A komplex számok definíciója

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:

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

A műveletek tulajdonságai

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. feladat. Fejezze be az 1.3. Tétel bizonyítását.

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.).

A valós számok beágyazása

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.

Kanonikus alak

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: $i^2 = -1$.

Számolás kanonikus alakban

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:

$$(a + bi) \cdot (c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)\,i;$$
$$\frac{1}{a + bi} = \frac{1}{a + bi} \cdot \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \quad (\text{ha } a + bi \neq 0).$$

2. feladat. Számítsa ki kanonikus alakban: $\dfrac{1 + \sqrt{3}i}{1 + i} = \dfrac{\sqrt{3} + 1}{2} + \dfrac{\sqrt{3} - 1}{2} i$

3. feladat. Számítsa ki kanonikus alakban: $\dfrac{2 + 3i}{1 + 4i} = ?,\quad \dfrac{5 - 7i}{2 - i} = ?$

Konjugált

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

4. feladat. Fejezze be az 1.11. Tétel bizonyítását.

A komplex számsík

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.

Az abszolút érték tulajdonságai

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

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

5. feladat. Fejezze be az 1.15. Tétel bizonyítását.

6. feladat. Számítsa ki az $u\overline{v} + \overline{u}v$, $\frac{\overline{u}}{v} + \frac{u}{\overline{v}}$, $|uv|$, $\left|\frac{u}{v}\right|$ komplex számokat, ahol $u = 2 - 3i$ és $v = 1 + i$.

7. feladat. Ábrázolja a Gauss-féle számsíkon azon z komplex számok halmazát, amelyekre $0 \leq \operatorname{Re}(z + 3) < 1$, illetve $|iz - i| = 1$.

8. feladat. Ábrázolja a Gauss-féle számsíkon azon z komplex számok halmazát, amelyekre $\operatorname{Re}(iz) = 2$, $\operatorname{Im}(\overline{z} - i) > 1$, $|\overline{z} + 2 - i| \leq 2$, illetve $|iz - 1 - i| > 1$.

Argumentum

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.

Trigonometrikus alak

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

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

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

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

Számolás trigonometrikus alakban

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.

9. feladat. Számítsa ki trigonometrikus alakban: $\dfrac{1+\sqrt{3}i}{1+i} = \sqrt{2}\,\mathrm{cis}\,\frac{\pi}{12}$

10. feladat. Számítsa ki trigonometrikus és kanonikus alakban is:
$(3 - \sqrt{3}i)(2 - 2i) = ?$, $\dfrac{-\sqrt{2} + \sqrt{2}i}{\sqrt{3} + i} = ?$

Számolás trigonometrikus alakban

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

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

11. feladat. Számítsa ki trigonometrikus alakban, és adja meg a végeredményt kanonikus alakban is: $(-1+i)^{2422} = \sqrt{2}^{2422}\,\mathrm{cis}\,\frac{\pi}{2} = 2^{1211}i$

12. feladat. Számítsa ki trigonometrikus alakban, és adja meg a végeredményt kanonikus alakban is: $(\sqrt{3}+i)^{1208} = ?$, $(2 + 2\sqrt{3}i)^{605} = ?$

13. feladat. Ábrázolja a Gauss-féle számsíkon azon z komplex számok halmazát, amelyekre $\arg(z + zi) = \pi$.

14. feladat. Ábrázolja a Gauss-féle számsíkon azon z komplex számok halmazát, amelyekre $0 \leq \arg(zi) < \frac{\pi}{3}$, illetve $\frac{\pi}{6} < \arg(\overline{z}) \leq \frac{\pi}{4}$.

Gyökvonás

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 $u^n = z$.

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:

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

15. feladat. Számítsa ki trigonometrikus alakban, és adja meg a végeredményt kanonikus alakban is: $\sqrt[3]{-2+2i} = \ldots$
$\sqrt{2}\,\mathrm{cis}\,\frac{\pi}{4} = 1 + i$, $\sqrt{2}\,\mathrm{cis}\,\frac{11\pi}{12} = -\frac{\sqrt{3}+1}{2} + \frac{\sqrt{3}-1}{2}i$, $\sqrt{2}\,\mathrm{cis}\,\frac{19\pi}{12} = \frac{\sqrt{3}-1}{2} - \frac{\sqrt{3}+1}{2}i$

16. feladat. Számítsa ki trigonometrikus alakban, és adja meg a végeredményt kanonikus alakban is: $\sqrt[3]{i} = ?$, $\sqrt[4]{-1-\sqrt{3}i} = ?$, $\sqrt[6]{64} = ?$, $\sqrt[6]{-27} = ?$

Egységgyökök

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:

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

Ezzel a jelöléssel $\varepsilon_0 = 1$ és $\varepsilon_k = \varepsilon_1^k$ minden $k \in \{0, 1, \ldots, n-1\}$ 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:

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

Primitív egységgyökök

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:

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

17. feladat. Írja és rajzolja fel a 6. egységgyököket, és mindegyikről állapítsa meg, hogy hányadik primitív egységgyök.

18. feladat. Írja és rajzolja fel a 8. és a 12. egységgyököket, és mindegyikről állapítsa meg, hogy hányadik primitív egységgyök.

19. feladat. Egységgyökök-e a következő komplex számok, és ha igen, akkor hányadik primitív egységgyökök? $\frac{1}{2} + \frac{1}{2}i$ (nem), $-\frac{\sqrt{2}}{2} + \frac{\sqrt{2}}{2}i$ (8.), $\mathrm{cis}\,\frac{5\pi}{12}$ (24.)

20. feladat. Egységgyökök-e a következő komplex számok, és ha igen, akkor hányadik primitív egységgyökök? $-\frac{\sqrt{3}}{2} + \frac{1}{2}i$, $-\frac{1}{2} + \frac{\sqrt{2}}{2}i$, $-\frac{1}{2} + \frac{\sqrt{3}}{2}i$, $\mathrm{cis}\,\frac{6\pi}{7}$, $\mathrm{cis}\,\frac{7\pi}{10}$

Primitív egységgyökök

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.

Félcsoportok

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).

Csoportok

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.

	$a \circ b$	e	a^*	$b \circ a^*$
multiplikatív írásmód:	ab	1	a^{-1}	b/a
additív írásmód:	$a + b$	0	$-a$	$b - a$

(Ellen)példák additív csoportokra

Az alábbi H számhalmazok közül melyek alkotnak csoportot az összeadásra nézve?

- $H = \{0\}$: igen (Abel-csoport)
- $H = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}$: igen (Abel-csoport)
- $H = \mathbb{R}^+,\ \mathbb{Q}^+,\ \mathbb{N}$: nem (*csak* félcsoport)
- $H = \{$páros számok$\}$: igen (Abel-csoport)
- $H = \{$páratlan számok$\}$: nem (nem is zárt)
- $H = \{$irracionális számok$\}$: nem (nem is zárt)
- $H = \{$véges tizedestörtek$\}$: igen (Abel-csoport)
- $H = \{a + bi : a, b \in \mathbb{Z}\}$: igen (Abel-csoport)

(Ellen)példák multiplikatív csoportokra

Az alábbi H számhalmazok közül melyek alkotnak csoportot a szorzásra nézve?

- $H = \{1\}$: igen (Abel-csoport)
- $H = \mathbb{C},\ \mathbb{R},\ \mathbb{Q},\ \mathbb{Z}$: nem (*csak* egységelemes félcsoport)
- $H = \mathbb{C} \setminus \{0\},\ \mathbb{R} \setminus \{0\},\ \mathbb{Q} \setminus \{0\}$: igen (Abel-csoport)
- $H = \mathbb{Z} \setminus \{0\}$: nem (*csak* egységelemes félcsoport)
- $H = \mathbb{R}^+,\ \mathbb{Q}^+$: igen (Abel-csoport)
- $H = \mathbb{N}$: nem (*csak* egységelemes félcsoport)
- $H = \{$irracionális számok$\}$: nem (nem is zárt)
- $H = \{$véges tizedestörtek$\} \setminus \{0\}$: nem (*csak* egységelemes félcsoport)
- $H = \{a + bi : a, b \in \mathbb{Z}\}$: nem (*csak* egységelemes félcsoport)

További (ellen)példák csoportokra

- $(\mathbb{R}^{n\times n}; \cdot)$: *csak* egységelemes félcsoport
- $(\{M \in \mathbb{R}^{n\times n} : \det(M) \neq 0\}; \cdot) = \mathrm{GL}_n(\mathbb{R})$: (nemkommutatív) csoport
  neve: általános lineáris csoport
- $(\{A \to A \text{ leképezések}\}; \circ) = T_A$: *csak* egységelemes félcsoport
  neve: (A feletti) transzformációfélcsoport
- $(\{A \to A \text{ bijekciók}\}; \circ) = S_A$: (nemkommutatív) csoport
  neve: (A feletti) szimmetrikus csoport

Gyűrűk

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.

(Ellen)példák gyűrűkre

21. feladat. Az alábbi halmazok közül melyek alkotnak gyűrűt a szokásos összeadás és szorzás műveletével?

- $\mathbb{C},\ \mathbb{R},\ \mathbb{Q}$: gyűrű
- $\mathbb{Z}$: gyűrű
- $\mathbb{R}^+,\ \mathbb{Q}^+,\ \mathbb{N}$: nem gyűrű (nem zárt $-$-ra)
- $\{$páros számok$\}$: gyűrű
- $\{$páratlan számok$\}$: nem gyűrű (nem zárt $+, -$-ra)
- $\{$irracionális számok$\}$: nem gyűrű (nem zárt $+, -, \cdot$-ra)
- $\{$véges tizedestörtek$\}$: gyűrű
- $\mathbb{R}^{n\times n}$: gyűrű
- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$: gyűrű

Számolás gyűrűkben

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

$$a(b - c) = ab - ac, \qquad -(ab) = (-a)b = a(-b).$$

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!

Integritástartományok

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

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

(Ellen)példák integritástartományokra

22. feladat. Az alábbi halmazok közül melyek alkotnak integritástartományt a szokásos összeadás és szorzás műveletével?

- $\mathbb{C},\ \mathbb{R},\ \mathbb{Q}$: integritástartomány
- $\mathbb{Z}$: integritástartomány
- $\mathbb{R}^+,\ \mathbb{Q}^+,\ \mathbb{N}$: nem is gyűrű
- $\{$páros számok$\}$: *csak* kommutatív, zérusosztómentes gyűrű (nem egységelemes)
- $\{$páratlan számok$\}$: nem is gyűrű
- $\{$irracionális számok$\}$: nem is gyűrű
- $\{$véges tizedestörtek$\}$: integritástartomány
- $\mathbb{R}^{n\times n}$: *csak* egységelemes gyűrű (nem kommutatív és nem zérusosztómentes)
- $\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}$: integritástartomány

Egységek

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.

Testek

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. Állítás.
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.

(Ellen)példák testekre

23. feladat. Az alábbi halmazok közül melyek alkotnak testet a szokásos összeadás és szorzás műveletével?

- $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$: test
- $\mathbb{Z}$: *csak* integritástartomány (egységcsoportja: $\{1,-1\}$)
- $\mathbb{R}^+$, $\mathbb{Q}^+$, $\mathbb{N}$: nem is gyűrű
- {páros számok}: nem is integritástartomány
- {páratlan számok}: nem is gyűrű
- {irracionális számok}: nem is gyűrű
- {véges tizedestörtek}: *csak* integritástartomány (mi az egységcsoportja?)
- $\mathbb{R}^{n\times n}$: nem is integritástartomány (egységcsoportja: $\mathrm{GL}_n(\mathbb{R})$)
- $\mathbb{Z}[i] = \{a+bi : a,b \in \mathbb{Z}\}$: integritástartomány (mi az egységcsoportja?)

Gyűrű-e, integritástartomány-e, test-e?

24. feladat. Az alábbi számhalmazok közül melyek alkotnak gyűrűt, integritástartományt, illetve testet a szokásos összeadás és szorzás műveletével?

- $\mathbb{Z}[\sqrt{2}] = \left\{a + b\sqrt{2} : a,b \in \mathbb{Z}\right\}$
- $\mathbb{Q}(\sqrt{2}) = \left\{a + b\sqrt{2} : a,b \in \mathbb{Q}\right\}$
- $\mathbb{Q}(i) = \{a+bi : a,b \in \mathbb{Q}\}$
- $\{a+bi : a,b \in \mathbb{Z}$ és a páros$\}$
- $\{a+bi : a,b \in \mathbb{Z}$ és b páros$\}$
- $\{a+bi : a,b \in \mathbb{Z}$ és a is és b is páros$\}$
- $\{a+bi : a,b \in \mathbb{Z}$ és $a \equiv b \pmod 2\}$
- $\{a+bi : a,b \in \mathbb{Z}$ és $a \equiv b \pmod 3\}$

Ré(s)zgyűrűk és altestek

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.

Példa.
- $(\mathbb{Z};+)$ részcsoportja a $(\mathbb{C};+)$ csoportnak
- $(\mathbb{N};+)$ részfélcsoportja a $(\mathbb{C};+)$ csoportnak
- $(\mathbb{Z};\cdot)$ részfélcsoportja a $(\mathbb{C};\cdot)$ félcsoportnak
- $(\mathbb{Q}^+;\cdot)$ részcsoportja az $(\mathbb{R}^*;\cdot)$ csoportnak
- $(\mathrm{GL}_n(\mathbb{R})\,;\cdot)$ részcsoportja az $(\mathbb{R}^{n\times n};\cdot)$ félcsoportnak
- $(S_A;\circ)$ részcsoportja a $(T_A;\circ)$ félcsoportnak
- $(\mathbb{Z};+,\cdot)$ részgyűrűje a $(\mathbb{C};+,\cdot)$ testnek
- $(\mathbb{Q};+,\cdot)$ részteste a $(\mathbb{C};+,\cdot)$ testnek

Maradékosztály-gyűrűk

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

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

Gauss-egészek

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 polinom definíciója

2.26. Definíció.
Az R integritástartomány feletti *polinom*nak olyan R-beli elemekből képezett $(a_0, a_1, \ldots)$ 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 $f = (a_0, a_1, \ldots)$ polinom *fokszám*án a legnagyobb olyan n nemnegatív egész számot értjük, amelyre $a_n \neq 0$. Ha nincs ilyen n, azaz ha $f = (0,0,\ldots)$, akkor azt mondjuk, hogy f fokszáma $-\infty$.
- Ha f fokszáma kisebb, mint 1 (azaz 0 vagy $-\infty$), akkor f-et *konstans* polinomnak nevezzük.
- Ha f foka $n \geq 0$, akkor az $a_n \in R$ elemet f *főegyüttható*jának hívjuk.
- Az olyan polinomot, amelynek főegyütthatója 1, *főpolinom*nak nevezzük.

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

Műveletek polinomokkal

2.28. Definíció.
Az $f = (a_0, a_1, \ldots)$ és $g = (b_0, b_1, \ldots)$ polinomok *összeg*ét és *szorzat*át az alábbi képletekkel értelmezzük:

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

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

2.29. Állítás.
Tetszőleges $f, g \in R[x]$ polinomokra

$$\deg(f+g) \leq \max(\deg f, \deg g) \quad \textit{és} \quad \deg(fg) = \deg f + \deg g.$$

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

25. feladat. Fejezze be a 2.30. Tétel bizonyítását.

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

De mi az az x?

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

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

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

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

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

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

A polinomgyűrű egységei

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 $a_{n+1} = a_{n+2} = \ldots = 0$.
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: $R[x]^* = R^*$.

Polinom és polinomfüggvény

Az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomhoz természetes módon tartozik egy

$$f\colon T \to T,\ c \mapsto a_n c^n + \dots + a_1 c + a_0$$

függvény (az f-hez tartozó polinomfüggvény). Ez azonban NEM azonos az f polinommal!
A polinom egy formális kifejezés (avagy együtthatók sorozata), míg a polinomfüggvény egy leképezés a T halmazon.

Példa.
Tekintsük $\mathbb{Z}_2$ felett az $f = x$ és $g = x^{2015}$ polinomokat. Ez nyilván két különböző polinom (még a fokszámuk is különbözik), de ugyanaz a polinomfüggvény tartozik hozzájuk:

$$f\colon \{\bar{0}, \bar{1}\} \to \{\bar{0}, \bar{1}\}, \quad \bar{0} \mapsto \bar{0}, \qquad \bar{1} \mapsto \bar{1};$$

$$g\colon \{\bar{0}, \bar{1}\} \to \{\bar{0}, \bar{1}\}, \quad \bar{0} \mapsto \bar{0}^{2015}, \quad \bar{1} \mapsto \bar{1}^{2015}.$$

Oszthatóság

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

3.2. Tétel.
Tetszőleges $f, g, h \in T[x]$ polinomokra érvényesek az alábbiak:

(1) $f \mid f$;
(2) $(f \mid g \text{ és } g \mid h) \implies f \mid h$;
(3) $(f \mid g \text{ és } g \mid f) \iff \exists c \in T^*: g = cf$;
(4) $1 \mid f$;
(5) $f \mid 0$;
(6) $f \mid 1 \iff f \in T^*$;
(7) $0 \mid f \iff f = 0$;
(8) $(f \mid g \text{ és } f \mid h) \implies f \mid g \pm h$;
(9) $f \mid g \implies f \mid gh$;
(10) $f \mid g \iff fh \mid gh$, ha $h \neq 0$;
(11) $f \mid g \implies \deg f \leq \deg g$, ha $g \neq 0$.

Asszociáltság

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

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

3.5. Megjegyzés.
Asszociált polinomokat 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 $(T[x]/\sim; |)$ részbenrendezett halmaz legkisebb eleme $1/\sim = T^*$, legnagyobb eleme $0/\sim = \{0\}$.

Test feletti polinomgyűrű esetén minden asszociáltsági osztály (a nulláét kivéve) pontosan egy főpolinomot tartalmaz, tehát asszociáltság erejéig mindig dolgozhatunk főpolinomokkal.

Maradékos osztás, lnko

3.6. 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 $\deg r < \deg g$.

3.7. 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.

3.8. Megjegyzés.
Természetesebbnek tűnhet a legnagyobb közös osztót a legmagasabb fokszámú közös osztóként definiálni. Ha d legnagyobb közös osztója f-nek és g-nek a 3.7. 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 3.2. Tételbeli (11) tulajdonságot).

Euklideszi algoritmus

3.9. 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”: $\exists u, v \in T[x]:\ fu + gv = d$.

26. feladat. Határozza meg az alábbi két polinom legnagyobb közös osztóját:

$$f = x^4 + 2x^3 + 4x^2 + 2x + 3, \qquad g = x^3 + x^2 + x - 3.$$

$$\begin{aligned} x^4 + 2x^3 + 4x^2 + 2x + 3 &= (x+1) \cdot (x^3 + x^2 + x - 3) &+\ & 2x^2 + 4x + 6 \\ x^3 + x^2 + x - 3 &= (x-1) \cdot (x^2 + 2x + 3) &+\ & 0 \end{aligned}$$

Tehát $\operatorname{lnko}(f, g) \sim x^2 + 2x + 3$.
Hab a tortán:

$$\begin{aligned} f &= (x^2+1)(x^2+2x+3), \quad \text{gyökei: } \pm i,\ -1 \pm \sqrt{2}i \\ g &= (x-1)(x^2+2x+3), \quad \text{gyökei: } 1,\ -1 \pm \sqrt{2}i \end{aligned}$$

Relatív prímség

3.10. Definíció.
Azt mondjuk, hogy az $f, g \in T[x]$ polinomok *relatív prím*ek, ha $\operatorname{lnko}(f, g) \sim 1$.

3.11. Tétel.
Tetszőleges $0 \neq f, g \in T[x]$ polinomok esetén $\frac{f}{\operatorname{lnko}(f,g)}$ és $\frac{g}{\operatorname{lnko}(f,g)}$ relatív prím.

3.12. Tétel.
Tetszőleges $f, g, h \in T[x]$ esetén ha f és g relatív prím, akkor $f \mid gh \iff f \mid h$.

3.13. Tétel.
Tetszőleges $f, g, h \in T[x]$ polinomok esetén ha $\operatorname{lnko}(f, g) \neq 0$, akkor

$$f \mid gh \iff \frac{f}{\operatorname{lnko}(f,g)} \mid h.$$

Diofantoszi egyenlet polinomgyűrűben

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

Ha (u_0, v_0) egy megoldás, akkor bármely $t \in T[x]$ esetén az alábbi (u, v) pár is megoldás, továbbá minden megoldás előáll ilyen alakban a t polinom alkalmas megválasztásával:

$$u = u_0 + \frac{g}{\operatorname{lnko}(f,g)} \cdot t;$$

$$v = v_0 - \frac{f}{\operatorname{lnko}(f,g)} \cdot t.$$

Diofantoszi egyenlet polinomgyűrűben

27. feladat. Oldja meg az $fu + gv = \operatorname{lnko}(f, g)$ egyenletet az $\mathbb{R}[x]$ polinomgyűrűben, ahol

$$f = x^4 + 2x^3 + 4x^2 + 2x + 3, \qquad g = x^3 + x^2 + x - 3.$$

$$\begin{aligned} f &= (x+1) \cdot g &+\ & 2x^2 + 4x + 6 \\ g &= (x-1) \cdot (x^2 + 2x + 3) &+\ & 0 \end{aligned}$$

Tehát $\operatorname{lnko}(f, g) \sim x^2 + 2x + 3$.

Fejezzük ki a legnagyobb közös osztót f és g segítségével:

$$x^2 + 2x + 3 = \frac{1}{2}(f - (x+1) \cdot g) = \frac{1}{2} \cdot f + \left(-\frac{1}{2}x - \frac{1}{2}\right) \cdot g$$

Az egyenlet egy megoldása: $u_0 = \frac{1}{2}$, $\quad v_0 = -\frac{1}{2}x - \frac{1}{2}$.

Diofantoszi egyenlet polinomgyűrűben

28. feladat. Oldja meg az $fu+gv=\overline{1}$ egyenletet az $\mathbb{Z}_5[x]$ polinomgyűrűben, ahol

$$f = x^2+\overline{3}x+\overline{1}, \qquad g = x^3+\overline{2}x^2+\overline{4}x+\overline{2}.$$

$$\begin{aligned}
x^3+\overline{2}x^2+\overline{4}x+\overline{2} &= (x+\overline{4})\cdot(x^2+\overline{3}x+\overline{1}) &+\quad & x+\overline{3}\\
x^2+\overline{3}x+\overline{1} &= x\cdot(x+\overline{3}) &+\quad & \overline{1}\\
x+\overline{3} &= (x+\overline{3})\cdot\overline{1} &+\quad & \overline{0}
\end{aligned}$$

Fejezzük ki $\overline{1}$-et f és g segítségével:

$$\overline{1} = f - x\cdot(x+\overline{3}) = f - x\cdot\left(g-(x+\overline{4})\cdot f\right) = (x^2+\overline{4}x+\overline{1})\cdot f - x\cdot g$$

Az egyenlet egy megoldása: $u_0 = x^2+\overline{4}x+\overline{1}$, $\quad v_0 = -x$.

Diofantoszi egyenlet polinomgyűrűben

29. feladat. Határozza meg f és g legnagyobb közös osztóját, oldja meg az $fu+gv=\operatorname{lnko}(f,g)$ egyenletet, és számítsa ki f és g komplex gyökeit:
$f = x^4+2x^3-x^2-4x-2, \quad g = x^4+x^3-x^2-2x-2.$

30. feladat. Határozza meg f és g legnagyobb közös osztóját, oldja meg az $fu+gv=\operatorname{lnko}(f,g)$ egyenletet, és számítsa ki f és g komplex gyökeit:
$f = x^4+x^3+2x^2+3x-3, \quad g = x^4+x^3+x^2+3x-6.$

31. feladat. Oldja meg az $fu+gv=\operatorname{lnko}(f,g)$ egyenletet $\mathbb{Z}_2[x]$-ben:
$f = x^4+x^3+x^2+\overline{1},\ g = x^3+\overline{1}.$

32. feladat. Oldja meg az $fu+gv=\operatorname{lnko}(f,g)$ egyenletet $\mathbb{Z}_2[x]$-ben:
$f = x^4+x^3+x,\ g = x^4+x^2+x.$

33. feladat. Oldja meg az $fu+gv=\overline{1}$ egyenletet $\mathbb{Z}_7[x]$-ben:
$f = x^4+\overline{6}x^3+\overline{3}x^2+\overline{2}x+\overline{4},\ g = x^2+\overline{6}x+\overline{3}.$

34. feladat. Oldja meg az $fu+gv=\overline{1}$ egyenletet $\mathbb{Z}_5[x]$-ben:
$f = x^3+\overline{4}x,\ g = \overline{2}x^2+\overline{3}x+\overline{2}.$

Kongruenciareláció

3.15. 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 $m \mid f-g$.

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

3.17. Tétel.
Tetszőleges $f,g,h,f_1,g_1,f_2,g_2,m\in T[x]$ esetén érvényesek az alábbiak:

- $\left.\begin{aligned} f_1\equiv g_1 \pmod m\\ f_2\equiv g_2 \pmod m\end{aligned}\right\} \implies \begin{aligned} f_1\pm f_2 \equiv g_1\pm g_2 \pmod m\\ f_1\cdot f_2\equiv g_1\cdot g_2 \pmod m\end{aligned}$
- *Ha $h\neq 0$, akkor $hf\equiv hg \pmod m \iff f\equiv g \left(\operatorname{mod} \frac{m}{\operatorname{lnko}(m,h)}\right)$.*
- *Ha $\operatorname{lnko}(m,h)\sim 1$, akkor $hf\equiv hg \pmod m \iff f\equiv g \pmod m$.*

Lineáris kongruencia

3.18. Tétel.
Tetszőleges $f,g,h\in T[x]$ esetén az $f\cdot u\equiv h \pmod m$ lineáris kongruencia akkor és csak akkor oldható meg, ha $\operatorname{lnko}(f,m)\mid h$. Ha ez teljesül, akkor a megoldások egyetlen modulo $\frac{m}{\operatorname{lnko}(f,m)}$ maradékosztályt alkotnak.

35. feladat. Oldja meg az $f\cdot u\equiv\overline{1} \pmod m$ konruenciát a $\mathbb{Z}_5[x]$ polinomgyűrűben, ahol

$$f = x^2+\overline{3}x+\overline{1}, \qquad m = x^3+\overline{2}x^2+\overline{4}x+\overline{2}.$$

$$\begin{aligned}
f\cdot u\equiv\overline{1} \pmod m \quad &\iff \quad \exists v\in\mathbb{Z}_5[x]:\ fu = \overline{1}+mv\\
&\iff \quad \exists v\in\mathbb{Z}_5[x]:\ fu-mv = \overline{1}
\end{aligned}$$

Egy megoldás: $u_0 = x^2+\overline{4}x+\overline{1}$.

Az általános megoldás: $u\equiv x^2+\overline{4}x+\overline{1} \pmod m$.

Lineáris kongruencia

36. feladat. Oldja meg az $f\cdot u\equiv\overline{1} \pmod m$ konruenciát a $\mathbb{Z}_2[x]$ polinomgyűrűben, ahol

$$f = x^2+\overline{1}, \qquad m = x^3+x^2+\overline{1}.$$

A szokásos módszer:

$$\begin{aligned}
f\cdot u\equiv\overline{1} \pmod m \quad &\iff \quad \exists v\in\mathbb{Z}_2[x]:\ fu = \overline{1}+mv\\
&\iff \quad \exists v\in\mathbb{Z}_2[x]:\ fu-mv = \overline{1}
\end{aligned}$$

$\ldots\ u_0 = x^2+x+\overline{1}$. Tehát a kongruencia megoldása: $u\equiv x^2+x+\overline{1} \pmod m$.

Egy másik gondolatmenet:

$$\begin{aligned}
f\cdot u\equiv\overline{1} \pmod m \quad &\iff \quad (x+\overline{1})^2\cdot u\equiv x^3+x^2 \pmod{x^3+x^2+\overline{1}}\\
&\iff \quad (x+\overline{1})\cdot u\equiv x^2 \pmod{x^3+x^2+\overline{1}}\\
&\iff \quad (x+\overline{1})\cdot u\equiv x^3+\overline{1} \pmod{x^3+x^2+\overline{1}}\\
&\iff \quad u\equiv x^2+x+\overline{1} \pmod{x^3+x^2+\overline{1}}
\end{aligned}$$

Maradékosztály-gyűrű

3.19. Definíció.
A mod 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 $T[x]\,/\,(m) = \left\{\overline{f} : f\in T[x]\right\}$.

3.20. 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

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

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

A maradékosztály-gyűrű egységei

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

37. feladat. Határozza meg az $\overline{f}\in\mathbb{Z}_5[x]\,/\,(m)$ maradékosztály multiplikatív inverzét, ahol

$$f = x^2+\overline{3}x+\overline{1}, \qquad m = x^3+\overline{2}x^2+\overline{4}x+\overline{2}.$$

$$\begin{aligned}
\overline{u}\text{ inverze }\overline{f}\text{-nak} \quad &\iff \quad \overline{f}\cdot\overline{u} = \overline{\overline{1}}\\
&\iff \quad f\cdot u\equiv\overline{1} \pmod m\\
&\iff \quad u\equiv x^2+\overline{4}x+\overline{1} \pmod m
\end{aligned}$$

Tehát $\overline{f}$ multiplikatív inverze: $\overline{x^2+\overline{4}x+\overline{1}}$.

A maradékosztály-gyűrű egységei

38. feladat. Határozza meg az $\overline{f}\in\mathbb{Z}_2[x]\,/\,(m)$ maradékosztály multiplikatív inverzét, ahol

$$f = x^2+1 \qquad m = x^3+x^2+1.$$

$$\begin{aligned}
\overline{u}\text{ inverze }\overline{f}\text{-nak} \quad &\iff \quad \overline{f}\cdot\overline{u} = \overline{1}\\
&\iff \quad f\cdot u\equiv 1 \pmod m\\
&\iff \quad u\equiv x^2+x+1 \pmod m
\end{aligned}$$

Tehát $\overline{f}$ multiplikatív inverze: $\overline{x^2+x+1}$.

39. feladat. Számítsa ki a $\mathbb{Z}_5[x]\,/\,(x^3+x+1)$ gyűrűben $\overline{3x^2+2}$ inverzét.

40. feladat. Számítsa ki a $\mathbb{Z}_5[x]\,/\,(x^3+x^2+x+1)$ gyűrűben $\overline{2x^2+4}$ inverzét.

41. feladat. Számítsa ki a $\mathbb{Z}_2[x]\,/\,(x^3+x^2+1)$ gyűrűben $\overline{x^2}$ inverzét.

42. feladat. Számítsa ki a $\mathbb{Z}_2[x]\,/\,(x^3+x+1)$ gyűrűben $\overline{x}$ inverzét.

Polinomfüggvény

3.23. Definíció.
Az $f = a_nx^n+\cdots+a_1x+a_0\in T[x]$ polinom $c\in T$ helyen vett *helyettesítési érték*én az $f(c) = a_nc^n+\cdots+a_1c+a_0\in T$ elemet értjük.
Az $f\in T[x]$ polinomhoz tartozó *polinomfüggvény* pedig nem más, mint az

$$f:\ T\to T,\ c\mapsto f(c)$$

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).

Polinom vs. polinomfüggvény

Példa.
Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \bar{0} \mapsto \bar{0}^3 = \bar{0},\ \bar{1} \mapsto \bar{1}^3 = \bar{1},\ \bar{2} \mapsto \bar{2}^3 = \bar{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \bar{0} \mapsto \bar{0},\ \bar{1} \mapsto \bar{1},\ \bar{2} \mapsto \bar{2}.$$

Látjuk, hogy f-hez és g-hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha f és g két különböző polinom. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Polinom vs. polinomfüggvény

Általánosabban, ha T egy q-elemű test, akkor

- a $T \to T$ leképezések száma q^q, míg
- T feletti polinomból végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Gyökök és oszthatóság

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

3.25. Tétel (Bézout tétele).
Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.
Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom. Értékeljük ki az $x = \alpha$ helyen a fenti egyenlőség mindkét oldalát:

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r.$$

Tehát

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

□

Közös gyökök

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

Bizonyítás.
Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\begin{aligned}
\alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\
&\iff x - \alpha \mid f \text{ és } x - \alpha \mid g && \text{(Bézout)} \\
&\iff x - \alpha \mid d && \text{(lnko def.)} \\
&\iff d(\alpha) = 0. && \text{(tuozéB)}
\end{aligned}$$

□

Több gyöktényező kiemelése

3.27. Következmény.
Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

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

Bizonyítás.

$$\begin{aligned}
f(\alpha_1) = \ldots = f(\alpha_k) = 0 &\iff x - \alpha_1, \ldots, x - \alpha_k \mid f && \text{(Bézout)} \\
&\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f && \text{(miért?)}
\end{aligned}$$

□

A gyökök száma

3.28. Következmény.
Ha az $0 \neq f \in T[x]$ polinom fokszáma n, akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás.
Legyenek $\alpha_1, \ldots, \alpha_k \in T$ az f polinom összes különböző gyökei. Ekkor

$$(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \implies k \leq \deg f = n.$$

□

3.29. Megjegyzés.
Ha nem *test* feletti polinomokat tekintünk, akkor a gyökök száma meghaladhatja a fokszámot!
Például az $x^2 - \bar{1} \in \mathbb{Z}_{12}[x]$ polinomnak négy gyöke is van!

Polinom vs. polinomfüggvény

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

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

3.32. Megjegyzés.
Ha a T test véges, akkor találhatók különböző T feletti polinomok, amelyekhez ugyanaz a polinomfüggvény tartozik (keressünk végtelen sok ilyen példát!). Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Lagrange-interpoláció

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

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

3.35. 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.

Lagrange-interpoláció

43. feladat. Határozza meg azt a legalacsonyabb fokszámú $f \in \mathbb{R}[x]$ polinomot, amelyre $f(0) = 1,\ f(1) = 2,\ f(2) = 4,\ f(3) = 8$.

$$\begin{aligned}
\Phi_1 &= (x - 1)(x - 2)(x - 3) & \Phi_1(0) &= -6 \\
\Phi_2 &= x(x - 2)(x - 3) & \Phi_2(1) &= 2 \\
\Phi_3 &= x(x - 1)(x - 3) & \Phi_3(2) &= -2 \\
\Phi_4 &= x(x - 1)(x - 2) & \Phi_4(3) &= 6
\end{aligned}$$

$$f = 1 \cdot \frac{\Phi_1}{-6} + 2 \cdot \frac{\Phi_2}{2} + 4 \cdot \frac{\Phi_3}{-2} + 8 \cdot \frac{\Phi_4}{6} = \frac{1}{6}x^3 + \frac{5}{6}x + 1 = \binom{x}{0} + \binom{x}{1} + \binom{x}{2} + \binom{x}{3}$$

44. feladat. Határozza meg azt a legalacsonyabb fokszámú $f \in \mathbb{R}[x]$ polinomot, amelyre $f(1) = 2,\ f(2) = 1,\ f(3) = 4,\ f(4) = 3$.

45. feladat. Határozza meg azt a legalacsonyabb fokszámú $f \in \mathbb{R}[x]$ polinomot, amelyre $f(-1) = 10,\ f(0) = 5,\ f(1) = 3,\ f(2) = 4$.

Horner-elrendezés

3.36. 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.

3.37. Megjegyzés.

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

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ egy n-edfokú polinom és $c \in T$. Ha $f(c)$ értékét szereténk kiszámítani, akkor a szokásos $f(c) = a_n c^n + \cdots + a_1 c + a_0$ 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:

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

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.)

Horner-módszer

A számolást kényelmesebb az alábbi táblázatban elvégezni.

	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.

3.38. 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:

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

46. feladat. Fejezze be a 3.38. Tétel bizonyítását.

Iterált Horner-módszer

3.39. 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}	$\cdots$	a_1	a_0
c			$\cdots$		d_0
c			$\cdots$	d_1	
$\vdots$	$\vdots$	$\vdots$	$\iddots$		
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:

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

Ha $d_0 = \cdots = d_{k-1} = 0$ és $d_k \neq 0$, akkor a $c \in T$ elem k-szoros gyöke f-nek.

(Iterált) Horner-módszer

47. feladat. Hányszoros gyöke $c = 1$ az $f = x^3 - 4x^2 + 5x - 2$ polinomnak?

Kétszeres: $f = (x-1)^2 (x-2)$.

48. feladat. Hányszoros gyöke $c = 2$ az $f = x^5 - 5x^4 + 7x^3 - 2x^2 + 4x - 8$ polinomnak?

49. feladat. Hányszoros gyöke $c = -2$ az $f = x^5 + 7x^4 + 16x^3 + 8x^2 - 16x - 16$ polinomnak?

50. feladat. Számítsa ki az $f = x^4 + 4ix^3 - 7x^2 - 6ix - 4$ polinom komplex gyökeit az $y = x + i$ határozatlanra való áttérés segítségével.

$f \rightsquigarrow y^4 - y^2 - 6$, ennek gyökei $\pm\sqrt{3}, \pm\sqrt{2}i$, tehát f gyökei:

$$\sqrt{3} - i, \quad -\sqrt{3} - i, \quad (\sqrt{2} - 1)i, \quad (-\sqrt{2} - 1)i.$$

51. feladat. Számítsa ki az $f = x^4 - 4ix^3 - 3x^2 - 2ix - 12$ polinom komplex gyökeit az $y = x - i$ határozatlanra való áttérés segítségével.

52. feladat. Számítsa ki az $f = x^4 + 8ix^3 - 26x^2 - 40ix + 21$ polinom komplex gyökeit az $y = x + 2i$ határozatlanra való áttérés segítségével.

Irreducibilitás

3.40. Definíció.

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

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

3.41. 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.

Bizonyítás.

- triviális felbontás: $p = f \cdot g$, ahol $\deg f = 0, \deg g = \deg p$ (vagy fordítva)
- nemtriviális felbontás: $p = f \cdot g$, ahol $1 \leq \deg f, \deg g < \deg p$

□

Egyértelmű irreducibilis faktorizáció

3.42. Definíció.

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

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

3.43. Tétel.

Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

3.44. 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 minden $i = 1, \ldots, n$ esetén

$$p_i \sim q_{\pi(i)}.$$

Irreducibilitás vs. gyökök

3.45. Állítás.

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f = g \cdot h$, akkor $\deg g + \deg h = 1$, és így

$$\deg g = 1, \deg h = 0 \quad \text{vagy} \quad \deg g = 0, \deg h = 1.$$

Mindkét esetben triviális a felbontás. □

3.46. Tétel.

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

Bizonyítás.

Ha α gyöke f-nek, akkor $f = (x - \alpha)(\cdots)$ nemtriviális felbontás. □

Irreducibilitás vs. gyökök

3.47. Tétel.

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

Bizonyítás.

Ha $f = g \cdot h$, akkor $\deg g + \deg h \in \{2, 3\}$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg g$	$\deg h$
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója. Egy elsőfokú polinom asszociáltság erejéig mindig $x - \alpha$ alakban írható*, ez pedig akkor és csak akkor osztja f-et, ha α gyöke f-nek. □

*$ax + b = a\left(x + \frac{b}{a}\right) \sim x + \frac{b}{a} = x - \left(-\frac{b}{a}\right) = x - \alpha$

Irreducibilitás vs. gyökök

Összefoglalva:

Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

implikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!

A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Példa.

Az $f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ polinomnak nincs valós gyöke, mégsem irreducibilis $\mathbb{R}$ felett:

$$f = (x^2 + 1)(x^2 + 1).$$

Irreducibilis faktorizáció

53. feladat. Bontsa irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^6 + 3x^4 - x^3 + 2x^2 + x - 1 \in \mathbb{Z}_5[x].$$

Mivel az alaptestnek csak öt eleme van, egyenként kipróbálhatjuk, hogy gyöke-e valamelyik az f polinomnak.

Amelyik igen, annál a Horner-módszerrel megállapítjuk a multiplicitást, és leválasztjuk a gyöktényezőket:

$$f = (x-1)^2 (x-3)(x-4)(x^2+4x+2).$$

Az x^2+4x+2 polinomnak nincs gyöke (ha lenne, megtaláltuk volna), és csak másodfokú, ezért irreducibilis.

(Ha negyed- vagy magasabb fokú polinom marad a gyöktényezők kiemelése után, akkor valami trükkre van szükség …)

Irreducibilis faktorizáció

54. feladat. Bontsa irreducibilis tényezők szorzatára az $x^5+x^4+2x^3+x^2+1 \in \mathbb{Z}_3[x]$ polinomot.

55. feladat. Bontsa irreducibilis tényezők szorzatára az $x^5+x^4+2x^3+2x+1 \in \mathbb{Z}_3[x]$ polinomot.

56. feladat. Bontsa irreducibilis tényezők szorzatára az $x^5+x^4+2x^3+1 \in \mathbb{Z}_5[x]$ polinomot.

57. feladat. Bontsa irreducibilis tényezők szorzatára az $x^5+x^3+4x^2+4 \in \mathbb{Z}_5[x]$ polinomot.

58. feladat. Határozza meg $\mathbb{Z}_2$ felett az összes legfeljebb harmadfokú irreducibilis polinomot.

59. feladat. Bontsa irreducibilis tényezők szorzatára az x^4+x+1 és x^4+x^2+1 polinomokat $\mathbb{Z}_2$ felett.

Irreducibilitás különböző testek felett

Példa.
Az $f = x^2+1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik: $x^2+1 = (x+i)(x-i)$.

Példa.
Az $f = x^2-2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik: $x^2-2 = (x-\sqrt{2})(x+\sqrt{2})$.

(És persze $\mathbb{C}[x]$-ben is felbomlik.)

Általában, minél nagyobb az alaptest, annál „több esélye” van egy polinomnak felbomlani.

Ha T részteste K-nak és $f \in T[x]$, akkor

$$f \text{ irreducibilis } K \text{ felett } \overset{\Rightarrow}{\not\Leftarrow} \; f \text{ irreducibilis } T \text{ felett.}$$

Az algebra alaptétele, irreducibilis polinomok $\mathbb{C}$ felett

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

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

Bizonyítás.
Tudjuk, hogy az elsőfokúak bármely test felett irreducibilisek.

Ha $f \in \mathbb{C}[x]$ legalább másodfokú, akkor az algebra alaptétele szerint van valódi (pl. elsőfokú) osztója. □

Irreducibilis faktorizáció a komplex számtest felett

3.50. 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 felbontásának.

Bizonyítás.
Mivel $\mathbb{C}$ test, minden $\mathbb{C}$ feletti legalább elsőfokú polinom irreducibilisek, azaz elsőfokúak szorzatára bomlik. Ezek az elsőfokúak asszociáltság erejéig $x-\alpha$ alakúak. Tehát $f \in \mathbb{C}[x]$ irreducibilis faktorizációja így fest:

$$f \sim (x-\alpha_1) \cdots (x-\alpha_n).$$

Világos, hogy ekkor f gyökei éppen az $\alpha_1, \ldots, \alpha_n$ komplex számok. □

Oszthatóság vs. gyökök

3.51. 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.

Bizonyítás.
Az f polinom gyökei „egy az egybe” megfelelnek f prímosztóinak, továbbá az α gyök multiplicitása éppen az $x-\alpha$ prímtényező kitevője f prímfelbontásában.

A prímfelbontásból pedig ugyanúgy lehet az oszthatóságot kiolvasni, mint az egész számok körében. □

Valós polinom komplex gyökei

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

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

Bizonyítás.
Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \\ &= \overline{a_n z^n + \cdots + a_1 z + a_0} \\ &= \overline{f(z)} \end{aligned}$$

Tehát $f(z) = 0 \implies f(\overline{z}) = \overline{f(z)} = \overline{0} = 0$. □

Irreducibilis polinomok a valós számtest felett

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

Bizonyítás.
Tudjuk, hogy a legfeljebb másodfokú polinomok között pontosan a fentiek az irreducibilisek. Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett.
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek, és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$. Ezért az $(x-\alpha)(x-\overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben. Node
$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\,\mathrm{Re}\,\alpha \cdot x + |\alpha|^2 \in \mathbb{R}[x],$$
így f-nek $(x-\alpha)(x-\overline{\alpha})$ valódi osztója $\mathbb{R}[x]$-ben (miért?). □

Irreducibilis faktorizáció a valós számtest felett

60. feladat. Határozza meg az $f = x^6 - 27$ polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

A polinom komplex gyökei: $\sqrt{3}$, $-\sqrt{3}$, α, $\overline{\alpha}$, β, $\overline{\beta}$, ahol

$$\alpha = \sqrt{3} \cdot \left(\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) = \frac{\sqrt{3}}{2} + \frac{3}{2} i, \qquad \beta = \sqrt{3} \cdot \left(-\frac{1}{2} + \frac{\sqrt{3}}{2} i\right) = -\frac{\sqrt{3}}{2} + \frac{3}{2} i$$

A $\mathbb{C}$ feletti felbontás (azaz a gyöktényezős alak):

$$f = (x-\sqrt{3})(x+\sqrt{3})(x-\alpha)(x-\overline{\alpha})(x-\beta)(x-\overline{\beta}).$$

Az $\mathbb{R}$ feletti felbontás:

$$\begin{aligned} f &= (x-\sqrt{3})(x+\sqrt{3})\left(x^2 - 2\,\mathrm{Re}\,\alpha \cdot x + |\alpha|^2\right)\left(x^2 - 2\,\mathrm{Re}\,\beta \cdot x + |\beta|^2\right) \\ &= (x-\sqrt{3})(x+\sqrt{3})(x^2 - \sqrt{3}x + 3)(x^2 + \sqrt{3}x + 3). \end{aligned}$$

A $\mathbb{Q}$ feletti felbontás:
$$f = (x^2-3)(x^4+3x^2+9).$$

Irreducibilis faktorizáció a valós számtest felett

61. feladat. Határozza meg az $f = x^6 + 1$ polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

62. feladat. Határozza meg az $f = x^8 - 16$ polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

63. feladat. Határozza meg az $f = x^4 - x^2 + 1$ polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

64. feladat. Határozza meg az $f = x^6 + 7x^3 - 8$ polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

65. feladat. Határozza meg az $f = x^5 + x^4 + x^3 + x^2 + x + 1$ polinom irreducibilis felbontását $\mathbb{C}$ és $\mathbb{R}$ felett.

Primitív polinomok

3.54. 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 $\operatorname{lnko}(a_0, \ldots, a_n) = 1$.

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

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

Példa.

$$f = \tfrac{15}{7}x^2 + \tfrac{45}{4}x + \tfrac{5}{2} = \tfrac{60}{28}x^2 + \tfrac{315}{28}x + \tfrac{70}{28}$$

$$= \tfrac{1}{28} \cdot (60x^2 + 315x + 70) = \underbrace{\tfrac{5}{28}}_{r} \cdot \underbrace{(12x^2 + 63x + 14)}_{f^*}$$

Primitív polinomok

Bizonyítás.
Legyen $f = \sum_{i=0}^{n} \frac{p_i}{q_i} \cdot x^i$, ahol $p_i, q_i \in \mathbb{Z}$, $\operatorname{lnko}(p_i, q_i) = 1 \;\; (i = 0, \ldots, n)$.

$$f = \tfrac{1}{Q} \cdot \sum_{i=0}^{n} \underbrace{\tfrac{Q}{q_i} p_i}_{b_i \in \mathbb{Z}} \cdot x^i, \qquad \text{ahol } Q = \operatorname{lkkt}(q_0, \ldots, q_n)$$

$$f = \tfrac{d}{Q} \cdot \sum_{i=0}^{n} \tfrac{b_i}{d} \cdot x^i, \qquad \text{ahol } d = \operatorname{lnko}(b_0, \ldots, b_n)$$

Tehát $f = r \cdot f^*$, ahol $r = \frac{d}{Q} \in \mathbb{Q}$ és $f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x]$ primitív polinom. □

Redukció modulo p

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.
A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x] : \; \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \nmid a_n$, akkor (és csak akkor!) $\overline{a_n} \neq \overline{0}$, és így $\deg \overline{f} = \deg f = n$.

Példa.
Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$. Ekkor

$$\overline{f} = \overline{10}x^3 + \overline{7}x^2 + \overline{25}x + \overline{-2} = \overline{0}x^3 + \overline{2}x^2 + \overline{0}x + \overline{3} = \overline{2}x^2 + \overline{3} \in \mathbb{Z}_5[x].$$

Egy trükk

Példa.
Felbontható-e az $f = x^4 + 2x^3 + 6x^2 + 7x + 5 \in \mathbb{Z}[x]$ polinom kisebb fokszámú egész együtthatós polinomok szorzatára?

Tegyük fel, hogy igen:

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \;\text{ és } 0 < \deg g, \deg h < 4.$$

Redukáljuk modulo 2: $\overline{f} = \overline{g} \cdot \overline{h}$, ahol $\overline{g} \cdot \overline{h} \in \mathbb{Z}_2[x]$ és $0 < \deg \overline{g}, \deg \overline{h} < 4$.

Node $\overline{f} = x^4 + x + 1$ irreducibilis $\mathbb{Z}_2[x]$-ben, mert nincs neki se első- se másodfokú irreducibilis osztója. ↯

Tehát f nem bontható fel kisebb fokú egész együtthatós polinomok szorzatára.
Nemsokára bebizonyítjuk, hogy ekkor f nem bontható fel kisebb fokú racionális együtthatós polinomok szorzatára sem, tehát irreducibilis $\mathbb{Q}$ felett.

Gauss-lemma

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

Bizonyítás.
$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját, és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.
$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

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

Bizonyítás.
Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f és g primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$ és $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Tehát $\mathbb{Z}_p[x]$-ben $\overline{f}$ és $\overline{g}$ zérusosztók, ez pedig lehetetlen, mivel $\mathbb{Z}_p$ test. □

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

3.59. 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* $0 < \deg g, \deg h < n$.

3.60. 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).

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

3.59. Tétel.
$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ *esetén* (1) $\Longleftrightarrow$ (2)

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

Bizonyítás.
Az világos, hogy (1) $\Longrightarrow$ (2).
Tegyük fel, hogy (2) teljesül, és legyen

$$g = r \cdot g^*, \;\; h = s \cdot h^*, \;\text{ ahol } r, s \in \mathbb{Q} \text{ és } g^*, h^* \in \mathbb{Z}[x] \text{ primitív polinomok.}$$

Legyen $rs = \frac{p}{q}$, ahol $\operatorname{lnko}(p, q) = 1$ és $q > 0$. Ekkor

$$f = g \cdot h = rg^* \cdot sh^* = rs \cdot g^* h^* = \frac{p}{q} \cdot g^* h^*.$$

Meg fogjuk mutatni, hogy $q = 1$.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \;\Longrightarrow\; q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned}
&\forall i \in \{0, \ldots, n\} : \; q \mid p \cdot a_i \\
\Longrightarrow \;& \forall i \in \{0, \ldots, n\} : \; q \mid a_i && (q \perp p) \\
\Longrightarrow \;& q \mid \operatorname{lnko}(a_0, \ldots, a_n) && (\text{lnko def.}) \\
\Longrightarrow \;& q = 1
\end{aligned}$$

Tehát

$$f = \frac{p}{q} \cdot g^* h^* = \underbrace{pg^*}_{\in \mathbb{Z}[x]} \cdot \underbrace{h^*}_{\in \mathbb{Z}[x]}.$$

A fenti felbontásban a fokszámok ugyanazok, mint az eredeti $f = gh$ felbontásban, hiszen $pg^* \sim g$ és $h^* \sim h$. □

Pontos oszthatóság

3.61. 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 $\|$ jelöli: $p \| a \iff p \mid a$ és $p^2 \nmid a$.

Példa.

$$3 \| 12 \quad \text{de} \quad 2 \not\| 12$$

Schönemann–Eisenstein

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

$$p \nmid a_n,\, p \mid a_{n-1}, \ldots, p \mid a_1,\, p \| a_0,$$

akkor f irreducibilis a racionális számok teste felett.

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

Bizonyítás.
$x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak az elsőfokúak,
- $\mathbb{R}$ felett csak az elsőfokúak és bizonyos másodfokúak

irreducibilisek.
Még szerencse, hogy a racionális számok testének már nincs valódi részteste!

VIZSGÁN KÉRDEZNI FOGOM!

3.64. 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”.

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

Racionális gyökök

3.66. Tétel (Rolle tétele).
Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ 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.

Természetesen a fenti nyíl nem fordítható meg: $q \mid a_n$ és $p \mid a_0$ nem garantálja, hogy $\frac{p}{q}$ gyöke f-nek.

A Rolle-tételben „az a jó”, hogy egy véges halmazt ad meg, amelyben az összes racionális gyököt megtalálhatjuk (ha van egyáltalán racionális gyök).

Racionális gyökök

Bizonyítás.
Tegyük fel, hogy $\frac{p}{q}$ gyöke f-nek ($\operatorname{lnko}(p,q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1}}_{p \mid} + \underbrace{a_0 q^n}_{p \mid} \implies p \mid a_0$$

Hasonlóan:

$$q \mid a_n \Longleftarrow \underbrace{a_n p^n}_{q \mid} \Longleftarrow + \underbrace{a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1} + a_0 q^n}_{q \mid} = 0$$

□

Irreducibilis felbontás $\mathbb{Q}$ felett

66. feladat. Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az alábbi polinomot:

$$f = 2x^7 + 5x^6 + 4x^5 + 13x^4 + 54x^3 + 84x^2 + 54x + 12.$$

Racionális gyök csak $\pm1, \pm2, \pm3, \pm4, \pm6, \pm12, \pm\frac{1}{2}, \pm\frac{3}{2}$ lehet.
Ezek közül -1 és $-\frac{1}{2}$ valóban gyök. Horner-módszerrel leválasztva a gyöktényezőket azt kapjuk, hogy

$$f = \left(x + \frac{1}{2}\right)(x+1)^2 (2x^4 + 12x + 24) = (2x+1)(x+1)^2 (x^4 + 6x + 12).$$

A kék polinom irreducibilis $\mathbb{Q}$ felett: Schönemann-Eisenstein ($p = 3$).

67. feladat. Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az alábbi polinomot:

$$f = 3x^{100} - 10x^{50} + 100x - 50.$$

A polinom irreducibilis $\mathbb{Q}$ felett: Schönemann-Eisenstein ($p = 2$).

Irreducibilis felbontás $\mathbb{Q}$ felett

68. feladat. Bontsa $\mathbb{Q}$ felett irreducibilis polinomok szorzatára az alábbi polinomot:

$$f = 4x^4 - 7x^2 - 5x - 1.$$

Racionális gyök csak $\pm1, \pm\frac{1}{2}, \pm\frac{1}{4}$ lehet. Ezek közül $-\frac{1}{2}$ kétszeres gyök:

$$f = \left(x + \frac{1}{2}\right)^2 (4x^2 - 4x - 4) = (2x+1)^2 (x^2 - x - 1).$$

A kék polinom irreducibilis $\mathbb{Q}$ felett: csak másodfokú, és nincs racionális gyöke.

69. feladat. Adja meg $3x^6 + 2x^5 - 7x^4 + 2 \in \mathbb{Q}[x]$ irr. felbontását.

70. feladat. Adja meg $2x^6 - x^5 + 15x + 12 \in \mathbb{Q}[x]$ irr. felbontását.

71. feladat. Adja meg $x^5 - 2x^3 + x^2 + x - 1 \in \mathbb{Q}[x]$ irr. felbontását.

72. feladat. Adja meg $x^5 - x^4 - x^3 + 2x^2 - 1 \in \mathbb{Q}[x]$ irr. felbontását.

73. feladat. Adja meg $x^6 - x^5 - 2x^3 - 3x^2 - x - 2 \in \mathbb{Q}[x]$ irr. felbontását.

74. feladat. Adja meg $x^6 + x^5 + 2x^4 + 4x^3 - 4x^2 + 4x - 8 \in \mathbb{Q}[x]$ irr. felbontását.

Kronecker módszere

Példa.
Irreducibilis-e az $f = x^4 - 4x^3 + 7x^2 - 6x + 3 \in \mathbb{Q}[x]$ polinom?

Tfh. $f = g \cdot h$, ahol $g, h \in \mathbb{Z}[x]$ és $0 < \deg g \overset{\text{ÁMN}}{\leq} \deg h < n$.

Ekkor $\deg g \leq 2$, és minden $k \in \mathbb{Z}$ esetén $g(k) \mid f(k)$. Például

$$a := g(0) \mid f(0) = 3, \quad b := g(1) \mid f(1) = 1, \quad c := g(2) \mid f(2) = 3.$$

Tehát az (a, b, c) számhármasra 32 lehetőség van:

$$(a, b, c) \in \{-3, -1, 1, 3\} \times \{-1, 1\} \times \{-3, -1, 1, 3\}.$$

Mind a 32 esetben egyértelműen meg tudjuk határozni a g polinomot Lagrange-interpolációval.

Ha valamelyik osztja f-et, akkor kapunk egy nemtriviális felbontást;
ha egyik se osztja f-et, akkor f irreducibilis.

$$(a, b, c) = (1, 1, 3) \rightsquigarrow g = x^2 - x + 1 \rightsquigarrow f = (x^2 - x + 1)(x^2 - 3x + 3)$$

Polinomgyűrű faktorteste

3.67. Tétel.
A $T[x]\,/\,(m)$ maradékosztály-gyűrű akkor és csak akkor test, ha m irreducibilis T felett.

Bizonyítás.
Tudjuk, hogy

1. $T[x]\,/\,(m)$ kommutatív egységelemes gyűrű (3.21. Áll.);
2. $T[x]\,/\,(m)$ egységcsoportja: $\{\overline{f} : f \perp m\}$ (3.22. Tétel);
3. tehát $T[x]\,/\,(m)$ akkor és csak akkor test, ha legalább kételemű, és

$$(*) \qquad \forall f \in T[x] :\ f \perp m \iff m \nmid f \qquad (2.19. \text{ Áll.}).$$

- Ha m irreducibilis, akkor $(*)$ teljesül, mert $\operatorname{lnko}(f, m)$ csak 1 vagy m lehet.
- Ha $m = f \cdot g$ egy nemtriviális felbontás, akkor $(*)$-ra f egy ellenpélda.
- Ha $m = 0$, akkor $(*)$-ra $f = x$ egy ellenpélda. (Ekkor $T[x]/(m) \cong T[x]$.)
- Ha $m \in T \setminus \{0\}$, akkor (és csak akkor) $T[x]\,/\,(m)$ egyelemű, tehát nem test.

□

Polinomgyűrű faktorteste

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

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

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

Bizonyítás.
A maradékos osztás tétele (3.6. Tétel) szerint

$$\forall f \in T[x] \ \exists! r \in T[x]: \ f \equiv r \pmod{m} \text{ és } \deg r \leq n-1.$$

Ezért $T[x] / (m)$ minden eleme egyértelműen felírható

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

alakban.
Ha $T = \mathbb{Z}_p$, akkor p választási lehetőségünk van minden a_i-re ezért összesen p^n-féleképp tudjuk az $a_{n-1}, \ldots, a_1, a_0$ (n db) együtthatókat megválasztani.

Polinomgyűrű faktorteste

Bizonyítás (folyt.)
Tetszőleges $a, b \in T$ esetén $\overline{a} = \overline{b} \iff a = b$, továbbá

$$\overline{a+b} = \overline{a} + \overline{b} \quad \text{és} \quad \overline{a \cdot b} = \overline{a} \cdot \overline{b}.$$

Ez azt jelenti, hogy az $\{\overline{a}: a \in T\}$ egy T-vel izomorf résztest K-ban. Ha ezt azonosítjuk magával T-vel (azaz $\overline{a}$-t azonosítjuk a-val minden $a \in T$-re), akkor T részteste lesz K-nak (azaz K egy **ki**bővítése T-nek).

Legyen $\alpha = \overline{x}$, így egy $\overline{f} \in K$ elem „kanonikus alakja”:

$$\begin{aligned} \overline{f} &= \overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} \\ &= \overline{a_0} + \overline{a_1}\,\overline{x} + \cdots + \overline{a_{n-1}}\,\overline{x}^{n-1} \\ &= a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T). \end{aligned}$$

Hasonló számolás mutatja, hogy

$$m(\alpha) = m(\overline{x}) = \overline{m(x)} = \overline{0},$$

hiszen $m \equiv 0 \pmod{m}$. Tehát $\alpha \in K$ valóban gyöke m-nek. □

ÖRÖMHÍR!

Minden polinomnak van gyöke! Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz $\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$. Tehát a számolási szabály:

$$\alpha^n = -b_{n-1}\alpha^{n-1} - \cdots - b_1\alpha - b_0.$$

(És ha m nem irreducibilis?)

A komplex számtest újratöltve

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

$$K = \{\overline{a_0 + a_1x} \mid a_0, a_1 \in \mathbb{R}\}.$$

Vegyük észre, hogy $\overline{x}^2 = \overline{-1}$, hiszen $x^2 \equiv -1 \pmod{x^2+1}$.

Írjunk $\overline{x}$ helyett i betűt, és hagyjuk el a vonásokat a konstansokról.

Ekkor K egy tipikus eleme:

$$\overline{a_0 + a_1x} = \overline{a_0} + \overline{a_1} \cdot \overline{x} = a_0 + a_1 \cdot i.$$

Tehát K elemei $a_0 + a_1 \cdot i$ $(a_0, a_1 \in \mathbb{R})$ alakúak, és az i szimbólumra vonatkozó (egyetlen) számolási szabály: $i^2 = -1$.

Egy véges test

Példa.
Számoljunk a $\mathbb{Z}_2[x] / (x^3 + x + 1)$ testben! Ennek 8 eleme van:

$$\overline{0}, \ \overline{1}, \ \overline{x}, \ \overline{x+1}, \ \overline{x^2}, \ \overline{x^2+1}, \ \overline{x^2+x}, \ \overline{x^2+x+1}.$$

$$\overline{x+1} + \overline{x^2+x} = \overline{x^2+2x+1} = \overline{x^2+1} \qquad \text{(semmi vész)}$$

$$\overline{x+1} \cdot \overline{x^2+x} = \overline{x^3+2x^2+x} = \overline{x^3+x} = \overline{1} \quad \text{(redukció mod } x^3+x+1\text{)}$$

Menjünk le alfába... A 8 elem:

$$0, \ 1, \ \alpha, \ \alpha+1, \ \alpha^2, \ \alpha^2+1, \ \alpha^2+\alpha, \ \alpha^2+\alpha+1.$$

A számolási szabály:

$$\alpha^3 + \alpha + 1 = 0, \quad \text{azaz} \quad \alpha^3 = \alpha + 1.$$

$$(\alpha+1) + (\alpha^2+\alpha) = \alpha^2 + 2\alpha + 1 = \alpha^2 + 1 \qquad \text{(s.v.)}$$

$$(\alpha+1) \cdot (\alpha^2+\alpha) = \alpha^3 + 2\alpha^2 + \alpha = \alpha^3 + \alpha = (\alpha+1) + \alpha = 1 \qquad \text{(sz.sz.)}$$

A nyolcelemű test művelettáblázatai

$+$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
1	1	0	$\alpha+1$	α	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$
α	α	$\alpha+1$	0	1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1
$\alpha+1$	$\alpha+1$	α	1	0	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2
α^2	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	0	1	α	$\alpha+1$
α^2+1	α^2+1	α^2	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	1	0	$\alpha+1$	α
$\alpha^2+\alpha$	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	α^2	α^2+1	α	$\alpha+1$	0	1
$\alpha^2+\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α^2+1	α^2	$\alpha+1$	α	1	0

$\cdot$	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
0	0	0	0	0	0	0	0	0
1	0	1	α	$\alpha+1$	α^2	α^2+1	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$
α	0	α	α^2	$\alpha^2+\alpha$	$\alpha+1$	1	$\alpha^2+\alpha+1$	α^2+1
$\alpha+1$	0	$\alpha+1$	$\alpha^2+\alpha$	α^2+1	$\alpha^2+\alpha+1$	α^2	1	α
α^2	0	α^2	$\alpha+1$	$\alpha^2+\alpha+1$	$\alpha^2+\alpha$	α	α^2+1	1
α^2+1	0	α^2+1	1	α^2	α	$\alpha^2+\alpha+1$	$\alpha+1$	$\alpha^2+\alpha$
$\alpha^2+\alpha$	0	$\alpha^2+\alpha$	$\alpha^2+\alpha+1$	1	α^2+1	$\alpha+1$	α	α^2
$\alpha^2+\alpha+1$	0	$\alpha^2+\alpha+1$	α^2+1	α	1	$\alpha^2+\alpha$	α^2	$\alpha+1$

Faktorgyűrűk

75. feladat. Írja fel a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű test összeadó- és szorzótábláját.

76. feladat. Hány elemű a $\mathbb{Z}_2[x] / (x^3 + x^2 + 1)$ gyűrű? Test-e ez a gyűrű?

$\mathbb{Z}_2[x] / (x^3 + x^2 + 1) = \{\overline{ax^2 + bx + c}: a, b, c \in \mathbb{Z}_2\}$, tehát $2^3 = 8$ eleme van.
A faktorgyűrű test, mivel $x^3 + x^2 + 1$ irreducibilis $\mathbb{Z}_2$ felett.

77. feladat. Hány elemű a $\mathbb{Z}_5[x] / (x^2 + 1)$ gyűrű? Test-e ez a gyűrű?

$\mathbb{Z}_5[x] / (x^2 + 1) = \{\overline{ax + b}: a, b \in \mathbb{Z}_5\}$, tehát $5^2 = 25$ eleme van.
A faktorgyűrű nem test, mivel $x^2 + 1$ nem irreducibilis $\mathbb{Z}_5$ felett.

78. feladat. Hány elemű a $\mathbb{Z}_3[x] / (x^2 + 1)$ gyűrű? Test-e ez a gyűrű?

79. feladat. Hány elemű a $\mathbb{Z}_3[x] / (x^3 + x^2 + 1)$ gyűrű? Test-e ez a gyűrű?

80. feladat. Hány elemű a $\mathbb{Z}_5[x] / (x^3 + 2)$ gyűrű? Test-e ez a gyűrű?

81. feladat. Hány elemű a $\mathbb{Z}_7[x] / (x^2 + 2)$ gyűrű? Test-e ez a gyűrű?

Számolás faktortestekben

82. feladat. Számítsa ki a $\mathbb{Z}_3[x] / (x^3 - x + 1)$ testben az alábbi hányadosokat:

$$\overline{1} / \overline{2x^2+1} = \overline{x}, \qquad \overline{x} / \overline{x+1} = \overline{x^2-x+1}.$$

83. feladat. Számítsa ki a $\mathbb{Z}_3[x] / (x^3 - x^2 + x + 1)$ testben az alábbi hányadosokat:

$$\overline{1} / \overline{x+1} = ?, \qquad \overline{x^2} / \overline{x-1} = ?.$$

84. feladat. Számítsa ki a $\mathbb{Z}_3[x] / (x^3 + x^2 - x + 1)$ testben az alábbi hányadosokat:

$$\overline{1} / \overline{x} = ?, \qquad \overline{x} / \overline{x-1}.$$

Egy végtelen faktortest

85. feladat. Határozza meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned} \overline{2-x}^{-1} = \overline{u} &\iff \overline{2-x} \cdot \overline{u} = \overline{1} \\ &\iff (2-x)\,u \equiv 1 \pmod{x^3-7} \\ &\iff \exists v \in \mathbb{Q}[x] : (2-x)\,u = 1 + (x^3-7)\,v \\ &\iff u \equiv x^2 + 2x + 4 \pmod{x^3-7} \\ &\iff \overline{u} = \overline{x^2+2x+4} \end{aligned}$$

Tehát $\overline{2-x}^{-1} = \overline{x^2+2x+4}$.

Gyöktelenítés

Menjünk le alfába:
$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$
ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7} \operatorname{cis} \frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:
$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$
Az előbb kiszámoltuk, hogy $\overline{2-x}^{\,-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2-\alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz
$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$
Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyökteleníteni.

Gyöktelenítés

86. feladat. Határozza meg a $\mathbb{Q}[x] \,/\, (x^3 - 2)$ testben az $\overline{x^2 + 3x + 4}$ elem multiplikatív inverzét, majd gyöktelenítse ennek segítségével a következő tört nevezőjét:
$$\frac{1}{\sqrt[3]{4} + 3\sqrt[3]{2} + 4}.$$

87. feladat. Határozza meg a $\mathbb{Q}[x] \,/\, (x^3 - 5)$ testben az $\overline{x^2 + 3x - 2}$ elem multiplikatív inverzét, majd gyöktelenítse ennek segítségével a következő tört nevezőjét:
$$\frac{1}{\sqrt[3]{25} + 3\sqrt[3]{5} - 2}.$$

Véges testek

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

Bizonyítás helyett.
Bármely p prímszám és n pozitív egész szám esetén létezik n-edfokú irreducibilis polinom $\mathbb{Z}_p$ felett (messze nem triviális!).

Ha $f \in \mathbb{Z}_p[x]$ egy ilyen polinom, akkor $T[x] \,/\, (f)$ egy p^n-elemű test.

Ha K egy q-elemű test, akkor tartalmaz prím elemszámú résztestet (közel sem triviális!).

Ha T egy p-elemű résztestе K-nak, akkor K vektorteret alkot T felett.

Ha ez a vektortér n-dimenziós, akkor $K \cong T^n$, ezért $|K| = p^n$. □

A q-elemű testet (mely izomorfia erejéig egyértelműen meghatározott), Galois tiszteletére $\mathrm{GF}(q)$ jelöli (Galois Field).

Véges testek

Példa.

- kételemű test: $\mathrm{GF}(2) \cong \mathbb{Z}_2$
- háromelemű test: $\mathrm{GF}(3) \cong \mathbb{Z}_3$
- négyelemű test: $\mathrm{GF}(4) \cong \mathbb{Z}_2[x] \,/\, (x^2 + x + 1)$
- ötelemű test: $\mathrm{GF}(5) \cong \mathbb{Z}_5$
- hatelemű test: nincs!
- hételemű test: $\mathrm{GF}(7) \cong \mathbb{Z}_7$
- nyolcelemű test: $\mathrm{GF}(8) \cong \mathbb{Z}_2[x] \,/\, (x^3 + x + 1)$
- kilencelemű test: $\mathrm{GF}(9) \cong \mathbb{Z}_3[x] \,/\, (x^2 + 1) = \{a + bi \colon a, b \in \mathbb{Z}_3\}$
- tízelemű test: nincs!
- ...

Polinom deriváltja

3.71. Definíció.
Az $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ polinom *derivált*ján az
$$n a_n x^{n-1} + \cdots + 2a_2 x + a_1$$
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.

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

Polinom deriváltja

Bizonyítás.
A fenti definíció alapján „egyszerű" számolással ellenőrizhető (nem kell hozzá határérték!). Például, ha már (1) megvan, akkor (2)-ben elég *monomok*kal foglalkozni.
$$\begin{aligned} f &= a \cdot x^k & g &= b \cdot x^l & fg &= ab \cdot x^{k+l} \\ f' &= ka \cdot x^{k-1} & g' &= lb \cdot x^{l-1} & (fg)' &= (k+l)\, ab \cdot x^{k+l-1} \end{aligned}$$
Ezek alapján
$$\begin{aligned} f'g + fg' &= kax^{k-1} \cdot bx^l + ax^k \cdot lbx^{l-1} \\ &= kab \cdot x^{k-1+l} + lab \cdot x^{k+l-1} \\ &= (kab + lab) \cdot x^{k+l-1} \\ &= (k+l)\, ab \cdot x^{k+l-1}. \end{aligned}$$
□

88. feladat. Fejezze be a 3.72. Tétel bizonyítását.

Derivált és többszörös gyökök

3.73. 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.)

Bizonyítás.
Ha az α gyök multiplicitása k, akkor
$$f = (x-\alpha)^k \cdot g, \text{ ahol } g(\alpha) \neq 0.$$
Deriváljunk!
$$\begin{aligned} f' &= k(x-\alpha)^{k-1} \cdot g + (x-\alpha)^k \cdot g' \\ &= (x-\alpha)^{k-1} \cdot (kg + (x-\alpha)\, g'). \end{aligned}$$
Tehát α legalább $(k-1)$-szeres gyöke f'-nak. Hogy pontosan $(k-1)$-szeres gyöke legyen, ahhoz az kell, hogy a kék polinomnak már ne legyen gyöke:
$$kg(\alpha) + (\alpha - \alpha)\, g'(\alpha) = kg(\alpha) \neq 0.$$
□

Derivált és többszörös gyökök

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

3.75. 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 $f(\alpha) = f'(\alpha) = \ldots = f^{(k-1)}(\alpha) = 0$, de $f^{(k)}(\alpha) \neq 0$.

Bizonyítás.

	α	k-szoros gyöke	f-nek
$\Longrightarrow$	α	$(k-1)$-szeres gyöke	f'-nak
$\Longrightarrow$	α	$(k-2)$-szörös gyöke	f''-nak
$\vdots$	$\vdots$	$\vdots$	$\vdots$
$\Longrightarrow$	α	1-szeres gyöke	$f^{(k-1)}$-nak
$\Longrightarrow$	α	0-szoros gyöke	$f^{(k)}$-nak.

□

Derivált és többszörös gyökök

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

Bizonyítás.
α többszörös gyöke f-nek $\iff$ α közös gyöke f-nek és f'-nak
$\iff$ α gyöke $\mathrm{lnko}(f, f')$-nak □

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

Bizonyítás.
Tfh. α egy k-szoros gyöke f-nek ($k \geq 1$). Hányadik hatványon szerepel $(x - \alpha)$ ...?

	f	felbontásában	k-adik hatványon
$\Longrightarrow$	f'	felbontásában	$(k-1)$-edik hatványon
$\Longrightarrow$	$\mathrm{lnko}(f, f')$	felbontásában	$(k-1)$-edik hatványon
$\Longrightarrow$	$f \,/\, \mathrm{lnko}(f, f')$	felbontásában	első hatványon.

□

Derivált és többszörös gyökök

89. feladat. A derivált vizsgálatával határozza meg az alábbi f polinom többszörös gyökeit, majd az összes gyökét (multiplicitással együtt):

$$f = x^5 + x^4 - 5x^3 - x^2 + 8x - 4.$$

$$\begin{aligned} f' &= 5x^4 + 4x^3 - 15x^2 - 2x + 8 \\ \operatorname{lnko}(f, f') &= x^3 - 3x + 2 && \text{(euklideszi algoritmus)} \\ \frac{f}{\operatorname{lnko}(f,f')} &= x^2 + x - 2 = (x-1)(x+2) && \text{(maradékos osztás)} \\ f &= (x-1)^3 (x+2)^2 && \text{(Horner vagy deriválás)} \end{aligned}$$

90. feladat. A derivált vizsgálatával határozza meg a $3x^4 - 4x^3 + 1$ polinom többszörös gyökeit, majd az összes gyökét (multiplicitással együtt).

91. feladat. A derivált vizsgálatával határozza meg az $x^5 - 10x^3 - 20x^2 - 15x - 4$ polinom többszörös gyökeit, majd az összes gyökét (multiplicitással együtt).

Irreducibilis polinomnak nincs többszörös gyöke

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

Bizonyítás.
Mivel $\operatorname{lnko}(f, f') \in T[x]$ osztója f-nek és f irreducibilis, csak két lehetőség van:

1. $\operatorname{lnko}(f, f') \sim f$: Ez nem lehet, mert $\deg \operatorname{lnko}(f, f') \leq \deg f' < \deg f$.
2. $\operatorname{lnko}(f, f') \sim 1$: Ekkor f-nek nincs többszörös gyöke.

□

A Cardano-képlet

3.79. 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.

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

Pozitív szám a gyök alatt

Példa.
Oldjuk meg az $x^3 + 6x = 20$ egyenletet.
Behelyettesítve a Cardano-képletebe ($p = 6$, $q = -20$), ezt kapjuk:

$$\underbrace{\sqrt[3]{10 + 6\sqrt{3}}}_{u} + \underbrace{\sqrt[3]{10 - 6\sqrt{3}}}_{v}.$$

A két köbgyök három-három értéke (figyelni kell a párbaállításra: $u_i v_i = -2$):

$$\begin{aligned} u_1 &= \sqrt[3]{10 + 6\sqrt{3}} & u_2 &= \sqrt[3]{10 + 6\sqrt{3}} \cdot \varepsilon & u_3 &= \sqrt[3]{10 + 6\sqrt{3}} \cdot \bar{\varepsilon} \\ v_1 &= \sqrt[3]{10 - 6\sqrt{3}} & v_2 &= \sqrt[3]{10 - 6\sqrt{3}} \cdot \bar{\varepsilon} & v_3 &= \sqrt[3]{10 - 6\sqrt{3}} \cdot \varepsilon \end{aligned}$$

Tehát az egyenlet megoldásai:

$$\begin{aligned} \alpha_1 &= \sqrt[3]{10 + 6\sqrt{3}} + \sqrt[3]{10 - 6\sqrt{3}} = 2 \\ \alpha_2 &= -1 + 3i \\ \alpha_3 &= -1 - 3i \end{aligned}$$

Negatív szám a gyök alatt (casus irreducibilis)

Példa.
Oldjuk meg az $x^3 = 15x + 4$ egyenletet.
Behelyettesítve a Cardano-képletebe ($p = -15$, $q = -4$), ezt kapjuk:

$$\underbrace{\sqrt[3]{2 + \sqrt{-121}}}_{u} + \underbrace{\sqrt[3]{2 - \sqrt{-121}}}_{v}.$$

A $\sqrt[3]{2 + 11i}$ köbgyökvonást elvégezni bajos! Vegyük észre, hogy $(2 + i)^3 = 2 + 11i$!

Tehát az egyenlet megoldásai:

$$\begin{aligned} \alpha_1 &= (2 + i) + (2 - i) = 4 \\ \alpha_2 &= (2 + i)\,\varepsilon + (2 - i)\,\bar{\varepsilon} = -2 - \sqrt{3} \\ \alpha_3 &= (2 + i)\,\bar{\varepsilon} + (2 - i)\,\varepsilon = -2 + \sqrt{3} \end{aligned}$$

A valós együtthatós harmadfokú egyenlet

3.81. 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 irreducibilisnek).*

A diszkrimináns

3.82. 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.

3.83. 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.

A diszkrimináns

3.83. Megjegyzés (folyt.).
Hasonlóan lehet definiálni tetszőleges fokszámú polinom diszkriminánsát is: az $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$ polinom diszkriminánsa

$$a_n^{2n-2} \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2.$$

92. feladat. Mutassa meg a fenti definíció alapján, hogy az $ax^2 + bx + c$ polinom diszkriminánsa $a^2 (\alpha_1 - \alpha_2)^2 = b^2 - 4ac$.

TILOS MEGTANULNI!

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

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

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

Ferrari módszere

3.85. 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.

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:

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

Viète-formulák

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:

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

Még formálisabban:

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

Többhatározatlanú polinomok

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.

4.5. Megjegyzés.

Az n-határozatlanú polinomok gyűrűjét lehetne rekurzívan is definiálni: legyen

$$T[x_1, \ldots, x_n] = (T[x_1, \ldots, x_{n-1}])[x_n],$$

azaz a $T[x_1, \ldots, x_{n-1}]$ integritástartomány feletti (egyhatározatlanú) polinomgyűrű.

Többhatározatlanú polinomok

Példa.

$$\begin{aligned}
f = {} & 7x_1^2x_3 - 2x_1x_2x_3^4 + 9x_1x_2 - 3x_1^2x_2x_3^2 + x_1x_2x_3^3 - 2x_1^2 + \\
& 5x_1x_2^2x_3 - x_1^2x_2x_3 - 6x_1x_3 + 2x_3^2 + x_1x_3^2 + 4x_2^2x_3^2 + 8 \qquad \in \mathbb{R}[x_1, x_2, x_3]\\
f = {} & x_1^2 \cdot \left(-3x_2x_3^2 - x_2x_3 + 7x_3 - 2\right) + \\
& x_1 \cdot \left(5x_2^2x_3 - 2x_2x_3^4 + x_2x_3^3 + 9x_2 + x_3^2 - 6x_3\right) + \\
& \left(4x_2^2x_3^2 + 2x_3^2 + 8\right) \qquad \in \mathbb{R}[x_2, x_3][x_1]\\
f = {} & x_1^2 \cdot \Big(x_2 \cdot \left(-3x_3^2 - x_3\right) + (7x_3 - 2)\Big) + \\
& x_1 \cdot \Big(x_2^2 \cdot (5x_3) - x_2\left(2x_3^4 + x_3^3 + 9\right) + \left(x_3^2 - 6x_3\right)\Big) + \\
& \Big(x_2^2 \cdot \left(4x_3^2\right) + \left(2x_3^2 + 8\right)\Big) \qquad \in \mathbb{R}[x_3][x_2][x_1]
\end{aligned}$$

Lexikografikus rendezés

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

$$\exists i \in \{1, \ldots, n\}: \; k_1 = l_1, \ldots, k_{i-1} = l_{i-1} \text{ és } k_i > l_i.$$

(Vagyis megkeressük az első eltérést a $k_1, k_2, \ldots, k_n$ és az $l_1, l_2, \ldots, l_n$ kitevősorozatok között, és amelyikben nagyobb szám áll ezen a helyen, az kerül előrébb a lexikografikus sorrendben.)

Jelölés.

Tetszőleges $M, N \in T[x_1, \ldots, x_n]$ monomok esetén $M \sqsupset N$ jelöli azt, hogy M lexikografikusan megelőzi N-et, $M \underset{\sim}{\sqsupset} N$ pedig azt, hogy $M \sqsupset N$ vagy $M \sim N$. A $\underset{\sim}{\sqsupset}$ relációt *lexikografikus rendezés*nek nevezzük.

Lexikografikus rendezés

Példa.

$$\begin{aligned}
x_1^2x_2^{99}x_3^{23}x_4^{71} &\quad \sqsubset \quad x_1^3x_2x_3^2x_4^5\\
-2x_1^3x_2x_3^4x_4^2 &\quad \sqsupset \quad 14x_1^3x_2x_3^2x_4^3\\
x_1x_2x_3^2x_4 &\quad \sqsupset \quad 3x_2^4x_3^6x_4^2\\
12x_1^2x_2^3x_3x_4^5 &\quad \sim \quad -9x_1^2x_2^3x_3x_4^5
\end{aligned}$$

Lexikografikus rendezés

4.7. Állítás.

A monomok halmazán $\underset{\sim}{\sqsupset}$ reflexív, tranzitív és dichotóm reláció, valamint $M \underset{\sim}{\sqsupset} N$ és $M \underset{\sim}{\sqsubset} N$ akkor és csak akkor áll fenn egyszerre, ha M és N asszociált.

4.8. Megjegyzés.

Az előző állítás szerint a $\underset{\sim}{\sqsupset}$ 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 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 $M \underset{\sim}{\sqsupset} N$ és $\hat{M} \underset{\sim}{\sqsupset} \hat{N}$, akkor $M\hat{M} \underset{\sim}{\sqsupset} N\hat{N}$, és itt asszociáltság csak akkor teljesül, ha $M \sim N$ és $\hat{M} \sim \hat{N}$.

4.10. Állítás.

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

Lexikografikus rendezés

Példa.

A korábbi példában szereplő polinom tagjai lexikografikusan csökkenő sorrendben:

$$\begin{aligned}
f = {} & -3x_1^2x_2x_3^2 - x_1^2x_2x_3 + 7x_1^2x_3 - 2x_1^2 + 5x_1x_2^2x_3 - 2x_1x_2x_3^4 + \\
& + x_1x_2x_3^3 + 9x_1x_2 + x_1x_3^2 - 6x_1x_3 + 4x_2^2x_3^2 + 2x_3^2 + 8
\end{aligned}$$

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

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

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.

Szimmetrikus polinomok

Példa.
Határozzuk meg az x^3+2x^2+8x+6 polinom gyökeinek négyzetösszegét.

A Viète-formulák szerint

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3 &= \sigma_1(\alpha_1,\alpha_2,\alpha_3) = -2,\\
\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= \sigma_2(\alpha_1,\alpha_2,\alpha_3) = 8,\\
\alpha_1\alpha_2\alpha_3 &= \sigma_3(\alpha_1,\alpha_2,\alpha_3) = -6.
\end{aligned}$$

$$\alpha_1^2+\alpha_2^2+\alpha_3^2 = (\alpha_1+\alpha_2+\alpha_3)^2 - 2(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) = 4-16 = -12$$

A megoldás kulcsa az, hogy az $x_1^2+x_2^2+x_3^2 \in \mathbb{Q}[x_1,x_2,x_3]$ polinomot ki lehet fejezni az elemi szimmetrikus polinomok segítségével:

$$x_1^2+x_2^2+x_3^2 = \sigma_1^2 - 2\sigma_2.$$

Ez pedig azért tehető meg, mert $x_1^2+x_2^2+x_3^2$ szimmetrikus polinom.

A szimmetrikus polinomok alaptétele

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

$$k_1 \ge \cdots \ge k_n.$$

4.16. Lemma.
Tetszőleges $k_1 \ge \cdots \ge k_n$ 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:

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

A szimmetrikus polinomok alaptétele

93. feladat. Fejezze ki az $f = x_1^3+x_2^3+x_3^3 \in \mathbb{R}[x_1,x_2,x_3]$ polinomot az elemi szimmetrikus polinomok polinomjaként.

$f = x_1^3+x_2^3+x_3^3$

$f-\sigma_1^3 = -3x_1^2x_2 - 3x_1^2x_3 - 3x_1x_2^2 - 6x_1x_2x_3 - 3x_1x_3^2 - 3x_2^2x_3 - 3x_2x_3^2$

$f-\sigma_1^3+3\sigma_1\sigma_2 = 3x_1x_2x_3$

$f-\sigma_1^3+3\sigma_1\sigma_2-3\sigma_3 = 0$

Tehát

$$f = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3 = h(\sigma_1,\sigma_2,\sigma_3), \text{ ahol } h(x_1,x_2,x_3) = x_1^3 - 3x_1x_2 + 3x_3.$$

SZPAT+Viète

94. feladat. Anélkül, hogy megkeresné a gyököket, határozza meg az $f = x^3-3x^2+x-8$ polinom gyökeinek köbösszegét, valamint számtani, mértani és harmonikus közepét.

A Viète-formulák szerint

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3 &= \sigma_1(\alpha_1,\alpha_2,\alpha_3) = 3,\\
\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= \sigma_2(\alpha_1,\alpha_2,\alpha_3) = 1,\\
\alpha_1\alpha_2\alpha_3 &= \sigma_3(\alpha_1,\alpha_2,\alpha_3) = 8.
\end{aligned}$$

Az előző feladat alapján

$$\begin{aligned}
\alpha_1^3+\alpha_2^3+\alpha_3^3 &= \sigma_1(\alpha_1,\alpha_2,\alpha_3)^3 - 3\sigma_1(\alpha_1,\alpha_2,\alpha_3)\sigma_2(\alpha_1,\alpha_2,\alpha_3) + 3\sigma_3(\alpha_1,\alpha_2,\alpha_3) =\\
&= 3^3 - 3\cdot 3\cdot 1 + 3\cdot 8 = 42
\end{aligned}$$

SZPAT+Viète

$$\begin{aligned}
\alpha_1+\alpha_2+\alpha_3 &= \sigma_1(\alpha_1,\alpha_2,\alpha_3) = 3,\\
\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3 &= \sigma_2(\alpha_1,\alpha_2,\alpha_3) = 1,\\
\alpha_1\alpha_2\alpha_3 &= \sigma_3(\alpha_1,\alpha_2,\alpha_3) = 8.
\end{aligned}$$

számtani közép:

$$\frac{\alpha_1+\alpha_2+\alpha_3}{3} = \frac{3}{3} = 1$$

mértani közép:

$$\sqrt[3]{\alpha_1\alpha_2\alpha_3} = \sqrt[3]{8} = 2$$

harmonikus közép:

$$\frac{3}{\frac{1}{\alpha_1}+\frac{1}{\alpha_2}+\frac{1}{\alpha_3}} = \frac{3}{\frac{\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3}{\alpha_1\alpha_2\alpha_3}} = \frac{3\alpha_1\alpha_2\alpha_3}{\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3} = \frac{3\cdot 8}{1} = 24$$

95. feladat. Fejezze ki az $x_1^4+x_2^4+x_3^4 \in \mathbb{R}[x_1,x_2,x_3]$ polinomot az elemi szimmetrikus polinomok polinomjaként.

96. feladat. Anélkül, hogy megkeresné a gyököket, határozza meg az $f = 2x^3+4x^2-6x+2$ polinom gyökeinek negyedik hatványösszegét.

Diszkrimináns

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

Példa.
Ha a $g = \prod_{1\le i<j\le n}(x_i-x_j)^2$ polinomra alkalmazzuk a fenti következményt, akkor azt kapjuk, hogy racionális együtthatós polinom diszkriminánsa racionális szám (hiszen kifejezhető az együtthatók racionális polinomjaként).

A harmadfokú polinom diszkriminánsa

$$D = (x_1-x_2)^2(x_1-x_3)^2(x_2-x_3)^2 = \sigma_1^2\sigma_2^2 - 4\sigma_1^3\sigma_3 - 4\sigma_2^3 + 18\sigma_1\sigma_2\sigma_3 - 27\sigma_3^2$$

Ha $(x-\alpha_1)(x-\alpha_2)(x-\alpha_3) = x^3+px+q$, akkor a Viéte-formulák szerint

$$\begin{aligned}
\sigma_1(\alpha_1,\alpha_2,\alpha_3) &= 0,\\
\sigma_2(\alpha_1,\alpha_2,\alpha_3) &= p,\\
\sigma_3(\alpha_1,\alpha_2,\alpha_3) &= -q,
\end{aligned}$$

tehát

$$\begin{aligned}
D(\alpha_1,\alpha_2,\alpha_3) &= -4\sigma_2(\alpha_1,\alpha_2,\alpha_3)^3 - 27\sigma_3(\alpha_1,\alpha_2,\alpha_3)^2\\
&= -4p^3 - 27q^2\\
&= -108\left(\left(\frac{q}{2}\right)^2 + \left(\frac{p}{3}\right)^3\right).
\end{aligned}$$

Algebrai és transzcendens 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.

Algebrai és transzcendens számok

Példa.

- $\sqrt{2}$ algebrai szám, minimálpolinomja: $x^2 - 2$ (miért irreducibilis?).
- $\sqrt[n]{2}$ algebrai szám, minimálpolinomja: $x^n - 2$ (miért irreducibilis?).
- i algebrai szám, minimálpolinomja: $x^2 + 1$ (miért irreducibilis?).
- π és e transzcendens számok.
- A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- Gelfond–Schneider-tétel: Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám.
  Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $i^i = e^{-\pi/2}$ transzcendens számok.

Algebrai számok és gyökmennyiségek

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.

Példa.
Ez a szám algebrai:

$$\frac{\sqrt[3]{3 - \sqrt{\sqrt[4]{2} + \sqrt[5]{\frac{3}{17}}}} + \sqrt[17]{323 - \sqrt{2014}}}{\sqrt{2} + \sqrt[3]{3} + \sqrt[5]{5}}$$

Algebrai számok és gyökmennyiségek

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

A fenti ártatlannak látszó tételből következik, hogy nem minden egyenlet oldható meg gyökjelek segítségével. Az ötödfokú egyenletnek már nincs általános megoldóképlete, sőt, például az $x^5 - 4x + 2 = 0$ egyenletnek még „ad hoc” megoldóképlete sincs, mert gyökei nem gyökmennyiségek.

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.

Oszthatóság

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) $a \mid a$

Biz: $a = a \cdot 1$

(2) $(a \mid b$ és $b \mid c) \implies a \mid c$

Biz: $(b = au$ és $c = bv) \implies c = (au)v = a(uv)$

Oszthatóság

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

(3) $(a \mid b$ és $b \mid a) \iff \exists u \in R^* : b = ua$

Biz: $(b = au$ és $a = bv) \implies a = a(uv) \overset{a \neq 0}{\implies} 1 = uv \implies u, v \in R^*$
$b = ua \implies a = u^{-1}b \implies (a \mid b$ és $b \mid a)$

(4) $1 \mid a$

Biz: $a = 1 \cdot a$

(5) $a \mid 0$

Biz: $0 = a \cdot 0$

(6) $a \mid 1 \iff a \in R^*$

Biz: $a \mid 1 \iff \exists u \in R : 1 = au \iff a \in R^*$

Oszthatóság

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

(7) $0 \mid a \iff a = 0$

Biz: $0 \mid a \iff \exists u \in R : a = 0 \cdot u \iff a = 0$

(8) $(a \mid b$ és $a \mid c) \implies a \mid b \pm c$

Biz: $(b = au$ és $c = av) \implies b \pm c = au \pm av = a(u \pm v)$

(9) $a \mid b \implies a \mid bc$

Biz: $b = au \implies bc = a(uc)$

(10) $a \mid b \iff ac \mid bc$, ha $c \neq 0$

Biz: $b = au \implies bc = (ac)u$
$bc = auc \overset{c \neq 0}{\implies} b = au$

□

Asszociáltság

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.

Asszociáltság

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 $(R/\sim; \mid)$ 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 $(\mathbb{N}_0; \mid)$ részbenrendezett halmazt kapjuk, ami lényegében ugyanaz, mint a $(\mathbb{Z}/\sim; \mid)$ 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.

Kongruencia

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

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

Az 5.9. Állítás bizonyítása

reflexivitás: $a \equiv a \pmod m \iff m \mid a - a = 0$

szimmetria: $a \equiv b \pmod m \implies m \mid a - b$

$\implies m \mid (-1)\cdot(a-b) = b - a$

$\implies b \equiv a \pmod m$

tranzitivitás: $a \equiv b$ és $b \equiv c \pmod m \implies m \mid a - b$ és $m \mid b - c$

$\implies m \mid (a-b)+(b-c) = a - c$

$\implies a \equiv c \pmod m$

Tfh. $a_1 \equiv b_1 \pmod m$ és $a_2 \equiv b_2 \pmod m$. Ekkor $m \mid a_1 - b_1$ és $m \mid a_2 - b_2$.

$$a_1 \cdot a_2 \stackrel{?}{\equiv} b_1 \cdot b_2 \pmod m \iff m \stackrel{?}{\mid} a_1a_2 - b_1b_2$$

$$\iff m \stackrel{?}{\mid} a_1a_2 - b_1a_2 + b_1a_2 - b_1b_2$$

$$\iff m \stackrel{?}{\mid} (a_1 - b_1)\cdot a_2 + b_1\cdot(a_2 - b_2) \qquad \square$$

97. feladat. Fejezze be az 5.9. Állítás bizonyítását.

Maradékosztály-gyűrű

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 (addditív inverze, szorzata) nem függ attól, hogy az egyes maradékosztályokból melyik elemet választjuk reprezentánsnak, és ezekkel a műveletekkel $R/(m)$ kommutatív egységelemes gyűrűt alkot.

Az 5.12. Állítás bizonyítása

A műveletek jóldefiniáltságát az 5.9. Állítás biztosítja. Például (a többi HF):

$$\overline{u_1} = \overline{v_1} \text{ és } \overline{u_2} = \overline{v_2} \implies u_1 \equiv v_1 \text{ és } u_2 \equiv v_2 \pmod m$$

$$\implies u_1 + u_2 \equiv v_1 + v_2 \pmod m$$

$$\implies \overline{u_1 + u_2} = \overline{v_1 + v_2}$$

Az azonosságokat (asszociativitás, kommutativitás, disztributivitás) „örökli" az $R/(m)$ faktorgyűrű az R gyűrűtől. Például (a többi HF):

$$\overline{u}\cdot(\overline{v}+\overline{w}) = \overline{u}\cdot\overline{v+w} = \overline{u\cdot(v+w)} = \overline{u\cdot v + u\cdot w} = \overline{u\cdot v} + \overline{u\cdot w} = \overline{u}\cdot\overline{v} + \overline{u}\cdot\overline{w}$$

additív egységelem: $\overline{0}$

$$\overline{u} + \overline{0} = \overline{u+0} = \overline{u}$$

$\overline{u}$ additív inverze: $\overline{-u}$

$$\overline{u} + \overline{-u} = \overline{u+(-u)} = \overline{0}$$

multiplikatív egységelem: $\overline{1}$

$$\overline{u}\cdot\overline{1} = \overline{u\cdot 1} = \overline{u} \qquad \square$$

98. feladat. Fejezze be az 5.12. Állítás bizonyítását.

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.

Legnagyobb közös osztó

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).

Osztóhalmazok

Jelölés.
Tetszőleges $a \in R$ esetén legyen $D_a = \{k \in R : k \mid a\}$.

5.15. Állítás.
Minden $a, b \in R$ esetén $a \mid b \iff D_a \subseteq D_b$.

Bizonyítás.
$a \mid b \stackrel{?}{\implies} D_a \subseteq D_b$: Tfh. $a \mid b$, és legyen $k \in D_a$.
Ekkor $k \mid a \mid b$, tehát az oszthatóság tranzitivitása miatt $k \in D_b$.

$D_a \subseteq D_b \stackrel{?}{\implies} a \mid b$: Tfh. $D_a \subseteq D_b$.
Ekkor $a \in D_a$ miatt $a \in D_b$ teljesül, ezért $a \mid b$. $\square$

5.16. Következmény.
Minden $a, b \in R$ esetén $a \sim b \iff D_a = D_b$.

Bizonyítás.
$a \sim b \iff a \mid b$ és $b \mid a \iff D_a \subseteq D_b$ és $D_b \subseteq D_a \iff D_a = D_b$ $\square$

Osztóhalmazok és lnko

5.17. Tétel.
Tetszőleges $a, b, d \in R$ esetén d akkor és csak akkor legnagyobb közös osztója a-nak és b-nek, ha $D_a \cap D_b = D_d$.

Bizonyítás.
Először tegyük fel, hogy d legnagyobb közös osztója a-nak és b-nek.

$D_a \cap D_b \stackrel{?}{\subseteq} D_d$: Minden $k \in R$ esetén

$$k \in D_a \cap D_b \implies k \mid a, b \xRightarrow{5.13/(2)} k \mid d \implies k \in D_d.$$

$D_d \stackrel{?}{\subseteq} D_a \cap D_b$: Minden $k \in R$ esetén

$$k \in D_d \implies k \mid d \xRightarrow{5.13/(1)+\text{tr.}} k \mid a, b \implies k \in D_a \cap D_b.$$

Most tegyük fel, hogy $D_a \cap D_b = D_d$.

(1) $d \stackrel{?}{\mid} a$ és $d \stackrel{?}{\mid} b$: $d \in D_d = D_a \cap D_b \implies d \mid a, b$

(2) $\forall k \in R : (k \mid a \text{ és } k \mid b) \stackrel{?}{\implies} k \mid d$: Minden $k \in R$ esetén

$$k \mid a \text{ és } k \mid b \implies k \in D_a \cap D_b = D_d \implies k \mid d. \qquad \square$$

A legnagyobb közös osztó egyértelműsége

5.18. 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.

Bizonyítás.
(1) Tfh. d_1 és d_2 is legnagyobb közös osztója a-nak és b-nek.
Ekkor $D_{d_1} = D_a \cap D_b = D_{d_2} \implies d_1 \sim d_2$.
(2) Tfh. d_1 legnagyobb közös osztója a-nak és b-nek, és $d_1 \sim d_2$.
Ekkor $D_{d_2} = D_{d_1} = D_a \cap D_b \implies d_2$ is lnko-ja a-nak és b-nek. $\square$

5.19. Megjegyzés.
Az előző tétel szerint a lnko (és a lkkt) nem egyértelmű, ezért általában nem azt írjuk, hogy $d = \operatorname{lnko}(a,b)$, hanem azt, hogy $d \sim \operatorname{lnko}(a,b)$.
(Az egész számok gyűrűjében megállapodtunk abban, hogy mindig a nemnegatív legnagyobb közös osztót vesszük, test feletti polinomgyűrűben pedig mindig választhatunk főpolinomot legnagyobb közös osztónak.)

A legnagyobb közös osztó tulajdonságai

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

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

(1) $\operatorname{lnko}(\operatorname{lnko}(a,b), c) \sim \operatorname{lnko}(a, \operatorname{lnko}(b,c))$

Biz: $D_{(a,b)} \cap D_c = (D_a \cap D_b) \cap D_c = D_a \cap (D_b \cap D_c) = D_a \cap D_{(b,c)}$
$\implies ((a,b),c) \sim (a,(b,c))$

(2) $\operatorname{lnko}(a,b) \sim \operatorname{lnko}(b,a)$

Biz: $D_{(a,b)} = D_a \cap D_b = D_b \cap D_a = D_{(b,a)} \implies (a,b) \sim (b,a)$

(3) $\operatorname{lnko}(a,a) \sim a$

Biz: $D_{(a,a)} = D_a \cap D_a = D_a \implies (a,a) \sim a$

(4) $\operatorname{lnko}(0,a) \sim a$

Biz: $D_{(0,a)} = D_0 \cap D_a = R \cap D_a = D_a \implies (0,a) \sim a$

A legnagyobb közös osztó tulajdonságai

(5) $1 \perp a$

Biz: $D_{(1,a)} = D_1 \cap D_a = R^* \cap D_a = R^* = D_1 \implies (1, a) \sim 1$

(6) $\operatorname{lnko}(a, b) \sim a \iff a \mid b$

Biz: $(a, b) \sim a \iff D_a \cap D_b = D_a \iff D_a \subseteq D_b \iff a \mid b$

(7) $\operatorname{lnko}(a + bc, b) \sim \operatorname{lnko}(a, b)$

Biz: $\forall k \in R : \ k \mid a + bc, b \iff k \mid a, b$
$\implies (a + bc, b) \sim (a, b)$

(8) $\operatorname{lnko}(a, b) \cdot c \sim \operatorname{lnko}(ac, bc)$

Biz: a táblán.

(9) $\operatorname{lnko}(a, b) \not\sim 0 \implies \frac{a}{\operatorname{lnko}(a,b)} \perp \frac{b}{\operatorname{lnko}(a,b)}$

Biz: $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) \cdot (a, b) \sim (a, b) \implies \left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) \sim 1$

(10) $a \perp b \implies \operatorname{lnko}(a, bc) \sim \operatorname{lnko}(a, c)$

Biz: a táblán. □

A legnagyobb közös osztó tulajdonságai

5.22. Következmény.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R$, $a \perp b$ esetén teljesülnek az alábbiak:

(1) $a \mid bc \iff a \mid c$

Biz: $a \mid bc \iff (a, bc) \sim a \iff (a, c) \sim a \iff a \mid c$

(2) $(a \mid c \text{ és } b \mid c) \iff ab \mid c$

Biz: $a \mid b \cdot \frac{c}{b} \implies a \mid \frac{c}{b} \implies ab \mid c$ □

5.23. Következmény.

Ha az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, akkor tetszőleges $a, b, c \in R$, $\operatorname{lnko}(a, b) \not\sim 0$ esetén

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

Bizonyítás.

$a \mid bc \iff (a, b) \cdot \frac{a}{(a,b)} \,\Big|\, (a, b) \cdot \frac{b}{(a,b)} \cdot c \iff \frac{a}{(a,b)} \,\Big|\, \frac{b}{(a,b)} \cdot c \iff \frac{a}{(a,b)} \,\Big|\, c$ □

Legkisebb közös többszörös

5.24. 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

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

Bizonyítás.

Ha $a = b = 0$, akkor $\operatorname{lnko}(a, b) = \operatorname{lkkt}(a, b) = 0$.
Ellenkező esetben $d := \operatorname{lnko}(a, b) \neq 0$. Megmutatjuk, hogy $t := \frac{ab}{d}$ eleget tesz a legkisebb közös többszörös definíciójának.

(1) $a \overset{?}{\mid} t$ és $b \overset{?}{\mid} t$:

Világos, hiszen $t = \frac{a}{d} \cdot b = a \cdot \frac{b}{d}$.

(2) $\forall k \in R : (a \mid k \text{ és } b \mid k) \overset{?}{\implies} t \mid k$:

$a, b \mid k \implies \frac{a}{d}, \frac{b}{d} \mid \frac{k}{d} \implies \frac{a}{d} \cdot \frac{b}{d} \mid \frac{k}{d} \implies \frac{ab}{d} \mid k$ □

A legnagyobb közös osztó létezése

5.25. 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 az 5.21. Tétel (és a következményei) úgy, hogy „**Ha** az R integritástartományban bármely két elemnek létezik legnagyobb közös osztója, **akkor** ...”.

A legnagyobb közös osztó létezése

Példa.

A $\mathbb{Z}\left[\sqrt{-5}\right] = \left\{a + b\sqrt{-5} : a, b \in \mathbb{Z}\right\} = \left\{a + b\sqrt{5}i : a, b \in \mathbb{Z}\right\}$ integritástartományban nem létezik bármely két elemnek legnagyobb közös osztója.

Legyen $u = 6$ és $v = 2 + 2\sqrt{-5}$.

$$\begin{aligned} D_u &= \left\{\pm 1, \pm 2, \pm 3, \pm\left(1 + \sqrt{-5}\right), \pm\left(1 - \sqrt{-5}\right), \pm 6\right\} \\ D_v &= \left\{\pm 1, \pm 2, \pm\left(1 + \sqrt{-5}\right), \pm\left(2 + \sqrt{-5}\right)\right\} \\ D_u \cap D_v &= \left\{\pm 1, \pm 2, \pm\left(1 + \sqrt{-5}\right)\right\} \end{aligned}$$

A $(D_u \cap D_v / \sim; \mid)$ részbenrendezett halmaznak nincs legnagyobb eleme, ezért $\operatorname{lnko}(u, v)$ nem létezik.

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.

5.26. 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 $\|r\| < \|b\|$.

5.27. 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).

Nevezetes euklideszi gyűrűk

5.28. 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.

Bizonyítás.

A táblán. □

5.29. 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

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

Euklideszi algoritmus euklideszi gyűrűben

5.30. Tétel.

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

Bizonyítás.

Szinte szóról szóra ugyanaz, mint számelméletből (lásd ott az 1.18. Tételt).
Ha $a = 0$, akkor $\operatorname{lnko}(a, b) \sim b$, és $a \cdot 1 + b \cdot 1 \sim \operatorname{lnko}(a, b)$. A $b = 0$ eset hasonló.
Most tfh. $a, b \neq 0$, és hajtsuk végre az $a =: r_0$ és $b =: r_1$ elemekre az euklideszi algoritmust:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 && (0 < \|r_2\| < \|r_1\|); \\ r_1 &= q_2 r_2 + r_3 && (0 < \|r_3\| < \|r_2\|); \\ r_2 &= q_3 r_3 + r_4 && (0 < \|r_4\| < \|r_3\|); \\ &\vdots \\ r_{i-1} &= q_i r_i + r_{i+1} && (0 < \|r_{i+1}\| < \|r_i\|); \\ &\vdots \end{aligned}$$

Mivel $\|r_1\| > \|r_2\| > \|r_3\| > \cdots$, az eljárás véges számú lépés után véget ér: létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$.

Euklideszi algoritmus euklideszi gyűrűben

Biz. (folyt.)

Könnyű ellenőrizni, hogy minden i-re $D_{r_{i-1}} \cap D_{r_i} = D_{r_i} \cap D_{r_{i+1}}$ (HF). Tehát

$$D_a \cap D_b = D_{r_0} \cap D_{r_1} = D_{r_1} \cap D_{r_2} = \cdots = D_{r_n} \cap D_{r_{n+1}} = D_{r_n} \cap D_0 = D_{r_n},$$

és így $\operatorname{lnko}(a, b) \sim r_n$.

Teljes indukcióval megmutatható, hogy minden i-re $\exists x_i, y_i \in R : \ ax_i + by_i = r_i$.

Kezdőlépések: $a \cdot 1 + b \cdot 0 = r_0$ és $a \cdot 0 + b \cdot 1 = r_1$.

Tfh. $j = 0, 1, \ldots, i$ esetén $\exists x_j, y_j \in R : \ ax_j + by_j = r_j$. (IH)

Fejezzük ki r_{i+1}-et a és b segítségével:

$$\begin{aligned} r_{i+1} &= r_{i-1} - r_i \cdot q_i \overset{\text{(IH)}}{=} (ax_{i-1} + by_{i-1}) - (ax_i + by_i) \cdot q_i \\ &= a \cdot (\underbrace{x_{i-1} - x_i q_i}_{x_{i+1}}) + b \cdot (\underbrace{y_{i-1} - y_i q_i}_{y_{i+1}}). \end{aligned}$$

Mivel $\operatorname{lnko}(a, b) \sim r_n$, azt kapjuk, hogy $ax_n + by_n \sim \operatorname{lnko}(a, b)$. □

99. feladat. Fejezze be az 5.30. Tétel bizonyítását.

Lineáris diofantoszi egyenlet euklideszi gyűrűben

5.31. 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 $\text{lnko}\,(a, b) \mid c$.

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:

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

Bizonyítás.

Szinte szóról szóra ugyanaz, mint számelméletből (lásd ott az 1.23. Tételt).
Legyen $d \sim \text{lnko}\,(a, b) \neq 0$.

Ha x, y egy megoldás, akkor $d \mid ax + by = c$.

Tudjuk, hogy $\exists x', y' \in R : ax' + by' = d$.
Ha $d \mid c$, akkor $x = x'\frac{c}{d}, y = y'\frac{c}{d}$ egy megoldás: $ax'\frac{c}{d} + by'\frac{c}{d} = c$.

Lineáris diofantoszi egyenlet euklideszi gyűrűben

Biz. (folyt.)

Tfh. x_0, y_0 egy megoldás, azaz $ax_0 + by_0 = c$.

Az világos, hogy minden $t \in R$ esetén $x = x_0 + \frac{b}{d}t, y = y_0 - \frac{a}{d}t$ szintén megoldás:

$$a\left(x_0 + \frac{b}{d}t\right) + b\left(y_0 - \frac{a}{d}t\right) = ax_0 + by_0 + \frac{ab}{d}t - \frac{ab}{d}t = c.$$

Legyen most x, y egy tetszőleges megoldás.

$$\begin{aligned} ax + by = c = ax_0 + by_0 &\implies ax - ax_0 = by_0 - by \\ &\implies b \mid a(x - x_0) \\ &\implies \tfrac{b}{d} \mid x - x_0 \\ &\implies \exists t \in R : \; x - x_0 = \tfrac{b}{d}t \end{aligned}$$

Az y-ra vonatkozó képlet ezután már egyszerű visszahelyettesítéssel kijön:

$$by_0 - by = a(x - x_0) = \tfrac{abd}{t} \implies y = y_0 - \tfrac{a}{d}t.$$

□

Irreducibilitás és prímtulajdonság

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

5.32. 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:

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

5.33. 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:

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

Prímtulajdonság

5.34. 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.

Bizonyítás.

$$\begin{aligned} p \mid a_1 \cdot (a_2 \cdot \ldots \cdot a_n) &\implies p \mid a_1 \text{ vagy } p \mid a_2 \cdot \ldots \cdot a_n = a_2 \cdot (a_3 \cdot \ldots \cdot a_n) \\ &\implies p \mid a_1 \text{ vagy } p \mid a_2 \text{ vagy } p \mid a_3 \cdot \ldots \cdot a_n = a_3 \cdot (a_4 \cdot \ldots \cdot a_n) \\ &\implies \cdots \\ &\implies p \mid a_1 \text{ vagy } p \mid a_2 \text{ vagy } p \mid a_3 \text{ vagy } \ldots \text{ vagy } p \mid a_n \end{aligned}$$

□

Irreducibilitás vs. prímtulajdonság

5.35. Tétel.

Minden integritástartományban a prímelemek irreducibilisek.

Bizonyítás.

Legyen R egy tetszőleges integritástartomány és $p \in R$ egy prímtulajdonságú elem. Ekkor $p \nsim 0, 1$, így csak azt kell belátnunk, hogy p-nek minden felbontása triviális.

Tekintsük p egy tetszőleges felbontását: $p = ab$.
Világos, hogy ekkor $a \mid p$ és $b \mid p$.

Az is világos, hogy $p \mid ab$, tehát p prímtulajdonsága miatt $p \mid a$ vagy $p \mid b$.
Az első esetben $p \sim a$, a második esetben $p \sim b$, azaz a felbontás triviális.

□

Irreducibilitás vs. prímtulajdonság

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

5.36. Tétel.

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

Bizonyítás.

Legyen R egy olyan integritástartomány, amelyben bármely két elemnek létezik legnagyobb közös osztója, és legyen $p \in R$ irreducibilis. Ekkor $p \notin R^* \cup \{0\}$, így csak azt kell belátnunk, hogy p rendelkezik a prímtulajdonsággal.

Ha $p \mid ab$, akkor $\frac{p}{(p,a)} \mid b$. Mivel p felbonthatatlan, $(p, a) \sim 1$ vagy $(p, a) \sim p$.
Az első esetben $p \mid b$, a második esetben $p \mid a$.

□

Példa.

A $\mathbb{Z}\left[\sqrt{-5}\right]$ gyűrűben a 2 irreducibilis, de nem prím:

$$2 \mid (1 + \sqrt{-5})(1 - \sqrt{-5}), \text{ de } \quad 2 \nmid 1 + \sqrt{-5} \quad \text{és} \quad 2 \nmid 1 - \sqrt{-5}.$$

Gauss-gyűrűk

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

5.37. 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, hogy $a = p_1 \cdot \ldots \cdot p_n$; 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 $p_i \sim q_{i\pi}$ $(i = 1, \ldots, n)$.

5.38. Tétel.

Minden euklideszi gyűrű Gauss-gyűrű.

5.39. Megjegyzés.

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

Gauss-gyűrűk

5.40. Következmény.

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

5.41. Megjegyzés.

Ha megvizsgáljuk az 5.38. Tétel bizonyítását, megfigyelhetjük, hogy az irreducibilis felbontás létezése azon múlik, hogy nem létezik végtelen leszálló lánc az oszthatóság szerinti „rendezésben":

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

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

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

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

Gauss-gyűrűk

5.42. Tétel.

Legyen R Gauss-gyűrű, és legyen $a, b \in R$ prímfelbontása

$$a \sim p_1^{\alpha_1} \cdot \ldots \cdot p_n^{\alpha_n} \text{ és } b \sim p_1^{\beta_1} \cdot \ldots \cdot p_n^{\beta_n}.$$

Ekkor teljesülnek az alábbiak:

(1) $a \mid b \iff \alpha_i \leq \beta_i \;\; (i = 1, \ldots, n)$;

(2) $\text{lnko}\,(a, b) \sim p_1^{\min(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\min(\alpha_n, \beta_n)}$;

(3) $\text{lkkt}\,(a, b) \sim p_1^{\max(\alpha_1, \beta_1)} \cdot \ldots \cdot p_n^{\max(\alpha_n, \beta_n)}$.

100. feladat. Fejezze be az 5.42. Tétel bizonyítását.