

Test fölötti polinomgyűrűk 3.

Klukovits Lajos

TTIK Bolyai Intézet

2020. november 27.

Irreducibilis polinomok a $\mathbb{R}$ és $\mathbb{C}$ testek fölött.

Komplex eset.

Az algebra alaptételéből és Bezout tételéből következően pontosan az elsőfokú polinomok irreducibilisek a $\mathbb{C}$ test fölött.

Állítás.

Ha $f = a_n x^n + \dots + a_1 x + a_0 \in \mathbb{C}[x]$, $a_n \neq 0$, akkor léteznek olyan (nem feltétlenül különböző) $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ komplex számok, hogy $f = a_n(x - \alpha_1) \dots (x - \alpha_n)$. Ez azt is jelenti, hogy minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bontható a $\mathbb{C}[x]$ gyűrűben.

Viète-formulák/képletek.

Tétel.

Legyenek az $f = x^n + a_{n-1}x^{n-1} + \dots + a_1x + a_0 \in \mathbb{C}[x]$ n -edfokú főpolinom komplex gyökei (mindegyiket annyiszor föltüntetve, ahányszoros gyök) $\alpha_1, \dots, \alpha_n$. Ekkor érvényesek az alábbi egyenlőségek.

$$\begin{aligned} -a_{n-1} &= \alpha_1 + \dots + \alpha_n \\ a_{n-2} &= \alpha_1\alpha_2 + \alpha_1\alpha_3 + \dots + \alpha_{n-1}\alpha_n \\ -a_{n-3} &= \alpha_1\alpha_2\alpha_3 + \alpha_1\alpha_2\alpha_4 + \dots + \alpha_{n-2}\alpha_{n-1}\alpha_n \\ &\vdots \\ (-1)^{n-1}a_1 &= \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_{n-1} + \alpha_1\alpha_2 \dots \alpha_{n-2}\alpha_n + \\ &\quad \dots + \alpha_2\alpha_3 \dots \alpha_{n-1}\alpha_n \\ (-1)^na_0 &= \alpha_1\alpha_2 \dots \alpha_{n-1}\alpha_n. \end{aligned}$$

Alaptétel és közvetlen következményei.

A klasszikus algebra alaptétele (Gauss 1799.)

Ha $f \in \mathbb{C}[x]$, $\deg f \geq 1$, akkor van olyan $\alpha \in \mathbb{C}$, hogy $f(\alpha) = 0$.

Következmények.

- Ha $f \in \mathbb{R}[x]$ és $f(\alpha) = 0$ valamely $\alpha \in \mathbb{C}$ -re, akkor $f(\bar{\alpha}) = 0$, továbbá, α és $\bar{\alpha}$ multiplicitása megegyezik.
- A valós számtest fölötti irreducibilis polinomok legfőljebb másodfokúak.
- Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste fölött, ha elsőfokú, vagy olyan másodfokú polinom, amelynek nincs valós gyöke. Tehát az $\mathbb{R}$ fölött irreducibilis polinomok a következők:
 - $ax + b$ ($a, b \in \mathbb{R}$, $a \neq 0$);
 - $ax^2 + bx + c$ ($a, b, c \in \mathbb{R}$, $a \neq 0$, $b^2 - 4ac < 0$).

A következmények bizonyítása.

1. Következmény.

- $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{R}[x]$, $f(\alpha) = 0$, $\alpha \in \mathbb{C}$.
- $f(\bar{\alpha}) = a_n \bar{\alpha}^n + a_{n-1} \bar{\alpha}^{n-1} + \dots + a_1 \bar{\alpha} + a_0 = \overline{f(\alpha)} = \overline{0} = 0$

2. Következmény.

- Ha $f(\alpha) = 0$, $\alpha \in \mathbb{C} \setminus \mathbb{R}$, akkor $f(\bar{\alpha}) = 0$.
- Bezout tételéből: $(x - \alpha)(x - \bar{\alpha}) \mid f$, és
- $(x - \alpha)(x - \bar{\alpha}) = x^2 + (\alpha + \bar{\alpha})x + \alpha\bar{\alpha} \in \mathbb{R}[x]$.

Rádás.

Ha $f \in \mathbb{R}[x]$ páratlan fokszámú, akkor van valós zéróhelye.

- Ha $\deg f = n$, akkor multiplicitással számolva n számú gyöke van.
- Ha ezeket párokba soroljuk: mindegyikhez a konjugáltját, akkor
- legalább egy (vagy páratlan sok) gyöknek önmaga lesz a párja.

Irreducibilis polinomok $\mathbb{Q}$ fölött.

Definíció.

Az $a_n x^n + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot **primitív polinomnak** nevezzük, ha $\text{ln. k. o.}(a_0, \dots, a_n) = 1$.

Lemma.

Minden racionális együtthatós polinom fölbontható egy racionális szám és egy primitív polinom szorzatára, formálisan:

$$\forall f \in \mathbb{Q}[x] \exists r \in \mathbb{Q} \exists f^* \in \mathbb{Z}[x]: f = r f^* \text{ ahol } f^* \text{ primitív polinom.}$$

Tétel.

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható föl nála alacsonyabb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ fölött sem, és megfordítva.

Schönemann-Eisenstein-féle irreducibilitási kritérium.

Definíció.

Azt mondjuk, hogy a p prímszám **pontos osztója** az a egész számnak, ha $p \mid a$, de $p^2 \nmid a$. Jelölése: $p \parallel a$.

Tétel.

Legyen $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám, hogy $p \nmid a_n$, $p \mid a_i$ minden $0 \leq i \leq n-1$, és $p \nmid a_0$, akkor f irreducibilis a racionális számok teste fölött.

Megjegyzés.

Az előbbi tétel megfordítása nem igaz! Abból, hogy nem létezik a tételbeli feltételnek megfelelő prímszám, nem következik a polinom reducibilitása.

Következmény.

Minden $n \geq 1$ -re létezik $\mathbb{Q}$ fölött irreducibilis n -edfokú polinom.

Polinomok irreducibilis fölbontása.

Néhány tény.

- 1 Ha meg tudjuk határozni a zéróhelyeket, nincs nagy gond. DE erre nem létezik algoritmus, kivéve néhány egyszerű esetet.
- 2 A zéróhelyek ismerete nélkül még rosszabb a helyzet, csak próbálkozni lehet.

Egyszerű feladat.

Bontsuk irreducibilis tényezők szorzatára $\mathbb{R}$ és $\mathbb{C}$ fölött az $x^6 + 27$ polinomot.

- (1) A $\mathbb{C}$ fölötti fölbontás a gyöktényezős alak.
- (2) A gyökök: $\pm\sqrt{3}i$, $\pm\frac{3}{2} \pm \frac{\sqrt{3}}{2}i$.
- (3) $x^6 + 27 = (x - \sqrt{3}i)(x + \sqrt{3}i)(x - (-\frac{3}{2} + \frac{\sqrt{3}}{2}i))(x - (-\frac{3}{2} - \frac{\sqrt{3}}{2}i))(x - (\frac{3}{2} + \frac{\sqrt{3}}{2}i))(x - (\frac{3}{2} - \frac{\sqrt{3}}{2}i))$

Polinomok irreducibilis fölbontása.

Folytatás

A valós fölbontás 2-2 tényező (amelyekben konjugált gyökpárok szerepelnek) összeszorozásával kapható:

$$x^6 + 27 = (x^2 + 3)(x^2 - 3x + 3)(x^2 + 3x + 3).$$

Véges test fölötti polinomok irreducibilis fölbontása.

Legyen T a kételemű test.

(1) Irreducibilisek-e az alábbi polinomok a $T[x]$ polinomgyűrűben?

$$x^4 + 1, \quad x^3 + x^2 + 1, \quad x^4 + x + 1.$$

(2) Adja meg az összes legfőbb harmadfokú irreducibilis polinomot a $T[x]$ polinomgyűrűben.

(3) Bontsa föl irreducibilis tényezőkre az $x^7 + 1 \in T[x]$ polinomot.

Véges test fölötti polinomok irreducibilis fölbontása.

Megoldások 1.

(1) $x^4 + 1 = (x + 1)^4$, azaz nem irreducibilis.

- Az $x^3 + x^2 + 1$ polinom pontosan akkor reducibilis, ha van gyöke T -ben, de nincs, így irreducibilis.
- Az $x^4 + x + 1$ polinomnak nincs elsőfokú osztója, így csak két másodfokú tényezőre lehetne bontani.

$$\begin{aligned} x^4 + x + 1 &= (x^2 + ax + b)(x^2 + cx + d) \\ &= x^4 + (a + c)x^3 + (b + d + ac)x^2 + (ad + bc)x + bd \end{aligned}$$

$$a + c = 0$$

$$b + d + bc = 0$$

$$ad + bc = 1$$

$$bd = 1$$

- Az utóbbi egyenletrendszernek nincs megoldása T -ben,
- így a polinom irreducibilis.

Véges test fölötti polinomok irreducibilis fölbontása.

Megoldások 2.

(2) A másod- és harmadfokú polinomok közül azok irreducibilisek, amelyeknek nincs gyökük az alaptestben (az elsőfokúak nyilván mind irreducibilisek): x , $x + 1$, $x^2 + x + 1$, $x^3 + x^2 + 1$, $x^3 + x + 1$.

(3) Az 1 nyilván gyök, így

$$x^7 + 1 = (x + 1)(x^6 + x^5 + x^4 + x^3 + x^2 + x + 1)$$

- Tovább csak próbálgatásokkal haladhatunk. Másod- és harmadfokú irreducibilis osztókat kell keresnünk.
- $x^2 + x + 1 \mid x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, de
- $x^6 + x^5 + x^4 + x^3 + x^2 + x + 1 = (x^3 + x^2 + 1)(x^3 + x + 1)$,
- így a keresett fölbontás: $x^7 + 1 = (x + 1)(x^3 + x^2 + 1)(x^3 + x + 1)$.

Polinomok többszörös zéróhelyei.

Definíciók.

- 1 Azt mondjuk, hogy az $f \in F[x]$ polinomnak $\alpha \in F$ többszörös gyöke, ha $(x - \alpha)^2 | f$.
- 2 Az előbbi jelölésekkel: α k -szoros gyök, ha $(x - \alpha)^k | f$, de $(x - \alpha)^{k+1} \nmid f$.

Definíció.

Az $f = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 \in \mathbb{C}[x]$ polinom **deriváltján** az $f' = n a_n x^{n-1} + (n-1) a_{n-1} x^{n-2} + \dots + 2 a_2 x + a_1 \in \mathbb{C}[x]$ polinomot értjük.

Tétel.

Ha $k \geq 1$ egész, és az $\alpha \in \mathbb{C}$ k -szoros gyöke az f polinomnak, akkor α f' -nek $k-1$ -szeres gyöke. (Ha $k=1$, akkor α nem gyöke f' -nek.)

Polinomok többszörös zéróhelyei.

Bizonyítás.

- 1 Ha $f = (x - \alpha)^k g$, $g(\alpha) \neq 0$, akkor
- 2 $f' = k(x - \alpha)^{k-1} g + (x - \alpha)^k g' = (x - \alpha)^{k-1} (kg + (x - \alpha)g')$.

□

Következmények.

- 1 Az α komplex szám pontosan akkor többszörös gyöke az f polinomnak, ha gyöke az $\text{In. k. o.}(f, f')$ polinomnak.
- 2 Bármely legalább elsőfokú f polinomnak és az $\frac{f}{\text{In. k. o.}(f, f')}$ polinomnak ugyanazok a gyökei, csak az utóbbi polinom minden gyöke egyszeres.
- 3 Ha T egy számtest, azaz $\mathbb{C}$ egy részteste, és az $f \in T[x]$ polinom irreducibilis T -fölött, akkor f minden komplex gyöke egyszeres.

Polinomok közös zéróhelyei.

Egyszerű észrevételek.

- 1 Legyen $f, g \in F[x]$, $\alpha \in F$. Ha $f(\alpha) = g(\alpha) = 0$, akkor $x - \alpha | \text{In. k. o.}(f, g)$.
- 2 Két polinom közös zéróhelyei éppen legnagyobb közös osztójuknak zéróhelyei.
- 3 Két polinomnak pontosan akkor van közös zéróhelye, ha legnagyobb közös osztójuk legalább elsőfokú, azaz van legalább elsőfokú közös faktoruk.

Tétel.

Legyen $f, g \in F[x]$. E polinomoknak pontosan akkor van nem konstans közös faktora, közös zéróhelye, ha léteznek olyan $f_1, g_1 \in F$ fölötti polinomok, amelyekre $\deg f_1 < \deg f$, $\deg g_1 < \deg g$, és $f g_1 = g f_1$.

Polinomok közös zéróhelyei.

A tétel bizonyítása.

- 1 Legyen $d \sim \text{In. k. o.}(f, g)$, $\deg d > 0$. Ekkor az $f_1 = f/d$, $g_1 = g/d$ polinomokra teljesülnek a tétel feltételei.
- 2 Ha pedig léteznek a tételbeli f_1, g_1 polinomok és mégis $\text{In. k. o.}(f, g) \sim 1$, akkor az $f g_1 = g f_1$ egyenlőségből $f | f_1$, ami lehetetlen a fokszámra kirótt feltételek miatt.
- 3 Ezel a bizonyítás kész.