Polinomok

(előadásvázlat, 2016. október 11.)

Maróti Miklós

Ennek az előadásnak a megértéséhez a következő fogalmakat kell tudni: gyűrű, gyűrű additív csoportja, zéruseleme, és multiplikatív félcsoportja, egységelemes és kommutatív gyűrű, test, generált részalgebra, egész számok

Az előadáshoz ajánlott jegyzet:

- Klukovits Lajos: *Klasszikus és lineáris algebra*, Polygon Kiadó, Szeged, 1999.
- Szendrei Ágnes: *Diszkrét matematika*, Polygon Kiadó, Szeged, 1994–2002.

1. Példa. A következő algebrai struktúrák gyűrűk:

(1) $(\mathbb{R}; +, \cdot)$, $(\mathbb{Q}; +, \cdot)$, $(\mathbb{C}; +, \cdot)$, és általában minden test,
(2) $(\mathbb{Z}; +, \cdot)$, $(\mathbb{P}; +, \cdot)$ ahol $\mathbb{P} = \{\, 2a : a \in \mathbb{Z} \,\}$,
(3) $(\mathbb{Z}_n; +, \cdot)$ (modulo n maradékosztályok),
(4) $(P(U); \triangle, \cap)$ tetszőleges U halmazra.
(5) $(T^{n\times n}; +, \cdot)$ tetszőleges T testre,
(6) $(R^{n\times n}; +, \cdot)$ tetszőleges kommutatív R gyűrűre,
(7) test feletti egyváltozós polinomok.

2. Tétel. *Tetszőleges kommutatív, egységelemes R gyűrűben teljesülnek a következő tulajdonságok:*

(1) $0 \cdot a = a \cdot 0 = 0$ *ahol* 0 *az* R *gyűrű zéruseleme,*
(2) $(-a)b = a(-b) = -(ab)$,
(3) $(a_1 + \cdots + a_m)(b_1 + \cdots + b_n) = \sum_{i=1}^{m} \sum_{j=1}^{n} a_i b_j$ *(általános disztributivitás),*
(4) $(a + b)^n = \sum_{i=0}^{n} \binom{n}{i} \cdot a^i b^{n-i}$ *(binomiális tétel).*

3. Definíció. A T test fölötti egyhatározatlanú polinomok az

$$a_0 + a_1 x + \cdots + a_n x^n \quad (a_i \in T)$$

formális kifejezések, amelyek halmazát $T[x]$-el jelöljük. Ha $a_{i+1} = a_{i+2} = \cdots = a_n = 0$, akkor az $a_0 + a_1 x + \cdots + a_n x^n$ és $a_0 + a_1 x + \cdots + a_i x^i$ polinomokat egyenlőknek tekintjük (tehát a kezdő zéró együtthatós tagokat figyelmen kívül hagyjuk). Az $a \in T$ elemeket konstans polinomoknak hívjuk.

4. Definíció. Legyen T test. Az $f = a_0 + a_1 x + \cdots + a_n x^n \in T[x]$ polinom polinomfüggvényén az

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

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

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

6. Definíció. Legyen T tetszőleges test és

$$f = a_0 + a_1 x + \cdots + a_n x^n \in T[x], \qquad g = b_0 + b_1 x + \cdots + b_m x^m \in T[x].$$

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.

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

8. 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:

$$\deg f = \begin{cases} f \text{ fokszáma}, & \text{ha } f \neq 0, \\ -1, & \text{ha } f = 0. \end{cases}$$

9. Tétel. *Legyen T tetszőleges test és $f, g \in T[x]$ nemzéró polinomok. Ekkor*

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

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

11. Következmény. *Tetszőleges T test esetén $T[x]$ zérusosztómentes.*

12. Tétel. *Tetszőleges zérusosztómentes R gyűrűben teljesülnek a következő ún. kancellatív tulajdonságok:*

(1) *ha $ac = bc$ és $c \neq 0$, akkor $a = b$,*
(2) *ha $ab = ac$ és $a \neq 0$, akkor $b = c$.*

13. 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 $h \in T[x]$ polinom, amelyre $fh = g$.

14. Tétel. *Tetszőleges T test feletti $T[x]$ polinomgyűrűben teljesülnek a következő oszthatósági tulajdonságok:*

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

15. Definíció. Az f és g polinomok asszociáltak, ha $f|g$ és $g|f$, amelyet az $\sim$ relációval jelölünk.

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

17. Következmény. *Az asszociáltság ekvivalenciareláció a polinomok halmazán. A 0 polinomhoz semelyik másik polinom sem asszociált. A $\{0\}$ osztályt kivéve minden asszociáltsági osztályban pontosan egy főpolinom van.*

18. Definíció. A h polinom az f, g polinomok legnagyobb közös osztója, ha

(1) $h \mid f$ és $h \mid g$ (azaz közös osztó), és
(2) ha $p \mid f$ és $p \mid g$, akkor $p \mid h$ (azaz minden közös osztónak a többszöröse).

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

(1) $f \mid h$ és $g \mid h$ (azaz közös többszörös), és
(2) ha $f \mid p$ és $g \mid p$, akkor $h \mid p$ (azaz minden közös többszörösnek az osztója).

19. 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.*

20. Definíció. Az f és g polinomok legnagyobb közös osztóját $\operatorname{lnko}(f, g)$-vel jelöljük, és általában nem azt írjuk, hogy $h = \operatorname{lnko}(f, g)$, hanem azt, hogy $h \sim \operatorname{lnko}(f, g)$. Hasonlóan a legkisebb közös többszöröst $\operatorname{lkkt}(f, g)$-vel jelöljük.

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

22. Tétel. *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 $\deg r < \deg g$. Ezt a műveletet maradékos osztásnak nevezzük, ahol f az osztandó, g az osztó, q a hányados és r a maradék.*

23. Tétel (Euklideszi algoritmus). *Bármely két $f, g \in T[x]$ polinomnak van legnagyobb közös osztója, amely a következő maradékos osztások elvégzésével megkapható:*

$$\begin{aligned} f &= q_1 g + r_2 && (\deg r_2 < \deg g) \\ g &= q_2 r_2 + r_3 && (\deg r_3 < \deg r_2) \\ r_2 &= q_3 r_3 + r_4 && (\deg r_4 < \deg r_3) \\ &\vdots && \vdots \\ r_{i-1} &= q_i r_i + r_{i+1} && (\deg r_{i+1} < \deg r_i) \end{aligned}$$

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

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

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

Így a legnagyobb közös osztó: $\operatorname{lnko}(f, g) \sim x + \overline{4}$.

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

(1) $\operatorname{lnko}(\operatorname{lnko}(f, g), h) \sim \operatorname{lnko}(f, \operatorname{lnko}(g, h))$,
(2) $\operatorname{lnko}(f, g) \sim \operatorname{lnko}(g, f)$,
(3) $\operatorname{lnko}(f, g) \sim f \iff f \mid g$,
(4) $\operatorname{lnko}(f, f) \sim f$,
(5) $\operatorname{lnko}(0, f) \sim f$,
(6) $\operatorname{lnko}(1, f) \sim 1$,
(7) $\operatorname{lnko}(f, g) \sim 0 \iff f = g = 0$,
(8) $\operatorname{lnko}(f, g) \sim \operatorname{lnko}(f + gh, g)$,
(9) $\operatorname{lnko}(f, g) \cdot h \sim \operatorname{lnko}(fh, gh)$,
(10) $\operatorname{lnko}(f, g) \neq 0 \implies \operatorname{lnko}(f / \operatorname{lnko}(f, g), g / \operatorname{lnko}(f, g)) \sim 1$
(11) $\operatorname{lnko}(f, g) \sim 1 \implies \operatorname{lnko}(f, gh) \sim \operatorname{lnko}(f, h)$.

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

(1) *ha* $\operatorname{lnko}(f, g) \sim 1$, $f \mid h$ *és* $g \mid h$, *akkor* $fg \mid h$;
(2) *ha* $\operatorname{lnko}(f, g) \sim 1$ *és* $f \mid gh$, *akkor* $f \mid h$;
(3) *ha* $\operatorname{lnko}(f, g) \neq 0$ *és* $f \mid gh$, *akkor* $f / \operatorname{lnko}(f, g) \mid h$.

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

$$\operatorname{lnko}(f, g) \cdot \operatorname{lkkt}(f, g) \sim fg.$$

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

$$u = u_0 + \frac{g}{\operatorname{lnko}(f, g)} \cdot t, \qquad v = v_0 - \frac{f}{\operatorname{lnko}(f, g)} \cdot t,$$

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

29. Példa. Megoldjuk az $fu + gv = h$ diofantoszi egyenletet, ahol $f, g, h \in \mathbb{Z}_5[x]$, $f = \overline{2}x^4 + \overline{3}x^3 + \overline{3}x^2 + \overline{2}x$, $g = x^3 + \overline{3}x + \overline{1}$ és $h = \overline{2}x^2 + \overline{4}x + \overline{4}$. A 24. példában megadtuk, hogy $\operatorname{lnko}(f, g) \sim x + \overline{4}$. A diofantoszi egyenlet megoldható, ugyanis $h = \overline{2}x^2 + \overline{4}x + \overline{4} = (\overline{2}x + 1)(x + \overline{4})$, így az előző tételben megadott feltétel teljesül. A 24. példában szereplő euklideszi algoritmus lépéseinél kifejezzük a maradékot:

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

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

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

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

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

Így az általános megoldás:

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

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

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

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

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

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

	a_n	a_{n-1}	$\cdots$	a_1	a_0
c	b_n	b_{n-1}	$\cdots$	b_1	b_0

ahol

$$b_n = a_n,$$
$$b_i = b_{i+1} \cdot c + a_i \qquad (i = n-1, \ldots, 0).$$

Ekkor 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:

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

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

34. Tétel. *Alkalmazzuk a Horner-módszert az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinomra és a $c \in T$ 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		
$\vdots$	$\vdots$	$\vdots$	$\vdots$	$\iddots$			
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 $d_k \neq 0$.

35. 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, továbbá

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

36. 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.

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

38. Tétel. *A prím és irreducibilis polinomok megegyeznek.*

39. 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, $p_1, \ldots, p_n \in T[x]$ pedig irreducibilis főpolinomok.

40. Tétel. *Bármley test felett minden elsőfokú polinom irreducibilis.*

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

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

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

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

45. Következmény. *Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_nx^n + \cdots + a_1x + a_0 \in \mathbb{C}[x]$ ahol $a_n \neq 0$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, akkor $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük az f polinom gyöktényezős felbontásának.*

46. Tétel. *Ha $f \in \mathbb{R}[x]$ és ha $f(z) = 0$ valamely $z \in \mathbb{C}$ komplex számra, akkor $f(\bar{z}) = 0$.*

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

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

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

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

50. Tétel (Rolle tétele). *Legyen $f = a_nx^n + \cdots + a_1x + a_0$ egész együtthatós polinom, azaz $f \in \mathbb{Z}[x]$. Ekkor f minden racionális gyöke $\frac{p}{q} \in \mathbb{Q}$ alakú, ahol $p \mid a_0$ és $q \mid a_n$. Speciálisan, egész együtthatós főpolinom racionális gyökei mind egész számok.*

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

52. Példa. Eldöntjük az $f = 3x^3 - 7x^2 + 17x - 5$ polinomról, hogy irreduciblis-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 50. 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 $\frac{1}{3}$.

53. Tétel (Schönemann-Eisenstein-féle irreducibilitási kritérium). *Legyen $f = a_n x^n + \dots + a_1 x + a_0$ egész együtthatós polinom, azaz $f \in \mathbb{Z}[x]$. 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.*

54. Példa. Az $f = x^{102} + 14x^{78} - 56x^{65} + 42x^{11} - 28$ irreducibilis $\mathbb{Q}[x]$-ben, mert a $p = 7$ prímszám kielégíti a 53. tételben szereplő feltételeket.

55. Megjegyzés. 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 53. tételben szereplő feltételek.

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

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