának. Keressünk x_1-et, amely megoldása az $x^n \equiv a \pmod{p^{e+1}}$ kongruenciának, úgy hogy $x_1 = x_0 + bp^e$ alakú legyen (ha $x_1^n \equiv a \pmod{p^{e+1}}$, akkor $x^n \equiv a \pmod{p^e}$, és akarjuk, hogy $x_1 \equiv x_0 \pmod{p^e}$). Tehát ha $x_1 = x_0 + bp^e$, ahol $b \in \{0, 1, \ldots, p-1\}$, akkor

$$x_1^n = (x_0 + bp^e)^n = x_0^n + nx_0^{n-1}bp^e + \underbrace{C_n^2 x_0^{n-2} b^2 p^{2e}}_{p^{e+1}|} + \cdots \equiv (x_0^n + nx_0^{n-1}bp^e) \pmod{p^{e+1}}.$$

Keressük x_1-et úgy, hogy $x_1^n \equiv a (\bmod\ p^{e+1})$, azaz keressük b-t úgy, hogy

$$x_0^n + nx_0^{n-1}bp^e \equiv a \pmod{p^{e+1}} \Leftrightarrow nx_0 b \equiv \frac{a - x_0^n}{p^e} \pmod{p}.$$

Ez egy első fokú kongruencia, $\frac{a-x_0^n}{p^e} \in \mathbb{Z}$ mert $x_0^n \equiv a (\bmod\ p^e)$. Mivel $(p, nx_0) = 1$, következik, hogy $\exists!$ $b \in \{0, 1, \ldots, p-1\}$ megoldás modulo p, tehát $\exists!$ x_1 a fenti alakú megoldás.

Összefoglalva:

∘ Ha $x^n \equiv a \pmod{p^e}$ megoldható, akkor az $x^n \equiv a \pmod{p}$ is megoldható;

∘ Fordítva, ha $x^n \equiv a (\bmod\ p)$ megoldható, akkor kiindulva egy x_0 megoldásból, a fenti módszerrel szerkesztünk egy megoldást az $x^n \equiv a \pmod{p^e}$ kongruenciának;

∘ Feltéve, hogy $a^{\frac{\varphi(m)}{(n,\varphi(m))}} \equiv 1 \pmod{p}$, a megoldások száma

$$(n, \varphi(m)) = (n, \varphi(p^e)) = (n, p^{e-1}(p-1)) = (n, p-1)$$

nem függ e-től. ■

6.73. feladat. Oldjuk meg az $x^0 \equiv 3 \pmod{11^e}$ kongruenciákat, ahol $e = 1, 2, 3$.

6.2.39. tétel. *Legyen $n = 2^l n'$, n' páratlan, $a \in \mathbb{Z}$ páratlan. Feltételezzük, hogy az $x^n \equiv a \pmod{2^{2l+1}}$ kongruencia megoldható. Akkor az $x^n \equiv a \pmod{2^e}$ kongruencia megoldható $\forall\ e \geq 2l+1$ (tehát $\forall\ e \geq 1$). Ha $e \geq 2l+1$, akkor a megoldások száma nem függ e-től.*

Bizonyítás. Legyen $m \geq 2l+1$ és legyen x_0 megoldása az $x^n \equiv a \pmod{2^m}$ kongruenciájának. Keresünk x_1-et, megoldása az $x^n \equiv a \pmod{2^{m+1}}$ kongruenciának úgy, hogy $x_1 = x_0 + b2^{m-l}$ alakú. Meghatározzuk b-t:

$$x_1^n = (x_0 + b2^{m-l})^n \equiv x_0^n + nx_0^{n-1}b2^{m-l} \pmod{2^{m+1}},$$

mert $2(m-l) \geq m+1 \Leftrightarrow m \geq 2l+1$. Tehát

$$\begin{aligned} x_1^n \equiv a \pmod{2^{m+1}} &\Longleftrightarrow x_0^n + nx_0^{n-1}b2^{m-l} \equiv a \pmod{2^{m+1}} \Longleftrightarrow \\ &\overset{n=2^l n'}{\Longleftrightarrow} 2^l n' b x_0^{n-1} 2^{m-l} \equiv a - x_0 \pmod{2^{m+1}} \Longleftrightarrow \\ &\overset{2^m | a - x_0^n}{\Longleftrightarrow} n' b x_0^{n-1} \equiv \frac{a - x_0^n}{2^n} \pmod{2} \end{aligned}$$

Mivel $(2, n'x_0^{n-1}) = 1$, $\exists!$ $b \in \{0, 1\}$ megoldás. Tehát $\exists!$ $x_1 = x_0 + b2^{m-l}$ alakú megoldása az $x^n \equiv a \pmod{2^{m+1}}$ kongruenciának.

Összefoglalva:

◦ Ha $x^n \equiv a \pmod{2^{2l+1}}$ megoldhatatlan, akkor $x^n \equiv a \pmod{2^l}$ megoldhatatlan $e \geq 2l+1$ esetén.
◦ Ha $x^n \equiv a \pmod{2^{2l+1}}$ megoldható, akkor a fentiekből, $x^n \equiv a \pmod{2^l}$ is megoldható, minden $e \geq 2l+1$ esetén.
◦ A megoldások száma:

$$(n, \varphi(2^{2l+1})) = (2^l n', 2^{2l}) = 2^l \overset{e \geq 2l+1}{=} (2^l n', 2^{e-1}) = (n, \varphi(2^e)). \qquad \blacksquare$$

6.74. feladat. Oldjuk meg az $x^2 \equiv 17 \pmod{2^e}$ kongruenciát, ahol $e = 3, 4, 5, 6, 7$.

6.3. Kvadratikus maradékok

6.3.1. A másodfokú kongruencia

6.3.1. definíció. Legyen $m \geq 2$, $a \in \mathbb{Z}$, $(a, m) = 1$. Azt mondjuk, hogy:
◦ a **kvadratikus maradék** modulo m, ha létezik $x \in \mathbb{Z}$ úgy, hogy $x^2 \equiv a \pmod{m}$;
◦ a **kvadratikus nemmaradék** modulo m, ha minden $x \in \mathbb{Z}$ esetén $x^2 \not\equiv a \pmod{m}$.

6.3.2. példa. Legyen $m = 7$; $(\pm 1)^2 \equiv 1$, $(\pm 2)^2 \equiv 4$, $(\pm 3)^2 \equiv 2 \pmod 7$, tehát $1, 2, 4$ kvadratikus maradékok, $3, 5, 6$ kvadratikus nemmaradékok modulo 7.

A következő tétel redukálja az $x^2 \equiv a \pmod{m}$ kongruenciát az $m = p$ esetre.

6.3.3. tétel. *Legyen* $m = 2^e p_1^{e_1} \dots p_l^{e_l}$, $l, e_i \in \mathbb{N}^*$, $p_i \geq 3$ *prímszámok,* $a \in \mathbb{Z}$, $(a, m) = 1$. *Az* $x^2 \equiv a \pmod{m}$ *kongruencia megoldható akkor és csak akkor, ha*
- *ha* $e = 2$, *akkor* $a \equiv 1 \pmod 4$*; ha* $e \geq 3$, *akkor* $a \equiv 1 \pmod 8$*;* (ha $e = 1$, nincs más feltétel)*;*
- $\forall\ i = 1, \dots, l$, *esetén* $a^{\frac{p_i - 1}{2}} \equiv 1 \pmod{p_i}$.

Bizonyítás. A kínai maradéktétel szerint, az $x^2 \equiv a \pmod{m}$ kongruencia ekvivalens az

$$\begin{cases} x^2 \equiv a \pmod{2^e} \\ x^2 \equiv a \pmod{p_1^{e_1}} \\ \quad \dots \\ x^2 \equiv a \pmod{p_i^{e_i}} \end{cases}$$

kongruenciarendszerrel.

Tekintsük az $x^2 \equiv a \pmod{2^e}$ kongruenciát.

- 1 az egyetlen kvadratikus maradék modulo 4;
- 1 az egyetlen kvadratikus maradék modulo 8, mert $(\pm 1)^2 \equiv (\pm 3)^2 \equiv 1 \pmod 8$.

Tehát az $x^2 \equiv a \pmod{2^e}$ kongruencia megoldható akkor és csak akkor, ha

$$\begin{cases} a \equiv 1 \pmod 4, & \text{ha } e = 2 \\ a \equiv 1 \pmod 8, & \text{ha } e = 3 \end{cases}.$$

Ha $e \geq 3$, tudjuk, hogy $x^2 \equiv a \pmod{2^e}$ megoldható $\Leftrightarrow x^2 \equiv a \pmod 8$ megoldható.

Tekintsük az $x^2 \equiv a \pmod{(p_i^{e_i})}$ kongruenciát. Mivel $(2, p_i) = 1$, a 6.2.38 tétel szerint, ez a kongruencia megoldható $\Leftrightarrow x^2 \equiv a \pmod{p_i}$ megoldható. Alkalmazzuk most az 6.2.32 tételt az $n = 2, m = p_i, d = (n, \varphi(m)) = 2$ esetben: az $x^2 \equiv a \pmod{p_i}$ kongruencia megoldható $\Leftrightarrow a^{\frac{p_i - 1}{2}} \equiv 1 \pmod{p_i}$. $\blacksquare$

6.3.2. A Legendre-szimbólum

Legyen $p > 2$ prímszám, $a \in \mathbb{Z}$.

6.3.4. definíció. Az $\left(\frac{a}{p}\right)$ („a per p”) **Legendre-szimbólum**ot a következőképpen definiáljuk:

$$\left(\frac{a}{p}\right) \overset{\text{def}}{=} \begin{cases} 0, & \text{ha } p \mid a; \\ 1, & \text{ha } a \text{ kvadratikus maradék modulo } p \\ -1, & \text{ha } a \text{ kvadratikus nemmaradék modulo } p \end{cases}$$

6.3.5. példa. a) $(\frac{1}{3}) = 1$, mert $1^2 \equiv 1 \pmod 3$; $(\frac{2}{3}) = -1$, mert $x^2 \not\equiv 2 \pmod 3$, $\forall\ x \in \mathbb{Z}$.
b) Legyen $p = 5$; $(\pm 1)^2 \equiv 1 \pmod 5$, $(\pm 2)^2 \equiv 4 \pmod 5$, tehát $\left(\frac{1}{5}\right) = \left(\frac{4}{5}\right) = 1$, $\left(\frac{2}{5}\right) = \left(\frac{3}{5}\right) = -1$.

6.3.6. tétel (A Legendre-szimbólum alaptulajdonságai). 0) $a \equiv b \pmod p \Rightarrow (\frac{a}{p}) = (\frac{b}{p})$;

1) $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod p$;

2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Bizonyítás. 0) Evidens a definíció alapján. 1), 2) evidens, ha $p \mid a$ (vagy $p \mid b$). Feltételezzük, hogy $p \nmid a$, $p \nmid b$, azaz $(a, p) = (b, p) = 1$.

1) A Fermat-tétel alapján

$$a^{p-1} \equiv 1 \pmod p \Rightarrow 0 \equiv a^{p-1} - 1 = \left(a^{\frac{p-1}{2}} - 1\right)\left(a^{\frac{p-1}{2}} + 1\right) \pmod p;$$

Mivel $\mathbb{Z}_p$ test, következik, hogy $a^{\frac{p-1}{2}} \equiv 1 \pmod p$) vagy $a^{\frac{p-1}{2}} \equiv (-1) \pmod p$. Továbbá, tudjuk, hogy a kvadratikus maradék modulo $p \Leftrightarrow$ az $x^2 \equiv a \pmod p$ kongruencia megoldható $\Leftrightarrow a^{\frac{p-1}{2}} \equiv 1 \pmod p$.

2) Az 1) alapján $(ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod p$ és $a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$, tehát $\left(\frac{ab}{p}\right) \equiv \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$. Mivel $\left(\frac{a}{p}\right), \left(\frac{b}{p}\right), \left(\frac{ap}{p}\right) \in \{-1, 1\}$ és $p \geq 2$, következik, hogy $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$. ■

6.3.7. következmény. *A modulo* p *kvadratikus maradékok száma egyenlő a modulo* p *kvadratikus nemmaradékok számával és mindkettő egyenlő* $\frac{p-1}{2}$*-vel.*

Bizonyítás. Vegyük észre, hogy az $a^{\frac{p-1}{2}} \equiv 1 \pmod p$ kongruenciának $\frac{p-1}{2}$ megoldása van, mert ekvivalens a $\frac{p-1}{2} \log a \equiv 0 \pmod{p-1}$ kongruenciával, és $(\frac{p-1}{2}, p-1) = \frac{p-1}{2} \mid 0$. Tehát létezik $\frac{p-1}{2}$ kvadratikus maradék és létezik $(p-1) - \frac{p-1}{2} = \frac{p-1}{2}$ kvadratikus nemmaradék. ■

6.75. feladat. Igazoljuk, hogy:

1) az $x^2 \equiv a \pmod p$ kongruencia megoldásainak száma $1 + \left(\frac{a}{p}\right)$;

2) ha $p \nmid a$, akkor az $ax^2 + bx + c = 0 \pmod p$ kongruencia megoldásainak száma $1 + \left(\frac{\Delta}{p}\right)$, ahol $\Delta = b^2 - 4ac$.

6.3.3. Kvadratikus reciprocitás

A következő fontos tétel segítségével ki lehet számítani a Legendre-szimbólumot.

6.3.8. tétel. *Legyenek* $p, q > 2$ *prímszámok,* $p \neq q$.

1) **(Euler)** $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \pmod p = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod 4 \\ -1, & \text{ha } p \equiv -1 \pmod 4 \end{cases}$.

2) $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \textit{ha } p \equiv \pm 1 \pmod 8 \\ -1, & \textit{ha } p \equiv \pm 3 \pmod 8 \end{cases}$.

3) **(Gauss-féle reciprocitástétel)**

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} = \begin{cases} 1, & \textit{ha } p \equiv 1 \pmod 4 \textit{ vagy } q \equiv 1 \pmod 4 \\ -1, & \textit{ha } p \equiv q \equiv -1 \pmod 4 \end{cases}.$$

6.3.9. megjegyzés. 1) A 6.3.8. 1) állítás azonnal következik a 6.3.6. tételből.

2) Gyakorlatban a reciprocitástételt a következőképpen használjuk:

$$\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{q}{p}\right), & \text{ha } p \equiv 1 \pmod 4 \text{ vagy } q \equiv 1 \pmod 4 \\ -\left(\frac{q}{p}\right), & \text{ha } p \equiv q \equiv (-1) \pmod 4 \end{cases}.$$

6.3.10. példa. Számítsuk ki a $\left(\frac{58}{97}\right)$ Legendre-szimbólumot a fenti tétel segítségével:

$$\left(\frac{58}{97}\right) = \left(\frac{2 \cdot 29}{97}\right) = \left(\frac{2}{97}\right)\left(\frac{29}{97}\right) = \left(\frac{29}{97}\right) = \left(\frac{97}{29}\right) = \left(\frac{10}{29}\right) = \left(\frac{2}{29}\right)\left(\frac{5}{29}\right) =$$
$$= -\left(\frac{5}{29}\right) = -\left(\frac{29}{5}\right) = -\left(\frac{4}{5}\right) = -\left(\frac{2}{5}\right)\left(\frac{2}{5}\right) = -1,$$

tehát $\nexists\, x \in \mathbb{Z}$ úgy, hogy $x^2 \equiv 58 \pmod{97}$.

6.76. feladat. 1) Számítsuk ki a $\left(\frac{79}{101}\right)$ Legendre szimbólumot.

2) Számítsuk ki a $\left(\frac{67}{103}\right)$ Legendre-szimbólumot.

A következőkben bibizonyítjuk a A 6.3.8. 2) és 3) állításokat.

6.3.11. lemma (Gauss). *Legyen* $a \in \mathbb{Z}$ *és* $p \nmid a$ *egy prímszám.*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{2ai}{p}\right]}.$$

Bizonyítás. Jelöljük $p_1 := \frac{p-1}{2}$. Tekintsük az $1a, 2a, \ldots, p_1 a$ szorzatokat. Ekkor

$$ia \equiv \varepsilon_i r_i \pmod{p},$$

ahol $\varepsilon_i \in \{1, -1\}$, $1 \le r_i \le p_1$ ($\varepsilon_i r_i$ az abszolút értékben vett legkisebb maradék). Akkor $r_1, \ldots, r_{p_1}$ páronként különböző számok, és a maradékos osztás tétele szerint

$$\varepsilon_i = \begin{cases} 1, & \text{ha } \left\{\frac{ia}{p}\right\} < \frac{1}{2} \\ -1, & \text{ha } \left\{\frac{ia}{p}\right\} > \frac{1}{2} \end{cases}.$$

Továbbá, minden $x \in \mathbb{R}$ esetén $x = [x] + \{x\}$, tehát $2x = 2[x] + 2\{x\}$. Innen

$$[2x] = 2[x] + [2\{x\}].$$

Ezt alkalmazzuk $x = \frac{ai}{p}$-re; következik, hogy

$$(-1)^{\sum_{i=1}^{p_1} \left[\frac{2ai}{p}\right]} = (-1)^{\sum_{i=1}^{p_1} \left[2\left\{\frac{ai}{p}\right\}\right]} = (-1)^{\mu},$$

ahol $\mu = |\{\varepsilon_i \mid \varepsilon_i = -1\}|$. Összeszorozva a $1a, 2a, \ldots, p_1 a$ számokat, kapjuk, hogy

$$\left(\frac{p-1}{2}\right)! a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \left(\frac{p-1}{2}\right)! \pmod{p}, \qquad a^{\frac{p-1}{2}} \equiv (-1)^{\mu} \pmod{p},$$

tehát

$$\left(\frac{a}{p}\right) \equiv (-1)^{\mu} \pmod{p} \equiv (-1)^{\sum_{i=1}^{p_1} \left[\frac{2ai}{p}\right]}. \qquad \blacksquare$$

6.77. feladat. Alkalmazva a Gauss-lemmát, számítsuk ki a $\left(\frac{5}{7}\right)$, $\left(\frac{3}{11}\right)$, $\left(\frac{6}{13}\right)$ és $\left(\frac{-1}{p}\right)$ Legendre-szimbólumokat.

6.3.12. lemma. *Feltételezzük, hogy* $a \in \mathbb{Z}$, $2 \nmid a$, $p \nmid a$. *Ekkor*

$$\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{\frac{p-1}{2}} \left[\frac{ai}{p}\right]}, \qquad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}.$$

Bizonyítás. Alkalmazva a Gauss-lemmát, kapjuk, hogy

$$\left(\frac{2a}{p}\right) = \left(\frac{2a+2p}{p}\right) = \left(\frac{4\frac{a+p}{2}}{p}\right) = \left(\frac{4}{p}\right)\left(\frac{a+\frac{p}{2}}{p}\right) = \left(\frac{\frac{a+p}{2}}{p}\right)$$
$$= (-1)^{\sum_{i=1}^{p_1} \left[\frac{(a+p)i}{p}\right]} = (-1)^{\sum_{i=1}^{p_1} \left[\frac{2ai}{p}+i\right]} = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right]} (-1)^{\sum_{i=1}^{p_1} i} = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right]} (-1)^{\frac{p^2-1}{8}}.$$

Ha $a = 1$, akkor $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, és $\left[\frac{ai}{p}\right] = \left[\frac{i}{p}\right] = 0$, mert $i = p_1 = \frac{p-1}{2} < p$. Minden a páratlan szám esetén $\left(\frac{2a}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{a}{p}\right) = (-1)^{\frac{p^2-1}{8}}\left(\frac{a}{p}\right)$. Innen következik, hogy $\left(\frac{a}{p}\right) = (-1)^{\sum_{i=1}^{p_1} \left[\frac{ai}{p}\right]}$. $\blacksquare$

A reciprocitástétel bizonyítása.

Jeloljük $p_1 := \frac{p-1}{2}$, $q_1 := \frac{q-1}{2}$, és igazoljuk, hogy $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{p_1 q_1}$. Legyen

$$M := \{(qi, pi) \mid 1 \le i \le p_1, 1 \le j \le q_1\} \subseteq \mathbb{N} \times \mathbb{N},$$

tehát $|M| = p_1q_1$. Vegyük észre, hogy $qi \neq pj$ (valóban, ha $qi = pj \Rightarrow q \mid pj \Rightarrow q \mid j$). Legyen

$$M_1 := \{(qi, pj) \in M \mid qi > pj\}, \qquad M_2 := \{(qi, pj) \in M \mid qi < pj\}.$$

Következik, hogy $M = M_1 \cup M_2$, $M_1 \cap M_2 = \varnothing$, tehát $p_1q_1 = |M_1| + |M_2|$.

Rögzítsük i-t. Akkor létezik $\left[\frac{qi}{p}\right]$ db. $j \in \mathbb{N}$ szám úgy, hogy $1 \leq j \leq \frac{qi}{p}$. Mivel $1 \leq i \leq p_1$, $\frac{qp_1}{p} < \frac{q}{2} \Rightarrow \left[\frac{qp_1}{p}\right] \leq q_1 = \frac{q-1}{2}$, tehát $|M_1| = \sum\limits_{i=1}^{p_1} \left[\frac{qi}{p}\right]$. Szimmetria okokból, $|M_2| = \sum\limits_{j=1}^{q_1} \left[\frac{pj}{q}\right]$.

Felhasználva a 6.3.12. lemmát, következik, hogy

$$\left(\frac{q}{p}\right) = (-1)^{\sum\limits_{i=1}^{p_1}\left[\frac{qi}{p}\right]} = (-1)^{|M_1|}, \quad \left(\frac{p}{q}\right) = (-1)^{\sum\limits_{j=1}^{q_1}\left[\frac{pj}{q}\right]} = (-1)^{|M_2|},$$

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{|M_1|+|M_2|} = (-1)^{|M|} = (-1)^{p_1q_1}. \qquad \blacksquare$$

6.78. feladat. Határozzuk meg a p prímszámokat úgy, hogy a kvadratikus maradék modulo p, ahol:
1) $a = -2$; 2) $a = 3$; 2) $a = -3$; 3) $a = 7$; 4) $a = 5$; 5) $a = 15$; 6) $a = 6$; 7) $a = 10$.

Tekintsük a következő általános feladatot. Adott $a \in \mathbb{Z}$. Határozzuk meg p-t úgy, hogy $\left(\frac{a}{p}\right) = 1$. A következő tétel választ ad erre a kérdésre, amikor $a = q$ prímszám.

6.3.13. tétel. *Legyenek p,q páratlan prímszámok.*

1) *Ha* $q \equiv 1 \pmod 4$, *akkor* q *kvadratikus maradék modulo* $p \iff p \equiv r \pmod q$, *ahol* $\left(\frac{r}{q}\right) = 1$, $(0 < r < q)$.

2) *Ha* $q \equiv -1 \pmod 4$, *akkor* q *kvadratikus maradék modulo* $p \iff p \equiv \pm b^2 \pmod{4q}$, *ahol* b *páratlan,* $q \nmid b$.

Bizonyítás. 1) Feltételezzük, hogy $q \equiv 1 \pmod 4$. Akkor $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, tehát $\left(\frac{q}{p}\right) = \left(\frac{r}{q}\right)$, ahol $r \equiv p \pmod q$. Innen $\left(\frac{q}{p}\right) = 1 \iff \left(\frac{r}{q}\right) = 1$.

2) Feltételezzük, hogy $q \equiv -1 \pmod 4$. Akkor $\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{q}\right) = \begin{cases} \left(\frac{p}{q}\right), & \text{ha } p \equiv 1 \pmod 4 \\ -\left(\frac{p}{q}\right), & \text{ha } p \equiv -1 \pmod 4. \end{cases}$

„$\Longleftarrow$„ Feltételezzük, hogy $p \equiv \pm b^2 \pmod{4q}$, ahol b páratlan, $q \nmid b$.

A „+” esetben $p \equiv b^2 \equiv 1 \pmod 4$ (mert b páratlan) $\Longrightarrow \frac{p-1}{2}$ páros. Innen $p \equiv b^2 \pmod q \Longrightarrow \left(\frac{p}{q}\right) = \left(\frac{b^2}{q}\right) = 1$, Tehát $\left(\frac{q}{p}\right) = 1$.

A „$-$” esetben $p \equiv -b^2 \equiv -1 \pmod 4 \Longrightarrow \frac{p-1}{2}$ páratlan. Mivel $p \equiv -b^2 \pmod q$, következik, hogy

$$\left(\frac{p}{q}\right) = \left(\frac{-b^2}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{b^2}{q}\right) = (-1) \cdot 1 = 1.$$

Tehát $\left(\frac{q}{p}\right) = (-1) \cdot (-1) = 1$

„$\Longrightarrow$” Feltételezzük $\left(\frac{q}{p}\right) = 1$, és $q \equiv -1 \pmod 4$.

<u>1. eset</u> Legyen $(-1)^{\frac{p-1}{2}} = 1$ és $\left(\frac{p}{q}\right) = 1$. Ekkor

$$\begin{cases} p \equiv 1 \pmod 4 \\ p \equiv b^2 \pmod q, \text{ ahol } q \nmid b, \ b \text{ páratlan.} \end{cases}$$

(Feltételezhetjük, hogy b páratlan, mert ha b áros, legyen $b := b + q$.)

A fenti rendszer $\iff p \equiv b^2 \pmod{4q}$, mert $(4, q) = 1$, és $b^2 \equiv 1 \pmod 4$.

<u>2. eset</u> Legyen $(-1)^{\frac{p-1}{2}} = -1$ és $\left(\frac{p}{q}\right) = -1$. Ekkor

$$\begin{cases} p \equiv -1 \pmod 4 \\ p \equiv -b^2 \pmod q, \end{cases}$$

mert $\left(\frac{-b^2}{q}\right) = \left(\frac{-1}{q}\right) \cdot \left(\frac{b^2}{q}\right) = -1$. (Feltételezhetjük, hogy b páratlan, mert ha b páros, legyen $b := b + q$.)

A fenti rendszer $\iff p \equiv -b^2 \pmod{4q}$, mert $(4, q) = 1$, és valóban $-b^2 \equiv -1 \pmod 4$. $\blacksquare$

6.3.14. példa. 1) Legyen $q = 5 \equiv 1 \pmod 4$. Itt $(\pm 1)^2 \equiv 1 \pmod 5$, $(\pm 2)^2 \equiv 1 \pmod 5$, tehát $\left(\frac{5}{p}\right) = 1 \iff p \equiv \pm 1 \pmod 5$.

2) Legyen $q = 3 \equiv -1 \pmod 4$. Itt $(\pm 1)^2 = 1$, $b = \pm 1$, tehát $\left(\frac{3}{p}\right) = 1 \iff p \equiv \pm 1 \pmod{12}$.

3) Legyen $q = 7 \equiv -1 \pmod 4$. Itt $1^2 = 1$, $3^2 = 9, 5^2 = 25 \equiv -3 \pmod{28}$, tehát $\left(\frac{7}{p}\right) = 1 \iff p \equiv \pm 1$ vagy $p \equiv \pm 9$ vagy $p \equiv \pm 3 \pmod{28}$.

6.3.15. példa. *Végtelen sok* $4k+1$ *alakú prímszám létezik.*

Valóban, feltételezzük, hogy $p_1, \dots, p_r$ az összes $4k+1$ alakú prímszám. Legyen

$$N := (2p_1 \dots p_r)^2 + 1.$$

Az aritmetika alaptételéből következik, hogy létezik olyan $p \neq 2$ prím, amelyre $p \mid N$, azaz

$$(2p_1 \dots p_r)^2 \equiv (-1) \pmod p.$$

Innen $\left(\frac{-1}{p}\right) = 1 \Rightarrow p = 4k+1$ alakú $\Rightarrow p \in \{p_1, \dots, p_r\}$ ellentmondás, mert $p_i \nmid N$, $\forall\, i = 1, \dots, r$.

6.79. feladat. 1) Igazoljuk, hogy végtelen sok $8k-1$ alakú prímszám létezik.

2) Igazoljuk, hogy végtelen sok $6k+1$ alakú prímszám létezik. (Útmutatás: legyen $N = (2p_1 \dots p_r)^2 + 3$.)

A fenti állítások partikuláris esetei a következő tételnek, amelynek bizonyítása sokkal bonyolultabb módszereket igényel.

6.3.16. tétel (Dirichlet). *Ha* $a, b \in \mathbb{Z}$, $(a, b) = 1$, *akkor végtelen sok* $ak + b$ *alakú prímszám létezik.*

6.80. feladat. Feltételezzük, hogy $p \equiv 3 \pmod 4$, $p > 3$ prímszám, és feltételezzük, hogy $q = 2p+1$ is prímszám. Igazoljuk, hogy $2^p - 1$ nem prímszám.

6.81. feladat. Legyen $p > 2$ prím és $g \in \mathbb{Z}$. Igazoljuk, hogy:

a) g primitív gyök modulo $p \iff g^{\frac{p-1}{2}} \equiv -1 \pmod p$;

b) ha g primitív gyök modulo p, akkor g kvadratikus nemmaradék modulo p.

6.82. feladat. 1) Legyen $p = 4q+1$ alakú prím, ahol q is prím. Igazoljuk, hogy 2 primitív gyök modulo p.

2) Legyenek $p \equiv 3 \pmod 8$ és $q = \frac{p-1}{2}$ prímek. Igazoljuk, hogy 2 primitív gyök modulo p.

3) Legyenek p, q prímek, $p = 2q+1$, $q \equiv 3 \pmod 4$. Igazoljuk, hogy -2 primitív gyök modulo p.

4) Igazoljuk, hogy ha $p = 2^n + 1$ Fermat-féle prímszám, akkor 3 primitív gyök modulo p. Általában, ha $p = 2^n + 1$ alakú prím, akkor minden kvadratikus nemmaradék modulo p primitív gyök modulo p. (Megjegyzés: $n = 2^k$ alakú.)

6.3.4. A Jakobi-szimbólum

Az $\left(\frac{a}{p}\right)$ Legendre-szimbólum kiszámítása a reciprocitástétel segitségével igényli az a faktorizálását. Most a célunk a Legendre szimbólum meghatározása faktorizálás nélkül.

6.3.17. definíció. Legyen $b \in \mathbb{N}$, páratlan, $b \neq 1$, $b = p_1 \dots p_r$, ahol $p_1, \dots, p_r$ nem feltétlenül különböző prímszámok. Legyen $a \in \mathbb{Z}$. Ekkor az a per b **Jakobi-szimbólum** a Legendre-szimbólumok szorzata:

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right) \dots \left(\frac{a}{p_r}\right).$$

6.3.18. megjegyzés. 1) Ha b prímszám, akkor a Jacobi-szimbólum megeggyezik a Legendre-szimbólummal.

2) $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{5}\right) = (-1) \cdot (-1) = 1$.

Most határozzuk meg a kvadratikus maradékokat modulo 15: $(\pm 1)^2 = 1$, $(\pm 2)^2 = 4$, $(\pm 3)^2 = 9 \equiv -6$, $(\pm 4)^2 \equiv 1$, $(\pm 5)^2 \equiv -5$, $(\pm 6)^2 \equiv 6$, $(\pm 7)^2 \equiv 4$. Következik, hogy 2 kvadratikus nemmaradék modulo 15, annak ellenére, hogy $\left(\frac{2}{15}\right) = 1$.

3) Ha a kvadratikus maradék modulo b, akkor a kvadratikus maradék modulo p_i, ahol $p_i \mid b$, tehát $\left(\frac{a}{p_i}\right) = 1$, $\forall i = 1, \dots, r$. Innen $\left(\frac{a}{b}\right) = 1$, azaz ha $\left(\frac{a}{b}\right) = -1$, akkor a kvadratikus nem maradék modulo b.

6.3.19. tétel. 1) $a_1 \equiv a_2 \pmod b \Longrightarrow \left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$.

2) $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right)\left(\frac{a_2}{b}\right)$, $a_1, a_2 \in \mathbb{Z}$.

3) $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right)\left(\frac{a}{b_2}\right)$, $b_1, b_2 \in \mathbb{N}^*$ *páratlanok.*

Bizonyítás. Alkalmazzuk az értelmezést és a Legendre szimbólumok tulajdonságait. ■

6.3.20. lemma. *Legyenek* $r_1, \dots, r_n \in \mathbb{Z}$ *páratlan számok.*
1) $\sum_{i=1}^{n} \frac{r_i - 1}{2} \equiv \frac{r_1 \cdot \ldots \cdot r_n - 1}{2} \pmod 2$.
2) $\sum_{i=1}^{n} \frac{r_i^2 - 1}{8} \equiv \frac{r_1^2 \cdot \ldots \cdot r_n^2 - 1}{8} \pmod 2$.

Bizonyítás. Indukció n szerint. A részleteket az olvasóra bizzuk. ■

6.3.21. tétel. *Legyenek* $a, b \in \mathbb{N}^*$, $a, b > 1$, a, b *páratlan számok.*
1) $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}} = \begin{cases} 1, & \text{ha } b \equiv 1 \pmod 4 \\ -1, & \text{ha } b \equiv -1 \pmod 4 \end{cases}$.
2) $\left(\frac{2}{b}\right) = (-1)^{\frac{b-1}{8}} = \begin{cases} 1, & \text{ha } b \equiv \pm 1 \pmod 8 \\ -1, & \text{ha } b \equiv \pm 3 \pmod 8 \end{cases}$.
3) $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2} \cdot \frac{b-1}{2}} = \begin{cases} 1, & \text{ha } a \equiv 1 \pmod 4 \text{ vagy } b \equiv 1 \pmod 4 \\ -1, & \text{ha } a \equiv b \equiv -1 \pmod 4 \end{cases}$.

Bizonyítás. A részleteket az olvasóra bizzuk. ■

6.3.22. példa. Számítsuk ki a következő Legendre szimbólumot:

$$\left(\frac{101}{131}\right) = \left(\frac{131}{101}\right) = \left(\frac{30}{101}\right) = \left(\frac{2}{101}\right)\left(\frac{15}{101}\right) = -\left(\frac{15}{101}\right) = -\left(\frac{101}{15}\right) = -\left(\frac{11}{15}\right) = \left(\frac{15}{11}\right) = \left(\frac{4}{15}\right) = 1.$$

6.83. feladat. Számítsuk ki a következő Legendre szimbólumokat:
a) $\left(\frac{215}{267}\right)$; b) $\left(\frac{25}{307}\right)$; c) $\left(\frac{753}{811}\right)$; d) $\left(\frac{48}{1117}\right)$; e) $\left(\frac{514}{1093}\right)$.

6.84. feladat. Legyen $D \in \mathbb{N}$ páratlan és négyzetmentes szám.
1) Igazoljuk, hogy $\exists\, b \in \mathbb{N}$ úgy, hogy $(b, D) = 1$, és $\left(\frac{b}{D}\right) = -1$.
2) Igazoljuk, hogy $\sum_{\hat{a} \in U(\mathbb{Z}_D)} \left(\frac{a}{D}\right) = 0$, és $\left|\left\{\hat{a} \in U(\mathbb{Z}_D) \mid \left(\frac{a}{D}\right) = 1\right\}\right| = \frac{\varphi(D)}{2}$.
3) Legyenek $a_1, \dots, a_{\frac{\varphi(D)}{2}} \in \mathbb{Z}$, úgy, hogy $(a_i, D) = 1$, $\left(\frac{a_i}{D}\right) = 1$. Igazoljuk, hogy $\left(\frac{D}{p}\right) = 1 \iff \exists i$ úgy, hogy $p \equiv a_i \pmod D$.
4) Határozzuk meg azokat a p prímszámokat, amelyekre $\left(\frac{21}{p}\right) = 1$.

6.85. feladat. Ha p, q prímek, $a < 0$, $b \equiv q \pmod{4a}$, $p \nmid a$, akkor $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.

6.86. feladat. Igazoljuk, hogy $\left(\frac{2}{p}\right) = \left(\frac{8-p}{p}\right) = \left(\frac{p}{p-8}\right) = \left(\frac{8}{p-8}\right) = \left(\frac{2}{p-8}\right)$.
2) Következtesük, hogy $\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{ha } p \equiv \pm 1 \pmod 8 \\ -1, & \text{ha } p \equiv \pm 3 \pmod 8 \end{cases}$.

6.87. feladat. Feltételezzük, hogy $a \in \mathbb{N}^*$ és p prím, $p \nmid a$. Igazoljuk, hogy $\left(\frac{a}{p}\right) = \left(\frac{a}{p-4a}\right)$.

6.3.23. tétel. *Legyen* $a \in \mathbb{Z}$, *a nem teljes négyzet. Végtelen sok prímszám létezik, amelyre* $\left(\frac{a}{p}\right) = -1$.

Bizonyítás. Feltételezhetjük, hogy a négyzetmentes, mert ha $a = q^2 a'$, akkor $\left(\frac{a}{p}\right) = \left(\frac{q^2}{p}\right)\left(\frac{a'}{p}\right) = \left(\frac{a'}{p}\right)$. Legyen $a = 2^e q_1 \dots q_m$, ahol q_i páronként különböző páratlan prímszámok, $e = 0$ vagy $e = 1$.

I. eset: $n \geq 1$.

Legyenek $e_1, \dots, e_r$ különböző páratlan prímszámok úgy, hogy $q_i \notin \{e_1, \dots, e_r\}$. Legyen $s \in \mathbb{Z}$ úgy, hogy $\left(\frac{s}{q_n}\right) = -1$. Legyen $b \in \mathbb{Z}$ megoldása a következő kongruenciarendszernek:

$$\begin{cases} x \equiv 1 \pmod{e_i}, & i = 1, \dots, r \\ x \equiv 1 \pmod 8 \\ x \equiv 1 \pmod{q_i}, & i = 1, \dots, n-1 \\ x \equiv s \pmod{q_n} \end{cases}.$$

(Partikulárisan b páratlan, mert $b \equiv 1 \pmod 8$.) Legyen $b = p_1 \dots p_n$ a b felbontása prímtényezőkre. Mivel $b \equiv 1 \pmod 8$ következik, hogy $\left(\frac{2}{b}\right) = 1$ és $\left(\frac{q_i}{b}\right) = \left(\frac{b}{q_i}\right)$. Következik, hogy

$$\left(\frac{a}{b}\right) = \left(\frac{2}{b}\right)^e \left(\frac{q_1}{b}\right) \dots \left(\frac{q_{n-1}}{b}\right) = 1 \left(\frac{b}{q_1}\right) \dots \left(\frac{b}{q_{n-1}}\right)\left(\frac{b}{q_n}\right) = \left(\frac{1}{q_1}\right) \dots \left(\frac{1}{q_{n-1}}\right)\left(\frac{1}{q_n}\right) = -1.$$

Másfelől $-1 = \left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\dots\left(\frac{a}{p_n}\right)$. Tehát $\exists i \in \{1,\dots,n\}$ úgy, hogy $\left(\frac{a}{p_i}\right) = -1$. Mivel $e_j \nmid b$, $i = 1,\dots,r$, következik, hogy $p_i \notin \{2, e_1,\dots,e_r\}$.

II. eset: $n = 0$, $a = 2$.

Legyenek $e_1,\dots,e_r$ prímek úgy, hogy $2,3 \notin \{e_1,\dots,e_r\}$ és $\left(\frac{2}{e_r}\right) = -1$, $i = 1,\dots,r$. Legyen $b = 8e_1\dots e_r + 3$. Tehát $2 \nmid b$, $3 \nmid b$, $e_i \nmid b$, $\forall i = 1,\dots,r$.

Legyen $b = p_1\dots p_m$ a b felbontása prímtényezőkre. Mivel $b \equiv 3 \pmod 8$, következik, hogy $\left(\frac{2}{b}\right) = -1$. Másfelől $-1 = \left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right)\dots\left(\frac{2}{p_m}\right)$.

Tehát $\exists i$ úgy, hogy $\left(\frac{2}{p_i}\right) = -1$. Végül vegyük észre, hogy $p_i \notin \{2,3,e_1,\dots,e_r\}$. ■

6.4. Kvadratikus egészek

6.4.1. Kvadratikus egészek

6.4.1. definíció. *Egy a komplex számot* **algebrai egész***nek nevezzük, ha a minimálpolinomja egész együtthatós polinom.*

6.4.2. tétel. *A racionális egészek halmaza egyelő az egész számok halmazával.*

Bizonyítás. Legyen $a \in \mathbb{Q}$ feltételezzük, hogy $\exists f \in \mathbb{Z}[X]$ úgy, hogy $f(a) = 0$. Igazoljuk, hogy $a \in \mathbb{Z}$. Valóban, legyen $a = \frac{m}{n}$ irreducibilis tört, és legyen $f = \sum_{i=0}^{s} a_i X^i \in \mathbb{Z}[X]$, $\quad a_s = 1$, $\quad s \geq 1$. Akkor

$$f(a) = 0 \;\Rightarrow\; a_0 n^s + a_1 m n^{s-1} + \dots + a_{s-1} m^{s-1} n + a_s m^s = 0, \;\Rightarrow\; n \mid a_s m^s.$$

Mivel $(n,m) = 1$, következik, hogy $n \mid a_s = 1$, tehát $n = 1$, és $a \in \mathbb{Z}$. ■

6.4.3. definíció. Legyen $K/\mathbb{Q}$ egy testbövités. Ha $[K:\mathbb{Q}] = 2$ akkor K-t **kvadratikus test**nek nevezzük.

6.4.4. definíció. Legyen $d \in \mathbb{Z}$. Azt mondjuk, hogy d **négyzetmentes**, ha $d \neq 0,1$ és $\forall p$ prímszám esetén $p^2 \nmid d$, azaz $d \in \{-1, \pm 2, \pm 3, \pm 5, \pm 6, \dots\}$.

6.4.5. tétel. *Legyen $\mathbb{Q} \leqslant K \leqslant \mathbb{C}$, $[K:\mathbb{Q}] = 2$. Akkor $\exists d \in \mathbb{Z}$ négyzetmentes szám úgy, hogy $K = \mathbb{Q}(\sqrt{d})$.*

Bizonyítás. Tudjuk, hogy $K/\mathbb{Q}$ véges bővítés, $\operatorname{char}\mathbb{Q} = 0 \Rightarrow K/\mathbb{Q}$ szeparábilis $\Rightarrow \exists \alpha \in K$ primitív elem úgy, hogy $K = \mathbb{Q}(\alpha)$. Legyen $m_{\mathbb{Q},\alpha} \in \mathbb{Q}[X]$ az α minimálpolinomja:

$$m_{\mathbb{Q},\alpha} = X^2 + aX + b \in \mathbb{Q}(\sqrt{d}) \;\Rightarrow\; \alpha = \frac{-a + \sqrt{a^2 - 4b}}{2}.$$

Az $a^2 - 4b$ szám, nem teljes négyzet mert $\alpha \notin \mathbb{Q}$. Következik, hogy $\alpha = r + s\sqrt{d}$, ahol $r, s \in \mathbb{Q}$, $s \neq 0$ és d négyzetmentes. Azonnal belátható, hogy $\mathbb{Q}(\alpha) = \mathbb{Q}(r + s\sqrt{d}) = \mathbb{Q}(\sqrt{d})$. ■

6.4.6. definíció. Legyen $\alpha \in K = \mathbb{Q}(\sqrt{d})$.

a) Azt mondjuk, hogy $\alpha \in \mathbb{Q}$ **kvadratikus egész**, ha $m_{\mathbb{Q},\alpha} \in \mathbb{Z}[X]$.

b) Feltételezzük, hogy

$$m_{\mathbb{Q},\alpha} = X^2 + ax + b, \quad \alpha \notin \mathbb{Q},$$

ahol az $m_{\mathbb{Q},\alpha}$ gyökei α, $\bar{\alpha}$. Értelmezés szerint, $\operatorname{Tr}(\alpha) + \bar{\alpha} = -a$ az α **nyoma** és $N(\alpha) = \alpha\bar{\alpha} = b$ az α **normája**. Akkor α kvadratikus egész $\Leftrightarrow \operatorname{Tr}(\alpha), N(\alpha) \in \mathbb{Z}$.

Jelöljük a kvadratikus egészek halmazát A_K-val: $A_K = \{\alpha \in K \mid \alpha \text{ kvadratikus egész}\}$. Ha $\alpha = x + y\sqrt{d} \in K$, akkor $\operatorname{Tr}(\alpha) = 2x$ és $N(\alpha) = x^2 - dy^2$.

6.4.7. tétel. *Legyen $K = \mathbb{Q}(\sqrt{d})$ egy kvadratikus test és A_K az egészek halmaza.*

1) *Ha $d \equiv 2 \pmod 4$ vagy $d \equiv 3 \pmod 4$ akkor $\{1, \sqrt{d}\}$ bázis $\mathbb{Z}$ felett A_K-ban, azaz*

$$A_K = \mathbb{Z}[\sqrt{d}] = \left\{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\right\}.$$

2) *Ha $d \equiv 1 \pmod 4$ akkor $\left\{1, \frac{1+\sqrt{d}}{2}\right\}$ bázis $\mathbb{Z}$ felett A_K-ban, azaz*

$$A_K = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right] = \left\{a + b\frac{1+\sqrt{d}}{2} \mid a, b \in \mathbb{Z}\right\} \supset \mathbb{Z}[\sqrt{d}].$$

Bizonyítás. Legyen $\alpha = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, $y \neq 0$. Akkor

$$\alpha \in A_K \Leftrightarrow \mathrm{Tr}(\alpha),\ N(\alpha) \in \mathbb{Z} \Leftrightarrow 2x,\ x^2 - y^2 d \in \mathbb{Z}.$$

Következik, hogy $(2x)^2 - (2y)^2 d \in 4\mathbb{Z}$.

Igazoljuk, hogy $2y \in 4\mathbb{Z}$. Valóban, feltételezzük, hogy $y \notin \mathbb{Z}$ Ekkor $2y = \frac{s}{pt}$, ahol p prím, $s, t \in \mathbb{Z}$, $p \nmid s$. Innen $ds^2 = p^2t^2w$, ahol $w \in \mathbb{Z}$, tehát $p^2 \mid d$ ellentmondás, tehát $2y \in \mathbb{Z}$.

Legyen $2x = u$, $2y = v$. Akkor $\alpha \in A_K \Leftrightarrow u, v \in \mathbb{Z},\ u^2 - dv^2 \equiv 0 \pmod 4$.

Ha $d \equiv 2 \pmod 4$ vagy $d \equiv 3 \pmod 4$ akkor $u^2 - v^2 d \equiv 0 \pmod 4 \Leftrightarrow u, v$ párosak, azaz $x, y \in \mathbb{Z}$. Tehát ha $d \equiv 2 \pmod 4$ vagy $d \equiv 3 \pmod 4$, akkor $\alpha = x + y\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$.

Ha $d \equiv 1 \pmod 4$ akkor $u^2 - v^2 d \equiv 0 \pmod 4 \Leftrightarrow u, v$ párosak vagy u, v páratlanok, azaz

$$A_K = \{\frac{u}{2} + \frac{v}{2}\sqrt{d} \mid u, v \in \mathbb{Z} \text{ azonos párosságúak}\}.$$

Tehát ha $d \equiv 1 \pmod 4$ akkor $\alpha = x + y\sqrt{d}$ ahol $x, y \in \mathbb{Z}$, vagy $\alpha = x + y\frac{1+\sqrt{d}}{2}$, ahol $x = \frac{u}{2}$, $y = \frac{v}{2}$ és $u, v \in \mathbb{Z}$ páratlanok. ■

6.88. feladat. Legyen $K = \mathbb{Q}(\frac{-77+\sqrt{76}}{36})$. A fenti jelölésekkel, határozzuk meg d-t és A_K-t.

6.89. feladat. Igazoljuk, hogy A_K részgyűrűje $\mathbb{C}$-nek (tehát A_K integritástartomány).

A következő lemmák bizonyítását is az olvasóra bizzuk.

6.4.8. lemma. *Legyen $K = \mathbb{Q}(\sqrt{d})$ egy kvadratikus test és A_K az egészek halmaza.*
1) *A norma teljesen multiplikativ függvény, azaz $N(\alpha\beta) = N(\alpha)N(\beta)$, $\forall \alpha, \beta \in A_K$.*
2) *α invertálható A_K-ban $\Leftrightarrow |N(\alpha)| = 1$.*
3) *Ha $|N(\alpha)| = p$ prímszám, akkor α irreducibilis A_K-ban.*

Bizonyítás. 1) Legyen $\alpha = a + b\sqrt{d}$ és $\beta = e + f\sqrt{d}$. Először, igazoljuk, hogy $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$. Valóban,

$$\overline{\alpha\beta} = \overline{(a + b\sqrt{d})(e + f\sqrt{d})} = \overline{ae + bfd + (af + be)\sqrt{d}} = ae + bfd - (af + be)\sqrt{d}$$
$$\overline{\alpha}\overline{\beta} = (a - b\sqrt{d})(e - f\sqrt{d}) = ae + bfd - (af + be)\sqrt{d}$$

Innen $N(\alpha\beta) = \alpha\beta\overline{\alpha\beta} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta)$ ■

6.4.9. lemma (invertálható elemek imaginárius esetben). *Legyen $d < 0$.*
1) *$U(A_K) = \{1, -1\}$, ha $d \neq -1, -3$.*
2) *Ha $d = -1$, akkor $U(\mathbb{Z}[i]) = \{1, i - 1, -i\}$.*
3) *Ha $d = -3$, akkor $U(\mathbb{Z}[\frac{1+i\sqrt{3}}{2}]) = \{1, \epsilon, \epsilon^2, \epsilon^3, \epsilon^4, \epsilon^5\}$, ahol $\epsilon = \frac{1+i\sqrt{3}}{2} = \cos\frac{2\pi}{6} + i\sin\frac{2\pi}{6}$.*

6.4.2. Prímszámok felbontása A_K-ban

6.4.10. lemma. *Legyen $K = \mathbb{Q}(\sqrt{d})$ egy kvadratikus test és $A = A_K$ az egészek gyűrűje.*
1) *Ha p prímszám, akkor vagy p irreduciblis A-ban, vagy $p = \pi_1\pi_2$, ahol $\pi_1, \pi_2 \in A_K$ irreducibilisek.*
2) *p irreducibilis A-ban $\Leftrightarrow A/Ap$ test.*
3) *$p \simeq \pi_1\pi_2$, ahol $\pi_1 \nsim \pi_2$ irreducibilisek A-ban $\Leftrightarrow A/Ap$ izomorf két test szorzatával.*
4) *$p \simeq \pi^2$, ahol π irreducibilis A-ban $\Leftrightarrow A/Ap$-ban létezik nemnulla nilpotens elem.*

6.4.11. tétel. *Legyen $p > 2$ egy prímszám. Legyen $K = Q(\sqrt{d})$ és $A := A_K$. Ekkor:*
1) *$p \simeq \pi_1\pi_2$, ahol $\pi_1 \nsim \pi_2$ irreducibilisek A-ban $\Leftrightarrow (\frac{d}{p}) = 1$.*
2) *p irreducibilis A-ban $\Leftrightarrow (\frac{d}{p}) = -1$.*
3) *$p \simeq \pi^2$, ahol π irreducibilis A-ban $\Leftrightarrow p \mid d$.*

Bizonyítás. Be fogjuk bizonyítani mindkét esetben, hogy $A/pA \simeq Z[\sqrt{d}]/pZ[\sqrt{d}]$. Igazoljuk, hogy a $Z[\sqrt{d}] \hookrightarrow A \to A/Ap$ összetett kanonikus morfizmus szürjektív és a magja $Z[\sqrt{d}] \cap Ap$.

Valóban, ha $d \equiv 1 \pmod 4$, és ha $a, b \in Z$ és b páratlan, akkor

$$(a + b\frac{1+\sqrt{d}}{2}) - (a + (b+p)\frac{1+\sqrt{d}}{2}) = -p\frac{1+\sqrt{d}}{2},$$

és $b + p$ páros, tehát $x = a + (b+p)\frac{1+\sqrt{d}}{2} \in Z[\sqrt{d}]$, vagyis $a + b\frac{1+\sqrt{d}}{2} \equiv x \pmod{Ap}$, ahol $x \in Z[\sqrt{d}]$. Tehát a morfizmus szürjektív.

Igazoljuk, hogy $Z[\sqrt{d}] \cap Ap = pZ[\sqrt{d}]$; valóban evidens, hogy $pZ[\sqrt{d}] \subseteq Z[\sqrt{d}]$ és fordítva, $a + b\sqrt{d} = p(a' + b'\frac{1+\sqrt{d}}{2}) \in Z[\sqrt{d}] \cap Ap$, ahol a, b, $a', b' \in Z \Rightarrow a = pa' + p \cdot \frac{b'}{2}$ és $b = p \cdot \frac{b'}{2}$; ahol p páratlan, tehát b' páros innen $a' + b'\frac{1+\sqrt{d}}{2}$.

Az 1. izomorfizmustételből kapjuk, hogy $Z[\sqrt{d}]/pZ[\sqrt{d}] \simeq A/Ap$.

Másfelől a

$$\varphi : Z[X] \to Z[\sqrt{d}], \quad \varphi(f) = f(\sqrt{d})$$

morfizmus szürjektív, és $\operatorname{Ker}\varphi = (X^2 - d)Z[X]$. Valóban a $(X^2 - d)Z[X] \subseteq \operatorname{Ker}\varphi$ bennfoglalás evidens, és fordítva, ha $f \in \operatorname{Ker}\varphi$, akkor $f(\sqrt{d}) = 0$ tehát, mivel $X^2 - d$ az $\sqrt{d}$ minimálpolinomja Q felett, következik, hogy $f = (X^2 - d)g$, ahol $g \in Q[X]$. Mivel $f \in Z[X]$, következik, hogy $g \in Z[X]$, tehát $f \in (X^2 - d)Z[x]$.

Tehát $\mathbb{Z}[X]/(X^2 - d) \simeq \mathbb{Z}[\sqrt{d}]$. Következik, hogy

$$\begin{aligned} A/Ap &\simeq \mathbb{Z}[\sqrt{d}]/p\mathbb{Z}[\sqrt{d}] \simeq (\mathbb{Z}[X]/(X^2 - d))/p(\mathbb{Z}[X]/(X^2 - d)) = \\ &= (\mathbb{Z}[X]/(X^2 - d))/p\mathbb{Z}[X] + (X^2 - d)\mathbb{Z}[X]/(X^2 - d)) \simeq \\ &\simeq \mathbb{Z}[X]/(p, X^2 - d) \simeq (\mathbb{Z}[X]/p\mathbb{Z}[X])/((p, X^2 - d)/p\mathbb{Z}[X]) \simeq \\ &\simeq \mathbb{Z}_p[X]/(X^2 - \bar{d}), \end{aligned}$$

ahol $\bar{d}$ a d osztálya modulo p. A fenti izomorfizmus sorozatban a $\mathbb{Z}[X]/p\mathbb{Z}[X] \simeq \mathbb{Z}/p\mathbb{Z}[X]$ kanonikus izomorfizmust használtuk, ami következik a

$$\mathbb{Z}[X] \to \mathbb{Z}_p[X], \quad a_0 + a_1X + \cdots + a_mX^m \mapsto \bar{a}_0 + \bar{a}_1X + \cdots + \bar{a}_mX^m$$

szürjektív morfizmusból.

Ha $X^2 - \bar{d} \in \mathbb{Z}_p[X]$ irreducibilis $\mathbb{Z}_p[X]$-ben, akkor $\mathbb{Z}_p[X]/(X^2 - \bar{d})$ test, tehát A/Ap is test, vagyis p irreducibilis A-ban (mivel Ap maximális ideál).

Ha $X^2 - \bar{d} \in \mathbb{Z}_p[X]$ nem irreducibilis $\mathbb{Z}_p[X]$-ben, akkor két lehetőség áll fenn:

(i) $X^2 - \bar{d} = h_1h_2 \in \mathbb{Z}_p[X]$ különböző elsőfokú főpolinomok $\mathbb{Z}_p[X]$-ből; ebben az esetben, mivel $(h_1, h_2) = 1$, alkalmazzuk a kínai maradék tételt:

$$A/Ap \simeq \mathbb{Z}_p[X]/(h_1h_2) \simeq \mathbb{Z}_p[X]/(h_1) \times \mathbb{Z}_p[X]/(h_2)$$

Továbbá $h_i = X - \bar{a}_i \in \mathbb{Z}_p[X]$, $i = 1, 2$, és $\mathbb{Z}_p[X]/(X - \bar{a}_i) \simeq \mathbb{Z}_p$. Tehát ebben az esetben kapjuk, hogy $A/Ap \simeq \mathbb{Z}_p \times \mathbb{Z}_p$, vagyis p felbontható A-ban.

(ii) $X^2 - \bar{d} = h^2$, ahol $h = X - \bar{a} \in F_p[X]$, vagyis $X^2 - \bar{d} = X^2 - 2\bar{a}X + \bar{a}^2$; mivel $p \neq 2$, következik, hogy $\bar{a} = \bar{0}$, vagyis $\bar{d} = -\bar{a}^2$-ből következik, hogy $p \mid d$, és fordítva, $p \mid d \Rightarrow X^2 - \bar{d} = X^2$.

Tehát $p \mid d \Leftrightarrow X^2 - \bar{d} = h^2$, ahol $h \in \mathbb{Z}_p[X]) \Leftrightarrow X^2 - \bar{d} = X^2 \Leftrightarrow A/Ap$ tartalmaz nemnula nilpotens elemet (mivel a $\mathbb{Z}_p[X]/(X^2)$ gyűrűben az $X + /(X^2)$ elem nem nulla és $(X + /(X^2))^2 = 0$).

Ha továbbá p nem osztja d-t, akkor a fentebb említetteknek megfelelően kapjuk, hogy: p felbontható A-ban $\Leftrightarrow$ A/Ap izomorf két test szorzatával $\Leftrightarrow X^2 - \bar{d} = (X + \bar{a})(X + \bar{b})$, ahol $a \neq b \Leftrightarrow \bar{a} + \bar{b} = \bar{0}$, $\bar{a}\bar{b} = -\bar{d}$, $\bar{a}^2 = \bar{d} \Leftrightarrow (\frac{d}{p}) = 1$.

Vegül kizárással marad, hogy p irreducibilis A-ban $\Leftrightarrow p \nmid d$ és $\left(\frac{d}{p}\right) = -1$. ■

6.4.12. tétel. *Legyen* $p = 2$. *Az előző tétel jelöléseit alkalmazva*

1) $2 \sim \pi^2 \iff d \equiv 2 \pmod 4$, $d \equiv 3 \pmod 4$.

2) 2 *irreducibilis* A*-ban* $\iff d \equiv 5 \pmod 8$.

3) $2 = \pi_1\pi_2$, *ahol* $\pi_1 \nsim \pi_2$ *irreducibilis elemek* A*-ban* $\iff d \equiv 1 \pmod 8$.

Bizonyítás. Ha $d \equiv 2 \pmod 4$ vagy $d \equiv 3 \pmod 4$, akkor $A = \mathbb{Z}[\sqrt{d}]$ és tehát

$$A/2A = \mathbb{Z}[\sqrt{d}]/2\mathbb{Z}[\sqrt{d}] \simeq \mathbb{Z}_2[X]/(X^2 - \bar{d}),$$

az előző tétel bizonyítása szerint. Ha $\bar{d} = \bar{0}$ vagy $\bar{d} = \bar{1}$, $X^2 - \bar{d} = X^2$ vagy $X^2 - \bar{d} = (X - \bar{1})^2$, tehát A/2A-nak nemnulla, nílpotens elemei vannak (mivel $A/2A \simeq \mathbb{Z}_2[X]/(h^2)$, ahol $h \in \mathbb{Z}_2[X]$ egy elsőfokú polinom és $h + (h^2)$ nemnulla elem, melynek négyzete 0-val egyenlő).

Ha $d \equiv 1 \pmod 4$, akkor $A = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ és mitöbb $\mathbb{Z}[\frac{1+\sqrt{d}}{2}] \simeq \mathbb{Z}[X]/(X^2 - X - \frac{d-1}{4})$, mivel $X^2 - X - \frac{d-1}{4} \in \mathbb{Z}[X]$ az $\frac{1+\sqrt{d}}{2}$ minimálpolinomja $\mathbb{Q}$ felett. Tehát

$$\begin{aligned} A/2A &\simeq (\mathbb{Z}[X]/(X^2 - X - a))/2(\mathbb{Z}[X]/(X^2 - X - a)) = \\ &= (\mathbb{Z}[X]/(X^2 - X - a))/(X^2 - X - a)\mathbb{Z}[X] + 2\mathbb{Z}[X]/(X^2 - X - a) \simeq \\ &\simeq \mathbb{Z}[X]/(X^2 - X - a, 2) \simeq \\ &\simeq (\mathbb{Z}[X]/2\mathbb{Z}[X])/((X^2 - X - a, 2)/2\mathbb{Z}[X]) \simeq \\ &\simeq \mathbb{Z}_2[X]/\left(X^2 - X - \bar{a}\right), \end{aligned}$$

ahol $\bar{a}$ az a egész szám osztálya modulo 2.

Ha $a \equiv 1 \pmod 2$, vagyis $d \equiv 5 \pmod 8$, akkor $X^2 - X - \bar{1}$ irreducibilis $\mathbb{Z}_2[X]$-en (mert nincs gyöke $\mathbb{Z}_2$-ben), vagyis $A/2A$ test, és akkor 2 irreducibilis A-ban.

Ha $a \equiv 0 \pmod 2$, vagyis $d \equiv 1 \pmod 8$, akkor $X^2 - X - \bar{a} = X(X - \bar{1})$ vagyis

$$A/2A \simeq \mathbb{Z}_2[X]/(X(X-\bar{1})) \simeq \mathbb{Z}_2[X]/(X) \times \mathbb{Z}_2[X]/(X-\bar{1}) \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$$

vagyis 2 felbontható A-ban. ■

6.4.3. Euklideszi gyűrűk

Legyen $K = \mathbb{Q}(\sqrt{d})$ és $A := A_K$ és $N : A \to \mathbb{Z}$, $n(z) = |z\bar{z}|$ az euklideszi norma.

6.4.13. lemma. (A, N) *euklideszi gyűrű* $\Leftrightarrow$ $(\forall) z \in \mathbb{Q}(\sqrt{d})$ $(\exists) q \in \mathbb{Z}[\sqrt{d}]$ *úgy, hogy* $N(z-q) < 1$.

Bizonyítás. Legyen $z = a/b \in K$, ahol $a, b \in A$, $b \neq 0$. Létezik $q, r \in A$ úgy, hogy $a = bq + r$, $N(r) < N(b)$. Ekkor $N(z-q) = N(r/b) = N(r)/N(b) < 1$.

Fordítva, legyen $a, b \in A$, $b \neq 0$. Legyen $z = a/b$. Akkor létezik $q \in A$ úgy, hogy $N(z-q) < 1$. Legyen $r := a - bq$, tehát $a = bq + r$; akkor $N(r) = N(a - bq) = N(b(a/b - q)) = N(b)N(z-q) < N(b)$. ■

Immaginárius euklidészi kvadratikus testek

6.4.14. tétel. *Legyen* $d < 0$. *Ekkor* (A, N) *euklidészi akkor és csak akkor, ha* $d \in \{-1, -2, -3, -7, -11\}$.

Bizonyítás. Az előbbi lemma szerint olyan $\mathbb{Q}(\sqrt{d})$ testeket kell találnunk melyekre adott $z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ esetén létezik $q \in A$ úgy hogy $N(z-q) < 1$. Két esetet különböztetünk meg:

Legyen $d \equiv 2 \pmod 4$ vagy $d \equiv 3 \pmod 4$, és feltételezzük, hogy A euklidészi a normára nézve. Ha $z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$, létezik $q = a + b\sqrt{d} \in \mathbb{Z}[\sqrt{d}]$ úgy hogy $N(z-q) = (x-a)^2 - d(y-b)^2 < 1$. Legyen $x = y = \frac{1}{2}$; kapjuk, hogy

$$\frac{1}{4} + \frac{1}{4}m \leq \left(\frac{1}{2} - a\right)^2 - d\left(\frac{1}{2} - b\right)^2 < 1,$$

ahol $m = -d$. Innen $m + 1 < 4$, azaz $m < 3$ tehát $d > -3$. Következtetésképpen, a $d \equiv 2 \pmod 4$ vagy $d \equiv 3 \pmod 4$ esetben, ha $A = \mathbb{Z}[\sqrt{d}]$ euklidészi, akkor $d = -1$ vagy $d = -2$.

Fordítva, ha $d = -1$ vagy $d = -2$ akkor legyenek a és b az adott x és y racionális számokhoz legközelebb eső egész számok. Kapjuk hogy $|x - a| \leq \frac{1}{2}$ és $|y - b| \leq \frac{1}{2}$, tehát ha $q = a + b\sqrt{d}$, akkor

$$N(z-q) = (x-a)^2 - d(y-b)^2 \leq \frac{1}{4} + m\frac{1}{4} = \frac{m+1}{4} < 1,$$

ahol $m = -d = 1$ vagy $m = -d = 2$. Tehát $\mathbb{Z}[i] = \mathbb{Z}[\sqrt{-1}]$ és $\mathbb{Z}[\sqrt{-2}]$ euklidészi gyűrűk a normára nézve.

Legyen $d \equiv 1 \pmod 4$, és feltételezzük, hogy $A = \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ euklidészi a normára nézve. Ekkor bármely $z = x + y\sqrt{d} \in \mathbb{Q}(\sqrt{d})$ esetén létezik $q = a + \frac{b}{2}(1 + \sqrt{d}) \in \mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$, melyre

$$N(z-q) = \left(x - a - \frac{b}{2}\right)^2 - d\left(y - \frac{b}{2}\right)^2 < 1.$$

Legyen $x = y = \frac{1}{4}$; kapjuk, hogy

$$\frac{1}{16} + \frac{1}{16}m \leq \left(\frac{1}{4} - a - \frac{b}{2}\right)^2 - d\left(\frac{1}{4} - \frac{b}{2}\right)^2 < 1,$$

ahol $m = -d$ (mert $1 - 4a - 2b \neq 0$ és $1 - 2b \neq 0$). Tehát $m + 1 < 16$, vagyis $m < 15$. Mivel $d \equiv 1 \pmod 4$, kapjuk hogy $m \equiv 3 \pmod 4$ azaz $m = 3$ vagy $m = 7$ vagy $m = 11$. Ezért ha $d \equiv 1 \pmod 4$ és $\mathbb{Z}\left[\frac{1+\sqrt{d}}{2}\right]$ euklidészi a normára nézve, akkor $d = -3$ vagy $d = -7$ vagy $d = -11$.

Fordítva, legyen $d = -3$ vagy $d = -7$ vagy $d = -11$. Ha, $x, y \in \mathbb{Q}$ adottak, akkor meghatározhatjuk az $a, b \in \mathbb{Z}$ számokat úgy hogy $|2y - b| \leq \frac{1}{2}$ és $\left|x - \frac{b}{2} - a\right| \leq \frac{1}{2}$, azaz b a $2y$-hoz legközelebb levő egész szám, és az így meghatározott b esetén a lesz az $x - \frac{b}{2}$-höz legközelebb levő egész szám. Legyen $q = a + \frac{b}{2}(1 + \sqrt{d})$. Kapjuk, hogy

$$\begin{aligned} N(z-q) &= N\left(x - a - \frac{b}{2} + \sqrt{d}\left(y - \frac{b}{2}\right)\right) = \left(x - a - \frac{b}{2}\right)^2 - d\left(y - \frac{b}{2}\right)^2 \leq \\ &\leq \frac{1}{4} + m\frac{1}{16} = \frac{4+m}{16} \leq \frac{4+11}{16} = \frac{15}{16} < 1, \end{aligned}$$

ahol $m = -d$. Tehát $\mathbb{Z}\left[\frac{1+\sqrt{-3}}{2}\right]$, $\mathbb{Z}\left[\frac{1+\sqrt{-7}}{2}\right]$ és $\mathbb{Z}\left[\frac{1+\sqrt{-11}}{2}\right]$ euklidészi gyűrűk a normára nézve. ■

Valós euklidészi kvadratikus testek

Ha $d > 0$ akkor a az euklideszi kvadratikus testek meghatározása sokkal nehezebb. A pontos valaszat a következő tétel adja meg:

6.4.15. tétel (Chatland–Davenport, 1950; Barnes–Swinnerton-Dyer, 1952). *Legyen* $d > 0$. *Ekkor* A *euklidészi a normára vonatkozóan akkor és csak akkor, ha* $d \in \{2, 3, 5, 6, 7, 11, 13, 17, 19, 21, 29, 33, 37, 41, 57, 73\}$.

Példa olyan főideálgyűrűre, amely nem euklideszi gyűrű

A következőkben bebizonyítjuk azt, hogy a $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ kvadratikus egészek gyűrűje egy főideálgyűrű.

6.4.16. lemma. *Legyen* A *a* $K = \mathbb{Q}(i\sqrt{d})$ *kvadratikus egészek gyűrűje. Feltételezzük, hogy bármely* $x, y \in A$ *nem nulla elemek esetén, ha* $N(x) \geq N(y)$, *akkor* $y \mid x$ *vagy létezik* $z, w \in A$ *úgy, hogy* $0 < N(xz - yw) < N(y)$.

Akkor A *főideálgyűrű.*

Bizonyítás. Legyen $I \neq 0$ A-nak egy ideálja, és legyen $y \in A$ úgy, hogy $N(y) = \min\{N(t) \mid t \in I \setminus \{0\}\}$. Legyen $x \in I \setminus \{0\}$; bármely $z, w \in A$ esetén $xz - yw \in I$, tehát $xz - yw = 0$ vagy $N(xz - yw) \geq N(y)$. Következik, hogy $y \mid x$, tehát $x \in Ay$ bármely $x \in I$ esetén, vagyis $I = Ay$, ami azt mutatja, hogy A főideálgyűrű. ■

6.4.17. tétel. *A* $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ *főideálgyűrű, de nem euklideszi gyűrű.*

Bizonyítás. A 6.4.14. tételből következik, hogy $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ nem euklideszi gyűrű. Ahhoz, hogy bebizonyítsuk, hogy $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ főideálgyűrű, meg kell vizsgálnunk, hogy teljesíti-e az előző lemma feltételeit.

Legyen $x, y \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right] \setminus \{0\}$ úgy, hogy $y \nmid x$. Ekkor $0 < N(xz - yw) < N(y) \Leftrightarrow 0 < N(\frac{x}{y} \cdot z - w) < 1$. Jelöljük

$$\frac{x}{y} = \frac{a + bi\sqrt{19}}{c} \in \mathbb{Q}(i\sqrt{19}),$$

ahol $a, b, c \in \mathbb{Z}$, $(a, b, c) = 1$, ami lehetséges mivel, ha $\frac{x}{y} \in \mathbb{Z}[i\sqrt{19}]$, akkor $\frac{x}{y} \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$, vagyis $y \mid x$, ami lehetetlen.

Feltételezzük, hogy $c \geq 5$. Legyen $d, e, f, q, r \in Z$ úgy, hogy $ae + bd + cf = 1, ad - 19be = cq + r$ és $|r| \leq \frac{c}{2}$. Legyen $z := d + ei\sqrt{19}$, $w := q - fi\sqrt{19}$. Akkor

$$\frac{x}{y} \cdot z - w = \frac{(a + bi\sqrt{19})(d + ei\sqrt{19})}{c} - (q - fi\sqrt{19}) = \frac{(ad - 19be) + (bd + ae)i\sqrt{19}}{c} - q + fi\sqrt{19} =$$
$$= \frac{cq + r + (1 - cf)i\sqrt{19}}{c} - q + fi\sqrt{19} = \frac{r}{c} + \frac{i\sqrt{19}}{c}.$$

Evidens, hogy $\frac{x}{y}z - w \neq 0$ és $N(\frac{x}{y}z - w) = N(\frac{r}{c} + \frac{i\sqrt{19}}{c}) = \frac{r^2+19}{c^2}$. Ha $c = 5$, akkor mivel $|r| \frac{c}{2}$, kapjuk, hogy $|r| \leq 2$, vagyis $r^2 + 19 \leq 23 < c^2$. Ha $c > 5$, akkor mivel $|r| \leq \frac{c}{2}$, kapjuk, hogy $\frac{r^2+19}{c^2} \leq \frac{\frac{c^2}{4}+19}{c^2} < 1$, mivel $c^2 > \frac{4 \cdot 19}{3}$.

Tehát, ha $c \geq 5$, akkor létezik $z, w \in \mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ úgy, hogy $0 < N(\frac{x}{y} \cdot z - w) < 1$. A továbbiakban a következő eseteket kell megvizsgálni: $c = 2$, $c = 3$ vagy $c = 4$.

(1) Legyen $c = 2$. Mivel $y \nmid x$ és $(a, b, c) = 1$, következik, hogy a és b különböző párosságuak (mert $Z\left[\frac{1+i\sqrt{19}}{2}\right] = \{\frac{u+vi\sqrt{19}}{2} \mid u, v \in Z$ azonos párosságú$\}$). Legyen $z = 1$ és $w = \frac{(a-1)+bi\sqrt{19}}{2}$. Evidens, hogy $z, w \in Z\left[\frac{1+i\sqrt{19}}{2}\right]$, $\frac{x}{y} \cdot z - w = \frac{1}{2} \neq 0$ és $0 < N\left(\frac{x}{y} \cdot z - w\right) < \frac{1}{4} < 1$.

(2) Legyen $c = 3$. Akkor $(a, b, c) = 1$, tehát $a^2 + 19b^2 \equiv a^2 + 19b^2 \neq 0 \pmod 3$, mert bármely $n \in \mathbb{Z}$ esetén $n^2 \equiv 0 \pmod 3$ vagy $n^2 \equiv 1 \pmod 3$. Legyen $z := a - bi\sqrt{19}$ és $w := q$, ahol $a^2 + 19b^2 = 3q + r$, ahol $r = 1$ vagy $r = 2$. Akkor $\frac{x}{y} \cdot z - w = \frac{a^2+19b^2}{3} - q = r \neq 0$ és $0 < N(\frac{x}{y} \cdot z - w) < 1$.

(3) Legyen $c = 4$. Akkor a és b nem egyszerre párosak. Abban az esetben, amikor a és b különböző párosságuak, $a^2 + 19b^2 \equiv a^2 - b^2 \not\equiv 0 \pmod 4$. Legyen $z := a - bi\sqrt{19}$ és $w := q$, ahol $a^2 + 19b^2 = 4q + r$, ahol $0 < r < 4$. Tehát $\frac{x}{y} \cdot z - w = \frac{a^2+19b}{4} - q = \frac{r}{4} \neq 0$ és $0 < N(\frac{x}{y} \cdot z - w) < 1$.

Ha a és b páratlan számok, akkor $a^2 + 19b^2 \equiv a^2 + 3b^2 \not\equiv 0 \pmod 8$, mert bármely $m \in \mathbb{Z}$ páratlan számra $m^2 \equiv 1 \pmod 8$. Legyen $z := \frac{a-bi\sqrt{19}}{2}$ és $w := q$, ahol $a^2 + 19b^2 = 8q + r$, $0 < r < 8$. Ekkor $\frac{x}{y} \cdot z - w = \frac{a^2+19b^2}{8} - q = \frac{r}{8} \neq 0$ és $0 < N(\frac{x}{y} \cdot z - w) < 1$.

Következik, hogy $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ teljesíti a 6.4.16. lemma feltételeit, tehát főideálgyűrű. ■

6.5. Diofantikus egyenletek

Ha $f \in \mathbb{Z}[X_1, X_2, \ldots, X_n]$ egy n-határozatlanú polinom és $n \geq 2$, akkor

$$f(x_1, x_2, \ldots, x_n) = 0 \tag{6.2}$$

egyenletet diofantikus egyenletnek nevezzük, ha megköveteljük, hogy a megoldások egész vagy racionális számok legyenek.

Ha $f(x_1, x_2, \ldots, x_n) = 0$ homogén polinom, akkor a $(0, 0, \ldots, 0)$-tól különböző megoldások a nem triviális megoldások. A homogén esetben a probléma, hogy racionális megoldást keressünk egyenértékű azzal, hogy egész megoldást keressünk (miért?).

A diofantikus egyenleteknek végtelen sok fajtája van; megoldásukra nincs általános módszer. A továbbiakban az egyszerübbek közül néhányat tárgyalni fogunk.

6.5.1. Az $a_1x_1 + \cdots + a_nx_n = m$ elsőfokú egyenlet

1) Legyen $n = 2$. Tekintsük az

$$ax + by = c,$$

egyenletet, ahol $a, b, c \in \mathbb{Z}$, $a \neq 0$, $b \neq 0$ adottak, $x, y \in \mathbb{Z}$ ismeretlenek.

Legyen $d = (a, b)$. Ha $\exists\,(x, y)$ megoldás, akkor $d \mid c$. Tehát, ha $d \nmid c$ akkor nincs megoldás.

Feltételezzük, hogy $d \mid c$. Legyen $a = a'd$, $b = b'd$. Keressünk egy partikuláris megoldást. $\exists u, v \in \mathbb{Z}$ úgy, hogy $d = au + bv$ (ezeket kiszámítjuk az euklideszi algoritmussal). Szorzunk c'-tel: $\Longrightarrow c = ac'u + bc'v$. Legyen $x_0 := c'u$, $y := c'v$, tehát (x_0, y_0) partikuláris megoldás.

Keressük most az általános megoldást.

$$ax + by = c \Longleftrightarrow ax + by = ax_0 + by_0 \Longleftrightarrow a\,(x - x_0) + b\,(y - y_0) = 0 \Longleftrightarrow a'(x - x_0) + b'(y - y_0) = 0.$$

Feltételezzük, hogy $(x, y) \in \mathbb{Z}$ megoldás. Következik, hogy $a' \mid b'\,(y - y_0)$, $b' \mid a'\,(x - x_0)$ De $(a', b') = 1$, tehát $a' \mid y - y_0$, $b' \mid x - x_0$. Következik, hogy $y - y_0 = a't$, ahol $t \in \mathbb{Z}$. Innen $a'\,(x - x_0) + b'a't = 0$, tehát $x - x_0 = -b't$. Így a megoldás:

$$\begin{cases} x = x_0 - b't \\ y = y_0 + a't \end{cases},$$

ahol $t \in \mathbb{Z}$. Fordítva, evidens, hogy $\forall t \in \mathbb{Z}$ esetén $(x = x_0 - b't, y = y_0 + a't)$ valóban megoldása az $ax + by = c$ egyenletnek.

2) Általában, az $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ diofantikus egyenlet akkor és csak akkor oldható meg, ha $(a_1, \ldots, a_n) \mid c$.

Valóban, ha az $a_1x_1 + a_2x_2 + \ldots + a_nx_n = c$ egyenlet megoldható, akkor $(a_1, \ldots, a_n)$ a bal oldalnak osztója, tehát osztója a jobb oldalnak is. Fordítva, tegyük fel, hogy $c = (a_1, \ldots, a_n)c'$. Tudjuk, hogy létezik $x_1', \ldots, x_n'$ egész számok melyekre:

$$a_1x_1' + a_2x_2' + \ldots + a_nx_n' = (a_1, \ldots, a_n).$$

Ezt c'-tel szorozva kapjuk, hogy:

$$x_1 = c'x_1',\ x_2 = c'x_2',\ \ldots,\ x_n = c'x_n'.$$

6.5.1. megjegyzés. Vegyük észre, hogy az $ax + by = c$ egyenlet ekvivalens az $ax \equiv c \pmod{b}$ vagy a $by \equiv c \pmod{a}$ kongruenciával.

Legyen $d = (a, b)$, akkor $a = a_1d$, $b = b_1d$ és $c = c_1d$, ahol $(a_1, b_1) = 1$. Ekkor

$$a_1x + b_1y = c_1 \Leftrightarrow a_1x \mid c_1 \pmod{b_1} \Leftrightarrow \hat{a_1}\hat{x_1} = \hat{c_1}$$

a $\mathbb{Z}_{b_1}$ maradékosztály gyűrűben. De $(a_1, b_1) = 1 \Rightarrow \exists \hat{a}_1^{-1}$ amiből következik, hogy $\hat{x} = \hat{a}_1^{-1}c_1$ az egyetlen megoldás.

6.5.2. példa. Tekintsük a $18x + 28y = 10$ egyenletet. Mivel $(18, 28) = 2 \mid 10$ következik, hogy van megoldás. Tekintsük a $9x + 14y = 5$ egyenletet. Megoldjuk a $9x \equiv 5 \pmod{14}$ kongruenciát, azaz a $\hat{9}\hat{x} = \hat{5}$ egyenletet $\mathbb{Z}_{14}$-ben. $(9, 14) = 1 \Rightarrow \exists u, v \in \mathbb{Z}$: $9u + 14v = 1$. Mivel $14 = 9 \cdot 1 + 5$, $9 = 5 \cdot 1 + 4$, $5 = 4 \cdot 1 + 1$, kapjuk, hogy $u = -3$, $v = 2$. Tehát $\hat{x} = \hat{11} \cdot \hat{5}$ a $\mathbb{Z}_{14}$ gyűrűben, azaz $x \equiv 13 \pmod{14}$.

6.5.3. példa (Az egyenlet megoldása az eggyütthatók abszolut értékének csökkentésével).
1) Tekintsük a $25x + 7y = 4$ egyenletet. Mivel $|25| > |7| \Rightarrow y$-t fejezzük ki.

$$y = \frac{4-25x}{7} = \frac{4+3x}{7} - 4x \in \mathbb{Z} \Leftrightarrow 4+3x = 7z,\ |3| < |7|$$
$$x = \frac{7z-4}{3} = \frac{6z+z-3-1}{3} = 2z - 1 + \frac{z-1}{3} \in \mathbb{Z} \Leftrightarrow z-1 = 3t \Leftrightarrow z = 3t+1$$
$$\Rightarrow x = \frac{21t+3}{3} = 7t+1,\ y = \frac{4-175t-25}{7} = -25t-3, \quad t \in \mathbb{Z}.$$

2) Oldjuk meg a $16x-23y+9z = 15$ diofantoszi egyeneletet. Célszerű a legkisebb abszolú értékű eggyütthatóval rendelkező ismeretlent kifejezni:

$$z = \frac{15-16x+23}{5} = 1 - 2x + 2y + \frac{6+2x+5y}{9}.$$

Az utolsó tagot t-vel jelölve $\frac{6+2x+5y}{9} = t$. Innen $2x + ty - 9t = -6$. Ebből ismét azt az ismeretlent fejezzük ki, amelynek együtthatója legkisebb abszolút értékű.

$$x = \frac{-6-5y+9t}{2} = -3 - 2y + 4t + \frac{-y+t}{2}.$$

Az utolsó tagot jelöljük u-val: $\frac{-y+t}{2} = u$, ahonnan $y = t - 2u$. Helyettesítsük ezt vissza x-be, majd ezt az előbb kapott z-be. Ekkor

$$x = -3 + 2t + 5u, \qquad y = t - 2u, \qquad z = 7 - t - 14u, \qquad t, u \in \mathbb{Z}$$

a tekintett diofantoszi egyenlet megoldása. Hogy ezek az értékek bármely t és u értéke mellett megoldásai a diofantoszi egyenletnek, arról behelyettesítéssel győződhetünk meg:

$$16(-3+2t+5u) - 23(t-2u) + 9(7-t-14u) = 25 + (32-23-9)t + (80+46-126)u = 25.$$

6.90. feladat. Oldjuk meg:
1) $12x + 31y = 23$; 2) $25x - 13y - 7z = 4$; 3) $6x - 5y + 4z = 8$;
4) $\begin{cases} 25x - 13y + 7z = 4 \\ 7x + 4y - 2z + 3t = 2 \end{cases}$

6.5.4. megjegyzés. Az $ax + by = c$ egyenlet egy egyenest jelent a síkban. Az egyenlet megoldhatósága azt jelenti geometriailag, hogy átmegy-e az egyenes egész koordinátáju pontokon, azaz ún. rácspontokon. Ha az $ax + by = c$ egyenes átmegy egy rácsponton, akkor végtelen sok rácsponton megy át.

6.5.2. Redukció modulo p

Feltételezzük, hogy az 6.2 egyenletnek van megoldása $\mathbb{Z}^n$-ben. Akkor $\forall p$ prímszám esetén, az

$$f(x_1, \ldots, x_n) \equiv 0 \pmod p \tag{6.3}$$

kongruenciának is van megoldása. Tehát ha $\exists p$ prím szám úgy, hogy az 6.3-nek nincs megoldása, akkor 6.2-nek sincs medoldása.

6.5.5. példa. Igazoljuk, hogy $y^2 = x^3 + 7$ egyenletnek nincs egész megoldása.
I. eset: Feltételezzük, hogy x páros megoldás, akkor $y^3 \equiv 3 \pmod 4$, ami lehetetlen.
II. eset: Feltételezzük, hogy x páratlan megoldás.

$$y^2 + 1 = x^3 + 8 \Leftrightarrow y^2 + 1 = (x+2)(x^2 - 2x + 4) \Leftrightarrow y^2 + 1 = (x+2)((x-1)^2 + 3)$$

$(x-1)^2 + 3$ páratlan, $4k - 1$ alakú, tehát $\exists p \equiv -1 \pmod 4$ úgy, hogy $p \mid (x-1)^2 + 3$, tehát $y^2 \equiv -1 \pmod p$. Innen $\left(\frac{-1}{p}\right) = 1$, tehát $p \equiv 1 \pmod 4$, ellentmondás.

6.91. feladat. Legyen p prímszám. Igazoljuk, hogy az $x^3 + py^3 + p^2z^3 = 0$ egyenletnek az egyetlen megoldása $(x, y, z) = (0, 0, 0)$.

6.92. feladat. Oldjuk meg a következő egyenletet:

$$\sqrt{x + \sqrt{x + \ldots + \sqrt{x}}} = z,$$

(y-darab gyökjel), $x, y, z \in \mathbb{Z}$.

6.93. feladat. Oldjuk meg az $y^2 + 31 = x^3$ diofantikus egyenletet.

6.5.3. A Pithagoraszi számhármasok

Az $x^2 + y^2 = z^2$ egyenlet pozitív, egész megoldásait keressük. Ezeket a megoldásokat úgy ismerjük mint Pithagoraszi számhármasok, mely elnevezés onnan ered, hogy a másodfokú diofantikus egyenletek megoldása az olyan derékszögű háromszögek keresésével kezdődött amelyekben az oldalak természetes számok.

Tegyük fel, hogy az x, y, z megoldás és legyen $d = (x, y)$, az x és y számok legnagyobb közös osztója. Tehát $d^2|z^2$, azaz $d|z$ és mivel $(x, y, z) = ((x, y), z) \Rightarrow (x, y, z) = d$. Szimetria okok miatt $(x, y, z) = (x, y) = (y, z) = (x, z)$, és

$$\left(\frac{x}{d}\right)^2 + \left(\frac{y}{d}\right)^2 = \left(\frac{z}{d}\right)^2, \qquad \left(\frac{x}{d}, \frac{y}{d}\right) = \left(\frac{y}{d}, \frac{z}{d}\right) = \left(\frac{x}{d}, \frac{z}{d}\right) = 1.$$

Az olyan x_1, y_1, z_1 megoldásokat amelyre x_1, y_1, z_1 páronként relativ prímek, az egyenlet *prímitív* megoldásainak nevezzük. Így minden x, y, z megoldás dx_1, dy_1, dz_1 alakú, ahol x_1, y_1, z_1 valamely prímitív megoldás. Fordítva, ha x_1, y_1, z_1 prímitív megoldás, akkor dx_1, dy_1, dz_1 szintén megoldás, ha d pozitív egész. Tehát elég a prímitív megoldásokat keresni, a továbbiakban ezekkel foglalkozunk.

Az x és y mindegyike nem lehet páros, de páratlanok sem lehetnek mindketten, mert, ha így lenne akkor $x^2 \equiv 1 \pmod 4$ és $y^2 \equiv 1 \pmod 4$ kongruenciákbol következne a hamis $z^2 \equiv 2 \pmod 4$ kongruencia. Mivel x és y szerepe szimetrikus, feltehetjük, hogy y páros és x páratlan. Ezzel az eredeti egyenlet a következő alakban írható:

$$\left(\frac{z+x}{2}\right)\left(\frac{z-x}{2}\right) = \left(\frac{y}{2}\right)^2,$$

ahol $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) = 1$, mert $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \mid \left(\frac{z+x}{2} + \frac{z-x}{2}\right) = z$ és $\left(\frac{z+x}{2}, \frac{z-x}{2}\right) \mid \left(\frac{z+x}{2} - \frac{z-x}{2}\right) = x$. Tehát $\frac{z+x}{2} = a^2$ és $\frac{z-x}{2} = b^2$, ahol a, $b > 0$ vegyük észre, hogy

$$(a, b) = 1, \quad a > b > 0, \quad x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Mivel z páratlan, az a és b ellenkező paritásúak.

Forditva, legyenek a és b olyan egészek, amelyekre $(a, b) = 1$, a és b ellenkező paritásúak; akkor az $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$ választással kapjuk, hogy x, y, z pozitivak és $x^2 + y^2 = (a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2 = z^2$, ahol $(x, y) = 1$ és y páros. Ezért az x, y, z az egyenlet prímitiv megoldását adják.

Az $x^4 + y^4 = z^4$ egyenlet és a végtelen leszállás módszere

A végtelen leszállás módszer alapgondolata a következő. Induljunk ki abból minden n természetes számhoz tartozik egy $P(n)$ állítás. Amenyiben létezik olyan természetes szám, amelyre $P(n)$ igaz, akkor az ilyen természetes számok között van legkisebb. Ha abból a feltételezésből, hogy n' a legkisebb természetes szám, amelyre $P(n)$ igaz, következtetni tudunk arra, hogy $P(n)$ egy n'-nel kisebb n'' számra is igaz, akkor ez az ellentmondás azt jelenti, hogy a $P(n)$ állítás minden n-re hamis.

6.5.6. tétel. *Az $x^4 + y^4 = z^2$ diofantikus egyenletnek nincs egész megoldása $xyz \neq 0$, $z > 0$ esetén.*

Pontosabban, az $x^4 + y^4 = z^2$ egyenlet egész megoldásai a triviális $x = 0$, $y, z = \pm y^2$ és $x, y = 0$, $z + \pm x^2$ megoldások.

Bizonyítás. Feltételezzük, hogy $x^4 + y^4 = z^2$ egyenletnek van ilyen megoldása, legyenek ezek x, y, z ahol z a lehető legkisebb pozitiv egész szám. Ellentmondásra jutunk, ha megmutatjuk, hogy van olyan, ettől eltérő megoldás, melyben z ennél is kisebb.

Először belátjuk, hogy x, y, z páronként relatív prímek. Valóban, ha p osztója az (x, y), akkor $p^4 \mid x^4 + y^4$, így $p^4 \mid z^2$, azaz $p^2 \mid z$ és az eredeti egyenletből következik

$$\left(\frac{x}{p}\right)^4 + \left(\frac{y}{p}\right)^4 = \left(\frac{z}{p^2}\right)^2.$$

ellentmond z minimalitásának. Hasonlóan $(x, z) = (y, z) = 1$.

Másfelől x és y nem lehet egyszerre páratlan mert, ha x és y páratlan, akkor redukáva az egyenletet modulo 4, az $z^2 \equiv 2 \pmod 4$ kongruenciához jutunk, ami lehetetlen. Tehát, legyen x páros, y páratlan; következik, hogy z páratlan.

Egyenletünket az $y^4 = (z - x^2)(z + x^2)$ alakra írjuk. Ha p osztja a $z - x^2$ és $z + x^2$ egészeket, akkor osztja az y^4, $2z$ és $2x^2$ egészeket, tehát $(z - x^2, z + x^2) = 1$. Azonban az $(z - x^2)(z + x^2)$ szorzat egy negyedik hatvány, így létezik $u, v \in \mathbb{Z}$ páratlanok, úgy, hogy $z - x^2 = u^4$, $z + x^2 = v^4$, $(u, v) = 1$. Ekkor $(v^2 - u^2)(v^2 + u^2) = 2x^2$, ahol $u^2 + v^2 \equiv 2 \pmod 4$, és $(v^2 - u^2, v^2 + u^2) = 1$. Következik, hogy létezik $a, b \in \mathbb{Z}$ úgy, hogy $v^2 - u^2 = a^2$, $v^2 + u^2 = 2b^2$. Akkor u, a, v pithagorászi számhármas, tehát $v = r^2 + s^2$, $u = r^2 - s^2$, $a = 2rs$, ahol $r, s > 0$. Továbbá $v^2 + u^2 = 2b^2 \Rightarrow r^4 + s^4 = b^2$. Ha $u = v = 1$, akkor $x = 0$ ellentmondás, teht́ $u^4 + v^4 > u^2 + v^2$, ahonnan $z = \frac{1}{2}(u^2 + v^4) > \frac{1}{2}(u^2 + v^2) = b^2 \geq b$, ami ellentmond a z minimalitásának. ■

6.5.7. megjegyzés. Abból a tényből, hogy az $x^4 + y^4 = z^2$ egyenletnek nincs pozitív megoldása, következik, hogy az $x^4 + y^4 = z^4$ egyenletnek sincs megoldása. Ez speciális esete a nagy Fermat-tételnek, amely szerint, ha $n > 2$ akkor az $x^n + y^n = z^n$ egyenletnek csak triviális egész megoldásai vannak. Az $n = 3$ esetet később tárgyaljuk.

6.5.4. A $\mathbb{Z}[i]$ Gauss-egészek gyürüje. Négyzetszámok összege

Legyen $d = -1 \equiv 3 \pmod 4$, tehát $A_K = \mathbb{Z}[i]$, melyet **Gauss-egészek** gyűrűjének nevezünk. Láttuk, hogy $\mathbb{Z}[i]$ euklideszi a normára nézve, ahol ha $\alpha = x + iy$, akkor $N(\alpha) = x^2 + y^2$. Azt is tudjuk, hogy

$$U(\mathbb{Z}[i]) = \{1, i, -1, -i\}.$$

A prímszámok felbontását már tárgyaltuk, de ebben az esetben adunk egy elemi bizonyítást is.

6.5.8. tétel. a) $2 = (1 + i)(1 - i)$, *ahol* $1 \pm i$ *irreducibilis elemek, és* $1 + i \sim 1 - i$, *azaz* $2 \sim (1 + i)^2$.

b) *Ha* p *prím úgy, hogy* $p \equiv -1 \pmod 4$, *akkor* p *irreducibilis (prím)* $\mathbb{Z}[i]$*-ben is.*

c) *Ha* p *prím úgy, hogy* $p \equiv 1 \pmod 4$, *akkor* $p = \pi\bar{\pi}$, *ahol* π, $\bar{\pi}$ *irreducibilis (prím) elemek* $\mathbb{Z}[i]$*-ben,* $\pi \nsim \bar{\pi}$.

d) *Ha* $\pi \in \mathbb{Z}[i]$ *irreducibilis(prim) elem akkor vagy* $\pi \sim 1 + i$, *vagy* $\pi \sim p = 4k + 3$ *prímszám* $\mathbb{Z}$*-ben, vagy létezik* $p = 4k + 1$ *alakú prímszám, úgy, hogy* $\pi \mid p$.

Bizonyítás. a) $2 = (1 + i)(1 - i)$, és mivel $N(1 \pm i) = 2$, következik, hogy $1 \pm i$ irreducibilis elemek. $\frac{1+i}{1-i} = \frac{(1+i)^2}{2} = \frac{1+2i-1}{2} = i$ tehát $1 + i = i(1 - i)$ és $i \in U(\mathbb{Z}[i])$.

b) Feltételezzük, hogy $p > 2$, $p = \pi\bar{\pi}$. Akkor $p^2 = N(p) = N(\pi)N(\bar{\pi}) = N(\pi)^2$, tehát $N(\pi) = p$. Ha $\pi = a + bi \Rightarrow p = a^2 + b^2$. Legyen $a = 2l$, $b = 2k + 1$; akkor $p = 4l^2 + 4k^2 + k + 1 \equiv 1 \pmod 4$, ellentmondás.

c) Feltételezzük, hogy $p \equiv 1 \pmod 4$; akkor -1 kvadratikus maradék modulo p, tehát létezik $x \in \mathbb{Z}$ úgy, hogy $x^2 \equiv -1 \pmod p$; következik, hogy $p \mid 1 + x^2 = (1 + ix)(1 - ix)$.

Ha p irreducibilis (prim) $\mathbb{Z}[i]$-ben, akkor $p \mid 1+ix$ vagy $p \mid 1-ix$ $\mathbb{Z}[i]$-ben. Tehát $\frac{1}{p}+i\frac{x}{p} \in \mathbb{Z}[i]$ ami ellentmondás. Következik, hogy p felbontható, azaz $\exists \pi, \rho \in \mathbb{Z}[i]$ úgy, hogy $p = \pi\rho$. Ha $\pi = a + bi$, $b \neq 0 \Rightarrow p = a^2 + b^2$. Azonnal belátható, hogy $\rho = \bar{\pi}$.

Igazoljuk, hogy $\pi \nsim \bar{\pi}$. Feltételezzük, hogy $\pi \sim \bar{\pi}$, azaz $\frac{\pi}{\bar{\pi}} \in U(\mathbb{Z}[i])$.

- ha $\frac{\pi}{\bar{\pi}} = 1 \Rightarrow \pi = \bar{\pi}$ ellentmondás;
- ha $\frac{\pi}{\bar{\pi}} = -1 \Rightarrow \pi = -\bar{\pi} \Rightarrow a + bi = -a + bi \Rightarrow a = 0$ ellentmondás;
- ha $\frac{\pi}{\bar{\pi}} = i \Rightarrow \pi = i\bar{\pi} \Rightarrow a + bi = ai + b \Rightarrow a = b$ ellentmondás;
- ha $\frac{\pi}{\bar{\pi}} = -i \Rightarrow \pi = -i\bar{\pi} \Rightarrow a + bi = -ai - b \Rightarrow a = -b$ ellentmondás.

d) Mivel $\mathbb{Z}[i]$ euklideszi, tehát faktoriális, akkor, ha π irreducibilis (prím) $\mathbb{Z}[i]$-ben, létezik $p \in \mathbb{Z}$ prímszám úgy, hogy $\pi \mid p$ $\mathbb{Z}[i]$-ben. Valóban, $\pi\bar{\pi} = N(\pi) \in \mathbb{Z} \Rightarrow \pi\bar{\pi} = p_1 \dots p_n$, ahol $p_i \in \mathbb{Z}$ prímszám. Mivel π prím $\mathbb{Z}[i]$-ben, következik, hogy létezik i úgy, hogy $\pi \mid p_i$ $\mathbb{Z}[i]$-ben, és alkalmazzuk az előző pontokat. ■

Pithagorászi számhármasok

Tekintsük a $x^2 + y^2 = z^2$ egyenletet. Feltételezzük, hogy (x, y, z) megoldás úgy, hogy $(x, y) = 1$. Feltételezzúk, hogy x, y páratlanok; következik, hogy z páratlan. Ekkor $\mathbb{Z}[i]$-ben

$$z^2 = (x + iy)(x - iy).$$

Először igazoljuk, hogy $z + iy$ és $x - iy$ relativ prímek $\mathbb{Z}[i]$-ben.

Legyen $\pi \in \mathbb{Z}[i]$ irreducibilis (prím) elem úgy, hogy $\pi \mid x + iy$ és $\pi \mid x - iy$. $\pi \nsim 1 + i$ mert, ha $\pi \sim 1 + i$ akkor $(1 + i)(1 - i) \sim \pi^2$, azaz $\pi^2 \mid z^2 \Rightarrow 2 \mid z^2$ ami ellentmondás. Tehát π osztja $2x$-et és $2y$-t, és mivel $\pi \nsim 1 + i$, azaz $(\pi, 2) = 1$ következik, hogy $\pi \mid x$, $\pi \mid y$. Vesszúk a π normáját, amely nem egyenlő 1-gyel; következik, hogy $N(\pi) \mid x^2$ és $N(\pi) \mid y^2$ amely ellentmond annak, hogy $(x, y) = 1$. Tehát $(x + iy, x - iy) = 1$ $\mathbb{Z}[i]$-ben.

Legyen $z = u\pi_1^{a_1} \dots \pi_s^{a_s}$, ahol $u \in U(\mathbb{Z}[i])$, $a_i \in \mathbb{N}^*$, $\pi_i \in \mathbb{Z}[i]$ primek. Mivel $(x + iy, x - iy) = 1$, következik, hogy $x + iy = u\beta^2$, ahol $\beta = a + bi$ és feltételezhetjük, hogy $u = 1$. Ekkor $x + iy = a^2 - b^2 + 2ab$. Tehát létezik $a, b \in \mathbb{Z}$ úgy, hogy

$$x = a^2 - b^2, \quad y = 2ab, \quad z = a^2 + b^2.$$

Forditva egyszerü behejettesitéssel, látjuk, hogy

$$(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2.$$

Tehát az $x^2 + y^2 = z^2$ diofantikus egyenlet megoldásai:

$$x = k(a^2 - b^2), \quad y = 2ab, \quad z = k(a^2 + b^2),$$

ahol a, b, k egész számok, a páros, b páratlan és $(a, b) = 1$.

Fermat tétele

Az alábbi eredmény azonnal következik a 6.5.8. tételből.

6.5.9. következmény (Fermat). 1) *Ha* $p = 2$ *vagy* $p = 4k+1$ *prím, akkor létezik egyetelen* $a, b \in \mathbb{Z}$ *úgy, hogy* $p = a^2 + b^2$.

2) *Ha* $p = 4k+3$ *prím, akkor az* $x^2 + y^2 = p$ *egyenletnek nincs megoldása.*

6.5.10. következmény. *Egy* 2*-nél nagyobb természetes szám akkor es csak akkor írható fel két természetes szám négyzetösszegeként, ha az* n *prímtényezőkre való felbontásában minden* $4k+3$ *alakú prímtényező páros hatványon szerepel.*

Bizonyítás. Legyen

$$S = \{x \in \mathbb{N} \mid \exists a, b \in \mathbb{N} : \ x = a^2 + b^2\}.$$

Akkor $2 \in S$ (mivel $2 = 1^2 + 1^2$), $x^2 \in S$ bármely $z \in \mathbb{Z}$ (mivel $x^2 = x^2 + 0^2$) és S zárt a szorzásra nézve, mert

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2.$$

Legyen $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$, ahol $p_i \in \mathbb{N}$ különböző prímszámok, és $a_i \geq 1$. Ha a_j páros bármely $p_j \equiv 3 \pmod 4$ esetén, akkor mivel $p_t \in S$ minden $p_t \equiv 1 \pmod 4$ esetén, kapjuk, hogy $n \in S$.

Fordítva, ha $p \equiv 3 \pmod 4$, p prím, $n = p^{2s+1}m$, ahol $s \geq 0$ és m nem osztható p-vel, akkor n nem lehet két szám négyzetösszege. Valóban, ha $n = a^2 + b^2$, ahol $a, b \in \mathbb{N}$, legyen $d := (a, b)$. Ekkor $a = da_1$ és $b = db_1$, $(a_1, b_1) = 1$. Legyen $a_1^2 + b_1^2 =: n_1$, tehát $n = d^2 n_1 = p^{2s+1}m$; innen következik, hogy $p \mid n_1$ (valóban, ha $p \mid d$ akkor a d^2 prímtényezőkre való felbontásában p páros hatványon szerepel). Ekkor p nem osztja a_1-et és b_1-et mert ez ellentmondana annak, hogy $(a_1, b_1) = 1$.

Kapjuk, hogy $0 \neq \bar{a}_1 \in \mathbb{Z}_p$, tehát létezik $c \in \mathbb{Z}$ úgy hogy $a_1 c \equiv b_1 \pmod p$. Akkor $n_1 = a_1^2 + b_1^2 \equiv a_1^2(1 + c^2) \equiv 0 \pmod p$, tehát $c^2 = -1 \pmod p$, vagyis -1 négyzetes maradék modulo p, ami ellentmondás. ■

A Fermat-tételnek adunk egy másik bizonyítását is, melyhez felhasználjuk a következő lemmát.

6.5.11. lemma (Thue). *Ha* $m > 1$ *egész szám,* $(a, m) = 1$*, akkor léteznek olyan* $0 < |x| \neq [\sqrt{m}]$, $0 < |y| \neq [\sqrt{m}]$ *egész számok, amelyre* $ax \equiv y \pmod m$.

Bizonyítás. Az állítás bizonyítása skatulyaelven alapul. Tekintjük a $0 \neq x \neq [\sqrt{m}]$, $0 \neq y \neq [\sqrt{m}]$ számokat és képezzük az összes lehetséges $ax + y$ számot Mivel x és y egyaránt $[\sqrt{m}]$ számot fut végig, ezért $([\sqrt{m}+1])^2 > m$ $ax + y$ alakú számot kapunk. A skatulyaelv szerint létezik két olyan szám amely ugyanabban a modulo m maradékosztályban van. Legyenek ezek (x_1, y_1) és az (x_2, y_2) számpárok. Akkor igazak a következők:

$$ax_1 + y_1 \equiv ax_2 + y_2 \pmod m, \quad a(x_1 - x_2) \equiv y_2 - y_1 \pmod m.$$

Az (x_1, y_1) számpárnak egyik komponense se lehet egyenlőaz (x_2, y_2) számpáréval, ugyanis $x_1 = x_2$-ből következik, hogy $y_1 = y_2$ és forditva. Ez nem lehetséges, hiszen, kikótóttük, hogy a párok kúlömbözőek. Legyen $x_1 - x_2 =: x$ és $y_2 - y_1 =: y$; akkor teljesül, hogy $0 < |x| \neq [\sqrt{m}]$, $0 < |y| \neq [\sqrt{m}]$, valamint $ax \equiv y \pmod m$. ■

A Fermat tétel egy más bizonyítása

Legyen $p = 4k+1$ alakú prímszám. Tudjuk, hogy $(\frac{-1}{p}) = 1$, és legyen a úgy, hogy $a^2 \equiv -1 \pmod p$. Ekkor $(a, p) = 1$, tehát alkalmazhatjuk a Thue-lemmát. Léteznek a $0 < |x| \neq [\sqrt{p}]$, $0 < |y| \neq [\sqrt{p}]$ számok amelyekre $ax \equiv \pmod p$. Innen következik $a^2x^2 \equiv y^2 \pmod p$. Ekkor

$$x^2 + y^2 = x^2 + ax^2 = x^2(1 + a^2) \equiv 0 \pmod p.$$

Mivel $0 < x^2 + y^2 < 2p$, következik, hogy $x^2 + y^2 = p$. ■

Négy négyzetszám összege

1621-ben Bachet megállapította bizonyitás nélkül, hogy minden pozitiv egész szám felírható négy négyzetszám összegeként. Ezt 1770-ben Lagrange bizonyitotta, majd 1834-ben Jacobi adott egy egyszerü képletet az összes ilyen számra.

6.5.12. lemma. *Ha* $p = 4k+1$ *alakú prímszám, akkor létezik olyan* x *egész szám, amelyre* $1 + x^2 = mp$*, ahol* $0 < m < p$.

Bizonyítás. Létezik $x \in \mathbb{Z}$ úgy, hogy $1 + x^2 \equiv 0 \pmod p$ és $1 \leq |x| \leq \frac{p-1}{2}$; ekkor

$$0 < 1 + x^2 \leq 1 + \left(\frac{p-1}{2}\right)^2 < p^2 \Rightarrow 0 < m < p. \qquad ■$$

6.5.13. lemma. *Ha $p > 2$ prímszám, akkor léteznek olyan x, y egész számok amelyekre $1 + x^2 + y^2 = mp$, ahol $0 < m < p$.*

Bizonyítás. A bizonyítás a skatulyaelven alapul. Tekintsük a következő $\frac{p+1}{2}$ számból álló halmazokat:

$$\{x^2 \mid 0 \le y \le \frac{p-1}{2}\}, \quad \{-1 - y^2 \mid 0 \le y \le \frac{p-1}{2}\}.$$

Mindegkben a számok inkongruensek modulo p. Összesen van $p + 1$ szám, amelyiknek külön az egyik és külön a másik feléről tudjuk, hogy modulo p inkongruensek. Mivel a maradékosztályok száma száma p, ezért biztos van olyan az elsö halmazhoz tartozó szám, amelyik kongruens amásodik halmazbeli számmal modulo p azaz, van az $x^2 \equiv -1 - y^2 \pmod p$ kongruenciának megoldása, ahol $0 \le x \le \frac{p-1}{2}$ és $0 \le y \le \frac{p-1}{2}$ is teljesül. Az előző kongruencia alapján

$$1 + x^2 + y^2 = mp, \quad 0 < 1 + x^2 + y^2 \le 2\left(\frac{p}{2}\right)^2 < p^2,$$

tehát $1 + x^2 + y^2 = mp$, ahol $0 < m < p$. ■

6.5.14. tétel (Lagrange). *Bármely természetes szám előállítható négy négyzetszám összegeként.*

Bizonyítás. A bizonyítás lényege a következő azonosság, ami azt mutatja, hogy ha két szám külön-külön előáll négy négyzetszám összegeként, akkor szorzatuk is:

$$\begin{aligned}(x_1^2 + x_2^2 + x_3^2 + x_4^2)(y_1^2 + y_2^2 + y_3^2 + y_4^2) = {} & (x_1y_1 + x_2y_2 + x_3y_3 + x_4y_4)^2 + \\ & + (x_1y_2 - x_2y_1 + x_3y_4 - x_4y_3)^2 + \\ & + (x_1y_3 - x_3y_1 + x_4y_2 - x_2y_4)^2 + \\ & + (x_1y_4 - x_4y_1 + x_2y_3 - x_3y_2)^2.\end{aligned} \tag{6.4}$$

A tételt elegendő prímszámokra igazolni, mivel $1 = 1^2 + 0^2 + 0^2 + 0^2$, és csak a páratlan prímekre, mivel $2 = 1^2 + 1^2 + 0^2 + 0^2$. Alkalmazható a 6.5.13. lemma, amely szerint bármely $p > 2$ prím esettén van olyan m pozitiv egész szám, amelyre $mp = 1^2 + x^2 + y^2 + 0^2$, azaz

$$mp = x_1^2 + x_2^2 + x_3^2 + x_4^2; \tag{6.5}$$

az is teljesül, hogy x_1, x_2, x_3, x_4 közül nem mindegyik osztható p-vel. Legyen m_0 a lehető legkisebb szám, amelyre (6.5) teljesül, és igazoljuk, hogy $m_0 = 1$.

Tegyük fel, hogy $m_0 > 1$. A 6.5.13. lemma szerint $m_0 < p$. Ha m_0 páros, akkor $x_1^2 + x_2^2 + x_3^2 + x_4^2$ is páros és a következő lehetőségek vannak:

- mind a négy szám páros;
- mind a négy szám páratlan;
- kettő páros, kettő páratlan

Az utolsó esetben tegyük fel, hogy x_1, x_2 párosak, x_3, x_4 páratlanok. Mind a három esetben az $x_1 + x_2$, $x_1 - x_2$, $x_3 + x_4$, $x_3 - x_4$ számok párosak, és így a (6.5)-ból kiindulva kapjuk, hogy:

$$\frac{1}{2}m_0p = \left(\frac{x_1 + x_2}{2}\right)^2 + \left(\frac{x_1 - x_2}{2}\right)^2 + \left(\frac{x_3 + x_4}{2}\right)^2 + \left(\frac{x_3 - x_4}{2}\right)^2.$$

A jobb oldalon lévő négyzetszámok nem mindegyike osztható p-vel, hiszen az x_1, x_2, x_3, x_4 számokról feltettük a 6.5.13. lemma alapján, hogy nem mindegyike osztható p-vel. Ellentmondásra jutottunk azzal a feltevéssel, hogy m_0 a legkisebb olyan szám ami a (6.5)-nak eleget tesz, mert találtunk egy kisebbet: $\frac{m_0}{2}$-t. Tehát m_0 nem lehet páros szám.

Tegyük fel, hogy m_0 páratlan. Ekkor az $m_0 > 1$ feltevés miatt $m_0 \ge 3$. Nyilvánvaló, hogy x_1, x_2, x_3, x_4 számok nem mindegyike osztható m_0-val, mert $m_0^2 \mid m_0p$-ből következik, hogy $m_0 \mid p$, ami lehetetlen. Végezzünk euklideszi osztásokat az x_1, x_2, x_3, x_4 számokon m_0-val, és maradékként a legkisebb abszolut értékü maradékot vegyük. Ezeket jelolje y_1, y_2, y_3, y_4; az osztók hányadosait pedig a_1, a_2, a_3, a_4. Akkor:

$$x_i = a_im_0 + y_i, \quad |y_i| < \frac{1}{2}m_0 \quad i = 1, 2, 3, 4 \tag{6.6}$$

$$0 < y_1^2 + y_2^2 + y_3^2 + y_4^2 < 4(\frac{1}{2}m_0)^2 = m_0^2 \tag{6.7}$$

A (6.7) összefüggésben az y_1, y_2, y_3, y_4 négyzeteinek összege szigorúan pozitiv, mert a velük modulo m_0 kongruens x_1, x_2, x_3, x_4 számokról megmutattuk, hogy nem lehet mindegyikük m_0-val osztható. A (6.5) összefüggest

tekintve modulo m_0, az $x_1^2+x_2^2+x_3^2+x_4^2 \equiv 0 \pmod{m_0}$ kongruenciát kapjuk. A (6.6) alapján $x_i \equiv y_i \pmod{m_0}$, $i = 1,2,3,4$ és így $y_1^2+y_2^2+y_3^2+y_4^2 \equiv 0 \pmod{m_0}$ kongruencia is következik. Tehát

$$m_0 p = x_1^2 + x_2^2 + x_3^2 + x_4^2, \quad 3 < m_0 < p,$$

és a fentiek alapján, következik, hogy van olyan m_1, amelyre

$$m_0 m_1 = y_1^2 + y_2^2 + y_3^2 + y_4^2, \quad 0 < m_1 < m_0.$$

Az utóbbi két egyenlőség szerintn $m_0 p$ és $m_0 m_1$ olyan számok amelyek előállnak négy négyzetszám összegeként, íly módon alkalmazható az (6.4) azonosság. Kapjuk, hogy:

$$m_0^2 m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2$$

a megfelelő t_1, t_2, t_3, t_4 számokkal. Ekkor

$$t_1 = \sum_{i=1}^{4} x_i y_i = \sum_{i=1}^{4} x_i(x_i - a_i m_0) \equiv \sum_{i=1}^{4} x_i^2 \equiv 0 \pmod{m_0},$$

és hasonlóan a t_2, t_3, t_4 számok mindegyike osztható m_0-val; innen $t_i = m_0 u_i$, $i = 1,2,3,4$, amit behelyettesitünk az $m_0^2 m_1 p = t_1^2 + t_2^2 + t_3^2 + t_4^2$ egyenletbe; kapjuk, hogy

$$m_1 p = u_1^2 + u_2^2 + u_3^2 + u_4^2,$$

ami ellentmond m_0 definíciójának, hisz $m_1 < m_0$. Tehát $m_0 = 1$. ■

6.5.15. megjegyzés. *Van olyan természetes szám, amelyik nem állitható elő négynél kevesebb négyzetszám összegeként. Például:* $7 = 2^2 + 1^2 + 1^2 + 1^2$.

6.94. feladat. Igazoljuk, hogy a $8k+7$ alakú természetes számok nem írhatók fel három négyzetszám összegeként.

6.5.5. Az Euler-egészek gyűrűje. Az $x^3 + y^3 = z^3$ egyenlet

Tekintsük a $K = \mathbb{Q}(i\sqrt{3})$ kvadratikus testet. Mivel $d \equiv 1 \pmod 4$, $A_K = \mathbb{Z}[\frac{-1+i\sqrt{3}}{2}]$, ahol $\omega := \frac{-1+i\sqrt{3}}{3}$, tehát $1 + \omega + \omega^2 = 0$. Ha $z = a + b\omega \in A_K$ $a, b \in \mathbb{Z}$ akkor

$$N(z) = z\bar{z} = a^2 - ab + b^2.$$

Tudjuk, hogy a $\mathbb{Z}[\omega]$ **Euler-egészek** gyűrűje euklideszi a normára nézve, és az invertálható elemek (egységek) csoportja

$$U(\mathbb{Z}[\omega]) = \{1, -1, \omega, -\omega, \omega^2, -\omega^2\}.$$

Valóban, legyen $\alpha = a + b\omega$ úgy, hogy $N(\alpha) = \left(a + \frac{-b}{2} + \frac{bi\sqrt{3}}{2}\right)\left(a + \frac{-b}{2} - \frac{bi\sqrt{3}}{2}\right) = \left(a - \frac{b}{2}\right)^2 + \frac{3b^2}{4} = 1$, azaz $(2a - b)^2 + 3b^2 = 4$.

- $b = 0 \Rightarrow (2a)^2 = 4 \Leftrightarrow (2a)^2 = 4 \Leftrightarrow a = \pm 1 \Rightarrow \alpha = \pm 1$;
- $b = 1 \Rightarrow (2a - 1)^2 = 1 \Leftrightarrow a = 1$ vagy $a = 0 \Rightarrow \alpha = \frac{1+i\sqrt{3}}{2} = -\omega^2$ vagy $\alpha = \frac{-1+i\sqrt{3}}{2} = \omega$;
- $b = -1 \Rightarrow (2a + 1)^2 = 1 \Leftrightarrow a = 0$ vagy $a = -1 \Rightarrow \alpha = \frac{1-i\sqrt{3}}{2} = -\omega$ vagy $\alpha = \frac{-1-i\sqrt{3}}{2} = \omega^2$;
- ha $|b| > 2$, akkor nincs megoldás.

A kóvetkező tétel is már ismert, de most adunk egy elemi bizonyítást ebben a partikuláris esetben.

6.5.16. tétel. *Legyen* p *prímszám. Akkor:*
1) *ha* $p \equiv 2 \pmod 3$ *akkor* p *prímszám (irreducibilis)* A_K*-ban is.*
2) *ha* $p \equiv 1 \pmod 3$ *akkor* p *felbontható, azaz* $p = \pi\bar{\pi}$*, ahol* π *prím* A_K*-ban és* $\pi \nsim \bar{\pi}$.
3) $3 = -\omega^2(1 - \omega)^2$*, ahol* $1 - \omega$ *prím* A_K*-ban, azaz* $3 \sim (1 - \omega)^2$.

Bizonyítás. 1) Feltételezzük, hogy p nem prím A_K-ban, tehát $p = \pi\gamma$, ahol $N(\pi) > 1$, $N(\gamma) > 1$; innen $p^2 = N(p) = N(\pi)N(\gamma) \Rightarrow N(\pi) = N(\gamma) = p$. Legyen $\pi = a + b\omega$, $a, b \in \mathbb{Z}$, $p = N(\pi) = a^2 - ab + b^2$, $4p = 4a^2 - 4ab + b^2 + 3b^2 = (2a - b)^2 + 3b^2$, tehát $p \equiv (2a - b)^2 \pmod 3$.

Ha $3 \nmid p$, akkor $\left(\frac{p}{3}\right) = 1$, tehát $p \equiv 1 \pmod 3$). Következik, hogy ha $p \equiv 2 \pmod 3$, akkor p prím A_K-ban.

b) Feltételezzük, hogy $p \equiv 1 \pmod 3$ és igazoljuk, hogy létezik $p = \pi\bar{\pi}$ felbontás. Valóban,

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) = \left(\frac{1}{3}\right) = 1,$$

tehát -3 kvadratikus maradék modulo p, azaz $\exists a \in \mathbb{Z}$ úgy, hogy $a^2 \equiv -3 \pmod p$). Következik, hogy $\exists b \in \mathbb{Z}$ úgy, hogy:

$$a^2 + 3 = pb \Rightarrow p \mid a^2 + 3 \Rightarrow p \mid (a - i\sqrt{3})(a + i\sqrt{3}) \Rightarrow p \mid (a + 1 + 2\omega)(a - 1 - 2\omega).$$

Ha p prím A_K-ban, akkor $\dfrac{a+1}{p} \pm \dfrac{2\omega}{p} \in A_K$, ellentmondás, mert $p \nmid 2$. Következik, hogy p nem prím, tehát reducibilis A_K-ban, és ekkor $p = \pi\bar{\pi}$, ahol π, $\bar{\pi}$ prímek (irreducibilisek) A_K-ban.

c) $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2) = (x-1)(1+x+x^2)$, tehát $1+x+x^2 = (x-\omega)(x-\omega^2)$. Legyen $x = 1$. Akkor $3 = (1-\omega)(1-\omega^2) = (1+\omega)(1-\omega)^2 = -\omega^2(1-\omega)^2$, $N(3) = N(-\omega^2)N((1-\omega)^2)$, $9 = N(1-\omega)^2 \Rightarrow N(1-\omega) = 3$, tehát $1 - \omega$ prím A_K-ban. ■

6.95. feladat. A fenti tétel 2) pontja esetén igazoljuk, hogy $\pi \nsim \bar{\pi}$.

Tekintsük az $x^3 + y^3 = z^3$ diofantikus egyenletet. Euler igazolta, hogy ennek az egyenletnek nincs valódi ($xyz \neq 0$) megoldása.

Az $x^3 + y^3 = z^3$ egyenlet helyett tanulmányozni fogjuk az általánosabb

$$x^3 + y^3 = uz^3$$

egyenletet, ahol u egy rögzitett egység a $\mathbb{Z}[\omega]$ gyűrűben. Legyen

$$\lambda := 1 - \omega.$$

Láttuk, hogy λ irreducibilis $\mathbb{Z}[\omega]$-ban és $\lambda^2 \sim 3$. Ha $\alpha \in \mathbb{Z}[\omega]$, akkor írhatjuk egyértelműen, hogy

$$\alpha = u\lambda^n\beta,$$

ahol $u \in U(\mathbb{Z}[\omega])$, $\lambda \nmid \beta$, $\beta \nsim 1$ és $n \geq 0$. Jelöles: $\operatorname{ord}_\lambda \alpha := n$.

6.96. feladat. Ha $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, akkor $\alpha \equiv 1 \pmod\lambda$ vagy $\alpha \equiv -1 \pmod\lambda$ vagy $\alpha \equiv 0 \pmod\lambda$.

6.5.17. tétel. *Az* $x^3 + y^3 = uz^3$ *egyenletnek, ahol* $u \in U(\mathbb{Z}[\omega])$*, nincs nemtriviális* (x, y, z) *megoldása* $\mathbb{Z}[\omega]$*-ban.*

A tétel bizonyítása következni fog az alábbi lemmákból.

6.5.18. lemma. *Az* $x^3 + y^3 = uz^3$ *,* $u \in \mathbb{Z}[\omega]$ *egyenletnek nincs olyan* (x, y, z) *megoldása amelyre* $\lambda \nmid xyz$*.*

Bizonyítás. Mivel λ irreducibilis $\mathbb{Z}[\omega]$-ban következik, hogy $\lambda \nmid xyz \Leftrightarrow \lambda \nmid x,\ \lambda \nmid y,\ \lambda \nmid z$. Ha $x \in \mathbb{Z}[\omega]$, $x \equiv 1 \pmod\lambda$), akkor $x^3 \equiv 1 \pmod{\lambda^4}$). Valóban, legyen $x = 1 + \lambda t$, ahol $t \in \mathbb{Z}[\omega]$. Akkor

$$x^3 - 1 = (x-1)(x-\omega)(x-\omega^2) = \lambda t(1-\omega+\lambda t)(1-\omega^2+\lambda t) = \lambda t(\lambda+\lambda t)(\lambda(1+\omega)+\lambda t) = \lambda^3 t(1+t)(t-\omega^2).$$

Mivel $\omega \equiv 1 \pmod\lambda$ és $t \equiv 1,\ -1$ vagy $0 \pmod\lambda$, következik, hogy $x^3 \equiv 1 \pmod{\lambda^4}$.

Feltételezzük, hogy az $x^3 + y^3 = uz^3$ egyenletnek létezik egy (x, y, z) megoldása úgy, hogy $\lambda \nmid xyz$. Ekkor redukáljuk az egyenletet modulo λ^4. Kapjuk, hogy $\pm 1 \pm 1 \equiv \pm u \pmod{\lambda^4}$, ami lehetetlen. ■

6.5.19. lemma. *Feltételezzük, hogy létezik* $x,\ y,\ z \in \mathbb{Z}[\omega]$ *megoldása az* $x^3 + y^3 = uz^3$ *egyenletnek úgy, hogy* $\lambda \mid z$*,* $(x, y) = 1$*. Akkor* $\lambda^2 \mid z$*.*

Bizonyítás. Feltételezzük, hogy (x, y, z) megoldás, $\lambda \mid z$, $(x, y) = 1$. Redukáljuk az egyenletet modulo λ^4 és vizsgáljuk az eseteket:

$$\pm 1 \pm 1 \equiv uz^3 \pmod{\lambda^4}.$$

1. eset: $0 \equiv uz^3 \pmod{\lambda^4} \Rightarrow \lambda^4 \mid z^3 \Rightarrow 3\operatorname{ord}_\lambda z \geq 4 \Rightarrow \operatorname{ord}_\lambda z \geq 2$, azaz $\lambda^2 \mid z$.
2. eset: $\pm 2 \equiv uz^3 \pmod{\lambda^4} \Rightarrow \lambda \mid uz^3 \pm 2 \Rightarrow \lambda \mid \pm 2$ lehetetlen. ■

6.5.20. lemma. *Ha* $x,\ y,\ z \in \mathbb{Z}[\omega]$ *úgy, hogy* $x^3 + y^3 = uz^3$*,* $(x, y) = 1$*,* $\lambda \nmid xy$ *és* $\operatorname{ord}_\lambda z \geq 2$*, akkor* $\exists u_1,\ x_1,\ y_1,\ z_1 \in \mathbb{Z}[\omega]$ *úgy, hogy* $u_1 \in U(\mathbb{Z}[\omega])$*,* $\lambda \nmid x_1y_1$*,* $\operatorname{ord}_\lambda z_1 = \operatorname{ord}_\lambda z - 1$ *és* $x_1^3 + y_1^3 = u_1z_1^3$*.*

Bizonyítás. Tudjuk, ha $\operatorname{ord}_\lambda \alpha \neq \operatorname{ord}_\lambda \beta$ akkor $\operatorname{ord}_\lambda(\alpha \pm \beta) = \min\{\operatorname{ord}_\lambda \alpha, \operatorname{ord}_\lambda \beta\}$. Vegyük észre, hogy

$$uz^3 = (x + y)(x + \omega y)(x + \omega^2 y).$$

Mivel $\operatorname{ord}_\lambda uz^3 \geq 6$, létezik egy tényező az egyenlet jobb oldalán amely osztható λ^2-el. Ha szükséges helyettesithetjük y-t ωy-nal vagy $\omega^2 y$-nal és feltételezhetjük, hogy $\operatorname{ord}_\lambda(x + y) \geq 2$. Mivel $\operatorname{ord}_\lambda(1 - \omega)y = \operatorname{ord}_\lambda \lambda y = 1$, következik, hogy $\operatorname{ord}_\lambda(x+\omega y) = \operatorname{ord}_\lambda(x+y-(1-\omega)y) = 1$. Hasonlóan $\operatorname{ord}_\lambda(x+\omega^2 y) = 1$. Tehát $\operatorname{ord}_\lambda(x+\omega y) = 3\operatorname{ord}_\lambda z - 2$.

Könyen belátható, hogy $(x+y, x+\omega y) = (x+y, x+\omega^2 y) = (x+\omega y, x+\omega^2 y) = \lambda$. A $\mathbb{Z}[\omega]$-beli egyértelmű felbontás alapján írhatjuk:

$$\begin{aligned} x+y &= u_1\alpha^3\lambda^t, & t &= 3\operatorname{ord}_\lambda z - 2, & \lambda &\nmid \alpha \\ x+\omega y &= u_2\beta^3\lambda, & \lambda &\nmid \beta \\ x+\omega^2 y &= u_3\gamma^3\lambda, & \lambda &\nmid \gamma, \end{aligned}$$

ahol u_1, u_2, u_3 egységek $\mathbb{Z}[\omega]$-ban és $(\alpha,\beta) = (\alpha,\gamma) = (\beta,\gamma) = 1$. Megszorozva az második egyenlőséget ω-val, a harmadikat ω^2-el és összeadva, kapjuk:

$$0 = u_1\alpha^3\lambda^t + \omega u_2\beta^3\lambda + \omega^2 u_3\gamma^3\lambda,$$

$$0 = u_1\alpha^3\lambda^{3(\mathrm{ord} z-1)} + \omega u_2\beta^3 + \omega^2 u_3\gamma^3.$$

Legyen $\alpha\lambda^{\mathrm{ord} z-1} =: z_1$, $\beta =: x_1$, $\gamma =: y_1$; akkor $x_1^3 + \epsilon_1 y_1^3 = \epsilon_2 z_1^3$, ahol ϵ_1, ϵ_2 egységek. Redukáljuk az egyenletet modulo λ^2; mivel $\operatorname{ord}_\lambda z_1^3 > 2$, kapjuk, hogy

$$\pm 1 \pm \epsilon_1 \equiv 0 \pmod{\lambda^2}.$$

Itt $\epsilon_1 = \pm 1$ vagy $\pm\omega$ vagy $\pm\omega^2$; de $\pm 1 \pm \omega$, $\pm 1 \pm \omega^2$ közül egyik sem osztható λ^2-tel, ezért $\epsilon_1 = \pm 1$. Tehát $x_1^3 + y_1^3 = \epsilon z_1^3$ ahol $\lambda \nmid x_1, y_1$, $\operatorname{ord}_\lambda z_1 = \operatorname{ord}_\lambda z - 1$ és ϵ egység. ■

A 6.5.17. tétel bizonyítása

Legyen (x,y,z) egy megoldás, ahol $\operatorname{ord}_\lambda z$ minimális, és $(x,y) = 1$.

Ha $\lambda \nmid xyz$ akkor alkalmazzuk az 6.5.18. lemmát.

Feltételezzük, hogy $\exists(x,y,z)$ megoldás úgy, hogy $\lambda \nmid xy$, $\lambda \mid z$. Akkor a 6.5.18. lemmá alapján $\lambda^2 \mid z$, azaz $\operatorname{ord}_\lambda z \geq 2$. Alkalmazzuk a 6.5.20. lemmát: $\exists x_1$, y_1, z_1, u_1, ahol $\operatorname{ord}_\lambda z_1 < \operatorname{ord}_\lambda z$ úgy, hogy $x_1^3 + y_1^3 = u_1 z_1^3$, ami ellentmond a $\operatorname{ord}_\lambda z$ minimálításával.

Feltételezzük, hogy $\exists(x,y,z)$ megoldás úgy, hogy $\lambda \mid x$, $\lambda \nmid yz$. Akkor a 6.96. megjegyzés alapján

$$\pm 1 \equiv u \pmod{\lambda^3} \Longrightarrow u = \pm 1 \Longrightarrow (\pm z)^3 + (-y)^3 = x^3,$$

amely az előbbi eset ($\lambda \nmid yz$, $\lambda \mid x$). ■

6.5.6. A Pell-egyenlet

A következőkben az $x^2 - dy^2 = \pm 1$ egyenleteket tárgyaljuk.

6.5.21. lemma. *Legyen $\xi \in \mathbb{R} \setminus \mathbb{Q}$. Végtelen sok $\frac{x}{y}$ racionális szám létezik úgy, hogy $(x,y) = 1$ és $\left|\frac{x}{y} - \xi\right| < \frac{1}{y^2}$.*

Bizonyítás. Tekintsük a övetkező intervallumot:

$$[0,1) = \left[0, \frac{1}{n}\right) \cup \left[\frac{1}{n}, \frac{2}{n}\right) \cup \ldots \cup \left[\frac{n-1}{n}, 1\right), \quad n > 1.$$

Tekintsük a $0, \xi, 2\xi, \ldots, n\xi$ számokat ($n+1$ darab). A skatulyaelv alapján $\exists n \geq j > k \geq 0$ úgy, hogy

$$|\{j\xi\} - \{k\xi\}| < \frac{1}{n}, \qquad |j\xi - [j\xi] - k\xi + [k\xi]| < \frac{1}{n}.$$

Legyen $y := j - k$, $x := [k\xi] - [j\xi]$; akkor

$$|x - y\xi| < \frac{1}{n} \Leftrightarrow \left|\frac{x}{y} - \xi\right| < \frac{1}{ny}, \qquad 0 < y < n \Rightarrow \left|\frac{x}{y} - \xi\right| < \frac{1}{ny} < \frac{1}{y^2}.$$

Végül, igazoljuk, hogy végtelen sok $\frac{x}{y}$ tört létezik. Mivel $\frac{x}{y} \in \mathbb{Q}$ és $\xi \notin \mathbb{Q} \Rightarrow \left|\frac{x}{y} - \xi\right| \neq 0$. Legyen $m > \dfrac{1}{\left|\frac{x}{y} - \xi\right|}$; akkor $\exists x_1, y_1$ úgy, hogy

$$\left|\frac{x_1}{y_1} - \xi\right| < \frac{1}{my_1} < \left|\frac{x}{y} - \xi\right|, \quad 0 < y_1 < m.$$

Folytatva ezt az eljárást, kapjuk, hogy végtelen sok megoldás van: $x, y, x_1, y_1, \ldots$ ■

6.5.22. lemma. *Legyen* $d > 0$ *négyzetmentes egész szám. Akkor* $\exists M > 0$ *úgy, hogy* $|x^2 - dy^2| < M$ *végtelen sok* (x, y) *számpár esetén.*

Bizonyítás. Az 6.5.21. lemma szerint, végtelen sok (x, y) számpár létezik, úgy, hogy $(x, y) = 1$ és $|x - y\sqrt{d}| < \frac{1}{y}$. Ekkor

$$|x + y\sqrt{d}| < |x - y\sqrt{d}| + 2\sqrt{d}|y| < \frac{1}{y} + 2\sqrt{d}y,$$

$$|x^2 - dy^2| = |(x - \sqrt{d}y)(x + \sqrt{d}y)| < \frac{1}{y}(\frac{1}{y} + 2y\sqrt{d}) = \frac{1}{y^2} + 2\sqrt{d} < 2\sqrt{d} + 1.$$

Tehát $|x^2 - dy^2| < M$, ahol $M := 2\sqrt{d} + 1$. ■

6.5.23. tétel. *Az* $x^2 - dy^2 = 1$ *egyenletnek végtelen sok megoldása van. Létezik egy* $(x_1, y_1) \in \mathbb{N}^* \times \mathbb{N}^*$ *megoldás úgy, hogy minden* $(x, y) \in \mathbb{Z} \times \mathbb{Z}$ *megoldás* $\pm(x_n, y_n)$ *alakú, ahol*

$$x_n + y_n\sqrt{d} := (x_1 + y_1\sqrt{d})^n, \quad n \in \mathbb{Z}.$$

Bizonyítás. A 6.5.22. lemma alapján $\exists m \in \mathbb{Z}$ úgy, hogy az $x^2 - dy^2 = m$ egyenletnek végtelen sok megoldása van, mert $(-M, M) \cap \mathbb{Z}$ véges halmaz. Feltételezzük, hogy (x, y) megoldás, $x, y > 0$. Mivel csak véges sok maradékosztály modulo $|m|$ van, feltételezhetjük, hogy (x_1, y_1), (x_2, y_2) megoldásai az $x^2 - dy^2 = m$ egyenletnek úgy, hogy $x_1 \neq x_2$, $x_1, x_2 > 0$, és

$$x_1 \equiv x_2 \pmod{m}, \qquad y_1 \equiv y_2 \pmod{m}).$$

Legyen $\alpha = x_1 - y_1\sqrt{d}$ és $\beta = x_2 - y_2\sqrt{d} = (x_1 + km) - (y_1 + lm)\sqrt{d}$. Ekkor

$$\begin{aligned}\alpha\bar{\beta} &= x_1(x_1 + km) - y_1(y_1 + lm)d + (x_1(y_1 + lm) - y_1(x_1 + km))\sqrt{d} = \\ &= (x_1^2 - y_1^2 d) + m(x_k + y_1 ld) + (x_1 lm - y_1 km)\sqrt{d},\end{aligned}$$

azaz $\alpha\bar{\beta} = m(u + v\sqrt{d})$, ahol $u, v \in \mathbb{Z}$. Alkalmazzuk a normát:

$$N(\alpha\bar{\beta}) = N(\alpha)N(\bar{\beta}) = m^2 = N(m)N(u^2 + v^2\sqrt{d} = m^2(u^2 - v^2\sqrt{d}),$$

tehát $u^2 - v^2 d = 1$. Ha $v = 0$, akkor $u = \pm 1$, tehát $\alpha\bar{\beta} = \pm m$ és $m = \pm 1$. Innen $\alpha = \pm\beta$, tehát $x_1 = x_2$ ami ellentmondás, tehát $\alpha = \beta$. Tehát létezik (u, v) megoldása az $x^2 - dy^2 = 1$ egyenletnek úgy, hogy $uv \neq 0$, azaz létezik nemtrivialis megoldás.

Értelmezünk egy relációt a pozitiv megoldások kózött a következőképpen: az (x, y) megoldás nagyobb mint az (u, v) megoldás (jelölés: $(x, y) > (u, v)$), ha $x + y\sqrt{d} > u + v\sqrt{d}$ $\mathbb{R}$-ben. Legyen α a legkisebb megoldás. Létezik egy ilyen megoldás mivel $(x, y) \in \mathbb{N} \times \mathbb{N}$; ezt nevezzük *alapmegoldás*nak.

Legyen $\beta := u + v\sqrt{d}$, $u > 0$, $v > 0$ tetszőleges megoldás, és igazoljuk, hogy $\exists n \in \mathbb{N}^*$ úgy, hogy $\beta = \alpha^n$. Reductio ad absurdum: mivel $\alpha > 1$ következik, hogy $(\alpha^n)_{n\geq 1}$ szigorúan növekvő sorozat; feltételezzük, hogy létezik n úgy, hogy $\alpha^n < \beta < \alpha^{n+1}$, tehát $1 < \beta\alpha^{-n} < \alpha$. Akkor $\beta\alpha^{-n} := A + B\sqrt{d} > 0$. Továbbbá, (A, B) megoldás, mivel $A^2 - B^2 d = N(\beta)N(\alpha)^{-1} = 1$, és mi több

$$A - B\sqrt{d} = \frac{1}{A + B\sqrt{d}} > 0 \Rightarrow A > 0,$$

$$B\sqrt{d} > A - 1 \Rightarrow B > 0.$$

Tehát (A, B) pozitiv megoldás, és $A + B\sqrt{d} < \alpha$ ellentmond azzal, hogy α a legkisebb.

- Ha $\beta = a + b\sqrt{d}$ megoldás úgy, hogy $a > 0$, $b < 0$, akkor $\beta^{-1} = \bar{\beta} = a + (-b)\sqrt{d} = \alpha^n$, tehát $\beta = \alpha^{-n}$.
- Ha $\beta = a + b\sqrt{d}$ megoldás, $a < 0$, $b > 0$, akkor $-\beta = (-a) + (-b)\sqrt{d}$, $-a > 0$, $-b < 0$.
- Ha $\beta = a + b\sqrt{d}$ megoldás, $a < 0$, $b < 0$, akkor $-\beta = (-a) + (-b)\sqrt{d}$, $-a > 0$, $-b > 0$. ■

Az $x^2 - dy^2 = -1$,,non-Pell" egyenletet hasonló módszerekkel lehet tárgyalni. Ebben az esetben nem mindig létezik megoldás.

6.97. feladat. 1) Ha $p = 4k-1$ alakú prímszám, akkor az $x^2 - py^2 = -1$ diofantikus egyenletnek nincs megoldása.

2) Feltételezzük, hogy $(x_1^-, y_1^-) > (0, 0)$ az $x^2 - dy^2 = -1$ egyenlet legkisebb megoldása, és legyen $x_1^+ + \sqrt{d}y_1^+ := (x_1^- + \sqrt{d}y_1^-)^2$. Igazoljuk, hogy (x_1^+, y_1^+) az $x^2 - dy^2 = 1$ egenlet alapmegoldása.

3) Legyen (x_1^-, y_1^-) az $x^2 - dy^2 = -1$ egyenlet legkisebb pozitív megoldása, és minden $n \in \mathbb{Z}$ esetén jelöljük

$$x_n^- + \sqrt{d}y_n^- := (x_1^- + \sqrt{d}y_1^-)^n.$$

Igazoljuk, hogy az $x^2 - dy^2 = -1$ egyenlet összes megoldásai: $\pm(x_n^-, y_n^-)$, ahol $n = \pm 1, \pm 3, \pm 5, \ldots$

6.98. feladat. Legyen A a $K = \mathbb{Q}(\sqrt{d})$ kvradratikus test egészeinek a gyűrűje. Igazoljuk, hogy

$$U(A) \simeq (\mathbb{Z}, +) \times (U_2, \cdot).$$

6.5.24. megjegyzés. 1) *Az alapmegoldás meghatározása*: a egyenleteket az $x^2 = dy^2 \pm 1$ alakban írjuk, és legyen $y = 1, 2, 3 \ldots$ amíg $dy^2 \pm 1$ teljes négyzet.

Például, az $x^2 - 3y^2 = 1$ egyenlet alapmegoldása $(2, 1)$, és az $x^2 - 2y^2 = 1$ egyenlet alapmegoldása $(3, 2)$.

2) *A megoldás általános alakja*: Legyen $\alpha = x_1 + y_1\sqrt{d}$ alapmegoldás, tehát $x_1^2 - dy_1^2 = \pm 1$, $x_1 > 0$, $y_1 > 0$, és legyen $\alpha^n = x_n + y_n\sqrt{d}$. Ekkor

$$\alpha^{n+1} = x_{n+1} + yn + 1\sqrt{d} = (x_1 + y_1\sqrt{d})(x_n + y_n\sqrt{d}) = x_1x_n + y_1y_nd + (x_1y_n + y_1x_n)\sqrt{d}.$$

Kapjuk a következő lineéaris rekurziórendszert:

$$\begin{cases} x_{n+1} = x_1x_n + y_1y_nd & x_{n+1} > x_n \\ y_{n+1} = x_1y_n + y_1x_n & y_{n+1} > y_n, \end{cases}$$

ami visszavezethető két mśodfokú lineáris rekurzióra, amelyenek a karakterisztikus egyenlete

$$r^2 - 2x_1r + x_1^2 - dy_1^2 = 0.$$

6.99. feladat. Oldjuk meg az $x^2 - dy^2 = \pm 1$ egyenleteket, ahol
a) $d = 5$; b) $d = 6$; c) $d = 10$; d) $d = 14$; e) $d = 19$; f) $d = 23$.

6.100. feladat. Igazoljuk, hogy a $165x^2 - 21y^2 = 19$ diofantikus egyenletenek nincs megoldása.

Irodalomjegyzék

[1] Albu, T.–Ion, D.I.: *Capitole de teoria algebrică a numerelor*, Editura Academiei, Bucureşti 1984.

[2] Artin, M.: *Algebra*, Birkhäuser, Basel 1998.

[3] Bálint M.–Czédli G.–Szendrei Á.: *Absztrakt algebrai feladatok*, Tankönyvkiadó, Budapest 1988.

[4] Călugăreanu, G.–Hamburg, P.: *Exercises in basic ring theory*, Kluwer Academic Publishers, Dordrecht, Boston 1998.

[5] Crivei, S.: *Basic Abstract Algebra*, Casa Cărţii de Ştiinţă, Cluj-Napoca 2002.

[6] Erdős P.–Surányi J.: *Válogatott fejezetek a számelméletből*, Polygon, Szeged, 1996.

[7] Fadeev, D.–Sominski, I.: *Recueil d'exercises d'algébre supérieure*, Edition Mir, Moscou 1977.

[8] Fenrick, M.H.: *Introduction to the Galois Correspondence*, 2nd Edition, Birkhauser, Basel 1996.

[9] Fraleigh, J.B. *A first course in abstract algebra*, Addison-Wesley, Reading 1968.

[10] Fried E.: *Klasszikus és lineáris algebra*, Tankönyvkiadó, Budapest 1974.

[11] Fried E.: *Általános algebra*, Tankönyvkiadó, Budapest 1981.

[12] Friedberg, S.H.–Insel, A.J.–Spence, L.E.: *Linear Algebra*, Prentice Hall, Inc. 1997.

[13] Fuchs L.: *Bevezetés az algebrába és számelméletbe II*, Tankönyvkiadó, Budapest 1991.

[14] Fuchs L.: *Algebra*, Tankönyvkiadó, Budapest 1992.

[15] Gabriel, P.: *Matrizen, Geometrie, Lineare Algebra*, Birkhauser-Verlag, Basel-Boston-Berlin 1996.

[16] Godement, R.: *Cours d'Algébre*, Hermann, Paris 1963.

[17] Halmai E.: *Lineáris algebra*, Tankönyvkiadó, Budapest 1991.

[18] Halmos P.: *Véges dimenziós vektorterek*, Műszaki Könyvkiadó, Budapest 1984.

[19] Horváth E.: *Lineáris algebra*, Műegyetemi Kiadó, Budapest 1995.

[20] Ion, I.D.–Radu, N.: *Algebra*, Ed. Didactică şi Pedagogică, Bucureşti 1981.

[21] Ion, I.D.–Niţă, C.–Popescu, D.–Radu, N.: *Probleme de algebră*, Ed. Didactică şi Pedagogică, Bucureşti 1981.

[22] Jacobson, N.: *Basic algebra I,II*, Freeman, San-Francisco 1984.

[23] Kaluzsnyin L.A. *Bevezetés az algebrába*, Tankönyvkiadó, Budapest 1979.

[24] Kargapolov, M.I.–Merzliakov, Iou. I.: *Éléments de la théorie des groupes*, Edition Mir, Moscou 1985.

[25] Kostrikin, A.I.: *Introduction à l'algébre*, Edition Mir, Moscou 1981.

[26] Koulikov, L.: *Algébre et théorie des nombres*, Edition Mir, Moscou 1973.

[27] Lang, S.: *Algebra*, Addison-Wesley, Reading 1965.

[28] Năstăsescu, C.–Niţă, C.–Vraciu, C.: *Teoria calitativă a ecuaţiilor algebrice*, Editura tehnică, Bucureşti 1979.

[29] Năstăsescu, C.–Niţă, C.–Vraciu, C.: *Bazele algebrei I*, Ed. Academiei, Bucureşti 1986.

[30] Niven, I.–Zuckerman, H.S.: *Bevezetés a számelméletbe*, Műszaki Könyvkiadó, Budapest, 1978.

[31] Proskuriakov, I.V.: *Problems in linear algebra*, Mir Publishers, Moscow 1978.

[32] Purdea, I.–Pic, Gh.: *Tratat de algebră modernă I*, Ed. Academiei, Bucureşti 1977.

[33] Purdea, I.: *Tratat de algebră modernă II*, Ed. Academiei, Bucureşti 1982.

[34] Rédei L.: *Algebra I*, Akadémiai Kiadó, Budapest 1954.

[35] Sárközy A.–Surányi J.: *Számelmélet-feladatgyűjtemény*, Tankönyvkiadó, Budapest, 1979.

[36] Scheja, G.–Storch, U.: *Lehrbuch der Algebra 1,2*, B.G. Teubner, Stuttgart 1994.

[37] Schmidt T.: *Algebra*, Tankönyvkiadó, Budapest 1992.

[38] Szele T.: *Bevezetés az algebrába*, Tankönyvkiadó, Budapest 1963.

[39] Szendrei J.: *Algebra és számelmélet*, Tankönyvkiadó, Budapest 1974.

[40] Şafarevici, I.R.: *Noţiunile fundamentale ale algebrei*, Ed. Academiei, Bucureşti 1989.

[41] Turán P.–Környei I.: *Algebra*, Tankönyvkiadó, Budapest 1992.

[42] Warner, S.: *Modern Algebra*, Dover, New York 1990.

Tárgymutató

$(S_n, \circ)$, 10
$(\mathrm{End}(A, +), +, \circ)$, 16
$A[X]$, 19
$A[[X]]$, 19
A^h, 25
A^t, 25
$A^{(\mathbb{N})}$, 18
$A^{\mathbb{N}}$, 18
A_P, 151
A_n, 10
$C_R(X)$, 18
D_n, 89, 107, 109, 110, 115
$G_n^k(q)$, 41
$H \trianglelefteq\trianglelefteq G$, 110
$I : J$, 119
I_n, 15
$M_n(R)$, 15
$M_{m,n}(R)$, 15, 23
Q_8, 15, 91, 114
R^I, 22
S_n, 107, 116
$T_n(R)$, 17, 23
$U(R)$, 12
U_n, 14
$Z(R)$, 17
$[\beta]_e$, 75
$[a_{ij}]_{\substack{1\le i\le m\\ 1\le j\le n}}$, 15
$\mathbb{C}$, 13, 123
$\Delta(f)$, 137
$\mathbb{N}$, 1
$\Phi(G)$, 108
$\mathbb{Q}$, 1, 130
$\mathbb{Q}(\sqrt[3]{p})$, 17, 123
$\mathbb{Q}(\sqrt{d})$, 21
$\mathbb{R}$, 1
$\mathbb{Z}$, 1, 130
$\mathbb{Z}[\sqrt{d}]$, 14, 17, 123
$\mathbb{Z}_n$, 13
$\aleph_0$, 5
$\deg(f)$, 19
δ_{ij}, 15
$\left(\frac{a}{p}\right)$, 212
$\mathbb{H}$, 15, 21
$\mathrm{Aut}(G)$, 8
$\mathrm{Aut}(R)$, 13
$\mathrm{Aut}_R(M)$, 24
$\mathrm{End}(G)$, 8
$\mathrm{End}(R)$, 13
$\mathrm{End}_R(M)$, 24
$\mathrm{Hom}(R, R')$, 13
$\mathrm{Hom}_R(M, M')$, 24
$\mathrm{Im}(f)$, 24
$\mathrm{Ker}(f)$, 24
$\mathrm{Tr}(A)$, 25
$\mathrm{inv}(\sigma)$, 10
$\mathrm{supp}(f)$, 18
$\mathrm{GL}_n(R)$, 25, 40
$\mathrm{Idemp}(R)$, 12
$\mathrm{SL}_n(K)$, 40
$\mathrm{SO}(n)$, 40
$\mathrm{SU}(n)$, 40
$\mathrm{char}(R)$, 125
$\mathrm{ord}(x)$, 96
$\mathrm{rang}\, A$, 43
$\mathrm{rang}\, \beta$, 75
$\mathrm{sgn}(\sigma)$, 10
$\rho\langle x\rangle$, 3
$\sqrt{I}$, 119
$m_{\mathrm{alg}}(\lambda)$, 54
$m_{\mathrm{geom}}(\lambda)$, 54
$o(f)$, 19
$r(R)$, 12
általános lineáris csoport, 40

Abel-csoport endomorfizmusgyűrűje, 16
aldeterminány, 41
algebrai multiplicitás, 54
alternáló csoport, 11
antikommutatív, 12
antiszimmetrikus mátrix, 25
anulátorideál, 118
Arkhimedesz axiómája, 130
automorfizmus
    csoport, 8

balideál, 118
beágyazás, 9
belső automorfizmus, 8
Bertrand-posztulátum, 194
Bessel-egyenlőtlenség, 78
Bezout-tétel, 21
Binet–Cauchy-képlet, 42

Carmichael-szám, 201
Cauchy–Schwartz-egyenlőtlenség, 73, 76, 78
Cayley–Hamilton-tétel, 54
centralizátor, 18
centrum
    gyűrű, 12
    részgyűrű, résztest, 17
ciklus
    általánosított sajátvektorokat tartalmazó, 60
cosinus-tétel, 77
Csebisev-tétel, 194

definiáló reláció, 89
diédercsoport, 89
direkt összeg, 62
direkt szorzat
    gyűrűk, 14, 124
Dirichlet, 195
Dirichlet-tétel, 216
disztributív, 11

egységgyök, 14
egyszerű gyűrű, 118
Eisenstein-kritérium, 149
endomorfizmus
    csoport, 8
    gyűrű, 13
epimorfizmus, 16
Erdős Pál, 194
Euklidesz, 197
Euklideszi algoritmus, 1
Euler, 197
Euler-függvény, 5, 195

függvényalgebra, 22, 25
függvények gyűrűje, 14
Fermat-prím, 193
Fermat-prímszám, 189
Fermat-számok, 201
formális derivált, 131
formális sor, 19
Frattini-részcsoport, 108
Frobenius-endomorfizmus, 126

Galois-bővítés, 173
Gauss–d'Alembert-tétel, 21
Gauss–Lagrange-tétel, 72
Gauss-féle reciprocitástétel, 213
Gauss-lemma, 148, 214
Gauss-szám, 41
generátor, 89
geometriai multiplicitás, 54
Goldbach-sejtés, 194
Gram–Schmidt-ortogonalizáció, 78
Gram-determináns, 42
gyökökkel való bővítés, 182

hányadostest, 128
Hall–Witt-azonosság, 107
helyettesítési érték, 20
Hermite-képlet, 192
hermitikus mátrix, 25

idempotens, 12
ikerprímek, 194
index, 90
indextábla, 208
integritástartomány, 12
inverzió, 10
involució, 25
izometria, 89
izomorfizmus
    R-modulus, 24
    csoport, 8
    gyűrű, 13

Jacobi-azonosság, 11
jobbideál, 118
Jordan–Hölder-tétel, 111

kép
    csoportmorfizmus, 9
    lineáris függvény, 24
kanonikus projekció
    direkt szorzat, 8
karakterisztikus minor, 45
kezdővektor, 60
kicserélési lemma, 48
Komplex spektráltétel, 82
komplex számok, 13
konvolució, 195
Kronecker–Capelli-tétel, 45
Kronecker-szimbólum, 15
Kronecker-tétel, 43
kváziciklikus csoport, 98
kvadratikus maradék, 212
kvadratikus test, 14
kvaternió, 15, 21, 22
kvaterniócsoport, 15, 91, 114
kínai maradéktétel, 124

Lagrange-féle rezolvens, 183
Lagrange-tétel, 90
Laplace-kifejtés, 41
Laurent-féle formális sorok, 130
lexikografikus rendezés, 135
Lie-algebra, 22
Lie-gyűrű, 11
lineáris függvény, 24
lokális gyűrű, 151

Möbius-függvény, 195
Möbius-féle inverziós képlet, 197
mátrix
    antiszimmetrikus, 25
    idempotens, 25
    invertáható, 25
    ortogonális, 25, 40
    szimmetrikus, 25
    unitér, 40
mátrixalgebra, 23
mátrixgyűrű, 15
mag
    csoportmorfizmus, 9
    lineáris függvény, 24
Mersenne-prím, 193
metaciklikus csoport, 98
Minkowski-egyenlőtlenség, 73, 76
minor, 41
moduláris háló, 92
modulo n maradékosztályok gyűrűje, 13
monomorfizmus, 16
morfizmus
    R-algebra, 24
    R-modulus, 24
    csoport, 8
    gyűrű, 13
multiplikatív számelméleti függvény, 195

nagy prímszámtétel, 194
nilpotencia osztály, 113
nilpotens, 12
norma
    euklideszi, 14
nyom
    mátrix, 25

orbit, 87
ortogonális, 77
ortonormált, 77
oszthatósági szabályok, 199

pálya, 87
paralelogramma-azonosság, 77
Parseval-azonosság, 78
permutáció, 10
permutáció típusa, 103
pitagorikus testbővítés, 188
Poláris felbontás, 83
polinomalgebra, 25
polinomfüggvény, 20
primitív gyök, 207

rend
    formális sor, 19
Rouché-tétel, 45

Schreier-tétel, 111
skalár, 22
speciális lineáris csoport, 40
speciális ortogonális csoport, 40
speciális unitér csoport, 40
Sylvester-tétel, 74
számrendszer, 191
szabad vektorok, 22
szignatúra
    kvadratkus alak, 74
    permutáció, 10
szimmetria csoport, 89
szimmetrikus csoport, 107, 116
szimmetrikus mátrix, 25
szitaformula, 5
szubnormális részcsoport, 110

tartóhalmaz, 18
Taylor-képlet, 132
test, 11
torziórészcsoport, 98
transzponált mátrix, 25
transzpozíció, 10
trianguláris mátrix, 17, 23

unitér gyűrűmorfizmus, 13
unitér részgyűrű, 16

végvektor, 60
valós spektráltétel, 82
vektor, 22
vektoriális szorzat, 22
Viéte-formulák, 21

Wendt-részcsoport, 117
Wilson-tétel, 200

zérusosztó, 12
zérusosztómentes gyűrű, 12
Zassenhaus-lemma, 110