Testelmélet és Galois-elmélet

Dormán Miklós

SZTE, Bolyai Intézet

2009. március 20.

Automorfizmusok és fixtestek

Fixtestek és Galois-csoportok

Definíció: Galois-kapcsolat.

Legyenek A és B tetszőleges halmazok, és $\Delta \subseteq A \times B$. Legyenek φ és γ a következő leképezések:

$$\varphi\colon P(A) \to P(B), \quad U \mapsto \{b \in B \mid (u,b) \in \Delta \text{ minden } u \in U\text{-ra}\},$$
$$\gamma\colon P(B) \to P(A), \quad V \mapsto \{a \in A \mid (a,v) \in \Delta \text{ minden } v \in V\text{-re}\}.$$

A (φ, γ) leképezéspárt a $P(A)$ és $P(B)$ halmazok közötti (a Δ megfeleltetéshez tartozó) **Galois-kapcsolatnak** nevezzük.

Definíció: antimonoton leképezés.

Legyenek A és B tetszőleges halmazok, $\xi\colon P(A) \longrightarrow P(B)$ tetszőleges leképezések. Ekkor azt mondjuk, hogy a ξ leképezés **antimonoton**, ha bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\xi(U') \subseteq \xi(U)$.

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és
- idempotens, azaz bármely $U \in P(A)$-ra $\omega(\omega(U)) = \omega(U)$.

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és
- idempotens, azaz bármely $U \in P(A)$-ra $\omega(\omega(U)) = \omega(U)$.

Definíció: polaritás

Legyen A tetszőleges halmaz, $\omega\colon P(A) \to P(A)$ tetszőleges leképezés. Az ω leképezés **polaritás** az A halmazon, ha ω

- monoton, azaz bármely $U, U' \in P(A)$-ra $U \subseteq U'$ esetén $\omega(U) \subseteq \omega(U')$,
- extenzív, azaz bármely $U \in P(A)$-ra $U \subseteq \omega(U)$, és
- idempotens, azaz bármely $U \in P(A)$-ra $\omega(\omega(U)) = \omega(U)$.

Azt mondjuk, hogy az $U \subseteq A$ halmaz **zárt ω-ra vonatkozóan**, ha $\omega(U) = U$.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

(1) A φ és γ leképezések antimonotonok.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

(1) A φ és γ leképezések antimonotonok.

(2) A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás a B, illetve az A halmazon.

Tétel (A Galois-kapcsolat tulajdonságai).

Legyenek A és B nemüres halmazok, és (φ, γ) Galois-kapcsolat a $P(A)$ és $P(B)$ halmazok között. Ekkor teljesülnek a következők.

(1) A φ és γ leképezések antimonotonok.

(2) A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás a B, illetve az A halmazon.

(3) Az $U \subseteq A$ halmaz pontosan akkor zárt $\gamma\varphi$-re vonatkozóan, ha van olyan $V \subseteq B$, amelyre $U = \gamma(V)$.

Bizonyítás.

Bizonyítás.

Bizonyítás.

(1) A φ és γ leképezések antimonotonok.

Bizonyítás.

(1) A φ és γ leképezések antimonotonok.

Ez az állítás nyilvánvaló.

Bizonyítás.

(1) A φ és γ leképezések antimonotonok.

Ez az állítás nyilvánvaló.

(2) A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás a B, illetve az A halmazon.

Bizonyítás.

(1) A φ és γ leképezések antimonotonok.
Ez az állítás nyilvánvaló.
(2) A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás a B, illetve az A halmazon.
Az állítást $\varphi\gamma$-ra igazoljuk. Legyen $U, U' \in P(A)$, $U \subseteq U'$. Ekkor (1)-et felhasználva azt kapjuk, hogy $\gamma(U') \subseteq \gamma(U)$, és így szintén (1) szerint:

$$\varphi\gamma(U) = \varphi(\gamma(U)) \subseteq \varphi(\gamma(U')) = \varphi\gamma(U'),$$

azaz $\varphi\gamma$ monoton.

Bizonyítás (folytatás).

Legyen V tetszőleges részhalmaza B-nek. Tegyük fel, hogy van olyan $v \in V$, amely nem eleme $\varphi\gamma(V)$-nek. Ekkor

$$v \notin \varphi\gamma(V) \Longleftrightarrow \text{van olyan } u_0 \in \gamma(V), \text{ amelyre } (u_0, v) \notin \Delta.$$

Így azonban γ definíciója miatt azt kapjuk, hogy

$$u_0 \in \gamma(V) \Longleftrightarrow \text{minden } v \in V\text{-re, } (u_0, v) \in \Delta,$$

ami ellentmond az előzőeknek. Ezzel igazoltuk, hogy $\varphi\gamma$ extenzív.

Bizonyítás (folytatás).

Legyen V tetszőleges részhalmaza B-nek. Ekkor $\varphi\gamma$ extenzivitása miatt $V \subseteq \varphi\gamma(V)$. Felhasználva, hogy γ antimonoton azt kapjuk, hogy $\gamma(V) \supseteq \gamma(\varphi\gamma(V)) = \gamma\varphi\gamma(V)$. Másrészt, $\gamma\varphi$ extenzitvitása miatt $\gamma(V) \subseteq \gamma\varphi(\gamma(V)) = \gamma\varphi\gamma(V)$, és így az adódik, hogy

$$\gamma(V) = \gamma\varphi\gamma(V). \tag{1}$$

Ebből pedig már következik, hogy

$$\varphi\gamma\varphi\gamma(V) = \varphi\gamma(V),$$

azaz $\varphi\gamma$ idempotens. Ezzel igazoltuk, hogy a $\varphi\gamma$ leképezés polaritás. A $\gamma\varphi$ leképezésre az állítás hasonlóan igazolható.

Bizonyítás (folytatás).

(3) Az $U \subseteq A$ halmaz pontosan akkor zárt $\gamma\varphi$-re vonatkozóan, ha van olyan $V \subseteq B$, amelyre $U = \gamma(V)$.

Bizonyítás (folytatás).

(3) Az $U \subseteq A$ halmaz pontosan akkor zárt $\gamma\varphi$-re vonatkozóan, ha van olyan $V \subseteq B$, amelyre $U = \gamma(V)$.

Bizonyítás (folytatás).

(3) Az $U \subseteq A$ halmaz pontosan akkor zárt $\gamma\varphi$-re vonatkozóan, ha van olyan $V \subseteq B$, amelyre $U = \gamma(V)$.
Tegyük fel, hogy $U \subseteq A$ zárt $\gamma\varphi$-re vonatkozóan, azaz $\gamma\varphi(U) = U$. Ekkor $V = \varphi(U) \subseteq B$-re teljesül, hogy $U = \gamma\varphi(U) = \gamma(\varphi(U)) = \gamma(V)$.
Fordítva, tegyük fel, hogy $U = \gamma(V)$ valamely $V \subseteq B$-re. Ekkor (1) miatt

$$U = \gamma(V) = \gamma\varphi\gamma(V) = \gamma\varphi(\gamma(V)) = \gamma\varphi(U),$$

azaz U zárt $\gamma\varphi$-re vonatkozóan. Ezzel a tétel állításait igazoltuk.

Példa.

Legyen L test, $A = \mathrm{Aut}(L)$, $B = L$, valamint legyen Δ az alábbi megfeleltetés A-ból B-be: $\Delta = \{(\sigma, a) \in \mathrm{Aut}(L) \times L \mid \sigma(a) = a\}$. Ekkor tetszőleges $U \subseteq \mathrm{Aut}(L)$, $V \subseteq L$ halmazokra azt kapjuk, hogy

$$\begin{aligned}
\varphi(U) &= \{a \in L \mid (\tau, a) \in \Delta \text{ minden } \tau \in U\text{-ra}\}, \\
&= \{a \in L \mid \tau(a) = a \text{ minden } \tau \in U\text{-ra}\} \subset L, \\
\gamma(V) &= \{\sigma \in \mathrm{Aut}(L) \mid (\sigma, v) \in \Delta \text{ minden } v \in V\text{-re}\}, \\
&= \{\sigma \in \mathrm{Aut}(L) \mid \sigma(v) = v \text{ minden } v \in V\text{-re}\} \subset \mathrm{Aut}_{\cdot}(L)
\end{aligned}$$

A továbbiakban rögzítsük az L testet és a (φ, γ) Galois-kapcsolatot.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Bizonyítás.

Az, hogy $\varphi(U)$ test, azaz részteste L-nek, nyilvánvaló.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Bizonyítás.

Az, hogy $\varphi(U)$ test, azaz részteste L-nek, nyilvánvaló.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Bizonyítás.

Az, hogy $\varphi(U)$ test, azaz részteste L-nek, nyilvánvaló. Mivel $U \subseteq \langle U \rangle$, ezért φ antimonotonitása miatt $\varphi(\langle U \rangle) \subseteq \varphi(U)$.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Bizonyítás.

Az, hogy $\varphi(U)$ test, azaz részteste L-nek, nyilvánvaló. Mivel $U \subseteq \langle U \rangle$, ezért φ antimonotonitása miatt $\varphi(\langle U \rangle) \subseteq \varphi(U)$. Felhasználva, hogy $\gamma\varphi(U)$ olyan részcsoportja $\mathrm{Aut}(L)$-nek, amely tartalmazza U-t, azt kapjuk, hogy $U \subseteq \langle U \rangle \subseteq \gamma\varphi(U)$.

Tétel.

Legyen L tetszőleges test és $U \subseteq \mathrm{Aut}(L)$. Ekkor $\varphi(U)$ részteste L-nek, valamint $\varphi(U) = \varphi(\langle U \rangle)$.

Bizonyítás.

Az, hogy $\varphi(U)$ test, azaz részteste L-nek, nyilvánvaló. Mivel $U \subseteq \langle U \rangle$, ezért φ antimonotonitása miatt $\varphi(\langle U \rangle) \subseteq \varphi(U)$. Felhasználva, hogy $\gamma\varphi(U)$ olyan részcsoportja $\mathrm{Aut}(L)$-nek, amely tartalmazza U-t, azt kapjuk, hogy $U \subseteq \langle U \rangle \subseteq \gamma\varphi(U)$. A Galois-kapcsolatok tulajdonságait alkalmazva azt kapjuk, hogy

$$\varphi(U) = \varphi\gamma\varphi(U) = \varphi(\gamma\varphi(U)) \subseteq \varphi(\langle U \rangle) \subseteq \varphi(U),$$

azaz $\varphi(U) = \varphi(\langle U \rangle)$. Ezzel az állítást igazoltuk.

Az előző tétel állítása éppen azt mondja, hogy általában elegendő csupán $\mathrm{Aut}(L)$ részcsoportjaival foglalkozni. Legyen G részcsoportja $\mathrm{Aut}(L)$-nek. Tetszőleges $\alpha \in L$-re definiáljuk a T_α leképezést az alábbi módon:

$$T_\alpha \colon G \to L, \quad \sigma \mapsto \sigma(\alpha).$$

Mivel L^G vektortér L felett, ezért L^G az L test $\varphi(G)$ részteste felett is vektortér.

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

(i) A lineárisan független $\varphi(G)$ felett;

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

(i) A lineárisan független $\varphi(G)$ felett;

(ii) $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett;

Tétel.

Legyen G részcsoportja $\mathrm{Aut}(L)$-nek, és legyen $A \subseteq L$. Ekkor a következő állítások ekvivalensek:

(i) A lineárisan független $\varphi(G)$ felett;

(ii) $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett;

(iii) $\{T_\alpha \mid \alpha \in A\}$ lineárisan független L felett.

Bizonyítás.

(iii)$\Longrightarrow$(ii), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független L felett, akkor $\varphi(G)$ felett is.

Bizonyítás.

(iii)$\Longrightarrow$(ii), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független L felett, akkor $\varphi(G)$ felett is.

Bizonyítás.

(iii)$\Longrightarrow$(ii), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független L felett, akkor $\varphi(G)$ felett is.

Mivel $\varphi(G) \leqslant L$, ezért az állítás nyilvánvaló.

Bizonyítás (folytatás).

(ii)$\Longrightarrow$(i), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett, akkor A is lineárisan független független $\varphi(G)$ felett.

Bizonyítás (folytatás).

(ii)$\Longrightarrow$(i), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett, akkor A is lineárisan független független $\varphi(G)$ felett.

Bizonyítás (folytatás).

(ii)$\Longrightarrow$(i), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett, akkor A is lineárisan független független $\varphi(G)$ felett.

Tegyük fel, hogy A nem lineárisan független $\varphi(G)$ felett.

Bizonyítás (folytatás).

(ii)$\Longrightarrow$(i), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett, akkor A is lineárisan független független $\varphi(G)$ felett.

Tegyük fel, hogy A nem lineárisan független $\varphi(G)$ felett. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_n \in A$ vektorok és $a_1, \ldots, a_n \in \varphi(G)$ skalárok, amelyek nem mind 0-ák, és amelyekre

$$a_1\alpha_1 + \cdots + a_n\alpha_n = 0$$

teljesül.

Bizonyítás (folytatás).

(ii)$\Longrightarrow$(i), azaz ha $\{T_\alpha \mid \alpha \in A\}$ lineárisan független $\varphi(G)$ felett, akkor A is lineárisan független független $\varphi(G)$ felett.

Tegyük fel, hogy A nem lineárisan független $\varphi(G)$ felett. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_n \in A$ vektorok és $a_1, \ldots, a_n \in \varphi(G)$ skalárok, amelyek nem mind 0-ák, és amelyekre

$$a_1\alpha_1 + \cdots + a_n\alpha_n = 0$$

teljesül. Ekkor tetszőleges $\sigma \in G$-re

$$0 = \sigma(0) = \sigma(a_1\alpha_1 + \cdots + a_n\alpha_n) = a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_n),$$

azaz $a_1 T_{\alpha_1} + \cdots + a_n T_{\alpha_n} = 0$. Így a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer sem lineárisan független $\varphi(G)$ felett.

Bizonyítás (folytatás).

(i)$\Longrightarrow$(iii), azaz ha A lineárisan független $\varphi(G)$ felett, akkor a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer lineárisan független L felett.

Bizonyítás (folytatás).

(i)$\Longrightarrow$(iii), azaz ha A lineárisan független $\varphi(G)$ felett, akkor a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer lineárisan független L felett.

Bizonyítás (folytatás).

(i)$\Longrightarrow$(iii), azaz ha A lineárisan független $\varphi(G)$ felett, akkor a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer lineárisan független L felett.

Tegyük fel, hogy a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer nem lineárisan független L felett.

Bizonyítás (folytatás).

(i)$\Longrightarrow$(iii), azaz ha A lineárisan független $\varphi(G)$ felett, akkor a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer lineárisan független L felett.

Tegyük fel, hogy a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer nem lineárisan független L felett. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_n \in A$ vektorok és $a_1, \ldots, a_n \in L$ skalárok, amelyekre

$$a_1 T_{\alpha_1} + \cdots + a_n T_{\alpha_n} = 0. \tag{2}$$

teljesül.

Bizonyítás (folytatás).

(i)$\Longrightarrow$(iii), azaz ha A lineárisan független $\varphi(G)$ felett, akkor a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer lineárisan független L felett.

Tegyük fel, hogy a $\{T_\alpha \mid \alpha \in A\}$ vektorrendszer nem lineárisan független L felett. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_n \in A$ vektorok és $a_1, \ldots, a_n \in L$ skalárok, amelyekre

$$a_1 T_{\alpha_1} + \cdots + a_n T_{\alpha_n} = 0. \tag{2}$$

teljesül. Tegyük fel, hogy az $\alpha_1, \ldots, \alpha_n \in A$ és $a_1, \ldots, a_n \in L$ elemeket úgy választottuk meg, hogy n minimális.

Bizonyítás (folytatás).

A (2) formulából következik, hogy tetszőleges $\sigma \in G$-re

$$a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_n) = 0 \tag{3}$$

is fennáll, és így tetszőleges $\tau \in G$-re igaz az

$$a_1\tau^{-1}\sigma(\alpha_1) + \cdots + a_n\tau^{-1}\sigma(\alpha_n) = 0$$

egyenlőség. A τ automorfizmust az előbbi egyenlőség mindkét oldalára alkalmazva kapjuk, hogy a G csoport bármely σ elemére teljesül, hogy

$$\tau(a_1)\sigma(\alpha_1) + \cdots + \tau(a_n)\sigma(\alpha_n) = 0. \tag{4}$$

Bizonyítás (folytatás).

Szorozzuk meg a (2) egyenlőséget $\tau(a_n)$-nel, a (4) egyenlőséget pedig a_n-nel:

$$\tau(a_n)a_1\sigma(\alpha_1) + \cdots + \tau(a_n)a_n\sigma(\alpha_n) = 0,$$
$$a_n\tau(a_1)\sigma(\alpha_1) + \cdots + a_n\tau(a_n)\sigma(\alpha_n) = 0,$$

majd a kapott egyenlőségeket vonjuk ki egymásból. Ekkor azt kapjuk, hogy tetszőleges $g \in G$-re

$$\big(a_1\tau(a_n) - a_n\tau(a_1)\big)\sigma(\alpha_1) + \cdots + \big(a_{n-1}\tau(a_n) - a_n\tau(a_{n-1})\big)\sigma(\alpha_{n-1}) = 0$$

teljesül.

Bizonyítás (folytatás).

Azaz

$$\big(a_1\tau(a_n) - a_n\tau(a_1)\big)\,T_{\alpha_1} + \cdots + \big(a_{n-1}\tau(a_n) - a_n\tau(a_{n-1})\big)\,T_{\alpha_{n-1}} = 0.$$

Ekkor az n természetes szám minimalitása miatt azt kapjuk, hogy az $a_j\tau(a_n) - a_n\tau(a_j)$ elemek mindegyike 0 ($j = 1, \ldots, n$). Azaz $\tau(a_n^{-1}a_j) = a_n^{-1}a_j$ ($j = 1, \ldots, n$) teljesül bármely $\tau \in G$-re. Ez pedig azt jelenti, hogy $a_n^{-1}a_j \in \varphi(G)$ ($j = 1, \ldots, n$). A (3) egyenlőséget a_n^{-1}-gyel megszorozva, és $\sigma = \mathrm{id}_L \in G$-t helyettesítve kapjuk, hogy

$$(a_n^{-1}a_1)\alpha_1 + \cdots + (a_n^{-1}a_{n-1})\alpha_{n-1} + \alpha_n = 0,$$

azaz A nem lineárisan független $\varphi(G)$ felett. Ezzel a tételt igazoltuk.

Tétel.

Tegyük fel, hogy G véges részcsoportja $\mathrm{Aut}(L)$-nek. Ekkor $|G| = [L : \varphi(G)]$, $G = \gamma\varphi(G)$ és $L : \varphi(G)$ Galois-bővítés.

Tétel.

Tegyük fel, hogy G véges részcsoportja $\mathrm{Aut}(L)$-nek. Ekkor $|G| = [L : \varphi(G)]$, $G = \gamma\varphi(G)$ és $L : \varphi(G)$ Galois-bővítés.

Bizonyítás.

Ha $A \subseteq L$ lineárisan független részhalmaz $\varphi(G)$ felett, akkor az előző tétel szerint $\{T_\alpha \mid \alpha \in A\} \subseteq L^G$ lineárisan független L felett. Mivel $\dim(L^G) = |G|$, ezért $|A| \leqslant |G|$. Ez pedig azt mutatja, hogy az $L : \varphi(G)$ bővítés véges és $[L : \varphi(G)] \leqslant |G|$. Másrészt $|G| \leqslant |\gamma\varphi(G)| \leqslant [L : \varphi(G)]$ is teljesül, mivel $G \subseteq \gamma\varphi(G)$. A fentiekből már következnek a $|G| = [L : \varphi(G)]$ és $G = \gamma\varphi(G)$ egyenlőségek, és így $L : \varphi(G)$ Galois-bővítés.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges. Ha $L : K$ Galois-bővítés, akkor $|\gamma(K)| = [L : K]$ és $K = \varphi\gamma(K)$. Másrészt, ha az $L : K$ bővítés nem Galois-bővítés, akkor $|\gamma(K)| < [L : K]$ és K valódi részteste $\varphi\gamma(K)$-nek.

Tétel.

Tegyük fel, hogy az $L : K$ testbővítés véges. Ha $L : K$ Galois-bővítés, akkor $|\gamma(K)| = [L : K]$ és $K = \varphi\gamma(K)$. Másrészt, ha az $L : K$ bővítés nem Galois-bővítés, akkor $|\gamma(K)| < [L : K]$ és K valódi részteste $\varphi\gamma(K)$-nek.

Bizonyítás.

Az előző tétel szerint $|\gamma(K)| = [L : \varphi\gamma(K)]$. Mivel $L : K$ normális és szeparábilis, ezért $[L : K] = [L : \varphi\gamma(K)]$. Azonban $K \subseteq \varphi\gamma(K)$ is teljesül, így $K = \varphi\gamma(K)$. Különben $[L : \varphi\gamma(K)] < [L : K]$ áll fenn, azaz K valódi részteste $\varphi\gamma(K)$-nak.

A testbővítések elméletének legfontosabb célja a polinomok és felbontási testeiknek vizsgálata.

A testbővítések elméletének legfontosabb célja a polinomok és felbontási testeiknek vizsgálata.

Definíció: polinom Galois-csoportja.

Tegyük fel, hogy $f \in K[x]$ és L az f polinom felbontási teste a K számtest felett. Ekkor az $L : K$ testbővítés $\mathrm{Gal}(L : K)$ Galois-csoportját az f polinom Galois-csoportjának nevezzük, és $\mathrm{Gal}_K(f)$-val fogjuk jelölni.

A testbővítések elméletének legfontosabb célja a polinomok és felbontási testeiknek vizsgálata.

Definíció: polinom Galois-csoportja.

Tegyük fel, hogy $f \in K[x]$ és L az f polinom felbontási teste a K számtest felett. Ekkor az $L : K$ testbővítés $\mathrm{Gal}(L : K)$ Galois-csoportját az f polinom Galois-csoportjának nevezzük, és $\mathrm{Gal}_K(f)$-val fogjuk jelölni.

A $\mathrm{Gal}_K(f)$ csoport természetesen függ f-től és K-tól, de nem függ a felbontási test választásától.

Tétel.

Legyen L az $f \in K[x]$ polinom felbontási teste K felett. Ha f szeparábilis, akkor $|\mathrm{Gal}_K(f)| = [L : K]$ és $K = \varphi(\mathrm{Gal}_K(f))$; különben $|\mathrm{Gal}_K(f)| < [L : K]$ és K valódi részteste $\varphi(\mathrm{Gal}_K(f))$-nek.

A $\mathrm{Gal}_K(f)$ csoport egy tetszőleges σ eleme az L test automorfizmusa. Számunkra a legfontosabb az lesz, hogy σ hogyan hat az f polinom gyökeinek halmazán. A következő tétel szerint nem vesztünk információt, ha csak ezt a hatást vizsgáljuk.

A $\mathrm{Gal}_K(f)$ csoport egy tetszőleges σ eleme az L test automorfizmusa. Számunkra a legfontosabb az lesz, hogy σ hogyan hat az f polinom gyökeinek halmazán. A következő tétel szerint nem vesztünk információt, ha csak ezt a hatást vizsgáljuk.

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

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

leképezés injektív homomorfizmus.

Bizonyítás.

Legyen σ a $\mathrm{Gal}(K : L)$ csoport tetszőleges eleme. Ekkor $\sigma_f = f$, mivel $f \in K[x]$. Ha $\alpha \in L$ gyöke f-nek, akkor

$$f(\sigma(\alpha)) = \sigma(f(\alpha)) = \sigma(0) = 0,$$

azaz $\sigma(\alpha)$ is gyöke f-nek. Ez azt jelenti, hogy $\sigma(R) \subseteq R$. Ha azt is figyelembe veszzük, hogy σ bijektív és R véges, akkor azt kapjuk, hogy $\sigma(R) = R$. Így $\sigma|_R \in S_R$. A $\mathfrak{G}$ leképezés nyilván (csoport) homomorfizmus. Tegyük fel, hogy $\mathfrak{G}(\sigma) = \mathfrak{G}(\tau)$. Ekkor $\sigma|_R = \tau|_R$, és így $\tau^{-1}\sigma(a) = a$ teljesül tetszőleges $a \in K \cup R$-re. Mivel $L = K(R)$, ezért $\tau^{-1}\sigma = \mathrm{id}_L$, azaz $\mathfrak{G}$ injektív leképezés. Ezzel a bizonyítást befejeztük.

Ha f irreducibilis, akkor $\mathrm{Gal}_K(f)$ tarnzitívan 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 $\mathrm{Gal}_K(f)$ tarnzitívan 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 $\mathrm{Gal}_K(f)$ tarnzitívan 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 $\mathrm{Gal}_K(f)$ tarnzitívan 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 $\mathrm{Gal}_K(f)$ tarnzitívan 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 $f = km$ valamely $k \in K$-ra. Ezért f irreducibilis.

Automorfizmusok és fixtestek
Egy példa.

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

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

Automorfizmusok és fixtestek
Egy példa.

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

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

Automorfizmusok és fixtestek
Egy példa.

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 $y \sim z$. Ha $x = y$ vagy $y = z$, akkor $x \sim z$ nyilván teljesül. Tegyük fel, hogy $x \neq y$ és $y \neq z$, 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 $\sim$-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 $x = x'$ vagy $(x\,x') \in G$ teljesül. Így $x \neq x'$ esetén

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

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.

Automorfizmusok és fixtestek
Egy példa.

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 $G = S_X$.

Automorfizmusok és fixtestek
Egy példa.

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

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

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

$$\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_R \cong S_p.$$

Példa.

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

Példa.

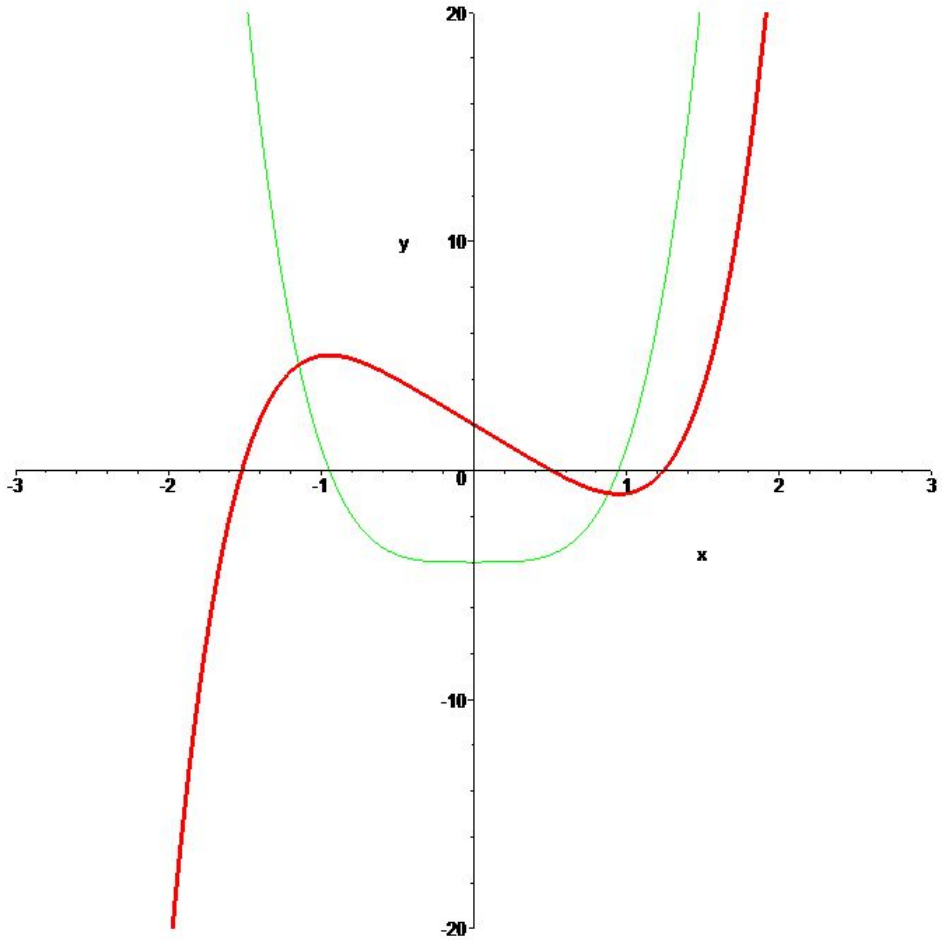
Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot.

Példa.

Tekintsük az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinomot. A Schönemann–Eisenstein-tétel szerint az f polinom irreducibilis és pontosan 3 darab valós gyöke van. Az előző tétel szerint $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_5$.

Automorfizmusok és fixtestek

Egy példa.



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