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.

$K(\alpha,\beta,\ldots)$ tehát olyan, mint lineáris algebrában a generált altér. De elemei nem lineáris kombinációk, hanem 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. Egyszerű testbővítés

Minimálpolinom test fölött

6.1.11. Definíció
Legyen K részteste L-nek (főpélda: $\mathbb{Q} \leq \mathbb{C}$). Az $\alpha \in L$ *algebrai* K fölött, ha van olyan nem nulla $f \in K[x]$, melyre $f(\alpha) = 0$. Különben α *transzcendens* K fölött.

6.1.13. Tétel, 5.10.10. Tétel
Egy K fölött algebrai $\alpha \in L$ 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. Ha $f \in K[x]$ normált és $f(\alpha) = 0$, akkor $f = m_\alpha$ pontosan akkor teljesül, ha f irreducibilis K fölött.

A bizonyítás ugyanaz, mint a már látott $\mathbb{Q} \leq \mathbb{C}$ esetben.

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 a $\mathrm{Ker}(\varphi)$ főideál 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: $f(\alpha)/g(\alpha) = h(\alpha)/k(\alpha) \iff f(x)k(x) = g(x)h(x)$.

3. 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 $\gamma = c + d\sqrt{3}$, 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.*

4. 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.

5. Testbővítések fokának szorzástétele

A szorzástétel

Tétel (6.2.3. Következmény)
Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek. Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán
$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$.
$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).
$1, \sqrt{3}$ bázis M-ben L fölött (mert $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: HF).
Láttuk: az $M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$ általános eleme felírható
$\alpha + \gamma\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alakban, ahol $\alpha = a + b\sqrt{2}$ és $\gamma = c + d\sqrt{3}$.
Ekkor $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}$ bázis lesz az $L \leq M$ bővítésben.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: *az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.*

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ *generátorrendszer.*

A *függetlenséghez* tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött, mindegyik $\alpha_i = 0$.
Mivel $v_1, \ldots, v_n$ független K fölött, $a_{ij} = 0$ minden i, j-re.
Ezért $v_i u_j$ tényleg független rendszer. □

A bővítések végességéről szóló állítás HF.

A szorzástétel első következménye

6.2.4. Állítás
Elem foka *osztója* a bővítés fokának. Pontosabban: Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás
Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$. Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges. Így α algebrai K fölött, és $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$. A szorzástételt alkalmazzuk a

$$K \leq K(\alpha) \leq L$$

testláncra. Azt kapjuk, hogy $|L : K| = |L : K(\alpha)| \cdot \mathrm{gr}_K(\alpha)$. Ezért $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak. □

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$. Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött. Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$. Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$. De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,|$-nak. Ezért $7 \mid 6k$, ahonnan $(7, 6) = 1$ miatt $7 \mid k$. Így $k = 7$, és az is kijött, hogy $x^7 - 7 = m(x)$, vagyis $x^7 - 6$ *irreducibilis* $\mathbb{Q}(\sqrt[6]{7})$ *fölött.*

6. Az algebrai számok teste

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)
Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor *véges*, ha α *algebrai* K fölött. A $K \leq L$ *véges bővítés*, ha $|L : K|$ véges. Ekkor L minden eleme algebrai K fölött. A $K \leq L$ *algebrai bővítés*, ha L minden eleme algebrai K fölött. Tehát minden véges bővítés algebrai.

6.2.12. Tétel
Az L-nek a K fölött algebrai elemei résztestet alkotnak.

Speciálisan az algebrai számok $\mathbb{A}$ halmaza résztest $\mathbb{C}$-ben. Ez tehát az *algebrai számok teste*. A $\mathbb{Q} \leq \mathbb{A}$ bővítés algebrai (nyilván), de nem véges (HF).

Fok bővebb test fölött

6.2.5. Állítás
Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$. Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. □

6.2.8. Lemma
Elem foka nagyobb test fölött nem nőhet. Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az α minimálpolinomja K, illetve L fölött, akkor $s \in L[x]$ és $s(\alpha) = 0$ miatt $t \mid s$. Így $\mathrm{gr}_L(\alpha) = \mathrm{gr}(t) \leq \mathrm{gr}(s) = \mathrm{gr}_K(\alpha)$. □

Összeg és szorzat foka

6.2.10. Következmény
Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött. Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is *algebrai* K fölött, és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás
$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \leq K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \leq \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.
De $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$, így fokuk $\leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$. □

Így például $\sqrt[7]{3 - \sqrt[5]{23}} - \sqrt[4]{5 + i\sqrt{7 + \sqrt[6]{3}}}$ is algebrai szám. Foka legfeljebb $7 \cdot 5 \cdot 4 \cdot 2 \cdot 2 \cdot 6$.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)
Egy T test *algebrailag zárt,* ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF
Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt. Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak.

6.4.6, NB
Minden testnek van algebrailag zárt bővítése.

Ezért minden polinomnak számolhatunk formálisan a gyökeivel! Ez az algebrailag zárt bővítés analízis nélkül is megkonstruálható. Halmazelméleti (transzfinit) módszereket igényel.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel
Az algebrai számok $\mathbb{A}$ teste *algebrailag zárt.*

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1x + \ldots + a_kx^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám. Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is. Ezért az a_j elemekkel sorban bővítve mindegyik lépésben *véges* bővítést kapunk. Így $|\,\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}\,|$ *véges.*
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\,\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}\,|$ is véges. Beláttuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének, így algebrai szám. Tehát minden $f \in \mathbb{A}[x]$ komplex gyökei algebrai számok. Mivel $\mathbb{C}$ algebrailag zárt, f gyöktényezőkre bomlik $\mathbb{C}$ fölött. De minden gyöke $\mathbb{A}$-beli, és így $\mathbb{A}$ fölött is. □
A bizonyításban *kihasználtuk, hogy $\mathbb{C}$ algebrailag zárt!*

7. Összefoglaló

A 14. előadás összefoglalója

Fogalmak
Testbővítés. Generált résztest. Egyszerű bővítés, algebrai elem foka. Testbővítés foka. Véges és algebrai bővítés.

Tételek
Egyszerű bővítés elemeinek normálalakja az algebrai és transzcendens esetben. A testbővítések fokainak szorzástétele. Elem foka osztója a bővítés fokának. Véges és algebrai bővítés kapcsolata. Összeg és szorzat fokának becslése. Az algebrai elemek résztestet alkotnak. Az algebrai számok teste algebrailag zárt.