1. Testbővítések

A résztestek fontossága

Adottak a síkon pontok. Azon pontok koordinátái, amelyek ezekből kiindulva megszerkeszthetők, résztestet alkotnak $\mathbb{R}$-ben. Például a kockakettőzés feladata akkor lenne megoldható, ha racionális koordinátájú pontokból indulva ebben benne lenne a $\sqrt[3]{2}$.

Egyenletek gyökjelekkel való megoldhatóságának vizsgálatában is testet alkotnak az úgynevezett gyökkifejezések. Diofantikus egyenletek vizsgálatakor hasznos a szorzattá bontást $\mathbb{C}$ résztesteiben elvégezni, pl. $x^2+y^2=(x+iy)(x-iy)$.

A hibajavító kódok elméletében a véges testek játszanak szerepet.

Ezekben az alkalmazásokban tipikusan egy test résztesteit kell felderíteni, vagy olyan kérdésekre adni választ, hogy $\sqrt[3]{2}$ felírható-e racionális számokból kiindulva négyzetgyökvonások segítségével.

Generált résztest

6.1.5. Definíció
Ha K részteste L-nek, akkor *testbővítésről* beszélünk.
Ha $\alpha,\beta,\ldots\in L$, akkor $N=K(\alpha,\beta,\ldots)$ a *legszűkebb* olyan részteste L-nek, amely K-t és az $\alpha,\beta,\ldots$ elemeket tartalmazza.
Vagyis ha $T\leq L$ résztest, $K\subseteq T$, $\alpha,\beta,\ldots\in T$, akkor $N\subseteq T$.
Egyszerű bővítés: $K\leq K(\alpha)$ alkalmas $\alpha\in L$-re.

$K(\alpha,\beta,\ldots)$ *létezik*, mint a K-t és $\alpha,\beta,\ldots$ elemeket tartalmazó résztestek metszete. Elemei úgy kaphatók, hogy vesszük az $\alpha,\beta,\ldots$ elemek összes, többhatározatlanú K-beli együtthatós polinomjait, majd ezek hányadosait.

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ elemei $a+b\sqrt{2}+c\sqrt{3}+d\sqrt{6}$, ahol $a,b,c,d\in\mathbb{Q}$. Összeadásra, kivonásra, szorzásra zártság: HF. Reciprokra zártság: kerülő úton.

Bővítés egy szám négyzetgyökével

Gauss-racionális számok
Az $a+bi$ alakú számok ($a,b\in\mathbb{Q}$) részgyűrűt alkotnak $\mathbb{C}$-ben.
Ez *résztest* is: $\dfrac{1}{a+bi}=\dfrac{a-bi}{a^2+b^2}$, és $\dfrac{a}{a^2+b^2},\dfrac{-b}{a^2+b^2}\in\mathbb{Q}$.

Általánosítás
Legyen $u \in Q$ rögzített szám. Az $a+b\sqrt{u}$ alakú számok (ahol $a, b \in \mathbb{Q}$) *résztestet* alkotnak $\mathbb{C}$-ben. HF: Ez $\mathbb{Q}(\sqrt{u})$.
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 $ac + bdu \in BQ$ és $ac + bc \in \mathbb{Q}$, ezért szorzásra is zárt.
Reciprokképzés: $\dfrac{1}{a + b\sqrt{u}} = \dfrac{a - b\sqrt{u}}{a^2 - b^2u}$. 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 $1/4 \in \mathbb{Q}(\sqrt{4})$.

Két eset van:
Ha $\sqrt{u} \in \mathbb{Q}$, akkor $\mathbb{Q}(\sqrt{u}) = \mathbb{Q}$, ami test.
Ha nem, 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: $\sqrt{u} = (a-c)/(d-b) \in \mathbb{Q}$ lenne. Ezért ha $a-b\sqrt{u} = 0$, akkor $a = b = 0$, és $a+b\sqrt{u}$ is nulla lenne. Vagyis az $a+b\sqrt{u}$ számok mindenképpen testet alkotnak.

Fontos lenne $\mathbb{Q}(\alpha)$ elemeit jól kezelhető, egyértelmű alakban fölírni.
Pl.: $\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \,:\, a, b, c \in \mathbb{Q}\}$; a, b, c egyértelmű.

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. □

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

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_α *minimálpolinomja K fölött* a legalacsonyabb fokú olyan normált, $K[x]$-beli polinom, amelynek α 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 α gyöke, *ideált* alkotnak $K[x]$-ben (HF). (Ez az ideál az „α behelyettesítése" homomorfizmus magja!)
Mivel $K[x]$ *euklideszi* gyűrű, ez egy *főideál*. Az egyetlen normált generátoreleme éppen m_α. □

Algebrai és transzcendens elemek

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

Mátrixoknál ez lehetetlen: beláttuk, hogy egy $n \times n$-es mátrix mindig gyöke egy legfeljebb n^2 fokú nem nulla polinomnak. Sőt, a Cayley-Hamilton tétel miatt M karakterisztikus polinomja (ami n-edfokú) 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.

Transzcendens számok

Konkrét számokról nehéz bizonyítani, hogy transzcendensek.

$\sum_{k=0}^{\infty} 10^{-k!}$ transzcendens (Liouville, 1851).
e transzcendens (Hermite, 1873).
π transzcendens (Lindemann, 1882), környégyszögesítés.
$2^{\sqrt{3}}$ transzcendens. Általában: α^β transzcendens, ha
α, β algebrai, β irracionális, $\alpha \neq 0, 1$ (Gelfond-Schneider, 1935).
$e + \pi$ transzcendens-e, racionális-e: *megoldatlan.*

Cantor (1874): *a valós számok döntő többsége transzcendens.*
Ugyanis az algebrai számok *megszámlálható* halmazt alkotnak (fel lehet őket sorolni: $\alpha_1, \alpha_2, \ldots, \alpha_n, \ldots$). A megszámlálható a „legkisebb lehetséges végtelen halmaz", de a transzcendens számok halmaza nem megszámlálható.

A minimálpolinom felismerése

6.1.13. Tétel, 5.10.12. Tétel
Legyen K részteste L-nek és $\alpha \in L$ algebrai. Ekkor az m_α minimálpolinom *irreduciblis* K fölött.
Megfordítva, ha $f \in K[x]$ normált, irreducibilis, és α 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_α 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_α nem nulla konstans, vagy f egységszerese. De m_α nem konstans, mert $m_\alpha(\alpha) = 0$. Ezért $m_\alpha = f$, mert mindkettő normált. □

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 $n = \mathrm{gr}(m_\alpha)$.
Ekkor $K(\alpha)$ elemei egyértelműen fölírhatók $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ alakban, ahol $a_0, a_1, \ldots, a_{n-1} \in K$.

Jelölje T az $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ alakú elemek halmazát.
Nyilván $K \subseteq T \subseteq K(\alpha)$ és $\alpha \in T$. Kell: T test.
Legyen $f(x) = b_0 + b_1x + \ldots + b_kx^k \in K[x]$. Ekkor $f(\alpha) = b_0 + b_1\alpha + \ldots + b_k\alpha^k$ az α egy *polinomja.*

Az α minden polinomja benne van T-ben. Valóban:
ha $f \in K[x]$ akkor $f(x) = m_\alpha(x)q(x) + (a_0 + \ldots + a_{n-1}x^{n-1})$ (*maradékos osztás*).
Innen $f(\alpha) = a_0 + \ldots + a_{n-1}\alpha^{n-1} \in T$.

Így T az α (K-beli együtthatós) polinomjainak halmaza. Ezért T zárt összeadásra, kivonásra és szorzásra is.

Elem normálalakja: bizonyítás

Reciprokképzés:
Legyen $g \in K(x)$, $g(\alpha) \neq 0$, $\mathrm{gr}(g) \leq n-1$. Mivel m_α irreducibilis és n-edfokú, m_α és g relatív prímek. 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
$$a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} = b_0 + b_1\alpha + \ldots + b_{n-1}\alpha^{n-1}.$$
Legyen $f(x) = (a_0 - b_0) + (a_1 - b_1)x + \ldots + (a_{n-1} - b_{n-1})x^{n-1}$. 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. □

A transzcendens eset

Reciprokképzés (második bizonyítás):
Tekintsük azt a $\varphi : K[x] \to L$ homomorfizmust, ami f-hez $f(\alpha)$-t rendel. Nyilván $T = \mathrm{Im}(\varphi)$ és $(m_\alpha) = \mathrm{Ker}(\varphi)$ (hiszen T az α K-beli együtthatós polinomjainak a halmaza, a minimálpolinom pedig definíció szerint $\mathrm{Ker}(\varphi)$ generátoreleme). Így a homomorfizmus-tétel miatt $T \cong K[x]/(m_\alpha)$. Mivel m_α irreducibilis, a gyűrűknél tanultak szerint T test. □

6.1.9. Tétel, 6.1.21. Gyakorlat (HF)
Legyen K részteste L-nek és $\alpha \in L$ transzcendens K fölött. Ekkor $K(\alpha)$, azaz L-nek a K-t és α-t tartalmazó legszűkebb részteste az összes olyan $f(\alpha)/g(\alpha)$ törtekből áll, ahol $f, g \in K[x]$, $g \neq 0$. Ez az előállítás *egyértelmű* is a következő értelemben: $f(\alpha)/g(\alpha) = h(\alpha)/k(\alpha) \iff f(x)k(x) = g(x)h(x)$.

4. Generált résztest

A generálásfogalom haszna

Kulcs: $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}) \leq \mathbb{C}$.

Bizonyítás
$\subseteq$: Legyen $T = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$. Ekkor $\sqrt{3} \in T$ és $\mathbb{Q}(\sqrt{2}) \subseteq T$.
Ezért $\mathbb{Q} \subseteq T$ és $\sqrt{2} \in T$. Mivel T résztest, így $\mathbb{Q}(\sqrt{2},\sqrt{3}) \subseteq T$.
$\supseteq$: Legyen $S = \mathbb{Q}(\sqrt{2},\sqrt{3})$. Ekkor $\mathbb{Q} \subseteq S$ és $\sqrt{2},\sqrt{3} \in S$.
Mivel S résztest, ezért $\mathbb{Q}(\sqrt{2}) \subseteq S$. Így $\big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}) \subseteq S$. □

6.1.8. Gyakorlat, HF

(1) $\big(K(\alpha)\big)(\beta) = K(\alpha,\beta) = \big(K(\beta)\big)(\alpha)$.

(2) $K(\alpha,\beta) = K(\alpha,\alpha+\beta)$.

(3) Ha $\alpha \neq 0$, akkor $K(\alpha,\beta) = K(\alpha,\alpha\beta)$.

$\mathbb{Q}(\sqrt{2},\sqrt{3})$ elemei

$\big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$ elemei $\alpha + \gamma\sqrt{3}$, ahol $\alpha,\gamma \in \mathbb{Q}(\sqrt{2})$.
Valóban: $\sqrt{3}$ gyöke az $x^2 - 3 \in \mathbb{Q}(\sqrt{2})[x]$ polinomnak, így $\sqrt{3}$ minimálpolinomja $\mathbb{Q}(\sqrt{2})$ fölött legfeljebb másodfokú, ezért az $a_0 + a_1\sqrt{3} + \ldots + a_{n-1}\sqrt{3}^{n-1}$ képletben $n \leq 2$. Itt $\alpha = a + b\sqrt{2}$ és $\gamma = c + d\sqrt{2}$, ahol $a,b,c,d \in \mathbb{Q}$.

Ezért $\alpha + \gamma\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$. Vagyis $\mathbb{Q}(\sqrt{2},\sqrt{3}) = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$ minden eleme ilyen alakú. Mivel ez test, az ilyen alakú elemek reciproka is ilyen alakú. □

Általánosítás (6.1.22. Gyakorlat)
Ha $K \leq T$ testbővítés és $\alpha_1,\ldots,\alpha_k \in L$ algebrai K fölött, akkor $K(\alpha_1,\ldots,\alpha_k)$ elemei $p(\alpha_1,\ldots,\alpha_k)$ alakúak, ahol $p \in K[x_1,\ldots,x_n]$, így *osztásra nincs szükség.*

5. Testbővítés foka

A testbővítés, mint vektortér

Állítás (5.10.4. Gyakorlat, HF)
Ha $K \leq L$ testbővítés, akkor L *vektortér* K fölött. Az összeadás az L-beli összeadás, az L elemeinek a K elemeivel, mint skalárokkal szorzása az L-beli szorzás. E vektortér dimenziója a testbővítés *foka*, jele $|L : K|$.

6.1.20. Következmény
Ha $\alpha \in L$ algebrai K fölött, akkor $|K(\alpha) : K| = \mathrm{gr}(m_\alpha)$.

Bizonyítás
$K(\alpha)$ elemei egyértelműen $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ alakban írhatók, ahol $a_0, a_1, \ldots, a_{n-1} \in K$ és $n = \mathrm{gr}(m_\alpha)$. Ezért $1, \alpha, \ldots, \alpha^{n-1}$ *bázis* L-ben K fölött, elemszáma n. □

Véges bővítés

6.1.18. Definíció
Legyen K részteste L-nek, $\alpha \in L$ algebrai és $n = \mathrm{gr}(m_\alpha)$.
Ekkor az n szám az α *foka* K fölött, jele $\mathrm{gr}_K(\alpha)$.

Tehát $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$.

6.1.20. Következmény
Ha $\alpha \in L$ transzcendens K fölött, akkor $|K(\alpha) : K|$ végtelen.

Valóban: $1, \alpha, \alpha^2, \ldots, \alpha^k$ független K fölött minden k-ra.

6.1.17. Definíció
$K \leq L$ *véges bővítés*, ha L véges dimenziós K fölött.

Tehát $K \leq K(\alpha)$ akkor és csak akkor véges bővítés, ha α algebrai K fölött.

Véges bővítés egyszerűsége

6.3.8. Tétel, NB
Legyen $K \leq L \leq \mathbb{C}$ véges testbővítés. Ekkor $K \leq L$ egyszerű, azaz van olyan $\gamma \in L$, hogy $L = K(\gamma)$.

Ahelyett, hogy $\mathbb{C}$ résztesteiről van szó, elég föltenni, hogy K karakterisztikája nulla, vagy hogy K véges (6.3.9-11).

Példa (vö. 6.4.22-27), nem kell tudni
Legyen L az $f(x, y)/g(x, y)$ polinom-hányadosok teste, ahol $f, g \in \mathbb{Z}_p[x, y]$ és $g \neq 0$ (p prím). Vegyük az x^p, y^p elemek által generált K résztestet. Ekkor $K \leq L$ véges, de nem egyszerű bővítés.

Nyilván $K(x, y) = L$, és x, y algebrai K fölött, hiszen $x^p, y^p \in K$, belátható, hogy $|L : K| = p^2$. A p-edik hatványra emelés művelettartó, ezért ha $\gamma \in L$, akkor $\gamma^p \in K$. Így $|K(\gamma) : K| \leq p$.