11. AUTOMORFIZMUSOK ÁLTAL FIXEN HAGYOTT ELEMEK

11.A.Definíció. Egy $K \subseteq L \subseteq \mathbb{C}$ testbővítés $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusa által fixen hagyott L-beli elemek halmazára bevezetjük a következő jelölést:

$$L^{\Phi} = \{a \mid a \in L \text{ és } \Phi(a) = a\}.$$

Egy $\mathcal{A} \subseteq \mathcal{G}(K \subseteq L)$ részhalmaz esetén az $\mathcal{A}$ minden eleme által fixen hagyott L-beli elemek halmazát az

$$L^{\mathcal{A}} = \{a \mid a \in L \text{ és } \Phi(a) = a \text{ minden } \Phi \in \mathcal{A} \text{ relatív automorfizmusra}\} = \bigcap_{\Phi \in \mathcal{A}} L^{\Phi}$$

módon jelöljük.♡

11.1.Állítás. *Tetszőleges $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra és $\mathcal{A} \subseteq \mathcal{G}(K \subseteq L)$ részhalmazra $K \subseteq L^{\oplus} \subseteq L$ és $K \subseteq L^{\mathcal{A}} \subseteq L$ számtestek, továbbá*

$$\mathcal{A} \subseteq \mathcal{G}(L^{\mathcal{A}} \subseteq L) \subseteq \mathcal{G}(K \subseteq L) = \mathcal{G}(L^{\mathcal{G}(K \subseteq L)} \subseteq L).$$

Bizonyítás. Mivel $\Phi \in \mathcal{G}(K \subseteq L)$ miatt bármely $a \in K$ elemre $\Phi(a) = a$, ezért $K \subseteq L^{\oplus} \subseteq L$. Ha $a, b \in L^{\oplus}$, akkor

$$\Phi(a \pm b) = \Phi(a) \pm \Phi(b) = a \pm b \text{ és } \Phi(ab) = \Phi(a)\Phi(b) = ab,$$

továbbá

$$b \neq 0 \text{ esetén } \Phi(\frac{a}{b}) = \frac{\Phi(a)}{\Phi(b)} = \frac{a}{b}.$$

Tehát $a \pm b, ab \in L^{\oplus}$ és $b \neq 0$ esetén $\frac{a}{b} \in L^{\oplus}$, ami azt igazolja, hogy $L^{\oplus}$ számtest.
Ismert, hogy számtestek tetszőleges metszete is számtest, ezért

$$L^{\mathcal{A}} = \bigcap_{\Phi \in \mathcal{A}} L^{\Phi}$$

szintén számtest, amelyre a $K \subseteq L^{\oplus} \subseteq L$ tartalmazások miatt $K \subseteq L^{\mathcal{A}} \subseteq L$ is teljesül.
Ha $\Phi \in \mathcal{A}$, akkor $L^{\mathcal{A}}$ értelmezése szerint $\Phi(a) = a$ minden $a \in L^{\mathcal{A}}$ elemre, ami azt jelenti, hogy $\Phi \in \mathcal{G}(L^{\mathcal{A}} \subseteq L)$. Tehát $\mathcal{A} \subseteq \mathcal{G}(L^{\mathcal{A}} \subseteq L)$ és $K \subseteq L^{\mathcal{A}}$ miatt a $\mathcal{G}(L^{\mathcal{A}} \subseteq L) \subseteq \mathcal{G}(K \subseteq L)$ tartalmazás is teljesül.
A fentieket az $\mathcal{A} = \mathcal{G}(K \subseteq L)$ speciális esetben alkalmazva előbb a

$$\mathcal{G}(K \subseteq L) \subseteq \mathcal{G}(L^{\mathcal{G}(K \subseteq L)} \subseteq L) \text{ majd a fordított } \mathcal{G}(L^{\mathcal{G}(K \subseteq L)} \subseteq L) \subseteq \mathcal{G}(K \subseteq L)$$

tartalmazást kapjuk.

□□□

11.2.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges bővítés, $n = [L : K]$ és az $a \in L$ elemet az egymástól és az identikustól különböző $\Phi_1, \Phi_2, ..., \Phi_{n-1} \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusok mindegyike fixen hagyja (azaz $\Phi_1(a) = \Phi_2(a) = ... = \Phi_{n-1}(a) = a$), akkor $a \in K$ teljesül. Tehát*

$$L^{\{\Phi_1, \Phi_2, ..., \Phi_{n-1}\}} = L^{\Phi_1} \cap L^{\Phi_2} \cap ... \cap L^{\Phi_{n-1}} = K.$$

Bizonyítás. A relatív automorfizmusoknak a 9.4.Tételben megadott leírását használjuk. Ha $\alpha \in L$ olyan elem, amelyre $K(\alpha) = L$ és amelynek a K-feletti minimálpolinomja $p(x) \in K[x]$, akkor $n = \deg(p(x)) = [L : K]$ és bármely $a \in K(\alpha) = L$ elem egyértelműen felírható

$$a = u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}$$

alakban alkalmas $u_0, u_1, ..., u_{n-1} \in K$ számokkal (itt $u_0, u_1, , ..., u_{n-1}$ az a-nak az $1, \alpha, ..., \alpha^{n-1}$ K-bázisra vonatkozó koordinátái). Az egymástól különböző $\Phi_1, \Phi_2, ..., \Phi_{n-1}$,$\mathrm{id}_L \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusokra a $\beta_i = \Phi_i(\alpha)$, $1 \leq i \leq n-1$ és a $\beta_n = \alpha = \mathrm{id}_L(\alpha)$ (L-beli) számok a $p(x)$ minimálpolinomnak egymástól különböző gyökei ($\beta_i = \beta_j$ esetén $\Phi_i = \Phi_j$ vagy $\Phi_i = \mathrm{id}_L$ teljesülne), amelyek teljesen meghatározzák a Φ_1, Φ_2,...,Φ_{n-1} relatív automorfizmusokat az egész L-en: az $1 \leq i \leq n$ egészre

$$\Phi_i(a) = \Phi_i(u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}) = u_0 + u_1\beta_i + ... + u_{n-1}\beta_i^{n-1}.$$

Most a $\Phi_1(a) = a, \Phi_2(a) = a, ..., \Phi_{n-1}(a) = a$ egyenlőségeket rendre felírva kapjuk, hogy

$$u_0 + u_1\beta_1 + ... + u_{n-1}\beta_1^{n-1} = u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1},$$

$$u_0 + u_1\beta_2 + ... + u_{n-1}\beta_2^{n-1} = u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1},$$

$$\vdots$$

$$u_0 + u_1\beta_{n-1} + ... + u_{n-1}\beta_{n-1}^{n-1} = u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}.$$

Átrendezésekkel jutunk az alábbiakhoz

$$u_1(\beta_1 - \alpha) + ... + u_{n-1}(\beta_1^{n-1} - \alpha^{n-1}) = 0,$$

$$u_1(\beta_2 - \alpha) + ... + u_{n-1}(\beta_2^{n-1} - \alpha^{n-1}) = 0,$$

$$\vdots$$

$$u_1(\beta_{n-1} - \alpha) + ... + u_{n-1}(\beta_{n-1}^{n-1} - \alpha^{n-1}) = 0.$$

Mivel a

$$B = \begin{bmatrix} \beta_1 - \alpha & . & . & . & \beta_1^{n-1} - \alpha^{n-1} \\ \beta_2 - \alpha & . & . & . & \beta_2^{n-1} - \alpha^{n-1} \\ . & . & . & . & . \\ . & . & . & . & . \\ \beta_{n-1} - \alpha & . & . & . & \beta_{n-1}^{n-1} - \alpha^{n-1} \end{bmatrix}$$

$(n-1) \times (n-1)$-es mátrix determinánsa nem zéró, ezért (Cramer szabálya szerint) a fenti lineáris egyenletrendszernek csak a triviális $u_1 = u_2 = ... = u_{n-1} = 0$ megoldása létezik, ahonnan $a = u_0 \in K$ adódik.
Érdemes megjegyezni, hogy az általunk tekintett B mátrix determinánsa megegyezik az alábbi $n \times n$-es Vandermonde mátrix determinánsával (ez úgy látható, ha V-nek az első sorát kivonjuk az összes többi sorából):

$$V = \begin{bmatrix} 1 & \alpha & . & . & . & \alpha^{n-1} \\ 1 & \beta_1 & . & . & . & \beta_1^{n-1} \\ 1 & \beta_2 & . & . & . & \beta_2^{n-1} \\ . & . & . & . & . & . \\ . & . & . & . & . & . \\ 1 & \beta_{n-1} & . & . & . & \beta_{n-1}^{n-1} \end{bmatrix}.$$

□□□

11.3.Következmény. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges normális testbővítés, akkor $L^{\mathcal{G}(K \subseteq L)} = K$.*

Bizonyítás. A 9.5.Következmény szerint a $K \subseteq L$ véges normális bővítés relatív automorfizmusainak a száma pontosan az előbbi 11.2.Tételben szereplő $n = [L : K]$ egész szám. Tehát most $\mathcal{G}(K \subseteq L) = \{\mathrm{id}_L, \Phi_1, \Phi_2, ..., \Phi_{n-1}\}$, ahol $\Phi_1, \Phi_2, ..., \Phi_{n-1}$ egymástól és az identikustól különböznek. Így $L^{\mathrm{id}_L} = L$ figyelembe vételével és a 11.2.Tételt használva kapjuk, hogy

$$L^{\mathcal{G}(K \subseteq L)} = L^{\mathrm{id}_L} \cap L^{\Phi_1} \cap L^{\Phi_2} \cap ... \cap L^{\Phi_{n-1}} = K.$$

□□□

11.4.Lemma. *Legyen $K \subseteq L \subseteq \mathbb{C}$ tetszőleges testbővítés és $\Phi \in \mathcal{G}(K \subseteq L)$, egy $f(x) = c_0 + c_1 x + ... + c_m x^m \in L[x]$ polinomra értelmezzük annak az ún. Φ-képét a*

$$f_\Phi(x) = \Phi(c_0) + \Phi(c_1)x + ... + \Phi(c_m)x^m \in L[x]$$

módon. Ekkor bármely $a \in L$ elemre $\Phi^{-1}(f_\Phi(a)) = f(\Phi^{-1}(a))$ teljesül, az $a \in K$ esetben $f_\Phi(a) = \Phi(f(a))$. Amennyiben a $h(x), f(x), g(x) \in L[x]$ polinomokra $h(x) = f(x)g(x)$, akkor

$$h_\Phi(x) = f_\Phi(x) g_\Phi(x)$$

(és ez többtényezős szorzatra is igaz).

Bizonyítás.

$$\Phi^{-1}(f_\Phi(a)) = \Phi^{-1}(\Phi(c_0) + \Phi(c_1)a + ... + \Phi(c_m)a^m) =$$
$$= \Phi^{-1}(\Phi(c_0)) + \Phi^{-1}(\Phi(c_1))\Phi^{-1}(a) + ... + \Phi^{-1}(\Phi(c_m))\Phi^{-1}(a^m) =$$
$$= c_0 + c_1\Phi^{-1}(a) + ... + c_m(\Phi^{-1}(a))^m = f(\Phi^{-1}(a)).$$

Ha $a \in K$, akkor $\Phi^{-1} \in \mathcal{G}(K \subseteq L)$ miatt $\Phi^{-1}(a) = a$ és az előbbiek szerint $\Phi^{-1}(f_\Phi(a)) = f(\Phi^{-1}(a)) = f(a)$, ahonnan $f_\Phi(a) = \Phi(\Phi^{-1}(f_\Phi(a))) = \Phi(f(a))$ adódik.
Legyen $g(x) = b_0 + b_1 x + ... + b_n x^n$, ekkor a $h(x) = f(x)g(x) = d_0 + d_1 x + ... + d_{m+n} x^{m+n}$ szorzat polinom együtthatóira

$$d_k = c_0 b_k + c_1 b_{k-1} + ... + c_{k-1} b_1 + c_k b_0.$$

Mivel $\Phi \in \mathcal{G}(K \subseteq L)$ megőrzi a műveleteket, ezért

$$\Phi(d_k) = \Phi(c_0 b_k + c_1 b_{k-1} + ... + c_{k-1} b_1 + c_k b_0) =$$

$$= \Phi(c_0)\Phi(b_k) + \Phi(c_1)\Phi(b_{k-1}) + ... + \Phi(c_{k-1})\Phi(b_1) + \Phi(c_k)\Phi(b_0),$$

ami pontosan azt jelenti, hogy az

$$f_\Phi(x) = \Phi(c_0) + \Phi(c_1)x + ... + \Phi(c_m)x^m \text{ és a } g_\Phi(x) = \Phi(b_0) + \Phi(b_1)x + ... + \Phi(b_n)x^n$$

polinomok szorzata a $h_\Phi(x) = \Phi(d_0) + \Phi(d_1)x + ... + \Phi(d_{m+n})x^{m+n}$ polinom: $h_\Phi(x) = f_\Phi(x)g_\Phi(x)$.

□□□

11.5.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ tetszőleges testbővítés és relatív automorfizmusoknak az m-elemű $\mathcal{A} = \{\Phi_1, \Phi_2, ..., \Phi_m\} \subseteq \mathcal{G}(K \subseteq L)$ halmaza (így $\Phi_i \neq \Phi_j$) zárt a kompozícióra nézve ($\Phi, \Psi \in \mathcal{A}$ esetén $\Phi \circ \Psi \in \mathcal{A}$), akkor tetszőleges $a \in L$ elemre az*

$$f(x) = (x - \Phi_1(a))(x - \Phi_2(a))...(x - \Phi_m(a)) = \prod_{\Phi \in \mathcal{A}} (x - \Phi(a))$$

polinom együtthatói az $L^{\mathcal{A}}$ számtestben vannak: $f(x) \in L^{\mathcal{A}}[x]$.

Bizonyítás. Ha $f(x) = c_0 + c_1x + ... + c_mx^m$ a $c_0, c_1, ..., c_m \in L$ együtthatókkal, akkor a 11.4.Lemma szerint tetszőleges $\Phi \in \mathcal{A}$ relatív automorfizmusra

$$f_\Phi(x) = \Phi(c_0) + \Phi(c_1)x + ... + \Phi(c_m)x^m = (x - \Phi(\Phi_1(a)))(x - \Phi(\Phi_2(a)))...(x - \Phi(\Phi_m(a))) =$$

$$= (x - (\Phi \circ \Phi_1)(a))(x - (\Phi \circ \Phi_2)(a))...(x - (\Phi \circ \Phi_m)(a)) =$$

$$= (x - \Psi_1(a))(x - \Psi_2(a))...(x - \Psi_m(a)) = f(x) = c_0 + c_1x + ... + c_mx^m,$$

hiszen

$$\{\Psi_1 = \Phi \circ \Phi_1, \Psi_2 = \Phi \circ \Phi_2, ..., \Psi_m = \Phi \circ \Phi_m\} = \mathcal{A}.$$

Valóban, $\mathcal{A}$-nak a kompozícióra vonatkozó zártsága miatt $\{\Phi \circ \Phi_1, \Phi \circ \Phi_2, ..., \Phi \circ \Phi_m\} \subseteq \mathcal{A}$ és ha az $1 \leq i < j \leq m$ egészekre $\Phi \circ \Phi_i = \Phi \circ \Phi_j$ teljesülne, akkor a

$$\Phi_i = \mathrm{id}_L \circ \Phi_i = (\Phi^{-1} \circ \Phi) \circ \Phi_i = \Phi^{-1} \circ (\Phi \circ \Phi_i) = \Phi^{-1} \circ (\Phi \circ \Phi_j) = (\Phi^{-1} \circ \Phi) \circ \Phi_j = \mathrm{id}_L \circ \Phi_j = \Phi_j$$

ellentmondáshoz jutnánk. Így $\Phi \circ \Phi_1, \Phi \circ \Phi_2, ..., \Phi \circ \Phi_m$ egymástól különböző elemei az m elemű $\mathcal{A}$-nak, ahonnan a kívánt egyenlőséget kapjuk. Tehát $\Phi(c_i) = c_i$ teljesül minden $0 \leq i \leq m$ egészre. Az $f(x)$ polinom $c_i, 0 \leq i \leq m$ együtthatóira így azt kaptuk, hogy $c_i \in L^\Phi$ bármely $\Phi \in \mathcal{A}$ relatív automorfizmus esetében. Következésképpen $c_i \in L^{\mathcal{A}}$ minden $0 \leq i \leq m$ egészre, azaz $f(x) \in L^{\mathcal{A}}[x]$.

□□□

11.6.Tétel. *Legyen $K \subseteq L \subseteq \mathbb{C}$ véges normális bővítés és $p(x) \in K[x]$ irreducibilis polinom $K[x]$-ben. Ha az $a, b \in L$ elemek a $p(x)$ polinom gyökei, akkor létezik olyan $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus, amelyre $\Phi(a) = b$.*

Bizonyítás. Most a 9.5.Következmény szerint a $\mathcal{G}(K \subseteq L)$ elemeinek a száma $n = [L : K]$, azaz $\mathcal{G}(K \subseteq L) = \{\Phi_1 = \mathrm{id}_L, \Phi_2, ..., \Phi_n\}$. Tekintsük az

$$f(x) = (x - \Phi_1(a))(x - \Phi_2(a))...(x - \Phi_n(a)) = \prod_{\Phi \in \mathcal{G}(K \subseteq L)} (x - \Phi(a))$$

polinomot, amelynek $\Phi_1(a) = \mathrm{id}_L(a) = a$ miatt gyöke az $a \in L$ szám. A 11.5.Tétel alapján $f(x) \in L^{\mathcal{G}(K \subseteq L)}[x]$ és a itt a 11.3.Következményre való tekintettel $L^{\mathcal{G}(K \subseteq L)} = K$. Tehát az $f(x) \in K[x]$ polinomnak és a $p(x) \in K[x]$ irreducibilis polinomnak az $a \in L$ közös gyöke, ami a 4.5.Állítás 4.része szerint azt eredményezi, hogy $p(x)$ osztója $f(x)$-nek: $p(x) \mid f(x)$. Így a $p(x)$ polinomnak a $b \in L$ gyöke az $f(x)$-nek is gyöke:

$$f(b) = (b - \Phi_1(a))(b - \Phi_2(a))...(b - \Phi_n(a)) = \prod_{\Phi \in \mathcal{G}(K \subseteq L)} (b - \Phi(a)) = 0.$$

Nyilvánvaló, hogy ez csak úgy teljesülhet, ha $b = \Phi(a)$ valamelyik $\Phi = \Phi_i \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra.

□□□

11.7.Következmény (a 10.2.Tétel élesítése). *Ha $K \subseteq L \subseteq \mathbb{C}$ véges normális testbővítés és $K \subseteq T \subseteq L$ tetszőleges köztes számtest, akkor bármely $\Psi \in \mathcal{G}(K \subseteq T)$ relatív automorfizmus kiterjeszthető a $K \subseteq L$ bővítés valamilyen relatív automorfizmusává, azaz létezik olyan $\Phi \in \mathcal{G}(K \subseteq L)$, amelyre $\Phi \restriction T = \Psi$.*

Bizonyítás. Mivel a $[T : K]$ dimenzió is véges, ezért létezik olyan $\gamma \in T$ elem, amelyre $T = K(\gamma)$. Legyen $s(x) \in K[x]$ a γ algebrai elemnek a K számtest feletti minimálpolinomja (amely irreducibilis $K[x]$-ben). A 9.2.Állítás szerint a $\Psi(\gamma) \in T$ is gyöke az $s(x)$ polinomnak. A 11.6.Tétel szerint létezik olyan $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus, amelyre $\Phi(\gamma) = \Psi(\gamma)$. Belátjuk, hogy $\Phi \restriction T = \Psi$.
Ha $k = \deg(s(x)) = [T : K]$, akkor bármely $a \in K(\gamma) = T$ elem egyértelműen felírható

$$a = u_0 + u_1\gamma + ... + u_{k-1}\gamma^{k-1}$$

alakban alkalmas $u_0, u_1, ..., u_{k-1} \in K$ számokkal (itt $u_0, u_1, , ..., u_{k-1}$ az a-nak az $1, \gamma, ..., \gamma^{k-1}$ K-bázisra vonatkozó koordinátái). Nyilvánvaló, hogy $\Phi \in \mathcal{G}(K \subseteq L)$ és $\Psi \in \mathcal{G}(K \subseteq T)$ (valamint a 9.2.Állítás) miatt

$$\Phi(a) = u_0 + u_1\Phi(\gamma) + ... + u_{k-1}(\Phi(\gamma))^{k-1} = u_0 + u_1\Psi(\gamma) + ... + u_{k-1}(\Psi(\gamma))^{k-1} = \Psi(a).$$

□□□

11.8.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges normális testbővítés és relatív automorfizmusoknak az $\mathcal{A} \subseteq \mathcal{G}(K \subseteq L)$ halmaza zárt a $\mathcal{G}(K \subseteq L)$ elemeivel való konjugálásra nézve (tetszőleges $\Psi \in \mathcal{A}$ és $\Phi \in \mathcal{G}(K \subseteq L)$ esetén $\Phi^{-1} \circ \Psi \circ \Phi \in \mathcal{A}$), akkor $K \subseteq L^{\mathcal{A}}$ normális bővítés.*

Bizonyítás. Ha $a \in L^{\mathcal{A}}$ és $b \in \mathbb{C}$ egy $p(x) \in K[x]$ irreducibilis polinomnak a gyökei, akkor a $K \subseteq L$ bővítés normalitása miatt $b \in L$ is teljesül. A 11.6.Tétel szerint létezik olyan
$\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus, amelyre $\Phi(a) = b$. Most tetszőleges $\Psi \in \mathcal{A}$ elemre $a \in L^{\mathcal{A}}$ és $\Phi^{-1} \circ \Psi \circ \Phi \in \mathcal{A}$ miatt $(\Phi^{-1} \circ \Psi \circ \Phi)(a) = a$, ahonnan $\Phi \circ \Phi^{-1} = \mathrm{id}_L$ figyelembe vételével

$$\Psi(b) = \Psi(\Phi(a)) = \Phi(\Phi^{-1}(\Psi(\Phi(a)))) = \Phi((\Phi^{-1} \circ \Psi \circ \Phi)(a)) = \Phi(a) = b$$

adódik. Tehát $b \in L^{\mathcal{A}}$, ami azt jelenti, hogy $K \subseteq L^{\mathcal{A}}$ normális testbővítés.

□□□

11.9.Következmény. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges normális testbővítés és relatív automorfizmusoknak az $\mathcal{A} \subseteq \mathcal{G}(K \subseteq L)$ halmaza centrális $\mathcal{G}(K \subseteq L)$-ben (tetszőleges $\Psi \in \mathcal{A}$ és $\Phi \in \mathcal{G}(K \subseteq L)$ esetén $\Psi \circ \Phi = \Phi \circ \Psi$), akkor $K \subseteq L^{\mathcal{A}}$ normális bővítés.*

Bizonyítás. Ha $\Psi \in \mathcal{A}$ és $\Phi \in \mathcal{G}(K \subseteq L)$, akkor a centralitás miatt

$$\Phi^{-1} \circ \Psi \circ \Phi = \Phi^{-1} \circ (\Psi \circ \Phi) = \Phi^{-1} \circ (\Phi \circ \Psi) = (\Phi^{-1} \circ \Phi) \circ \Psi = \mathrm{id}_L \circ \Psi = \Psi \in \mathcal{A},$$

ami azt jelenti, hogy $\mathcal{A}$ zárt a $\mathcal{G}(K \subseteq L)$ elemeivel való konjugálásra nézve. Tehát az előbbi 11.8.Tétel szerint $K \subseteq L^{\mathcal{A}}$ normális testbővítés.

□□□

11.10.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges bővítés és $\mathrm{id}_L \in \mathcal{A} \subseteq \mathcal{G}(K \subseteq L)$, továbbá $\mathcal{A}$ zárt a kompozícióra nézve, akkor $\mathcal{A} = \mathcal{G}(L^{\mathcal{A}} \subseteq L)$ és $L^{\mathcal{A}} \subseteq L$ normális testbővítés. ($K \subseteq L$ végessége helyett elegendő megkövetelni $L^{\mathcal{A}} \subseteq L$ végességét és $\mathrm{id}_L \in \mathcal{A}$ helyett azt, hogy $\mathcal{A} \neq \varnothing$).*

Bizonyítás. A 11.1.Állításban már láttuk, hogy $\mathcal{A} \subseteq \mathcal{G}(L^{\mathcal{A}} \subseteq L)$. Mivel $L^{\mathcal{A}} \subseteq L$ is véges testbővítés, ezért létezik olyan $\eta \in L$ elem, amelyre $L^{\mathcal{A}}(\eta) = L$. Ha $r(x) \in L^{\mathcal{A}}[x]$ jelöli a η-nek az $L^{\mathcal{A}}$ feletti minimálpolinomját, akkor $r(x)$ irreducibilis $L^{\mathcal{A}}[x]$-ben és

$$n = \deg(r(x)) = [L : L^{\mathcal{A}}] \geq \left|\mathcal{G}(L^{\mathcal{A}} \subseteq L)\right| \geq |\mathcal{A}| = m.$$

Tekintsük most az m elemű $\mathcal{A} = \{\Phi_1 = \mathrm{id}_L, \Phi_2, ..., \Phi_m\}$ halmazra az

$$f(x) = (x - \Phi_1(\eta))(x - \Phi_2(\eta))...(x - \Phi_m(\eta)) = \prod_{\Phi \in \mathcal{A}} (x - \Phi(\eta))$$

polinomot, amelynek $\Phi_1(\eta) = \mathrm{id}_L(\eta) = \eta$ miatt gyöke az $\eta \in L$ szám. A 11.5.Tétel alapján $f(x) \in L^{\mathcal{A}}[x]$. Most az $f(x) \in L^{\mathcal{A}}[x]$ polinomnak és az $r(x) \in L^{\mathcal{A}}[x]$ irreducibilis polinomnak az $\eta \in L$ közös gyöke, ami a 4.5.Állítás 4.része szerint azt eredményezi, hogy $r(x)$ osztója $f(x)$-nek. Így adódik, hogy $n = \deg(r(x)) \leq \deg(f(x)) = m$. Tehát $n = m$, ahonnan a fentiek alapján az

$$n = [L : L^{\mathcal{A}}] = \left|\mathcal{G}(L^{\mathcal{A}} \subseteq L)\right| = |\mathcal{A}| = m$$

egyenlőségeket kapjuk. Az $\mathcal{A} \subseteq \mathcal{G}(L^{\mathcal{A}} \subseteq L)$ tartalmazásra való tekintettel ez csak úgy teljesülhet, ha $\mathcal{A} = \mathcal{G}(L^{\mathcal{A}} \subseteq L)$. A 9.5.Következményt használva az $[L : L^{\mathcal{A}}] = \left|\mathcal{G}(L^{\mathcal{A}} \subseteq L)\right|$ egyenlőségből adódik az $L^{\mathcal{A}} \subseteq L$ bővítés normalitása.
Azt is érdemes megjegyezni, hogy az $r(x) \mid f(x)$ oszthatóság miatt $r(x)$ minden gyöke $\Phi_i(\eta) \in L$ alakú, ami az $L^{\mathcal{A}}(\eta) = L$ egyenlőségre való tekintettel azt jelenti, hogy L az $r(x) \in L^{\mathcal{A}}[x]$ polinom felbontási teste: $L = L^{\mathcal{A}}(r(x) = 0)$.

□□□

11.11.Következmény. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges testbővítés, akkor $L^{\mathcal{G}(K \subseteq L)} \subseteq L$ normális bővítés, $|\mathcal{G}(K \subseteq L)| = [L : L^{\mathcal{G}(K \subseteq L)}]$ és az $L^{\mathcal{G}(K \subseteq L)} = K$ esetben $K \subseteq L$ normális bővítés. (Ha $K \subseteq L$ véges normális bővítés, akkor a* 11.3.Következmény *szerint $L^{\mathcal{G}(K \subseteq L)} = K$.)*

Bizonyítás. Mivel $\mathrm{id}_L \in \mathcal{G}(K \subseteq L)$ és $\mathcal{G}(K \subseteq L) \subseteq \mathcal{G}(K \subseteq L)$ zárt a kompozícióra nézve, ezért az előbbi 11.10.Tétel szerint $L^{\mathcal{G}(K \subseteq L)} \subseteq L$ normális bővítés. Így a 11.1.Állítást és a 9.5.Következményt figyelembe véve kapjuk, hogy

$$|\mathcal{G}(K \subseteq L)| = \left|\mathcal{G}(L^{\mathcal{G}(K \subseteq L)} \subseteq L)\right| = [L : L^{\mathcal{G}(K \subseteq L)}].$$

Ha $L^{\mathcal{G}(K \subseteq L)} = K$, akkor a már tekintett $K = L^{\mathcal{G}(K \subseteq L)} \subseteq L$ bővítésről láttuk, hogy normális.

□□□

11.12.Következmény. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges testbővítés és $\Phi \in \mathcal{G}(K \subseteq L)$ tetszőleges relatív automorfizmus, akkor $L^{\Phi} \subseteq L$ normális bővítés.*

Bizonyítás. Mivel az $\mathcal{A} = \{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^k, ...\} \subseteq \mathcal{G}(K \subseteq L)$ részhalamazra teljesülnek az előbbi 11.10.Tétel feltételei, ezért az $L^{\mathcal{A}} \subseteq L$ bővítés normális. Az $L^{\Phi} \subseteq L = L^{\mathrm{id}_L}$ valamint a $k \geq 1$ egészekre teljesülő $L^{\Phi} \subseteq L^{\Phi^k}$ tartalmazások miatt

$$L^{\mathcal{A}} = L^{\{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^k, ...\}} = L^{\mathrm{id}_L} \cap L^{\Phi} \cap L^{\Phi^2} \cap ... \cap L^{\Phi^k} \cap ... = L^{\Phi}.$$

□□□

11.13.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges bővítés és $\Phi_1, \Phi_2, ..., \Phi_m \in \mathcal{G}(K \subseteq L)$ egymástól különböző relatív automorfizmusok, akkor létezik olyan $b^* \in L$ elem, amelyre a $\Phi_1(b^*), \Phi_2(b^*), ..., \Phi_m(b^*) \in L$ számok lineárisan függetlenek a K felett.*

Bizonyítás. Amennyiben egy $b \in L$ elemre a $\Phi_1(b), \Phi_2(b), ..., \Phi_m(b) \in L$ számok lineárisan összefüggenek K felett, akkor tetszőleges $1 \leq i \leq m$ indexre a $\Phi_i^{-1} \in \mathcal{G}(K \subseteq L)$ relatív automorfizmussal képzett $\Phi_i^{-1}(\Phi_1(b)), \Phi_i^{-1}(\Phi_2(b)), ...\Phi_i^{-1}(\Phi_m(b)) \in L$ számok is lineárisan összefüggenek a K felett, ráadásul ugyanazokkal a K-beli együtthatókkal mint az eredeti számok. Mivel $\lambda_1, \lambda_2, ..., \lambda_m \in K$ esetén $\Phi_i^{-1}(\lambda_1) = \lambda_1, \Phi_i^{-1}(\lambda_2) = \lambda_2, ..., \Phi_i^{-1}(\lambda_m) = \lambda_m$, ezért:

$$\lambda_1\Phi_1(b) + \lambda_2\Phi_2(b) + ... + \lambda_m\Phi_m(b) = 0$$

$$\Downarrow$$

$$\lambda_1\Phi_i^{-1}(\Phi_1(b))+\lambda_2\Phi_i^{-1}(\Phi_2(b))+...+\lambda_m\Phi_i^{-1}(\Phi_m(b))=0.$$

Tehát az alábbi $m\times m$-es

$$\Delta(b)=\begin{bmatrix}\Phi_1^{-1}(\Phi_1(b)) & ... & \Phi_1^{-1}(\Phi_j(b)) & ... & \Phi_1^{-1}(\Phi_m(b))\\ \vdots & & \vdots & & \vdots\\ \Phi_i^{-1}(\Phi_1(b)) & ... & \Phi_i^{-1}(\Phi_j(b)) & ... & \Phi_i^{-1}(\Phi_m(b))\\ \vdots & & \vdots & & \vdots\\ \Phi_m^{-1}(\Phi_1(b)) & ... & \Phi_m^{-1}(\Phi_j(b)) & ... & \Phi_m^{-1}(\Phi_m(b))\end{bmatrix}$$

mátrix oszlopai lineárisan összefüggenek (K felett), azaz $\det\Delta(b)=0$. Az eddigiek szerint a tétel igazolásához elegendő olyan $b^*\in L$ elemet találni, amelyre $\det\left[\Phi_i^{-1}(\Phi_j(b^*))\right]\neq 0$ (az $m\times m$-es $\left[\Phi_i^{-1}(\Phi_j(b^*))\right]$ mátrix i-edik sorának és j-edik oszlopának a kereszteződésében $\Phi_i^{-1}(\Phi_j(b^*))$ áll).
A $K\subseteq L$ bővítés végessége miatt létezik olyan $\alpha\in L$ szám (lásd a 7.6.Tételt), amelyre $L=K(\alpha)$. Tekintsük az alábbi $L[x]$-beli

$$f(x)=\eta\prod_{\substack{1\leq i\leq m,1\leq j\leq m\\ i\neq j}}\left(x-\Phi_i^{-1}(\Phi_j(\alpha))\right)$$

polinomot az

$$\eta=\frac{1}{\prod\limits_{\substack{1\leq i\leq m,1\leq j\leq m\\ i\neq j}}\left(\alpha-\Phi_i^{-1}(\Phi_j(\alpha))\right)}$$

főegyütthatóval (itt a nevező zérustól különböző, hiszen $i\neq j$ esetén az $\alpha-\Phi_i^{-1}(\Phi_j(\alpha))=0$ egyenlőségből előbb $\Phi_i(\alpha)=\Phi_j(\alpha)$, majd innen $L=K(\alpha)$ miatt $\Phi_i=\Phi_j$ következne). Nyilvánvaló, hogy $\Phi_i^{-1}(\Phi_i(\alpha))=\alpha$ miatt

$$f(\Phi_i^{-1}(\Phi_j(\alpha)))=\begin{cases}0\text{ az }i\neq j\text{ esetben}\\ 1\text{ az }i=j\text{ esetben}\end{cases}.$$

A 11.4.Lemma szerint tetszőleges $\Psi\in\mathcal{G}(K\subseteq L)$ relatív automorfizmusra és $b\in L$ elemre $f(\Psi^{-1}(b))=\Psi^{-1}(f_\Psi(b))$, ezért a $\Psi=\Phi_j^{-1}\circ\Phi_i$ és $b=\alpha$ választással kapjuk, hogy $\Psi^{-1}=\Phi_i^{-1}\circ\Phi_j$ és

$$f(\Phi_i^{-1}(\Phi_j(\alpha)))=\Phi_i^{-1}(\Phi_j(f_{\Phi_j^{-1}\circ\Phi_i}(\alpha))),$$

ahonnan az eddigieket és $\Phi_i^{-1}\circ\Phi_j$ injektívitását használva adódik, hogy

$$f_{\Phi_j^{-1}\circ\Phi_i}(\alpha)=\begin{cases}0\text{ az }i\neq j\text{ esetben}\\ 1\text{ az }i=j\text{ esetben}\end{cases}.$$

Tehát az $m\times m$-es $\left[f_{\Phi_j^{-1}\circ\Phi_i}(\alpha)\right]$ mátrix (amelyben a j-edik sor és az i-edik oszlop kereszteződésében $f_{\Phi_j^{-1}\circ\Phi_i}(\alpha)$ áll) nem más mint az egység mátrix, ami azt jelenti, hogy

$$\det\left[f_{\Phi_j^{-1}\circ\Phi_i}(\alpha)\right]=1.$$

A fentiek szerint az $L[x]$-beli $g(x)=\det\left[f_{\Phi_j^{-1}\circ\Phi_i}(x)\right]$ zérustól különböző polinom ($g(\alpha)=1$ miatt), ezért K végtelen sok elemére való tekintettel létezik olyan $a\in K$ (sőt $a\in\mathbb{Q}$ is

megkövetelhető), amire $g(a) \neq 0$. Mivel az $a \in K$ elemre a 11.4.Lemma szerint $f_\Psi(a) = \Psi(f(a))$, ezért a $b^* = f(a)$ választással

$$0 \neq g(a) = \det\left[f_{\Phi_j^{-1}\circ\Phi_i}(a)\right] = \det\left[(\Phi_j^{-1}\circ\Phi_i)(f(a))\right] = \det\left[(\Phi_j^{-1}\circ\Phi_i)(b^*)\right],$$

ahol a $\left[(\Phi_j^{-1}\circ\Phi_i)(b^*)\right]$ mátrixban a j-edik sor és az i-edik oszlop az $(\Phi_j^{-1}\circ\Phi_i)(b^*)$ elemnél metszi egymást.

□□□

11.14. Következmény (a normál bázisról). *Ha $K \subseteq L \subseteq \mathbb{C}$ véges normális bővítés és $\mathcal{G}(K \subseteq L) = \{\Phi_1, \Phi_2, ..., \Phi_n\}$, ahol $n = |\mathcal{G}(K \subseteq L)| = [L : K]$, akkor létezik olyan $b^* \in L$ elem, amelyre a $\Phi_1(b^*), \Phi_2(b^*), ..., \Phi_n(b^*) \in L$ számok L-nek bázisát alkotják a K felett.*

Bizonyítás. Most $n = |\mathcal{G}(K \subseteq L)|$ miatt $\Phi_1, \Phi_2, ..., \Phi_n$ egymástól különbözőek, ezért az előbbi 11.13.Tétel szerint létezik olyan $b^* \in L$ szám, amelyre $\Phi_1(b^*), \Phi_2(b^*), ..., \Phi_n(b^*)$ lineárisan függetlenek K felett. Mivel $n = [L : K]$, ezért bármely n darab K felett lineárisan független L-beli elem bázisát alkotja L-nek K felett.

□□□

11.15.Tétel (Dedekind függetlenségi tétele). *Legyen $K \subseteq L \subseteq \mathbb{C}$ tetszőleges bővítés, ha az egymástól különböző $\Phi_1, \Phi_2, ..., \Phi_m \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusokra és a $\lambda_1, \lambda_2, ..., \lambda_m \in \mathbb{C}$ számokra*

$$\lambda_1\Phi_1(b) + \lambda_2\Phi_2(b) + ... + \lambda_m\Phi_m(b) = 0$$

teljesül minden $b \in L$ elemre, akkor $\lambda_1 = \lambda_2 = ... = \lambda_m = 0$.

Bizonyítás. Az $m \geq 1$ egészre vonatkozó teljes indukciót használunk. Az $m = 1$ eset $\Phi_1(1) = 1$ miatt nyilvánvaló. Legyen most $m \geq 2$ és az egymástól különböző $\Phi_1, \Phi_2, ..., \Phi_m \in G(K \subseteq L)$ relatív automorfizmusokra teljesüljön

$$\lambda_1\Phi_1(b) + \lambda_2\Phi_2(b) + ... + \lambda_m\Phi_m(b) = 0$$

minden $b \in L$ számra. Tetszőlegesen választott $b', b'' \in L$ elemekre legyen $b = b'b''$, ekkor a

$$0 = \lambda_1\Phi_1(b'b'') + \lambda_2\Phi_2(b'b'') + ... + \lambda_m\Phi_m(b'b'') =$$
$$= \lambda_1\Phi_1(b')\Phi_1(b'') + \lambda_2\Phi_2(b')\Phi_2(b'') + ... + \lambda_m\Phi_m(b')\Phi_m(b'')$$

és

$$\lambda_1\Phi_1(b'') + \lambda_2\Phi_2(b'') + ... + \lambda_m\Phi_m(b'') = 0$$

egyenlőségekből előbb szorzással

$$0 = \Phi_m(b')\left\{\lambda_1\Phi_1(b'') + \lambda_2\Phi_2(b'') + ... + \lambda_m\Phi_m(b'')\right\} =$$
$$= \left\{\lambda_1\Phi_m(b')\right\}\Phi_1(b'') + \left\{\lambda_2\Phi_m(b')\right\}\Phi_2(b'') + ... + \left\{\lambda_m\Phi_m(b')\right\}\Phi_m(b''),$$

majd kivonással

$$\{\lambda_1(\Phi_1(b') - \Phi_m(b'))\}\Phi_1(b'') + \{\lambda_2(\Phi_2(b') - \Phi_m(b'))\}\Phi_2(b'') + ... + \{\lambda_{m-1}(\Phi_{m-1}(b') - \Phi_m(b'))\}\Phi_{m-1}(b'') = 0$$

adódik. Az $m-1$ egészre vonatkozó indukciós feltevést használva kapjuk, hogy bármely $b' \in L$ elemre

$$\lambda_1(\Phi_1(b') - \Phi_m(b')) = \lambda_2(\Phi_2(b') - \Phi_m(b')) = ... = \lambda_{m-1}(\Phi_{m-1}(b') - \Phi_m(b')) = 0.$$

Mivel egy $1 \leq i \leq m-1$ indexre $\Phi_i \neq \Phi_m$, ezért van olyan $b'_i \in L$ szám, amire $\Phi_i(b'_i) - \Phi_m(b'_i) \neq 0$. Tehát $\lambda_i(\Phi_i(b'_i) - \Phi_m(b'_i)) = 0$ miatt a $\lambda_i = 0$ egyenlőséghez jutunk. Az eredeti egyenlőség így a $\lambda_m\Phi_m(b) = 0$ alakot ölti, ahonnan $b = 1$ választással azonnal megkapjuk, hogy $\lambda_m = 0$.

□□□