

MBLK13E: Polinomok
(előadásvázlat, 2023. március 6.)

Kátai-Urbán Kamilla

1. Definíció. A T test fölötti egyhatározatlanú polinomok az

$$a_0 + a_1x + \cdots + a_nx^n \quad (a_i \in T)$$

formális kifejezések, amelyek halmazát $T[x]$ -el jelöljük. (Szokás a polinomokra az együtthatóikból álló sorozatként is gondolni.) Ha $a_{i+1} = a_{i+2} = \cdots = a_n = 0$, akkor az $a_0 + a_1x + \cdots + a_nx^n$ és $a_0 + a_1x + \cdots + a_ix^i$ polinomokat egyenlőknek tekintjük (tehát a zéró együtthatós tagokat figyelmen kívül hagyjuk). Az $a \in T$ elemeket **konstans polinomoknak** hívjuk.

2. Definíció. Legyen T test. Az $f = a_0 + a_1x + \cdots + a_nx^n \in T[x]$ polinom **polinomfüggvényén** az

$$f(c) = \sum_{i=0}^n a_i c^i \quad (c \in T)$$

képlet szerint definiált $f(x) : T \rightarrow T$ leképezést értjük.

3. Példa. A $\mathbb{Z}_2$ test feletti $f = \bar{0}$ és $g = x + x^2$ polinomokra $f \neq g$ de $f(x) = g(x)$. Azonban tetszőleges $f, g \in \mathbb{R}[x]$ polinomokra $f = g$ akkor és csak akkor, ha $f(x) = g(x)$.

4. Definíció. Legyen T tetszőleges test és

$$f = a_0 + a_1x + \cdots + a_nx^n \in T[x], \quad g = b_0 + b_1x + \cdots + b_mx^m \in T[x].$$

Az f és g polinomok **összegén** az

$$f + g = \sum_{i=0}^{\max(n,m)} (a_i + b_i)x^i,$$

polinomot értjük, ahol $a_i = 0$, illetve $b_i = 0$ értendő, ha $i > n$, illetve $i > m$. Az f és g **szorzatán** az

$$fg = \sum_{i=0}^{n+m} \left(\sum_{j=0}^i a_j b_{i-j} \right) x^i.$$

polinomot értjük.

5. Definíció. Ha az $f = a_0 + a_1x + \cdots + a_nx^n \in T[x]$ polinomban $a_n \neq 0$, akkor az n számot az f polinom **fokszámának** és az a_n elemet az f polinom **főegyütthatójának** hívjuk. Az f polinomot **főpolinomnak** nevezzük, ha f főegyütthatója $1 \in T$. Tehát a 0 polinomnak nincsen fokszáma (se főegyütthatója), de kényelmes lesz bevezetni a következő jelölést:

$$\deg f = \begin{cases} f \text{ fokszáma,} & \text{ha } f \neq 0, \\ -\infty, & \text{ha } f = 0. \end{cases}$$

6. Tétel. Legyen T tetszőleges test és $f, g \in T[x]$. Ekkor

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

7. Tétel. Tetszőleges T test esetén $T[x]$ kommutatív egységelemes gyűrűt alkot az előbb definiált műveletekkel, amit a **T test feletti egyhatározatlanú polinomgyűrűnek** hívunk. Tetszőleges T test esetén $T[x]$ zérusosztómentes is, tehát $T[x]$ integritástartomány.

1. POLINOMOK „SZÁMELMÉLETE”

1.1. Oszthatóság

8. Definíció. Legyen T tetszőleges test és $f, g \in T[x]$. Azt mondjuk, hogy f osztója g -nek, vagy g többszöröse f -nek, és azt írjuk, hogy $f \mid g$, ha van olyan $k \in T[x]$ polinom, amelyre $fk = g$.

9. Definíció. Tetszőleges T test feletti $T[x]$ polinomgyűrű esetén **egységeknek** nevezzük azokat a polinomokat, amelyek tetszőleges polinomnak osztói.

10. Tétel. Tetszőleges T test feletti $T[x]$ polinomgyűrűben teljesülnek a következő oszthatósági tulajdonságok, bármely $f, g, h \in T[x]$:

- (1) $f \mid f$,
- (2) ha $f \mid g$ és $g \mid h$, akkor $f \mid h$,
- (3) $1 \mid f$ és $f \mid 0$,
- (4) $0 \mid f$ akkor és csak akkor, ha $f = 0$,
- (5) ha $f \mid g$ és $f \mid h$, akkor $f \mid g \pm h$,
- (6) ha $f \mid g$ és $h \mid k$, akkor $fh \mid gk$,
- (7) ha $h \neq 0$ és $fh \mid gh$, akkor $f \mid g$.
- (8) ha $f \mid g$ és $g \neq 0$, akkor $\deg f \leq \deg g$.

11. Definíció. Az f és g polinomok **asszociáltak**, ha $f \mid g$ és $g \mid f$, amelyet a $\sim$ relációval jelölünk.

12. Példa. $\mathbb{Z}_3[x]$ -ben $\bar{2}x^3 + x + \bar{2} \sim x^3 + \bar{2}x + \bar{1}$, valamint $\mathbb{R}[x]$ -ben $6x^2 + 2x + 1 \sim x^2 + \frac{1}{3}x + \frac{1}{6}$.

13. Tétel. Az asszociáltság ekvivalenciareláció $T[x]$ -en.

14. Tétel. Tetszőleges $f, g \in T[x]$ esetén $f \sim g$ pontosan akkor, ha létezik $c \in T \setminus \{0\}$, melyre $f = cg$.

1.2. Legnagyobb közös osztó, Euklideszi algoritmus

15. Definíció. A h polinom az f, g polinomok **legnagyobb közös osztója**, ha teljesülnek a következők

- (lnko1) $h \mid f$ és $h \mid g$ (azaz közös osztó), és
- (lnko2) bármely k polinomra, ha $k \mid f$ és $k \mid g$, akkor $k \mid h$ (azaz minden közös osztónak a többszöröse).

Hasonlóan, a h polinom az f, g polinomok **legkisebb közös többszöröse**, ha

- (lkkt1) $f \mid h$ és $g \mid h$ (azaz közös többszörös), és
- (lkkt2) bármely k polinomra, ha $f \mid k$ és $g \mid k$, akkor $h \mid k$ (azaz minden közös többszörösnek az osztója).

16. Tétel. A legnagyobb közös osztó (és a legkisebb közös többszörös) asszociáltság erejéig egyértelműen meghatározott. Tehát, ha h az f és g polinomok legnagyobb közös osztója, akkor h minden asszociáltja is legnagyobb közös osztó és rajtuk kívül nincs más legnagyobb közös osztó. Ez úgy is megfogalmazható, hogy f, g polinomok legnagyobb közös osztói (legkisebb közös többszörösei) teljes asszociáltsági osztályt alkotnak.

17. Jelölés. Az f és g polinomok legnagyobb közös osztója $\sim$ erejéig meghatározott (ld. előző tétel). Az **lnko**(f, g) jelöli az lnko-k osztályából a főpolinomot, vagy a 0-t abban az esetben, ha az a legnagyobb közös osztó. Hasonlóan használjuk a legkisebb közös többszörös esetén az **lkkt**(f, g) jelölést.

18. Definíció. Az f és g polinomok **relatív prímek**, ha $\text{lnko}(f, g) = 1$.

19. Tétel (Maradékos osztás). Legyen T test, $f, g \in T[x]$ és $g \neq 0$. Ekkor léteznek olyan egyértelműen meghatározott $q, r \in T[x]$ polinomok, amelyekre $f = qg + r$ és $\deg r < \deg g$.

20. Definíció. Az előző tételben szereplő f polinomot **osztandónak**, g -t **osztónak**, q -t **hányadosnak** és r -t **maradéknak** nevezzük.

21. Tétel (Euklideszi algoritmus). Bármely két $f, g \in T[x]$ polinomnak van legnagyobb közös osztója, amely az alábbi euklideszi algoritmussal megkapható. Az $r_0 = f$ és $r_1 = g$ polinomokon végrehajtott euklideszi algoritmus maradékos osztások ismételt elvégzését jelenti:

$$\begin{aligned} r_0 &= q_1 r_1 + r_2 & (\deg r_2 < \deg r_1) \\ r_1 &= q_2 r_2 + r_3 & (\deg r_3 < \deg r_2) \\ &\vdots & \vdots \\ r_{n-2} &= q_{n-1} r_{n-1} + r_n & (\deg r_n < \deg r_{n-1}) \\ r_{n-1} &= q_n r_n + r_{n+1} & (r_{n+1} = 0). \end{aligned}$$

Az eljárás véges számú lépés után véget ér, azaz létezik olyan $n \in \mathbb{N}$, hogy $r_{n+1} = 0$. Ekkor a legnagyobb közös osztó az utolsó nemnulla maradék, azaz $\text{lko}(f, g) \sim r_n$. Az eljárás során kapott egyenleteket visszafejtve olyan u és v polinomokat kapunk, hogy $\text{lko}(f, g) = fu + gv$.

22. Példa. Euklideszi algoritmus segítségével meghatározzuk $\text{lko}(f, g)$ -t, ahol $f, g \in \mathbb{Z}_5[x]$, $f = 2x^4 + 3x^3 + 3x^2 + 2x$, $g = x^3 + 3x + 1$. A maradékos osztások elvégzésével kapjuk:

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

Így: $\text{lko}(f, g) = x + 4$.

23. Tétel. Bármely $f, g, h \in T[x]$ polinomra teljesülnek az alábbiak.

- (1) $\text{lko}(f, f) \sim f$,
- (2) $\text{lko}(f, g) = \text{lko}(g, f)$,
- (3) $\text{lko}(\text{lko}(f, g), h) = \text{lko}(f, \text{lko}(g, h))$,
- (4) $\text{lko}(f, g) \sim f$ akkor és csak akkor, ha $f \mid g$
- (5) $\text{lko}(f + gh, g) = \text{lko}(f, g)$,
- (6) $\text{lko}(f, g) \cdot h \sim \text{lko}(fh, gh)$,
- (7) ha $\text{lko}(f, g) \neq 0$, akkor $\text{lko}(f/\text{lko}(f, g), g/\text{lko}(f, g)) = 1$.

24. Tétel. Tetszőleges $f, g \in T[x]$ polinomoknak létezik legkisebb közös többszöröse, és

$$\text{lkt}(f, g) \text{lko}(f, g) \sim fg.$$

25. Következmény. Bármely $f, g, h \in T[x]$ polinomra teljesülnek az alábbiak.

- (1) ha $\text{lko}(f, h) = 1$ és $f \mid gh$, akkor $f \mid g$;
- (2) ha $\text{lko}(f, h) = 1$, akkor $\text{lko}(f, gh) = \text{lko}(f, g)$.

1.3. Diofantoszi egyenlet, kongruencia

26. Tétel. Tetszőleges adott $f, g, h \in T[x]$ polinomok esetén az $fu + gv = h$ diofantoszi egyenlet akkor és csak akkor oldható meg az $u, v \in T[x]$ ismeretlenekre nézve, ha $\text{lko}(f, g) \mid h$. Ha u_0, v_0 egy megoldás, akkor az általános megoldás

$$u = u_0 + \frac{g}{\text{lko}(f, g)} \cdot t, \quad v = v_0 - \frac{f}{\text{lko}(f, g)} \cdot t,$$

ahol $t \in T[x]$ tetszőlegesen választható.

27. Példa. Megoldjuk az $fu + gv = h$ diofantoszi egyenletet, ahol $f, g, h \in \mathbb{Z}_5[x]$, $f = 2x^4 + 3x^3 + 3x^2 + 2x$, $g = x^3 + 3x + 1$ és $h = 2x^2 + 4x + 4$. A 22. Példában megadtuk, hogy $\text{lko}(f, g) \sim x + 4$. A diofantoszi egyenlet megoldható, ugyanis $h = 2x^2 + 4x + 4 = (2x + 1)(x + 4)$, így az előző tételben megadott feltétel teljesül. A 22. Példában szereplő euklideszi algoritmus lépéseinél kifejezzük a maradékot:

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

Az utolsó egyenlőségtől indulva behelyettesítjük az előző sorban szereplő különbséget, és a zárójeleket felbontjuk úgy, hogy f és g polinomok többszöröseinek összege szerepeljen:

$$\begin{aligned} x + \bar{4} &= x^3 + \bar{3}x + \bar{1} - (\bar{3}x + \bar{1})(\bar{2}x^2 + x + \bar{2}) = \\ &= x^3 + \bar{3}x + \bar{1} - (\bar{3}x + \bar{1})[\bar{2}x^4 + \bar{3}x^3 + \bar{3}x^2 + \bar{2}x - (\bar{2}x + \bar{3})(x^3 + \bar{3}x + \bar{1})] = \\ &= (\bar{2}x^4 + \bar{3}x^3 + \bar{3}x^2)(\bar{2}x + \bar{4}) + (x^3 + \bar{3}x + \bar{1})(x^2 + x + \bar{4}) \end{aligned}$$

A cél az, hogy az $fu + gv = h$ diofantoszi egyenletet megoldjuk, ahogy korábban már láttuk a h többszöröse a legnagyobb közös osztónak ($h = \bar{2}x^2 + \bar{4}x + \bar{4} = (\bar{2}x + 1)(x + \bar{4})$), így $\bar{2}x + 1$ -gyel szorozva az előző egyenlőséget megkapjuk a diofantoszi egyenlet egy megoldását:

$$\bar{2}x^2 + \bar{4}x + \bar{4} = (\bar{2}x^4 + \bar{3}x^3 + \bar{3}x^2)(\bar{4}x^2 + \bar{4}) + (x^3 + \bar{3}x + \bar{1})(\bar{2}x^3 + \bar{3}x^2 + \bar{4}x + \bar{4}).$$

Így az általános megoldás:

$$u = \bar{4}x^2 + \bar{4} + \frac{x^3 + \bar{3}x + \bar{1}}{x + \bar{4}} \cdot t, \quad v = \bar{2}x^3 + \bar{3}x^2 + \bar{4}x + \bar{4} - \frac{\bar{2}x^4 + \bar{3}x^3 + \bar{3}x^2}{x + \bar{4}} \cdot t,$$

ahol $t \in \mathbb{Z}_5[x]$ tetszőlegesen választható.

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

29. Példa. Az $x^2 + 5x$ polinom kongruens $3x$ -szel modulo $x + 2$ az $\mathbb{R}[x]$ polinomgyűrűben, ugyanis $(x^2 + 5x) - 3x = x^2 + 2x = (x + 2)x$. Tehát $x + 2 \mid (x^2 + 5x) - 3x$ teljesül.

30. Állítás. Két polinom akkor és csak akkor kongruens modulo m , ha ugyanazt a maradékot adják m -mel osztva.

31. Következmény. A mod m kongruencia ekvivalenciareláció $T[x]$ -en, és bármely ekvivalenciaosztály pontosan egy m -nél kisebb fokszámú polinomot tartalmaz: az osztály (közös) m -mel vett maradékát.

32. Tétel. Bármely $f, g, h, k \in T[x]$ és $m \in T[x] \setminus \{0\}$ esetén, ha

$$f \equiv g \pmod{m}, \quad h \equiv k \pmod{m},$$

akkor

$$f + h \equiv g + k \pmod{m}, \quad fh \equiv gk \pmod{m}.$$

Jelölje a modulo m maradékosztályok halmazát $T[x]/\langle m \rangle$, és az f -et tartalmazó maradékosztályt $\bar{f}$. Ekkor az $\bar{f} + \bar{g} = \overline{f + g}$, $\bar{f} \cdot \bar{g} = \overline{fg}$ műveletek jóldefiniáltak $T[x]/\langle m \rangle$ -en.

33. Megjegyzés. A modulo m maradékosztályokat általában az egyetlen deg m -nél kisebb fokszámú polinommal reprezentáljuk. Az összes legfeljebb deg $m - 1$ -ed fokú polinom reprezentál 1-1 osztályt, ezek az osztályok $T[x]/\langle m \rangle$ elemei.

34. Példa. A $\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1} \rangle$ elemei $\bar{0}$, $\bar{1}$, $\bar{x}$, $\overline{x + \bar{1}}$. A műveletek pedig a következőképpen végezhetők: $\bar{x} + x + \bar{1} = \overline{x + x + \bar{1}} = \bar{1}$ és $\bar{x} \cdot \bar{x} = \overline{x^2} = \overline{x + \bar{1}}$, ugyanis $x^2 \equiv x + 1 \pmod{x^2 + x + \bar{1}}$ a $\mathbb{Z}_2[x]$ gyűrűben.

35. Tétel. $(T[x]/\langle m \rangle; +, \cdot)$ egységelemes, kommutatív gyűrű.

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

Speciálisan $fu \equiv 1 \pmod{m}$ megoldható $\iff \text{lko}(f, m) = 1$.

37. Következmény. Az $\bar{f}$ maradékosztálynak létezik multiplikatív inverze $T[x]/\langle m \rangle$ -ben $\iff \text{lko}(f, m) = 1$.

38. Példa. Meghatározzuk $\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1} \rangle$ -ben $\bar{x}$ multiplikatív inverzét, amennyiben létezik. Ehhez meg kell találnunk azt a legfeljebb elsőfokú $u \in \mathbb{Z}_2[x]$ polinomot, amelyre $x \cdot u \equiv 1 \pmod{x^2 + x + \bar{1}}$. Mivel a 34. Példában már meghatároztuk a $\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1} \rangle$ négy elemét, és kiszámoltuk $\bar{x} \cdot \bar{x}$ -et is, így látszik, hogy $u = x + 1$ lehet, ami tényleg megfelel. Ha ezt nem vesszük észre, akkor az $xu + (x^2 + x + 1)v = 1$ diofantoszi egyenlet megoldásával is megkapható u . Tehát $\bar{x}^{-1} = \overline{x + \bar{1}}$.

2. POLINOMOK GYÖKEI

39. Definíció. Az $f = \sum_{i=0}^n a_i x^i \in T[x]$ polinom **helyettesítési értéke** $c \in T$ helyen: $f(c) = a_n c^n + \dots + a_1 c + a_0$. A $c \in T$ elem **gyöke** (más szóval **zérushelye**) az $f \in T[x]$ polinomnak, ha $f(c) = 0$.

40. Tétel (Horner-módszer). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ egy n -edfokú polinom és $c \in T$. A Horner-módszerrel elkészített táblázat:

	a_n	a_{n-1}	$\dots$	a_1	a_0
c	b_{n-1}	b_{n-2}	$\dots$	b_0	$f(c)$

ahol

$$\begin{aligned} b_{n-1} &= a_n, \\ b_i &= b_{i+1} \cdot c + a_{i+1} \quad (i = n-2, \dots, 0). \end{aligned}$$

Ekkor

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

41. Tétel (Bézout tétele). Bármely $f \in T[x]$ és $c \in T$ esetén

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

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

43. Következmény. Tetszőleges $f \in T[x]$ n -edfokú polinomnak ($n \in \mathbb{N}_0$) legfeljebb n különböző gyöke van.

44. Definíció. Az $f \in T[x]$ polinomnak az $a \in T$ elem **k -szoros gyöke**, ha $(x - c)^k \mid f$, de $(x - c)^{k+1} \nmid f$. A $k \in \mathbb{N}$ számot az c gyök **multiplicitásának** nevezzük.

45.* Tétel. Alkalmazzuk a Horner-módszert az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomra és a $c \in T$ konstansra, majd egészítsük ki a táblázatot egy újabb, az előzőnél eggyel rövidebb sorral a szokásos Horner-módszer számolási szabályával. Folytassuk újabb, egyre rövidebb sorokkal, míg végül egy háromszög alakú táblázatot kapunk:

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

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

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

A táblázatból az is kiolvasható, hogy c hány-szoros gyöke f -nek: az a legkisebb k egész, amelyre $d_0 = d_1 = \dots = d_{k-1} = 0$ és $d_k \neq 0$.

46. Példa. Meghatározzuk, hogy hány-szoros gyöke az $f = x^5 + 4x^4 + 7x^3 + 13x^2 + 16x + 4 \in \mathbb{R}[x]$ polinomnak a -2 , és felírjuk f -et $x + 2$ polinomjaként. Alkalmazzuk a Horner-módszert f -re és a

$c = -2$ konstansra, amíg háromszög alakú táblázatot kapunk.

	1	4	7	13	16	4
-2	1	2	3	7	2	0
-2	1	0	3	1	0	
-2	1	-2	7	-13		
-2	1	-4	15			
-2	1	-6				
-2	1					

A táblázatból kiolvasható, hogy a -2 kétszeres gyöke f -nek, ugyanis a táblázatban az első két sor végén 0 szerepel, de a harmadik sor végén már nemnulla. Továbbá

$$f = x^5 + 4x^4 + 7x^3 + 13x^2 + 16x + 4 = (x+2)^5 - 6(x+2)^4 + 15(x+2)^3 - 13(x+2)^2 + 0(x+2) + 0.$$

3. IRREDUCIBILIS POLINOMOK

47. 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; az ilyen felbontást **triviális faktorizációnak** nevezzük.

48. Tétel. Legyen $p \in T[x]$. A p polinom akkor és csak akkor irreducibilis T felett, ha legalább elsőfokú, és nem bontható fel úgy két polinom szorzatára, hogy mindkét polinom fokszáma kisebb $\deg p$ -nél.

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

50. Tétel. A prím és irreducibilis polinomok megegyeznek.

51. Tétel. Legyen T tetszőleges test. Minden nemnulla $f \in T[x]$ polinom felírható, mégpedig a tényezők sorrendjétől eltekintve egyértelműen,

$$f = ap_1 \cdots p_n$$

alakban, ahol $a \in T \setminus \{0\}$ az f főegyütthatója, $p_1, \dots, p_n \in T[x]$ pedig irreducibilis főpolinomok.

52. Tétel. Bármely test felett minden elsőfokú polinom irreducibilis, és van gyöke.

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

54. Tétel. Bármely test feletti másod- vagy harmadfokú polinom akkor és csak akkor irreducibilis, ha nincs gyöke.

55. Tétel. Bármely test feletti legalább 4-ed fokú polinom ha irreducibilis, akkor nincs gyöke, de az implikáció megfordítása nem igaz.

56. Példa. A $\mathbb{Z}_2$ feletti legfeljebb harmadfokú polinomok felírásához egyrészt használhatjuk az 52. Tételt, tehát x és $x + \bar{1}$ irreducibilis. Másrészt a másod- és harmadfokú polinomok esetén az 54. Tétel alapján elég megvizsgálni, hogy van-e gyöke a polinomnak. Mivel az x^2 gyöke a $\bar{0}$ és $x^2 + \bar{1}$ -nek az $\bar{1}$, így $x^2 + x + \bar{1}$ az egyetlen másodfokú irreducibilis polinom $\mathbb{Z}_2$ felett. Hasonlóan megkapható, hogy a harmadfokú irreducibilisek $\mathbb{Z}_2$ felett $x^3 + x + \bar{1}$ és $x^3 + x^2 + \bar{1}$. Ügyeljünk arra, hogy a negyedfokú polinomok esetén már nem elég csak a gyökök vizsgálata (ld. 55. Tétel), például az $x^4 + x^2 + \bar{1}$ polinomnak nem gyöke sem a $\bar{0}$, sem az $\bar{1}$, de mégsem irreducibilis, ugyanis $x^4 + x^2 + \bar{1} = (x^2 + x + \bar{1})^2$.

3.1. Irreducibilis polinomok $\mathbb{C}$ és $\mathbb{R}$ felett

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

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

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

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

$$\begin{aligned} -a_{n-1} &= \alpha_1 + \alpha_2 + \dots + \alpha_n, \\ a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n, \\ &\vdots \\ (-1)^k a_{n-k} &= \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} \alpha_{i_1} \alpha_{i_2} \dots \alpha_{i_k}, \\ &\vdots \\ (-1)^n a_0 &= \alpha_1 \alpha_2 \dots \alpha_n. \end{aligned}$$

61. Tétel. Ha $f \in \mathbb{R}[x]$ és ha $f(z) = 0$ valamely $z \in \mathbb{C}$ komplex számra, akkor $f(\bar{z}) = 0$, ahol $\bar{z}$ a z komplex szám konjugáltját jelöli.

62. Következmény. Egy valós együtthatós polinom pontosan akkor irreducibilis $\mathbb{R}[x]$ -ben, ha elsőfokú, vagy olyan másodfokú polinom, amelynek nincs valós gyöke.

63. Következmény. Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

64. Példa. Felírjuk az $f = x^5 + 2x^3 - 8x$ polinomot irreducibilis polinomok szorzataként $\mathbb{C}[x]$ -ben, $\mathbb{R}[x]$ -ben és $\mathbb{Q}[x]$ -ben. Alakítsuk szorzattá az f polinomot.

$$f = x^5 + 2x^3 - 8x = x(x^4 + 2x^2 - 8) = x(x^2 - 2)(x^2 + 4) = x(x - \sqrt{2})(x + \sqrt{2})(x - 2i)(x + 2i)$$

Mivel minden tényező elsőfokú, így megkaptuk $\mathbb{C}[x]$ -ben az irreducibilis felbontást. A 61. Tétel alapján egy $f \in \mathbb{R}[x]$ polinom nem valós gyökei között mindig találunk konjugált párokat. Ezt felhasználva a $\mathbb{C}[x]$ -beli felbontásból általában úgy kapjuk az $\mathbb{R}$ feletti felbontást, ha a nem valós gyököknek megfelelő elsőfokú polinomokat megszorozzuk a konjugáltjának megfelelő elsőfokú polinommal. A mi esetünkben $(x - 2i)(x + 2i) = x^2 + 4$ teljesül, így az $\mathbb{R}$ feletti irreducibilis felbontás:

$$f = x(x - \sqrt{2})(x + \sqrt{2})(x^2 + 4).$$

Mivel $\pm\sqrt{2} \notin \mathbb{Q}$, így az irreducibilis felbontás $\mathbb{Q}[x]$ -ben:

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

3.2. Irreducibilis polinomok $\mathbb{Q}$ felett

65. Definíció. Az $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinom primitív, ha $\text{luko}(a_n, \dots, a_1, a_0) = 1$.

66. Tétel. Bármely $f \in \mathbb{Q} \setminus \{0\}$ polinom előáll rf^* alakban, ahol $r \in \mathbb{Q} \setminus \{0\}$ és $f^* \in \mathbb{Z}[x]$ primitív polinom, tehát $f \sim f^*$.

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

68. Tétel (Rolle tétele). Legyen $f = a_n x^n + \dots + a_1 x + a_0$ egész együtthatós polinom, azaz $f \in \mathbb{Z}[x]$. Ekkor f minden racionális gyöke $\frac{p}{q} \in \mathbb{Q}$ alakú (nem egyszerűsíthető tört), ahol $p \mid a_0$ és $q \mid a_n$. Speciálisan, egész együtthatós főpolinom racionális gyökei mind egész számok.

69. Következmény. A legfeljebb harmadfokú $\mathbb{Q}[x]$ -beli polinomokról eldönthető, hogy irreducibilisek-e.

70. Példa. Eldöntjük az $f = 3x^3 - 7x^2 + 17x - 5$ polinomról, hogy irreducibilis-e $\mathbb{Q}[x]$ -ben. Mivel f harmadfokú polinom, ha nem irreducibilis, akkor a felbontásában lennie kell elsőfokú $\mathbb{Q}[x]$ -beli polinomnak is, ami azt jelenti, hogy f -nek van racionális gyöke. A 68. Tétel alapján ha a $\frac{p}{q} \in \mathbb{Q}$ gyöke f -nek, akkor $p \mid -5$ és $q \mid 3$, így $\frac{p}{q}$ lehetséges értékei $1, -1, \frac{1}{3}, -\frac{1}{3}, 5, -5, \frac{5}{3}, -\frac{5}{3}$. Mivel $f(1) = 13 \neq 0$ és $f(-1) = -17 \neq 0$, így az 1 és a -1 nem gyöke, a többi lehetséges gyök vizsgálatához használhatjuk a Horner-módszernél szereplő táblázatot.

	3	-7	17	-5
$\frac{1}{3}$	3	-6	15	0

A táblázatból leolvasható, hogy $f(\frac{1}{3}) = 0$, így az $\frac{1}{3}$ gyöke f -nek továbbá

$$f = \left(x - \frac{1}{3}\right)(3x^2 - 6x + 15).$$

Tehát az f polinom nem irreducibilis $\mathbb{Q}[x]$ -ben. A $g = 3x^2 - 6x + 15$ polinom diszkriminánsa $D = (-6)^2 - 4 \cdot 3 \cdot 15 < 0$, azaz g irreducibilis $\mathbb{R}[x]$ -ben, és így $\mathbb{Q}[x]$ -ben is. Tehát az f polinom egyetlen racionális gyöke az $\frac{1}{3}$.

71. Tétel (Schönemann-Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, amelyre $p \nmid a_n$, $p \mid a_{n-1}, \dots, p \mid a_1$, $p \mid a_0$ és $p^2 \nmid a_0$, akkor f irreducibilis $\mathbb{Q}[x]$ -ben.

72. Példa. Az $f = x^{102} + 14x^{78} - 56x^{65} + 42x^{11} - 28$ irreducibilis $\mathbb{Q}[x]$ -ben, mert a $p = 7$ prímszám kielégíti a 71. Tételben szereplő feltételeket.

73. Következmény. Tetszőleges fokszámú irreducibilis polinom megadható $\mathbb{Q}[x]$ -ben. Például az $x^n - 2$ polinom bármely $n \in \mathbb{N}$ -re irreducibilis lesz $\mathbb{Q}[x]$ -ben, ugyanis $p = 2$ -re teljesülnek a 71. Tételben szereplő feltételek.

74. 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. A megfordítás helyett viszont teljesül a tétel „tükörképe”.

75. Tétel (Schönemann-Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre $p \nmid a_0$, $p \mid a_1, \dots, p \mid a_{n-1}$, $p \mid a_n$, és $p^2 \nmid a_n$, akkor f irreducibilis $\mathbb{Q}[x]$ -ben.

4. VÉGES TESTEK, EGYSZERŰ ALGEBRAI BŐVÍTÉS

Korábban a 32. Tételben definiáltunk polinom szerinti maradékosztályokon műveleteket, és így gyűrűket kaptunk. Most azt vizsgáljuk, hogy mikor lesznek ezek a gyűrűk testek.

76. Tétel. A $T[x]/\langle m \rangle$ gyűrű pontosan akkor test, ha m irreducibilis.

77. Példa. A 34. Példában a $\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1} \rangle$ maradékosztály-gyűrű elemeit meghatároztuk, illetve a 38. Példában megadtuk $\bar{x}$ multiplikatív inverzét. Van-e minden nemnulla elemnek multiplikatív inverze ebben a gyűrűben? Azaz teljesül-e, hogy ez a maradékosztály test? Az előző tétel alapján azt kell eldöntenünk, hogy $x^2 + x + \bar{1}$ irreducibilis-e $\mathbb{Z}_2$ felett. Mivel ez a polinom másodfokú, az 54. Tétel szerint elég azt vizsgálni, hogy van-e gyöke, ami a $\bar{0}, \bar{1}$ elemek behelyettesítésével eldönthető (ld. 56. Példa). Mivel egyik behelyettesítésnél sem kapunk $\bar{0}$ -át, így az $x^2 + x + \bar{1}$ polinom irreducibilis, azaz $\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1} \rangle$ test, tehát minden nemnulla elemnek van inverze.

78.* Tétel. Bármely p prím és $k \in \mathbb{N}$ esetén létezik $\mathbb{Z}_p[x]$ -ben k -adfokú irreducibilis polinom, tehát bármely prímszámra létezik ilyen elemszámú test. Továbbá, minden véges test elemszáma prímszám, ráadásul a p^k elemű testek mind izomorfak egymással.

79. Példa. Ahhoz, hogy például 8-elemű testet konstruáljunk, mivel $8 = 2^3$, így $\mathbb{Z}_2$ feletti 3-adfokú irreducibilis polinomot kell találnunk. Mivel nincs gyöke, az $x^3 + x + \bar{1}$ polinom megfelelő lesz (ld. 54. Tétel). Így megkaptuk a $\mathbb{Z}_2[x]/\langle x^3 + x + \bar{1} \rangle$ 8-elemű testet. Hasonlóan 8-elemű testet kaptunk volna, ha az $x^3 + x^2 + \bar{1}$ irreducibilis polinomot választjuk, és más harmadfokú irreducibilis polinom

nincs $\mathbb{Z}_2[x]$ -ben (ld. 56. Példa). Az előző tétel alapján $\mathbb{Z}_2[x]/\langle x^3 + x + \bar{1} \rangle \cong \mathbb{Z}_2[x]/\langle x^3 + x^2 + \bar{1} \rangle$ teljesül.

80. Definíció. Ha K, T olyan testek, melyre $T \subseteq K$ és a két testben a T -beli elemekkel ugyanúgy számolunk, akkor K **bővítése** T -nek.

81. Példa. Például a $\mathbb{Z}_2[x]/\langle x^3 + x + \bar{1} \rangle$ test bővítése a $\mathbb{Z}_2$ -nek.

82.* Tétel. Tetszőleges T test és $m \in T[x]$ irreducibilis polinom esetén létezik T -nek olyan K bővítése, melyre

- (1) létezik K -ban olyan α elem, amely gyöke m -nek (mint K feletti polinomnak);
- (2) K minden eleme egyértelműen előáll $a_n \alpha^n + \dots + a_1 \alpha + a_0$ alakban, ahol $a_i \in T$, $n = \deg m - 1$.
Ekkor K a T **egyszerű algebrai bővítése**, és $T(\alpha)$ jelöli.

83. Példa. Tekintsük az $m = x^2 + 1 \in \mathbb{R}[x]$ irreducibilis polinomot. Mivel m másodfokú, ezért a lehetséges maradékok legfeljebb elsőfokúak, azaz

$$\mathbb{R}[x]/\langle x^2 + 1 \rangle = \{ \overline{ax + b} : a, b \in \mathbb{R} \}.$$

A 32. Tételben definiált műveleteket erre az esetre felírva kapjuk, hogy

$$\begin{aligned} \overline{ax + b} + \overline{cx + d} &= \overline{(a + c)x + (b + d)}, \\ \overline{ax + b} \cdot \overline{cx + d} &= \overline{(ac)x^2 + (ad + bc)x + bd} = \overline{(ad + bc)x + (bd - ac)}. \end{aligned}$$

Ha azonosítjuk az $\overline{ax + b}$ maradékosztályt az $ai + b$ komplex számmal, akkor a számolási szabályok $\mathbb{R}[x]/\langle m \rangle$ -ben lényegében ugyanazok mint a komplex számok esetében, ezért

$$\mathbb{R}[x]/\langle x^2 + 1 \rangle \cong \mathbb{C}.$$

Az előző tétel alapján $\mathbb{C}$ az $\mathbb{R}$ egyszerű algebrai bővítése, ugyanis az $x^2 + 1$ polinomnak $\mathbb{C}$ felett gyöke i és $\mathbb{C}$ minden eleme előáll $a_1 i + a_0$ alakban, ahol $a_0, a_1 \in \mathbb{R}$.

5. LAGRANGE INTERPOLÁCIÓ

A Bézout-tétel (41. Tétel) néhány következménye.

84. Következmény. Ha $f, g \in T[x]$ olyan legfeljebb n -edfokú polinomok, amelyek helyettesítési értéke legalább $n + 1$ helyen megegyezik, akkor $f = g$.

85. Következmény. Ha T végtelen test, akkor különböző $T[x]$ -beli polinomok polinomfüggvénye is különböző.

86. Tétel (Lagrange interpolációs tétele). Legyen T számtest, $(c_1, d_1), \dots, (c_n, d_n) \in T^2$, és tegyük fel, hogy a c_i -k páronként különböznek. Ekkor létezik pontosan egy $L \in T[x]$ legfeljebb $n - 1$ -edfokú polinom, amelyre $L(c_1) = d_1, \dots, L(c_n) = d_n$. Ez az L polinom a következő:

$$L = \sum_{i=1}^n \frac{(x - c_1) \dots (x - c_{i-1})(x - c_{i+1}) \dots (x - c_n)}{(c_i - c_1) \dots (c_i - c_{i-1})(c_i - c_{i+1}) \dots (c_i - c_n)} \cdot d_i.$$

Az L polinomot a $c_1, \dots, c_n$ alappontokhoz tartozó **Lagrange-féle interpolációs polinomnak** nevezzük.

87. Megjegyzés. Ha $T = \mathbb{R}$, akkor az L által meghatározott polinomfüggvény grafikonja a $(c_1, d_1), \dots, (c_n, d_n)$ pontokon megy át.

88. Példa. Meghatározzuk a $(-1, 1), (-2, 4), (-3, -7)$ pontokra illeszkedő L Lagrange-polinomot. A Lagrange-féle interpolációs polinom a következő tagokból áll:

$$\begin{aligned} L_1 &= \frac{(x - (-2))(x - (-3))}{(-1 - (-2))(-1 - (-3))} \cdot 1 = \frac{1}{2} \cdot (x^2 + 5x + 6), \\ L_2 &= \frac{(x - (-1))(x - (-3))}{(-2 - (-1))(-2 - (-3))} \cdot 4 = (-4) \cdot (x^2 + 4x + 3), \\ L_3 &= \frac{(x - (-1))(x - (-2))}{(-3 - (-1))(-3 - (-2))} \cdot (-7) = \left(-\frac{7}{2}\right) \cdot (x^2 + 3x + 2). \end{aligned}$$

Tehát $L = L_1 + L_2 + L_3 = -7x^2 - 24x - 16$.

6. POLINOM DERIVÁLTJA

89. Definíció. Tetszőleges T test és $f = \sum_{i=0}^n a_i x^i \in \mathbb{C}[x]$ polinom esetén f deriváltja az $f' = \sum_{i=1}^n i a_i x^{i-1} \in \mathbb{C}[x]$ polinom.

90. Tétel. Legyen $f \in \mathbb{C}[x]$ és $k \in \mathbb{N}$. Ha c komplex szám k -szoros gyöke f -nek, akkor $(k-1)$ -szeres gyöke f' -nak. (Speciálisan, ha $k=1$, akkor c nem gyöke f' -nak.)

91. Következmény. Tetszőleges $f \in \mathbb{C}[x]$ nemzérus polinom esetén a c komplex szám akkor és csak akkor többszörös gyöke f -nek, ha $f(c) = f'(c) = 0$.

92. Következmény. Legyen T számtest, és $f \in T[x]$ nemzérus polinom. Az $\text{lko}(f, f')$ polinom gyökei pontosan az f polinom többszörös gyökei, mégpedig 1-gyel kisebb multiplicitással, mint f -ben.

93. Példa. Az $f = x^6 - 2x^5 - 2x^4 + 2x^3 + x^2 + 4x + 4$ polinom többszörös gyökeinek megkereséséhez, először meghatározzuk az f' polinomot: $f' = 6x^5 - 10x^4 - 8x^3 + 6x^2 + 2x + 4$. Ezután kiszámítjuk a legnagyobb közös osztót (pl. euklidesz algoritmussal), $\text{lko}(f, f') = x^2 - x - 2$. Ennek a polinomnak már egyszerűen meg tudjuk határozni a gyökeit, $x_1 = -1$, $x_2 = 2$, ezek az f polinom többszörös gyökei. Mivel egyszeres gyökei a legnagyobb közös osztónak, így f -nek kétszeres gyökei. Ez segíthet f összes gyökének meghatározásában is, hiszen ha ezen c gyökök esetén $x - c$ -vel leosztjuk f -et a multiplicitást is figyelembe véve (pl. Horner-elrendezéssel), akkor már egy másodfokú polinomot kapunk, $x^2 + 1$ -et, amelynek gyökei könnyen meghatározhatók. Tehát f gyökei multiplicitással felírva: $-1, -1, 2, 2, i, -i$.

94. Megjegyzés. Ügyeljünk arra, hogy 90. Tétel megfordítva nem igaz, azaz ha egy $f \in \mathbb{C}[x]$ polinom esetén f' -nak egy c komplex szám $k-1$ -szeres gyöke, akkor nem biztos, hogy f -nek k -szoros gyöke. Tekintsük az előző példát, ahol két többszörös gyöke volt az f 6-odfokú polinomnak, amelyek már csak 1-szeres gyökei f' -nak (f többi gyöke pedig nem gyöke f' -nak). De f' ötödfokú, tehát multiplicitással számolva 5 gyöke van $\mathbb{C}$ -ben, azaz jelentek meg olyan gyökök is, amelyek nem gyökei f -nek. Ezért van szükségünk az $\text{lko}(f, f')$ -ra, hogy f többszörös gyökeit meg tudjuk határozni, és nem elég csak f' gyökeit vizsgálni.