8. FELBONTÁSI TEST, NORMÁLIS BŐVÍTÉS, GYÖKBŐVÍTÉS

8.A.Definíció. Egy $f(x) \in K[x]$ **polinomnak a** $K \subseteq \mathbb{C}$ **számtest feletti felbontási testén** a

$$K(f(x) = 0) = K(\alpha_1, \alpha_2, ..., \alpha_t)$$

alakban jelölt bővített számtestet értjük, ahol

$$f(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2}...(x - \alpha_t)^{k_t}$$

az $f(x)$ polinom gyöktényezős felbontása (itt $a_n \in K$ az $f(x)$ főegyütthatója és $\alpha_1, \alpha_2, ..., \alpha_t \in \mathbb{C}$ az $f(x)$ összes gyökei ismétlődés nélkül). A 7.4.Állítás szerint $K \subseteq K(f(x) = 0)$ véges bővítés.♡

8.B.Definíció. A $K \subseteq L$ (itt $L \subseteq \mathbb{C}$) **testbővítésről** azt mondjuk, hogy **normális**, ha nem létezik olyan K felett irreducibilis $p(x) \in K[x]$ polinom, amelynek van L-beli gyöke és L-en kívüli gyöke is. Tehát $K \subseteq L$ pontosan akkor normális, ha minden $K[x]$-ben irreducibilis $p(x)$ polinomra teljesül az alábbi esetek valamelyike:

1. $p(x)$ minden gyöke L-ben van.
2. $p(x)$-nek nem létezik gyöke L-ben.

Tetszőleges $K \subseteq \mathbb{C}$ számtestre a $K \subseteq \mathbb{C}$ bővítés nyilvánvalóan normális.♡

8.1.Állítás. *Ha $K \subseteq L$ véges és normális testbővítés (itt $L \subseteq \mathbb{C}$), akkor létezik olyan K felett irreducibilis $p(x) \in K[x]$ polinom, amelynek a K feletti felbontási teste az L, azaz*

$$L = K(p(x) = 0).$$

Bizonyítás. A 7.6.Tétel szerint létezik olyan K felett algebrai $\alpha \in L$ szám, amelyre $K(\alpha) = L$. Mivel az α-nak a K feletti $p(x) \in K[x]$ minimál polinomja irreducibilis $K[x]$-ben és $p(x)$-nek az α gyöke L-beli, ezért a $K \subseteq L$ bővítés normalitása azt eredményezi, hogy $p(x)$ minden gyöke L-ben van. Így az $L = K(\alpha) \subseteq K(p(x) = 0) \subseteq L$ tartalmazások teljesülnek, amelyekből a kívánt $L = K(p(x) = 0)$ egyenlőséget kapjuk.

□□□

8.2.Tétel. *Tetszőleges $f(x) = a_0 + a_1x + ... + a_nx^n \in K[x]$ polinomnak a $K \subseteq \mathbb{C}$ számtest feletti felbontási teste K-nak normális bővítése, azaz $K \subseteq K(f(x) = 0)$ normális bővítés.*

Bizonyítás. Tekintsünk egy olyan K felett irreducibilis $p(x) \in K[x]$ polinomot, amelynek létezik egy $\gamma \in K(f(x) = 0)$ gyöke. Ha

$$f(x) = a_n(x - \alpha_1)^{k_1}(x - \alpha_2)^{k_2}...(x - \alpha_t)^{k_t}$$

az $f(x)$ polinom gyöktényezős felbontása (itt $0 \neq a_n \in K$ az $f(x)$ főegyütthatója és $\alpha_1, \alpha_2, ..., \alpha_t \in \mathbb{C}$ az $f(x)$ összes gyökei ismétlődés nélkül), akkor $K(f(x) = 0) = K(\alpha_1, \alpha_2, ..., \alpha_t)$. A 7.4.Állítás szerint van olyan t változós $g(x_1, x_2, ..., x_t) \in K[x_1, x_2, ..., x_t]$ polinom, amelyre

$$\gamma = g(\alpha_1, \alpha_2, ..., \alpha_t).$$

Legyen most $\beta_1, \beta_2, ..., \beta_n \in \mathbb{C}$ az $f(x)$ gyökeinek multiplicitással történő olyan felsorolása (ebben α_i pontosan k_i-szer fordul elő), amelyben $\beta_i = \alpha_i$ teljesül az $1 \leq i \leq t$ indexekre (itt $n = \deg(f(x)) = k_1 + k_2 + ... + k_t$), ekkor

$$f(x) = a_n(x - \beta_1)(x - \beta_2)...(x - \beta_n).$$

A $g(x_1, x_2, ..., x_t)$ polinomot nyilvánvalóan tekinthetjük olyan n változós

$$g(x_1, x_2, ..., x_t) = g(x_1, x_2, ..., x_t, x_{t+1}, ..., x_n) \in K[x_1, x_2, ..., x_t, x_{t+1}, ..., x_n]$$

polinomnak is, amelyben nem szerepelnek az $x_{t+1}, x_{t+2}, ..., x_n$ változók. Így a helyettesítési értékekre teljesülnek az alábbiak

$$g(\alpha_1, \alpha_2, ..., \alpha_t) = g(\beta_1, \beta_2, ..., \beta_t) = g(\beta_1, \beta_2, ..., \beta_t, \beta_{t+1}, ..., \beta_n).$$

A $\beta_1, \beta_2, ..., \beta_n$ gyökök minden lehetséges $\beta_{\pi(1)}, \beta_{\pi(2)}, ..., \beta_{\pi(n)}$ permutációjával képezzük a $g(x_1, x_2, ..., x_t, x_{t+1}, ..., x_n)$ polinom helyettesítési értékét

$$\gamma_\pi = g(\beta_{\pi(1)}, \beta_{\pi(2)}, ..., \beta_{\pi(n)}) \in K(\beta_1, \beta_2, ..., \beta_n) = K(\alpha_1, \alpha_2, ..., \alpha_t)$$

és tekintsük az alábbi $K(\alpha_1, \alpha_2, ..., \alpha_t)[x]$-beli

$$h(x) = \prod_{\pi \in \mathrm{Sym}(\{1,2,...,n\})} (x - \gamma_\pi) = \prod_{\pi \in \mathrm{Sym}(\{1,2,...,n\})} (x - g(\beta_{\pi(1)}, \beta_{\pi(2)}, ..., \beta_{\pi(n)}))$$

polinomot. Ekkor $\deg(h(x)) = n!$ és az identikus $\mathrm{id} \in \mathrm{Sym}(\{1, 2, ..., n\})$ permutációval kapjuk a $\gamma_{\mathrm{id}} = g(\alpha_1, \alpha_2, ..., \alpha_n) = \gamma$ közös gyökét a $p(x)$ és a $h(x)$ polinomoknak. A $p(x)$-nek a $K[x]$-beli irreducibilitása és a $h(x) \in K[x]$ tartalmazás igazolása lehetővé teszi a 4.5.Állítás 4.részének az alkalmazását, amiből a $p(x) \mid h(x)$ oszthatóságot kapjuk. Tehát $p(x)$ minden gyöke a $h(x)$-nek is gyöke, azaz $p(x)$ minden gyöke $\gamma_\pi = g(\alpha_{\pi(1)}, \alpha_{\pi(2)}, ..., \alpha_{\pi(n)})$ alakban írható valamilyen $\pi \in \mathrm{Sym}(\{1, 2, ..., n\})$ permutációval. Végeredményben azt kaptuk, hogy $p(x)$ minden gyöke $K(\alpha_1, \alpha_2, ..., \alpha_t)$-beli, ami a $K \subseteq K(\alpha_1, \alpha_2, ..., \alpha_t)$ bővítés normalitását eredményezi.
A $h(x) \in K[x]$ tartalmazás igazolása következik. A $h(x)$ értelmezésében a szorzás elvégzésével olyan polinomot kapunk, amelynek bármely együtthatója valamilyen n változós K-beli együtthatós polinomnak a $\beta_1, \beta_2, ..., \beta_n \in \mathbb{C}$ számokon felvett helyettesítési értéke, azaz

$$h(x) = x^m + b_{m-1}(\beta_1, \beta_2, ..., \beta_n)x^{m-1} + ... + b_k(\beta_1, \beta_2, ..., \beta_n)x^k + ... + b_1(\beta_1, \beta_2, ..., \beta_n)x + b_0(\beta_1, \beta_2, ..., \beta_n),$$

ahol $m = n!$ és $b_k(x_1, ..., x_n) \in K[x_1, ..., x_n]$.
Mivel β_i és β_j felcserélése a $h(x)$ polinomot nem változtatja meg, ezért ez a csere változatlanul hagyja a $b_k(\beta_1, \beta_2, ..., \beta_n)$, $0 \leq k \leq m - 1$ együtthatókat is.
Tehát a $b_k(x_1, ..., x_n)$, $0 \leq k \leq m - 1$ polinomok mindegyike szimmetrikus. A 6.5.Tétel szerint minden $K[x_1, x_2, ..., x_n]$-beli szimmetrikus polinom kifejezhető a $K[x_1, x_2, ..., x_n]$-beli elemi szimmetrikus polinomok K-beli együtthatós polinomjaként, ezért

$$b_k(x_1, ..., x_n) = F_k(s_1, ..., s_n)$$

alkalmas $F_k(x_1,...,x_n) \in K[x_1,...,x_n]$ polinommal. Egy $s_i(x_1,...,x_n)$ elemi szimmetrikus polinomnak a $(\beta_1,\beta_2,...,\beta_n)$ helyen felvett helyettesítési értékét (Viete képleteit, azaz a 6.6.Állítást felhasználva) az $f(x)$-nek a K-ban található együtthatóival adhatjuk meg:

$$s_i(\beta_1,\beta_2,...,\beta_n) = (-1)^i \frac{a_{n-i}}{a_n} \in K$$

Tehát

$$b_k(\beta_1,\beta_2,...,\beta_n) = F_k(s_1(\beta_1,\beta_2,...,\beta_n),...,s_n(\beta_1,\beta_2,...,\beta_n)) = F_k(-\frac{a_{n-1}}{a_n},...,(-1)^i\frac{a_{n-i}}{a_n},...,(-1)^n\frac{a_0}{a_n}) \in K,$$

azaz $h(x)$ együtthatói valóban K-beliek.

□□□

Megjegyzés. A későbbiekben a $K \subseteq K(f(x)=0)$ bővítés normalitását, a 9.5.Következményt és a 9.6.Állítást felhasználva könnyen megkaphatjuk, hogy

$$[K(f(x)=0):K] \leq t!\ ,$$

ahol a $t \geq 1$ az $f(x) \in K[x]$ polinom (különböző) gyökeinek a számát jelenti.

8.3.Állítás. *Ha $K \subseteq L$ véges és normális testbővítés (itt $L \subseteq \mathbb{C}$), akkor bármely $K \subseteq T \subseteq L$ köztes számtestnek az L normális bővítése, azaz $T \subseteq L$ (véges és) normális.*
Ha $K \subseteq L_1$ és $K \subseteq L_2$ véges normális bővítések, akkor a $K \subseteq L_1 \vee L_2$ bővítés is (véges és) normális.

Bizonyítás. A 8.1.Állítás szerint létezik olyan K felett irreducibilis $p(x) \in K[x]$ polinom, amelynek a K feletti felbontási testére $L = K(p(x)=0)$. Mivel $K \subseteq T \subseteq L$ miatt $p(x) \in T[x]$ és $L = K(p(x)=0) \subseteq T(p(x)=0) \subseteq L$, ezért a $p(x) \in T[x]$ polinomnak a T feletti felbontási testére $L = T(p(x)=0)$ teljesül. Így a 8.2.Tételre való tekintettel kapjuk, hogy a $T \subseteq L$ bővítés is normális.
A 8.1.Állítás szerint léteznek olyan K felett irreducibilis $p_1(x), p_2(x) \in K[x]$ polinomok, amelyekre $L_1 = K(p_1(x)=0)$ és $L_2 = K(p_2(x)=0)$. Most

$$L_1 \vee L_2 = K(p_1(x)=0) \vee K(p_2(x)=0) = K(p_1(x)p_2(x)=0)$$

a $p_1(x)p_2(x) \in K[x]$ szorzat polinom K feletti felbontási teste, ami a 8.2.Tétel szerint normális bővítése K-nak.

□□□

8.C.Definíció. A $K \subseteq L$ (itt $L \subseteq \mathbb{C}$) **testbővítésről** azt mondjuk, hogy **elemi gyökbővítés**, ha létezik olyan $c \in K$ elem és $n \geq 1$ egész, hogy az $x^n - c \in K[x]$ polinomnak a K-feletti felbontási teste az L számtest: $K(x^n - c = 0) = L$. Az $x^n - c \in K[x]$ polinomnak a K-feletti felbontási teste pontosan akkor lesz az L számtest, ha van olyan $b \in L$ elem és $\varepsilon \in \mathbb{C}$ primitív n-edik egységgyök, amelyre $b^n - c = 0$ és $L = K(b,\varepsilon)$. Minden felbontási test (véges) normális bővítése az alaptestnek, ezért egy elemi gyökbővítés (véges és) normális.
A $K \subseteq L$ testbővítésről azt mondjuk, hogy **gyökbővítés**, ha létezik köztes számtesteknek olyan

$$K = T_0 \subseteq T_1 \subseteq ... \subseteq T_{m-1} \subseteq T_m = L$$

sorozata, amelyben minden $0 \leq i \leq m-1$ egészre $T_i \subseteq T_{i+1}$ elemi gyökbővítés. Egy gyökbővítés mindig véges bővítés, de nem feltétlenül normális bővítés.
Ha $K \subseteq \mathbb{C}$ egy számtest, akkor azt mondjuk, hogy az $\alpha \in \mathbb{C}$ szám **K-ból gyökvonással elérhető**, ha K-nak létezik olyan $K \subseteq L$ gyökbővítése, amelyre $\alpha \in L$.♡

8.4.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ gyökbővítés, akkor K-nak létezik olyan $K \subseteq \overline{L} \subseteq \mathbb{C}$ gyökbővítése, amelyre $K \subseteq L \subseteq \overline{L}$ és $K \subseteq \overline{L}$ normális bővítés.*

Bizonyítás. Ha $K \subseteq L \subseteq \mathbb{C}$ gyökbővítés, akkor létezik köztes számtesteknek olyan

$$K = T_0 \subseteq T_1 \subseteq ... \subseteq T_{m-1} \subseteq T_m = L$$

sorozata, amelyben minden $0 \leq i \leq m-1$ egészre $T_i \subseteq T_{i+1}$ elemi gyökbővítés. Az $m \geq 1$ egészre vonatkozó teljes indukciót alkalmazunk. Ha $m = 1$, akkor $K = T_0 \subseteq T_1 = L$ és így $\overline{L} = L$ megfelelő, hiszen a $T_0 \subseteq T_1$ elemi gyökbővítés normális. Tegyük fel most, hogy minden olyan $K' \subseteq L' \subseteq \mathbb{C}$ gyökbővítésre igaz a tétel állítása, amelyhez létezik köztes számtesteknek olyan m hosszúságú

$$K' = T'_0 \subseteq T'_1 \subseteq ... \subseteq T'_{m-1} \subseteq T'_m = L'$$

sorozata, amelynél minden $0 \leq i \leq m-1$ egészre $T'_i \subseteq T'_{i+1}$ elemi gyökbővítés. Legyen most $K \subseteq L \subseteq \mathbb{C}$ olyan gyökbővítés, hogy a

$$K = T_0 \subseteq T_1 \subseteq ... \subseteq T_{m-1} \subseteq T_m \subseteq T_{m+1} = L$$

köztes számtestekre $T_i \subseteq T_{i+1}$ elemi gyökbővítés minden $0 \leq i \leq m$ egészre. Tehát létezik olyan $c \in T_m$ elem és $n \geq 1$ egész, hogy az $x^n - c \in T_m[x]$ polinomnak a T_m-feletti felbontási teste a $T_{m+1} = L$ számtest: $T_m(x^n - c = 0) = L$.
Az indukciós feltevésünk szerint van olyan $K \subseteq L^* \subseteq \mathbb{C}$ gyökbővítése K-nak, amelyre $K \subseteq T_m \subseteq L^*$ és $K \subseteq L^*$ normális. Legyen $p(x) \in K[x]$ a $c \in T_m$ elem (ez K-felett algebrai, hiszen $K \subseteq T_m$ véges) K-feletti minimálpolinomja, ekkor $c \in L^*$ és a $K \subseteq L^*$ bővítés normalitása miatt $p(x)$ minden további gyöke is L^*-ban található, azaz

$$p(x) = (x - c_1)(x - c_2)...(x - c_k),$$

ahol $c = c_1, c_2, ..., c_k \in L^*$. Tekintsük az alábbi

$$p(x^n) = (x^n - c_1)(x^n - c_2)...(x^n - c_k) \in K[x]$$

polinommal az

$$\overline{L} = L^* \vee K(p(x^n) = 0).$$

bővítését L^*-nak. Mivel $K \subseteq L^*$ és $K \subseteq K(p(x^n) = 0)$ véges normális bővítések, ezért

$$K \subseteq L^* \vee K(p(x^n) = 0) = L^*(p(x^n) = 0),$$

azaz $K \subseteq \overline{L}$ is normális. Tekintsük az

$$L^* \subseteq L^*(x^n - c_1 = 0) \subseteq L^*((x^n - c_1)(x^n - c_2) = 0) \subseteq ... \subseteq L^*((x^n - c_1)(x^n - c_2)...(x^n - c_k) = 0) = \overline{L}$$

egymás utáni bővítések sorozatát, ekkor minden lépésben elemi gyökbővítést találunk, hiszen minden $0 \leq i \leq k-1$ egészre

$$M_{i+1} = L^*((x^n - c_1)(x^n - c_2)...(x^n - c_i)(x^n - c_{i+1}) = 0)$$

nyilvánvalóan elemi gyökbővítése az

$$M_i = L^*((x^n - c_1)(x^n - c_2)...(x^n - c_i) = 0)$$

számtestnek:

$$c_{i+1} \in L^* \subseteq M_i \text{ és } M_{i+1} = M_i(x^n - c_{i+1} = 0).$$

Mivel $K \subseteq L^*$ és $L^* \subseteq \overline{L}$ gyökbővítések, ezért $K \subseteq \overline{L}$ is gyökbővítés és már láttuk, hogy $K \subseteq \overline{L}$ normális. Végül $T_m \subseteq L^*$ és $T_m(x^n - c_1 = 0) = L$ miatt

$$L \subseteq L^*(x^n - c_1 = 0) = M_1 \subseteq \overline{L}.$$

□□□