Magasabbfokú egyenletek és geometriai szerkeszthetőség

Dormán Miklós

SZTE, Bolyai Intézet

2010. november 19.

Automorfizmusok és fixtestek

Tétel.

Legyen L az $f \in K[x]$ polinom felbontási teste K felett, és jelölje R az f polinom L-beli gyökeinek halmazát. Ekkor tetszőleges $\sigma \in \mathrm{Gal}_K(f)$-ra $\sigma|_R \in S_R$, és a

$$\mathrm{Gal}_K(f) \to S_R,\ \sigma \mapsto \sigma|_R$$

leképezés injektív homomorfizmus.

Ha f irreducibilis, akkor $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \mathrm{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$.

Ha f irreducibilis, akkor $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \mathrm{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$.

Ha f irreducibilis, akkor $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \mathrm{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Tegyük fel, hogy $f \in K[x]$ egy n-edfokú polinom, amelynek n különböző gyöke van egy L felbontási testében és $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán.

Ha f irreducibilis, akkor $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \mathrm{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Tegyük fel, hogy $f \in K[x]$ egy n-edfokú polinom, amelynek n különböző gyöke van egy L felbontási testében és $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán. Legyen m az f polinom α gyökének minimálpolinomja K felett, valamint $\beta \in L$ az f polinom egy tetszőleges gyöke.

Ha f irreducibilis, akkor $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán, azaz ha α és β az f polinom gyökei f valamely felbontási testében, akkor van olyan $\sigma \in \mathrm{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Tegyük fel, hogy $f \in K[x]$ egy n-edfokú polinom, amelynek n különböző gyöke van egy L felbontási testében és $\mathrm{Gal}_K(f)$ tranzitívan hat f gyökeinek halmazán. Legyen m az f polinom α gyökének minimálpolinomja K felett, valamint $\beta \in L$ az f polinom egy tetszőleges gyöke. Ekkor van olyan $\sigma \in \mathrm{Gal}_K(f)$, amelyre $\sigma(\alpha) = \beta$. Ezért

$$m(\beta) = m(\sigma(\alpha)) = \sigma(m)(\sigma(\alpha)) = \sigma(m(\alpha)) = 0,$$

és így m-nek legalább n gyöke van. Mivel $m \mid f$, ezért $m = f$. Azaz f irreducibilis.

Legyen G permutációcsoport az X véges halmazon. Az X halmazon definiáljuk a $\sim$ relációt a következőképpen:

$$x \sim y \iff x = y \text{ vagy } (x\,y) \in G.$$

Legyen G permutációcsoport az X véges halmazon. Az X halmazon definiáljuk a $\sim$ relációt a következőképpen:

$$x \sim y \iff x = y \text{ vagy } (x\,y) \in G.$$

Legyen G permutációcsoport az X véges halmazon. Az X halmazon definiáljuk a $\sim$ relációt a következőképpen:

$$x \sim y \iff x = y \text{ vagy } (x\,y) \in G.$$

A $\sim \subseteq X \times X$ reláció nyilván reflexív és szimmetrikus. Tegyük fel, hogy az $x, y, z \in X$ elemekre teljesül, hogy $x \sim y$ és $y \sim z$. Ekkor $(x\,y), (y\,z) \in G$. Mivel G csoport, ezért $(x\,z) = (x\,y) \cdot (y\,z) \cdot (x\,y) \in G$. Azaz $(x\,z) \in G$, és így $x \sim z$. Ezzel igazoltuk, hogy $\sim$ ekvivalenciareláció.

Tegyük fel, hogy G tranzitív, és legyen rendre E_x, illetve E_y az x, illetve y elemeket tartalmazó ekvivalenciaosztály. Mivel G tranzitív, ezért van olyan $\sigma \in G$, amelyre $y = \sigma(x)$ teljesül. Ha $x' \in E_x$, akkor $x \sim x'$ miatt $(x\,x') \in G$. Így

$$G \ni \sigma^{-1}(x\,x')\sigma = (\sigma(x)\,\sigma(x')) = (y\,\sigma(x'))$$

miatt $\sigma(x') \in E_y$. Azaz $\sigma(E_x) \subseteq E_y$. Ez pedig éppen azt jelenti, hogy $|E_x| \leqslant |E_y|$. Az x és y elemek szerepét felcserélve azt kapjuk, hogy $|E_x| = |E_y|$. Ezzel megmutattuk, hogy bármely két ekvivalenciaosztály elemszáma megegyezik.

Tegyük fel, hogy G tranzitív, és legyen rendre E_x, illetve E_y az x, illetve y elemeket tartalmazó ekvivalenciaosztály. Mivel G tranzitív, ezért van olyan $\sigma \in G$, amelyre $y = \sigma(x)$ teljesül. Ha $x' \in E_x$, akkor $x \sim x'$ miatt $(x\,x') \in G$. Így

$$G \ni \sigma^{-1}(x\,x')\sigma = (\sigma(x)\,\sigma(x')) = (y\,\sigma(x'))$$

miatt $\sigma(x') \in E_y$. Azaz $\sigma(E_x) \subseteq E_y$. Ez pedig éppen azt jelenti, hogy $|E_x| \leqslant |E_y|$. Az x és y elemek szerepét felcserélve azt kapjuk, hogy $|E_x| = |E_y|$. Ezzel megmutattuk, hogy bármely két ekvivalenciaosztály elemszáma megegyezik.

Ha X elemszáma prímszám és G tartalmaz legalább egy transzpozíciót, akkor G tranzitivitása miatt G az összes transzpozíciót tartalmazza, amelyek azonban generálják S_X-et, így $G = S_X$.

Tétel.

Legyen p prímszám, és tegyük fel, hogy $f \in \mathbb{Q}[x]$ olyan p-edfokú irreducibilis polinom, amelynek pontosan $p-2$ darab valós gyöke van. Ekkor $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_p$.

Bizonyítás.

Legyen $L \subseteq \mathbb{C}$ az f polinom felbontási teste $\mathbb{Q}$ felett. Mivel f irreducibilis, ezért $\mathrm{Gal}_{\mathbb{Q}}(f)$ tranzitívan hat f (L-beli) gyökeinek R halmazán. Az $\xi\colon L \to L,\ z \to \overline{z}$ leképezés nyilván eleme f Galois-csoportjának, és $\xi|_R \in S_R$ transzpozíció. Így a

$$\{\sigma|_R \mid \sigma \in \mathrm{Gal}_K(f)\} \leqslant S_R$$

permutációcsoport tranzitív és tartalmaz transzpozíciót. Ekkor az előzőek szerint $\{\sigma|_R \mid \sigma \in \mathrm{Gal}_K(f)\} = S_R$. Továbbá,

$$\mathrm{Gal}_K(f) \cong S_R \cong S_p.$$

Példa.

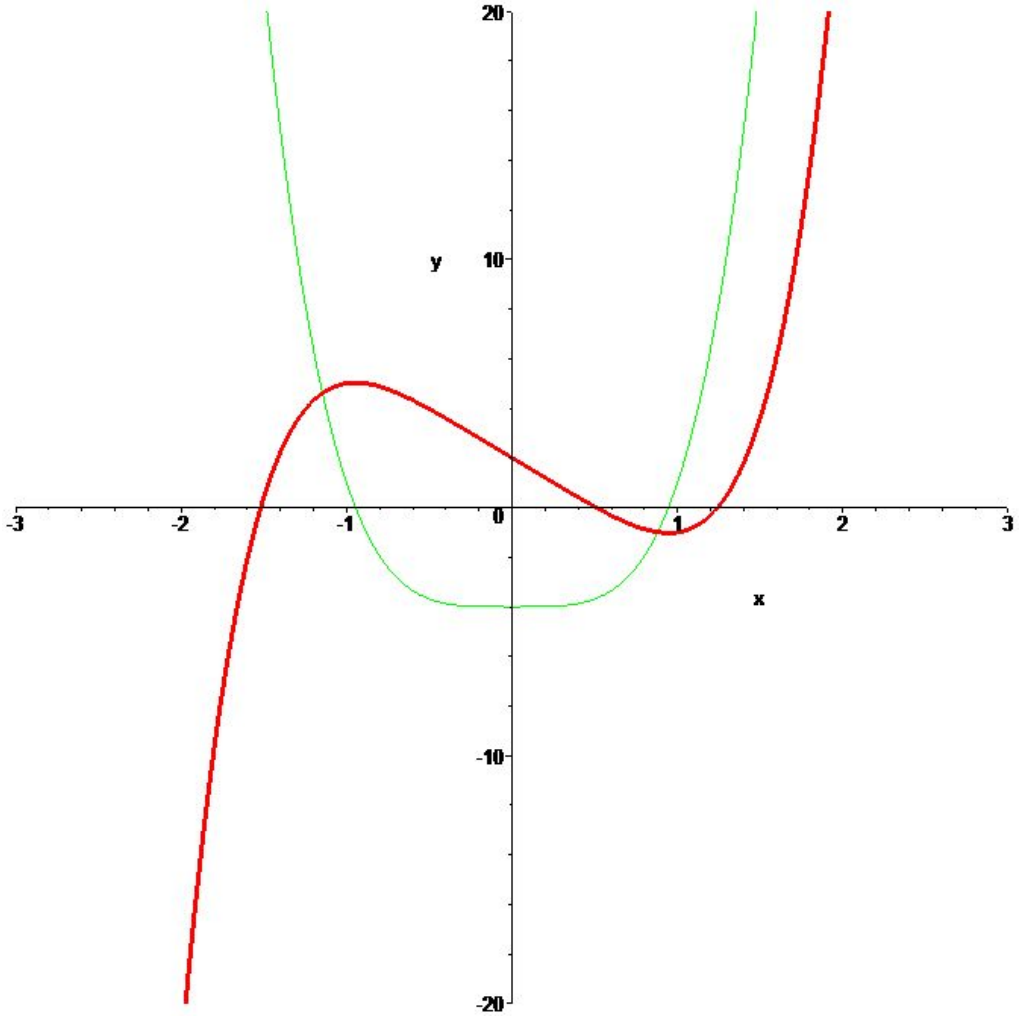
Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot.

Példa.

Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot.

Példa.

Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot. A Schönemann–Eisenstein-tétel szerint az f polinom irreducibilis.



1. ábra: Az f és $D_x(f)$ polinomok grafikonja.

A polinomnak pontosan 3 darab valós gyöke van. Az előző tétel szerint $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_5$.

A Galois-elmélet főtétele részleteiben írja le a fejezet elején bevezetett polaritást.

A Galois-elmélet főtétele részleteiben írja le a fejezet elején bevezetett polaritást.

Tétel (A Galois-elmélet Főtétele).

Legyen $L : K$ véges bővítés, $G = \mathrm{Gal}(L : K)$ és $K_0 = \varphi(G)$. Az $L : K_0$ bővítés tetszőleges M közbülső testére legyen $\gamma(M) = \mathrm{Gal}(L : M)$. Ekkor teljesülnek a következők.

Tétel (A Galois-elmélet Főtétele).

Tétel (A Galois-elmélet Főtétele).

(a) A

$$\mathrm{Sub}(G) \to \{M \mid M \text{ közbülső teste az } L : K_0 \text{ bővítésnek}\},$$
$$G \mapsto \varphi(G)$$

leképezés rendezéstartó bijekció, melynek inverze

$$\{M \mid M \text{ közbülső teste az } L : K_0 \text{ bővítésnek}\} \to \mathrm{Sub}(G),$$
$$M \mapsto \gamma(M).$$

Tétel (A Galois-elmélet Főtétele).

(a) A

$$\mathrm{Sub}(G) \to \{M \mid M \text{ közbülső teste az } L : K_0 \text{ bővítésnek}\},$$
$$G \mapsto \varphi(G)$$

leképezés rendezéstartó bijekció, melynek inverze

$$\{M \mid M \text{ közbülső teste az } L : K_0 \text{ bővítésnek}\} \to \mathrm{Sub}(G),$$
$$M \mapsto \gamma(M).$$

(b) A G csoport H részcsoportja pontosan akkor normális, ha a $\varphi(H) : K_0$ bővítés normális.

Tétel (A Galois-elmélet Főtétele).

Tétel (A Galois-elmélet Főtétele).

(c) Tegyük fel, hogy H normális részcsoport G-ben. Ha $\sigma \in G$, akkor $\sigma|_{\varphi(H)} \in \mathrm{Gal}(\varphi(H) : K_0)$. A

$$G \to \mathrm{Gal}(\varphi(H) : K_0),\ \sigma \mapsto \sigma|_{\varphi(H)}$$

leképezés szürjektív homomorfizmus, melynek magja H. Így

$$\mathrm{Gal}(\varphi(H) : K_0) \cong G/H.$$

Tétel (A Galois-elmélet Főtétele).

(c) Tegyük fel, hogy H normális részcsoport G-ben. Ha $\sigma \in G$, akkor $\sigma|_{\varphi(H)} \in \mathrm{Gal}(\varphi(H) : K_0)$. A

$$G \to \mathrm{Gal}(\varphi(H) : K_0),\ \sigma \mapsto \sigma|_{\varphi(H)}$$

leképezés szürjektív homomorfizmus, melynek magja H. Így

$$\mathrm{Gal}(\varphi(H) : K_0) \cong G/H.$$

Tétel (A Galois-elmélet Főtétele).

(c) Tegyük fel, hogy H normális részcsoport G-ben. Ha $\sigma \in G$, akkor $\sigma|_{\varphi(H)} \in \mathrm{Gal}(\varphi(H) : K_0)$. A

$$G \to \mathrm{Gal}(\varphi(H) : K_0),\ \sigma \mapsto \sigma|_{\varphi(H)}$$

leképezés szürjektív homomorfizmus, melynek magja H. Így

$$\mathrm{Gal}(\varphi(H) : K_0) \cong G/H.$$

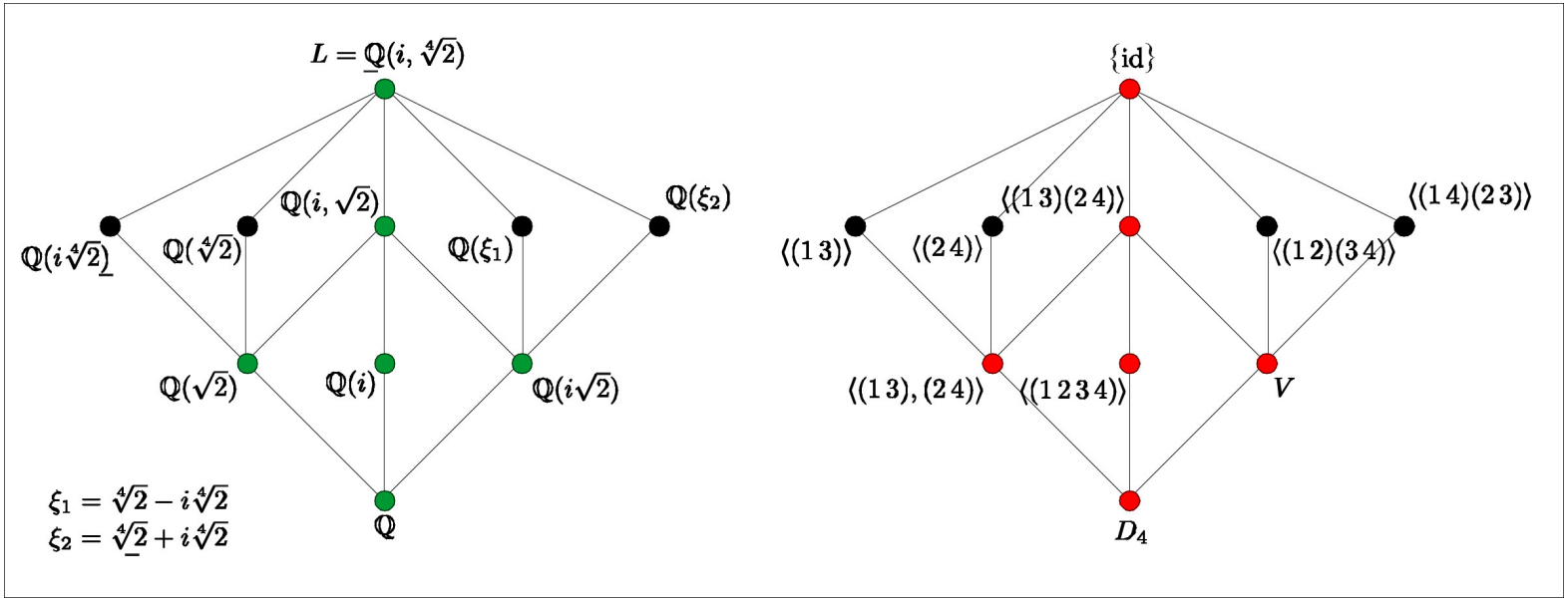
Ha az $L : K$ bővítés Galois-bővítés, akkor $K_0 = K$

Példa: az $x^4 - 2 \in \mathbb{Q}[x]$ polinom vizsgálata.

Az $x^4 - 2$ polinom $\mathbb{Q}$ feletti felbontási teste $F = \mathbb{Q}(\sqrt[4]{2}, i) = \mathbb{Q}(\sqrt[4]{2} + i)$:

$$x^4 - 2 = (x - \sqrt[4]{2})(x + \sqrt[4]{2})(x - i\sqrt[4]{2})(x + i\sqrt[4]{2}).$$

Mivel $\sqrt[4]{2} + i$ minimálpolinomja $\mathbb{Q}$ felett: $x^8 + 4x^6 + 2x^4 + 28x^2 + 1$, ezért $[F : \mathbb{Q}] = 8 = |\mathrm{Gal}(F : \mathbb{Q})| = |\mathrm{Gal}_{\mathbb{Q}}(x^4 - 2)|$. Ha $\varphi \in \mathrm{Gal}_{\mathbb{Q}}(x^4 - 2)$, akkor $\varphi(\sqrt[4]{2}) \in \{\sqrt[4]{2}, i\sqrt[4]{2}, -\sqrt[4]{2}, -i\sqrt[4]{2}\}$ és $\varphi(i) \in \{-i, i\}$. Az $x^4 - 2$ ($\mathbb{Q}$ felett irrdeucibilis) polinom Galois-csoportja izomorf D_4-gyel. A Galois-elmélet főtételét a következő ábra szemlélteti.



2. ábra: Az $L : \mathbb{Q}$ bővítés és közbülső testei.

Tétel.

Legyen K számtest, $\alpha \in K$ és p prímszám. Ekkor az $x^p - \alpha$ polinom vagy irreducibilis K felett, vagy van gyöke K-ban. Ha legalább két gyöke van K-ban, akkor elsőfokú polinomok szorzatára bomlik K felett.

Tétel.

Legyen K számtest, $\alpha \in K$ és p prímszám. Ekkor az $x^p - \alpha$ polinom vagy irreducibilis K felett, vagy van gyöke K-ban. Ha legalább két gyöke van K-ban, akkor elsőfokú polinomok szorzatára bomlik K felett.

Tétel.

Legyen K számtest, $\alpha \in K$, és p prímszám. Ha K tartalmazza a p-edik egységgyököket, akkor a $K(\beta) : K$ bővítés normális, ahol $\beta^p = \alpha$. A bővítés foka 1 vagy p. Ez utóbbi esetben $x^p - \alpha$ irreducibilis K felett.

Definíció: normállánc, faktor, feloldható csoport

A G csoport **normálláncának** nevezzük G részcsoportjainak egy $G_0, \ldots, G_n$ sorozatát, amelyre

$$\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{n-1} \lhd G_n = G$$

teljesül. A G_i/G_{i-1} faktorcsoportokat e normállánc **faktorainak** nevezzük; n a normállánc **hossza**.
Azt mondjuk, hogy a G csoport **feloldható**, ha G-nek van olyan normállánca, amelynek faktorai Abel-csoportok.

Példák feloldható csoportokra.

Az S_3 csoport feloldható, mivel a

$$\{\mathrm{id}\} \triangleleft A_3 \triangleleft S_3$$

normállánc faktorai Abel-csoportok, sőt ciklikus csoportok:

$$A_3/\{\mathrm{id}\} \cong A_3 = \langle (1\,2\,3) \rangle, \quad S_3/A_3 \cong C_2.$$

Az S_4 csoport is feloldható, az

$$\{\mathrm{id}\} \triangleleft \{\mathrm{id}, (1\,2)(3\,4)\} \triangleleft \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \triangleleft A_4 \triangleleft S_3$$

normállánc faktorai Abel-csoportok.

Tétel.

Az A_n alternáló csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Az A_n alternáló csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

Tétel.

Az A_n alternáló csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

(a) ha G feloldható, akkor H is feloldható;

Tétel.

Az A_n alternáló csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

(a) ha G feloldható, akkor H is feloldható;

(b) a G csoport pontosan akkor feloldható, ha N és G/N is feloldható.

Tétel.

Az A_n alternáló csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen G csoport, $H \leqslant G$ és $N \triangleleft G$. Ekkor igazak a következők:

(a) ha G feloldható, akkor H is feloldható;

(b) a G csoport pontosan akkor feloldható, ha N és G/N is feloldható.

Tétel.

Az S_n csoport $n \geqslant 5$ esetén nem feloldható.

Tétel.

Legyen K számtest, és ε primitív n-edik egységgyök. Ekkor a $K(\varepsilon) : K$ bővítés normális, és $\mathrm{Gal}(K(\varepsilon) : K)$ izomorf $\mathbb{Z}_n^\times$ egy részcsoportjával.

Tétel.

Legyen K számtest, és ε primitív n-edik egységgyök. Ekkor a $K(\varepsilon) : K$ bővítés normális, és $\mathrm{Gal}(K(\varepsilon) : K)$ izomorf $\mathbb{Z}_n^\times$ egy részcsoportjával.

Tétel.

Legyen K számtest és $f \in K[x]$ irreducibilis polinom. Ha f valamelyik komplex gyöke felírható egy olyan képlettel, amely f együtthatóiból a négy alapművelet és gyökvonások felhasználásával keletkezik, akkor az f polinom K feletti Galois-csoportja feloldható csoport.

Tétel.

Legyen K számtest, és ε primitív n-edik egységgyök. Ekkor a $K(\varepsilon) : K$ bővítés normális, és $\mathrm{Gal}(K(\varepsilon) : K)$ izomorf $\mathbb{Z}_n^\times$ egy részcsoportjával.

Tétel.

Legyen K számtest és $f \in K[x]$ irreducibilis polinom. Ha f valamelyik komplex gyöke felírható egy olyan képlettel, amely f együtthatóiból a négy alapművelet és gyökvonások felhasználásával keletkezik, akkor az f polinom K feletti Galois-csoportja feloldható csoport.

Példa.

Az $x^5 - 4x + 2$ polinom egyik gyöke sem gyökkifejezés $\mathbb{Q}$ felett.

Tétel.

Legyenek $y_1, \ldots, y_n$ határozatlanok, K a $\mathbb{Q}[y_1, \ldots, y_n]$ hányadosteste, és

$$f = x^n + y_1 x^{n-1} + \cdots + y_{n-1} x + y_n \in K[x].$$

Legyen F egy felbontási teste f-nek. Ekkor $\mathrm{Gal}(F : K)$ izomorf S_n-nel.

Tétel.

Legyenek $y_1, \ldots, y_n$ határozatlanok, K a $\mathbb{Q}[y_1, \ldots, y_n]$ hányadosteste, és

$$f = x^n + y_1 x^{n-1} + \cdots + y_{n-1} x + y_n \in K[x].$$

Legyen F egy felbontási teste f-nek. Ekkor $\mathrm{Gal}(F : K)$ izomorf S_n-nel.

Tétel (Ruffini–Abel).

Ha $n \geqslant 5$, akkor az általános n-edfokú egyenletre nem létezik gyökképlet.

Definíció: gyökkifejezés.

Legyen K számtest. Azt mondjuk, hogy a $z \in \mathbb{C}$ komlex szám **gyökkifejezés** K felett, ha van olyan $n \in \mathbb{N}_0$ és egy

$$K = K_0 < K_1 < \cdots < K_{n-1} < K_n \leqslant \mathbb{C}$$

testlánc, amelyre $z \in K_n$, és minden $0 \leqslant i \leqslant n-1$-re $K_{i+1} = K_i(\beta_i)$, ahol $\beta_i^{p_i} \in K_i$, p_i prímszám, és az $x^{p_i} - \beta_i$ polinom irreducibilis K_i felett.

Lemma.

Legyen K számtest és p prímszám Tegyük fel, hogy a K számtest tartalmazza a p-edik egységgyököket. Ha az $L : K$ bővítés egy p-edfokú normális bővítés, akkor van olyan $\alpha \in K$, hogy az L test az $x^p - \alpha \in K[x]$ irreducibilis polinom felbontási teste K felett.

Lemma.

Legyen K számtest és p prímszám Tegyük fel, hogy a K számtest tartalmazza a p-edik egységgyököket. Ha az $L : K$ bővítés egy p-edfokú normális bővítés, akkor van olyan $\alpha \in K$, hogy az L test az $x^p - \alpha \in K[x]$ irreducibilis polinom felbontási teste K felett.

Tétel.

Legyen K olyan számtest, amelynek minden eleme gyökkifejezés egy $K_0 \leqslant K$ számtest felett. Ha ε primitív n-edik egységgyök, akkor $K(\varepsilon)$ minden eleme gyökkifejezés K_0 felett.

Tétel.

Legyen K számtest, és $L : K$ véges normális bővítés, amelynek Galois-csoportja feloldható. Ekkor L minden eleme gyökkifejezés K felett.

Tétel.

Legyen K számtest, és $L : K$ véges normális bővítés, amelynek Galois-csoportja feloldható. Ekkor L minden eleme gyökkifejezés K felett.

Következmény.

Ha az $f \in K[x]$ polinom egyik gyöke gyökkifejezés, akkor mindegyik gyöke az.