

1. Tétel (Egyszerű bővítés előállítása faktorgyűrűként)

Ha $K \leq L$ testek és $\alpha \in L$ algebrai K fölött, akkor $K(\alpha) \cong K[x]/(p(x))$ valamely $p(x) \in K[x]$ irreducibilis polinomra, amelyre $p(\alpha) = 0$

Biz.: Tekintsük a $\varphi : K[x] \rightarrow L$, $f(x) \mapsto f(\alpha)$ gyűrűhomomorfizmust.

$$\text{Ker } \varphi = \{ f(x) \in K[x] \mid f(\alpha) = 0 \} \triangleleft K[x],$$

és $\neq 0$, mivel α algebrai. De $K[x]$ főideálgyűrű, így van olyan $0 \neq p(x) \in K[x]$ polinom, hogy $\text{Ker } \varphi = (p(x))$. A homomorfizmustétel szerint

$$K[x]/(p(x)) = K[x]/\text{Ker } \varphi \cong \text{Im } \varphi, \text{ ami részgyűrűje } L\text{-nek,}$$

ezért $K[x]/(p(x))$ 0-osztómentes $\Rightarrow p(x)$ irreducibilis. De akkor $(p(x))$ maximális ideál $K[x]$ -ben, tehát $K[x]/(p(x))$, és így a vele izomorf $\text{Im } \varphi$ is, test.

$\forall c \in K$, $\varphi(c) = c$, és $\varphi(x) = \alpha$, így $K(\alpha) \leq \text{Im } \varphi$, másrészt $\text{Im } \varphi = \{ f(\alpha) \mid f(x) \in K[x] \}$ nyilván benne van $K(\alpha)$ -ban. Tehát

$$K(\alpha) = \text{Im } \varphi \cong K[x]/(p(x)).$$

2. Tétel (Algebrai bővítések egymásutánja)

Ha $K \leq L \leq M$ testek, ahol $L|K$ és $M|L$ algebrai, akkor $M|K$ is algebrai.

Biz.: Legyen $\alpha \in M$. Mivel $M|L$ algebrai,

$$\exists 0 \neq f(x) = a_n x^n + \dots + a_1 x + a_0 \in L[x], \text{ hogy } f(\alpha) = 0.$$

Legyen $K_i = K(a_0, \dots, a_i)$ ($i = 0, 1, \dots, n$). Ekkor $f(x) \in K_n[x]$, tehát α algebrai K_n fölött is, s mivel $K_n(\alpha)|K_n$ egyszerű bővítés, véges fokú is. Minden i -re $a_i \in L$, tehát a_i algebrai K fölött, és így K_{i-1} fölött is, amiből $(K_i : K_{i-1}) = (K_{i-1}(a_i) : K_{i-1}) < \infty \forall i$, és $(K_0 : K) = (K(a_0) : K) < \infty$ is következik. A szorzattétel szerint

$$(K_n(\alpha) : K) = (K_n(\alpha) : K_n) \cdot (K_n : K_{n-1}) \cdots (K_1 : K_0) \cdot (K_0 : K) < \infty,$$

ezért α algebrai K fölött.

3. Tétel (Véges normális bővítések jellemzése)

Az $N|K$ véges fokú bővítés pontosan akkor normális, ha valamely K fölötti polinom felbontási teste.

Biz.: \Rightarrow : Mivel $(N : K) < \infty$, van véges sok olyan algebrai elem, $\alpha_1, \dots, \alpha_n \in N$, hogy $N = K(\alpha_1, \dots, \alpha_n)$. Legyen $p_i(x) \in K[x]$ az α_i minimálpolinomja minden i -re, és $f(x) = p_1(x) \cdots p_n(x) \in K[x]$. A $p_i(x)$ polinomok irreducibilisek, és van N -ben gyökük, ezért a bővítés normalitása miatt lineáris faktorokra bomlanak, és így $f(x)$ is lineáris faktorokra bomlik. Másrészt a bővítést generálja f néhány gyöke, tehát N az f felbontási teste K fölött.

\Leftarrow : Legyen N az $f(x) \in K[x]$ felbontási teste, tehát f felbomlik N fölött:

$$f(x) = (x - \alpha_1) \cdots (x - \alpha_n), \text{ és } N = K(\alpha_1, \dots, \alpha_n).$$

Legyen továbbá $p(x) \in K[x]$ irreducibilis, amelynek van gyöke N -ben: $p(\beta) = 0$ valamely $\beta \in N$ -re. Mivel $N = K(\alpha_1, \dots, \alpha_n)$, a β elem előáll az α_i -k polinomjaként: $\beta = g(\alpha_1, \dots, \alpha_n)$ valamely $g(x_1, \dots, x_n) \in K[x_1, \dots, x_n]$ többváltozós polinomra. Legyen

$$h(x) = \prod_{\sigma \in S_n} (x - g(\alpha_{1\sigma}, \dots, \alpha_{n\sigma})).$$

Ez a polinom invariáns az α_i -k permutációira, így az együtthatói α_i -knek szimmetrikus polinomjai, tehát α_i -k elemi szimmetrikus polinomjainak polinomjai. Ezek az elemi szimmetrikus polinomok pedig — előjeltől eltekintve — az f együtthatói, ezért $h(x) \in K[x]$. De $(x - \beta) \mid h(x) \Rightarrow h(\beta) = 0 \Rightarrow p(x) \mid h(x)$. De $h(x)$ felbomlik lineáris tényezőkre szorzatára N fölött, tehát $p(x)$ is felbomlik.

4. Tétel (Véges szeparábilis bővítés egyszerűsége)

Ha $L|K$ véges fokú szeparábilis bővítés, akkor van olyan $\gamma \in L$, hogy $L = K(\gamma)$.

Biz.: Ha K véges test, akkor L is az, és akkor az L^\times ciklikus csoport generátoreleme megfelel γ -nak. Ezért a továbbiakban feltesszük, hogy K végtelen.

$L = K(\gamma_1, \dots, \gamma_k)$. Mivel $K \leq M \leq L$ -re $M|K$ is szeparábilis, elég azt belátni, hogy minden $\alpha, \beta \in L$ -re van olyan γ , amelyre $K(\alpha, \beta) = K(\gamma)$.

Legyen $f(x), g(x) \in K[x]$ az α , illetve β minimálpolinomja, és $F \geq L$ az $f(x)g(x)$ felbontási teste L fölött. F -ben $f(x) = (x - \alpha_1) \cdots (x - \alpha_n)$ és $g(x) = (x - \beta_1) \cdots (x - \beta_m)$, ahol $\alpha = \alpha_1, \dots, \alpha_n$, illetve $\beta = \beta_1, \dots, \beta_m$ különbözők az $L|K$ szeparabilitása miatt. Mivel K végtelen, van olyan $c \in K$, amelyre $\gamma := \alpha + c\beta \neq \alpha_i + c\beta_j$ minden $(i, j) \neq (1, 1)$ -re. Megmutatjuk, hogy erre a γ -ra $K(\alpha, \beta) = K(\gamma)$.

A $g(x), f(\gamma - cx) \in K(\gamma)[x]$ polinomoknak a felbontási testben egyetlen közös gyöke a β , így a legnagyobb közös osztójuk $F[x]$ -ben, és így $K(\gamma)[x]$ -ben is, $x - \beta$. Ezért $\beta \in K(\gamma)$, amiből $\alpha = \gamma - c\beta \in K(\gamma) \Rightarrow K(\alpha, \beta) \leq K(\gamma) \Rightarrow K(\alpha, \beta) = K(\gamma)$.

5. Tétel (A Galois-elmélet főtétele)

Legyen $G = \text{Gal}(L|K)$, $K \leq M \leq L$, $H \leq G$. Ekkor

$M^{**} = M$ és $H^{**} = H$, így a $*$ Galois-kapcsolat rendezésfordító bijekció G részcsoportjai és $L|K$ közbülső testeinek között.

Biz.:

$M^{**} = M$: Tudjuk, hogy $M^{**} \geq M$. Másrészt $|M^*| = |\text{Gal}(L|M)| = (L : M)$, és ugyanezt M^{**} -ra alkalmazva, $|M^{***}| = |\text{Gal}(L|M^{**})| = (L : M^{**})$, s mivel $M^{***} = M^*$, azt kapjuk, hogy $(L : M) = (L : M^{**})$, amiből $(M : K) = \frac{(L : K)}{(L : M)} = \frac{(L : K)}{(L : M^{**})} = (M^{**} : K)$. Ez az $M^{**} \geq M$ tartalmazással együtt azt adja, hogy $M^{**} = M$.

$H^{**} = H$: Tudjuk, hogy $H^{**} \geq H$. Mivel $L|H^*$ Galois-bővítés, van olyan $\alpha \in L$, amelyre $L = H^*(\alpha)$. Legyenek α képei a H elemeinél $\alpha_1, \alpha_2, \dots, \alpha_t$, ahol $|H| = t$, és $\alpha = \alpha_1$, és tekintsük a $h(x) = \prod_{i=1}^t (x - \alpha_i) \in L[x]$ polinomot. Ez a polinom invariáns H -ra nézve, mert H elemei permutálják az α_i -ket. Ebből következik, hogy a polinom együtthatói is H -invariánsak, azaz $h(x) \in H^*[x]$, így α H^* fölötti minimálpolinomja osztója $h(x)$ -nek.

Következésképpen $|H^{**}| = |\text{Gal}(L|H^*)| = (L : H^*) \leq \deg h(x) = |H|$. Ez az $H^{**} \geq H$ tartalmazással együtt azt adja, hogy $H^{**} = H$.

6. Tétel (Az algebra alaptétele)

\mathbb{C} fölött minden nem konstans polinomnak van gyöke.

Biz.: Azt kell belátni, hogy $\mathbb{C}[x]$ -ben minden irreducibilis polinom elsőfokú, azaz hogy \mathbb{C} -nek nincs véges fokú bővítése.

Tegyük fel, hogy nem igaz az állítás. Legyen $L \geq \mathbb{C}$ véges fokú bővítés, ahol $L \neq \mathbb{C}$. Feltehető, hogy L normális \mathbb{R} fölött (és így \mathbb{C} fölött is): ha nem lenne az, akkor is egyszerű bővítése \mathbb{R} -nek, és akkor vehetjük L helyett a bővítést adó elem \mathbb{R} fölötti minimálpolinomjának felbontási testét, az is véges fokú bővítés.

Tekintsük az $\mathbb{R} \leq \mathbb{C} \leq L$ bővítéssorozatot, és a $G = \text{Gal}(L|\mathbb{R})$ Galois-csoportot. Legyen $|G| = 2^k m$, ahol m páratlan. Ha $P \in \text{Syl}_2(G)$, akkor $(P^* : \mathbb{R}) = |G : P| = m$ páratlan, de \mathbb{R} -nek nincs páratlan fokú valódi bővítése, ugyanis \mathbb{R} -en kívüli elemnek nem lehet páratlan fokú minimálpolinomja, mert minden páratlan fokú valós polinomnak van valós gyöke a Bolzano-tétel miatt. Tehát $m = 1 \Rightarrow (L : \mathbb{R}) = |G| = 2^k \Rightarrow (L : \mathbb{C}) = 2^{k-1}$.

Legyen $G_1 = \text{Gal}(L|\mathbb{C})$. Mivel G_1 2-csoport, $\exists G_2 \leq G_1$, hogy $|G_1 : G_2| = 2$. De akkor az $L|\mathbb{C}$ bővítés és G_1 közötti Galois-kapcsolatot használva azt kapjuk, hogy G_2^* a \mathbb{C} -nek másodfokú bővítése, holott ilyen nem létezik, mert \mathbb{C} fölött minden másodfokú egyenlet megoldható. Ezzel ellentmondásra jutottunk.