1. Generált résztest

Egyszerű testbővítés.

Ismétlés (6.1.16. Tétel)
Legyen K részteste L-nek, $\alpha \in L$ algebrai és $n = \mathrm{gr}(m_\alpha)$.
Ekkor az $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$ $(a_0, a_1, \ldots, a_{n-1} \in K)$ alakú elemek *résztestet* alkotnak L-ben. Jele: $K(\alpha)$.

Állítás
A $K(\alpha)$ a *legszűkebb* olyan részteste L-nek, amely K összes elemét és α-t is tartalmazza. Vagyis ha $T \leq L$ résztest, $K \subseteq T$ és $\alpha \in T$, akkor $K(\alpha) \subseteq T$.

Bizonyítás
Be kell látni, hogy $a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1} \in T$. Ez igaz, mert $a_j, \alpha \in T$, és T zárt az összeadásra, szorzásra.

A transzcendens eset.

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

Példa
$\dfrac{\pi^2 + 3\pi + 2}{\pi^2 + \pi}$ és $\dfrac{\pi^4 + 2\pi^3}{\pi^4}$ egyenlő elemei $\mathbb{Q}(\pi)$-nek.

Valóban: mindkét tört $\dfrac{\pi + 2}{\pi}$-vé egyszerűsíthető.

Generálás több elemmel.

6.1.5. Definíció
Legyen K részteste L-nek (ilyenkor *testbővítésről* beszélünk).
Egyszerű bővítés: $K \leq K(\alpha)$ alkalmas $\alpha \in L$-re.
Ha $\alpha, \beta, \ldots \in L$, akkor $K(\alpha, \beta, \ldots)$ 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 $K(\alpha) \subseteq T$.

$K(\alpha, \beta, \ldots)$ *létezik.* Úgy kapható, hogy vesszük az $\alpha, \beta, \ldots$ elemek összes, többhatározatlanú K-beli együtthatós polinomjait, majd ezek hányadosait.

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

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, és így 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 $p \in K[x_1, \ldots, x_n]$, vagyis *osztásra nincs szükség*.

2. 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 résztteste 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, HF
Ha $\alpha \in L$ transzcendens K fölött, akkor $|K(\alpha) : K|$ végtelen.

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.

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 $\gamma = c + d\sqrt{3}$.
Ezért $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}$ bázis 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. $\square$

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. $\square$

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 $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})$-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.