

# 1. A komplex számok résztestei

**Bővítés egy szám négyzetgyökével.**

**Gauss-rationális számok**

Az  $a + bi$  alakú számok ( $a, b \in \mathbb{Q}$ ) részgyűrűt alkotnak  $\mathbb{C}$ -ben.

Ez résztest is:  $\frac{1}{a + bi} = \frac{a - bi}{a^2 + b^2}$ , és  $\frac{a}{a^2 + b^2}, \frac{-b}{a^2 + b^2} \in \mathbb{Q}$ .

**Általánosítás**

Legyen  $u \in \mathbb{Q}$  rögzített szám. Az  $a + b\sqrt{u}$  alakú számok (ahol  $a, b \in \mathbb{Q}$ ) résztestet alkotnak  $\mathbb{C}$ -ben. Jele:  $\mathbb{Q}(\sqrt{u})$ .

**Valóban:** Összeadásra, ellentettképzésre zárt,  $0 \in \mathbb{Q}(\sqrt{u})$ : **HF**.

Ha  $a + b\sqrt{u}, c + d\sqrt{u} \in \mathbb{Q}(\sqrt{u})$ , akkor

$$(a + b\sqrt{u})(c + d\sqrt{u}) = (ac + bdu) + (ad + bc)\sqrt{u}.$$

Itt  $ac + bdu \in B\mathbb{Q}$  és  $ad + bc \in \mathbb{Q}$ , ezért szorzásra is zárt.

Reciprokképzés:  $\frac{1}{a + b\sqrt{u}} = \frac{a - b\sqrt{u}}{a^2 - b^2u}$ . Lehet-e  $a^2 - b^2u = 0$ ?

**A reciprok  $\mathbb{Q}(\sqrt{u})$ -ban van-e.**

$a, b, u \in \mathbb{Q}, a + b\sqrt{u} \neq 0$ . Előfordulhat-e, hogy  $a^2 - b^2u = 0$ ?

Előfordulhat! Például ha  $a = 2, b = 1, u = 4$ . De ekkor sincs baj, mert  $a + b\sqrt{u} = 4$  reciproka  $1/4 \in \mathbb{Q}(\sqrt{4})$ .

$a^2 - b^2u = (a + b\sqrt{u})(a - b\sqrt{u})$ . Lehet-e  $a - b\sqrt{u} = 0$ ?

Ha  $a - b\sqrt{u} = 0$ , akkor  $b = 0$ , vagy  $\sqrt{u} = a/b \in \mathbb{Q}$ .

Ha  $b = 0$ , akkor  $a + b\sqrt{u} = a \neq 0$ , így  $a^2 - b^2u$  mégsem 0.

Ha  $\sqrt{u} \in \mathbb{Q}$ , akkor  $a + b\sqrt{u} \in \mathbb{Q}$ , ezért  $\frac{1}{a + b\sqrt{u}} \in \mathbb{Q}$ . □

Ha  $\sqrt{u} \notin \mathbb{Q}$ , akkor az  $a + b\sqrt{u}$  előállítás egyértelmű.

**Valóban:**  $a + b\sqrt{u} = c + d\sqrt{u} \implies a - c = (d - b)\sqrt{u}$ .

Ha  $b = d$ , akkor  $a = c$ . Ha nem, akkor  $\sqrt{u} \in \mathbb{Q}$  lenne.

**Bővítés egy szám köbgyökével.**

**Állítás (3.5.18. Feladat)**

Az  $a + b\sqrt[3]{2}$  ( $a, b \in \mathbb{Q}$ ) számok *nem* alkotnak részgyűrűt.

**Valóban:** elég megmutatni, hogy  $\sqrt[3]{2} \cdot \sqrt[3]{2} = \sqrt[3]{4}$  nincs benne. Tegyük föl, hogy  $a + b\sqrt[3]{2} = \sqrt[3]{4}$ , ahol  $a, b \in \mathbb{Q}$ . Legyen  $f(x) = x^2 - bx - a \in \mathbb{Q}[x]$ . Ekkor  $f$ -nek gyöke a  $\sqrt[3]{2}$ . De  $g(x) = x^3 - 2$ -nek is gyöke a  $\sqrt[3]{2}$ . Legyen  $h \in \mathbb{Q}[x]$  az  $f$  és  $g$  **kitüntetett közös osztója**. Az euklideszi algoritmus miatt ez ugyanaz  $\mathbb{R}$  és  $\mathbb{Q}$  fölött. Mivel  $x - \sqrt[3]{2}$  közös osztója  $f$ -nek és  $g$ -nek, ezért osztója  $h$ -nak. Vagyis  $h$  nem lehet konstans polinom. De  $h \mid g(x) = x^3 - 2$ , ami a Schönemann–Eisenstein miatt **irreducibilis**  $\mathbb{Q}$  fölött. Ez ellentmondás, mert  $h \mid f$  miatt  $h$  legfeljebb másodfokú. □

A  $\sqrt[3]{2}$ -t tartalmazó legszűkebb résztest.

**Állítás (vö. 6.1.16. Tétel)**

Az  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$  ( $a, b, c \in \mathbb{Q}$ ) alakú számok *résztestet* alkotnak  $\mathbb{C}$ -ben. Jele:  $\mathbb{Q}(\sqrt[3]{2})$ .

**Bizonyítás**

Zárttság összeadásra, kivonásra, szorzásra: HF.

$a + b\sqrt[3]{2} + c\sqrt[3]{4}$  reciproka: legyen  $g(x) = a + bx + cx^2 \in \mathbb{Q}[x]$ .

Mivel  $x^3 - 2$  irreducibilis,  $x^3 - 2$  és  $g(x)$  relatív prímekek. Ezért van olyan  $p, q \in \mathbb{Q}[x]$ , hogy  $p(x)g(x) + q(x)(x^3 - 2) = 1$ . Innen  $x \mapsto \sqrt[3]{2}$  helyettesítéssel  $p(\sqrt[3]{2})g(\sqrt[3]{2}) = 1$ .

**Maradékösztás:**  $p(x) = s(x)(x^3 - 2) + (ux^2 + vx + w)$ .

Ekkor  $p(\sqrt[3]{2}) = u\sqrt[3]{4} + v\sqrt[3]{2} + w$  (itt  $u, v, w \in \mathbb{Q}$ ). Ezért  $a + b\sqrt[3]{2} + c\sqrt[3]{4}$  reciproka  $u\sqrt[3]{4} + v\sqrt[3]{2} + w \in \mathbb{Q}(\sqrt[3]{2})$ .  $\square$

## 2. Szám minimálpolinomja

**Mátrix minimálpolinomja.**

**Ismétlés**

Ha  $K$  test, akkor egy  $M \in K^{n \times n}$  mátrix  $m_M$  *minimálpolinomja* a legalacsonyabb fokú olyan normált,  $K[x]$ -beli polinom, amelynek  $M$  gyöke. Minden  $f \in K[x]$ -re  $f(M) = 0 \iff m_M \mid f$ . A minimálpolinom egyértelműen meghatározott.

**Bizonyítás**

Azok az  $f \in K[x]$  polinomok, melyeknek  $M$  gyöke, *ideált* alkotnak  $K[x]$ -ben (HF). Mivel  $K[x]$  **euklideszi** gyűrű, ez egy **főideál**. Az egyetlen normált generátoreleme éppen  $m_M$ .  $\square$

**Példa:**  $\begin{bmatrix} 1 & 0 \\ 0 & 2 \end{bmatrix}$  minimálpolinomja  $(x - 1)(x - 2)$ .

**Szám minimálpolinomja test fölött.**

**6.1.13. Tétel, 5.10.10. Tétel**

Legyen  $K$  részteste  $L$ -nek (főpélda:  $\mathbb{Q} \leq \mathbb{C}$ ). Egy  $\alpha \in L$  elem  $m_\alpha$  *minimálpolinomja*  $K$  fölött a legalacsonyabb fokú olyan normált,  $K[x]$ -beli polinom, amelynek  $\alpha$  gyöke. Minden  $f \in K[x]$ -re  $f(\alpha) = 0 \iff m_\alpha \mid f$ . A minimálpolinom egyértelműen meghatározott.

**Bizonyítás**

Azok az  $f \in K[x]$  polinomok, melyeknek  $\alpha$  gyöke, *ideált* alkotnak  $K[x]$ -ben (HF). (Ez az ideál az „ $\alpha$  behelyettesítése” homomorfizmus magja!) Mivel  $K[x]$  **euklideszi** gyűrű, ez egy **főideál**. Az egyetlen normált generátoreleme éppen  $m_\alpha$ .  $\square$

## Algebrai és transzcendens elemek.

Mi történik, ha ez az ideál csak a nullapolinomból áll?

Mátrixoknál ez lehetetlen: beláttuk, hogy mindig van benne legfeljebb  $n^2$  fokú polinom. Sőt, a Cayley-Hamilton tétel miatt  $M$  karakterisztikus polinomja is ebben az ideálban van.

### 6.1.11. Definíció

Az  $\alpha \in L$  transzcendens  $K$  fölött, ha a szóbanforgó ideál csak a nullapolinomból áll, azaz a nullán kívül nincs olyan  $f \in K[x]$ , melyre  $f(\alpha) = 0$ . Különben  $f$  algebrai  $K$  fölött. Transzcendens elemnél nem beszélünk minimálpolinomról.

Transzcendens szám:  $\mathbb{Q}$  fölött transzcendens komplex szám.

Példák:  $e, \pi, 2^{\sqrt{3}}$  transzcendens számok. Ezek nehéz tételek!

## A minimálpolinom felismerése.

### 6.1.13. Tétel, 5.10.12. Tétel

Legyen  $K$  részteste  $L$ -nek és  $\alpha \in L$  algebrai. Ekkor az  $m_\alpha$  minimálpolinom irreducibilis  $K$  fölött.

Megfordítva, ha  $f \in K[x]$  normált, irreducibilis, és  $\alpha$  gyöke, akkor  $f = m_\alpha$ .

### Bizonyítás

Ha  $m_\alpha(x) = g(x)h(x)$ , akkor  $g(\alpha)h(\alpha) = m_\alpha(\alpha) = 0$ . Mivel  $L$  nullosztómentes, innen  $g(\alpha) = 0$  vagy  $h(\alpha) = 0$ . Az első esetben  $m_\alpha \mid g$ , azaz  $g$  az  $m_\alpha$  egységszerese. Ezért az  $m_\alpha = gh$  felbontás triviális. A másik eset hasonló.

Megfordítva: Ha  $f(\alpha) = 0$  és  $f$  normált, irreducibilis  $K$  fölött, akkor  $m_\alpha \mid f$  miatt  $m_\alpha$  konstans, vagy  $f$  egységszerese. De  $m_\alpha$  nem konstans, mert  $m_\alpha(\alpha) = 0$ . Ezért  $m_\alpha = f$ , mert mindkettő normált.  $\square$

## Példák minimálpolinomra.

- (1) A 24 minimálpolinomja  $\mathbb{Q}$  fölött  $x - 24$ , mert ez normált, elsőfokú, és így irreducibilis  $\mathbb{Q}$  fölött.
- (2) Az  $\sqrt[n]{2}$  minimálpolinomja  $\mathbb{Q}$  fölött  $x^n - 2$ , ez a Schönemann-Eisenstein miatt irreducibilis  $\mathbb{Q}$  fölött.
- (3) A  $\sqrt{27}$  minimálpolinomja  $\mathbb{Q}$  fölött  $x^2 - 27$ . Ez irreducibilis, mert másodfokú, és nincs gyöke  $\mathbb{Q}$ -ban.
- (4) A  $\sqrt[3]{9}$  minimálpolinomja  $\mathbb{Q}$  fölött  $x^3 - 9$ . Ez irreducibilis, mert harmadfokú, és nincs gyöke  $\mathbb{Q}$ -ban. **Ismétlés:** racionális gyökteszt!
- (5) Tudjuk, hogy  $1 + i$  negyedik hatványa  $-4$ . A minimálpolinomja mégsem  $x^4 + 4$ , hanem  $x^2 - 2x + 2$ .
- (6) Az  $n$ -edik primitív egységgyökök közös minimálpolinomja  $\mathbb{Q}$  fölött a  $\Phi_n(x)$  ( $n$ -edik körosztási polinom).

### 3. Egyszerű testbővítés

**Elem normálalakja.**

#### 6.1.16. Tétel

Legyen  $K$  részteste  $L$ -nek,  $\alpha \in L$  algebrai és  $n = \text{gr}(m_\alpha)$ .

Ekkor az  $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$  ( $a_0, a_1, \dots, a_{n-1} \in K$ ) alakú elemek *résztestet* alkotnak  $L$ -ben. Jele:  $K(\alpha)$ . Az  $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1}$  előállítás *egyértelmű*.

Legyen  $f(x) = b_0 + b_1x + \dots + b_kx^k \in K[x]$ .

Ekkor  $f(\alpha) = b_0 + b_1\alpha + \dots + b_k\alpha^k \in K(\alpha)$  az  $\alpha$  egy *polinomja*.

Az  $\alpha$  minden polinomja benne van  $K(\alpha)$ -ban.

**Valóban:** ha  $f \in K[x]$  akkor  $f(x) = m_\alpha(x)q(x) + (a_0 + \dots + a_{n-1}x^{n-1})$  (**maradék oszttás**). Innen  $f(\alpha) = a_0 + \dots + a_{n-1}\alpha^{n-1} \in K(\alpha)$ .

Így  $K(\alpha)$  az  $\alpha$  ( $K$ -beli együtthatós) polinomjainak halmaza.

**Elem normálalakja: bizonyítás.**

#### Bizonyítás

Zártág összeadásra, kivonásra: **HF**.

**Szorzásra:**  $K(\alpha)$  az  $\alpha$  ( $K$ -beli együtthatós) polinomjainak halmaza.

De nyilván  $f(\alpha)g(\alpha) = (fg)(\alpha) \in K(\alpha)$ .

**Reciprokképzésre:** Legyen  $g \in K(x)$ ,  $g(\alpha) \neq 0$ ,  $\text{gr}(g) \leq n-1$ . Mivel  $m_\alpha$  irreducibilis és  $n$ -edfokú,  $m_\alpha$  és  $g$  relatív prímelek. Ezért van olyan  $p, q \in K[x]$ , hogy  $pg + qm_\alpha = 1$ . Innen  $x \mapsto \alpha$  helyettesítéssel  $p(\alpha)g(\alpha) = 1$ . Így  $p(\alpha) \in K(\alpha)$  reciproka  $g(\alpha)$ -nak.

**Egyértelműség:** Tegyük fel, hogy

$$a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \dots + b_{n-1}\alpha^{n-1}.$$

Legyen  $f(x) = (a_0 - b_0) + (a_1 - b_1)x + \dots + (a_{n-1} - b_{n-1})x^{n-1}$ . Ekkor  $f(\alpha) = 0$ , és így  $m_\alpha \mid f$ . Mivel  $f$  legfeljebb  $n-1$ -edfokú, csak a nullapolinom lehet. Így  $a_j = b_j$  minden  $j$ -re.  $\square$