4. Testbővítések, Galois-elmélet

Testbővítések fajtái

4.1. Definíció. Ha a K test részteste az L testnek, akkor azt mondjuk, hogy L ***testbővítése*** K-nak, és ezt így jelöljük: $L \mid K$ (lásd az 1.21. Definíciót). Az $L_1 \mid K$ és $L_2 \mid K$ testbővítések ***izomorfak***, ha létezik olyan $\varphi\colon L_1 \to L_2$ izomorfizmus, amelynek K-ra való megszorítása identikus (azaz $a\varphi = a$ minden $a \in K$ esetén).

A továbbiakban – hacsak mást nem mondunk – $L \mid K$ mindig egy tetszőleges testbővítést jelöl.

4.2. Definíció. Tetszőleges $\vartheta \in L$ esetén jelölje I_ϑ mindazon $f \in K[x]$ polinomok halmazát, amelyeknek ϑ gyöke: $I_\vartheta = \{f \in K[x] : f(\vartheta) = 0\}$. Ha $I_\vartheta = \{0\}$, akkor azt mondjuk, hogy ϑ ***transzcendens*** K felett, ellenkező esetben pedig azt mondjuk, hogy ϑ ***algebrai*** K felett. Könnyen ellenőrizhető, hogy $I_\vartheta \lhd K[x]$ (HF), és mivel $K[x]$ főideálgyűrű, I_ϑ főideál. Ezért, ha ϑ algebrai K felett, akkor létezik egy olyan egyértelműen meghatározott $m_{\vartheta,K} \in K[x]$ főpolinom, amelyre $I_\vartheta = \langle m_{\vartheta,K}\rangle$. Ekkor tehát minden $f \in K[x]$ esetén $f(\vartheta) = 0 \iff m_{\vartheta,K} \mid f$. Az $m_{\vartheta,K}$ polinomot a ϑ elem K feletti ***minimálpolinomjának***, $m_{\vartheta,K}$ gyökeit pedig a ϑ elem K feletti ***konjugáltjainak*** nevezzük. Ha L minden eleme algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ ***algebrai testbővítés***, ellenkező esetben pedig ***transzcendens testbővítésről*** beszélünk.

4.3. Példa. A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai elemeit ***algebrai számoknak***, transzcendens elemeit pedig ***transzcendens számoknak*** nevezzük.

4.4. Állítás. Bármely $\vartheta \in L$ algebrai elem esetén $m_{\vartheta,K}$ irreducibilis K felett. Fordítva, ha $f \in K[x]$ irreducibilis K felett és $f(\vartheta) = 0$, akkor $f \sim m_{\vartheta,K}$.

Bizonyítás. Ha $m_{\vartheta,K} = f \cdot g$ $(f, g \in K[x])$, akkor $0 = m_{\vartheta,K}(\vartheta) = f(\vartheta) \cdot g(\vartheta)$, ezért $f(\vartheta) = 0$ vagy $g(\vartheta) = 0$. Az első esetben $m_{\vartheta,K} \mid f$, és így $f \sim m_{\vartheta,K}$ (miért?), a második esetben pedig $g \sim m_{\vartheta,K}$. Tehát az $m_{\vartheta,K} = f \cdot g$ felbontás triviális (minden $f, g \in K[x]$ esetén), azaz $m_{\vartheta,K}$ valóban irreducibilis. A második állítás igazolásához tegyük fel, hogy $f \in K[x]$ irreducibilis K felett és $f(\vartheta) = 0$. Ekkor $m_{\vartheta,K} \mid f$ (miért?), de mivel f irreducibilis, asszociáltság erejéig csak két osztója van: 1 és $m_{\vartheta,K}$. Nyilván nem lehetséges, hogy $m_{\vartheta,K} \sim 1$ (miért?), tehát $m_{\vartheta,K} \sim f$. □

4.5. Definíció. Tetszőleges $T \subseteq L$ halmaz esetén $K[T]$ jelöli a $K \cup T$ halmaz által generált részgyűrűt, és $K(T)$ jelöli a $K \cup T$ halmaz által generált résztestet L-ben. Ha $T = \{\vartheta\}$ egyelemű halmaz, akkor egyszerűen csak $K[\vartheta]$-t és $K(\vartheta)$-t írunk. A $K(\vartheta) \mid K$ alakú testbővítéseket ***egyszerű testbővítéseknek*** nevezzük (lásd az 1.23. Definíciót és az 1.22. Tételt), és azt mondjuk, hogy $K(\vartheta)$ a ϑ elem K-hoz történő ***adjungálásával*** keletkezik.

4.6. Definíció. Ha $L \mid K$ egy testbővítés, akkor L vektortertet alkot K felett. Ha ez a vektortér véges dimenziós, akkor azt mondjuk, hogy $L \mid K$ ***végesfokú testbővítés***, és a $\dim_K L$ dimenziót az $L \mid K$ bővítés ***fokszámának*** nevezzük. Jelölés: $[L : K] = \dim_K L$.

4.7. Tétel. Legyen $m \in K[x]$ irreducibilis n-edfokú polinom, és legyen $L = K[x]/\langle m\rangle$. Ekkor L test, amelyben a konstans polinomok modulo m maradékosztályai egy K-val izomorf résztestet alkotnak ($K \to L$, $a \mapsto a + \langle m\rangle$ beágyazás), tehát tekinthetjük úgy, hogy L bővítése K-nak. Ha az $x + \langle m\rangle \in L$ elemet α-val jelöljük, akkor L minden eleme egyértelműen előáll $a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$ $(a_{n-1}, \ldots, a_1, a_0 \in K)$ alakban. Következésképp $L = K[\alpha] = K(\alpha)$ és $[L : K] = n$. Az α elem gyöke az m polinomnak, tehát $m_{\alpha,K} \sim m$.

Bizonyítás. A 3.37. Tétel szerint $K[x]/\langle m\rangle$ valóban test, hiszen $K[x]$ főideálgyűrű és $m \in K[x]$ irreducibilis. A $K[x]/\langle m\rangle$ test elemei a K feletti polinomok modulo m maradékosztályai. A $g \in K[x]$ polinom maradékosztályát $g + \langle m\rangle$ helyett jelölje egyszerűen csak $\overline{g}$. A maradékos osztás tétele alapján minden maradékosztály egyértelműen reprezentálható egy n-nél kisebb fokú polinommal, azaz L minden eleme egyértelműen felírható $\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0}$ $(a_i \in K)$ alakban. Az $\alpha = \overline{x}$ jelölést használva ez így is írható: $\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = \overline{a_{n-1}} \cdot \overline{x}^{n-1} + \cdots + \overline{a_1} \cdot \overline{x} + \overline{a_0} = a_{n-1}\alpha^{n-1} + \cdots + a_1\alpha + a_0$. (Itt az $a_i \in K$ elemekről lehagytuk a vonásokat, mert a K testet azonosítjuk az L-be beágyazott izomorf „másolatával”.) Összefoglalva, azt kaptuk, hogy

$$\forall \beta \in L\ \exists! a_0, a_1, \ldots, a_{n-1} \in K\colon \beta = a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1}. \qquad (\diamondsuit)$$

Ez azt jelenti, hogy L minden eleme felírható, mégpedig egyértelműen, az $1, \alpha, \ldots, \alpha^{n-1}$ elemek K-beli együtthatós lineáris kombinációjaként. Tehát $1, \alpha, \ldots, \alpha^{n-1}$ bázisa az ${}_KL$ vektortérnek, és így $[L : K] = \dim_K L = n$. Az is kiolvasható $(\diamondsuit)$-ból, hogy L minden elme előáll α-ból és K elemeiből az első három alapművelet segítségével, azaz $L \subseteq K[\alpha]$. Mivel $K[\alpha] \subseteq K(\alpha) \subseteq L$, az következik, hogy $L = K[\alpha] = K(\alpha)$.

Az utolsó állítás igazolásához írjuk fel az m polinomot: $m = c_nx^n + \cdots + c_1x + c_0 \in K[x]$. Számítsuk ki $m(\alpha)$ értékét (ismét az $\alpha = \overline{x}$ jelölést használjuk, és a K-beli konstansokra visszatesszük a vonásokat):

$$m(\alpha) = c_n\alpha^n + \cdots + c_1\alpha + c_0 = \overline{c_n} \cdot \overline{x}^n + \cdots + \overline{c_1} \cdot \overline{x} + \overline{c_0} = \overline{c_nx^n + \cdots + c_1x + c_0} = \overline{m}.$$

Az világos, hogy $\overline{m} = \overline{0}$ (miért?), tehát $m(\alpha) = \overline{0} = 0$. A 4.4. Állítás alapján ebből és m irreducibilitásából már következik, hogy $m_{\alpha,K} \sim m$. □

4.8. Tétel. Legyen $L = K(\vartheta)$ egyszerű algebrai bővítése K-nak, és legyen az $m = m_{\vartheta,K}$ polinom fokszáma n. Ekkor az $L \mid K$ bővítés izomorf a $K[x]/\langle m\rangle \mid K$ bővítéssel, és így $[L:K] = n$.

Bizonyítás. Tekintsük a $\varphi\colon K[x] \to L$, $f \mapsto f(\vartheta)$ „kiértékelő" leképezést. Könnyen ellenőrizhető, hogy φ gyűrűhomomorfizmus (HF). Az 1.22. Tétel szerint φ értékkészlete $K[\vartheta]$, a 4.2. Definíció szerint pedig φ magja $\operatorname{Ker}\varphi = I_\vartheta = \langle m\rangle$. A gyűrűelméleti homomorfiatételt alkalmazva azt kapjuk, hogy $K[x]/\langle m\rangle \cong K[\vartheta]$. A homomorfiatétel által szolgáltatott izomorfizmus a következő:

$$\psi\colon K[x]/\langle m\rangle \to K[\vartheta],\ a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} \mapsto a_0 + a_1\vartheta + \dots + a_{n-1}\vartheta^{n-1}. \qquad (\heartsuit)$$

(Itt kihasználtuk azt, hogy, az előző tétel jelöléseit használva, $K[x]/\langle m\rangle$ elmei egyértelműen írhatók $a_0 + a_1\alpha + \dots + a_{n-1}\alpha^{n-1} = a_0 + a_1\overline{x} + \dots + a_{n-1}\overline{x}^{n-1}$ $(a_i \in K)$ alakba.) Tudjuk, hogy m irreducibilis (4.4. Állítás), ezért $K[x]/\langle m\rangle$ test (3.37. Tétel). Mivel a $K[x]/\langle m\rangle$ és $K[\vartheta]$ gyűrűk izomorfak, és a $K[x]/\langle m\rangle$ gyűrűről most láttuk be, hogy test, az következik, hogy $K[\vartheta]$ is test, és így $K[\vartheta] = K(\vartheta)$. Tehát ψ izomorfizmust létesít a $K[x]/\langle m\rangle$ és $L = K(\vartheta)$ testek között, és $(\heartsuit)$-ből látható, hogy minden $a_0 \in K$ esetén $a_0\psi = a_0$. A 4.1. Definíció szerint ez épp azt jelenti, hogy $L \mid K$ izomorf a $K[x]/\langle m\rangle \mid K$ bővítéssel. Emiatt a két bővítés fokszáma is megegyezik, a $K[x]/\langle m\rangle \mid K$ bővítésről pedig az előző tétel alapján tudjuk, hogy n-edfokú, így $[L:K] = n$. □

4.9. Tétel. A $K(x) \mid K$ bővítés egyszerű transzcendens bővítés. Fordítva, ha $L = K(\vartheta)$ egyszerű transzcendens bővítése K-nak, akkor az $L \mid K$ bővítés izomorf a $K(x) \mid K$ bővítéssel, és $[L:K] = \infty$.

4.10. Tétel. Legyenek $L \mid K$ és $M \mid L$ végesfokú testbővítések (tehát $K \le L \le M$), és legyen $\alpha_1, \dots, \alpha_\ell$ bázisa az ${}_KL$ vektortérnek, $\beta_1, \dots, \beta_m$ pedig legyen egy bázisa az ${}_LM$ vektortérnek. Ekkor $\alpha_i\beta_j$ $(i = 1, \dots, \ell,\ j = 1, \dots, m)$ bázisa az ${}_KM$ vektortérnek. Következésképp $[M:K] = [M:L]\cdot[L:K] = m\cdot\ell$.

Bizonyítás. Tudjuk, hogy M minden μ eleme előáll a β_j elemek L-beli együtthatókkal felírt lineáris kombinációjaként. Itt minden együtthatót fel lehet írni az α_i elemek K-beli együtthatós lineáris kombinációjaként. Ezeket behelyettesítve a megfelelő együtthatók helyére, megkapjuk μ előállítását az $\alpha_i\beta_j$ elemek K-beli együtthatós lineáris kombinációjaként (HF felírni). Ezzel beláttuk, hogy az $\alpha_i\beta_j$ elemek generálják az ${}_KM$ vektorteret. A lineáris függetlenség igazolásához tegyük fel, hogy $\sum_{i,j} c_{ij}\alpha_i\beta_j = 0$ $(c_{ij} \in K)$. Átrendezve az összeget azt kapjuk, hogy $\sum_j \left(\sum_i c_{ij}\alpha_i\right)\beta_j = 0$. A β_j elemek L feletti lineáris függetlensége miatt $\sum_i c_{ij}\alpha_i = 0$ minden j esetén. Ebből pedig az α_i elemek K feletti lineáris függetlensége miatt következik, hogy $c_{ij} = 0$ minden i és j esetén. □

4.11. Tétel. Minden végesfokú bővítés algebrai. Nulla karakterisztikájú testek (pl. számtestek) esetén minden végesfokú bővítés egyszerű algebrai bővítés: ha $\operatorname{char} K = 0$ és $[L:K] < \infty$, akkor létezik olyan $\vartheta \in L$ ***primitív elem***, amelyre $L = K(\vartheta)$.

Bizonyítás. Csak az első állítást bizonyítjuk. Legyen $[L:K] = n$, és legyen $\vartheta \in L$ tetszőleges elem. Ekkor $1, \vartheta, \dots, \vartheta^n$ lineárisan függők K felett (miért?), tehát vannak olyan $a_0, a_1, \dots, a_n \in K$ elemek, amelyek közül legalább az egyik nem 0, és $a_0\cdot 1 + a_1\cdot\vartheta + \dots + a_n\cdot\vartheta^n = 0$. Ebből következik, hogy ϑ gyöke a nemnulla $f = a_nx^n + \dots + a_1x + a_0 \in K[x]$ polinomnak. (Az nem biztos, hogy $\deg f = n$, mert nem biztos, hogy $a_n \neq 0$. De az a_i együtthatók között van legalább egy nemzérus, tehát $f \neq 0$.) Látjuk tehát, hogy L minden eleme algebrai K felett, azaz $L \mid K$ valóban algebrai bővítés. □

4.12. Tétel. Minden testbővítésben az algebrai elemek résztestet alkotnak. Így például az algebrai számok is testet alkotnak (lásd a 4.3. Példát).

Bizonyítás. Legyenek $\alpha, \beta \in L$ algebrai elemek K felett, rendre n-edfokú és m-edfokú minimálpolinommal, és tekintsük a $K \le K(\alpha) \le K(\alpha)(\beta) = K(\alpha,\beta)$ testtornyot. A 4.8. Tétel szerint $[K(\alpha):K] = \deg m_{\alpha,K} = n$ és $[K(\alpha)(\beta):K(\alpha)] = \deg m_{\beta,K(\alpha)} \le \deg m_{\beta,K} = m$ (miért?). A 4.10. Tétel segítségével felülről becsülhetjük a $K(\alpha,\beta) \mid K$ bővítés fokát: $[K(\alpha,\beta):K] = [K(\alpha,\beta):K(\alpha)]\cdot[K(\alpha):K] \le m\cdot n$. Tehát $K(\alpha,\beta) \mid K$ végesfokú bővítés, és így a 4.11. Tételből következik, hogy $K(\alpha,\beta)$ minden eleme algebrai K felett. Ezen elemek között pedig ott van $\alpha+\beta$, $\alpha-\beta$, $\alpha\cdot\beta$ és $(\beta \neq 0$ esetén) α/β is. Ezzel beláttuk, hogy a K felett algebrai elemek halmaza zárt a négy alapműveletre. □

4.13. Definíció. Ha egy L testre teljesülnek az alábbi (egymással ekvivalens) feltételek, akkor azt mondjuk, hogy L ***algebrailag zárt***.

(1) Minden nemkonstans L feletti polinomnak van gyöke L-ben.
(2) Minden nemkonstans L feletti polinom elsőfokú polinomok szorzatára bomlik az $L[x]$ polinomgyűrűben.
(3) A L test felett csak az elsőfokú polinomok irreducibilisek.

Azt mondjuk, hogy L ***algebrai lezártja*** K-nak, ha L algebrailag zárt, és $L \mid K$ algebrai bővítés (jelölés: $L = \overline{K}$).

4.14. Tétel. Minden K testnek létezik algebrai lezártja, és az K feletti izomorfia erejéig egyértelmű (vagyis ha L_1 és L_2 is algebrai lezártja K-nak, akkor van olyan $\varphi\colon L_1 \to L_2$ izomorfizmus, amelynek K-ra való megszorítása identikus).

4.15. Megjegyzés. Algebrailag zárt testnek nincs valódi algebrai bővítése, tehát $\overline{K}$ maximális algebrai bővítése K-nak. Másrészt, $\overline{K}$ valódi résztestei már nem lesznek algebrailag zártak, tehát $\overline{K}$ minimális algebrailag zárt bővítése K-nak. Meg lehet mutatni, hogy ezen két tulajdonság bármelyike jellemzi az algebrai lezártat.

4.16. Példa. Az algebra alaptétele szerint a komplex számok teste algebrailag zárt. Mivel $\mathbb{C} \mid \mathbb{R}$ algebrai (miért?), $\overline{\mathbb{R}} = \mathbb{C}$. Ebben nem az a „pláne", hogy $\mathbb{R}$-nek van algebrai lezártja, hanem az, hogy az algebrai lezárt mindössze másodfokú bővítés: elég az x^2+1 polinom egy gyökét adjungálni, és máris minden polinomnak lesz gyöke. A racionális számok testével más a helyzet: $\overline{\mathbb{Q}}$ nem más, mint az algebrai számok teste (lásd a 4.3. Példát), és $\overline{\mathbb{Q}} \mid \mathbb{Q}$ végtelen fokú bővítés (miért?).