13. GYÖKBŐVÍTÉS GALOIS CSOPORTJA, POLINOMOK GYÖKEINEK ELÉRHETŐSÉGE

13.1.Állítás. *Legyen $\varepsilon \in \mathbb{C}$ primitív n-edik egységgyök és $K \subseteq \mathbb{C}$ olyan számtest, amelyre $\varepsilon \notin K$, ekkor $K(\varepsilon)$ az $x^n - 1 \in K[x]$ polinomnak a felbontási teste*

$$K(\varepsilon) = K(x^n - 1 = 0)$$

(ezért a $K \subseteq K(\varepsilon)$ testbővítés normális), továbbá minden $\Phi \in \mathcal{G}(K \subseteq K(\varepsilon))$ relatív automorfizmushoz létezik (egyetlen) olyan

$$1 \leq r = r(\Phi) \leq n-1 \text{ egész szám, amelyre } \Phi(\varepsilon) = \varepsilon^r.$$

Az így kapott r az n-hez relatív prím lesz ($\mathrm{lnko}(r,n) = 1$), továbbá a $\rho(\Phi) = \overline{r(\Phi)}$ módon értelmezett

$$\rho : \mathcal{G}(K \subseteq K(\varepsilon)) \longrightarrow U(\mathbb{Z}_n)$$

leképezés a $(\mathcal{G}(K \subseteq K(\varepsilon)), \circ, \mathrm{id}_{K(\varepsilon)})$ Galois csoportból a redukált maradékosztályok $(U(\mathbb{Z}_n), \cdot, \overline{1})$ csoportjába irányuló injektív homomorfizmus, azaz tetszőleges $\Phi', \Phi'' \in \mathcal{G}(K \subseteq K(\varepsilon))$ relatív automorfizmusokra

$$\rho(\mathrm{id}_{K(\varepsilon)}) = \overline{1},\ \rho(\Phi' \circ \Phi'') = \rho(\Phi')\rho(\Phi''),\ \rho(\Phi') = \rho(\Phi'') \Longleftrightarrow r(\Phi') = r(\Phi'') \Longleftrightarrow \Phi' = \Phi'',$$

továbbá $\Phi' \circ \Phi'' = \Phi'' \circ \Phi'$.

Bizonyítás. Az ε primitív, ezért $1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1} \in K(\varepsilon)$ az összes n-edik egységgyökök sorozata, tehát

$$K(x^n - 1 = 0) = K(1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}) = K(\varepsilon).$$

Ha $\Phi \in \mathcal{G}(K \subseteq K(\varepsilon))$, akkor a 9.2.Állítás szerint $\Phi(\varepsilon) \in K(\varepsilon)$ is gyöke az $x^n - 1 \in K[x]$ polinomnak, ami azt jelenti, hogy $\Phi(\varepsilon)$ is n-edik egységgyök. Most $1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}$ egymástól különböznek, ezért Φ injektívitása miatt az

$$1 = \Phi(1), \Phi(\varepsilon), \Phi(\varepsilon^2) = \Phi(\varepsilon)^2, ..., \Phi(\varepsilon^{n-1}) = \Phi(\varepsilon)^{n-1}$$

számok is különböznek egymástól, ami azt jelenti, hogy $\Phi(\varepsilon)$ is primitív n-edik egységgyök. Az 1.3.Állítás 4.része szerint az $1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}$ n-edik egységgyökök között pontosan azok primitívek, amelyeknek a kitevője n-hez relatív prím. Így azt kapjuk, hogy $\Phi(\varepsilon) = \varepsilon^r$ valamilyen egyértelműen meghatározott $1 \leq r = r(\Phi) \leq n-1$ egész számra, amely az n-hez relatív prím ($\mathrm{lnko}(r,n) = 1$). A 9.4.Tétel szerint egy $\Phi \in \mathcal{G}(K \subseteq K(\varepsilon))$ relatív automorfizmust egyértelműen meghatározza a $\Phi(\varepsilon)$ helyettesítési érték, azaz $r(\Phi') = r(\Phi'') \Longleftrightarrow \Phi' = \Phi''$. Mivel $1 \leq r(\Phi'), r(\Phi'') \leq n-1$, ezért

$$\rho(\Phi') = \overline{r(\Phi')} = \overline{r(\Phi'')} = \rho(\Phi'') \Longleftrightarrow r(\Phi') = r(\Phi''),$$

ami azt jelenti, hogy ρ injektív. Legyen most $i = r(\Phi')$ és $j = r(\Phi'')$, ekkor

$$(\Phi' \circ \Phi'')(\varepsilon) = \Phi'(\Phi''(\varepsilon)) = \Phi'(\varepsilon^j) = (\Phi'(\varepsilon))^j = (\varepsilon^i)^j = \varepsilon^{ij} \text{ és}$$

$$(\Phi'' \circ \Phi')(\varepsilon) = \Phi''(\Phi'(\varepsilon)) = \Phi''(\varepsilon^i) = (\Phi''(\varepsilon))^i = (\varepsilon^j)^i = \varepsilon^{ji},$$

ahonnan az eddigiekre való tekintettel $\Phi' \circ \Phi'' = \Phi'' \circ \Phi'$ és

$$\rho(\Phi' \circ \Phi'') = \overline{r(\Phi' \circ \Phi'')} = \overline{ij} = \overline{i} \cdot \overline{j} = \rho(\Phi')\rho(\Phi'')$$

a redukált maradékosztályok $(U(\mathbb{Z}_n), \cdot, \overline{1})$ csoportjában. Az $U(\mathbb{Z}_n)$-beli $\overline{r(\Phi' \circ \Phi'')} = \overline{ij}$ egyenlőség annak a következménye, hogy az 1.3.Állítás 3.része szerint a $k, l \in \mathbb{Z}$ egészekre

$$\varepsilon^k = \varepsilon^l \Longleftrightarrow n \mid k - l \Longleftrightarrow \overline{k} = \overline{l}.$$

□□□

13.2.Állítás. *Legyen $K \subseteq \mathbb{C}$ olyan számtest, hogy az $n \geq 1$ egészre K tartalmazza az összes n-edik egységgyököt. Egy $c \in K$ elemre tekintsük az $x^n - c \in K[x]$ polinom $L = K(x^n - c = 0)$ felbontási testét, ekkor létezik olyan $d \geq 1$ egész és $\Theta \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus, amelyekre*

$$\mathcal{G}(K \subseteq L) = \{\mathrm{id}_L, \Theta, \Theta^2, ..., \Theta^{d-1}\},$$

ahol $\mathrm{id}_L, \Theta, \Theta^2, ..., \Theta^{d-1}$ egymástól különbözőek (azaz $\mathcal{G}(K \subseteq L)$ pontosan d elemű). Ha $x^n - c$ irreducibilis $K[x]$-ben, akkor $d = n$.

Bizonyítás. Legyen $\varepsilon \in K$ primitív n-edik egységgyök és $b \in L$ az $x^n - c$ polinom egyik gyöke, ekkor az 1.3.Állítás 5.része szerint $x^n - c$ bármely gyöke $b\varepsilon^i$ alakban írható valamilyen $0 \leq i \leq n-1$ egész kitevővel és ezért $L = K(b)$. A 9.2.Állítás szerint bármely $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusra $\Phi(b) \in L$ is gyöke az $x^n - c$ polinomnak, ezért az eddigiek alapján $\Phi(b) = b\varepsilon^i$ teljesül valamilyen (Φ-től függő) egyértelműen meghatározott $0 \leq i \leq n-1$ kitevőre. Az $i = \exp(\Phi)$ és $\lambda(\Phi) = \overline{i} = \overline{\exp(\Phi)}$ módon értelmezett

$$\lambda : \mathcal{G}(K \subseteq L) \longrightarrow \mathbb{Z}_n$$

leképezés a $(\mathcal{G}(K \subseteq L), \circ, \mathrm{id}_L)$ Galois csoportból a $(\mathbb{Z}_n, +, 0)$ csoportba irányuló injektív homomorfizmus. Valóban, ha $\Psi \in \mathcal{G}(K \subseteq L)$ és $\exp(\Psi) = j$, akkor $\Psi(b) = b\varepsilon^j$, $\lambda(\Psi) = \overline{j}$ és

$$(\Phi \circ \Psi)(b) = \Phi(b\varepsilon^j) = \Phi(b)\Phi(\varepsilon^j) = (b\varepsilon^i)\varepsilon^j = b\varepsilon^{i+j},$$

ahonnan $(\Phi \circ \Psi)(b) = b\varepsilon^{\exp(\Phi \circ \Psi)}$ és $b \neq 0$ miatt előbb $\varepsilon^{\exp(\Phi \circ \Psi)} = \varepsilon^{i+j}$, majd az 1.3.Állítás 3.részében látható $\varepsilon^k = \varepsilon^l \Longleftrightarrow n \mid k - l$ ekvivalencia miatt

$$\lambda(\Phi \circ \Psi) = \overline{\exp(\Phi \circ \Psi)} = \overline{i + j} = \overline{i} + \overline{j} = \lambda(\Phi) + \lambda(\Psi)$$

adódik a $(\mathbb{Z}_n, +, 0)$ csoportban. A $b = 0$ eset (ilyenkor $c = 0$) triviális.
Ha $\lambda(\Phi) = \overline{\exp(\Phi)} = \overline{0}$, akkor $0 \leq \exp(\Phi) \leq n - 1$ miatt $\exp(\Phi) = 0$, ahonnan előbb $\Phi(b) = b\varepsilon^0 = b$ majd innen $L = K(b)$ figyelembe vételével $\Phi = \mathrm{id}_L$ adódik. Tehát λ olyan homomorfizmus, amely a 14.16.Állítás 7.része és a már igazolt $\ker(\lambda) = \{\mathrm{id}_L\}$ alapján injektív. Így $\mathcal{G}(K \subseteq L)$ a ciklikus $(\mathbb{Z}_n, +, 0)$ csoport részcsoportjának tekinthető és ezért a 14.7.Állítás figyelembe vételével maga is ciklikus. Létezik olyan $\Theta \in \mathcal{G}(K \subseteq L)$, amelyre

$$\mathcal{G}(K \subseteq L) = \langle\Theta\rangle = \{\mathrm{id}_L, \Theta, \Theta^2, ..., \Theta^k, ...\},$$

ahonnan a 14.6.Állítás szerint az következik, hogy Θ egy $d = |\mathcal{G}(K \subseteq L)|$-ed rendű relatív automorfizmus és

$$\{\mathrm{id}_L, \Theta, \Theta^2, ..., \Theta^k, ...\} = \{\mathrm{id}_L, \Theta, \Theta^2, ..., \Theta^{d-1}\}.$$

Ha $x^n - c$ irreducibilis $K[x]$-ben, akkor ez a b (és bármely más) gyökének a minimálpolinomja is, ezért $K \subseteq L$ normalitását figyelembe véve kapjuk, hogy

$$n = \deg(x^n - c) = [K(b) : K] = [L : K] =\mid \mathcal{G}(K \subseteq L) \mid = d.$$

□□□

13.A.Definíció. Legyen $K \subseteq L \subseteq \mathbb{C}$ tetszőleges testbővítés, $n \geq 1$ egész, $\varepsilon \in K$ egy n-edik egységgyök és $\Phi \in \mathcal{G}(K \subseteq L)$, ekkor a $\Phi^n(a) = a$ tulajdonsággal rendelkező $a \in L$ elemre értelmezzük az

$$(a, \varepsilon) = a + \varepsilon\Phi(a) + \varepsilon^2\Phi^2(a) + ... + \varepsilon^{n-1}\Phi^{n-1}(a)$$

Lagrange-féle rezolvenst (amely L-nek eleme). Ha $\Phi^n =\mathrm{id}_L$, akkor bármely $a \in L$ elemre értelmezve van (a, ε).♡

13.3.Állítás. *Legyen $K \subseteq L \subseteq \mathbb{C}$ tetszőleges testbővítés, $\varepsilon \in K$ egy n-edik egységgyök, $\Phi \in \mathcal{G}(K \subseteq L)$ és az $a \in L$ elemre teljesüljön $\Phi^n(a) = a$. Ekkor tetszőleges $k \geq 1$ egészre és a $b = (a, \varepsilon)$ Lagrange-féle rezolvensre $\Phi^k(b) = b\varepsilon^{-k}$ és $\Phi(b^n) = b^n$.*

Bizonyítás. Mivel $\varepsilon^i \in K$ és $\Phi \in \mathcal{G}(K \subseteq L)$ miatt $\Phi(\varepsilon^i) = \varepsilon^i$, ezért $\varepsilon^n = 1$ és $\Phi^n(a) = a$ figyelembe vételével kapjuk, hogy

$$\varepsilon\Phi(b) = \varepsilon\Phi(a + \varepsilon\Phi(a) + \varepsilon^2\Phi^2(a) + ... + \varepsilon^{n-1}\Phi^{n-1}(a)) =$$

$$= \varepsilon\left[\Phi(a) + \Phi(\varepsilon)\Phi(\Phi(a)) + \Phi(\varepsilon^2)\Phi(\Phi^2(a)) + ... + \Phi(\varepsilon^{n-1})\Phi(\Phi^{n-1}(a))\right] =$$

$$= \varepsilon\left[\Phi(a) + \varepsilon\Phi^2(a) + \varepsilon^2\Phi^3(a) + ... + \varepsilon^{n-2}\Phi^{n-1}(a) + \varepsilon^{n-1}\Phi^n(a)\right] =$$

$$= \varepsilon\Phi(a) + \varepsilon^2\Phi^2(a) + \varepsilon^3\Phi^3(a) + ... + \varepsilon^{n-1}\Phi^{n-1}(a) + \varepsilon^n\Phi^n(a) =$$

$$= a + \varepsilon\Phi(a) + \varepsilon^2\Phi^2(a) + ... + \varepsilon^{n-1}\Phi^{n-1}(a) = b.$$

A fentiekben igazolt $\varepsilon\Phi(b) = b$ egyenlőség alapján $\Phi(b) = b\varepsilon^{-1}$, ahonnan $\varepsilon^{-n} = 1$ miatt $\Phi(b^n) = \Phi(b)^n = (b\varepsilon^{-1})^n = b^n\varepsilon^{-n} = b^n$ is következik. A $\Phi^k(b) = b\varepsilon^{-k}$ igazolása teljes indukcióval történhet:

$$\Phi^{k+1}(b) = \Phi(\Phi^k(b)) = \Phi(b\varepsilon^{-k}) = \Phi(b)\Phi(\varepsilon^{-k}) = (b\varepsilon^{-1})\varepsilon^{-k} = b\varepsilon^{-(k+1)}.$$

□□□

13.4.Tétel. *Legyen $K \subseteq L \subseteq \mathbb{C}$ olyan véges testbővítés, hogy az $n \geq 1$ egészre K tartalmazza az összes n-edik egységgyököt, ekkor az alábbiak ekvivalensek.*

1. *Létezik olyan $c \in K$ szám, amelyre $x^n - c$ irreducibilis $K[x]$-ben és $L = K(x^n - c = 0)$.*
2. *$K \subseteq L$ normális bővítés és létezik olyan $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus, amelyre*

$$\mathcal{G}(K \subseteq L) = \{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1}\},$$

ahol $\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1}$ egymástól különbözőek (azaz $\mathcal{G}(K \subseteq L)$ pontosan n elemű).

3. *Létezik olyan n-ed rendű $\Phi \in \mathcal{G}(K \subseteq L)$ relatív automorfizmus ($\Phi^n = \mathrm{id}_L$ és $\Phi^m \neq \mathrm{id}_L$ az $1 \leq m \leq n-1$ egészekre), amelyre $L^\Phi = K$.*

Bizonyítás. (1)$\Longrightarrow$(2): Az 13.2.Állításban pontosan ezt igazoltuk.
(2)$\Longrightarrow$(1)&(3): Az $L^\Phi \subseteq L^{\Phi^i}$, $0 \leq i \leq n-1$ tartalmazások miatt nyilvánvaló

$$L^{\{\mathrm{id}_L, \Phi, \Phi^2, \ldots, \Phi^{n-1}\}} = L^{\mathrm{id}_L} \cap L^\Phi \cap L^{\Phi^2} \cap \ldots \cap L^{\Phi^{n-1}} = L^\Phi$$

egyenlőség és $\mathcal{G}(K \subseteq L) = \{\mathrm{id}_L, \Phi, \Phi^2, \ldots, \Phi^{n-1}\}$ alapján $L^{\mathcal{G}(K \subseteq L)} = L^\Phi$. A $K \subseteq L$ bővítés normalitása és a 11.3.Következmény miatt $L^{\mathcal{G}(K \subseteq L)} = K$, ahonnan $L^\Phi = K$ adódik.
A Φ relatív automorfizmus n-ed rendű, hiszen $\mathrm{id}_L, \Phi, \Phi^2, \ldots, \Phi^{n-1}$ egymástól különbözőek és a 14.9.Következmény szerint az n-elemű $\mathcal{G}(K \subseteq L)$-ben $\Phi^n = \mathrm{id}_L$. Megjegyezzük, hogy (2)$\Longrightarrow$(3) igazolása eddig megtörtént.
Ha $L \neq K$, akkor legyen $\alpha \in L \setminus K$ olyan (a $K \subseteq L$ végessége alapján létező) elem, amelyre $L = K(\alpha)$. Most $\Phi^n = \mathrm{id}_L$ miatt tetszőleges $\varepsilon \in K$ primitív n-edik egységgyökre és $0 \leq i \leq n-1$ kitevőre tekinthetjük az

$$(\alpha^i, \varepsilon) = \alpha^i + \varepsilon\Phi(\alpha^i) + \varepsilon^2\Phi^2(\alpha^i) + \ldots + \varepsilon^{n-1}\Phi^{n-1}(\alpha^i) =$$

$$= \alpha^i + \varepsilon(\Phi(\alpha))^i + \varepsilon^2(\Phi^2(\alpha))^i + \ldots + \varepsilon^{n-1}(\Phi^{n-1}(\alpha))^i,$$

Lagrange-féle rezolvenseket. Ha minden $1 \leq i \leq n-1$ egészre $(\alpha^i, \varepsilon) = 0$ teljesülne, akkor

$$(\alpha^0, \varepsilon) = (1, \varepsilon) = 1 + \varepsilon + \varepsilon^2 + \ldots + \varepsilon^{n-1} = 0$$

miatt az

$$x_0 + x_1 + x_2 + \ldots + x_{n-1} = 0$$

$$\vdots$$

$$x_0\alpha^i + x_1(\Phi(\alpha))^i + x_2(\Phi^2(\alpha))^i + \ldots + x_{n-1}(\Phi^{n-1}(\alpha))^i = 0$$

$$\vdots$$

$$x_0\alpha^{n-1} + x_1(\Phi(\alpha))^{n-1} + x_2(\Phi^2(\alpha))^{n-1} + \ldots + x_{n-1}(\Phi^{n-1}(\alpha))^{n-1} = 0$$

lineáris egyenlet-rendszernek

$$x_0 = 1, x_1 = \varepsilon, x_2 = \varepsilon^2, \ldots, x_{n-1} = \varepsilon^{n-1}$$

a triviálistól különböző megoldása lenne, ellentmondásban azzal, hogy a rendszer $n \times n$-es

$$A = \begin{bmatrix} 1 & 1 & 1 & . & . & 1 \\ \alpha & \Phi(\alpha) & \Phi^2(\alpha) & . & . & \Phi^{n-1}(\alpha) \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^i & (\Phi(\alpha))^i & (\Phi^2(\alpha))^i & . & . & (\Phi^{n-1}(\alpha))^i \\ \vdots & \vdots & \vdots & \vdots & \vdots & \vdots \\ \alpha^{n-1} & (\Phi(\alpha))^{n-1} & (\Phi^2(\alpha))^{n-1} & . & . & (\Phi^{n-1}(\alpha))^{n-1} \end{bmatrix}$$

Vandermonde mátrixának a determinánsa nem zéró. Valóban, $L = K(\alpha)$ miatt az egymástól különböző $\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1} \in \mathcal{G}(K \subseteq L)$ relatív automorfizmusokra az

$$\alpha, \Phi(\alpha), \Phi^2(\alpha), ..., \Phi^{n-1}(\alpha)$$

helyettesítési értékek is különbözőek (lásd 9.4.Tétel), ahonnan $\det(A) \neq 0$ adódik.
Tehát létezik olyan $1 \leq i \leq n-1$ egész, amelyre $b = (\alpha^i, \varepsilon) \neq 0$. A 13.3.Állítás szerint

$$\Phi(b) = b\varepsilon^{-1}, \Phi^2(b) = b\varepsilon^{-2}, ..., \Phi^{n-1}(b) = b\varepsilon^{-(n-1)},$$

továbbá $\Phi(b^n) = b^n$. Így $c = b^n \in L^\Phi = K$ miatt $x^n - c \in K[x]$ (b ennek a polinomnak nyilvánvalóan gyöke). Legyen $p(x) \in K[x]$ a b-nek a K számtest feletti minimálpolinomja, ekkor $p(x)$ irreducibilis $K[x]$-ben és a 4.5.Állítás 4.része szerint osztója az $x^n - c$ polinomnak. Mivel b gyöke a $p(x) \in K[x]$ polinomnak és $\Phi, \Phi^2, ..., \Phi^{n-1} \in \mathcal{G}(K \subseteq L)$, ezért a 9.2.Állítás szerint a $\Phi^i(b) = b\varepsilon^{-i}$, $0 \leq i \leq n-1$ számok is gyökei lesznek $p(x)$-nek.
Most $b \neq 0$ és ε primitív n-edik egységgyök, ezért a fenti gyökei $p(x)$-nek különbözőek, következésképpen $\deg(p(x)) \geq n$, ami a $p(x) \mid x^n - c$ oszthatóságra és a 3.5.Állítás 4.részére való tekintettel azt eredményezi, hogy $p(x)$ és $x^n - c$ asszociáltak. Tehát $\deg(p(x)) = n$ és így a 4.5.Állítás 6.része alapján $x^n - c$ is irreducibilis $K[x]$-ben. A $K \subseteq L$ bővítés normális, ezért a 9.5.Következményt figyelembe véve kapjuk, hogy

$$[K(b) : K] = \deg(p(x)) = n = \mid \mathcal{G}(K \subseteq L) \mid = [L : K].$$

Mivel $b \in L$ miatt $K \subseteq K(b) \subseteq L$, ezért a 2.8.Állítás szerint a dimenziók fenti egyenlősége csak úgy történhet meg, ha $L = K(b) = K(b, b\varepsilon, b\varepsilon^2, ..., b\varepsilon^{n-1}) = K(x^n - c = 0)$.
(3)$\Longrightarrow$(2): Most $\Phi^n = \mathrm{id}_L$ miatt $\{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1}\} \leq \mathcal{G}(K \subseteq L)$ részcsoport (lásd a 14.5.Állítás utáni Következményt), amelyre ($L^\Phi \subseteq L^{\Phi^i}$, $0 \leq i \leq n-1$ miatt)

$$L^{\{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1}\}} = L^{\mathrm{id}_L} \cap L^\Phi \cap L^{\Phi^2} \cap ... \cap L^{\Phi^{n-1}} = L^\Phi = K \subseteq L^{\mathcal{G}(K \subseteq L)} \subseteq L^\Phi.$$

Így az $L^\Phi = K = L^{\mathcal{G}(K \subseteq L)}$ egyenlőség adódik, ami a 11.11.Következményt figyelembe véve a $K \subseteq L$ bővítés normalitását jelenti. A 11.10.Tételt használva kapjuk, hogy

$$\{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1}\} = \mathcal{G}(L^{\{\mathrm{id}_L, \Phi, \Phi^2, ..., \Phi^{n-1}\}} \subseteq L) = \mathcal{G}(L^\Phi \subseteq L) = \mathcal{G}(K \subseteq L).$$

□□□

13.5.Állítás. *Ha $K \subseteq L \subseteq \mathbb{C}$ gyökbővítés, akkor a $\mathcal{G}(K \subseteq L)$ Galois csoport feloldható.*

Bizonyítás. Most 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. Tehát minden $0 \leq i \leq m-1$ index esetén létezik olyan $c_i \in T_i$ elem és $n_i \geq 1$ egész, hogy az $x^{n_i} - c_i \in T_i[x]$ polinomnak a T_i-feletti felbontási teste a T_{i+1} számtest: $T_i(x^{n_i} - c_i = 0) = T_{i+1}$. Ez azt jelenti, hogy létezik olyan $b_i \in T_{i+1}$ elem és $\varepsilon_i \in T_{i+1}$ primitív n_i-edik egységgyök, amelyekre

$$b_i^n - c_i = 0 \text{ és } T_{i+1} = T_i(b_i, \varepsilon_i) = (T_i(\varepsilon_i))(b_i).$$

Tekintsük a $K \subseteq L$ bővítés köztes testeinek az alábbi sorozatát:

$$K = T_0 \subseteq T_0(\varepsilon_0) \subseteq (T_0(\varepsilon_0))(b_0) = T_1 \subseteq T_1(\varepsilon_1) \subseteq (T_1(\varepsilon_1))(b_1) = T_2 \subseteq ...$$

$$... = T_i \subseteq T_i(\varepsilon_i) \subseteq (T_i(\varepsilon_i))(b_i) = T_{i+1} \subseteq ...$$

$$= T_{m-1} \subseteq T_{m-1}(\varepsilon_{m-1}) \subseteq (T_{m-1}(\varepsilon_{m-1}))(b_{m-1}) = T_m = L.$$

A fenti sorozatra a $\mathcal{G}(\square \subseteq L)$ Galois hozzárendelést alkalmazva kapjuk részcsoportoknak a következő sorozatát:

$$\{\mathrm{id}_L\} = \mathcal{G}(L \subseteq L) = \mathcal{G}(T_m \subseteq L) =$$

$$= \mathcal{G}((T_{m-1}(\varepsilon_{m-1}))(b_{m-1}) \subseteq L) \subseteq \mathcal{G}((T_{m-1}(\varepsilon_{m-1})) \subseteq L) \subseteq \mathcal{G}(T_{m-1} \subseteq L) = ...$$

$$... \subseteq \mathcal{G}(T_{i+1} \subseteq L) = \mathcal{G}((T_i(\varepsilon_i))(b_i) \subseteq L) \subseteq \mathcal{G}(T_i(\varepsilon_i) \subseteq L) \subseteq \mathcal{G}(T_i \subseteq L) = ...$$

$$... \subseteq \mathcal{G}(T_1 \subseteq L) = \mathcal{G}((T_0(\varepsilon_0))(b_0) \subseteq L) \subseteq \mathcal{G}(T_0(\varepsilon_0) \subseteq L) \subseteq \mathcal{G}(T_0 \subseteq L) = \mathcal{G}(K \subseteq L).$$

A 13.1.Állítás szerint a $T_i \subseteq T_i(\varepsilon_i)$ bővítés normális, ezért a 10.A.Definícióban értelmezett

$$\mathrm{res} : \mathcal{G}(T_i \subseteq L) \longrightarrow \mathcal{G}(T_i \subseteq T_i(\varepsilon_i))$$

leképezés olyan csoport homomorfizmus, amelynek a magja

$$\ker(\mathrm{res}) = \mathcal{G}(T_i(\varepsilon_i) \subseteq L) \lhd \mathcal{G}(T_i \subseteq L).$$

Így a homomorfizmus tétel (14.16.Állítás 11.része) szerint a $\mathcal{G}(T_i \subseteq L)/\mathcal{G}(T_i(\varepsilon_i) \subseteq L)$ faktor csoport izomorf a 13.1.Állítás szerint kommutatív $\mathcal{G}(T_i \subseteq T_i(\varepsilon_i))$ csoport egy részcsoportjával, ami a faktor kommutatívitását eredményezi.
Mivel $T_i(\varepsilon_i)$ tartalmazza az összes n_i-edik egységgyököt és $T_{i+1} = (T_i(\varepsilon_i))(b_i)$ nem más mint az $x^{n_i} - c_i \in T_i[x]$ polinomnak a $T_i(\varepsilon_i)$-feletti felbontási teste (ami normális bővítése $T_i(\varepsilon_i)$-nek), ezért a 13.2.Állítás szerint a $\mathcal{G}(T_i(\varepsilon_i) \subseteq T_{i+1})$ Galois csoport ciklikus. Ha újra a 10.A.Definícióban értelmezett

$$\mathrm{res} : \mathcal{G}(T_i(\varepsilon_i) \subseteq L) \longrightarrow \mathcal{G}(T_i(\varepsilon_i) \subseteq T_{i+1})$$

csoport homomorfizmust tekintjük, akkor ennek a magja

$$\ker(\mathrm{res}) = \mathcal{G}(T_{i+1} \subseteq L) \lhd \mathcal{G}(T_i(\varepsilon_i) \subseteq L).$$

A homomorfizmus tétel szerint a

$$\mathcal{G}(T_i(\varepsilon_i) \subseteq L)/\mathcal{G}(T_{i+1} \subseteq L)$$

faktor csoport izomorf a ciklikus $\mathcal{G}(T_i(\varepsilon_i) \subseteq T_{i+1})$ csoport egy részcsoportjával, ami a faktor ciklikusságát (és így a kommutatívitását is) eredményezi (lásd a 14.7.Állítást).
Végeredményben azt kaptuk, hogy a $\mathcal{G}(K \subseteq L)$ Galois csoport fent tekintett szubnormál láncának minden faktora kommutatív, tehát $\mathcal{G}(K \subseteq L)$ feloldható.

□□□

13.6.Tétel. *Egy $K \subseteq L \subseteq \mathbb{C}$ véges normális bővítésre az alábbiak ekvivalensek:*

1. $\mathcal{G}(K \subseteq L)$ *Galois csoport feloldható.*

2. *K-nak létezik olyan $K \subseteq \overline{L} \subseteq \mathbb{C}$ normális gyökbővítése, amelyre $K \subseteq L \subseteq \overline{L}$.*

Bizonyítás. (2)$\Longrightarrow$(1): A 13.5.Állítás szerint $\mathcal{G}(K \subseteq \overline{L})$ feloldható és a $K \subseteq L$ bővítés normalitása miatt tekinthető a 10.A.Definícióban értelmezett

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

csoport homomorfizmus, amely a 10.3.Állítás szerint szürjektív. Így a homomorfizmus tételt (14.16.Állítás 11.része) alkalmazva kapjuk, hogy

$$\mathcal{G}(K \subseteq \overline{L})/\mathcal{G}(L \subseteq \overline{L}) \cong \mathcal{G}(K \subseteq L),$$

ahol $\mathcal{G}(L \subseteq \overline{L}) = \ker(\mathrm{res}) \lhd \mathcal{G}(K \subseteq \overline{L})$. Mivel a feloldható $\mathcal{G}(K \subseteq \overline{L})$ csoport bármely faktora feloldható, ezért $\mathcal{G}(K \subseteq L)$ is feloldható (lásd a 14.14.Állítás 2.részét).
(1)$\Longrightarrow$(2): Mivel $\mathcal{G}(K \subseteq L)$ feloldható, ezért a 14.15.Tétel szerint létezik olyan szubnormál lánca, amelynek a faktorai ciklikus csoportok. Legyen

$$\{\mathrm{id}_L\} = H_s \subseteq H_{s-1} \subseteq ... \subseteq H_1 \subseteq H_0 = \mathcal{G}(K \subseteq L)$$

egyike a legrövidebbeknek a ciklikus faktorokkal rendelkező szubnormál láncok közül.
Az $s \geq 1$ egészre teljes indukciót alkalmazva végezzük el a bizonyítást.
Ha $s = 1$, akkor $H_0/H_1 = \mathcal{G}(K \subseteq L)/\{\mathrm{id}_L\} \cong \mathcal{G}(K \subseteq L)$ ciklikus. Legyen $|\mathcal{G}(K \subseteq L)| = m$, ekkor egy $\varepsilon \in \mathbb{C}$ primitív m-edik egységgyökre tekintsük a $K \subseteq K(\varepsilon) \subseteq L(\varepsilon)$ testbővítéseket. Most $K \subseteq L$ és $K \subseteq K(\varepsilon)$ normális (lásd 13.1.Állítás) bővítések és $L(\varepsilon) = L \vee K(\varepsilon)$, ezért a 8.3.Állítás szerint a $K \subseteq L(\varepsilon)$ bővítés (és így $K(\varepsilon) \subseteq L(\varepsilon)$ is) normális. Mivel $K \subseteq L \cap K(\varepsilon) \subseteq L$ miatt $L \cap K(\varepsilon) \subseteq L$ is normális, a 12.4.Állítás a

$$\overline{\mathrm{res}} : \mathcal{G}(K(\varepsilon) \subseteq L \vee K(\varepsilon)) \longrightarrow \mathcal{G}(K \subseteq L)$$

injektív csoport homomorfizmust (beágyazást) szolgáltatja.
Így $\mathcal{G}(K(\varepsilon) \subseteq L(\varepsilon)) = \mathcal{G}(K(\varepsilon) \subseteq L \vee K(\varepsilon))$ ciklikus, mert izomorf a ciklikus $\mathcal{G}(K \subseteq L)$ csoport egy részcsoportjával (lásd a 14.7.Állítást).
Ha $|\mathcal{G}(K(\varepsilon) \subseteq L(\varepsilon))| = n$, akkor a 14.8.Állítás (Lagrange tétele) miatt n osztója az $m = |\mathcal{G}(K \subseteq L)|$ egésznek és $K(\varepsilon)$ tartalmazza az összes n-edik egységgyököt is. Valóban, minden n-edik egységgyök m-edik egységgyök is, amelyek mindegyike az ε primitív m-edik egységgyöknek valamilyen hatványa. Most a 13.4.Tételt alkalmazva kapjuk a létezését egy olyan $b \in L(\varepsilon)$ elemnek, amelyre

$$c = b^n \in K(\varepsilon) \text{ és } L(\varepsilon) = (K(\varepsilon))(b) = (K(\varepsilon))(x^n - c = 0).$$

Mivel $K \subseteq K(\varepsilon) = K(x^m - 1 = 0)$ elemi gyökbővítés és az előbbiek szerint $K(\varepsilon) \subseteq L(\varepsilon)$ is elemi gyökbővítés, ezért $K \subseteq L(\varepsilon) = \overline{L}$ olyan (normális) gyökbővítés, amelyre $L \subseteq L(\varepsilon) = \overline{L}$.
Tegyük fel, hogy az olyan $K' \subseteq L'$ normális bővítésekre igaz a bizonyítandó implikáció, amelyre a $\mathcal{G}(K' \subseteq L')$ csoportnak van $s \geq 1$ hosszúságú ciklikus faktorokkal rendelkező szubnormál lánca. Legyen most $K \subseteq L$ olyan normális bővítés, amelyre

$$\{\mathrm{id}_L\} = N_{s+1} \subseteq N_s \subseteq N_{s-1} \subseteq ... \subseteq N_1 \subseteq N_0 = \mathcal{G}(K \subseteq L)$$

egy $s+1$ hosszúságú ciklikus faktorokkal rendelkező szubnormál lánc. Tekintsük az $L_1 = L^{N_1}$ számtestet, amelyre $K \subseteq L^{N_1} \subseteq L$ és $N_1 \lhd N_0 = \mathcal{G}(K \subseteq L)$ miatt (a 11.8.Tételt figyelembe véve) $K \subseteq L^{N_1} = L_1$ normális. A 10.2.Tétel szerint a 10.A.Definícióban értelmezett

$$\mathrm{res} : \mathcal{G}(K \subseteq L) \longrightarrow \mathcal{G}(K \subseteq L_1)$$

csoport homomorfizmus szürjektív, ahonnan $\ker(\mathrm{res}) = \mathcal{G}(L_1 \subseteq L)$ és a 11.8.Tétel alapján teljesülő $N_1 = \mathcal{G}(L^{N_1} \subseteq L) = \mathcal{G}(L_1 \subseteq L)$ egyenlőség valamint a homomorfizmus tétel (14.16.Állítás 11.része) miatt csoportoknak az

$$N_0/N_1 = \mathcal{G}(K \subseteq L)/\mathcal{G}(L_1 \subseteq L) \cong \mathcal{G}(K \subseteq L_1)$$

izomorfizmusát kapjuk. Tehát $\mathcal{G}(K \subseteq L_1)$ is ciklikus. Az $s = 1$ esetben már látottakhoz hasonlóan igazolhatjuk, hogy K-nak létezik olyan $K \subseteq \overline{L_1}$ normális gyökbővítése, amelyre $K \subseteq L_1 \subseteq \overline{L_1}$. A $K \subseteq L$ és a $K \subseteq \overline{L_1}$ bővítések normalitásából előbb a $K \subseteq L \vee \overline{L_1}$ (lásd a 8.3.Állítást), majd innen az $\overline{L_1} \subseteq L \vee \overline{L_1}$ normalitása adódik. A $K \subseteq L \cap \overline{L_1}$ tartalmazás és $K \subseteq L$ normalitása miatt $L \cap \overline{L_1} \subseteq L$ is normális, így a 12.4.Állítást használva kapjuk a

$$\overline{\mathrm{res}} : \mathcal{G}(\overline{L_1} \subseteq L \vee \overline{L_1}) \longrightarrow \mathcal{G}(L \cap \overline{L_1} \subseteq L) \subseteq \mathcal{G}(L_1 \subseteq L) = N_1$$

injektív csoport homomorfizmust. Ez azt jelenti, hogy az $M = \mathcal{G}(\overline{L_1} \subseteq L \vee \overline{L_1})$ csoportot tekinthetjük N_1 részcsoportjának és

$$\{\mathrm{id}_L\} = M \cap N_{s+1} \subseteq M \cap N_s \subseteq M \cap N_{s-1} \subseteq ... \subseteq M \cap N_1 = M$$

egy s hosszúságú szubnormál lánca M-nek ciklikus faktorokkal. Valóban, $M \cap N_{i+1} \lhd M \cap N_i$ és a 14.7.Állítás alapján $M \cap N_i / M \cap N_{i+1}$ ciklikus, hiszen természetes módon beágyazható a ciklikus N_i/N_{i+1} csoportba. Tehát az $\overline{L_1} \subseteq L \vee \overline{L_1}$ normális bővítésre alkalmazhatjuk az indukciós feltevést, ez $\overline{L_1}$-nek egy olyan $\overline{L_1} \subseteq W$ normális gyökbővítését szolgáltatja, amire $\overline{L_1} \subseteq L \vee \overline{L_1} \subseteq W$. Mivel $K \subseteq \overline{L_1}$ és $\overline{L_1} \subseteq W$ gyökbővítések, ezért $K \subseteq W$ is gyökbővítés. Végül a 8.4.Tétel egy olyan $K \subseteq \overline{W}$ normális gyökbővítés létezését garantálja, amire $K \subseteq W \subseteq \overline{W}$. Az

$$L \subseteq L \vee \overline{L_1} \subseteq W \subseteq \overline{W}$$

tartalmazások nyilvánvalóan teljesülnek.

□□□

13.7.Tétel. *A $K \subseteq \mathbb{C}$ számtestre és egy $p(x) \in K[x]$ irreducibilis polinomra, valamint ennek $F = K(p(x) = 0)$ felbontási testére az alábbiak ekvivalensek:*

1. *$\mathcal{G}(K \subseteq F)$ Galois csoport feloldható.*
2. *$p(x)$-nek létezik olyan gyöke, amely K-ból gyökvonással elérhető.*
3. *$p(x)$-nek minden gyöke K-ból gyökvonással elérhető.*

Bizonyítás. (1)$\Longrightarrow$(3): Most a 13.6.Tétel szerint K-nak létezik olyan $K \subseteq \overline{F} \subseteq \mathbb{C}$ normális gyökbővítése, amelyre $K \subseteq F \subseteq \overline{F}$. Mivel a $p(x)$ minden gyöke az F felbontási testben

van, ezért az ettől bővebb $\overline{F}$ is tartalmazza a $p(x)$ gyökeit. Tehát $p(x)$ minden gyöke K-ból gyökvonással elérhető.
(3)$\Longrightarrow$(2): Nyilvánvaló.
(2)$\Longrightarrow$(1): Ha $p(x)$-nek az $\alpha \in \mathbb{C}$ gyöke K-ból gyökvonással elérhető, akkor ez azt jelenti, hogy K-nak létezik olyan $K \subseteq L$ gyökbővítése, amelyre $\alpha \in L$. A 8.4.Tétel szerint K-nak létezik olyan $K \subseteq \overline{L} \subseteq \mathbb{C}$ normális gyökbővítése is, amelyre $K \subseteq L \subseteq \overline{L}$. A nyilvánvaló $\alpha \in \overline{L}$ tartalmazás és $K \subseteq \overline{L}$ normalitása miatt $\overline{L}$ tartalmazza a $K[x]$-ben irreducibilis $p(x)$ polinom minden további gyökét is, ami $p(x)$ felbontási testére az $F \subseteq \overline{L}$ következménnyel jár. Így a $K \subseteq F$ bővítés normalitására való tekintettel a 13.6.Tétel a $\mathcal{G}(K \subseteq F)$ Galois csoport feloldhatóságát biztosítja.

□□□

13.8.Tétel. *Ha egy $K \subseteq \mathbb{R}$ számtest felett irreducibilis $p(x) \in K[x]$ polinomnak pontosan két nem valós ($\mathbb{C} \setminus \mathbb{R}$-beli) gyöke van és a $\deg(p(x)) \geq 5$ fokszám prím, akkor $p(x)$ gyökei K-ból gyökvonással nem elérhetőek.*

Bizonyítás. Mivel $K \subseteq \mathbb{R}$, ezért a komplex számok konjugálása egy $\Lambda \in \mathcal{G}(K \subseteq \mathbb{C})$ relatív automorfizmus, amelyet megszorítva a $p(x)$ polinom $F = K(p(x) = 0)$ felbontási testére egy $\Lambda \restriction F$ relatív automorfizmusát kapjuk a $K \subseteq F$ testbővítésnek. Valóban, $K \subseteq F$ véges és normális, ezért a 10.1.Állítás miatt $\Lambda \restriction F \in \mathcal{G}(K \subseteq F)$. Jelölje $\alpha_1, \alpha_2, ..., \alpha_q$ a $p(x)$ polinomnak az összes gyökeit, ekkor bármely $\Phi \in \mathcal{G}(K \subseteq F)$ relatív automorfizmust egyértelműen meghatároz az

$$\begin{pmatrix} \alpha_1 & \alpha_2 & . & . & . & \alpha_q \\ \Phi(\alpha_1) & \Phi(\alpha_2) & . & . & . & \Phi(\alpha_q) \end{pmatrix} = \begin{pmatrix} \alpha_1 & \alpha_2 & . & . & . & \alpha_q \\ \alpha_{\pi(1)} & \alpha_{\pi(2)} & . & . & . & \alpha_{\pi(q)} \end{pmatrix}$$

módon értelmezett $\pi = \overline{\Phi}$ permutáció és a $\mathcal{G}(K \subseteq F)$ Galois csoport izomorf az S_q szimmetrikus csoportban a $\overline{\Phi}$ alakú permutációk által alkotott P részcsoportal (lásd 9.6.Állítás). A $K \subseteq F$ végessége és normalitása, továbbá $p(x)$ irreducibilitása miatt a 11.6.Tétel biztosítja, hogy P a permutációknak egy tranzitív részcsoportja S_q-ban.
A $\Lambda \restriction F$-nek megfelelő permutáció P-ben egy transzpozicíó. Valóban, $\Lambda \restriction F$ a két nem valós gyökét $p(x)$-nek felcseréli (ezek egymás konjugáltjai) és a többi (valós) gyököt fixen hagyja. Mivel $q = \deg(p(x))$ prímszám, ezért a permutáció csoportok elméletéből ismert (lásd a 15.7.Tételt), hogy a fenti tulajdonságokkal rendelkező $P \leq S_q$ részcsoportra $P = S_q$. Tehát $\mathcal{G}(K \subseteq F) \cong S_q$ és $q \geq 5$ esetén a 15.6.Következmény szerint S_q nem feloldható csoport. A 13.7.Tétel szerint a $p(x)$ polinomnak nincs olyan gyöke, amely K-ból gyökvonással elérhető.

□□□