

MTNM312E: Polinomok
(előadásvázlat, 2023. november 23.)

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

6. 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:

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

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

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

8. Definíció. Az R gyűrűt **zérusosztómentesnek** nevezzük, ha bármely két 0-tól különböző elem szorzata 0-tól különböző.

9. Példa. A testek zérusosztómentes gyűrűt alkotnak. NEM zérusosztómentes gyűrű például a $\mathbb{Z}_6$, ugyanis $\bar{2} \cdot \bar{3} = \bar{0}$.

10. Következmény. Tetszőleges T test esetén $T[x]$ zérusosztómentes.

1.1. Oszthatóság

11. 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 $fk = g$.

12. 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) $f \mid g$ és $g \mid f$ akkor és csak akkor, ha $f = cg$ valamely $c \in T \setminus \{0\}$ elemre,
- (4) $1 \mid f$
- (5) $f \mid 0$,
- (6) $f \mid 1$ akkor és csak akkor, ha $f \in T \setminus \{0\}$,
- (7) $0 \mid f$ akkor és csak akkor, ha $f = 0$,
- (8) ha $f \mid g$ és $f \mid h$, akkor $f \mid g \pm h$,
- (9) ha $f \mid g$, akkor $f \mid gh$,
- (10) ha $h \neq 0$, akkor $f \mid g$ akkor és csak akkor, ha $fh \mid gh$.
- (11) ha $f \mid g$ és $g \neq 0$, akkor $\deg f \leq \deg g$.

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

14. 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 $6x^2 + 2x + 1 \sim x^2 + \frac{1}{3}x + \frac{1}{6}$.

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

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

17. Definíció. Tetszőleges T test feletti $T[x]$ polinomgyűrű esetén az $f \in T[x]$ polinomot egységeknek nevezzük, ha $f \sim 1$ (vagy, ami ezzel ekvivalens: $f \mid 1$).

18. Tétel. Tetszőleges T test feletti $T[x]$ polinomgyűrű esetén az egységek a nemnulla konstans polinomok.

1.2. Legnagyobb közös osztó, Euklideszi algoritmus

19. 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).

20. 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.

21. Jelölés. Az f és g polinomok legnagyobb közös osztója $\sim$ erejéig meghatározott (ld. előző tétel). Az $\text{lnko}(f, g)$ 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 $\text{lkkt}(f, g)$ jelölést.

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

23. 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 $\deg r < \deg g$.

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

25. 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:

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

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 $\text{lko}(f, g) = fu + gv$.

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

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

Így: $\text{lko}(f, g) = x + \bar{4}$.

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

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

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

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

1.3. Diofantoszi egyenlet

29. 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.

30. Példa. Megoldjuk az $fu + gv = h$ diofantoszi egyenletet, ahol $f, g, h \in \mathbb{Z}_5[x]$, $f = \bar{2}x^4 + \bar{3}x^3 + \bar{3}x^2 + \bar{2}x$, $g = x^3 + \bar{3}x + \bar{1}$ és $h = \bar{2}x^2 + \bar{4}x + \bar{4}$. A 26. Példában megadtuk, hogy $\text{lko}(f, g) \sim x + \bar{4}$. A diofantoszi egyenlet megoldható, ugyanis $h = \bar{2}x^2 + \bar{4}x + \bar{4} = (\bar{2}x + 1)(x + \bar{4})$, így az előző tételben

megadott feltétel teljesül. A 26. Példában szereplő euklideszi algoritmus lépéseinél kifejezzük a maradékot:

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

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 ($h = \bar{2}x^2 + \bar{4}x + \bar{4} = (\bar{2}x + \bar{1})(x + \bar{4})$), így $\bar{2}x + \bar{1}$ -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.

2. POLINOMOK GYÖKEI

31. 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 $f(c) = 0$.

32. 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

$$f = (x - c) \cdot (b_{n-1}x^{n-1} + \dots + b_1x + b_0) + f(c).$$

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

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

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

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

36. 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.

37.* 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}	$\cdots$	a_2	a_1	a_0
c				$\cdots$			d_0
c				$\cdots$			d_1
c				$\cdots$			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 $d_n = a_n$):

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

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

38. Példa. Meghatározzuk, hogy hányszoros 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

39. 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.

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

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

42. Tétel. A prím és irreducibilis polinomok megegyeznek.

43. 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.

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

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

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

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

48. Példa. A $\mathbb{Z}_2$ feletti legfeljebb harmadfokú polinomok felírásához egyrészt használhatjuk az 44. Tételt, tehát x és $x + \bar{1}$ irreducibilis. Másrészt a másod- és harmadfokú polinomok esetén az 46. 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. 47. 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

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

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

51. 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**.

52. Tétel (Viète-formulák). Legyenek az n -edfokú $f = x^n + a_{n-1}x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ főpolinom gyökei $\alpha_1, \dots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása). Ekkor fennállnak a következő összefüggések:

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

53. 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.

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

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

56. 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 53. 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 polinnal. 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

57. 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.

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

59. Példa. Eldöntjük az $f = 3x^3 - 7x^2 + 17x - 5$ polinomról, hogy irreducibilise-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 57. 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 $\frac{1}{3}$.

60.* Tétel. Egy legalább elsőfokú egész együtthatós polinom pontosan akkor nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, ha $\mathbb{Q}$ felett sem bomlik így fel.

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

62. Példa. Az $f = x^{102} + 14x^{78} - 56x^{65} + 42x^{11} - 28$ irreducibilis $\mathbb{Q}[x]$ -ben, mert a $p = 7$ prímszám kielégíti a 61. Tételben szereplő feltételeket.

63. 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 61. Tételben szereplő feltételek.

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

65. 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. LAGRANGE INTERPOLÁCIÓ

A Bézout-tétel (33. Tétel) néhány következménye.

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

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

68. 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.

69. 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.

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

$$L_1 = \frac{(x - (-2))(x - (-3))}{(-1 - (-2))(-1 - (-3))} \cdot 1 = \frac{1}{2} \cdot (x^2 + 5x + 6),$$

$$L_2 = \frac{(x - (-1))(x - (-3))}{(-2 - (-1))(-2 - (-3))} \cdot 4 = (-4) \cdot (x^2 + 4x + 3),$$

$$L_3 = \frac{(x - (-1))(x - (-2))}{(-3 - (-1))(-3 - (-2))} \cdot (-7) = \left(-\frac{7}{2}\right) \cdot (x^2 + 3x + 2).$$

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

5. POLINOM DERIVÁLTJA

71. 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.

72. 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.)

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

74. Következmény. Legyen $f \in \mathbb{C}[x]$ nemzérus polinom. Az $\text{lko}(f, f')$ polinom gyökei pontosan az f polinom többszörös gyökei, mégpedig 1-gyel kisebb multiplicitással, mint f -ben.

75. 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. euklideszi 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: $-1, -1, 2, 2, i, -i$.

76. Megjegyzés. Ügyeljünk arra, hogy 72. 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.

6. POLINOM SZERINTI MARADÉKOSZTÁLYOK, VÉGES TESTEK

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

78. 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.

79. Állítás. Legyen $m \in T[x] \setminus \{0\}$. Két $T[x]$ -beli polinom akkor és csak akkor kongruens modulo m , ha ugyanazt a maradékot adják m -mel osztva.

80. Tétel. A mod m kongruencia ekvivalenciareláció $T[x]$ -en (azaz reflexív, szimmetrikus és tranzitív). Bármely $f, g, h, k \in T[x]$ és $m \in T[x] \setminus \{0\}$ esetén, ha

$$f_1 \equiv g_1 \pmod{m}, \quad f_2 \equiv g_2 \pmod{m},$$

akkor

$$f_1 + f_2 \equiv g_1 + g_2 \pmod{m}, \quad f_1 f_2 \equiv g_1 g_2 \pmod{m}.$$

81. Definíció. Legyen $f \in T[x]$ és $m \in T[x] \setminus \{0\}$. Az $f \in T[x]$ polinom modulo m maradékosztályán az $\bar{f} = \{g \in T[x] : f \equiv g \pmod{m}\}$ halmazt értjük (vagyis az f polinomnak a modulo m kongruenciareláció szerinti ekvivalenciaosztályát). Jelölje $T[x]/\langle m \rangle$ a modulo m maradékosztályok halmazát.

82. Definíció. A $T[x]/\langle m \rangle$ halmazon értelmezzük az összeadást és a szorzást a következőképpen: $\bar{f} + \bar{g} = \overline{f + g}$, $\bar{f} \cdot \bar{g} = \overline{fg}$.

83. Megjegyzés. Az hogy a fenti műveletek jól definiáltak hasonlóan látható be, mint a $\mathbb{Z}$ -n értelmezett maradékosztályok esetén. 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.

84. 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 $x^2 \equiv x + 1 \pmod{x^2 + x + 1}$ a $\mathbb{Z}_2[x]$ gyűrűben.

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

86. Definíció. Az $\bar{f}, \bar{g} \in T[x]/\langle m \rangle$ maradékosztályok egymás multiplikatív inverzei, ha $\bar{f} \cdot \bar{g} = \bar{1}$.

87. 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 $\iff \text{lko}(f, m) \sim 1$.

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

89. 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 84. 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 $\bar{x}^{-1} = \overline{x + \bar{1}}$.

90. Tétel. Legyen $m \in T[x]$ legalább elsőfokú polinom. A $T[x]/\langle m \rangle$ gyűrű pontosan akkor test, ha m irreducibilis.

91. Példa. A 84. Példában a $\mathbb{Z}_2[x]/\langle x^2 + x + \bar{1} \rangle$ maradékosztály-gyűrű elemeit meghatároztuk, illetve a 89. 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 46. Tétel szerint elég azt vizsgálni, hogy van-e gyöke, ami a $\bar{0}$, $\bar{1}$ elemek behelyettesítésével eldönthető (ld. 48. 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.

92.* Tétel. Bármely p prím és $k \in \mathbb{N}$ esetén létezik $\mathbb{Z}_p[x]$ -ben k -adfokú irreducibilis polinom, tehát bármely p^k prímszámra létezik ilyen elemszámú test. Továbbá teljesül, hogy minden véges test elemszáma prímszám.

93. 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. 46. 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. 48. Példa).

7. SZIMMETRIKUS POLINOMOK

94. Definíció. Adott T test feletti **n -határozatlanú monomnak** nevezzük az $ax_1^{k_1} \cdots x_n^{k_n}$ alakú formális kifejezéseket, ahol $0 \neq a \in T$ és $k_1, \dots, k_n \in \mathbb{N}_0$. Az ilyen monomok véges összegeit pedig T feletti **n -határozatlanú polinomoknak** nevezzük, és ezen polinomok halmazát $T[x_1, \dots, x_n]$ -nel jelöljük.

95. Tétel. A természetes módon definiált szorzással és összeadással $T[x_1, \dots, x_n]$ kommutatív, egységelemes zérusosztómentes gyűrűt alkot.

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

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

97. Példa. Például az $x_1x_2 + x_1 + x_2 + 2$ polinom 2-határozatlanú szimmetrikus polinom, $x_1^3 + x_2^3 + x_3^3$ 3-határozatlanú szimmetrikus polinom.

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

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \dots < i_k \leq n} x_{i_1} \cdot x_{i_2} \cdot \dots \cdot x_{i_k} \in T[x_1, \dots, x_n].$$

99. Példa.

- A 2-határozatlanú elemi szimmetrikus polinomok: $\sigma_1 = x_1 + x_2$, $\sigma_2 = x_1x_2$.
- A 3-határozatlanú elemi szimmetrikus polinomok: $\sigma_1 = x_1 + x_2 + x_3$, $\sigma_2 = x_1x_2 + x_1x_3 + x_2x_3$, $\sigma_3 = x_1x_2x_3$.

100. Megjegyzés. Az elemi szimmetrikus polinomokkal már találkoztunk: segítségükkel fejezhetők ki egy komplex együtthatós főpolinom együtthatói a polinom gyökeiből, ezek az 52. Tételben szereplő Viète-formulák. A tételben a k -adik egyenlet bal oldalán $(-1)^k a_{n-k}$ áll, a jobb oldalon pedig az $\alpha_1, \dots, \alpha_n$ betűkből képezett összes k -tényezős szorzat összege:

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

Tehát a Viète-formulák $(-1)^k a_{n-k} = \sigma_k(\alpha_1, \dots, \alpha_n)$ alakban is felírhatók a korábbi jelölés segítségével.

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

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

102. Példa. Az $f = (x_1 + 1)(x_2 + 1)$ 2-változós szimmetrikus polinomot a következőképpen fejezhetjük ki elemi szimmetrikus polinomok polinomjaként:

$$(x_1 + 1)(x_2 + 1) = x_1x_2 + x_1 + x_2 + 1 = \sigma_2 + \sigma_1 + 1 = h(\sigma_1, \sigma_2),$$

ahol $h = x_2 + x_1 + 1$.

103. Példa. Az $f = (x_1 - x_2)^2$ 2-változós polinomot ki tudjuk fejezni elemi szimmetrikusok polinomjaként:

$$(x_1 - x_2)^2 = (x_1 + x_2)^2 - 4x_1x_2 = \sigma_1^2 - 4\sigma_2 = h(\sigma_1, \sigma_2),$$

ahol $h = x_1^2 - 4x_2$.

104. Definíció. Legyen $f \in \mathbb{C}[x]$ n -ed fokú főpolinom, ahol $n \geq 2$. Ekkor f **diszkriminánsa**:

$$D = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2,$$

ahol $\alpha_1, \dots, \alpha_n$ az f polinom gyökei.

105. Példa. Tekintsük az $f = x^2 + bx + c$ másodfokú komplex együtthatós főpolinomot, melynek gyökeit jelölje α_1, α_2 . A 103. Példa felhasználásával $(\alpha_1 - \alpha_2)^2$, azaz f diszkriminánsa, előállítható elemi szimmetrikusok segítségével. Továbbá a 100. Megjegyzésben szerepelt, hogy a Viète-formulák éppen a gyökökből képzett elemi szimmetrikusok és az együtthatók közötti kapcsolatot írják le. Így kapjuk f diszkriminánsára a következőt:

$$D = (\alpha_1 - \alpha_2)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = (\sigma_1(\alpha_1, \alpha_2))^2 - 4\sigma_2(\alpha_1, \alpha_2) = (-b)^2 - 4c = b^2 - 4c,$$

ami a jól ismert diszkrimináns képlettel egyezik meg $a = 1$ esetén.

8. ALGEBRAI ÉS TRANZSCENDENS SZÁMOK

106. Definíció. Az α komplex számot **algebrai számnak** nevezzük, ha gyöke valamely nemzéró racionális együtthatós polinomnak. A nem algebrai számokat **transzcendens számoknak** nevezzük.

107. Példa. A $\sqrt{2}$ szám algebrai szám, gyöke például az $x^3 - 2x \in \mathbb{Q}[x]$ polinomnak. Az i szám algebrai szám, gyöke az $x^2 + 1 \in \mathbb{Q}[x]$ polinomnak. A π és az e szám esetén nem találunk olyan racionális együtthatós polinomot, aminek gyöke lenne, így π és e transzcendens szám (ennek igazolása nem könnyű).

108.* Tétel (Gelfond-Schneider-tétel). Ha $\alpha \neq 0$, 1 és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám.

109. Példa. Az előző tételből következik, hogy $3^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{3}}$ és $i^{\sqrt{5}}$ transzcendens számok.

110. 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 **minimálpolinomjának** nevezzük.

111. Tétel. Algebrai szám minimálpolinomja mindig egyértelműen meghatározott, és irreducibilis a racionális számtest felett.

112. Példa. A 107. Példában $\sqrt{2}$ esetén megadott $x^3 - 2x$ polinom nem minimálpolinomja $\sqrt{2}$ -nek, mert nem irreducibilis. A $\sqrt{2}$ szám minimálpolinomja $x^2 - 2$, i minimálpolinomja pedig $x^2 + 1$.

113. Definíció. Az $(S; +, \cdot)$ a $(T; +; \cdot)$ test részteste, ha

- (1) $S \subseteq T$;
- (2) $0, 1 \in S$;
- (3) S zárt a négy alapműveletre:
 - (i) $\forall a, b: a + b \in S$;
 - (ii) $\forall a, b: a - b = a + (-b) \in S$;
 - (iii) $\forall a, b: a \cdot b \in S$;
 - (iv) $\forall a, b: a/b = a \cdot b^{-1}$, ha $b \neq 0$.

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

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

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

117. Tétel. A gyökmennyiségek algebrai számok.

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

119. Példa. Az $x^5 - 4x + 2 = 0$ egyenlet gyökei nem gyökmennyiségek, ezért ennek az egyenletnek még „ad hoc” megoldóképlete sincs.

120. Következmény. Az ötödfokú egyenleteknek nincs általános megoldóképlete.

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

9. HARMAD- ÉS NEGYEDFOKÚ EGYENLETEK

122. Történet. A harmad- és negyedfokú egyenletek megoldóképletének története:

- Scipione del Ferro megoldja a harmadfokú egyenlet bizonyos típusait, de módszerét titokban tartja.
- 1526: del Ferro a halálos ágyán elárulja a titkot tanítványának, Fiornak, a jegyzetfüzetét pedig vejére bízta.
- 1535: Fior és Niccolo Fontana Tartaglia versenye. Tartaglia megoldja Fior összes feladványát, Fior viszont egyet sem old meg teljesen.
- 1539: Girolamo Cardano (nagy nehezen) kiszedi Tartagliából a módszert.
„Esküszöm Önnek az Úr Szent Evangéliumára, és nem csak egy igaz ember szavát adom Önnek, hogy soha nem publikálom az Ön felfedezését, ha rám bízta, de ígérem azt is, és legyen igaz keresztény lelkiismeretem az Ön biztosítéka, hogy oly módon titkosítom, hogy halálom után senki sem tudja majd elolvasni a feljegyzetteket. Ha Ön úgy gondolja, hogy megérdemlem a bizalmat, akkor tegye meg nekem ezt a szívességet, ha pedig nem, akkor fejezzük be ezt a beszélgetést.”
- 1539: Cardano tovább vizsgálja a harmadfokú egyenleteket, felfedezi a casus irreduciblist.
- 1540: Lodovico Ferrari megoldja a negyedfokú egyenletet, de nem publikálhatja Cardano fogadalma miatt.
- 1543: Cardano és Ferrari Bolognába utazik, és del Ferro veje megmutatja nekik a jegyzetfüzetet.
- 1545: Cardano kiadja Ars Magna című művét, benne a harmadfokú egyenlet megoldásával, hivatkozva del Ferro és Tartaglia munkájára. Tartaglia esküszegéssel vádolja Cardanot.
- 1548: Tartaglia nem akar Ferrarival megküzdeni, Cardano pedig Tartagliával nem akar. Tartaglia egy jó állás reményében mégis elfogadja Ferrari kihívását, de alulmarad, és az éj leple alatt megszökik.

9.1. Harmadfokú egyenletek

123. 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

$$x^3 + px + q = 0 \quad (p, q \in \mathbb{C})$$

alakú egyenletet kapunk.

124. 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 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):

$$u + v, \quad u\varepsilon + v\bar{\varepsilon}, \quad u\bar{\varepsilon} + v\varepsilon,$$

ahol ε primitív harmadik egységgyök.

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

$$\underbrace{\sqrt[3]{10 + 6\sqrt{3}}}_u + \underbrace{\sqrt[3]{10 - 6\sqrt{3}}}_v$$

Tehát ebben az esetben pozitív szám van a négyzetgyök alatt. A két köbgyök három-három értéke (figyelni kell a párbaállításra: $u_i v_i = -2$):

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

Tehát az egyenlet megoldásai:

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

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

$$\underbrace{\sqrt[3]{2 + \sqrt{-121}}}_u + \underbrace{\sqrt[3]{2 - \sqrt{-121}}}_v = \underbrace{\sqrt[3]{2 + 11i}}_u + \underbrace{\sqrt[3]{2 - 11i}}_v$$

Tehát ebben az esetben a négyzetgyök alatt negatív szám van (casus irreducibilis).

A $\sqrt[3]{2 + 11i}$ köbgyökvonást elvégezni nem könnyű. Vegyük észre, hogy $(2 + i)^3 = 2 + 11i$. Tehát az egyenlet megoldásai:

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

127. Megjegyzés. A 104. Definícióban megadtuk a diszkrimináns definícióját. Másodfokú polinom esetén a diszkrimináns meghatározásához először a 103. Példában megadtuk a különbség négyzetét elemi szimmetrikus polinomok segítségével. Ezt harmadfokú esetben a következőképpen tehetjük meg:

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

Másodfokú polinom esetén a 105. Példában adtuk meg a diszkriminánszt. Ha az $x^3 + px + q$ harmadfokú polinomot tekintjük, és gyökeit $\alpha_1, \alpha_2, \alpha_3$ jelöli, akkor a Viète-formulák a következők: $\sigma_1(\alpha_1, \alpha_2, \alpha_3) = 0$, $\sigma_2(\alpha_1, \alpha_2, \alpha_3) = p$, $\sigma_3(\alpha_1, \alpha_2, \alpha_3) = -q$. Tehát a diszkrimináns ebben az esetben:

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

128.* Tétel. A valós együtthatós $x^3 + px + q$ harmadfokú polinom valós, illetve nemvalós gyökeinek száma a D diszkrimináns előjelétől függ az alábbi módon:

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

9.2. Negyedfokú egyenletek. Tekintsük az $f = x^4 + ax^3 + bx^2 + cx + d \in \mathbb{C}[x]$ negyedfokú polinomot, és vegyük a $g = x^2 + \frac{a}{2}x + \alpha$ polinomot, ahol α komplex paraméter. Ekkor $g^2 = x^4 + ax^3 + \left(\frac{a^2}{4} + 2\alpha\right)x^2 + a\alpha x + \alpha^2$, és képezzük a $k = g^2 - f = \left(\frac{a^2}{4} + 2\alpha - b\right)x^2 + (a\alpha - c)x + (\alpha^2 - d)$ különbséget. Ha az α paramétert úgy választjuk meg, hogy k teljes négyzet legyen, azaz ha találunk olyan h legfeljebb elsőfokú polinomot, amelyre $k = h^2$, akkor $f = g^2 - h^2 = (g + h)(g - h)$ teljesül.

Így az f negyedfokú polinomot két másodfokú polinom szorzatára bontjuk, amelyeknek a komplex gyökeit meg tudjuk határozni. A k legfeljebb másodfokú polinom akkor lesz teljes négyzet, ha a $k = 0$ egyenlet diszkriminánsa 0, innen adódik a következő definícióban szereplő kubikus rezolvens.

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

130. Tétel (Ferrari módszere). 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

$$(1) \quad \left(\frac{a^2}{4} + 2\alpha - b \right) x^2 + (a\alpha - c)x + (\alpha^2 - d)$$

másodfokú polinom teljes négyzet, azaz valamely $h \in \mathbb{C}[x]$ legfeljebb elsőfokú polinom négyzete. A $g = x^2 + \frac{a}{2}x + \alpha$ 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.

131. Megjegyzés. A 129. Definícióban megadott kubikus rezolvenst α hatványaiként átírva a

$$(2) \quad -8\alpha^3 + 4b\alpha^2 + (8d - 2ac)\alpha + a^2d - 4bd + c^2 = 0$$

egyenletet kapjuk.

132. Példa. Megkeressük az $f = x^4 + 4x^3 - 6x^2 + 4x - 2$ polinom gyökeit. A (2) formula alapján a kubikus rezolvens α hatványaiként felírva:

$$-8\alpha^3 - 24\alpha^2 - 48\alpha - 64 = 0.$$

A 123. Állításban szereplő helyettesítés most $\beta = \alpha + 1$ alakú. A főegyütthatóval, -8 -cal, történő leosztás után a

$$\beta^3 + 3\beta + 4 = 0$$

egyenletet kapjuk, amelynek $\beta = -1$ egy megoldása, így $\alpha = -2$ megoldása a kubikus rezolvensnek. Ekkor az (1) polinom

$$6x^2 - 12x + 6 = (\sqrt{6}x - \sqrt{6})^2$$

alakú, tehát Ferrari módszerénél $h = \sqrt{6}x - \sqrt{6}$, továbbá $g = x^2 + 2x - 2$. Ekkor

$$f = (g + h)(g - h) = \left(x^2 + (2 + \sqrt{6})x - 2 - \sqrt{6} \right) \left(x^2 + (2 - \sqrt{6})x - 2 + \sqrt{6} \right).$$

A másodfokú egyenletek megoldásával megkapjuk a gyököket:

$$\frac{-2 - \sqrt{6} \pm \sqrt{18 + 8\sqrt{6}}}{2}, \quad \frac{-2 + \sqrt{6} \pm \sqrt{18 - 8\sqrt{6}}}{2}.$$

133. Megjegyzés. Érdekességként megadjuk a harmad- és negyedfokú egyenletek megoldóképletét.

Az $x^3 + ax^2 + bx + c = 0$ harmadfokú egyenlet megoldóképlete:

$$x = -\frac{a}{3} + \sqrt[3]{\frac{-2a^3 + 9ab - 27c + \sqrt{(2a^3 - 9ab + 27c)^2 + 4(-a^2 + 3b)^3}}{54}} + \sqrt[3]{\frac{-2a^3 + 9ab - 27c - \sqrt{(2a^3 - 9ab + 27c)^2 + 4(-a^2 + 3b)^3}}{54}}$$

Az $x^4 + ax^3 + bx^2 + cx + d = 0$ negyedfokú egyenlet megoldóképlete:

$$x = -\frac{a}{4} + \frac{1}{4} \sqrt[4]{\frac{27a^4 - 12a^2b^2 + 3b^4}{4}} + \frac{1}{4} \sqrt[4]{\frac{27a^4 - 12a^2b^2 + 3b^4}{4}} + \frac{1}{4} \sqrt[4]{\frac{27a^4 - 12a^2b^2 + 3b^4}{4}} + \frac{1}{4} \sqrt[4]{\frac{27a^4 - 12a^2b^2 + 3b^4}{4}}$$