

MBX114E: Diszkrét matematika III.

(előadásvázlat, 2007. május 22.)

Maróti Miklós

6. POLINOMOK

A diszkrét matematika I és II tárgyakból 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.

6.1. 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) $(P(U); \Delta, \cap)$ 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.

6.2. Tétel. Tetszőleges 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) $(a_1 + \dots + a_m)(b_1 + \dots + b_n) = \sum_{i=1}^m \sum_{j=1}^n a_i b_j$ (általános disztributivitás),
- (4) $(a + b)^n = \sum_{i=0}^n \binom{n}{i} \cdot a^i b^{n-i}$ (binomiális tétel).

6.3. Definíció. A **T test fölötti egyhatározatlanú polinomok** az

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

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

6.4. Definíció. Legyen T test. Az $f = a_0 + a_1x + \dots + a_nx^n \in T[x]$ 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.

6.5. 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 $f(x) = g(x)$.

6.6. Definíció. Legyen T tetszőleges test és

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

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.

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

6.8. Tétel. *Tetszőleges T testre a $T[x]$ polinomgyűrűt a konstanspolinomok és az x polinom generálja. A konstanspolinomok a T testtel izomorf résztestet alkotnak $T[x]$ -ben.*

6.9. Definíció. Ha az $f = a_0 + a_1x + \dots + a_nx^n \in T[x]$ 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:

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

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

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

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

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

6.13. 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 $b = c$.

6.14. 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 $fh = g$.

6.15. 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 $\deg f \leq \deg g$.

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

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.*

6.18. 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).

6.19. 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.

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

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

6.22. 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**.

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

$$\begin{array}{ll} f = q_1g + r_1 & (\deg r_1 < \deg g) \\ g = q_2r_1 + r_2 & (\deg r_2 < \deg r_1) \\ r_1 = q_3r_2 + r_3 & (\deg r_3 < \deg r_2) \\ \vdots & \vdots \\ r_{i-1} = q_{i+1}r_i + r_{i+1} & (\deg r_{i+1} < \deg r_i) \end{array}$$

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 $\text{lnko}(f, g) \sim r_n$. Az eljárás során kapott egyenleteket visszafejtve olyan u és v polinomokat kapunk, hogy $\text{lnko}(f, g) = fu + gv$.

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

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

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

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

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

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

6.27. 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 $\text{luko}(f, g) \mid h$. Ha u_0, v_0 egy megoldás, akkor az általános megoldás

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

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

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

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

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

6.30. Tétel (Horner-módszer). Legyen $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ egy n -edfokú polinom és $c \in T$. Ha a Horner-módszerrel elkészített táblázat alsó sorában álló számok $b_n, \dots, b_1, b_0$, azaz

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

akkor b_0 nem más, mint az f -nek az $x - c$ polinommal való osztásakor keletkező maradék, $b_n x^{n-1} + \dots + b_2 x + b_1$ pedig ugyanezen osztás hányadosa:

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

6.31. 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.

6.32. 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 háányszoros gyöke f -nek: az a legkisebb k egész, amelyre $d_0 = d_1 = \dots = d_{k-1} = 0$ és $d_k \neq 0$.

6.33. Definíció. A $p \in T[x]$ polinom **irreducibilis**, ha legalább elsőfokú, és csak úgy bontható két polinom szorzatára, hogy az egyik tényező asszociált p -hez. Ekkor a másik tényező szükségképpen asszociált 1-hez; az ilyen felbontást **triviális faktorizációnak** nevezzük.

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

6.35. Tétel. A prím és irreducibilis polinomok megegyeznek.

6.36. Tétel. Legyen T tetszőleges test. Minden nemnulla $f \in T[x]$ polinom felírható, mégpedig a tényezőik 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.

6.37. Tétel. Bármely test felett minden elsőfokú polinom irreducibilis.

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

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

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

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

6.42. Következmény. Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ 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 $f = a_n(x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük az f polinom **gyöktényezős felbontásának**.

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

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

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

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

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

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

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

6.49. Tétel (Schönemann-Eisenstein-féle irreducibilitási kritérium). Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ 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.