Irreducibilis polinomok

Polinomgyűrű maradékosztály-gyűrűje

Tétel.
Legyen T test, $m \in T[x]$ egy n-edfokú polinom ($n \geq 1$). Ekkor a modulo m maradékosztályok kommutatív egységelemes gyűrűt alkotnak.
Jelölés: $T[x]/(m)$.

A $T[x]/(m)$ gyűrű minden eleme egyértelműen felírható

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1 x + a_0} \quad (a_{n-1}, \ldots, a_0 \in T)$$

alakban. (Ha $T = \mathbb{Z}_p$, akkor $|T[x]/(m)| = p^n$.)

Egy kicsi példa

A $K := \mathbb{Z}_2[x]/(x^2 + x + \overline{1})$ gyűrűnek négy eleme van: $\overline{0}$, $\overline{1}$, $\overline{x}$, $\overline{x+1}$.

$+$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{1}$	$\overline{1}$	$\overline{0}$	$\overline{x+1}$	$\overline{x}$
$\overline{x}$	$\overline{x}$	$\overline{x+1}$	$\overline{0}$	$\overline{1}$
$\overline{x+1}$	$\overline{x+1}$	$\overline{x}$	$\overline{1}$	$\overline{0}$

$\cdot$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$	$\overline{0}$
$\overline{1}$	$\overline{0}$	$\overline{1}$	$\overline{x}$	$\overline{x+1}$
$\overline{x}$	$\overline{0}$	$\overline{x}$	$\overline{x+1}$	$\overline{1}$
$\overline{x+1}$	$\overline{0}$	$\overline{x+1}$	$\overline{1}$	$\overline{x}$

Ugyanez tömörebben, a $0 := \overline{0}$, $1 := \overline{1}$, $\alpha := \overline{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β
0	0	1	α	β
1	1	0	β	α
α	α	β	0	1
β	β	α	1	0

$\cdot$	0	1	α	β
0	0	0	0	0
1	0	1	α	β
α	0	α	β	1
β	0	β	1	α

Figyeljük meg, hogy

- K test, és $\{0, 1\} = \{\overline{0}, \overline{1}\}$ egy $\mathbb{Z}_2$-vel izomorf résztestet alkot K-ban;
- $\alpha = \overline{x}$ gyöke az $x^2 + x + 1 \in T[x]$ polinomnak: $\alpha^2 + \alpha + 1 = 0$.

Egy nevezetes példa

Az $\mathbb{R}[x]/(x^2+1)$ maradékosztály-gyűrű elemei: $\overline{a+bx}$ $(a, b \in \mathbb{R})$.
Az összeadás és a szorzás így végezhető ebben a gyűrűben:

$$\overline{a+bx} + \overline{c+dx} = \overline{(a+c)+(b+d)x},$$

$$\overline{a+bx} \cdot \overline{c+dx} = \overline{ac+(ad+bc)x+bdx^2} =$$
$$= \overline{ac+(ad+bc)x+bd(-1)} = \overline{(ac-bd)+(ad+bc)x} \quad .$$

A szorzat kiszámolásakor felhasználtuk azt, hogy $x^2 \equiv -1 \pmod{x^2+1}$.

Látjuk tehát, hogy $\mathbb{R}[x]/(x^2+1)$ lényegében ugyanaz, mint a komplex számtest (szaknyelven: $\mathbb{R}[x]/(x^2+1)$ izomorf $\mathbb{C}$-vel).

Ha bevezetjük az $i := \overline{x}$ jelölést (és elhagyjuk a vonásokat a konstansokról), akkor megkapjuk a komplex számok kanonikus alakját: $\overline{a+bx} = \overline{a} + \overline{b}\overline{x} = a+bi$.
Az $x^2 \equiv -1 \pmod{x^2+1}$ kongruencia azt jelenti, hogy $\overline{x}^2 = \overline{-1}$, azaz $i^2 = -1$.

ÖRÖMHÍR!

Minden polinomnak van gyöke!
Ha nem az eredeti testben, akkor annak egy alkalmas kibővítésében.

Ha az $m = x^n + b_{n-1}x^{n-1} + \cdots + b_1 x + b_0 \in T[x]$ irreducibilis főpolinomnak akarunk „gyököt csinálni”, akkor a $K = T[x] / (m)$ testet kell elkészítenünk.

A K test elemeinek kanonikus alakja:

$$a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1} \quad (a_0, a_1, \ldots, a_{n-1} \in T).$$

Az α szimbólumról csak annyit kell tudni, hogy $m(\alpha) = 0$, azaz
$\alpha^n + b_{n-1}\alpha^{n-1} + \cdots + b_1\alpha + b_0 = 0$.
Tehát a számolási szabály:

$$\alpha^n = -b_{n-1}\alpha^{n-1} - \cdots - b_1\alpha - b_0.$$

(És ha m nem irreducibilis?)

Na még egy példa

Határozzuk meg a $K = \mathbb{Q}[x] / \left(x^3 - 7\right)$ testben a $\overline{2 - x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ $(a, b, c \in \mathbb{Q})$ alakúak, ilyen alakban szeretnénk az $\overline{u} = \overline{2 - x}^{-1}$ elemet is megkapni.

$$
\begin{aligned}
\overline{2 - x}^{-1} = \overline{u} &\iff \overline{2 - x} \cdot \overline{u} = \overline{1} \\
&\iff (2 - x)\, u \equiv 1 \pmod{x^3 - 7} \\
&\iff \exists v \in \mathbb{Q}[x] : (2 - x)\, u = 1 + \left(x^3 - 7\right) v \\
&\iff (\text{...számolás...}) \\
&\iff u \equiv x^2 + 2x + 4 \pmod{x^3 - 7} \\
&\iff \overline{u} = \overline{x^2 + 2x + 4}
\end{aligned}
$$

Tehát $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.

Gyöktelenítés

Menjünk le alfába:

$$K = \left\{ a\alpha^2 + b\alpha + c \colon a, b, c \in \mathbb{Q} \right\},$$

ahol α gyöke az $x^3 - 7$ polinomnak.

Node ennek a polinomnak nem kell gyököt csinálni, mert már van neki: $\alpha = \sqrt[3]{7}$! (Vagy $\alpha = \sqrt[3]{7}\,\mathrm{cis}\,\frac{\pm 2\pi}{3}$.) Tehát K tekinthető számtestnek is:

$$K = \left\{ a\sqrt[3]{49} + b\sqrt[3]{7} + c \colon a, b, c \in \mathbb{Q} \right\}.$$

Az előbb kiszámoltuk, hogy $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$, ami azt jelenti, hogy $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, azaz

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Ezzel a módszerrel (lényegében az euklideszi algoritmussal) lehet bonyolult nevezőket gyöktelenníteni.

Irreducibilitás

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; ilyenkor *triviális faktorizációról* beszélünk.)
Formálisan:

$$\forall f, g \in T[x] : p = fg \implies (p \sim f \text{ vagy } p \sim g).$$

Állítás.

Egy legalább elsőfokú $p \in T[x]$ polinom akkor és csak akkor irreducibilis, ha p nem bontható $\deg p$-nél kisebb fokszámú polinomok szorzatára.

Bizonyítás.

- triviális felbontás: $p = f \cdot g$, ahol $\deg f = 0, \deg g = \deg p$ (vagy fordítva)
- nemtriviális felbontás: $p = f \cdot g$, ahol $1 \leq \deg f, \deg g < \deg p$ □

Megjegyzés.

Gyűrűk felett ez általában nem igaz! Például a $p = 2x \in \mathbb{Z}[x]$ polinom nem bontható kisebb fokszámú polinomok szorzatára, mégsem irreducibilis $\mathbb{Z}$ felett.

Egyértelmű irreducibilis faktorizáció

Definíció.

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

$$\forall f, g \in T[x] : p \mid fg \implies (p \mid f \text{ vagy } p \mid g).$$

Tétel.

Test feletti polinomokra az irreducibilitás és a prímtulajdonság ekvivalens.

Tétel.

Minden legalább elsőfokú polinom felbontható irreducibilis polinomok szorzatára.

Ez a felbontás a tényezők sorrendjétől és asszociáltságtól eltekintve egyértelműen meghatározott, azaz ha $p_1 \cdot \ldots \cdot p_n$ és $q_1 \cdot \ldots \cdot q_m$ ugyanazon polinom két irreducibilis faktorizációja, akkor $n = m$, és létezik olyan $\pi \in S_n$ permutáció, hogy minden $i = 1, \ldots, n$ esetén

$$p_i \sim q_{\pi(i)}.$$

Polinomgyűrű maradékosztályteste

Tétel.

A $T[x]/(m)$ gyűrű akkor és csak akkor test, ha m irreducibilis T felett.

Bizonyítás.

$T[x]/(m)$ kommutatív egységelemes gyűrű. A „testséghez" az kell még, hogy

- $T[x]/(m)$ legalább kételemű legyen,
- és minden nemzéró elemének legyen multiplikatív inverze.

Négy esetet vizsgálunk m szerint:

1. Ha $m \sim 1$, akkor (és csak akkor) $T[x]/(m)$ egyelemű, tehát nem test.
2. Ha $m = 0$, akkor $\overline{x} \neq \overline{0}$, még sincs multiplikatív inverze, ezért $T[x]/(m)$ nem test. (Ekkor egyébként $T[x]/(m) \cong T[x]$.)
3. Ha $m = f \cdot g$ egy nemtriviális felbontás, akkor $\overline{f} \cdot \overline{g} = \overline{0}$, tehát $T[x]/(m)$ nem test, sőt, nem is integritástartomány.
4. Ha m irreducibilis, akkor $\forall f : \overline{f} \neq \overline{0} \implies f \perp m$, ezért $\overline{f}$-nak van multiplikatív inverze, és így $T[x]/(m)$ test.

□

Irreducibilitás vs. gyökök

Állítás.

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f = g \cdot h$, akkor $\deg g + \deg h = 1$, és így

$$\deg g = 1, \deg h = 0 \quad \text{vagy} \quad \deg g = 0, \deg h = 1.$$

Mindkét esetben triviális a felbontás. □

Tétel.

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

Bizonyítás.

Ha α gyöke f-nek, akkor $f = (x - \alpha)(\cdots)$ nemtriviális felbontás. □

Irreducibilitás vs. gyökök

Tétel.

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = g \cdot h$, akkor $\deg g + \deg h \in \{2, 3\}$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg g$	$\deg h$
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója.
Egy elsőfokú polinom asszociáltság erejéig mindig $x - \alpha$ alakban írható*, ez pedig akkor és csak akkor osztja f-et, ha α gyöke f-nek. □

* $ax + b = a\left(x + \frac{b}{a}\right) \sim x + \frac{b}{a} = x - \left(-\frac{b}{a}\right) = x - \alpha$

Irreducibilitás vs. gyökök

Összefoglalva:

Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

implikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!

A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Példa.

Az $f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ polinomnak nincs valós gyöke, mégsem irreducibilis $\mathbb{R}$ felett:

$$f = (x^2 + 1)(x^2 + 1).$$

Irreducibilitás vs. gyökök

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM NEM NEM NEM NEM NEM NEM

KÖVETKEZIK

AZ IRREDUCIBILITÁS!!!

Irreducibilis faktorizáció

Példa.

Bontsa irreducibilis tényezők szorzatára az alábbi polinomot:

$$f = x^6 + 3x^4 - x^3 + 2x^2 + x - 1 \in \mathbb{Z}_5[x].$$

Mivel az alaptestnek csak öt eleme van, egyenként kipróbálhatjuk, hogy gyöke-e valamelyik az f polinomnak.

Amelyik igen, annál a Horner-módszerrel megállapítjuk a multiplicitást, és leválasztjuk a gyöktényezőket:

$$f = (x-1)^2 (x-3)(x-4)(x^2 + 4x + 2).$$

Az $x^2 + 4x + 2$ polinomnak nincs gyöke (ha lenne, megtaláltuk volna), és csak másodfokú, ezért irreducibilis.

(Ha negyed- vagy magasabb fokú polinom marad a gyöktényezők kiemelése után, akkor valami trükkre van szükség . . .)