Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. március 27.

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).

(i) A $\mathrm{Sub}(G) \to \{M \mid K_0 \leqslant M \leqslant L\}$, $G \mapsto \varphi(G)$ leképezés rendezéstartó bijekció, melynek inverze az $\{M \mid K_0 \leqslant M \leqslant L\} \to \mathrm{Sub}(G)$, $M \mapsto \gamma(M)$ leképezés.

Tétel (A Galois-elmélet Főtétele).

(i) A $\mathrm{Sub}(G) \to \{M \mid K_0 \leqslant M \leqslant L\}$, $G \mapsto \varphi(G)$ leképezés rendezéstartó bijekció, melynek inverze az $\{M \mid K_0 \leqslant M \leqslant L\} \to \mathrm{Sub}(G)$, $M \mapsto \gamma(M)$ leképezés.

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

Tétel (A Galois-elmélet Főtétele).

(i) A $\mathrm{Sub}(G) \to \{M \mid K_0 \leqslant M \leqslant L\}$, $G \mapsto \varphi(G)$ leképezés rendezéstartó bijekció, melynek inverze az $\{M \mid K_0 \leqslant M \leqslant L\} \to \mathrm{Sub}(G)$, $M \mapsto \gamma(M)$ leképezés.

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

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

A Galois-elmélet Főtételének bizonyítása.

(i) A $\mathrm{Sub}(G) \to \{M \mid K_0 \leqslant M \leqslant L\}$, $G \mapsto \varphi(G)$ leképezés rendezéstartó bijekció, melynek inverze az $\{M \mid K_0 \leqslant M \leqslant L\} \to \mathrm{Sub}(G)$, $M \mapsto \gamma(M)$ leképezés.

A Galois-elmélet Főtételének bizonyítása.

(i) A $\mathrm{Sub}(G) \to \{M \mid K_0 \leqslant M \leqslant L\}$, $G \mapsto \varphi(G)$ leképezés rendezéstartó bijekció, melynek inverze az $\{M \mid K_0 \leqslant M \leqslant L\} \to \mathrm{Sub}(G)$, $M \mapsto \gamma(M)$ leképezés.

A Galois-elmélet Főtételének bizonyítása.

(i) A $\mathrm{Sub}(G) \to \{M \mid K_0 \leqslant M \leqslant L\}$, $G \mapsto \varphi(G)$ leképezés rendezéstartó bijekció, melynek inverze az $\{M \mid K_0 \leqslant M \leqslant L\} \to \mathrm{Sub}(G)$, $M \mapsto \gamma(M)$ leképezés.

Ha $H \leqslant G$, akkor H véges, és így $H = \gamma\varphi(H)$. Ezért a $\varphi|_{\mathrm{Sub}(G)}$ leképezés injektív. Ha $K_0 \leqslant M \leqslant L$, akkor az $L : M$ bővítés normáls és szeparábilis, mivel $L : K_0$ Galois-bővítés. Így $\varphi\gamma(M) = M$ következtében φ szürjektív is, melynek inverze $\gamma|_{\{M|K_0 \leqslant M \leqslant L\}}$.

A Galois-elmélet Főtételének bizonyítása (folytatás).

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

A Galois-elmélet Főtételének bizonyítása (folytatás).

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

A Galois-elmélet Főtételének bizonyítása (folytatás).

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

Tegyük fel, hogy $K_0 \leqslant M \leqslant L$ és $\sigma \in G$. Ekkor $K_0 \leqslant \sigma(M) \leqslant L$. Vegyük észre, hogy

$$\begin{aligned}
\tau \in \gamma(\sigma(M)) &\iff \tau\sigma(m) = \sigma(m) \quad (\forall m \in M) \\
&\iff \sigma^{-1}\tau\sigma(m) = m \quad (\forall m \in M) \\
&\iff \sigma^{-1}\tau\sigma \in \gamma(M) \\
&\iff \tau \in \sigma(\gamma(M))\sigma^{-1},
\end{aligned}$$

azaz $\gamma(\sigma(M)) = \sigma(\gamma(M))\sigma^{-1}$.

A Galois-elmélet Főtételének bizonyítása (folytatás).

Tegyük fel, hogy $H \triangleleft G$. Ekkor tetszőleges $\sigma \in G$-re

$$H = \sigma H \sigma^{-1} = \sigma(\gamma\varphi(H))\sigma^{-1} = \gamma(\sigma(\varphi(H))),$$

így $\varphi(H) = \varphi(\gamma(\sigma(\varphi(H)))) = \sigma(\varphi(H))$ teljesül tetszőleges $\sigma \in G$-re. Ez pedig éppen azt jelenti, hogy a $\varphi(H) : K_0$ bővítés normális.
Tegyük fel, hogy a $\varphi(H) : K_0$ bővítés normális. Ekkor tetszőleges $\sigma \in G$-re

$$H = \gamma\varphi(H) = \gamma(\sigma(\varphi(H))) = \sigma(\gamma(\varphi(H)))\sigma^{-1} = \sigma H \sigma^{-1},$$

azaz H normális részcsoport G-ben.

A Galois-elmélet Főtételének bizonyítása (folytatás).

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

A Galois-elmélet Főtételének bizonyítása (folytatás).

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

A Galois-elmélet Főtételének bizonyítása (folytatás).

(iii) 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 $\mathrm{Gal}(\varphi(H) : K_0) \cong G/H$. Mivel $H \lhd G$, ezért a $\varphi(H) : K_0$ bővítés normális. Így tetszőleges $\sigma \in G$-re $\sigma(\varphi(H)) = \varphi(H)$ teljesül, azaz $\sigma|_{\varphi(H)} \in \mathrm{Gal}(\varphi(H) : K_0)$. Megmutatjuk, hogy a leképezés szürjektív. Legyen $\xi \in \mathrm{Gal}(\varphi(H) : K_0)$. Mivel az $L : \varphi(H)$ bővítés véges és normális, ezért L valamely $\varphi(H)$ feletti polinom felbontási teste. Ezért van olyan $\sigma : L \to L$ automorfizmus, amely kiterjesztése ξ-nek. Azaz a leképezés szürjektív. A fennmaradó állítás a homomorfia-tétel következménye. Ezzel igazoltuk a Galois-elmélet főtételét.

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

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

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

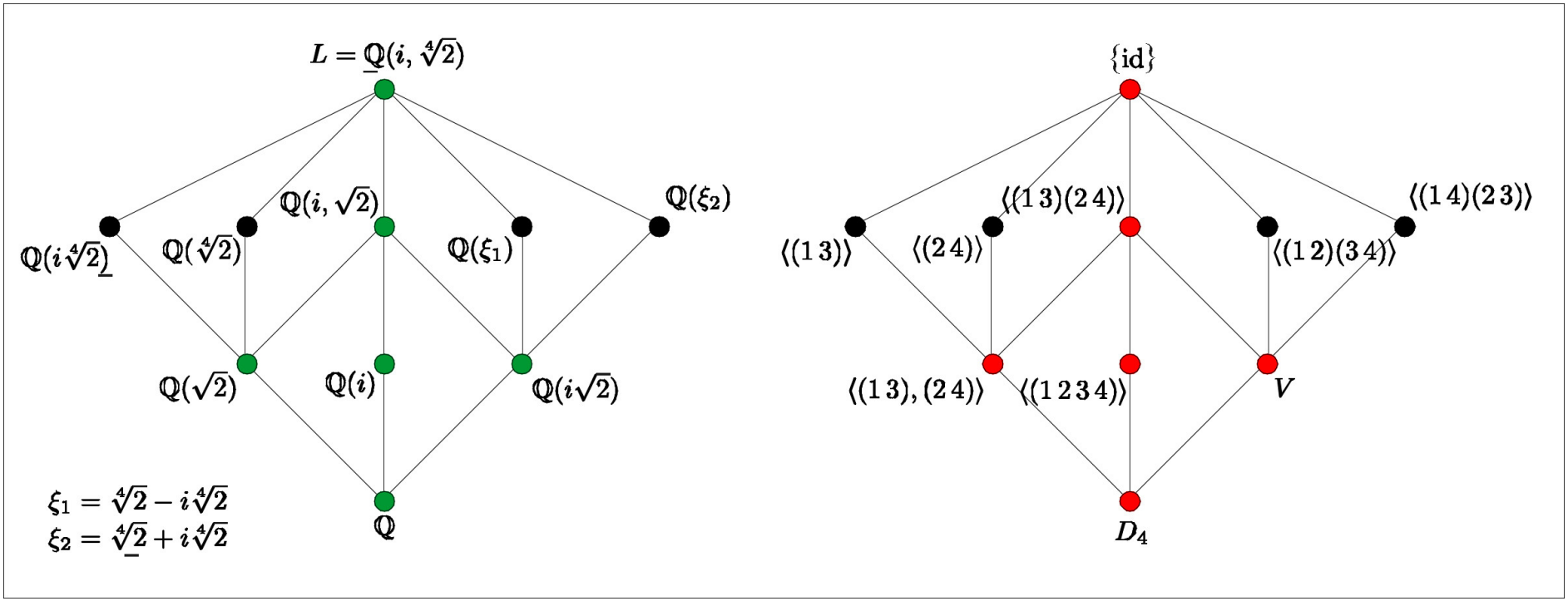
Mivel $\sqrt[4]{2} + i$ minimálpolinomja $\mathbb{Q}$ felett: $x^8 + 4x^6 + 2x^4 + 28x^2 + 1$, ezért

$$|\mathrm{Gal}_{\mathbb{Q}}(x^4 - 2)| = |\mathrm{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = 8.$$

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.

Automorfizmusok és fixtestek

A Galois-elmélet főtétele (egy példa).



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

Véges testek

Tétel.

Minden véges test elemszáma prímhatvány.

Véges testek

Tétel.

Minden véges test elemszáma prímhatvány.

Tétel.

Legyen p prímszám és n természetes szám. Ekkor van olyan K test, amelynek pontosan p^n eleme van. A K test az $f = x^{p^n} - x$ polinom felbontási teste prímteste felett. Ha az L test elemszáma is p^n, akkor $L \cong K$.

Bizonyítás.

Legyen K az $f \in \mathbb{Z}_p[x]$ polinom egy felbontási teste. Mivel $D_x(f) = -1$, ezért f-nek pontosan p^n darab különböző gyöke van K-ban. Felhasználva, hogy $\alpha \in K$ pontosan akkor gyöke f-nek, ha $\alpha^{p^n} = \alpha$, azt kapjuk, hogy f gyökeinek halmaza éppen $R = \{\alpha \in K \mid \mathfrak{F}^n(\alpha) = \alpha\}$. Így R olyan részteste K-nak, amely felett f elsőfokú tényezők szorzatára bomlik, azaz $R = K$. Legyen L olyan véges test, melynek elemszáma p^n. Ekkor bármely $u \in L^\times$-ra $u^{p^n-1} = u$, azaz L minden eleme gyöke az $x^{p^n} - x$ polinomnak. Ezért L éppen az $x^{p^n} - x$ polinom felbontási teste a prímteste, azaz $\mathbb{Z}_p$ felett. Így $L \cong K$.

Véges testek

Következmény.

Ha K véges test, melynek prímteste $\mathbb{Z}_p$, akkor a $K : \mathbb{Z}_p$ bővítés Galois-bővítés.

Véges testek

Következmény.

Ha K véges test, melynek prímteste $\mathbb{Z}_p$, akkor a $K : \mathbb{Z}_p$ bővítés Galois-bővítés.

Következmény.

Ha az L véges test a K test bővítése, akkor az $L : K$ bővítés Galois-bővítés.

Véges testek

Tétel.

Legyen K tetszőleges test és G véges részcsoportja $K^\times$-nak. Ekkor G ciklikus.

Véges testek

Tétel.

Legyen K tetszőleges test és G véges részcsoportja $K^\times$-nak. Ekkor G ciklikus.

Bizonyítás.

Legyen n a G véges Abel-csoport exponense. Ekkor $g^n = 1$ teljesül tetszőleges $g \in G$-re, azaz G minden eleme gyöke az $x^n - 1 \in K[x]$ polinomnak, így $|G| \leqslant n$. Mivel $n \leqslant |G|$ nyilván teljesül, ezért $n = |G|$. Azaz G ciklikus.

Véges testek

Tétel.

Legyen K tetszőleges test és G véges részcsoportja $K^\times$-nak. Ekkor G ciklikus.

Bizonyítás.

Legyen n a G véges Abel-csoport exponense. Ekkor $g^n = 1$ teljesül tetszőleges $g \in G$-re, azaz G minden eleme gyöke az $x^n - 1 \in K[x]$ polinomnak, így $|G| \leqslant n$. Mivel $n \leqslant |G|$ nyilván teljesül, ezért $n = |G|$. Azaz G ciklikus.

Következmény.

Ha K véges test, akkor $K^\times$ ciklikus.

Véges testek

Tétel.

Legyen K tetszőleges test és G véges részcsoportja $K^\times$-nak. Ekkor G ciklikus.

Bizonyítás.

Legyen n a G véges Abel-csoport exponense. Ekkor $g^n = 1$ teljesül tetszőleges $g \in G$-re, azaz G minden eleme gyöke az $x^n - 1 \in K[x]$ polinomnak, így $|G| \leqslant n$. Mivel $n \leqslant |G|$ nyilván teljesül, ezért $n = |G|$. Azaz G ciklikus.

Következmény.

Ha K véges test, akkor $K^\times$ ciklikus.

Következmény.

Ha az L test véges, akkor az $L : K$ testbővítés egyszerű. Ekkor G ciklikus.

Véges testek

Tétel.

Legyen K p^n-elemű test. Ekkor $\mathrm{Aut}(K) = \langle \mathfrak{F} \rangle$.

Véges testek

Tétel.

Legyen K p^n-elemű test. Ekkor $\mathrm{Aut}(K) = \langle \mathfrak{F} \rangle$.

Következmény.

Ha az L test véges és $L : K$ testbővítés, akkor $\mathrm{Gal}(L : K)$ ciklikus, melynek rendje $[L : K]$.