

KLASSZIKUS ALGEBRA

vázlat az előadáshoz[†]

2013 tavaszi félév

Waldhauser Tamás

5.15. Tétel (a szimmetrikus polinomok alaptétele). *Bármely szimmetrikus polinom felírható, mégpedig egyetlen módon, az elemi szimmetrikus polinomok polinomjaként. Formálisan:*

$$\forall f \in \mathcal{T}[x_1, \dots, x_n] : f \text{ szimmetrikus} \implies \exists! h \in \mathcal{T}[x_1, \dots, x_n] : f = h(\sigma_1, \dots, \sigma_n).$$

5.16. Következmény. *Tetszőleges n -edfokú $f \in \mathbb{Q}[x]$ polinom esetén ha f komplex gyökei (multiplicitással) $\alpha_1, \dots, \alpha_n$, akkor minden $g \in \mathbb{Q}[x_1, \dots, x_n]$ szimmetrikus polinomra $g(\alpha_1, \dots, \alpha_n) \in \mathbb{Q}$.*

Algebrai számok

5.17. Definíció. Az α komplex számot **algebrai szám**nak nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak. A nem algebrai számokat **transzcendens szám**oknak nevezzük.

5.18. Definíció. Ha $f \in \mathbb{Q}[x]$ minimális fokszámú mindazon nemzéró racionális együtthatós főpolinomok között, melyeknek α gyöke, akkor f -et az α algebrai szám **minimálpolinom**jának nevezzük.

5.19. Tétel. *Algebrai szám minimálpolinomja mindig egyértelműen meghatározott, és irreducibilis a racionális számtest felett. Továbbá, ha $f \in \mathbb{Q}[x]$ olyan irreducibilis főpolinom melynek az α algebrai szám gyöke, akkor f megegyezik α minimálpolinomjával.*

5.20. Tétel*. *Létezik transzcendens szám.*

5.21. Tétel*. *Az algebrai számok résztestet alkotnak a komplex számok testében.*

5.22. Tétel. *Ha α algebrai szám és $n \geq 2$, akkor $\sqrt[n]{\alpha}$ is algebrai szám (a gyöknek mind az n értékére).*

5.23. Definíció. Az α komplex számot **gyökmenntiség**nek nevezzük, ha megkapható racionális számokból kiindulva a négy alapművelet (összeadás, kivonás, szorzás, osztás) és egész kitevős gyökvonás véges számú alkalmazásával.

5.24. Következmény. *A gyökmenntiségek algebrai számok.*

5.25. Tétel*. *Van olyan algebrai szám, ami nem gyökmenntiség.*

5.26. Tétel*. *Az algebrai számok teste algebrailag zárt, azaz ha $\alpha \in \mathbb{C}$ gyöke a legalább elsőfokú $f = a_n x^n + \dots + a_1 x + a_0$ polinomnak, ahol a_0, \dots, a_n algebrai számok, akkor α maga is algebrai szám.*

1. Komplex számok

Kanonikus alak, konjugált, abszolút érték, komplex számsík

1.1. Definíció. A valós számokból álló számpárokat **komplex szám**oknak nevezzük.

Jelölés. A komplex számok halmazát \mathbb{C} jelöli, tehát $\mathbb{C} = \mathbb{R} \times \mathbb{R}$.

1.2. Definíció. Az (a, b) és (c, d) komplex számok **összegét** és **szorzatát** a következőképpen értelmezzük:

$$(a, b) + (c, d) = (a + c, b + d);$$

$$(a, b) \cdot (c, d) = (ac - bd, ad + bc).$$

1.3. Tétel. *Bármely u, v, w komplex számokra teljesülnek az alábbiak:*

$$(1) (u + v) + w = u + (v + w);$$

$$(6) u \cdot v = v \cdot u;$$

$$(2) u + v = v + u;$$

$$(7) u \cdot (1, 0) = u;$$

$$(3) u + (0, 0) = u;$$

$$(8) u \neq (0, 0) \implies \exists u^* \in \mathbb{C} : u \cdot u^* = (1, 0);$$

$$(4) \exists u' \in \mathbb{C} : u + u' = (0, 0);$$

$$(9) u \cdot (v + w) = u \cdot v + u \cdot w;$$

$$(5) (u \cdot v) \cdot w = u \cdot (v \cdot w);$$

$$(10) u \cdot (0, 0) = (0, 0).$$

1.4. Megjegyzés. Az előző tételbeli u' komplex számot (ami egyértelműen meghatározott) u **additív inverz**ének nevezzük és a továbbiakban $-u$ -val jelöljük. Hasonlóan u^* is egyértelműen meghatározott, neve u **multiplikatív inverz**e, jelölése u^{-1} . Két komplex szám **különbségét** a $v - u = v + (-u)$ képlettel definiálhatjuk, $u \neq (0, 0)$ esetén pedig v és u **hányadosa** $v/u = v \cdot u^{-1}$. A kivonás és osztás műveletére is érvényesek a valós számoknál megszokott tulajdonságok (például a szorzás disztributív a kivonásra, stb.).

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

$$(a, 0) + (b, 0) = (a + b, 0);$$

$$(a, 0) \cdot (b, 0) = (ab, 0).$$

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.

1.6. 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*

$$(a, b) = a + bi.$$

1.7. Definíció. A $z = (a, b)$ komplex szám $a + bi$ alakban való felírását z **kanonikus alak**jának, az a valós számot z **valós rész**ének, a b valós számot z **képzetes rész**ének nevezzük. Az i komplex szám neve **képzetes egység**.

Jelölés. A z komplex szám valós részét $\operatorname{Re} z$, képzetes részét $\operatorname{Im} z$ jelöli. Tehát $z = a + bi$ esetén $\operatorname{Re} z = a$ és $\operatorname{Im} z = b$.

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

1.9. Megjegyzés. Ezután a komplex számokat nem valós számokból álló számpárokként, hanem $a + bi$ alakú formális kifejezéseként kezeljük. Ezekkel ugyanúgy lehet számolni, ahogyan betűs kifejezésekkel szoktunk, de i^2 helyett szabad (sőt, többnyire kell is!) -1 -et írni. Az összeadás és a kivonás elég természetes ebben az alakban, a szorzás és a reciprokképzés pedig a következő módon végezhető el:

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i;$$

$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2}i \quad (\text{ha } a + bi \neq 0).$$

[†]A természetes számok halmazát \mathbb{N} , a nemnegatív egész számok halmazát \mathbb{N}_0 jelöli, azaz $\mathbb{N} = \{1, 2, 3, \dots\}$ és $\mathbb{N}_0 = \{0, 1, 2, \dots\}$. A csillaggal jelölt tételeket nem bizonyítjuk.

1.10. Definíció. A $z = a + bi$ komplex szám **konjugáltján** az $a - bi$ komplex számot értjük.

Jelölés. A z komplex szám konjugáltját \bar{z} jelöli. Tehát $\bar{z} = \operatorname{Re} z - i \operatorname{Im} z$.

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

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

1.12. Definíció. Legyen adott a síkban egy Descartes-féle derékszögű koordináta-rendszer, 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**.

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

Jelölés. A z komplex szám abszolút értékét $|z|$ jelöli. Tehát $|z| = \sqrt{(\operatorname{Re} z)^2 + (\operatorname{Im} z)^2}$.

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

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

1.15. 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.

Trigonometrikus alak, hatványozás, gyökvonás, egységgyökök

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

Jelölés. A z komplex szám argumentumát $\arg z$ jelöli.

1.17. Megjegyzés. A nullának nincs argumentuma, a nullától különböző komplex számok argumentuma pedig csak „modulo 2π ”, azaz 2π egész számú többszöröseitől eltekintve meghatározott.

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

$$z = r(\cos \varphi + i \sin \varphi).$$

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

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

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

$$r(\cos \varphi + i \sin \varphi) = r'(\cos \varphi' + i \sin \varphi') \iff r = r' \text{ és } \exists k \in \mathbb{Z} : \varphi' = \varphi + 2k\pi.$$

1.22. Tétel. *Tetszőleges nullától különböző $u = r(\cos \varphi + i \sin \varphi)$ és $v = s(\cos \psi + i \sin \psi)$ komplex számokra*

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

1.23. Megjegyzés. A szorzat trigonometrikus alakjára vonatkozó képletből látszik, hogy rögzített $v = \cos \psi + i \sin \psi$ esetén az $u \mapsto uv$ leképezés nem más, mint az origó körüli ψ szögű forgatás a komplex számsíkon.

1.24. Tétel (Moivre-képlet). *Bármely nemzérő $z = r(\cos \varphi + i \sin \varphi)$ komplex szám és $n \in \mathbb{Z}$ esetén*

$$z^n = r^n(\cos(n\varphi) + i \sin(n\varphi)).$$

1.25. 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 $u^n = z$.

5. Többhatározatlanú polinomok, szimmetrikus polinomok, algebrai számok

A többhatározatlanú polinomok gyűrűje, lexikografikus rendezés

5.1. Definíció. Adott T test feletti n -**határozatlanú monom**nak nevezzük az $ax_1^{k_1} \cdots x_n^{k_n}$ alakú formális kifejezéseket, ahol $0 \neq a \in T$ és $k_1, \dots, k_n \in \mathbb{N}_0$. Az ilyen monomok véges összegeit pedig T feletti n -**határozatlanú polinom**oknak nevezzük.

Jelölés. A T feletti n -határozatlanú polinomok halmazát $T[x_1, \dots, x_n]$ jelöli.

5.2. Tétel. *A természetes módon definiált szorzással és összeadással $T[x_1, \dots, x_n]$ integritástartomány.*

5.3. Megjegyzés. Az n -határozatlanú polinomok gyűrűjét lehetne rekurzívan is definiálni: legyen $T[x_1, \dots, x_n] = (T[x_1, \dots, x_{n-1}])[x_n]$, azaz a $T[x_1, \dots, x_{n-1}]$ integritástartomány feletti (egyhatározatlanú) polinomgyűrű.

5.4. Definíció. Azt mondjuk, hogy az $ax_1^{k_1} \cdots x_n^{k_n}$ monom **lexikografikusan megelőzi** a $bx_1^{l_1} \cdots x_n^{l_n}$ monomot, ha van olyan $i \in \{1, \dots, n\}$, amelyre $k_1 = l_1, \dots, k_{i-1} = l_{i-1}$ és $k_i > l_i$. (Vagyis megkeressük az első eltérést a k_1, k_2, \dots, k_n és az l_1, l_2, \dots, l_n kitevősorozatok között, és amelyekben nagyobb szám áll ezen a helyen, az kerül előrébb a lexikografikus sorrendben.)

Jelölés. Tetszőleges $M, N \in T[x_1, \dots, x_n]$ monomok esetén $M \sqsupset N$ jelöli azt, hogy M lexikografikusan megelőzi N -et, $M \sqsupseteq N$ pedig azt, hogy $M \sqsupset N$ vagy $M \sim N$. A \sqsupset relációt **lexikografikus rendezésnek** nevezzük.

5.5. Állítás. *A monomok halmazán \sqsupset reflexív, tranzitív és dichotóm reláció, valamint $M \sqsupseteq N$ és $M \sqsubseteq N$ akkor és csak akkor áll fenn egyszerre, ha M és N asszociált.*

5.6. Megjegyzés. Az előző állítás szerint a \sqsupset reláció teljes rendezés (dichotóm részbenrendezés) a monomok halmazán „modulo asszociáltság”. Általában egyszerre csak egy adott polinomban előforduló monomokat vizsgálunk, ezek között pedig nincsenek asszociáltak (azokat össze lehetne vonni egy taggá), tehát ilyenkor nagyjában teljesen rendezett halmazzal dolgozhatunk.

5.7. Állítás. *A monomok szorzása monoton a lexikografikus rendezésre nézve, azaz tetszőleges M, \hat{M}, N, \hat{N} monomokra ha $M \sqsupseteq N$ és $\hat{M} \sqsupseteq \hat{N}$, akkor $M\hat{M} \sqsupseteq N\hat{N}$, és itt asszociáltság csak akkor teljesül, ha $M \sim N$ és $\hat{M} \sim \hat{N}$.*

5.8. Állítás. *Tetszőleges $f, g \in T[x_1, \dots, x_n]$ nemzérő polinomokra fg lexikografikusan első tagja nem más, mint f és g lexikografikusan első tagjának szorzata.*

Szimmetrikus polinomok

5.9. Definíció. Az $f \in T[x_1, \dots, x_n]$ polinomot **szimmetrikus polinom**nak nevezzük, ha invariáns a határozatlanok minden permutációjára, azaz

$$\forall \pi \in \mathcal{S}_n : f(x_{1\pi}, \dots, x_{n\pi}) = f(x_1, \dots, x_n).$$

5.10. Definíció. A k -adik n -változós **elemi szimmetrikus polinom** az x_1, \dots, x_n határozatlanokból képezett összes k -tényezős szorzatok összege ($k = 1, \dots, n$).

Jelölés. A k -adik n -változós elemi szimmetrikus polinomot σ_k jelöli (az alaptest és n értéke általában világos a szöveg-környezetből), tehát

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_k} = \sum_{\substack{I \subseteq \{1, \dots, n\} \\ |I|=k}} \prod_{i \in I} x_i \in T[x_1, \dots, x_n].$$

5.11. Megjegyzés. Az elemi szimmetrikus polinomokkal már találkoztunk: segítségükkel fejezhetők ki egy komplex együtthatós főpolinom együtthatói a polinom gyökeiből. Tehát a Viète-formulák $\sigma_k(\alpha_1, \dots, \alpha_n) = (-1)^k a_{n-k}$ alakban is felírhatók.

5.12. Tétel. *A szimmetrikus polinomok részgyűrűt alkotnak a $T[x_1, \dots, x_n]$ polinomgyűrűben.*

5.13. Lemma. *Ha $ax_1^{k_1} \cdots x_n^{k_n}$ egy szimmetrikus polinom lexikografikusan első tagja, akkor $k_1 \geq \dots \geq k_n$.*

5.14. Lemma. *Tetszőleges $k_1 \geq \dots \geq k_n$ nemnegatív egészekhez léteznek olyan l_1, \dots, l_n nemnegatív egészek, hogy $\sigma_1^{l_1} \cdots \sigma_n^{l_n} \in T[x_1, \dots, x_n]$ lexikografikusan első tagja éppen $x_1^{k_1} \cdots x_n^{k_n}$.*

4.47. Tétel. A valós együtthatós $x^3 + px + q$ harmadfokú polinom valós, illetve nemvalós gyökeinek száma a $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3$ szám előjelétől függ az alábbi módon:

- ha $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 > 0$, akkor egy valós és két nemvalós konjugált komplex gyök van;
- ha $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 = 0$, akkor minden gyök valós, és közülük (legalább) kettő egybeesik;
- ha $\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 < 0$, akkor három különböző valós gyök van (ezt az esetet nevezzük **casus irreducibilis**nek).

4.48. Definíció. A $D = -108 \left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3 \right)$ számot nevezzük az $x^3 + px + q$ polinom **diszkrimináns**ának.

4.49. Megjegyzés. Az előző tétel szerint a diszkrimináns pontosan akkor nulla, ha van többszörös gyök. Deriválással meggyőződhetünk róla, hogy ez nem csak a valós esetre érvényes. A szimmetrikus polinomok alaptételének segítségével (5.15. Tétel) később igazolni tudjuk majd, hogy a diszkrimináns nem más, mint $(\alpha_1 - \alpha_2)^2 \cdot (\alpha_2 - \alpha_3)^2 \cdot (\alpha_3 - \alpha_1)^2$, ahol $\alpha_1, \alpha_2, \alpha_3$ a polinom komplex gyökei. Valójában ez a diszkrimináns definíciója. Ebből az alakból világosan látszik, hogy D akkor és csak akkor nulla, ha legalább két gyök egybeesik. Hasonlóan lehet definiálni tetszőleges fokszámú polinom diszkriminánsát is. Például, ha az $ax^2 + bx + c$ polinom komplex gyökei α_1 és α_2 , akkor diszkriminánsa $(\alpha_1 - \alpha_2)^2$, amit már középiskolai ismeretek birtokában is ki lehet számolni. Az eredmény: $\frac{b^2 - 4ac}{a^2}$, ami „majdnem ugyanaz”, mint amit a másodfokú polinom diszkriminánsának szoktunk nevezni.

Negyedfokú egyenlet

4.50. Definíció. Az $x^4 + ax^3 + bx^2 + cx + d = 0$ negyedfokú egyenlet **kubikus rezolvensének** az

$$(a\alpha - c)^2 - 4 \left(\frac{d^2}{4} + 2\alpha - b \right) (\alpha^2 - d) = 0$$

egyenletet nevezzük (ami az α ismeretlenre nézve harmadfokú egyenlet).

4.51. Tétel. Legyen $f = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$, és legyen α megoldása az $f(x) = 0$ negyedfokú egyenlet kubikus rezolvensének. Ekkor az $\left(\frac{a^2}{4} + 2\alpha - b\right)x^2 + (a\alpha - c)x + (\alpha^2 - d)$ másodfokú polinom teljes négyzet, azaz valamely $h \in \mathbb{C}[x]$ legfeljebb elsőfokú polinom négyzete. A $g = x^2 + \frac{c}{a}x + \alpha$ jelölést használva $f = g^2 - h^2 = (g + h)(g - h)$, vagyis f két másodfokú polinom szorzatára bomlik, és így gyökei a másodfokú egyenlet megoldóképletével meghatározhatók.

Polinom kontra polinomfüggvény, Lagrange-interpoláció

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

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

4.54. Megjegyzés. Ha a T test véges, akkor találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik. Például ha $T = \{c_1, \dots, c_n\}$, akkor az n -edfokú $(x - c_1) \cdots (x - c_n)$ polinomhoz éppúgy a konstans 0 függvény tartozik, mint a 0 polinomhoz.

4.55. 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 $f(c_i) = d_i$ ($i = 1, \dots, n+1$) teljesül.

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

4.57. 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 $f + (x - c_1) \cdots (x - c_{n+1}) \cdot g$ is megfelelő. Nem nehéz megmondolni (tegyük meg!), hogy minden olyan polinom, amely a c_i helyeken a d_i értékeket veszi fel, előáll ilyen alakban.

1.26. Tétel. Minden nemnulla komplex számnak pontosan n különböző n -edik gyöke van. A $z = r(\cos \varphi + i \sin \varphi)$ trigonometrius alakban megadott komplex szám n -edik gyökei:

$$\sqrt[n]{z} = \sqrt[n]{r} \left(\cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right) \quad (k = 0, 1, \dots, n-1).$$

1.27. Definíció. Az ε komplex számot **n -edik egységgyök**nek nevezzük, ha $\varepsilon^n = 1$.

1.28. Állítás. Az n -edik egységgyökök a következők:

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

Ezzel a jelöléssel $\varepsilon_0 = 1$ és $\varepsilon_k = \varepsilon_k^l$ minden $k \in \{0, 1, \dots, n-1\}$ esetén.

1.29. 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.)

1.30. 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:

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

1.31. Definíció. Legyen ε egy n -edik egységgyök. Azt mondjuk, hogy ε **primitív n -edik egységgyök**, ha nem l -edik egységgyök semmilyen n -nél kisebb l pozitív egészre. Másképp fogalmazva, n a legkisebb pozitív kitevő amelyre $\varepsilon^n = 1$ lesz:

$$n = \min \{ l \in \mathbb{N} : \varepsilon^l = 1 \}.$$

1.32. Állítás. Egy n -edik egységgyök pontosan akkor primitív n -edik egységgyök, ha hatványaiként megkapható az összes n -edik egységgyök.

1.33. Tétel. Az $\varepsilon_k = \cos \frac{2k\pi}{n} + i \sin \frac{2k\pi}{n}$ egységgyök akkor és csak akkor primitív n -edik egységgyök, ha k relatív prím n -hez.

1.34. Következmény. A primitív n -edik egységgyökök száma $\varphi(n)$ (itt φ az Euler-féle függvény).

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

2. Absztrakt algebrai struktúrák

Csoport, gyűrű, integritástartomány, test

A következőkben a számelmélet alapfogalmait és tételeit általánosítjuk az egész számok halmaza helyett tetszőleges halmazokra, amelyek elemeit lehet összeadni, kivonni és szorozni, és ezek a műveletek elég „szépen” viselkednek. Először pontosítjuk, hogy mit értünk szép viselkedésen, és nevet adunk a vizsgálandó struktúráknak.

2.1. Definíció. **Félcsoporton** egy asszociatív kétváltozós művelettel ellátott nemüres halmazt értünk. Formálisan: $(A; \circ)$ félcsoport, ha A nemüres halmaz, és

- (0) $\circ: A \times A \rightarrow A, (x, y) \mapsto x \circ y$;
- (1) $\forall a, b, c \in A: (a \circ b) \circ c = a \circ (b \circ c)$.

2.2. Definíció. Az $(A; \circ)$ félcsoport e elemét **egységelem**nek nevezzük, ha minden $a \in A$ -ra $a \circ e = e \circ a = a$ teljesül.

2.3. Definíció. Ha az $(A; \circ)$ félcsoportban e egységelem és $ab = ba = e$ teljesül az $a, b \in A$ elemekre, akkor azt mondjuk, hogy a és b egymás **inverze**.

2.4. Állítás. Félcsoportban az egységelem és az elemek inverzei egyértelműen meghatározottak (ha léteznek egyáltalán).

2.5. Definíció. Az $(A; \circ)$ félcsoport **csoport**, ha van benne egységelem és minden elemnek van inverze, azaz A nemüres halmaz, és

- (0) $\circ: A \times A \rightarrow A, (x, y) \mapsto x \circ y$;
- (1) $\forall a, b, c \in A: (a \circ b) \circ c = a \circ (b \circ c)$;
- (2) $\exists e \in A \forall a \in A: e \circ a = a \circ e = a$;
- (3) $\forall a \in A \exists a^* \in A: a a^* = a^* a = e$.

2.6. Definíció. Ha az $(A; \circ)$ csoport művelete kommutatív (azaz $\forall a, b \in A: a \circ b = b \circ a$), akkor **kommutatív csoport**nak, vagy **Abel-csoport**nak nevezzük.

Jelölés. Csoportban $a \circ b$ helyett általában ab -t írunk, és ezen multiplikatív írásmódnál az egységelemet 1 , az a elem inverzét pedig a^{-1} jelöli, továbbá kommutatív esetben szokás a ba^{-1} szorzat helyett b/a -t írni, még akkor is, ha a csoport elemei nem számok (és a művelet esetleg nem is szorzás). Abel-csoportok esetén használatos az additív írásmód is, ekkor $a \circ b$ helyett $a + b$ -t írunk, az egységelemet 0 , az a elem inverzét $-a$, a $b + (-a)$ összeget pedig $b - a$ jelöli.

2.7. Definíció. Ha egy nemüres halmazon kettő kétváltozós művelet is értelmezve van (nevezzük az egyiket összeadásnak, a másikat szorzásnak) úgy, hogy az alaphalmaz az összeadás műveletével kommutatív csoportot, a szorzás műveletével pedig félcsoportot alkot, és a szorzás disztributív az összeadásra, akkor ezt a kétműveletes struktúrát **gyűrűnek** nevezzük. Formálisan: $(R; +, \cdot)$ gyűrű, ha R nemüres halmaz, és

- (1) $(R; +)$ Abel-csoport;
- (2) $(R; \cdot)$ félcsoport;
- (3) $\forall a, b, c \in R : a \cdot (b + c) = a \cdot b + a \cdot c$ és $(b + c) \cdot a = b \cdot a + c \cdot a$.

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

Jelölés. Korábbi megállapodásunknak megfelelően 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.

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

2.10. Megjegyzés. Sok hasonló, az egész számokkal végzett műveleteknél megszokott tulajdonság érvényes tetszőleges gyűrűben, például $a(b - c) = ab - ac$, $-(ab) = (-a)b = a(-b)$, stb. De vigyázat: a szorzás általában nem kommutatív, így például $(a + b)(a - b) = a^2 - b^2$ vagy $(a + b)^2 = a^2 + 2ab + b^2$ már nem teljesül minden gyűrűben!

2.11. 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 **egység-elemes gyűrűről** beszélünk.

2.12. 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 **zérus-osztómentes gyűrűnek** nevezzük. A kommutatív, egység-elemes, zérusosztómentes gyűrű neve **integritástartomány**.

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

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

2.14. Definíció. Legyen R egység-elemes 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.

2.15. Tétel. Az egységek bármely egység-elemes gyűrűben csoportot alkotnak a szorzás műveletére nézve.

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

2.17. Definíció. *Testnek* nevezünk egy integritástartományt, ha legalább kételemű, és minden nemnulla elemének van multiplikatív inverze.

2.18. Definíció. Ha T test, akkor $(T \setminus \{0\}; \cdot)$ Abel-csoport, amelyet a T test **multiplikatív csoportjának** hívjuk.

2.19. Megjegyzés. A definíció alapján világos, hogy egy legalább kételemű R kommutatív egység-elemes gyűrű akkor és csak akkor test, ha egységcsoportja a nulla kivételével minden elemet tartalmaz, azaz $R^* = R \setminus \{0\}$.

Jelölés. Mivel gyűrűben és testben a két műveletet általában $+$ és \cdot jelöli, ezeket nem írjuk mindig ki, tehát $(R; +, \cdot)$ illetve $(T; +, \cdot)$ helyett egyszerűen csak R gyűrűről, illetve T testről beszélünk.

2.20. Definíció. Legyen R egy gyűrű és $S \subseteq R$. Ha S az R -ből „örökölt” műveletekkel maga is gyűrű, akkor azt mondjuk, hogy S **részgyűrűje** az R gyűrűnek. Hasonlóan definiálható a **résztest**, **részcsoport**, **részfélcsoport** fogalma is.

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

2.21. Állítás. Minden $m \geq 2$ egész szám esetén a modulo m maradékosztályok egység-elemes 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.

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

Gyökök és együtthatók közötti összefüggés

4.35. Tétel. 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 annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak az alábbi összefüggések:

$$-a_{n-1} = \alpha_1 + \alpha_2 + \dots + \alpha_n;$$

$$a_{n-2} = \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n;$$

$$-a_{n-3} = \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n;$$

$$\vdots$$

$$(-1)^{n-1} a_1 = \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_n + \dots + \alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n;$$

$$(-1)^n a_0 = \alpha_1\alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n.$$

4.36. Megjegyzés. A fenti képleteket **Viete-formuláknak** hívjuk. A k -adik 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:

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

Még formálisabban:

$$(-1)^k a_{n-k} = \sum_{I \subseteq \{1, \dots, n\}} \prod_{i \in I} \alpha_i.$$

Derivált, többszörös gyökök

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

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

$$(1) (f + g)' = f' + g';$$

$$(2) (fg)' = f'g + fg';$$

$$(3) (f^k)' = k f^{k-1} f'.$$

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

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

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

4.42. Következmény. Az α komplex szám akkor és csak akkor többszörös gyöke az $f \in \mathbb{C}[x]$ polinomnak, ha gyöke lanko (f, f') -nak.

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

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

Harmadfokú egyenlet

4.45. Állítás. Az $ay^3 + by^2 + cy + d = 0$ ($a, b, c, d \in \mathbb{C}, a \neq 0$) harmadfokú egyenletből az $x = y + \frac{b}{3a}$ új ismeretlenre való áttéréssel eltűnik a másodfokú tag, tehát a főegyütthatóval való leosztás után $x^3 + px + q = 0$ ($p, q \in \mathbb{C}$) alakú egyenletet kapunk.

4.46. Tétel. Az $x^3 + px + q = 0$ ($p, q \in \mathbb{C}$) harmadfokú egyenlet minden megoldása megkapható a **Cardano-képlet** segítségével:

$$x = \sqrt[3]{-\frac{q}{2} + \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}} + \sqrt[3]{-\frac{q}{2} - \sqrt{\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3}}.$$

A képlet kilenc számot is adhat, de ezek közül természetesen legfeljebb három lehet megoldása az egyenletnek, nevezetesen azok, ahol a két köbgyök szorzata $-\frac{p}{3}$. Ha u és v a két köbgyök egy-egy ilyen értéke, akkor az $x^3 + px + q$ polinom három gyöke (multiplicitással): $u + v$, $u\epsilon + v\bar{\epsilon}$, $u\bar{\epsilon} + v\epsilon$, ahol ϵ primitív harmadik egységgyök.

4.28. 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 $p \nmid a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \nmid a_0$, akkor f irreducibilis a racionális számok teste felett.

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

4.30. Megjegyzés. A Schönemann–Eisenstein-féle megfordítása *nem igaz!* Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítene a megfelelő oszthatósági feltételeket, nem következik, hogy a polinom nem irreducibilis (keressünk ellenpéldát!). A megfordítás helyett következtek inkább a tétel „tükkörképe”.

4.31. Tétel* (μυιὸν τῆν ἰσθμίδιον οὐβρηὶ ἐπι-νιστῆσαι—πρῶτον οὐβρῶν). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \mid a_n, p \mid a_{n-1}, \dots, p \mid a_1, p \nmid a_0$, akkor f irreducibilis a racionális számok teste felett.

4.32. 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.

Horner-módszer

Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ egy n -edfokú polinom és $c \in T$. Ha $f(c)$ értékét szeretnénk kiszámítani, akkor a szokásos $f(c) = a_n c^n + \dots + a_1 c + a_0$ felírást használva $2n - 1$ szorzást és n összeadást kell elvégeznünk. Ha viszont a disztributivitást kihasználva $f(c)$ -t a következő alakban írjuk fel, akkor csak n szorzást és n összeadást kell elvégeznünk:

$$f(c) = (\dots((a_n \cdot c + a_{n-1}) \cdot c + a_{n-2}) \cdot c + a_{n-3}) \dots + a_2) \cdot c + a_1) \cdot c + a_0.$$

Ezt nevezzük **Horner-elrendezésnek**. Figyeljük meg, hogy balról jobbra haladva elvégezve a műveleteket a következő részeredmény mindig úgy adódik, hogy az előzőt megszorozzuk c -vel, és hozzáadjuk f soron következő együtthatóját. (Itt részeredményen az egy zárójelpáron belüli kifejezéseket értjük.)

A számolást kényelmesebb az alábbi táblázatban elvégezni. A kettős vonaltól balra felírjuk emlékeztetőül c értékét, a kettős vonaltól jobbra a felső sorba f együtthatóit kerülnek, az alsó sort a_n -nel kezdjük, majd balról jobbra haladva sorra kitöltjük a mezőket. A következő üres mezőbe a tőle balra álló elem c -szeresének és az üres mező feletti elemnek az összegét kell írni. Az alsó sor utolsó eleme adja $f(c)$ értékét.

	a_n	a_{n-1}	\dots	a_2	a_1	a_0
c	a_n	$a_n \cdot c + a_{n-1}$	\dots	$a_2 \cdot c + a_1$	$a_1 \cdot c + a_0$	$f(c)$

Amint a következő tételből és következményéből kiderül, a Horner-elrendezés valójában nem csak $f(c)$ kiszámítására alkalmas.

4.33. Tétel (Horner-módszer). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ egy n -edfokú polinom és $c \in T$. Ha a Horner-módszerrel elkészített táblázat alsó sorában álló elemek b_n, \dots, b_1, b_0 , azaz $b_n = a_n$ és $b_i = b_{i+1} \cdot c + a_i$ ($i = n - 1, \dots, 0$), akkor b_0 nem más, mint az f -nek az $x - c$ polinommal való osztásakor keletkező maradék, $b_n x^{n-1} + \dots + b_2 x + b_1$ pedig ugyanazt az osztás hányadosa:

$$f = (x - c) \cdot (b_n x^{n-1} + \dots + b_2 x + b_1) + b_0.$$

4.34. Következmény (iterált Horner-módszer). Alkalmazzuk a Horner-módszert az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomra és a $c \in T$ elemre, majd egészítsük ki a táblázatot egy újabb, az előzőnél eggyel rövidebb sorral a fentebb leírt számolási szabályt követve. Folytassuk újabb, egyre rövidebb sorokkal, míg végül egy háromszög alakú táblázatot kapunk:

	a_n	a_{n-1}	a_{n-2}	\dots	a_2	a_1	a_0
c				\dots			d_0
c				\dots			d_1
c				\dots			d_2
\vdots	\vdots	\vdots	\vdots	\dots			\dots
c					d_{n-2}		
c					d_{n-1}		
c					d_n		

A táblázat jobb szélén átlósan elhelyezkedő elemek megadják annak a polinomnak az együtthatóit, amelyet f -ből az $x - c$ határozatlanra való áttéréssel kapunk (természetesen $d_0 = f(c)$ és $d_n = a_n$):

$$a_n x^n + \dots + a_1 x + a_0 = d_n (x - c)^n + \dots + d_1 (x - c) + d_0.$$

Kiolvasható a táblázatból az is, hogy c hányszoros gyöke f -nek: a c gyök multiplicitása nem más, mint a legkisebb olyan k , amelyre $d_k \neq 0$ (megengedve a $k = 0$ esetet is).

2.23. Definíció. **Gauss-egészeknek** nevezzük azokat a komplex számokat, melyeknek valós és képzetes része is egész szám.

Jelölés. A Gauss-egészek halmazát $\mathbb{Z}[i]$ jelöli: $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$.

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

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

A következőkben a polinom fogalmát definiáljuk, első ránézésre meglehetősen szokatlan módon. Itt R mindig tetszőleges integritástartományt jelöl.

2.26. 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.

Jelölés. Az R feletti polinomok halmazát $R[x]$ jelöli.

2.27. 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 fokszáma $n \geq 0$, akkor az $a_n \in R$ elemet f **főegyütthatójának** hívjuk. Az olyan polinomot, amelynek főegyütthatója 1, **főpolinomnak** nevezzük.

Jelölés. Az f polinom fokszámát $\deg f$ jelöli.

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

$$f + g = (c_0, c_1, \dots), \text{ ahol } c_n = a_n + b_n;$$

$$f \cdot g = (d_0, d_1, \dots), \text{ ahol } d_n = \sum_{i=0}^n a_i \cdot b_{n-i}.$$

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

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

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

2.32. Állítás. Minden $a, b \in R$ esetén

$$(a, 0, 0, \dots) + (b, 0, 0, \dots) = (a + b, 0, 0, \dots);$$

$$(a, 0, 0, \dots) \cdot (b, 0, 0, \dots) = (ab, 0, 0, \dots).$$

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. (Ügy tekintjük, hogy $R \subseteq R[x]$.) A $(0, 1, 0, \dots)$ polinomot pedig x jelöli a továbbiakban.

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

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

Jelölés. A polinomokat ezentúl $a_n x^n + \dots + a_1 x + a_0$ vagy $\sum_{i=0}^n a_i x^i$ 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 $R[y]$.)

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

A test feletti polinomokkal sok tekintetben hasonlóan lehet számolni, mint az egész számokkal. Értelmezhető például az oszthatóság, maradékos osztás, legnagyobb közös osztó, és egyértelmű prímfelbontás is létezik. Ezeket általánosabban, gyűrűkre fogjuk majd kidolgozni, most csak a maradékos osztás tételét bizonyítjuk be polinomokra. Ennek segítségével már az euklideszi algoritmust is végre tudjuk hajtani polinomokkal, és kétszemeretlen lineáris „diofantoszi” egyenleteket is meg tudunk oldani test feletti polinomgyűrűben.

2.35. Tétel. Ha T test, és $f, g \in T[x], g \neq 0$, akkor léteznek olyan egyértelműen meghatározott $q, r \in T[x]$ polinomok, amelyekre $f = gq + r$ és $\deg r < \deg g$.

2.36. Definíció. Adott f és g esetén az előző tételbeli q és r kiszámítását **maradékos osztásnak** nevezzük. Az f polinom az **osztandó**, g az **osztó**, q a **hányados**, és r a **maradék**.

3. „Számelmélet” integritástartományokban

Oszthatóság, asszociáltság, kongruencia, maradékosztály-gyűrű

A következőkben azokat a számelméleti eredményeket általánosítjuk, amelyek minden integritástartományban érvényben maradnak. Mostantól (hacsak mást nem mondunk) R tetszőleges integritástartományt jelöl.

3.1. Definíció. Azt mondjuk, hogy az $a \in R$ elem **osztója** a $b \in R$ elemnek (*b többszöröse* a -nak), ha létezik olyan $c \in R$, amelyre $b = ac$.

Jelölés. Az oszthatósági relációt $|$ jelöli: $a | b \iff \exists c \in R : b = ac$. Ha $a \neq 0$, akkor egyetlen ilyen c létezik (mert R zérusosztómentes), ilyenkor használjuk a $c = \frac{b}{a}$ jelölést. Ha $a \nmid b$, akkor a $\frac{b}{a}$ törtet (egyelőre) nem értelmezzük.

3.2. Tétel. *Tetszőleges $a, b, c \in R$ esetén érvényesek az alábbiak:*

- | | |
|---|--|
| (1) $a a$; | (6) $a 1 \iff a \in R^*$; |
| (2) $(a b \text{ és } b c) \implies a c$; | (7) $0 a \iff a = 0$; |
| (3) $(a b \text{ és } b a) \iff \exists u \in R^* : b = ua$; | (8) $(a b \text{ és } a c) \implies a b \pm c$; |
| (4) $1 a$; | (9) $a b \implies a bc$; |
| (5) $a 0$; | (10) $a b \iff ac bc$, ha $c \neq 0$. |

3.3. Megjegyzés. Amint az első két tulajdonság mutatja, az oszthatósági reláció reflexív és tranzitív, de a (3) tulajdonság szerint általában nem antiszimmetrikus (így nem is részbenrendezés). Ezen próbálunk segíteni az asszociáltság reláció bevezetésével.

3.4. Definíció. Azt mondjuk, hogy az a és b elemek **asszociáltak**, ha $a | b$ és $b | a$.

Jelölés. Az asszociáltság relációt \sim jelöli: $a \sim b \iff a | b$ és $b | a$.

3.5. Tétel. *Az asszociáltság ekvivalenciareláció R -en. Két elem akkor és csak akkor asszociált, ha egymástól csupán egység tényezőben különböznek.*

3.6. Következmény. *Az egész számok gyűrűjében $a \sim b$ akkor és csak akkor teljesül, ha $a = \pm b$. Két T test feletti polinom pontosan akkor asszociált, ha egymástól csupán egy nemnulla konstans szorzóban különböznek.*

3.7. Megjegyzés. Asszociált elemeket nem érdemes (sőt nem is lehet) megkülönböztetni, ha csak az oszthatóságot vizsgáljuk. Ha az oszthatósági relációt az asszociáltsági osztályok halmazán értelmezzük, akkor már nemcsak reflexív és tranzitív, hanem antiszimmetrikus is lesz, azaz részbenrendezés. A kapott $(R/\sim; |)$ részbenrendezett halmaz legkisebb eleme $1/\sim = R^*$, legnagyobb eleme $0/\sim = \{0\}$. Az egész számok gyűrűjében minden asszociáltsági osztály $\{a, -a\}$ alakú, tehát minden osztályban van egy (és csak egy) nemnegatív szám. Ha minden asszociáltsági osztályt a nemnegatív elemével reprezentálunk, akkor az $(\mathbb{N}_0; |)$ részbenrendezett halmazt kapjuk, ami lényegében ugyanaz, mint a $(\mathbb{Z}/\sim; |)$ részbenrendezett halmaz. Test feletti polinomgyűrű esetén minden asszociáltsági osztály (a nullát kivéve) pontosan egy főpolinomot tartalmaz, itt tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal. Egy tetszőleges integritástartományban azonban általában nincsenek kitüntetett elemek az asszociáltsági osztályokban.

3.8. Definíció. Legyen $a, b, m \in R$. Ha $a - b$ osztható m -mel, akkor azt mondjuk, hogy *a kongruens b-vel modulo m*. Az m elemet a kongruencia **modulusának** nevezzük.

Jelölés. A kongruenciát ugyanúgy jelöljük, mint az egész számok gyűrűjében: $a \equiv b \pmod{m} \iff m | a - b$.

3.9. Állítás. *A mod m kongruencia ekvivalenciareláció az R halmazon, továbbá „szabad” kongruenciákat összeadni, kivonni és összeszorozni: tetszőleges $a_1, b_1, a_2, b_2 \in R$ elemekre*

$$\left. \begin{array}{l} a_1 \equiv b_1 \pmod{m} \\ a_2 \equiv b_2 \pmod{m} \end{array} \right\} \implies a_1 + a_2 \equiv b_1 + b_2 \pmod{m}, a_1 - a_2 \equiv b_1 - b_2 \pmod{m}, a_1 \cdot a_2 \equiv b_1 \cdot b_2 \pmod{m}.$$

3.10. Definíció. A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m **maradékosztályoknak** nevezzük.

Jelölés. Az $a \in R$ elemet tartalmazó modulo m maradékosztályt \bar{a} jelöli (ha a modulus világos a szövegkörnyezetből), a maradékosztályok halmazát (vagyis a modulo m kongruenciához tartozó faktorhalmazt) pedig $R/(m)$ jelöli. Tehát $R/(m) = \{\bar{a} : a \in R\}$.

3.11. Definíció. A modulo m maradékosztályok halmazán értelmezzük az összeadást, az additív inverz képzését és a szorzást a következőképpen: tetszőleges $a, b \in R$ esetén legyen $\bar{a} + \bar{b} = \overline{a+b}$, $-\bar{b} = \overline{-b}$, $\bar{a} \cdot \bar{b} = \overline{a \cdot b}$.

3.12. 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 $R/(m)$ kommutatív egységelemes gyűrűt alkot.*

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

4.9. Megjegyzés. Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

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

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

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

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

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

4.15. Következmény. *Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ ($n \geq 1, a_n \neq 0$), akkor f -nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \dots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \dots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontásának**.*

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

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

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

4.18. Következmény. *Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.*

4.19. 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

4.20. 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 $\text{hko}(a_0, \dots, a_n) = 1$.

4.21. 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.*

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

Jelölés. Adott p prímszám esetén az $f = \sum_{i=0}^n a_i \cdot x^i \in \mathbb{Z}[x]$ polinom modulo p redukáltján az $\bar{f} := \sum_{i=0}^n \bar{a}_i \cdot x^i \in \mathbb{Z}_p[x]$ polinomot értjük, ahol \bar{a}_i az a_i egész számot tartalmazó modulo p maradékosztály.

4.23. Lemma. *Tetszőleges $f \in \mathbb{Z}[x]$ polinom akkor és csak akkor primitív, ha minden p prímszámmra $\bar{f} \neq \bar{0} \in \mathbb{Z}_p[x]$.*

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

4.25. 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 $0 < \deg g, \deg h < n$.

4.26. Megjegyzés. A második feltétel azzal ekvivalens, hogy f reducibilis \mathbb{Q} felett. Az első viszont *nem* ekvivalens azzal, hogy f reducibilis \mathbb{Z} felett. Tehát a fenti tételt *nem* fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor irreducibilis \mathbb{Z} felett, ha irreducibilis \mathbb{Q} felett. Ugyanis a 3.40. Definíció értelmében például a $2 \cdot x$ faktorizáció $\mathbb{Z}[x]$ -ben nemtriviális, ezért a $2x$ polinom nem irreducibilis \mathbb{Z} felett (\mathbb{Q} felett viszont irreducibilis, hiszen elsőfokú). Meg lehet mutatni, hogy a \mathbb{Z} feletti irreducibilis polinomok éppen a \mathbb{Q} felett irreducibilis primitív polinomok, valamint a prímszámok (mint konstans polinomok).

4.27. 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. A pontos oszthatóságot $\|$ jelöli: $p \| a \iff p | a$ és $p^2 \nmid a$.

3.50. Megjegyzés. A 3.46. Tétel megfordítása nem igaz: az egész együtthatós polinomok gyűrűje Gauss-gyűrű, de nem főideálgyűrű.

3.51. Tétel. *Legyen R Gauss-gyűrű, és legyen $a, b \in R$ prímfelbontása $a \sim p_1^{\alpha_1} \cdot \dots \cdot p_n^{\alpha_n}$ és $b \sim p_1^{\beta_1} \cdot \dots \cdot p_n^{\beta_n}$. Ekkor teljesülnek az alábbiak:*

- (1) $a \mid b \iff \alpha_i \leq \beta_i \ (i = 1, \dots, n)$;
- (2) $\text{lko}(a, b) \sim p_1^{\min(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\min(\alpha_n, \beta_n)}$;
- (3) $\text{lkkt}(a, b) \sim p_1^{\max(\alpha_1, \beta_1)} \cdot \dots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

Főideálgyűrű faktortestei, véges testek

3.52. Tétel. *Ha R főideálgyűrű, de nem test, akkor az $R/(m)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis.*

3.53. Tétel. *Legyen T test, $f \in T[x]$ irreducibilis polinom, és jelölje n az f polinom fokszámát. Ekkor a $K = T[x]/(f)$ faktorgyűrű test, amelynek minden eleme egyértelműen felírható $a_{n-1}x^{n-1} + \dots + a_1x + a_0$ ($a_{n-1}, \dots, a_0 \in T$) alakban. Ha $T = \mathbb{Z}_p$, akkor a kapott K test elemszáma p^n .*

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

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

4. Test feletti egyhatározatlanú polinomok

Polinomfüggvény, gyök, gyöktényezőz alak, irreducibilitás \mathbb{C} és \mathbb{R} felett

Eddig a polinomokkal mint formális kifejezésekkel számoltunk, nem éltünk azzal a lehetőséggel, hogy x helyébe az alaptest (vagy -gyűrű) elemeit be lehet helyettesíteni. Mostantól viszont a polinomokat függvényeknek (is) tekintjük, hiszen a klasszikus algebra központi kérdése polinomfüggvények zérushelyeinek (azaz a polinom gyökeinek) vizsgálata. Ebben a fejezetben T mindig tetszőleges testet jelöl.

4.1. Definíció. Az $f = a_nx^n + \dots + a_1x + a_0 \in T[x]$ 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 **változó**nak nevezzük (nem pedig határozatlannak).

4.2. Megjegyzés. Függvényeken az összeadást és a szorzást pontonként szoktuk értelmezni. Ez összhangban van a polinomok összeadásával és szorzásával, hiszen minden $f, g \in T[x]$ és $c \in T$ esetén

$$\begin{aligned}(f + g)(c) &= f(c) + g(c); \\ (f \cdot g)(c) &= f(c) \cdot g(c).\end{aligned}$$

Ez azt jelenti, hogy az $f + g$ polinomhoz tartozó polinomfüggvény ugyanaz, mint az f -hez tartozó polinomfüggvény és a g -hez tartozó polinomfüggvény (pontonkénti) összege. Figyeljük meg, hogy a fenti képletben két különböző összeadás szerepel: a kék a polinomok összeadása (azaz a $T[x]$ gyűrűbeli összeadás), a zöld pedig a T testbeli összeadás. Az elmondottak természetesen érvényesek a szorzás műveletére is.

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

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

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

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

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

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

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

Legnagyobb közös osztó

Az oszthatóság és a kongruencia fogalmát és alaptulajdonságait szinte szó szerint lehetett általánosítani tetszőleges integritástartományra. A legnagyobb közös osztó nem mindig létezik, de ha létezik, akkor hasonló tulajdonságokkal rendelkezik, mint az egész számok gyűrűjében, noha a bizonyítások kicsit nehezebbek.

3.13. Definíció. *A $d \in R$ elemet az a és b elemek **legnagyobb közös osztójának** nevezzük, ha kielégíti a következők két feltételt:*

- (1) $d \mid a$ és $d \mid b$;
- (2) $\forall k \in R: (k \mid a \text{ és } k \mid b) \implies k \mid d$.

A $t \in R$ elem **legkisebb közös többszöröse** a -nak és b -nek, ha kielégíti a következő két feltételt:

- (1) $a \mid t$ és $b \mid t$;
- (2) $\forall k \in R: (a \mid k \text{ és } b \mid k) \implies t \mid k$.

Jelölés. Az a és b elemek legnagyobb közös osztóját $\text{lko}(a, b)$ vagy (a, b) , legkisebb közös többszörösüket pedig $\text{lkkt}(a, b)$ vagy $[a, b]$ jelöli.

3.14. Megjegyzés. Ha az a elem osztóinak halmazát D_a jelöli, akkor $\text{lko}(a, b)$ asszociáltságú osztálya nem más, mint a $(D_a \cap D_b / \sim; |)$ részbenrendezett halmaz legnagyobb eleme. Tetszőleges integritástartomány esetén nincs „nagság szerinti” rendezés, csak az oszthatósági relációra támaszkodhatunk. Itt tehát nincs mód kétféleképpen definiálni a legnagyobb közös osztó fogalmát (lásd az 1.14. Megjegyzést a Bevezetés a számelméletbe tárgy előadásvázlatában).

3.15. Tétel. *A legnagyobb közös osztó asszociáltság erejéig egyértelműen meghatározott. Azaz bármely $a, b, d_1, d_2 \in R$ esetén*

- (1) ha d_1 és d_2 is legnagyobb közös osztója a -nak és b -nek, akkor $d_1 \sim d_2$;
- (2) ha d_1 legnagyobb közös osztója a -nak és b -nek, és $d_1 \sim d_2$, akkor d_2 is legnagyobb közös osztója a -nak és b -nek.

Hasonló állítás érvényes a legkisebb közös többszörösre is.

3.16. Megjegyzés. Az előző tétel szerint a legnagyobb közös osztó (és a legkisebb közös többszörös) nem egyértelmű, ezért általában nem azt írjuk, hogy $d = \text{lko}(a, b)$, hanem azt, hogy $d \sim \text{lko}(a, b)$, miként az a következő definícióban is látható. (Az egész számok gyűrűjében megállapodtunk abban, hogy mindig a nemnegatív legnagyobb közös osztót vesszük, test feletti polinomgyűrűben pedig mindig választhatunk főpolinomot legnagyobb közös osztónak.)

3.17. Definíció. Azt mondjuk, hogy az $a, b \in R$ elemek **relatív prímek**, ha $\text{lko}(a, b) \sim 1$.

3.18. Tétel. *Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor minden $a, b, c \in R$ esetén teljesülnek az alábbiak:*

- (1) $\text{lko}(\text{lko}(a, b), c) \sim \text{lko}(a, \text{lko}(b, c))$;
- (2) $\text{lko}(a, b) \sim \text{lko}(b, a)$;
- (3) $\text{lko}(a, a) \sim a$;
- (4) $\text{lko}(0, a) \sim a$;
- (5) $\text{lko}(1, a) \sim 1$;
- (6) $\text{lko}(a, b) \sim a \iff a \mid b$;
- (7) $\text{lko}(a + bc, b) \sim \text{lko}(a, b)$;
- (8) $\text{lko}(a, b) \cdot c \sim \text{lko}(ac, bc)$;
- (9) $\text{lko}(a, b) \approx 0 \implies \text{lko}\left(\frac{a}{\text{lko}(a, b)}, \frac{b}{\text{lko}(a, b)}\right) \sim 1$;
- (10) $\text{lko}(a, b) \sim 1 \implies \text{lko}(a, bc) \sim \text{lko}(a, c)$.

3.19. Következmény. *Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R, \text{lko}(a, b) \sim 1$ esetén teljesülnek az alábbiak:*

- (1) $a \mid bc \iff a \mid c$;
- (2) $(a \mid c \text{ és } b \mid c) \iff ab \mid c$.

3.20. Következmény. *Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R, \text{lko}(a, b) \approx 0$ esetén*

$$a \mid bc \iff \frac{a}{\text{lko}(a, b)} \mid c.$$

3.21. Következmény. *Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor bármely két elemnek létezik legkisebb közös többszöröse is, és minden $a, b \in R$ esetén*

$$\text{lko}(a, b) \cdot \text{lkkt}(a, b) \sim ab.$$

3.22. Megjegyzés. A legnagyobb közös osztó fenti tulajdonságai közül sokat az egész számok körében ki sem mondtunk, mert a prímtenyezés felbontásból triviálisan adódik. Némelyik tulajdonságot még a számelmélet alaptétele előtt láttuk be (hiszen szükségünk volt rájuk az alaptétel bizonyításához), de ezeket is könnyebb volt belátni, mert felhasználhattuk azt, hogy a legnagyobb közös osztó mindig előáll a két elem „lineáris kombinációjaként”. Tetszőleges integritástartományban ez a tulajdonság nem teljesül, és általában egyértelmű prímfelbontás sincs. Sőt, még a legnagyobb közös osztó sem mindig létezik, ezért kezdődik a 3.18. Tétel (és a következményei) ügy, hogy „**Ha** az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, **akkor** ...”.

Euklideszi gyűrűk és főideálgyűrűk

A következőkben speciális integritástartományokat vizsgálunk, amelyekben létezik bármely két elemnek legnagyobb közös osztója. Az egész számok körében a maradékos osztás, illetve az arra épülő euklideszi algoritmus garantálta a legnagyobb közös osztó létezését. Az euklideszi gyűrű fogalma ezt a tulajdonságot általánosítja.

3.23. Definíció. Az R integritástartományt **euklideszi gyűrűnek** nevezzük, ha létezik olyan $\|\cdot\| : R \rightarrow \mathbb{N}_0$, $a \mapsto \|a\|$ leképezés (úgynevezett **euklideszi norma**), amire teljesülnek az alábbiak tetszőleges $a \in R$ és $b \in R \setminus \{0\}$ esetén:

- (1) $\|a\| = 0 \iff a = 0$;
- (2) $a \mid b \implies \|a\| \leq \|b\|$;
- (3) $\exists q, r \in R : a = bq + r$ és $\|r\| < \|b\|$.

3.24. Megjegyzés. A fenti $a = bq + r$ előállítás itt is **maradékos osztásnak** nevezzük (q a **hányados**, r a **maradék**). A maradékos osztás lehetővé teszi az **euklideszi algoritmus** elvégzését (innen az euklideszi gyűrű elnevezés), és így euklideszi gyűrűben bármely két elemnek létezik legnagyobb közös osztója, és az előáll a két elem „lineáris kombinációjaként”. Ezt most itt nem részletezzük, mert hamarosan egy tágabb gyűrűosztályra fogjuk igazolni ezeket az állításokat.

3.25. Tétel. Az egész számok gyűrűjén $\|a\| = |a|$, test feletti polinomgyűrűn $\|f\| = 2^{\deg f}$ ($a 2^{-\infty} = 0$ megállapodással), a Gauss-egészek gyűrűjén pedig $\|z\| = |z|^2$ euklideszi normát definiál. Ezek tehát mind euklideszi gyűrűk.

3.26. Megjegyzés. Az előző tételben furcsának tűnhet a test feletti polinomgyűrűkre megadott euklideszi norma. Az exponenciális függvényre csak azért volt szükség, hogy a nulla polinomnak (de csak annak!) nulla legyen a normája. Ugyanezt elérhetjük másképpen is, például legyen

$$\|f\| = \begin{cases} \deg f + 1, & \text{ha } f \neq 0; \\ 0, & \text{ha } f = 0. \end{cases}$$

3.27. Definíció. A nemüres $I \subseteq R$ részhalmazt **ideálnak** nevezzük, ha bármely $a, b \in I, c \in R$ esetén teljesülnek az alábbiak:

- (1) $a + b \in I$;
- (2) $0 \in I$;
- (3) $-a \in I$;
- (4) $ac \in I$.

3.28. Megjegyzés. A negyedik tulajdonság neve **szívó tulajdonság**: az ideál magába szippantja a szorzatokat. Ez nyilván erősebb a szorzásra való zártásnál, így minden ideál részgyűrű.

3.29. Definíció. Az $a \in R$ elem által generált **főideálon** az $\{ab : b \in R\}$ halmazt értjük.

Jelölés. Az $a \in R$ elem által generált főideált (a) jelöli.

3.30. Megjegyzés. Vegyük észre, hogy (a) éppen a többszöröseinek halmaza, másképpen fogalmazva: (a) nem más, mint az a -val osztható elemek halmaza: $(a) = \{c \in R : a \mid c\}$. Speciálisan $(0) = \{0\}$ és $(1) = R$.

3.31. Állítás. Az a elem által generált főideál valóban ideál, és pedig ez a legszűkebb olyan ideál, ami tartalmazza az a elemet. Vagyis bármely $I \subseteq R$ ideál esetén, ha $a \in I$, akkor $(a) \subseteq I$.

3.32. Tétel. Bármely $a, b \in R$ esetén érvényesek az alábbi ekvivalenciák:

- (1) $a \mid b \iff (a) \supseteq (b)$;
- (2) $a \sim b \iff (a) = (b)$;
- (3) $a \sim 1 \iff (a) = R$.

3.33. Megjegyzés. Ha $I \subseteq R$ ideál, akkor az $a \approx b \iff a - b \in I$ képlettel definiált reláció ekvivalencia, és az ekvivalenciaosztályok halmazán lehet definiálni az összeadást és a szorzást pontosan úgy, mint a maradékosztályokon (lásd 3.11. Definíció). Így kapjuk az $(R/\approx; +, \cdot)$ gyűrűt, amelyet az R gyűrű I ideál szerinti **faktorgyűrűjének** nevezünk, és röviden R/I -vel jelölünk. Ha I főideál, mondjuk $I = (m)$, akkor a \approx reláció éppen a modulo m kongruencia, és ekkor a faktorgyűrű nem más, mint az $R/(m)$ maradékosztály-gyűrű. (Most már látjuk, hogy a maradékosztály-gyűrű jelölésében miért tettük zárójelbe m -et.) Az ideálok és a faktorgyűrűk fontos szerepet játszanak az absztrakt gyűrűelméletben, mi azonban az absztrakt algebrát most csak a számelméleti jelenségek leírására használjuk. A fenti tétel szerint a főideálok minden információt tartalmaznak az oszthatóságról, ezért a továbbiakban csak főideálokkal foglalkozunk. Külön nevet érdemelnek azok az integritástartományok, amelyekben nincs is más ideál.

3.34. Definíció. Az R integritástartományt **főideálgyűrűnek** nevezzük, ha minden ideálja főideál.

3.35. Tétel. Minden euklideszi gyűrű főideálgyűrű.

3.36. Következmény. Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje főideálgyűrű.

3.37. Megjegyzés. A tétel megfordítása nem igaz: létezik olyan főideálgyűrű, amely nem euklideszi. Ilyen például az $\mathbb{Z}[\omega] = \{a + b\omega : a, b \in \mathbb{Z}\}$ gyűrű, ahol $\omega = \frac{1+\sqrt{10}i}{2}$.

3.38. Tétel. Főideálgyűrűben bármely két elemnek létezik legnagyobb közös osztója, és az előáll a két elem „lineáris kombinációjaként”. Formálisan: R főideálgyűrű $\implies \forall a, b \in R \exists x, y \in R : ax + by \sim \text{lko}(a, b)$.

3.39. Tétel. Ha R főideálgyűrű, akkor tetszőlegesen adott $a, b, c \in R \setminus \{0\}$ elemek esetén az $ax + by = c$ egyenlet akkor és csak akkor oldható meg, ha $\text{lko}(a, b) \mid c$. Ha (x_0, y_0) egy megoldás, akkor bármely $t \in R$ esetén az alábbi (x, y) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t elem alkalmas megválasztásával:

$$\begin{aligned} x &= x_0 + \frac{b}{\text{lko}(a, b)} \cdot t; \\ y &= y_0 - \frac{a}{\text{lko}(a, b)} \cdot t. \end{aligned}$$

Irreducibilis és prímelemek, irreducibilis faktorizáció, Gauss-gyűrűk

Irreducibilis és prímelemek bármely integritástartományban (nem csak főideálgyűrűben) definiálhatók, és a korábban tanult tulajdonságok egy része érvényes ilyen általánosságban is.

3.40. Definíció. Azt mondjuk, hogy a $p \in R$ elem **irreducibilis**, ha nem nulla és nem egység, és csak úgy bontható két elem szorzatára, hogy az egyik tényező asszociált p -hez. (Ekkor a másik tényező szükségképpen egység; ilyenkor **triviális faktorizáció**ról beszélünk.) Formálisan:

$$\forall a, b \in R : p = ab \implies (p \sim a \text{ vagy } p \sim b).$$

3.41. Definíció. Azt mondjuk, hogy a $p \in R$ elem **prím**, ha nem nulla és nem egység, és valahányszor osztója egy szorzatnak, mindannyiszor osztója a szorzat egyik tényezőjének. Formálisan:

$$\forall a, b \in R : p \mid ab \implies (p \mid a \text{ vagy } p \mid b).$$

3.42. Állítás. Ha $p \in R$ rendelkezik a prímtulajdonsággal, $n \in \mathbb{N}, a_1, \dots, a_n \in R$ és $p \mid a_1 \cdot \dots \cdot a_n$, akkor $p \mid a_i$ valamely $i \in \{1, \dots, n\}$ -re.

3.43. Tétel. Minden integritástartományban a prímelemek irreducibilisek.

A másik irányú, „irreducibilis \implies prím” implikáció bizonyításánál már kihasználjuk a legnagyobb közös osztók létezését (de mást nem).

3.44. Tétel. Főideálgyűrűben minden irreducibilis elem prím.

A végső cél természetesen a számelmélet alapfeltételének általánosítása integritástartományokra, vagyis egyértelmű irreducibilis faktorizáció létezésének igazolása. Külön nevet is érdemelnek azok az integritástartományok, amelyekben ez megtehető.

3.45. Definíció. **Gauss-gyűrűnek** nevezzük az olyan integritástartományokat, amelyekben minden a nullától és az egységektől különböző elem irreducibilis elemek szorzatára bomlik, és ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelmű. Tehát az R integritástartomány Gauss-gyűrű, ha minden $a \in R$ ($a \neq 0, a \approx 1$) esetén léteznek olyan $p_1, \dots, p_n \in R$ irreducibilis elemek, amelyekre $a = p_1 \cdot \dots \cdot p_n$; továbbá amennyiben $a = q_1 \cdot \dots \cdot q_m$ egy másik irreducibilis faktorizáció, akkor $n = m$, és létezik olyan $\pi \in S_n$, amelyre $p_i \sim q_{i\pi}$ ($i = 1, \dots, n$).

3.46. Tétel. Minden főideálgyűrű Gauss-gyűrű.

3.47. Következmény. Az egész számok gyűrűje, minden test feletti polinomgyűrű, valamint a Gauss-egészek gyűrűje Gauss-gyűrű.

3.48. Megjegyzés. Ha megvizsgáljuk a tétel bizonyítását, megfigyelhetjük, hogy az irreducibilis felbontás létezése azon múlik, hogy nem létezik végtelen leszálló lánc az oszthatóság szerinti „rendezésben”:

$$\nexists a_0, a_1, a_2, \dots \in R : a_{i+1} \mid a_i \text{ és } a_{i+1} \approx a_i \quad (i = 0, 1, 2, \dots). \quad (\exists)$$

Az irreducibilis faktorizáció unicitásának igazolásához pedig csak arra volt szükségünk, hogy az irreducibilis elemek prímtulajdonságúak:

$$\forall p \in R : p \text{ irreducibilis} \implies p \text{ prím}. \quad (!)$$

Ez a két feltétel teljesül Gauss-gyűrűkben, tehát kimondhatjuk, hogy egy R integritástartomány akkor és csak akkor Gauss-gyűrű, ha rendelkezik az (\exists) és $(!)$ tulajdonságokkal.

3.49. Megjegyzés. Minden euklideszi gyűrű főideálgyűrű, ezért a 3.46. Tétel szerint minden euklideszi gyűrű is Gauss-gyűrű. Ha csak ezt az utóbbi állítást szeretnénk volna belátni, akkor könnyebb dolgunk lett volna, mert (\exists) triviálisan teljesül euklideszi gyűrűkben (hiszen $\|a_0\| > \|a_1\| > \|a_2\| > \dots$).