

# ALGEBRA ÉS SZÁMELMÉLET

vázlat az előadáshoz<sup>†</sup>

2018 őszi félév, BSc

Waldhauser Tamás

## 1. Komplex számok

### Kanonikus alak, konjugált, abszolút érték, komplex számsík

**1.1. Definíció.** A valós számokból álló számpárokat **komplex számoknak** nevezzük. A komplex számok halmazát  $\mathbb{C}$  jelöli, tehát  $\mathbb{C} = \mathbb{R} \times \mathbb{R}$ . Az  $(a, b)$  és  $(c, d)$  komplex számok **összegét** és **szorzatát** a következőképpen értelmezzük:

$$(a, b) + (c, d) = (a + c, b + d) \quad \text{és} \quad (a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

**1.2. Tétel.** A komplex számok *testet* alkotnak a fenti műveletekkel.

**1.3. Állítás.** Minden  $a, b \in \mathbb{R}$  esetén

$$(a, 0) + (b, 0) = (a + b, 0) \quad \text{és} \quad (a, 0) \cdot (b, 0) = (ab, 0).$$

**Jelölés.** Tetszőleges  $a \in \mathbb{R}$  esetén az  $(a, 0)$  komplex szám helyett egyszerűen  $a$ -t írunk, és nem is különböztetjük meg az  $a$  valós számtól. (Úgy tekintjük, hogy  $\mathbb{R} \subseteq \mathbb{C}$ .) A  $(0, 1)$  komplex számot pedig  $i$  jelöli a továbbiakban.

**1.4. Tétel.** Minden komplex szám előáll, mégpedig egyértelmű módon,  $x + yi$  ( $x, y \in \mathbb{R}$ ) alakban. Az  $(a, b)$  komplex szám ilyen felírásánál  $x = a$  és  $y = b$ , azaz  $(a, b) = a + bi$ .

**1.5. Definíció.** A  $z = (a, b)$  komplex szám  $a + bi$  alakban való felírását  $z$  **kanonikus alakjának**, az  $a$  valós számot  $z$  **valós részének** (jelölése:  $\operatorname{Re} z$ ), a  $b$  valós számot  $z$  **képzetes részének** (jelölése:  $\operatorname{Im} z$ ) nevezzük. Az  $i$  komplex szám neve **képzetes egység**.

**1.6. Állítás.** A képzetes egység négyzete:  $i^2 = -1$ .

**1.7. Definíció.** A  $z = a + bi$  komplex szám **konjugáltján** a  $\bar{z} = a - bi$  komplex számot értjük.

**1.8. Tétel.** Bármely  $u, v$  komplex számokra érvényesek az alábbiak:

$$\begin{array}{lll} (1) \overline{u + v} = \bar{u} + \bar{v}; & (4) \overline{u/v} = \bar{u}/\bar{v}, \text{ ha } v \neq 0; & (7) u + \bar{u} = 2 \operatorname{Re} u; \\ (2) \overline{u - v} = \bar{u} - \bar{v}; & (5) \bar{\bar{u}} = u; & (8) u \cdot \bar{u} = (\operatorname{Re} u)^2 + (\operatorname{Im} u)^2. \\ (3) \overline{u \cdot v} = \bar{u} \cdot \bar{v}; & (6) \bar{u} = u \iff u \in \mathbb{R}; & \end{array}$$

**1.9. Definíció.** Legyen adott a síkban egy Descartes-féle derékszögű koordinátarendszer, és feleltessük meg az  $a + bi$  komplex számnak az  $(a, b)$  koordinátájú pontot. Így kapjuk a **komplex számsíkot**, más néven **Gauss-féle számsíkot**. Az első tengelyt (abszcissa) **valós tengelynek**, a második tengelyt (ordináta) pedig **képzetes tengelynek** hívjuk. A valós tengelyen találhatóak a valós számok, a képzetes tengelyen pedig az úgynevezett **tiszta képzetes számok**.

**1.10. Definíció.** A  $z = a + bi$  komplex szám **abszolút értékén** a  $|z| = \sqrt{a^2 + b^2}$  nemnegatív valós számot értjük.

**1.11. Megjegyzés.** A komplex számsíkon az abszolút érték az origótól (nullától) való távolságot jelenti, a konjugálás nem más, mint a valós tengelyre való tükrözés, az összeadás pedig (hely)vektorok összeadásával írható le geometriailag.

**1.12. Tétel.** Bármely  $u, v$  komplex számokra érvényesek az alábbiak:

$$\begin{array}{lll} (1) |u| = \sqrt{u\bar{u}}; & (3) |u \cdot v| = |u| \cdot |v|; & (5) |\bar{u}| = |u|; \\ (2) 1/u = \bar{u}/|u|^2 \text{ ha } u \neq 0; & (4) |u/v| = |u|/|v| \text{ ha } v \neq 0; & (6) |u + v| \leq |u| + |v|. \end{array}$$

### Trigonometrikus alak, hatványozás, gyökvonás, egységgyökök

**1.13. Definíció.** Egy nemnulla  $z$  komplex szám **argumentumán** olyan  $\arg z$  irányított szöveget értünk, amellyel a valós tengely pozitív felét az origó körül elforgatva átmegy a  $z$ -nek megfelelő ponton.

**1.14. Megjegyzés.** A nullának nincs argumentuma, a nullától különböző komplex számok argumentuma pedig csak „modulo  $2\pi$ ”, azaz  $2\pi$  egész számú többszöröseitől eltekintve meghatározott.

<sup>†</sup>A természetes számok halmazát  $\mathbb{N}$ , a nemnegatív egész számok halmazát  $\mathbb{N}_0$  jelöli, azaz  $\mathbb{N} = \{1, 2, 3, \dots\}$  és  $\mathbb{N}_0 = \{0, 1, 2, \dots\}$ .

**1.15. Állítás.** Bármely  $0 \neq z \in \mathbb{C}$  esetén az  $r = |z|$  és  $\varphi = \arg z$  jelöléssel

$$z = r(\cos \varphi + i \sin \varphi) = r \operatorname{cis} \varphi.$$

**1.16. Definíció.** A nemnulla komplex számok fenti (azaz  $|z| \cdot (\cos \arg z + i \sin \arg z)$  alakú) felírását **trigonometrikus alaknak** nevezzük.

**1.17. Megjegyzés.** A nullának nincs trigonometrikus alakja, hiszen argumentuma sincs, de  $r = 0$  és bármely  $\varphi \in \mathbb{R}$  esetén nyilván  $0 = r(\cos \varphi + i \sin \varphi)$ .

**1.18. Állítás.** Bármely  $r, r' \in \mathbb{R}^+$  és  $\varphi, \varphi' \in \mathbb{R}$  esetén

$$r \operatorname{cis} \varphi = r' \operatorname{cis} \varphi' \iff r = r' \text{ és } \exists k \in \mathbb{Z} : \varphi' = \varphi + 2k\pi.$$

**1.19. Tétel.** Tetszőleges nullától különböző  $u = r \operatorname{cis} \varphi$  és  $v = s \operatorname{cis} \psi$  komplex számokra

$$(1) \bar{u} = r \operatorname{cis}(-\varphi); \quad (2) uv = rs \operatorname{cis}(\varphi + \psi); \quad (3) \frac{1}{v} = \frac{1}{s} \operatorname{cis}(-\psi); \quad (4) \frac{u}{v} = \frac{r}{s} \operatorname{cis}(\varphi - \psi).$$

**1.20. Megjegyzés.** A szorzat trigonometrikus alakjára vonatkozó képletből látszik, hogy rögzített  $v = \operatorname{cis} \psi$  egységnyi abszolút értékű komplex szám esetén a  $z \mapsto z \cdot v$  leképezés nem más, mint az origó körüli  $\psi$  szögű forgatás a komplex számsíkon.

**1.21. Tétel (Moivre-képlet).** Bármely nemzérő  $z = r \operatorname{cis} \varphi$  komplex szám és  $n \in \mathbb{Z}$  esetén

$$z^n = r^n \operatorname{cis}(n\varphi).$$

**1.22. Definíció.** Tetszőleges  $n$  pozitív egész szám és  $z \in \mathbb{C}$  esetén azt mondjuk, hogy az  $u$  komplex szám  **$n$ -edik gyöke**  $z$ -nek, ha  $u^n = z$ .

**1.23. Tétel.** Minden nemnulla komplex számnak pontosan  $n$  különböző  $n$ -edik gyöke van. A  $z = r \operatorname{cis} \varphi$  trigonometrikus alakban megadott komplex szám  $n$ -edik gyökei:

$$\sqrt[n]{z} = \sqrt[n]{r} \operatorname{cis} \frac{\varphi + 2k\pi}{n} \quad (k = 0, 1, \dots, n-1).$$

**1.24. Definíció.** Az  $\varepsilon$  komplex számot  **$n$ -edik egységgyöknek** nevezzük, ha  $\varepsilon^n = 1$ .

**1.25. Állítás.** Az  $n$ -edik egységgyökök a következők:  $\varepsilon_0, \varepsilon_1, \dots, \varepsilon_{n-1}$ , ahol  $\varepsilon_k = \operatorname{cis} \frac{2k\pi}{n}$ . Ezzel a jelöléssel  $\varepsilon_0 = 1$  és  $\varepsilon_k = \varepsilon_1^k$  minden  $k \in \{0, 1, \dots, n-1\}$  esetén.

**1.26. Megjegyzés.** Az  $n$ -edik egységgyökök egy szabályos  $n$ -szöget alkotnak a komplex számsíkon, amelynek körülírt köre az origó középpontú egységkör, és egyik csúcsa 1. (Ez a két információ egyértelműen meg is határozza az  $n$ -szöget.)

**1.27. Következmény.** Egy nemnulla komplex szám összes  $n$ -edik gyökét megkapjuk, ha egy rögzített  $n$ -edik gyökét megszorozzuk sorra az  $n$ -edik egységgyökökkel. Tehát ha  $u_0^n = z \neq 0$ , akkor a  $z$  komplex szám  $n$ -edik gyökei:

$$\sqrt[n]{z} = u_0 \varepsilon_k \quad (k = 0, 1, \dots, n-1).$$

**1.28. Tétel.** Ha  $n > 1$ , akkor az  $n$ -edik egységgyökök összege 0.

## 2. Gyűrűk és testek

### A gyűrű, integritástartomány, test fogalma

**2.1. Definíció.** Ha egy nemüres  $R$  halmazon kettő kétváltozós művelet is értelmezve van (nevezzük az egyiket összeadásnak, a másikat szorzásnak) úgy, hogy  $(R; +)$  Abel-csoport,  $(R; \cdot)$  félcsoport, és a szorzás disztributív az összeadásra, akkor az  $(R; +, \cdot)$  struktúrát **gyűrűnek** nevezzük.

**2.2. Definíció.** Az  $(R; +)$  csoportot az  $(R; +, \cdot)$  gyűrű **additív csoportjának** nevezzük, és ennek megfelelően beszélhetünk **additív egységelemről** és **additív inverzről** is. Az  $(R; \cdot)$  félcsoport neve: a gyűrű **multiplikatív félcsoportja**.

**Jelölés.** Tetszőleges gyűrűben 0 jelöli az additív egységelemet, az  $a$  gyűrűelem additív inverzét pedig  $-a$  jelöli, és értelmezhetjük a kivonás műveletét a  $b - a = b + (-a)$  képlettel.

**2.3. Állítás.** Ha  $(R; +, \cdot)$  gyűrű, akkor minden  $a \in R$  esetén  $a \cdot 0 = 0 \cdot a = 0$  teljesül.

**2.4. Definíció.** **Testnek** nevezzük egy  $(T; +, \cdot)$  gyűrűt, ha  $(T \setminus \{0\}; \cdot)$  Abel-csoport (ebből következik, hogy  $|T| \geq 2$ ).

**2.5. Definíció.** Ha egy gyűrűben nemcsak az összeadás, hanem a szorzás is kommutatív, akkor **kommutatív gyűrűnek** nevezzük. Ha pedig nemcsak additív, de **multiplikatív egységelem** is létezik (amelyet általában 1 jelöl), akkor **egységelemes gyűrűről** beszélünk.

**2.6. Definíció.** Legyen  $R$  egységelemes gyűrű. Az  $a \in R$  elemet **egységnek** nevezzük, ha létezik **multiplikatív inverze**, azaz létezik olyan  $a^{-1} \in R$  elem, amelyre  $aa^{-1} = a^{-1}a = 1$  teljesül.

**2.7. Tétel.** Az egységek bármely egységelemes gyűrűben csoportot alkotnak a szorzás műveletére nézve.

**2.8. Definíció.** Az  $R$  gyűrű egységeinek multiplikatív csoportját  $R$  **egységcsoportjának** nevezzük és  $R^*$ -gal jelöljük.

**2.9. Definíció.** Ha  $T$  test, akkor a  $(T^*; \cdot) = (T \setminus \{0\}; \cdot)$  Abel-csoportot a  $T$  test **multiplikatív csoportjának** hívjuk.

**2.10. Definíció.** Ha egy gyűrű  $a, b$  elemeire  $ab = 0$  teljesül, de se  $a$ , se  $b$  nem nulla, akkor azt mondjuk, hogy  $a$  és  $b$  **zérusosztók**. Ha egy gyűrűben nincsenek zérusosztók (azaz nullától különböző elemek szorzata sosem nulla), akkor **zérusosztómentes gyűrűnek** nevezzük. A kommutatív, egységelemes, zérusosztómentes gyűrű neve **integritástartomány**.

**2.11. Állítás.** Integritástartományban lehet nemzéró elemmel egyszerűsíteni, azaz tetszőleges  $a, b, c$  ( $c \neq 0$ ) elemekre

$$ac = bc \implies a = b.$$

**2.12. Állítás.** Minden test integritástartomány.

### Nevezetes gyűrűk: maradékosztály-gyűrűk, Gauss-egészek, polinomgyűrűk

**2.13. Állítás.** Minden  $m \geq 2$  egész szám esetén a modulo  $m$  maradékosztályok egységelemes kommutatív gyűrűt alkotnak. A  $\mathbb{Z}_m$  gyűrű egységei éppen a redukált maradékosztályok (innen a  $\mathbb{Z}_m^*$  jelölés). Ha  $m$  prímszám, akkor  $\mathbb{Z}_m$  test, ha  $m$  nem prím, akkor  $\mathbb{Z}_m$  még csak nem is integritástartomány.

**2.14. Definíció.** A  $\mathbb{Z}_m$  gyűrű neve modulo  $m$  **maradékosztály-gyűrű**, illetve prím modulus esetén **maradékosztálytest**.

**2.15. Definíció.** **Gauss-egészeknek** nevezzük azokat a komplex számokat, melyeknek valós és képzetes része is egész szám. A Gauss-egészek halmazát  $\mathbb{Z}[i]$  jelöli:  $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$ .

**2.16. Állítás.** A Gauss-egészek a komplex számok szokásos összeadásával és szorzásával integritástartományt alkotnak.

**2.17. Állítás.** A Gauss-egészek gyűrűjében az egységek éppen a negyedik egységgyökök:  $\mathbb{Z}[i]^* = \{1, -1, i, -i\}$ .

**2.18. Definíció.** Az  $R$  integritástartomány feletti **polinomnak** olyan  $R$ -beli elemekből képezett  $(a_0, a_1, \dots)$  végtelen sorozatot nevezünk, amely csak véges sok nullától különböző tagot tartalmaz. Az  $a_i$  elemeket a polinom **együtthatóinak** nevezzük. Az  $R$  feletti polinomok halmazát  $R[x]$  jelöli.

**2.19. Definíció.** Az  $f = (a_0, a_1, \dots)$  polinom **fokszámán** a legnagyobb olyan  $n$  nemnegatív egész számot értjük, amelyre  $a_n \neq 0$ . Ha nincs ilyen  $n$ , azaz ha  $f = (0, 0, \dots)$ , akkor azt mondjuk, hogy  $f$  fokszáma  $-\infty$ . Ha  $f$  fokszáma kisebb, mint 1 (azaz 0 vagy  $-\infty$ ), akkor  $f$ -et **konstans** polinomnak nevezzük. Ha  $f$  foka  $n \geq 0$ , akkor az  $a_n \in R$  elemet  $f$  **főegyütthatójának** hívjuk. Az olyan polinomot, amelynek főegyütthatója 1, **főpolinomnak** nevezzük. Az  $f$  polinom fokszámát  $\deg f$  jelöli.

**2.20. Definíció.** Az  $f = (a_0, a_1, \dots)$  és  $g = (b_0, b_1, \dots)$  polinomok **összegét** és **szorzatát** az alábbi képletekkel értelmezzük:

$$f + g = (c_0, c_1, \dots), \text{ ahol } c_n = a_n + b_n \quad \text{és} \quad f \cdot g = (d_0, d_1, \dots), \text{ ahol } d_n = \sum_{i=0}^n a_i \cdot b_{n-i}.$$

**2.21. Állítás.** Tetszőleges  $f, g \in R[x]$  polinomokra  $\deg(f + g) \leq \max(\deg f, \deg g)$  és  $\deg(fg) = \deg f + \deg g$ .

**2.22. Tétel.** A fent definiált összeadással és szorzással  $R[x]$  integritástartomány.

**2.23. Definíció.** Az  $R[x]$  gyűrűt az  $R$  feletti egyhatározatlanú polinomok gyűrűjének, röviden  $R$  feletti **polinomgyűrűnek** nevezzük.

**2.24. Állítás.** Minden  $a, b \in R$  esetén

$$(a, 0, 0, \dots) + (b, 0, 0, \dots) = (a + b, 0, 0, \dots) \quad \text{és} \quad (a, 0, 0, \dots) \cdot (b, 0, 0, \dots) = (ab, 0, 0, \dots).$$

**Jelölés.** Tetszőleges  $a \in R$  esetén az  $(a, 0, 0, \dots)$  polinom helyett egyszerűen  $a$ -t írunk, és nem is különböztetjük meg az  $a$  gyűrűelemtől. (Úgy tekintjük, hogy  $R \subseteq R[x]$ .) A  $(0, 1, 0, \dots)$  polinomot pedig  $x$  jelöli a továbbiakban.

**2.25. Tétel.** Minden nemzéró polinom előáll  $a_0 + a_1x + \dots + a_nx^n$  ( $a_n \neq 0$ ) alakban, és ez az előállítás egyértelmű. Ha  $f = (a_0, a_1, \dots)$  egy  $n$ -edfokú polinom, akkor

$$f = (a_0, a_1, \dots, a_n, 0, 0, \dots) = a_0 + a_1x + \dots + a_nx^n.$$

**Jelölés.** A polinomokat ezentúl  $a_nx^n + \dots + a_1x + a_0$  vagy  $\sum_{i=0}^n a_ix^i$  alakban írjuk fel. Egy ilyen felírásnál legtöbbször hallgatólagosan feltesszük, hogy  $a_n \neq 0$  (azaz a polinom  $n$ -edfokú), valamint hogy  $a_{n+1} = a_{n+2} = \dots = 0$ . Az  $x$  szimbólum neve: **határozatlan**. A határozatlant bármilyen más betű is jelölheti, ilyenkor az  $R[x]$  jelölés is megfelelően módosul. (Például ha a határozatlan  $y$ , akkor a polinomgyűrű  $R[y]$ .)

**2.26. Állítás.** Az  $R[x]$  polinomgyűrűben az egységek pontosan azok a konstans polinomok, amelyek (mint  $R$ -beli elemek) egységek  $R$ -ben. Formálisan:  $R[x]^* = R^*$ .

### 3. Test feletti egyhatározatlanú polinomok\*

#### A polinomok számelmélete

**3.1. Definíció.** Az  $f \in T[x]$  polinom **osztója** a  $g \in T[x]$  polinomnak (jelölés:  $f \mid g$ ), ha létezik olyan  $h \in T[x]$  polinom amelyre  $g = fh$ .

**3.2. Definíció.** Az  $f$  és  $g$  polinomok **asszociáltak** (jelölés:  $f \sim g$ ), ha  $f \mid g$  és  $g \mid f$ .

**3.3. Tétel.** A  $T[x]$  polinomgyűrűn az oszthatóság reflexív és tranzitív reláció, továbbá tetszőleges  $f, g \in T[x]$  polinomokra

$$(1) f \sim g \iff \exists c \in T \setminus \{0\} : g = cf; \quad (2) f \mid g \text{ és } g \neq 0 \implies \deg f \leq \deg g.$$

**3.4. Tétel.** Az asszociáltság ekvivalenciareláció  $T[x]$ -en. A nulla osztályát kivéve minden asszociáltsági osztály tartalmaz pontosan egy főpolinomot.

**3.5. Tétel (a maradékos osztás tétele).** Ha  $f, g \in T[x]$ , és  $g \neq 0$ , akkor léteznek olyan egyértelműen meghatározott  $q$  és  $r \in T[x]$  polinomok, amelyekre  $f = qg + r$  és  $\deg r < \deg g$ . Ebben a maradékos osztásban  $f$  az **osztandó**,  $g$  az **osztó**,  $q$  a **hányados** és  $r$  a **maradék**.

**3.6. Definíció.** A  $d \in T[x]$  polinom **legnagyobb közös osztója** az  $f$  és  $g \in T[x]$  polinomoknak, ha teljesül a következő két feltétel:

$$(1) d \mid f \text{ és } d \mid g; \\ (2) \forall k \in T[x] : (k \mid f \text{ és } k \mid g) \implies k \mid d.$$

Hasonlóan definiálható polinomok **legkisebb közös többszöröse** is.

**3.7. Tétel.** Bármely két  $f, g \in T[x]$  polinomnak létezik legnagyobb közös osztója és legkisebb közös többszöröse, és ezek asszociáltság erejéig egyértelműen meghatározottak. A legnagyobb közös osztó kiszámítható az *euklideszi algoritmussal*, és kifejezhető  $f$  és  $g$  „lineáris kombinációjaként”:  $\exists u, v \in T[x] : fu + gv = \text{lko}(f, g)$ .

**3.8. Tétel.** Tetszőleges adott nemzéró  $f, g, h \in T[x]$  polinomok esetén az  $fu + gv = h$  egyenlet akkor és csak akkor oldható meg az ismeretlen  $u, v \in T[x]$  polinomokra nézve, ha  $\text{lko}(f, g) \mid h$ .

**3.9. Definíció.** Tetszőleges  $f, g, m \in T[x]$  esetén azt mondjuk, hogy  $f$  **kongruens  $g$ -vel modulo  $m$** , ha  $m \mid f - g$  (jelölés:  $f \equiv g \pmod{m}$ ).

**3.10. Állítás.** A mod  $m$  kongruencia ekvivalenciareláció  $T[x]$ -en, és két polinom akkor és csak akkor kongruens modulo  $m$ , ha ugyanazt a maradékot adják  $m$ -mel osztva.

**3.11. Tétel.** Tetszőleges  $f, g, h \in T[x]$  esetén az  $fu \equiv h \pmod{m}$  lineáris kongruencia akkor és csak akkor oldható meg (az  $u$  ismeretlen polinomra nézve), ha  $\text{lko}(f, m) \mid h$ .

**3.12. Definíció.** A mod  $m$  kongruenciához tartozó ekvivalenciaosztályokat modulo  $m$  **maradékosztályoknak** nevezzük. Az  $f \in T[x]$  polinomot tartalmazó modulo  $m$  maradékosztályt  $\bar{f}$  jelöli, a maradékosztályok halmazát (vagyis a modulo  $m$  kongruenciához tartozó faktorhalmazt) pedig  $T[x]/(m)$  jelöli. Tehát  $T[x]/(m) = \{\bar{f} : f \in T[x]\}$ .

**3.13. Definíció.** A modulo  $m$  maradékosztályok halmazán értelmezzük az összeadást, az additív inverz képzését és a szorzást a következőképpen: tetszőleges  $f, g \in T[x]$  esetén legyen  $\bar{f} + \bar{g} = \overline{f + g}$ ,  $-\bar{g} = \overline{-g}$ ,  $\bar{f} \cdot \bar{g} = \overline{f \cdot g}$ .

**3.14. Állítás.** A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (additív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel  $T[x]/(m)$  kommutatív egységelemes gyűrűt alkot (**maradékosztály-gyűrű**).

**3.15. Tétel.** Az  $\bar{f} \in T[x]/(m)$  maradékosztálynak akkor és csak akkor létezik multiplikatív inverze, ha  $\text{lko}(f, m) \sim 1$ . Ilyenkor a multiplikatív inverz egyértelműen meghatározott.

\*Ebben a fejezetben  $T$  mindig tetszőleges testet jelöl, és – hacsak mást nem mondunk – minden polinomot ezen test felett tekintünk.

## Polinomfüggvények, gyökök, interpoláció

**3.16. Definíció.** Az  $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$  polinom  $c \in T$  helyen vett **helyettesítési értékén** az  $f(c) = a_n c^n + \dots + a_1 c + a_0 \in T$  elemet értjük. Az  $f \in T[x]$  polinomhoz tartozó **polinomfüggvény** pedig nem más, mint az  $f: T \rightarrow T, c \mapsto f(c)$  leképezés. A polinomot és a hozzá tartozó polinomfüggvényt ugyanúgy jelöljük; a szöveggörnyezetből kiderül, hogy mikor melyikről van szó. Ha polinomfüggvényekről van szó, akkor  $x$ -et **változónak** nevezzük (nem pedig határozatlannak).

**3.17. Definíció.** Az  $\alpha \in T$  elem **gyöke** az  $f \in T[x]$  polinomnak, ha  $f(\alpha) = 0$ .

**3.18. Tétel (Bézout tétele).** Bármely  $f \in T[x]$  és  $\alpha \in T$  esetén

$$f(\alpha) = 0 \iff x - \alpha \mid f.$$

**3.19. Következmény.** Tetszőleges  $f, g \in T[x]$  polinomok esetén  $f$  és  $g$  közös gyökei ugyanazok, mint  $\text{lko}(f, g)$  gyökei.

**3.20. Következmény.** Ha  $\alpha_1, \dots, \alpha_k \in T$  páronként különböző elemek és  $f \in T[x]$ , akkor

$$f(\alpha_1) = \dots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \dots \cdot (x - \alpha_k) \mid f.$$

**3.21. Definíció.** Azt mondjuk, hogy az  $f \in T[x]$  polinomnak az  $\alpha \in T$  elem  **$k$ -szoros gyöke**, ha  $(x - \alpha)^k \mid f$  de  $(x - \alpha)^{k+1} \nmid f$ . A  $k$  számot az  $\alpha$  gyök **multiplícitásának** nevezzük.

**3.22. Megjegyzés.** Megengedjük a  $k = 0$  esetet is:  $\alpha$  pontosan akkor nullaszoros gyök, ha nem gyök.

**3.23. Következmény.** Ha a nemnulla  $f \in T[x]$  polinom fokszáma  $n$ , akkor legfeljebb  $n$  különböző gyöke van a  $T$  testben.

**3.24. Következmény.** Ha az  $f, g \in T[x]$  polinomok legfeljebb  $n$ -edfokúak, és  $n+1$  különböző helyen ugyanaz a helyettesítési értékük, akkor  $f = g$ .

**3.25. Következmény.** Ha a  $T$  test végtelen, akkor két  $T$  feletti polinom akkor és csak akkor egyenlő, ha a hozzájuk tartozó polinomfüggvények megegyeznek.

**3.26. Megjegyzés.** Ha a  $T$  test véges, akkor található különböző  $T$  feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik (keressünk ilyen példákat!).

**3.27. Tétel (Lagrange-interpoláció).** Tetszőleges  $c_1, \dots, c_{n+1}$  páronként különböző és  $d_1, \dots, d_{n+1}$  (nem feltétlenül különböző)  $T$ -beli elemekhez létezik pontosan egy  $f \in T[x]$  legfeljebb  $n$ -edfokú polinom, amelyre  $f(c_i) = d_i$  ( $i = 1, \dots, n+1$ ).

**3.28. Definíció.** Az előző tételbeli  $f$  polinom neve **Lagrange-féle interpolációs polinom**.

**3.29. Megjegyzés.** Előfordulhat, hogy az  $n+1$  pontra illesztett Lagrange-féle interpolációs polinom foka kisebb, mint  $n$ . Pontosán  $n$ -edfokú polinom létezését nem lehet garantálni. Ha nem kötünk ki semmit a fokszámra, akkor elveszítjük az unicitást: bármely  $g \in T[x]$  polinomra  $f + (x - c_1) \cdot \dots \cdot (x - c_{n+1}) \cdot g$  is megfelelő. Nem nehéz meggondolni (tegyük meg!), hogy minden olyan polinom, amely a  $c_i$  helyeken a  $d_i$  értékeket veszi fel, előáll ilyen alakban.

## Irreducibilis polinomok, véges testek

**3.30. Definíció.** A  $p \in T[x]$  polinom **irreducibilis**, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált  $p$ -hez. (Ekkor a másik tényező szükségképpen asszociált 1-hez; ilyenkor **triviális faktorizációról** beszélünk.) Formálisan:

$$\forall f, g \in T[x] : p = fg \implies (p \sim f \text{ vagy } p \sim g).$$

**3.31. Állítás.** Egy legalább elsőfokú  $p \in T[x]$  polinom akkor és csak akkor irreducibilis, ha  $p$  nem bontható deg  $p$ -nél kisebb fokszámú polinomok szorzatára.

**3.32. Definíció.** A  $p \in T[x]$  polinom **prím**, ha legalább elsőfokú, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall f, g \in T[x] : p \mid fg \implies (p \mid f \text{ vagy } p \mid g).$$

**3.33. Tétel.** Test feletti polinomokra az irreducibilitás és a prím tulajdonság ekvivalens.

**3.34. Tétel.** Minden legalább elsőfokú  $T$  feletti polinom felbontható irreducibilis polinomok szorzatára. Ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelműen meghatározott, azaz ha  $p_1 \cdot \dots \cdot p_n$  és  $q_1 \cdot \dots \cdot q_m$  ugyanazon polinom két irreducibilis faktorizációja, akkor  $n = m$ , és létezik olyan  $\pi \in S_n$  permutáció, hogy  $p_i \sim q_{\pi(i)}$  minden  $i = 1, \dots, n$  esetén.

**3.35. Állítás.** Az elsőfokú polinomok bármely test felett irreducibilisek.

**3.36. Tétel.** Ha  $f \in T[x]$  irreducibilis és  $\deg f \geq 2$ , akkor  $f$ -nek nincs gyöke.

**3.37. Tétel.** Ha  $f \in T[x]$  és  $2 \leq \deg f \leq 3$ , akkor  $f$  pontosan akkor irreducibilis, ha nincs gyöke.

**3.38. Tétel.** A  $T[x]/(f)$  maradékosztály-gyűrű akkor és csak akkor test, ha  $f$  irreducibilis  $T$  felett.

**3.39. Tétel.** Legyen  $T$  test,  $f \in T[x]$  irreducibilis polinom, és jelölje  $n$  az  $f$  polinom fokszámát. Ekkor a  $K = T[x]/(f)$  maradékosztály-gyűrű olyan test, amelyben az  $f$  polinomnak van gyöke. A  $K$  test minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} \quad (a_{n-1}, \dots, a_0 \in T)$$

alakban. Ha  $T = \mathbb{Z}_p$ , akkor  $|K| = p^n$ .

**3.40. Következmény.** Tetszőleges  $T$  test és  $f \in T[x]$  irreducibilis polinom esetén létezik olyan  $K$  test, amelyre

- (1)  $K$  **bővítése**  $T$ -nek, azaz  $K \supseteq T$ ;
- (2) létezik olyan  $\alpha \in K$  elem, amely gyöke  $f$ -nek;
- (3)  $K$  minden eleme egyértelműen előáll  $a_{n-1}\alpha^{n-1} + \dots + a_1\alpha + a_0$  ( $a_{n-1}, \dots, a_0 \in T$ ) alakban, ahol  $n = \deg f$ .

**3.41. Definíció.** Azt mondjuk, hogy a  $K$  test  $T$ -ből az  $\alpha$  elem **adjungálásával** keletkezik (jelölés:  $K = T(\alpha)$ ), és az ilyen módon előállt testeket  $T$  **egyszerű algebrai bővítéseinek** nevezzük.

**3.42. Megjegyzés.** Ha a  $K$  testet a  $T = \mathbb{R}$  és  $f = x^2 + 1$  esetre felírjuk, éppen a komplex számok testét kapjuk.

**3.43. Tétel.** Akkor és csak akkor létezik  $q$ -elemű test, ha  $q$  prímhatvány.

### Irreducibilis polinomok $\mathbb{C}$ és $\mathbb{R}$ felett, gyöktényezős alak, Viète-formulák

**3.44. Tétel (az algebra alaptétele).** Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

**3.45. Következmény.** A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

**3.46. Következmény.** Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha  $f = a_nx^n + \dots + a_1x + a_0 \in \mathbb{C}[x]$  ( $n \geq 1, a_n \neq 0$ ), akkor  $f$ -nek multiplicitással számolva pontosan  $n$  gyöke van. Ha ezek a gyökök  $\alpha_1, \dots, \alpha_n$  (mindegyiket annyszor feltüntetve, amennyi a multiplicitása), akkor  $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$ . Ezt nevezzük a polinom **gyöktényezős felbontásának**.

**3.47. Következmény.** Bármely  $f, g \in \mathbb{C}[x]$  esetén  $f \mid g$  akkor és csak akkor teljesül, ha  $f$  minden gyöke egyúttal gyöke  $g$ -nek is, mégpedig legalább akkora multiplicitással, mint  $f$ -nek.

**3.48. Tétel (Viète-formulák).** Legyenek az  $n$ -edfokú  $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$  főpolinom komplex gyökei  $\alpha_1, \dots, \alpha_n$  (mindegyiket annyszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

$$\begin{aligned} -a_{n-1} &= \alpha_1 + \alpha_2 + \dots + \alpha_n; \\ a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n; \\ -a_{n-3} &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n; \\ &\vdots \\ (-1)^{n-1} a_1 &= \alpha_1\alpha_2 \cdots \alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2 \cdots \alpha_{n-2}\alpha_n + \dots + \alpha_2\alpha_3 \cdots \alpha_{n-1}\alpha_n; \\ (-1)^n a_0 &= \alpha_1\alpha_2\alpha_3 \cdots \alpha_{n-1}\alpha_n. \end{aligned}$$

**3.49. Megjegyzés.** A fenti képleteket **Viète-formuláknak** hívjuk. A  $k$ -edik sor bal oldalán  $(-1)^k a_{n-k}$  áll, a jobb oldalon pedig az  $\alpha_1, \dots, \alpha_n$  betűkből képezett összes  $k$ -tényezős szorzat összege, tehát egy  $\binom{n}{k}$ -tagú összeg. Formálisan:

$$(-1)^k a_{n-k} = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1} \cdot \alpha_{i_2} \cdot \dots \cdot \alpha_{i_k}.$$

**3.50. Tétel.** A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \quad \forall z \in \mathbb{C} : f(z) = 0 \implies f(\bar{z}) = 0.$$

**3.51. Következmény.** Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az  $\mathbb{R}$  feletti irreducibilis polinomok a következők:

- $ax + b$  ( $a, b \in \mathbb{R}, a \neq 0$ );
- $ax^2 + bx + c$  ( $a, b, c \in \mathbb{R}, a \neq 0, b^2 - 4ac < 0$ ).

## Irreducibilis polinomok $\mathbb{Q}$ felett

**3.52. Definíció.** Az  $a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$  polinomot **primitív polinomnak** nevezzük, ha együtthatói relatív prímek, azaz  $\text{lko}(a_0, \dots, a_n) = 1$ .

**3.53. Állítás.** Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára:  $\forall f \in \mathbb{Q}[x] \exists r \in \mathbb{Q} \exists f^* \in \mathbb{Z}[x] : f = r f^*$  és  $f^*$  primitív polinom.

**3.54. Megjegyzés.** Az előző állításban  $f \sim f^*$  (ha  $f \neq 0$ ), tehát  $\mathbb{Q}[x]$ -ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

**3.55. Tétel (Gauss-lemma).** Primitív polinomok szorzata is primitív.

**3.56. Tétel.** Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor  $\mathbb{Q}$  felett sem bomlik így fel, és viszont. Formálisan: ha  $f \in \mathbb{Z}[x]$  és  $\deg f = n \geq 1$ , akkor az alábbi két állítás ekvivalens:

- (1)  $\exists g, h \in \mathbb{Z}[x] : f = gh$  és  $0 < \deg g, \deg h < n$ ;
- (2)  $\exists g, h \in \mathbb{Q}[x] : f = gh$  és  $0 < \deg g, \deg h < n$ .

**3.57. Definíció.** Azt mondjuk, hogy a  $p$  prímszám **pontos osztója** az  $a$  egész számnak, ha  $a$  osztható  $p$ -vel, de  $p^2$ -tel már nem. Jelölés:  $p \parallel a$ .

**3.58. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).** Legyen  $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . Ha létezik olyan  $p$  prímszám amelyre  $p \nmid a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \parallel a_0$ , akkor  $f$  irreducibilis a racionális számok teste felett.

**3.59. Következmény.** Minden  $n \geq 1$  egész számra létezik  $\mathbb{Q}$  felett irreducibilis  $n$ -edfokú polinom.

**3.60. Megjegyzés.** A Schönemann–Eisenstein-tétel megfordítása *nem igaz!* Vagyis abból, hogy nem létezik olyan  $p$  prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, nem következik, hogy a polinom nem irreducibilis (keressünk ellenpéldát!). A megfordítás helyett következzen inkább a tétel „tükröképe”.

**3.61. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium).** Legyen  $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ . Ha létezik olyan  $p$  prímszám amelyre  $p \parallel a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \nmid a_0$ , akkor  $f$  irreducibilis a racionális számok teste felett.

**3.62. Tétel (Rolle(?) tétele).** Legyen  $f = a_n x^n + \dots + a_1 x + a_0$  egy tetszőleges egész együtthatós polinom. Ha  $\frac{p}{q}$  egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz  $p, q \in \mathbb{Z}, q \neq 0$  és  $\text{lko}(p, q) = 1$ ), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

## Derivált, többszörös gyökök

**3.63. Definíció.** Az  $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$  polinom **deriváltján** az  $n a_n x^{n-1} + \dots + 2 a_2 x + a_1$  polinomot értjük.

**Jelölés.** Az  $f$  polinom deriváltját  $f'$  jelöli, a  $k$ -adik deriváltat pedig  $f^{(k)}$ , az  $f^{(1)} = f'$  és  $f^{(0)} = f$  megállapodással.

**3.64. Tétel.** Minden  $f, g \in \mathbb{C}[x]$  polinomra és  $k$  pozitív egész számra érvényesek az alábbi deriválási szabályok:

$$(1) (f + g)' = f' + g'; \quad (2) (fg)' = f'g + fg'; \quad (3) (f^k)' = k f^{k-1} f'.$$

**3.65. Tétel.** Ha  $k \geq 1$  és az  $\alpha$  komplex szám  $k$ -szoros gyöke az  $f$  polinomnak, akkor  $k - 1$ -szeres gyöke  $f'$ -nek. (Ha  $k = 1$ , akkor  $\alpha$  nem gyöke  $f'$ -nek.)

**3.66. Megjegyzés.** Az előző tétel megfordítása nem igaz:  $f'$ -nek lehetnek olyan gyökei is, amelyekért nem  $f$  a „felelős”.

**3.67. Következmény.** Az  $f \in \mathbb{C}[x]$  polinom  $\alpha$  gyökének multiplicitása nem más, mint a legkisebb olyan  $k$  nemnegatív egész, amelyre  $f^{(k)}(\alpha) \neq 0$ , azaz  $\alpha$  akkor és csak akkor  $k$ -szoros gyök, ha  $f(\alpha) = f'(\alpha) = \dots = f^{(k-1)}(\alpha) = 0$ , de  $f^{(k)}(\alpha) \neq 0$ .

**3.68. Következmény.** Az  $\alpha$  komplex szám akkor és csak akkor többszörös gyöke az  $f \in \mathbb{C}[x]$  polinomnak, ha gyöke  $\text{lko}(f, f')$ -nak.

**3.69. Következmény.** Bármely legalább elsőfokú  $f \in \mathbb{C}[x]$  polinomra az  $\frac{f}{\text{lko}(f, f')}$  polinom gyökei ugyanazok, mint  $f$  gyökei, de mindegyik egyszeres gyök.

**3.70. Következmény.** Ha  $T$  számtest, azaz részteste  $\mathbb{C}$ -nek, és  $f \in T[x]$  irreducibilis  $T$  felett, akkor  $f$ -nek minden komplex gyöke egyszeres.

## 4. Csoportok

### A csoport fogalma, izomorfia

#### 4.1. Definíció.

(0) Az egyetlen kétváltozós művelettel rendelkező algebrát **grupoidnak** nevezzük. Tehát  $(A; *)$  grupoid, ha  $A$  nemüres halmaz és  $*$ :  $A^2 \rightarrow A$  kétváltozós művelet  $A$ -n.

(1) Ha egy grupoid művelete asszociatív, akkor **félcsoportnak** nevezzük.

(2) Ha egy félcsoportban van **egységelem**, akkor **monoidnak** nevezzük. Tehát az  $(A; *)$  félcsoport akkor monoid, ha létezik olyan  $e \in A$  elem, amelyre

$$\forall a \in A : a * e = e * a = a.$$

(3) Ha egy monoidban minden elemnek van **inverze**, akkor **csoportnak** nevezzük. Tehát az  $(A; *)$  monoid ( $e$  egységelemmel) akkor csoport, ha

$$\forall a \in A \exists b \in A : a * b = b * a = e.$$

(4) Ha egy csoport művelete kommutatív, akkor **Abel-csoportnak** nevezzük.

**4.2. Állítás.** Bármely grupoidban legfeljebb egy egységelem létezhet. Bármely monoidban egy elemnek legfeljebb egy inverze lehet.

**4.3. Megjegyzés.** Ha a művelet nem asszociatív, akkor létezhet egy elemnek több inverze is (keressünk ilyen példákat!).

**4.4. Definíció.** Legyen  $*$  egy kétváltozós művelet a nemüres  $A$  halmazon.

(1)  $*$  **invertálható** művelet, ha bármely  $a, b \in A$  elemek esetén az  $a * x = b$ , illetve  $y * a = b$  egyenleteknek **legalább** egy megoldása van.

(2)  $*$  **kancellatív** művelet, ha bármely  $a, b \in A$  elemek esetén az  $a * x = b$ , illetve  $y * a = b$  egyenleteknek **legfeljebb** egy megoldása van.

**4.5. Megjegyzés.** A kancellativitás így is megfogalmazható:

$$\forall a, u, v \in A : a * u = a * v \implies u = v \quad \text{és} \quad u * a = v * a \implies u = v.$$

**4.6. Tétel.** Csoport művelete mindig invertálható és kancellatív. Fordítva, minden invertálható művelettel rendelkező félcsoport csoport.

**4.7. Állítás.** Véges alaphalmaz esetén az invertálhatóság és a kancellativitás egymással ekvivalens.

**4.8. Definíció.** Legyen  $\mathbb{A} = (A; *)$  és  $\mathbb{B} = (B; \oplus)$  két csoport (vagy csak grupoid). Azt mondjuk, hogy a  $\varphi: A \rightarrow B$  leképezés **izomorfizmus**  $\mathbb{A}$ -ból  $\mathbb{B}$ -be, ha  $\varphi$  bijektív leképezés, és  $\varphi$  **felcserélhető a műveletekkel**, azaz

$$\forall a_1, a_2 \in A : (a_1 * a_2) \varphi = a_1 \varphi \oplus a_2 \varphi.$$

Ha létezik  $\varphi: \mathbb{A} \rightarrow \mathbb{B}$  izomorfizmus, akkor azt mondjuk, hogy  $\mathbb{A}$  és  $\mathbb{B}$  **izomorf** (jelölés:  $\mathbb{A} \cong \mathbb{B}$ ).

### Nevezetes példák

**4.9. Példa.** Tetszőleges gyűrű Abel-csoportot alkot az összeadás műveletével, és tetszőleges egységelemes gyűrű egységei csoportot alkotnak a szorzás műveletével (keressünk konkrét példákat!).

**4.10. Definíció.** Ha  $G$  egy csoport, és a  $H \subseteq G$  halmaz is csoportot alkot a  $G$ -ből „örökölt” művelettel, akkor azt mondjuk, hogy  $H$  **részcsoportha**  $G$ -nek. (Pontosabban lásd a 4.43. Definícióban.)

**4.11. Példa.** Tetszőleges  $T$  test esetén a  $T$  feletti  $n \times n$ -es mátrixok gyűrűjének egységcsoportja a  $T$  feletti  $n$ -dimenziós **általános lineáris csoport** (jelölés:  $\text{GL}_n(T)$ ), ebben az 1 determinánsú mátrixok alkotta részcsoportha a megfelelő **speciális lineáris csoport** (jelölés:  $\text{SL}_n(T)$ ):

$$\text{GL}_n(T) = \{A \in T^{n \times n} : \det(A) \neq 0\}, \quad \text{SL}_n(T) = \{A \in T^{n \times n} : \det(A) = 1\}.$$

**4.12. Példa.** A komplex egységgyökök csoportot alkotnak a szorzás műveletével; ezen belül az  $n$ -edik egységgyökök egy  $E_n$  részcsoporthat alkotnak minden  $n \geq 2$  egész számra. Az  $E_n$  csoport izomorf a  $\mathbb{Z}_n$  csoporttal:  $(E_n; \cdot) \cong (\mathbb{Z}_n; +)$

**4.13. Példa.** Egy tetszőleges nemüres  $A$  halmaz összes transzformációi monoidot alkotnak a leképezésszorzás műveletével, a bijektív transzformációk (azaz permutációk) pedig csoportot alkotnak. Ez utóbbit nevezzük az  $A$  feletti **szimmetrikus csoportnak** (jelölés:  $S_A$ ).

**4.14. Példa.** Az  $S_4$  csoportban a  $V = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$  részcsoporthat **Klein-féle csoportnak** nevezzük.



**4.15. Példa.** A sík összes egybevágósági transzformációi csoportot alkotnak a leképezésszorzás műveletével, egy adott síkidomot önmagába képező egybevágóságok pedig részcsoportot alkotnak ebben a csoportban (a síkidom **szimmetriacsoportja**).

**4.16. Definíció.** A szabályos  $n$ -szög szimmetriacsoportját  **$n$ -edfokú diédercsoportnak** nevezzük és  $D_n$ -nel jelöljük.

**4.17. Tétel.** A  $D_n$  csoportnak  $2n$  eleme van:  $D_n = \{ \text{id}, a, a^2, \dots, a^{n-1}, t, at, a^2t, \dots, a^{n-1}t \}$ , ahol  $a$  jelöli a szabályos  $n$ -szög középpontja körüli  $\frac{2\pi}{n}$  szögű forgatást,  $t$  pedig egy tetszőleges szimmetriatengelyre való tükrözést. Ekkor  $a^k$  a középpont körüli  $\frac{2k\pi}{n}$  szögű forgatás ( $0 \leq k \leq n-1$ ), a  $t, at, a^2t, \dots, a^{n-1}t$  transzformációk pedig tengelyes tükrözések (két „szomszédos” tengely  $\frac{\pi}{n}$  szöget zár be egymással). Fennáll továbbá a  $ta = a^{-1}t$  összefüggés.

## Permutációcsoportok

**4.18. Definíció.** A nemüres  $A$  halmaz összes permutációi alkotta  $S_A$  szimmetrikus csoport részcsoportjait **permutációcsoportoknak** nevezzük.

**4.19. Definíció.** Az  $A = \{1, 2, \dots, n\}$  halmaz összes permutációi alkotta csoportot  **$n$ -edfokú szimmetrikus csoportnak** nevezzük, és  $S_n$ -nel jelöljük.

**4.20. Definíció.** Legyenek  $a_1, \dots, a_k \in \{1, 2, \dots, n\}$  különböző elemek, és legyen  $\pi \in S_n$  az alábbi permutáció:

$$a_1\pi = a_2, \quad a_2\pi = a_3, \quad \dots, \quad a_{k-1}\pi = a_k, \quad a_k\pi = a_1 \quad \text{és} \quad b\pi = b \quad \text{ha} \quad b \notin \{a_1, \dots, a_k\}.$$

Ezt a  $\pi$  permutációt így jelöljük:  $\pi = (a_1 a_2 \dots a_{k-1} a_k)$  és **ciklikus permutációnak** vagy röviden **ciklusnak** nevezzük.

**4.21. Definíció.** Két permutáció **idegen**, ha *mozgatott elemeik* halmaza diszjunkt.

**4.22. Tétel.** Ha  $\pi$  és  $\rho$  idegen permutációk, akkor fölcserélhetőek, azaz  $\pi\rho = \rho\pi$ .

**4.23. Tétel.** Minden  $S_n$ -beli permutáció előáll páronként idegen ciklusok szorzataként, és ez az előállítás a tényezők sorrendjétől eltekintve egyértelmű.

**4.24. Definíció.** A 2 hosszúságú ciklusokat, vagyis az  $(ij)$  alakú permutációkat **transzpozícióknak** nevezzük.

**4.25. Tétel.** Az  $S_n$  csoportot *generálják* a transzpozíciók, azaz minden  $S_n$ -beli permutáció előáll transzpozíciók szorzataként.

**4.26. Tétel.** Egy  $S_n$ -beli permutáció transzpozíciók szorzataként való felírásában a tényezők számának paritása egyértelműen meghatározott.

**4.27. Állítás.** A páros hosszúságú ciklusok páratlan permutációk, míg a páratlan hosszúságú ciklusok páros permutációk.

**4.28. Tétel.** A páros permutációk egy 2 indexű részcsoportot alkotnak  $S_n$ -ben. Ezt a csoportot **alternáló csoportnak** nevezzük, és  $A_n$ -nel jelöljük.

**4.29. Tétel.** Az alternáló csoportot *generálják* a 3 hosszúságú ciklusok, azaz minden  $A_n$ -beli permutáció előáll 3 hosszúságú ciklusok szorzataként.

## Hatványozás, elem rendje, ciklikus csoportok

**Jelölés.** Ezentúl  $G$  mindig egy tetszőleges csoportot jelöl, a csoportműveletet szorzásnak nevezzük (és úgy is írjuk), az egységelemet 1, az  $a$  elem inverzét pedig  $a^{-1}$  jelöli.

**4.30. Definíció.** Az  $a \in G$  elem egész kitevős hatványait a következőképpen értelmezzük: tetszőleges  $n$  pozitív egészre legyen  $a^n = a \cdot \dots \cdot a$  ( $n$  db  $a$  szorzata),  $a^{-n} = a^{-1} \cdot \dots \cdot a^{-1}$  ( $n$  db  $a^{-1}$  szorzata), továbbá legyen  $a^0 = 1$ .

**4.31. Tétel.** Tetszőleges  $G$  csoport,  $a, b \in G$  és  $m, n \in \mathbb{Z}$  esetén teljesülnek az alábbiak:

- (1)  $a^m \cdot a^n = a^{m+n}$ ;
- (2)  $(a^m)^n = a^{mn}$ ;
- (3) ha  $ab = ba$ , akkor  $(ab)^n = a^n \cdot b^n$ .

**4.32. Definíció.** Az  $a \in G$  **elem rendje** az a legkisebb  $n$  pozitív egész szám, amelyre  $a^n = 1$ . Ha nincs ilyen  $n$ , akkor  $a$  rendje végtelen. Az  $a$  elem rendjét  $o(a)$  jelöli. Egy véges **csoport rendjén** pedig elemeinek számát értjük.

**4.33. Állítás.** Ha az  $a \in G$  elem rendje  $n$  (véges), akkor bármely  $k, \ell \in \mathbb{Z}$  esetén

- (1)  $a^k = 1 \iff n \mid k$ ;
- (2)  $a^k = a^\ell \iff k \equiv \ell \pmod{n}$ ;
- (3)  $o(a^k) = \frac{n}{\text{inco}(k, n)}$ .

**Jelölés.** Tetszőleges  $a \in G$  esetén jelölje  $[a]$  az  $a$  elem összes hatványainak halmazát:  $[a] = \{a^k : k \in \mathbb{Z}\}$ . (Ezt nevezzük majd később az  $a$  elem által *generált részcsoporthnak*; lásd a 4.47. Definíciót.)

**4.34. Definíció.** A  $G$  csoportot *ciklikus csoportnak* nevezzük, ha egyetlen elemmel generálható, azaz létezik olyan  $a \in G$ , amelyre  $[a] = G$ .

**4.35. Tétel.** Legyen  $G$  egy tetszőleges csoport és  $a \in G$ . Ha  $a$  rendje végtelen, akkor  $([a]; \cdot) \cong (\mathbb{Z}, +)$ , ha pedig  $o(a) = n \in \mathbb{N}$ , akkor  $([a]; \cdot) \cong (\mathbb{Z}_n, +)$ .

**4.36. Következmény.** Egy csoport akkor és csak akkor ciklikus, ha izomorf a  $\mathbb{Z}, \mathbb{Z}_2, \mathbb{Z}_3, \mathbb{Z}_4, \dots$  csoportok valamelyikével.

**4.37. Tétel.** Ciklikus csoport minden részcsoporthja is ciklikus.

**4.38. Definíció.** A  $\mathbb{C}^*$  csoport véges rendű elemei éppen az egységgyökök. Ha  $\varepsilon \in \mathbb{C}^*$  rendje  $n$ , akkor azt mondjuk, hogy  $\varepsilon$  *primitív  $n$ -edik egységgyök*

**4.39. Tétel.** Egy  $\varepsilon \in E_n$  egységgyök pontosan akkor primitív  $n$ -edik egységgyök, ha hatványaiként megkapható az összes  $n$ -edik egységgyök, azaz  $[\varepsilon] = E_n$ .

**4.40. Tétel.** Az  $\varepsilon_k = \text{cis} \frac{2k\pi}{n} \in E_n$  egységgyök akkor és csak akkor primitív  $n$ -edik egységgyök, ha  $k$  relatív prím  $n$ -hez.

**4.41. Következmény.** A primitív  $n$ -edik egységgyökök száma  $\varphi(n)$  (itt  $\varphi$  az Euler-féle függvény, lásd az 5.1. Definíciót).

## Részcsoporthok, generálás

**4.42. Definíció.** Legyen  $\mathbb{A} = (A; *)$  egy grupoid, és  $B \subseteq A$ . Azt mondjuk, hogy a  $B$  halmaz *zárt* a  $*$  műveletre, ha

$$\forall b_1, b_2 \in B : b_1 * b_2 \in B.$$

Ha  $B$  *nemüres* zárt halmaz, akkor  $B$  grupoidot alkot a  $*$  művelettel (pontosabban annak  $B$ -re való megszorításával). Az ilyen  $\mathbb{B} = (B; *)$  grupoidot  $\mathbb{A}$  *részgrupoidjának* nevezzük. Jelölés:  $\mathbb{B} \leq \mathbb{A}$ .

**4.43. Definíció.** Ha  $(G; \cdot)$  csoport,  $\emptyset \neq H \subseteq G$ , és a  $(H; \cdot)$  részgrupoid maga is csoport, akkor azt mondjuk, hogy  $(H; \cdot)$  *részcsoporthja*  $(G; \cdot)$ -nek.

**4.44. Állítás.** Tetszőleges  $G$  csoport és  $\emptyset \neq H \subseteq G$  esetén  $H$  akkor és csak akkor részcsoporthja  $G$ -nek, ha

- (0)  $H$  zárt a szorzásra:  $\forall h_1, h_2 \in H : h_1 \cdot h_2 \in H$ ;
- (2)  $H$  tartalmazza  $G$  egységelemét:  $1_G \in H$ ;
- (3)  $H$  zárt az inverzképzésre:  $\forall h \in H : h^{-1} \in H$ .

**4.45. Tétel.** Részcsoporthok metszete is részcsoporth: ha  $H_1$  és  $H_2$  részcsoporthjai a  $G$  csoportnak, akkor  $H_1 \cap H_2$  is részcsoporth.

**4.46. Megjegyzés.** A tétel nem csak kettő, hanem több részcsoporthra is érvényes (akár végtelen sokra is!).

**4.47. Definíció.** Legyen  $G$  egy csoport, és  $B \subseteq G$ . A  $B$  halmaz által *generált részcsoporth* a *legsűkebb* olyan részcsoporth, ami tartalmazza  $B$ -t:

$$[B] = \bigcap_{B \subseteq H \leq G} H.$$

**4.48. Megjegyzés.** Az üres halmaz generátuma a legsűkebb részcsoporth:  $[\emptyset] = \{1_G\}$ .

**4.49. Definíció.** Ha  $[B] = G$ , akkor azt mondjuk, hogy  $B$  *generátorrendszer* a  $G$  csoportnak.

**4.50. Állítás.** A  $G$  csoportban a  $B \subseteq G$  részhalmaz által generált részcsoporth azokból az elemekből áll, amelyek megkaphatók  $B$  elemeiből (és az egységelemből) szorzás és inverzképzés véges számú alkalmazásával:

$$[B] = \{b_1^{\varepsilon_1} \cdots b_n^{\varepsilon_n} : n \in \mathbb{N}_0, b_1, \dots, b_n \in B, \varepsilon_1, \dots, \varepsilon_n = \pm 1\}.$$

## Lagrange tétele

**4.51. Tétel.** Legyen  $H \leq G$ , és definiáljunk a  $G$  halmazon egy  $\sim$  relációt:  $a \sim b \iff a^{-1}b \in H$ . Ekkor  $\sim$  ekvivalencia-reláció, és egy  $a \in G$  elem ekvivalenciaosztálya  $aH = \{ah : h \in H\}$ .

**4.52. Definíció.** Az  $aH$  halmazt az  $a$  elem  $H$  szerinti **bal oldali mellékosztályának** nevezzük.

**4.53. Következmény.** Egy  $H \leq G$  részcsoport szerinti bal oldali mellékosztályok a  $G$  csoport egy osztályozását alkotják.

**4.54. Megjegyzés.** Hasonló módon definiálhatóak a  $Ha$  **jobb oldali mellékosztályok**, amelyek szintén osztályozást alkotnak.

**4.55. Definíció.** A  $G$  véges csoport  $H$  részcsoportja szerinti bal oldali (jobb oldali) mellékosztályok számát  $H$  **indexének** nevezzük. Jelölése:  $[G : H]$ .

**4.56. Tétel (Lagrange tétele).** Tetszőleges  $G$  véges csoport és  $H \leq G$  részcsoport esetén  $|G| = |H| \cdot [G : H]$ .

**4.57. Következmény.** Legyen  $G$  egy  $n$ -elemű csoport.

- (1) Minden  $H \leq G$  részcsoportra  $|H| \mid n$ .
- (2) Minden  $a \in G$  esetén  $o(a) \mid n$ .
- (3) Minden  $a \in G$  esetén  $a^n = 1$ .
- (4) Minden  $a \in G$  esetén  $a^{-1} = a^{n-1}$ .
- (5) Ha  $n$  prímszám, akkor  $G$  ciklikus.

**4.58. Tétel.** A legfeljebb 7-elemű csoportok (izomorfia erejéig) a következők:  $\{1\}$ ;  $\mathbb{Z}_2$ ;  $\mathbb{Z}_3$ ;  $\mathbb{Z}_4, V$ ;  $\mathbb{Z}_5$ ;  $\mathbb{Z}_6, S_3$ ;  $\mathbb{Z}_7$ .

## 5. Hatványozás modulo $m$

### Az Euler-féle $\varphi$ függvény

**5.1. Definíció.** Tetszőleges  $n$  természetes szám esetén legyen  $\varphi(n) = |\mathbb{Z}_n^*| = |\{a \in \mathbb{N} : 1 \leq a \leq n \text{ és } a \perp n\}|$ . Az így definiált  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$  függvényt **Euler-féle  $\varphi$  függvénynek** nevezzük.

**5.2. Tétel.** Az Euler-féle  $\varphi$  függvény **gyengén multiplikatív**, azaz  $m \perp n$  esetén  $\varphi(mn) = \varphi(m)\varphi(n)$ .

**5.3. Tétel.** Legyen az  $n$  természetes szám prímtényezős felbontása  $n = \prod_{i=1}^k p_i^{\alpha_i}$ . Ekkor

$$\varphi(n) = n \cdot \prod_{i=1}^k \left(1 - \frac{1}{p_i}\right) = \prod_{i=1}^k (p_i^{\alpha_i} - p_i^{\alpha_i-1}) = \prod_{i=1}^k p_i^{\alpha_i-1} (p_i - 1).$$

**5.4. Tétel.** Minden  $n$  természetes szám esetén  $\sum_{d \mid n} \varphi(d) = n$ .

**5.5. Tétel (Euler–Fermat-tétel).** Ha az  $a$  egész szám relatív prím az  $m$  moduluszhoz, akkor  $a^{\varphi(m)} \equiv 1 \pmod{m}$ .

**5.6. Következmény (kis Fermat-tétel).** Ha  $p$  prímszám és  $a$  nem osztható  $p$ -vel, akkor  $a^{p-1} \equiv 1 \pmod{p}$ .

**5.7. Következmény.** Ha  $a \in \mathbb{Z}$  relatív prím az  $m$  moduluszhoz és  $k, \ell \in \mathbb{Z}$ , akkor  $k \equiv \ell \pmod{\varphi(m)} \implies a^k \equiv a^\ell \pmod{m}$ .

### Rend, primitív gyök, index

**5.8. Definíció.** Legyen  $a \in \mathbb{Z}$  relatív prím az  $m$  moduluszhoz. Ekkor az  $a$  szám **modulo  $m$  rendjén** az  $\bar{a} \in \mathbb{Z}_m^*$  maradékosztály rendjét értjük (a  $\mathbb{Z}_m^*$  multiplikatív csoportban). Jelölés:  $o_m(a)$ .

**5.9. Állítás.** Tetszőleges  $a \in \mathbb{Z}$  és  $m \geq 2$  természetes szám esetén, ha  $a \perp m$ , akkor  $o_m(a) \mid \varphi(m)$ .

**5.10. Definíció.** Azt mondjuk, hogy a  $g$  egész szám **primitív gyök** modulo  $m$ , ha rendje éppen  $\varphi(m)$ .

**5.11. Állítás.** A  $g$  egész szám akkor és csak akkor primitív gyök modulo  $m$ , ha az összes mod  $m$  redukált maradékosztály megkapható  $\bar{g}$  hatványaként.

**5.12. Tétel.** Akkor és csak akkor létezik primitív gyök az  $m$  modulushoz (vagyis a  $\mathbb{Z}_m^*$  csoport akkor és csak akkor ciklikus), ha  $m = 2, 4, p^\alpha, 2p^\alpha$ , ahol  $p$  páratlan prímszám és  $\alpha \in \mathbb{N}$ . Ezekben az esetekben a mod  $m$  primitív gyökök száma  $\varphi(\varphi(m))$ .

**5.13. Definíció.** Tegyük fel, hogy  $g$  primitív gyök az  $m$  modulushoz. Az  $a$  egész szám *indexén* (az  $m$  modulusra és a  $g$  primitív gyökre nézve) olyan  $i$  kitevőt értünk, amelyre  $g^i \equiv a \pmod{m}$ . Jelölés:  $\text{ind}_g a$  (a modulus többnyire világos a szövegkörnyezetből).

**5.14. Megjegyzés.** Világos, hogy ha  $a$  és  $m$  nem relatív prím, akkor  $\text{ind}_g a$  nem értelmezett (ugyanis  $g^i$  mindig relatív prím  $m$ -hez). Ha viszont  $a$  és  $m$  relatív prím, akkor az 5.11. Következmény szerint  $a$  előáll  $g$  hatványaként modulo  $m$ , tehát ekkor  $\text{ind}_g a$  értelmezett. A 4.33. Állításból következik, hogy az index modulo  $\varphi(m)$  egyértelműen meghatározott.

**5.15. Tétel.** Legyen  $g$  primitív gyök modulo  $m$ , legyen  $k$  tetszőleges egész szám,  $a$  és  $b$  pedig relatív prímelek  $m$ -hez. Ekkor érvényesek az alábbi azonosságok:

$$\begin{aligned} (1) \text{ind}_g 1 &\equiv 0 \pmod{\varphi(m)}; & (3) \text{ind}_g a^k &\equiv k \cdot \text{ind}_g a \pmod{\varphi(m)}; \\ (2) \text{ind}_g(ab) &\equiv \text{ind}_g a + \text{ind}_g b \pmod{\varphi(m)}; & (4) \text{ind}_g(ab^{-1}) &\equiv \text{ind}_g a - \text{ind}_g b \pmod{\varphi(m)}. \end{aligned}$$

**5.16. Definíció.** Azt mondjuk, hogy az  $a$  egész szám  *$n$ -edik hatványmaradék* modulo  $m$ , ha az  $x^n \equiv a \pmod{m}$  kongruenciának van megoldása.

**5.17. Tétel.** Legyen  $g$  primitív gyök modulo  $m$ , és legyen  $a$  relatív prím  $m$ -hez. Ekkor  $a$  pontosan akkor  $n$ -edik hatványmaradék modulo  $m$ , ha  $\text{lko}(n, \varphi(m)) \mid \text{ind}_g a$ .

### Négyzetes maradékok, Legendre-szimbólum

**5.18. Definíció.** Az  $a$  egész számot *négyzetes maradéknak* nevezzük modulo  $m$ , ha az  $x^2 \equiv a \pmod{m}$  kongruenciának van megoldása. Ellenkező esetben azt mondjuk, hogy  $a$  *négyzetes nemmaradék* modulo  $m$ .

**5.19. Tétel.** Legyen  $p$  páratlan prímszám és  $g$  primitív gyök modulo  $p$ . Ekkor  $a \in \mathbb{Z}$  pontosan akkor négyzetes maradék modulo  $p$ , ha  $p \mid a$  vagy  $\text{ind}_g a$  páros.

**5.20. Definíció.** Tetszőleges  $p$  páratlan prímszám és  $p$ -vel nem osztható  $a$  egész szám esetén értelmezzük az  $\left(\frac{a}{p}\right)$  *Legendre-szimbólumot* a következőképpen:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{ha } a \text{ négyzetes maradék mod } p; \\ -1, & \text{ha } a \text{ négyzetes nemmaradék mod } p. \end{cases}$$

**5.21. Tétel (Euler-kritérium).** Ha  $p$  páratlan prímszám és  $p \nmid a$ , akkor

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

**5.22. Tétel.** Tetszőleges  $p$  páratlan prímszám és  $p$ -vel nem osztható  $a, b$  egész számok esetén teljesülnek az alábbiak:

$$(1) a \equiv b \pmod{p} \implies \left(\frac{a}{p}\right) = \left(\frac{b}{p}\right); \quad (2) \left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right) \left(\frac{b}{p}\right).$$

**5.23. Tétel.** Tetszőleges  $p$  páratlan prímszám esetén

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ha } p \equiv 1 \pmod{4}; \\ -1, & \text{ha } p \equiv 3 \pmod{4}. \end{cases}$$

**5.24. Tétel (négyzetes reciprocitási tétel).** Tetszőleges  $p, q$  különböző páratlan prímszámok esetén

$$\left(\frac{p}{q}\right) \left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \frac{q-1}{2}}.$$

**5.25. Tétel.** Tetszőleges  $p$  páratlan prímszámra

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} 1, & \text{ha } p \equiv 1, 7 \pmod{8}; \\ -1, & \text{ha } p \equiv 3, 5 \pmod{8}. \end{cases}$$