5.28. Tétel. *Ha R euklideszi gyűrű, akkor tetszőlegesen adott $a, b, c \in R \setminus \{0\}$ elemek esetén az $ax + by = c$ egyenlet akkor és csak akkor oldható meg, ha* $\operatorname{lnko}(a, b) \mid c$. *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:*

$$x = x_0 + \frac{b}{\operatorname{lnko}(a,b)} \cdot t;$$
$$y = y_0 - \frac{a}{\operatorname{lnko}(a,b)} \cdot t.$$

Irreducibilis és prímelemek, irreducibilis faktorizáció, Gauss-gyűrűk

Irreducibilis és prímelemek bármely integritástartományban definiálhatók, és a korábban tanult tulajdonságok egy része érvényes ilyen általánosságban is.

5.29. 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:

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

5.30. 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:

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

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

5.32. Tétel. *Minden integritástartományban a prímelemek irreducibilisek.*

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

5.33. Tétel. *Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor R-ben minden irreducibilis elem prím.*

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

5.34. Definíció. ***Gauss-gyűrű***nek 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 $a \in R$ $(a \neq 0, a \nsim 1)$ esetén léteznek olyan $p_1, \ldots, p_n \in R$ irreducibilis elemek, amelyekre $a = p_1 \cdot \ldots \cdot p_n$; továbbá amennyiben $a = q_1 \cdot \ldots \cdot q_m$ egy másik irreducibilis faktorizáció, akkor $n = m$, és létezik olyan $\pi \in S_n$, amelyre $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

5.35. Tétel. *Minden euklideszi gyűrű Gauss-gyűrű.*

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

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

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

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

$$\forall p \in R : p \text{ irreducibilis} \implies p \text{ prím}. \tag{!}$$

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.

5.38. Megjegyzés. A 5.35. Tétel megfordítása nem igaz: az egész együtthatós polinomok gyűrűje Gauss-gyűrű, de nem euklideszi gyűrű.

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

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

KLASSZIKUS ALGEBRA

vázlat az előadáshoz[†]

2014 tavaszi félév

Waldhauser Tamás

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 ***összeg***ét és ***szorzat***át 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) $(u + v) + w = u + (v + w)$;
(2) $u + v = v + u$;
(3) $u + (0, 0) = u$;
(4) $\exists u' \in \mathbb{C} : u + u' = (0, 0)$;
(5) $(u \cdot v) \cdot w = u \cdot (v \cdot w)$;
(6) $u \cdot v = v \cdot u$;
(7) $u \cdot (1, 0) = u$;
(8) $u \neq (0, 0) \implies \exists u^* \in \mathbb{C} : u \cdot u^* = (1, 0)$;
(9) $u \cdot (v + w) = u \cdot v + u \cdot w$;
(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 ***különbség***ét a $v - u = v + (-u)$ képlettel definiálhatjuk, $u \neq (0, 0)$ esetén pedig v és u ***hányados***a $v/u = v \cdot u^{-1}$. 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 kifejezésekként 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 $\mathbb{N} = \{1, 2, 3, \ldots\}$ és $\mathbb{N}_0 = \{0, 1, 2, \ldots\}$. A csillaggal jelölt tételeket nem bizonyítjuk.

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

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

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

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

1.12. 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 számsík***ot, más néven ***Gauss-féle számsík***ot. Az első tengelyt (abszcissza) ***valós tengely***nek, a második tengelyt (ordináta) pedig ***képzetes tengely***nek hívjuk. A valós tengelyen találhatók a valós számok, a képzetes tengelyen pedig az úgynevezett ***tiszta képzetes szám***ok.

1.13. Definíció. A $z = a + bi$ komplex szám ***abszolút érték***én 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. 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.

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

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

Trigonometrikus alak, hatványozás, gyökvonás, egységgyökök

1.16. Definíció. Egy nemnulla z komplex szám ***argumentum***án olyan szöget 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*

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

1.19. Definíció. A nemnulla komplex számok fenti (azaz $|z| \cdot (\cos\arg z + i \sin\arg z)$ alakú) felírását ***trigonometrikus alak***nak 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) $\overline{u} = r(\cos(-\varphi) + i\sin(-\varphi))$;
(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 nemzéró $z = r(\cos\varphi + i\sin\varphi)$ 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 $u^n = z$.

5.17. Definíció. Azt mondjuk, hogy az $a, b \in R$ elemek ***relatív prím***ek, ha $\operatorname{lnko}(a, b) \sim 1$.

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

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

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

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

5.20. Következmény. *Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R, \operatorname{lnko}(a,b) \nsim 0$ esetén*

$$a \mid bc \iff \frac{a}{\operatorname{lnko}(a,b)} \,\Big|\, c.$$

5.21. 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*

$$\operatorname{lnko}(a,b) \cdot \operatorname{lkkt}(a,b) \sim ab.$$

5.22. Megjegyzés. A legnagyobb közös osztó fenti tulajdonságai közül sokat az egész számok körében ki sem mondtunk, mert a prímtényezős 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 5.18. Tétel (és a következményei) úgy, hogy „**Ha** az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, **akkor** ...”.

Euklideszi gyűrűk

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.

5.23. Definíció. Az R integritástartományt ***euklideszi gyűrű***nek nevezzük, ha létezik olyan $\|\cdot\| : R \to \mathbb{N}_0$, $a \mapsto \|a\|$ 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 $\|r\| < \|b\|$.

5.24. Megjegyzés. A fenti $a = bq + r$ előállítást itt is ***maradékos osztás***nak nevezzük (q a ***hányados***, r a ***maradék***). A maradékos osztás lehetővé teszi az ***euklideszi algoritmus*** elvégzését (innen az euklideszi gyűrű elnevezés).

5.25. 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.*

5.26. 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

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

5.27. Tétel. *Euklideszi gyűrűben bármely két elemnek létezik legnagyobb közös osztója, és az előáll a két elem „lineáris kombinációjaként”. Formálisan: ha R euklideszi gyűrű, akkor $\forall a, b \in R\ \exists x, y \in R : ax + by \sim \operatorname{lnko}(a,b)$.*

5.7. 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 nulláét kivéve) pontosan egy főpolinomot tartalmaz, itt tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal. Egy tetszőleges integritástartományban azonban általában nincsenek kitüntetett elemek az asszociáltsági osztályokban.

5.8. 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 ***modulus***ának nevezzük.

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

5.9. 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*

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

5.10. Definíció. A mod m kongruenciához tartozó ekvivalenciaosztályokat modulo m ***maradékosztály***oknak nevezzük.

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

5.11. 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 $\overline{a}+\overline{b} = \overline{a+b}$, $-\overline{b} = \overline{-b}$, $\overline{a}\cdot\overline{b} = \overline{a\cdot b}$.

5.12. 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.*

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.

5.13. Definíció. A $d \in R$ elemet az a és b elemek ***legnagyobb közös osztó***jának nevezzük, ha kielégíti a következő 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 többszörös***e 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 $\operatorname{lnko}(a,b)$ vagy (a,b), legkisebb közös többszörösüket pedig $\operatorname{lkkt}(a,b)$ vagy $[a,b]$ jelöli.

5.14. Megjegyzés. Ha az a elem osztóinak halmazát D_a jelöli, akkor $\operatorname{lnko}(a,b)$ asszociáltsági osztálya nem más, mint a $(D_a \cap D_b/\sim;|)$ részbenrendezett halmaz legnagyobb eleme. Tetszőleges integritástartomány esetén nincs „nagyság 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).

5.15. 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.

5.16. Megjegyzés. Az előző tétel szerint a legnagyobb közös osztó (és a legkisebb közös többszörös) nem egyértelmű, ezért általában nem azt írjuk, hogy $d = \operatorname{lnko}(a,b)$, hanem azt, hogy $d \sim \operatorname{lnko}(a,b)$, 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.)

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

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

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:*

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

Ezzel a jelöléssel $\varepsilon_0 = 1$ *és* $\varepsilon_k = \varepsilon_1^k$ *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:*

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

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 emelve ε-t a hatvány értéke 1 lesz:

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

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

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

(0) $\circ\colon A \times A \to A$, $(x,y) \mapsto x \circ y$;
(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 $a\circ b = b\circ a = e$ teljesül az $a,b \in A$ elemekre, akkor azt mondjuk, hogy a és b egymás ***inverz***e.

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) $\circ\colon A \times A \to A$, $(x,y) \mapsto x \circ y$;
(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) $\forall a \in A\ \exists a^* \in A : a\circ a^* = a^*\circ a = e$.

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 ***gyűrű***nek 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 csoport***jának, nevezzük, és ennek megfelelően beszélhetünk ***additív egységelem***ről és ***additív inverz***ről is. Az $(R; \cdot)$ félcsoportot neve: a gyűrű ***multiplikatív félcsoport***ja.

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 gyűrű***nek nevezzük. Ha pedig nemcsak additív, de ***multiplikatív egységelem*** is létezik (amelyet általában 1 jelöl), akkor ***egységelemes gyűrű***ről 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 ***zérusosztó***k. Ha egy gyűrűben nincsenek zérusosztók (azaz nullától különböző elemek szorzata sosem nulla), akkor ***zérusosztómentes gyűrű***nek nevezzük. A kommutatív, egységelemes, 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 egységelemes gyűrű. Az $a \in R$ elemet ***egység***nek nevezzük, ha létezik ***multiplikatív inverz***e, azaz létezik olyan $a^{-1} \in R$ elem, amelyre $aa^{-1} = a^{-1}a = 1$ teljesül.

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

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

2.17. Definíció. ***Test***nek 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 csoport***jának hívjuk.

2.19. Megjegyzés. A definíció alapján világos, hogy egy legalább kételemű R kommutatív egységelemes 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 ***részgyűrű***je az R gyűrűnek. Hasonlóan definiálható a ***résztest***, ***részcsoport***, ***részfélcsoport*** fogalma is.

Algebrai számok

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

4.20. 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.

4.21. 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.*

4.22. Tétel*. *Létezik transzcendens szám.*

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

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

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

4.26. Következmény. *A gyökmennyiségek algebrai számok.*

4.27. Tétel*. *Van olyan algebrai szám, ami nem gyökmennyiség.*

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

5. Számelmélet integritástartományokban

Oszthatóság, asszociáltság, kongruencia, maradékosztály-gyűrű

A következőkben azokat a számelméleti eredményeket általánosítjuk, amelyek minden integritástartományban érvényben maradnak. Mostantól R mindig tetszőleges integritástartományt jelöl.

5.1. 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 $\mid$ jelöli: $a \mid b \iff \exists c \in R : b = ac$. 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.

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

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

5.3. 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 asszociáltsági reláció bevezetésével.

5.4. Definíció. Azt mondjuk, hogy az a és b elemek ***asszociáltak***, ha $a \mid b$ és $b \mid a$.

Jelölés. Az asszociáltsági relációt $\sim$ jelöli: $a \sim b \iff a \mid b$ és $b \mid a$.

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

5.6. 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.*

4.5. 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.

4.6. 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 amelyikben 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 $\sqsupseteq$ relációt ***lexikografikus rendezés***nek nevezzük.

4.7. Állítás. *A monomok halmazán $\sqsupseteq$ 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.*

4.8. Megjegyzés. Az előző állítás szerint a $\sqsupseteq$ 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 valójában teljesen rendezett halmazzal dolgozhatunk.

4.9. 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 $\hat{M}\sim\hat{N}$.*

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

Szimmetrikus polinomok

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

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

4.12. Definíció. A k-adik n-határozatlanú ***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-határozatlanú elemi szimmetrikus polinomot σ_k jelöli (az alaptest és n értéke általában világos a szövegkörnyezetből), tehát

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

4.13. 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.

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

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

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

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

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

4.18. 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 $g(\alpha_1,\dots,\alpha_n)\in\mathbb{Q}$.*

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

2.21. Állítás. *Minden $m\ge 2$ 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.*

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

2.23. Definíció. ***Gauss-egész***eknek 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 ***polinom***nak 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 ***együttható***inak nevezzük.

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

2.27. Definíció. Az $f=(a_0,a_1,\dots)$ polinom ***fokszám***án a legnagyobb olyan n nemnegatív egész számot értjük, amelyre $a_n\ne 0$. 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 $n\ge 0$, akkor az $a_n\in R$ elemet f ***főegyüttható***jának hívjuk. Az olyan polinomot, amelynek főegyütthatója 1, ***főpolinom***nak 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 ***összeg***ét és ***szorzat***át 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 $\deg(f+g)\le\max(\deg f,\deg g)$ 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 ***polinomgyűrű***nek 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. (Úgy tekintjük, hogy $R\subseteq R[x]$.) A $(0,1,0,\dots)$ polinomot pedig x jelöli a továbbiakban.

2.33. Tétel*. *Minden nemzéró polinom előáll $a_0+a_1x+\dots+a_nx^n$ $(a_n\ne 0)$ 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 $a_n\ne 0$ (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: $R[x]^* = R^*$.*

3. Test feletti egyhatározatlanú polinomok

A továbbiakban T mindig egy tetszőleges testet jelöl, és – hacsak mást nem mondunk – minden polinomot ezen test felett tekintünk.

A polinomok számelmélete

Test feletti polinomokkal sok tekintetben hasonló módon lehet számolni, mint egész számokkal. Most csak nagyon vázlatosan tekintjük át a legfontosabb számelméleti fogalmak és összefüggések megfelelőit a $T[x]$ polinomgyűrűben. A félév végén részletesebben tárgyaljuk mindezeket (majdnem) tetszőleges integritástartományokra (lásd az 5. fejezetet).

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. *Tetszőleges $f, g \in T[x]$ polinomokra*

(3) $f \sim g \iff \exists c \in T \setminus \{0\} : g = cf$

(11) $(f \mid g \text{ és } g \neq 0) \implies \deg f \leq \deg g$.

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 $\deg r < \deg g$.*

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

(1) $d \mid f$ 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 többszörös***e 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": $\exists u, v \in T[x] : \ fu + gv = d$.*

3.8. Megjegyzés. Természetesebbnek tűnhet a legnagyobb közös osztót a legmagasabb fokszámú közös osztóként definiálni. Ha d legnagyobb közös osztója f-nek és g-nek a 3.6 Definíció értelmében és $d \neq 0$, akkor h maximális fokszámú f és g közös osztói között. Valóban, ha k egy közös osztó, akkor $k \mid d$ és így $\deg k \leq \deg d$ (lásd a 3.3 Tételbeli (11) tulajdonságot).

3.9. 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 $\operatorname{lnko}(f, g) \mid h$.*

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

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

3.12. Tétel. *Tetszőleges $f, g, h \in T[x]$ esetén az $fu \equiv h \pmod m$ lineáris kongruencia akkor és csak akkor oldható meg, ha $\operatorname{lnko}(f, m) \mid h$.*

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

3.14. 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 $\overline{f} + \overline{g} = \overline{f + g}$, $-\overline{g} = \overline{-g}$, $\overline{f} \cdot \overline{g} = \overline{f \cdot g}$.

3.15. Állítás. *A fenti műveletek jóldefiniáltak, azaz maradékosztályok összege (addditív 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**).*

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

3.76. 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 (4.17. 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

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

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

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

3.78. 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 $\left(\frac{a^2}{4} + 2\alpha - b\right)x^2 + (a\alpha - c)x + \left(\alpha^2 - d\right)$ másodfokú polinom teljes négyzet, azaz valamely $h \in \mathbb{C}[x]$ legfeljebb elsőfokú polinom négyzete. A $g = x^2 + \frac{a}{2}x + \alpha$ 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.*

4. Viète-formulák, többhatározatlanú polinomok, szimmetrikus polinomok, algebrai számok

Gyökök és együtthatók közötti összefüggés

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

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

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

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

Még formálisabban:

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

A többhatározatlanú polinomok gyűrűje, lexikografikus rendezés

4.3. 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 $k_1, \ldots, k_n \in \mathbb{N}_0$. Az ilyen monomok véges összegeit pedig T feletti ***n-határozatlanú polinom***oknak nevezzük.

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

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

3.63. 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 $\operatorname{lnko}(p,q) = 1$), 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

3.64. Definíció. Az $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ polinom ***derivált***ján 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.

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

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

3.66. 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.)*

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

3.68. 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 $f^{(k)}(\alpha) \neq 0$.*

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

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

3.71. 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

3.72. 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.*

3.73. 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): $u + v, u\varepsilon + v\overline{\varepsilon}, u\overline{\varepsilon} + v\varepsilon$, ahol ε primitív harmadik egységgyök.

3.74. 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).*

3.75. 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 ***diszkriminánsa***nak.

Polinomfüggvények, gyökök, interpoláció

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.

3.17. Definíció. Az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett ***helyettesítési érték***én 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 $f\colon T \to T$, $c \mapsto f(c)$ leképezés. A polinomot és a hozzá tartozó polinomfüggvényt ugyanúgy jelöljük; a szövegkörnyezetből kiderül, hogy mikor melyikről van szó. Ha polinomfüggvényekről van szó, akkor x-et ***változó***nak nevezzük (nem pedig határozatlannak).

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

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

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

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

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

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

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

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

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

3.25. Megjegyzés. Ha a T test véges, akkor találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik (keressünk ilyen példákat!).

3.26. 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.*

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

3.28. Megjegyzés. Előfordulhat, hogy az $n+1$ pontra illesztett Lagrange-féle interpolációs polinom foka kisebb, mint n. Pontosan 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 meggondolni (tegyük meg!), hogy minden olyan polinom, amely a c_i helyeken a d_i értékeket veszi fel, előáll ilyen alakban.

Többszörös gyökök, Horner-módszer

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

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

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 elvégezni:

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

Ezt nevezzük ***Horner-elrendezés***nek. 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 együtthatói 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}	$\cdots$	$\diamondsuit$	$\spadesuit$	$\cdots$	a_0
c	a_n	$a_n \cdot c + a_{n-1}$	$\cdots$	$\clubsuit$	$\clubsuit \cdot c + \spadesuit$	$\cdots$	$f(c)$

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

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

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

3.32. Következmény (iterált Horner-módszer). *Alkalmazzuk a Horner-módszert az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ 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}	$\cdots$	a_2	a_1	a_0
c				$\cdots$			d_0
c				$\cdots$		d_1	
c				$\cdots$	d_2		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\iddots$			
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 $d_n = a_n$):

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

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).

Irreducibilis polinomok, gyöktényezős alak, irreducibilitás $\mathbb{C}$ és $\mathbb{R}$ felett

3.33. 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 faktorizáció***ról beszélünk.) Formálisan:

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

3.34. 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.*

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

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

3.36. Tétel. *Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.*

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

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 $K = \underline{T[x]/(f) \text{ faktorgyűrű olyan}}$ test, amelyben az f polinomnak van gyöke. A K test minden eleme egyértelműen felírható $\underline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0}$ $(a_{n-1}, \ldots, a_0 \in T)$ alakban. Ha $T = \mathbb{Z}_p$, akkor $|K| = p^n$.*

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

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

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

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

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

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

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

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

3.48. 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.*

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

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

3.50. 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:*

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

Irreducibilis polinomok $\mathbb{Q}$ felett

3.51. Definíció. Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot ***primitív polinom***nak nevezzük, ha együtthatói relatív prímek, azaz $\operatorname{lnko}(a_0, \ldots, a_n) = 1$.

3.52. 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.*

3.53. 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 $\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x]$ polinomot értjük, ahol $\overline{a_i}$ az a_i egész számot tartalmazó modulo p maradékosztály.

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

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. 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. Például a $2 \cdot x$ faktorizáció $\mathbb{Z}[x]$-ben nemtriviális, mert $2 \notin \mathbb{Z}[x]^*$ 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).

3.58. Definíció. Azt mondjuk, hogy a p prímszám ***pontos osztó***ja az a egész számnak, ha a osztható p-vel, de p^2-tel már nem.

Jelölés. A pontos oszthatóságot $\parallel$ jelöli: $p \parallel a \iff p \mid a$ és $p^2 \nmid a$.

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

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

3.61. 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 következzék inkább a tétel „tükörképe”.

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