10. AUTOMORFIZMUSOK MEGSZORÍTÁSA

10.1.Állítás. *Ha $K \subseteq L \subseteq \mathbb{C}$ tetszőleges bővítés és a $K \subseteq T \subseteq L$ köztes számtest véges normális bővítése K-nak, akkor bármely $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus T-beli elemet T-beli elembe visz ($\Phi(T) \subseteq T$) és a $(\Phi \restriction T) : T \longrightarrow T$ megszorított leképezés szürjektív, azaz $\Phi \restriction T$ a $K \subseteq T$ testbővítés relatív automorfizmusa: $(\Phi \restriction T) \in \mathcal{G}(K \subseteq T)$.*
Az is teljesül még, hogy ilyenkor a $\mathcal{G}(T \subseteq L) \subseteq \mathcal{G}(K \subseteq L)$ részhalmaz zárt a $\mathcal{G}(K \subseteq L)$ elemeivel való konjugálásra:

$$\textit{tetszőleges } \Psi \in \mathcal{G}(T \subseteq L) \textit{ és } \Phi \in \mathcal{G}(K \subseteq L) \textit{ esetén } \Phi^{-1} \circ \Psi \circ \Phi \in \mathcal{G}(T \subseteq L)).$$

Bizonyítás. Mivel $K \subseteq T$ véges, ezért létezik olyan $\gamma \in T$ elem, amelyre $T = K(\gamma)$. A γ algebrai elem a K számtest felett és így tekinthető γ-nak az $s(x) \in K[x]$ minimálpolinomja (amely irreducibilis $K[x]$-ben). A 9.2.Állítás szerint a $\Phi(\gamma) \in L$ is gyöke az $s(x)$ polinomnak. A $K \subseteq T$ bővítés normális és az $s(x)$ polinomnak a γ gyöke T-beli, ezért $s(x)$ minden további gyökének, azaz $\Phi(\gamma)$-nak is T-ben kell lennie: $\Phi(\gamma) \in T$.
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 a 9.2.Állítás) miatt

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

ahonnan $u_0, u_1, ..., u_{k-1} \in K \subseteq T$ és $\Phi(\gamma) \in T$ figyelembe vételével kapható, hogy $\Phi(a) \in T$. Tehát a Φ relatív automorfizmus T-beli elemet T-beli elembe visz:

$$\Phi(T) \subseteq T \text{ illetve } \Phi \restriction T : T \longrightarrow T.$$

Az $s(x)$ irreducibilis $K[x]$-ben, ami azt jelenti, hogy $s(x)$ a $\Phi(\gamma)$ gyökének is a minimálpolinomja a K számtest felett és így az $1, \Phi(\gamma), ..., (\Phi(\gamma))^{k-1}$ számok a $K(\Phi(\gamma))$-nak egy K-bázisát alkotják. Mivel $\Phi(\gamma) \in T$ miatt $K \subseteq K(\Phi(\gamma)) \subseteq T$ és

$$[K(\Phi(\gamma)) : K] = \deg(s(x)) = k = [T : K],$$

ezért a 2.8.Állítás szerint $K(\Phi(\gamma)) = T$. A $K(\Phi(\gamma))$-nak nyilvánvalóan minden eleme megkapható (egyértelműen)

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

alakban, ezért ugyanez igaz a vele megegyező T elemeire is, tehát $\Phi \restriction T$ szürjektív. A Φ megőrzi a műveleteket, ezért Φ-nek bármely megszorítása is hasonlóan viselkedik.
Mivel $(\Phi \restriction T) \restriction K = \Phi \restriction K = \mathrm{id}_K$, ezért $\Phi \restriction T$ valóban relatív automorfizmusa a $K \subseteq T$ testbővítésnek: $(\Phi \restriction T) \in \mathcal{G}(K \subseteq T)$.
Ha $a \in T$, akkor az eddigiek szerint $\Phi(a) \in T$, ahonnan $\Psi \in \mathcal{G}(T \subseteq L)$ miatt $\Psi(\Phi(a)) = \Phi(a)$ adódik. Tehát

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

ami azt jelenti, hogy $\Phi^{-1} \circ \Psi \circ \Phi \in \mathcal{G}(T \subseteq L)$.

□□□

10.2.Tétel. *Ha $K \subseteq L \subseteq \mathbb{C}$ véges normális testbővítés és a $K \subseteq T \subseteq L$ köztes számtest is normális bővítése K-nak, 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. Értelmezzük a $\approx$ relációt a $\mathcal{G}(K \subseteq L)$ halmaz elemein az alábbiak szerint: a $\Phi_1, \Phi_2 \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusokra

$$\Phi_1 \approx \Phi_2 \text{ pontosan akkor, ha } \Phi_1 \restriction T = \Phi_2 \restriction T,$$

ami azt jelenti, hogy $\Phi_1(a) = \Phi_2(a)$ minden $a \in T$ elemre. Az így definiált $\approx$ reláció nyilvánvalóan ekvivalencia, amely a $\mathcal{G}(K \subseteq L)$-t páronként diszjunkt osztályokra bontja.
Belátjuk, hogy bármely $\Theta \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusnak a $[\Theta]$-val jelölt ekvivalencia osztálya azonos számosságú az $\mathrm{id}_L \in \mathcal{G}(K \subseteq L)$ identikus automorfizmusnak az $[\mathrm{id}_L]$ ekvivalencia osztályával: $|[\mathrm{id}_L]| = |[\Theta]|$ minden $\Theta \in \mathcal{G}(K \subseteq L)$ esetén. Valóban, a $\Phi \in [\Theta]$ relatív automorfizmusra $\Theta^{-1} \circ \Phi \in [\mathrm{id}_L]$ és a $\Phi \longmapsto \Theta^{-1} \circ \Phi$ megfeleltetés egy bijektív $[\Theta] \longrightarrow [\mathrm{id}_L]$ függvényt értelmez. Mivel $\Phi \approx \Theta$, ezért előbb $\Phi(a) = \Theta(a)$, majd innen

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

adódik minden $a \in T$ elemre. Tehát a $\Theta^{-1} \circ \Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra $\Theta^{-1} \circ \Phi \approx \mathrm{id}_L$, illetve $\Theta^{-1} \circ \Phi \in [\mathrm{id}_L]$ adódott. Nyilvánvaló, hogy a fenti megfeleltetés injektív, hiszen a $\Phi_1, \Phi_2 \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusokra a $\Theta^{-1} \circ \Phi_1 = \Theta^{-1} \circ \Phi_2$ esetben

$$\Phi_1 = (\Theta \circ \Theta^{-1}) \circ \Phi_1 = \Theta \circ (\Theta^{-1} \circ \Phi_1) = \Theta \circ (\Theta^{-1} \circ \Phi_2) = (\Theta \circ \Theta^{-1}) \circ \Phi_2 = \Phi_2.$$

Az általunk tekintett megfeleltetés szürjektívitása abból következik, hogy egy tetszőleges $\Delta \in [\mathrm{id}_L]$ relatív automorfizmusra $\Theta \circ \Delta \in [\Theta]$ olyan elem, amelyre

$$\Theta^{-1} \circ (\Theta \circ \Delta) = (\Theta^{-1} \circ \Theta) \circ \Delta = \Delta,$$

azaz amelyre $\Theta \circ \Delta \longmapsto \Delta$. Itt a $\Theta \circ \Delta \in [\Theta]$ tartalmazás azért teljesül, mert $\Delta \approx \mathrm{id}_L$ miatt

$$(\Theta \circ \Delta)(a) = \Theta(\Delta(a)) = \Theta(a)$$

minden $a \in T$ elemre.
Mivel $\mathcal{G}(K \subseteq L)$ a $\approx$ reláció szerinti páronként diszjunkt ekvivalencia osztályok uniója, ezért az egyes osztályok számosságainak az összege a $\mathcal{G}(K \subseteq L)$ elemeinek a számával, azaz $[L : K]$-val egyenlő ($K \subseteq L$ normális testbővítés!). Ha a különböző ekvivalencia osztályok számát $r \geq 1$ jelöli, akkor $[L : K] = r \cdot |[\mathrm{id}_L]|$, hiszen minden osztályban pontosan annyi elem van, amennyi az $[\mathrm{id}_L]$ osztályban. Az $[\mathrm{id}_L] = \mathcal{G}(T \subseteq L)$ egyenlőség is könnyen látható, hiszen a $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra $\Phi \approx \mathrm{id}_L$ pontosan azt jelenti, hogy $\Phi(a) = a$ minden $a \in T$ elemre, ami a $\Phi \in \mathcal{G}(T \subseteq L)$ tartalmazással ekvivalens. Most $|\mathcal{G}(T \subseteq L)| \leq [L : T]$ és a dimenziók szorzási szabálya miatt előbb az

$$[L : T] \cdot [T : K] = [L : K] = r \cdot |[\mathrm{id}_L]| = r \cdot |\mathcal{G}(T \subseteq L)| \leq r \cdot [L : T],$$

majd innen a $|\mathcal{G}(K \subseteq T)| \leq [T : K] \leq r$ egyenlőtlenséget kapjuk. Mivel a $\mathcal{G}(K \subseteq L)$ különböző ekvivalencia osztályaiból vett relatív automorfizmusoknak a T-re való leszűkítései különböznek, ezért a $\{(\Phi \restriction T) \mid \Phi \in \mathcal{G}(K \subseteq L)\}$ halmaz elemeinek a száma pontosan r. A 10.1.Állításban már láttuk, hogy a $K \subseteq T$ bővítés normalitása miatt $\{(\Phi \restriction T) \mid \Phi \in \mathcal{G}(K \subseteq L)\} \subseteq \mathcal{G}(K \subseteq T)$, ahonnan a fentiekben igazolt $|\mathcal{G}(K \subseteq T)| \leq r$ egyenlőtlenség figyelembe vételével a

$$\{(\Phi \restriction T) \mid \Phi \in \mathcal{G}(K \subseteq L)\} = \mathcal{G}(K \subseteq T)$$

egyenlőséget kapjuk. Tehát minden $\Psi \in \mathcal{G}(K \subseteq T)$ megkapható $\Psi = \Phi \restriction T$ alakban, ahol $\Phi \in \mathcal{G}(K \subseteq L)$. Mivel $K \subseteq T$ normális és $K \subseteq L$ normalitásából a $T \subseteq L$ bővítés normalitása is következik, ezért bizonyításunkban a $|\mathcal{G}(K \subseteq T)| = [T : K]$ és $|\mathcal{G}(T \subseteq L)| = [L : T]$ egyenlőségeket is használhattuk volna (minden bővítés véges!).

$\square\square\square$

10.A.Definíció. Legyen $K \subseteq L \subseteq \mathbb{C}$ tetszőleges bővítés és a $K \subseteq T \subseteq L$ köztes számtest véges normális bővítése K-nak, ekkor egy $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra a 10.1.Állítás szerint $(\Phi \restriction T) \in \mathcal{G}(K \subseteq T)$. Tehát ilyenkor értelmezhetjük a **megszorításnak (restrikciónak)** nevezett

$$\mathrm{res} : \mathcal{G}(K \subseteq L) \longrightarrow \mathcal{G}(K \subseteq T)$$

alakban jelölt leképezést az alábbiak szerint: $\mathrm{res}(\Phi) = \Phi \restriction T.\heartsuit$

10.3.Állítás. *Legyen $K \subseteq L \subseteq \mathbb{C}$ tetszőleges bővítés és a $K \subseteq T \subseteq L$ köztes számtest véges normális bővítése K-nak, ekkor a* res: $\mathcal{G}(K \subseteq L) \longrightarrow \mathcal{G}(K \subseteq T)$ *leképezésnek az alábbi tulajdonságai vannak: az* $\mathrm{id}_L, \Phi_1, \Phi_2 \in \mathcal{G}(K \subseteq L)$ *relatív automorfizmusokra*

$$\mathrm{res}(\mathrm{id}_L) = \mathrm{id}_T \quad \textit{és} \quad \mathrm{res}(\Phi_1 \circ \Phi_2) = \mathrm{res}(\Phi_1) \circ \mathrm{res}(\Phi_2).$$

Ha $K \subseteq L$ véges és normális, akkor res: $\mathcal{G}(K \subseteq L) \longrightarrow \mathcal{G}(K \subseteq T)$ *szürjektív leképezés.*

Bizonyítás. $\mathrm{res}(\mathrm{id}_L) = \mathrm{id}_L \restriction T = \mathrm{id}_T$ és a $\Phi_1(T) \subseteq T$, $\Phi_2(T) \subseteq T$ tartalmazások figyelembe vételével kapjuk, hogy

$$\mathrm{res}(\Phi_1 \circ \Phi_2) = (\Phi_1 \circ \Phi_2) \restriction T = (\Phi_1 \restriction T) \circ (\Phi_2 \restriction T) = \mathrm{res}(\Phi_1) \circ \mathrm{res}(\Phi_2).$$

Ha $K \subseteq L$ véges normális testbővítés, akkor a 10.2.Tétel szerint minden $\Psi \in \mathcal{G}(K \subseteq T)$ megkapható $\Psi = \Phi \restriction T = \mathrm{res}(\Phi)$ alakban, ahol $\Phi \in \mathcal{G}(K \subseteq L)$. Tehát ebben az esetben a res valóban szürjektív.

$\square\square\square$