9. SZÁMTESTEK AUTOMORFIZMUSAI

9.A.Definíció. Legyenek $K \subseteq L \subseteq \mathbb{C}$ számtestek, ekkor egy $\Phi : L \longrightarrow L$ függvényt (amely az egész L halmazon értelmezve van és értékeit is L-ben veszi fel) az L **számtest automorfizmusának** nevezünk, ha Φ szürjektív (minden L-beli elem előáll valamilyen $a \in L$ elem $\Phi(a)$ képelemeként) és

$$\Phi(a+b) = \Phi(a) + \Phi(b) \text{ valamint } \Phi(ab) = \Phi(a)\Phi(b)$$

teljesül tetszőleges $a, b \in L$ elemekre. Ha még az is teljesül, hogy Φ a K résztest elemeit fixen hagyja (azaz $\Phi(u) = u$ minden $u \in K$ elemre), akkor Φ-t a $K \subseteq L$ **testbővítés relatív automorfizmusának** nevezzük.♡

9.1.Állítás. *Ha $\Phi : L \longrightarrow L$ az $L \subseteq \mathbb{C}$ számtest automorfizmusa és $a, b \in L$, akkor* $\Phi(0) = 0$, $\Phi(1) = 1$,

$$\Phi(a-b) = \Phi(a) - \Phi(b) \text{ és } b \neq 0 \text{ esetén } \Phi(\frac{a}{b}) = \frac{\Phi(a)}{\Phi(b)}, \text{ továbbá } \Phi(a) = \Phi(b) \Longleftrightarrow a = b$$

(azaz Φ injektív függvény, ami a szürjektívitás miatt azt is jelenti, hogy Φ bijektív is, tehát létezik a $\Phi^{-1} : L \longrightarrow L$ inverz függvény).
Az is teljesül, hogy tetszőleges $w \in \mathbb{Q}$ racionális számra $\Phi(w) = w$, *ami azt jelenti, hogy az L számtest bármely Φ automorfizmusa a $\mathbb{Q} \subseteq L$ testbővítés relatív automorfizmusa (innen az is következik, hogy $\mathbb{Q}$-nak csak egyetlen automorfizmusa van az identikus).*

Bizonyítás. A szürjektívitás miatt léteznek olyan $a_0, a_1 \in L$ elemek, amelyekre $\Phi(a_0) = 0$ és $\Phi(a_1) = 1$. Most

$$0 = \Phi(a_0) = \Phi(a_0 + 0) = \Phi(a_0) + \Phi(0) = 0 + \Phi(0) = \Phi(0),$$

$$1 = \Phi(a_1) = \Phi(a_1 \cdot 1) = \Phi(a_1)\Phi(1) = 1 \cdot \Phi(1) = \Phi(1),$$

$$0 = \Phi(0) = \Phi(a + (-a)) = \Phi(a) + \Phi(-a) \Longrightarrow \Phi(-a) = -\Phi(a),$$

$$\Phi(a-b) = \Phi(a + (-b)) = \Phi(a) + \Phi(-b) = \Phi(a) + (-\Phi(b)) = \Phi(a) - \Phi(b),$$

$$b \neq 0 \text{ esetén } \Phi(b)\Phi(\frac{1}{b}) = \Phi(b \cdot \frac{1}{b}) = \Phi(1) = 1 \Longrightarrow \Phi(b) \neq 0,$$

$$b \neq 0 \text{ esetén } \Phi(a) = \Phi(\frac{a}{b} \cdot b) = \Phi(\frac{a}{b})\Phi(b) \Longrightarrow \Phi(\frac{a}{b}) = \frac{\Phi(a)}{\Phi(b)},$$

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

Ha $n, m \geq 1$ egészek, akkor $n = 1 + 1 + ... + 1$ (n darab 1-essel), ahonnan előbb

$$\Phi(n) = \Phi(1 + 1 + ... + 1) = \Phi(1) + \Phi(1) + ... + \Phi(1) = 1 + 1 + ... + 1 = n$$

majd a már igazoltak alapján $\Phi\left(\frac{n}{m}\right) = \frac{\Phi(n)}{\Phi(m)} = \frac{n}{m}$, illetve $\Phi\left(-\frac{n}{m}\right) = -\Phi\left(\frac{n}{m}\right) = -\frac{n}{m}$ adódik. Tehát $\Phi(w) = w$ minden racionális $w = \pm\frac{n}{m}$ számra.

□□□

9.2.Állítás. *Ha $\Phi : L \longrightarrow L$ a $K \subseteq L \subseteq \mathbb{C}$ testbővítés relatív automorfizmusa és $f(x) \in K[x]$ polinom, akkor tetszőleges $a \in L$ elemre $f(a) \in L$ és $\Phi(f(a)) = f(\Phi(a))$. Speciálisan, ha $f(a) = 0$ (azaz ha a gyöke $f(x)$-nek), akkor $f(\Phi(a)) = 0$ (azaz $\Phi(a)$ is gyöke $f(x)$-nek). Egy*

n-változós $g(x_1, x_2, ..., x_n) \in K[x_1, x_2, ..., x_n]$ *polinomra és tetszőleges* $a_1, a_2, ..., a_n \in L$ *elemekre* $g(a_1, a_2, ..., a_n) \in L$ *és* $\Phi(g(a_1, a_2, ..., a_n)) = g(\Phi(a_1), \Phi(a_2), ..., \Phi(a_n))$.

Bizonyítás. Legyen $f(x) = u_0 + u_1x + ... + u_mx^m$ az $u_0, u_1, ..., u_m \in K$ együtthatókkal, ekkor $f(a) = u_0 + u_1a + ... + u_ma^m \in L$ és a Φ műveleteket megörző tulajdonsága miatt

$$\Phi(f(a)) = \Phi(u_0 + u_1a + ... + u_ma^m) = \Phi(u_0) + \Phi(u_1)\Phi(a) + ... + \Phi(u_m)\Phi(a^m) =$$

$$= \Phi(u_0) + \Phi(u_1)\Phi(a) + ... + \Phi(u_m)(\Phi(a))^m = u_0 + u_1\Phi(a) + ... + u_m(\Phi(a))^m = f(\Phi(a)).$$

A fentiekben felhasználtuk, hogy $\Phi(a^i) = (\Phi(a))^i$ bármely $1 \leq i$ egész kitevőre és azt is, hogy $\Phi(u) = u$ minden $u \in K$ elemre. Ha $f(a) = 0$, akkor az előbbiek szerint

$$f(\Phi(a)) = \Phi(f(a)) = \Phi(0) = 0,$$

ami azt jelenti, hogy $\Phi(a)$ is gyöke $f(x)$-nek.
Legyen

$$g(x_1, x_2, ..., x_n) = \sum_{i_1 \geq 0, i_2 \geq 0, ..., i_n \geq 0} u(i_1, i_2, ..., i_n)x_1^{i_1}x_2^{i_2}...x_n^{i_n}$$

az $u(i_1, i_2, ..., i_n) \in K$ együtthatókkal, ekkor

$$g(a_1, a_2, ..., a_n) = \sum_{i_1 \geq 0, i_2 \geq 0, ..., i_n \geq 0} u(i_1, i_2, ..., i_n)a_1^{i_1}a_2^{i_2}...a_n^{i_n}$$

és a Φ műveleteket megörző tulajdonsága miatt

$$\Phi(g(a_1, a_2, ..., a_n)) = \sum_{i_1 \geq 0, i_2 \geq 0, ..., i_n \geq 0} \Phi(u(i_1, i_2, ..., i_n))\Phi(a_1^{i_1})\Phi(a_2^{i_2})...\Phi(a_n^{i_n}) =$$

$$= \sum_{i_1 \geq 0, i_2 \geq 0, ..., i_n \geq 0} \Phi(u(i_1, i_2, ..., i_n))\Phi(a_1)^{i_1}\Phi(a_2)^{i_2}...\Phi(a_n)^{i_n} =$$

$$= \sum_{i_1 \geq 0, i_2 \geq 0, ..., i_n \geq 0} u(i_1, i_2, ..., i_n)\Phi(a_1)^{i_1}\Phi(a_2)^{i_2}...\Phi(a_n)^{i_n} = g(\Phi(a_1), \Phi(a_2), ..., \Phi(a_n)).$$

Ismételten felhasználtuk, hogy $\Phi(a^i) = (\Phi(a))^i$ bármely $0 \leq i$ egész kitevőre és azt is, hogy $\Phi(u) = u$ minden $u \in K$ elemre.

□□□

9.B.Definíció. Legyenek $\Phi, \Phi_1, \Phi_2 : L \longrightarrow L$ a $K \subseteq L \subseteq \mathbb{C}$ testbővítés relatív automorfizmusai, ekkor a $\Phi^{-1} : L \longrightarrow L$ **inverz függvényt** egy $b \in L$ elemen úgy értelmezzük, hogy $\Phi^{-1}(b) = a$, ahol $a \in L$ az egyetlen olyan eleme L-nek, amelyre $\Phi(a) = b$ (ez a Φ bijektívitása miatt értelmes megadását jelenti a-nak).
A $\Phi_1 \circ \Phi_2 : L \longrightarrow L$ **összetett függvényt** a szokásos $(\Phi_1 \circ \Phi_2)(a) = \Phi_1(\Phi_2(a))$ módon értelmezzük egy $a \in L$ elemen.
Egy $n \geq 1$ egészre a $\Phi^n : L \longrightarrow L$ ún. n**-edik hatvány** (vagy n**-edik iterált**) **függvényt** a szokásos $\Phi^n(a) = \Phi(\Phi(...\Phi(\Phi(a))...))$ módon értelmezzük az $a \in L$ elemen (a zárójelekben pontosan n darab Φ szerepel). Legyen továbbá $\Phi^0 = \mathrm{id}_L$ és $\Phi^{-n} = (\Phi^{-1})^n = (\Phi^n)^{-1}$ (a $(\Phi^{-1})^n = (\Phi^n)^{-1}$ egyenlőséget könnyű belátni).
A $K \subseteq L \subseteq \mathbb{C}$ testbővítés relatív automorfizmusainak halmazára az alábbi jelölést vezetjük be:

$$\mathcal{G}(K \subseteq L) = \{\Phi \mid \Phi : L \longrightarrow L \text{ relatív automorfizmusa a } K \subseteq L \text{ testbővítésnek}\},$$

a $\mathcal{G}(K \subseteq L)$ halmazt a $K \subseteq L$ testbővítés **Galois csoportjának** nevezzük.♡

9.3.Állítás. *Ha* $\Phi, \Phi_1, \Phi_2, \Phi_3 : L \longrightarrow L$ *a* $K \subseteq L \subseteq \mathbb{C}$ *testbővítés relatív automorfizmusai, akkor a* $\Phi^{-1} : L \longrightarrow L$ *inverz függvény, a* $\Phi_1 \circ \Phi_2 : L \longrightarrow L$ *összetett függvény (és így bármely* n *egészre a* $\Phi^n : L \longrightarrow L$ *hatvány is) relatív automorfizmusa a* $K \subseteq L$ *testbővítésnek. Teljesülnek még az alábbiak:*

$$(\Phi_1 \circ \Phi_2) \circ \Phi_3 = \Phi_1 \circ (\Phi_2 \circ \Phi_3) \text{ és } \Phi^k \circ \Phi^l = \Phi^{k+l}$$

tetszőleges k *és* l *egészekre.*

Bizonyítás. A bijektív Φ függvény inverze is nyilvánvalóan bijektív, ezért Φ^{-1} szürjektív. Mivel $\Phi \circ \Phi^{-1} = \mathrm{id}_L$ és Φ megőrzi a műveleteket, ezért az $a, b \in L$ elemekre

$$\Phi(\Phi^{-1}(a+b)) = a+b = \Phi(\Phi^{-1}(a)) + \Phi(\Phi^{-1}(b)) = \Phi(\Phi^{-1}(a) + \Phi^{-1}(b)),$$

$$\Phi(\Phi^{-1}(ab)) = ab = \Phi(\Phi^{-1}(a)) \cdot \Phi(\Phi^{-1}(b)) = \Phi(\Phi^{-1}(a) \cdot \Phi^{-1}(b)),$$

ahonnan Φ injektívitását felhasználva kapjuk, hogy

$$\Phi^{-1}(a+b) = \Phi^{-1}(a) + \Phi^{-1}(b) \text{ és } \Phi^{-1}(ab) = \Phi^{-1}(a) \cdot \Phi^{-1}(b).$$

Tehát Φ^{-1} is megőrzi a műveleteket. Ha $u \in K$, akkor $\Phi(u) = u$ és így Φ^{-1} értelmezése szerint $\Phi^{-1}(u) = u$. A fentiek alapján $\Phi^{-1} \in \mathcal{G}(K \subseteq L)$.
A bijektív Φ_1 és Φ_2 függvények $\Phi_1 \circ \Phi_2$ összetétele (kompozíciója) is nyilvánvalóan bijektív, ezért $\Phi_1 \circ \Phi_2$ szürjektív. Mivel Φ_1 és Φ_2 megőrzi a műveleteket, ezért az $a, b \in L$ elemekre

$$(\Phi_1 \circ \Phi_2)(a+b) = \Phi_1(\Phi_2(a+b)) = \Phi_1(\Phi_2(a) + \Phi_2(b)) =$$

$$= \Phi_1(\Phi_2(a)) + \Phi_1(\Phi_2(b)) = (\Phi_1 \circ \Phi_2)(a) + (\Phi_1 \circ \Phi_2)(b),$$

$$(\Phi_1 \circ \Phi_2)(ab) = \Phi_1(\Phi_2(ab)) = \Phi_1(\Phi_2(a) \cdot \Phi_2(b)) =$$

$$= \Phi_1(\Phi_2(a)) \cdot \Phi_1(\Phi_2(b)) = (\Phi_1 \circ \Phi_2)(a) \cdot (\Phi_1 \circ \Phi_2)(b).$$

Tehát $\Phi_1 \circ \Phi_2$ is megőrzi a műveleteket. Ha $u \in K$, akkor $\Phi_2(u) = \Phi_1(u) = u$, ahonnan $(\Phi_1 \circ \Phi_2)(u) = \Phi_1(\Phi_2(u)) = \Phi_1(u) = u$ adódik. Az eddigiek alapján $\Phi_1 \circ \Phi_2 \in \mathcal{G}(K \subseteq L)$. $(\Phi_1 \circ \Phi_2) \circ \Phi_3 = \Phi_1 \circ (\Phi_2 \circ \Phi_3)$ és $\Phi^k \circ \Phi^l = \Phi^{k+l}$ bizonyítása egyszerű, az utóbbi azonosságot illetően lásd a 14.3.Állítás (2) részét.

□□□

9.4.Tétel. *Legyen* $K \subseteq L \subseteq \mathbb{C}$ *véges testbővítés, ekkor létezik olyan* $\alpha \in L$ *elem, amelyre* $L = K(\alpha)$. *Legyen* $p(x) \in K[x]$ *az* α*-nak a* K *számtest feletti minimálpolinomja (amely irreducibilis* $K[x]$*-ben), ekkor* $n = \deg(p(x)) = [L : K]$ *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).*
Ha $\Phi \in \mathcal{G}(K \subseteq L)$ *relatív automorfizmusa a* $K \subseteq L$ *testbővítésnek, akkor a* $\beta = \Phi(\alpha)$ *szám egy* L*-beli gyöke a* $p(x)$ *minimálpolinomnak, amely a* Φ*-t teljesen meghatározza az egész* L*-en:*

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

Amennyiben β *egy* L*-beli gyöke a* $p(x)$ *minimálpolinomnak, akkor a fenti képlettel megadott* $\Phi : L \longrightarrow L$ *függvény valóban relatív automorfizmusa lesz a* $K \subseteq L$ *testbővítésnek:* $\Phi \in \mathcal{G}(K \subseteq L)$.

Bizonyítás. Mivel $\alpha \in L$ gyöke $p(x)$-nek, ezért a 9.2.Állítás szerint $\beta = \Phi(\alpha) \in L$ is gyöke $p(x)$-nek. Az $a = u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}$ elemhez rendeljük a $K[x]$-beli
$f(x) = u_0 + u_1x + ... + u_{n-1}x^{n-1}$ polinomot, ekkor $a = f(\alpha)$ nyilvánvalóan teljesül. A 9.2.Állítást ismételten alkalmazva kapjuk, hogy

$$\Phi(a) = \Phi(f(\alpha)) = f(\Phi(\alpha)) = f(\beta) = u_0 + u_1\beta + ... + u_{n-1}\beta^{n-1}.$$

Tehát minden $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmust egyértelműen meghatároz a $\beta = \Phi(\alpha)$ helyettesítési érték.
Legyen most a $\Phi : L \longrightarrow L$ függvény az alábbi képlettel értelmezve:

$$\Phi(a) = \Phi(u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}) = u_0 + u_1\beta + ... + u_{n-1}\beta^{n-1},$$

ahol $\beta \in L$ a $p(x)$ polinomnak egy tetszőleges L-beli gyöke ($p(x)$-nek lehetnek olyan gyökei is, amelyek nem L-beliek). A $p(x)$ irreducibilis $K[x]$-ben, ami azt jelenti, hogy $p(x)$ a β-nak is a minimálpolinomja a K számtest felett és így az $1, \beta, ..., \beta^{n-1}$ számok a $K(\beta)$-nak egy K-bázisát alkotják. Mivel $\beta \in L$ miatt $K \subseteq K(\beta) \subseteq L$ és $[K(\beta) : K] = \deg(p(x)) = n = [L : K]$, ezért a 2.8.Állítás szerint $K(\beta) = L$. A $K(\beta)$-nak nyilvánvalóan minden eleme (egyértelműen) megkapható

$$\Phi(u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}) = u_0 + u_1\beta + ... + u_{n-1}\beta^{n-1}$$

alakban, ezért ugyanez igaz a vele megegyező L elemeire is, tehát Φ szürjektív.
Belátjuk, hogy Φ megőrzi a műveleteket. Ha $b = v_0 + v_1\alpha + ... + v_{n-1}\alpha^{n-1}$ egy újabb eleme L-nek a $v_0, v_1, ..., v_{n-1} \in K$ számokkal felírva, akkor legyen $g(x) = v_0 + v_1x + ... + v_{n-1}x^{n-1} \in K[x]$. Most $b = g(\alpha)$ és

$$a + b = (u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}) + (v_0 + v_1\alpha + ... + v_{n-1}\alpha^{n-1}) =$$

$$= (u_0 + v_0) + (u_1 + v_1)\alpha + ... + (u_{n-1} + v_{n-1})\alpha^{n-1},$$

ahonnan a Φ függvény definíciója szerint

$$\Phi(a + b) = (u_0 + v_0) + (u_1 + v_1)\beta + ... + (u_{n-1} + v_{n-1})\beta^{n-1} =$$

$$= (u_0 + u_1\beta + ... + u_{n-1}\beta^{n-1}) + (v_0 + v_1\beta + ... + v_{n-1}\beta^{n-1}) = \Phi(a) + \Phi(b).$$

Végezzük el az $f(x)g(x)$ szorzatpolinomnak a $p(x)$ polinommal való maradékos osztását $K[x]$-ben:

$$f(x)g(x) = p(x)q(x) + h(x),$$

ahol a $q(x), h(x) \in K[x]$ polinomokról annyit tudunk, hogy a $h(x)$ osztási maradékra
$\deg(h(x)) \leq \deg(p(x)) - 1 = n - 1$. Most $p(\alpha) = p(\beta) = 0$ miatt

$$ab = f(\alpha)g(\alpha) = p(\alpha)q(\alpha) + h(\alpha) = h(\alpha),$$

$$f(\beta)g(\beta) = p(\beta)q(\beta) + h(\beta) = h(\beta).$$

A Φ függvény definíciója szerint $\Phi(a) = f(\beta)$, $\Phi(b) = g(\beta)$ és a $h(x) = w_0 + w_1x + ... + w_{n-1}x^{n-1}$ (ha $\deg(h(x)) = k \leq n - 1$, akkor $w_{k+1} = ... = w_{n-1} = 0$) polinomot használva az

$$ab = h(\alpha) = w_0 + w_1\alpha + ... + w_{n-1}\alpha^{n-1}$$

elemre a Φ értelmezése alapján a

$$\Phi(ab) = w_0 + w_1\beta + ... + w_{n-1}\beta^{n-1} = h(\beta)$$

egyenlőséget kapjuk. Így

$$\Phi(ab) = h(\beta) = f(\beta)g(\beta) = \Phi(a)\Phi(b).$$

Tehát Φ megőrzi a műveleteket és az $a \in K$ esetben $a = a + 0\alpha + ... + 0\alpha^{n-1}$, ahonnan a Φ értelmezése szerint $\Phi(a) = a$ adódik, következésképpen $\Phi \in \mathcal{G}(K \subseteq L)$.

□□□

9.5.Következmény. *A $K \subseteq L \subseteq \mathbb{C}$ véges testbővítés relatív automorfizmusainak a száma nem nagyobb az $[L : K]$ dimenziónál: $|\mathcal{G}(K \subseteq L)| \leq [L : K]$. Itt a $|\mathcal{G}(K \subseteq L)| = [L : K]$ egyenlőség pontosan akkor teljesül, ha L normális bővítése K-nak.*

Bizonyítás. Ha $\alpha \in L$ olyan elem, amlyre $K(\alpha) = L$ és $p(x) \in K[x]$ az α-nak a minimálpolinomja a K számtest felett, akkor $n = \deg(p(x)) = [L : K]$. Az előbbi 9.4.Tétel szerint bármely $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmust egyértelműen meghatározza a $\beta = \Phi(\alpha) \in L$ képelem ($\Phi_1, \Phi_2 \in \mathcal{G}(K \subseteq L)$ estén $\Phi_1 = \Phi_2 \Longleftrightarrow \Phi_1(\alpha) = \Phi_2(\alpha)$), amely a $p(x)$ polinomnak valamely L-beli gyöke lehet csak. Tehát a $K \subseteq L$ testbővítés lehetséges $\Phi : L \longrightarrow L$ relatív automorfizmusainak a száma nem nagyobb mint a $p(x)$ polinom gyökeinek a száma. Mivel $n = \deg(p(x))$ és $p(x)$ irreducibilis $K[x]$-ben, ezért (különböző) gyökeinek a száma ($\mathbb{C}$-ben) pontosan n. Ugyancsak az előbbi 9.4.Tétel szerint a $p(x)$ polinom bármely $\beta \in L$ gyöke a

$$\Phi(u_0 + u_1\alpha + ... + u_{n-1}\alpha^{n-1}) = u_0 + u_1\beta + ... + u_{n-1}\beta^{n-1}$$

képlettel megadja egy $\Phi : L \longrightarrow L$ relatív automorfizmusát a $K \subseteq L$ testbővítésnek. Tehát $\mathcal{G}(K \subseteq L)$ elemeinek a száma megegyezik a $p(x)$ polinom L-ben található gyökeinek a számával. Ha $K \subseteq L$ normális bővítés, akkor $\alpha \in L$ miatt a $p(x) \in K[x]$ irreducibilis polinom minden $\beta \in \mathbb{C}$ gyökének L-ben kell lennie. Tehát normális bővítés estén $\mathcal{G}(K \subseteq L)$ elemeinek a száma, azaz a $p(x)$ polinom L-ben található gyökeinek a száma pontosan $n = \deg(p(x)) = [L : K]$.
Ha $|\mathcal{G}(K \subseteq L)| = [L : K] = \deg(p(x))$, akkor a $p(x)$ polinom L-ben található gyökeinek a száma megegyezik $p(x)$ fokszámával. Tehát $p(x)$ minden gyöke L-beli, ami $L = K(\alpha)$ miatt azt jelenti, hogy $L = K(\alpha_1, \alpha_2, ..., \alpha_n)$, ahol $\alpha = \alpha_1, \alpha_2, ..., \alpha_n \in \mathbb{C}$ a $p(x)$ összes gyökeit (egy n-ed fokú irreducibilis polinomnak pontosan n különböző gyöke van) jelöli. Így $L = K(p(x) = 0)$ a $p(x) \in K[x]$ polinom felbontási teste, ami normális bővítése K-nak.

□□□

9.6.Állítás. *Legyen $K \subseteq \mathbb{C}$ tetszőleges számtest és $\alpha_1, \alpha_2..., \alpha_n \in \mathbb{C}$ algebrai számok a K felett, ekkor a*

$$K \subseteq K(\alpha_1, \alpha_2..., \alpha_n) = L$$

testbővítésnek egy $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusát teljesen meghatározzák a

$$\beta_1 = \Phi(\alpha_1), \beta_2 = \Phi(\alpha_2), ..., \beta_n = \Phi(\alpha_n)$$

értékek. Amennyiben $\alpha_1, \alpha_2..., \alpha_n$ egy $f(x) \in K[x]$ polinomnak az összes egymástól különböző gyökei, akkor $L = K(f(x) = 0)$ az $f(x)$ polinom felbontási teste a K felett és

$$\Phi(\alpha_1) = \alpha_{\pi(1)}, \Phi(\alpha_2) = \alpha_{\pi(2)}, ..., \Phi(\alpha_n) = \alpha_{\pi(n)}$$

egy permutációja az $\{\alpha_1, \alpha_2..., \alpha_n\}$ halmaznak. Az így értelmezett $\Phi \longmapsto \overline{\Phi} = \pi$ hozzárendelés a $\mathcal{G}(K \subseteq L)$ Galois csoportnak egy injektív és művelettartó leképezését jelenti a permutációk

S_n halmazába. Tehát egy $f(x) \in K[x]$ polinom Galois csoportja (azaz $\mathcal{G}(K \subseteq L)$) a polinom gyökeinek bizonyos permutációival adható meg.

Bizonyítás. Mivel $\alpha_1, \alpha_2..., \alpha_n$ algebrai számok K felett, ezért egy tetszőleges $a \in K(\alpha_1, \alpha_2..., \alpha_n)$ elem

$$a = g(\alpha_1, \alpha_2..., \alpha_n)$$

alakban írható, ahol $g(x_1, x_2..., x_n) \in K[x_1, x_2..., x_n]$ valamilyen n-változós polinom. Most a 9.2.Állítás szerint egy $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra

$$\Phi(a) = \Phi(g(\alpha_1, \alpha_2, ..., \alpha_n)) = g(\Phi(\alpha_1), \Phi(\alpha_2), ..., \Phi(\alpha_n)) = g(\beta_1, \beta_2, ..., \beta_n),$$

ami valóban azt jelenti, hogy a $\beta_i = \Phi(\alpha_i)$, $1 \leq i \leq n$ helyettesítési értékek meghatározzák tetszőleges $a \in L$ számra a $\Phi(a)$ értékét is. Tehát a $\Phi, \Psi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusokra

$$\Phi(\alpha_1) = \Psi(\alpha_1), \Phi(\alpha_2) = \Psi(\alpha_2), ..., \Phi(\alpha_n) = \Psi(\alpha_n) \Longleftrightarrow \Phi = \Psi.$$

Amennyiben $\alpha_i \in L$ gyöke az $f(x) \in K[x]$ polinomnak, akkor ugyancsak az 1.2.Állítást használva látjuk, hogy $\Phi(\alpha_i)$ is gyöke $f(x)$-nek. Így az $f(x)$ egymástól különböző $\alpha_1, \alpha_2..., \alpha_n$ gyökeiből a Φ alkalmazásával újra egymástól különböző gyökeit kapjuk $f(x)$-nek, hiszen Φ injektív (bijektív is). Mivel $\alpha_1, \alpha_2..., \alpha_n$ az $f(x)$ összes gyökeinek a felsorolása, ezért

$$\Phi(\alpha_1) = \alpha_{\pi(1)}, \Phi(\alpha_2) = \alpha_{\pi(2)}, ..., \Phi(\alpha_n) = \alpha_{\pi(n)}$$

valóban a gyököknek egy permutációja.
Az eddigiekből nyilvánvalóan következik, hogy a $\Phi \longmapsto \overline{\Phi} = \pi$ hozzárendelés injektív. Ha

$$\Psi(\alpha_1) = \alpha_{\tau(1)}, \Psi(\alpha_2) = \alpha_{\tau(2)}, ..., \Psi(\alpha_n) = \alpha_{\tau(n)},$$

akkor egy $1 \leq i \leq n$ indexre

$$(\Phi \circ \Psi)(\alpha_i) = \Phi(\alpha_{\tau(i)}) = \alpha_{\pi(\tau(i))},$$

ami azt jelenti, hogy az általunk tekintett hozzárendelés a $\Phi \circ \Psi$ relatív automorfizmushoz a $\pi \circ \tau$ permutációt rendeli. Tehát $\overline{\Phi \circ \Psi} = \overline{\Phi} \circ \overline{\Psi}$.

□□□