Galois-kapcsolatok

4.42. Definíció.

Az U halmazon értelmezett **lezárási operátoron** olyan $\mathcal{P}(U) \to \mathcal{P}(U)$, $A \mapsto \overline{A}$ leképezést értünk, amely rendelkezik az alábbi három tulajdonsággal:

(a) monoton: $A \subseteq B \implies \overline{A} \subseteq \overline{B}$ minden $A, B \subseteq U$ esetén;

(b) extenzív: $\overline{A} \supseteq A$ minden $A \subseteq U$ esetén;

(c) idempotens: $\overline{\overline{A}} = \overline{A}$ minden $A \subseteq U$ esetén.

Ha $\overline{A} = A$, akkor azt mondjuk, hogy A **zárt halmaz**.

4.43. Állítás.

Tetszőleges lezárási operátor esetén érvényesek az alábbiak (minden $A, B \subseteq U$ esetén):

(1) A zárt $\iff \exists B \subseteq U : A = \overline{B}$;

(2) A, B zárt $\implies A \cap B$ is zárt;

(3) $\overline{A \cup B}$ az a legszűkebb zárt halmaz, ami tartalmazza A-t és B-t;

(4) a zárt halmazok hálót alkotnak, amelyben $A \wedge B = A \cap B$ és $A \vee B = \overline{A \cup B}$.

4.44. Példa.

(1) Ha $\mathbb{A} = (A; F)$ egy algebra, akkor $\mathcal{P}(A) \to \mathcal{P}(A)$, $T \mapsto [T]$ lezárási operátor az A halmazon, és a zárt halmazok hálója nem más, mint $\mathbb{A}$ részalgebrahálója. Ennek a példának speciális esetei a részcsoporthálók, normálosztóhálók, részgyűrűhálók, ideálhálók, résztesthálók.

(2) Legyen U a sík (vagy a tér) pontjainak halmaza, és legyen $\overline{A}$ az A halmaz konvex burka. Ez egy lezárási operátor, amelynél a zárt halmazok éppen a konvex halmazok.

(3) A sík (vagy a tér) pontjainak halmazán a topológiai lezárás (torlódási pontok hozzávétele) is lezárási operátor; itt a zárt halmazok éppen a zárt halmazok(!).

Legyen adott objektumok egy G halmaza (németül Gegenstand) és tulajdonságok (attribútumok) egy M halmaza (németül Merkmal).

Minden $g \in G$ és $m \in M$ esetén meg van határozva, hogy g rendelkezik-e az m tulajdonsággal. Ezt egy $I \subseteq G \times M$ megfeleltetés írja le: $(g, m) \in I$ (vagy egyszerűbb jelöléssel gIm) akkor és csak akkor teljesül, ha g rendelkezik az m tulajdonsággal.

A (G, M, I) hármast **kontextusnak** nevezzük.

Példa.

$G = \{\mathtt{T}, \mathtt{K}, \mathtt{Ny}\}$, $M = \{\mathtt{f}, \mathtt{d}, \mathtt{g}, \mathtt{h}, \mathtt{l}\}$

	f	d	g	h	l
T		×		×	
K	×	×	×	×	
Ny	×			×	

Tetszőleges $X \subseteq G$ és $Y \subseteq M$ esetén legyen

$$X' = \alpha(X) = \{m \in M \mid \forall g \in X : gIm\} \subseteq M,$$
$$Y' = \beta(Y) = \{g \in G \mid \forall m \in Y : gIm\} \subseteq G.$$

Tehát $\alpha(X)$ mindazon tulajdonságok halmaza, amelyekkel X minden eleme rendelkezik, $\beta(Y)$ pedig mindazon objektumok halmaza, amelyek rendelkeznek az összes Y-beli tulajdonsággal.

Így definiáltunk

$$\alpha\colon \mathcal{P}(G) \to \mathcal{P}(M),\ X \mapsto X' \quad \text{és} \quad \beta\colon \mathcal{P}(M) \to \mathcal{P}(G),\ Y \mapsto Y'$$

leképezéseket; ezt a leképezéspárt nevezzük **Galois-kapcsolatnak**.

Példa.

$$\{\mathtt{T}\}' = \{\mathtt{d}, \mathtt{h}\}$$
$$\{\mathtt{K}, \mathtt{Ny}\}' = \{\mathtt{f}, \mathtt{h}\}$$
$$\{\mathtt{g}\}' = \{\mathtt{K}\}$$
$$\{\mathtt{f}, \mathtt{d}\}' = \{\mathtt{K}\}$$

4.45. Állítás.

Tetszőleges $X, X_1, X_2 \subseteq G$ és $Y, Y_1, Y_2 \subseteq M$ esetén teljesülnek az alábbiak:

(1) $X_1 \subseteq X_2 \implies X_1' \supseteq X_2'$ és $Y_1 \subseteq Y_2 \implies Y_1' \supseteq Y_2'$;

(2) $X'' \supseteq X$ és $Y'' \supseteq Y$;

(3) $X''' = X'$ és $Y''' = Y'$.

4.46. Következmény.

A „kettővessző" operátorok:

$$\mathcal{P}(G) \to \mathcal{P}(G),\ X \mapsto X'' \quad \text{és} \quad \mathcal{P}(M) \to \mathcal{P}(M),\ Y \mapsto Y'',$$

lezárási operátorok G-n illetve M-en.
A megfelelő zárt halmazokat **Galois-zárt** halmazoknak nevezzük.

4.47. Állítás.

Tetszőleges $X \subseteq G$ és $Y \subseteq M$ esetén

$$X \text{ Galois-zárt} \iff \exists Y \subseteq M\colon X = Y';$$

$$Y \text{ Galois-zárt} \iff \exists X \subseteq G\colon Y = X'.$$

Példa.

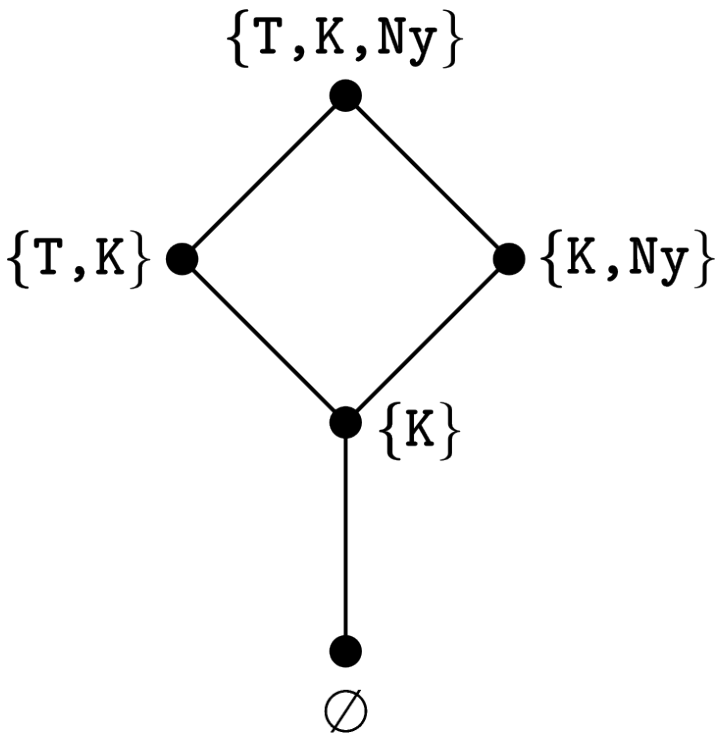
$$\{\mathtt{T}\} \text{ lezártja: } \{\mathtt{T}\}'' = \{\mathtt{d},\mathtt{h}\}' = \{\mathtt{T},\mathtt{K}\}$$

$$\{\mathtt{K},\mathtt{Ny}\} \text{ lezártja: } \{\mathtt{K},\mathtt{Ny}\}'' = \{\mathtt{f},\mathtt{h}\}' = \{\mathtt{K},\mathtt{Ny}\}$$

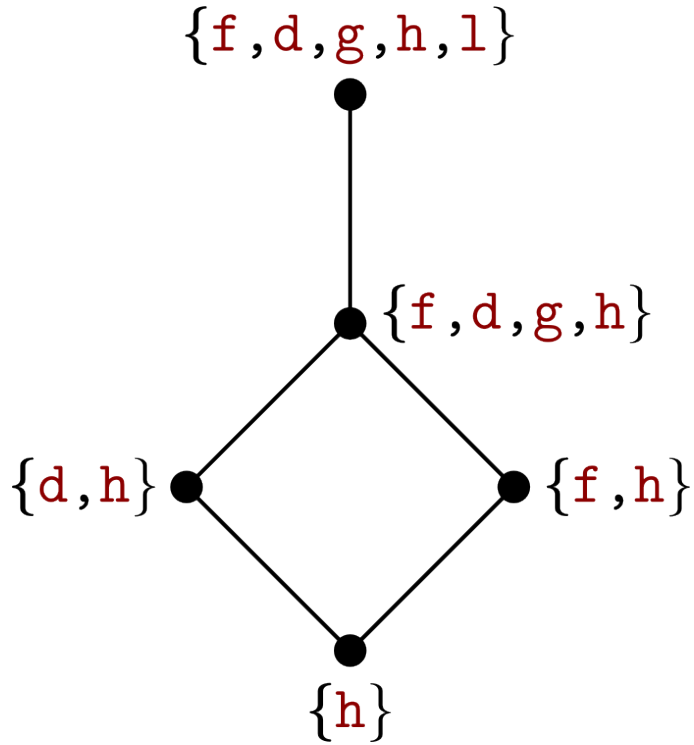
$$\{\mathtt{g}\} \text{ lezártja: } \{\mathtt{g}\}'' = \{\mathtt{K}\}' = \{\mathtt{f},\mathtt{d},\mathtt{g},\mathtt{h}\}$$

$$\{\mathtt{f},\mathtt{d}\} \text{ lezártja: } \{\mathtt{f},\mathtt{d}\}'' = \{\mathtt{K}\}' = \{\mathtt{f},\mathtt{d},\mathtt{g},\mathtt{h}\}$$

G zárt részhalmazainak hálója:



M zárt részhalmazainak hálója:



4.48. Tétel.

Legyen L_G a G halmaz Galois-zárt részhalmazainak hálója, L_M pedig az M halmaz Galois-zárt részhalmazainak hálója. Ekkor

$$\varphi\colon L_G \to L_M,\ X \mapsto X' \text{ és } \psi\colon L_M \to L_G,\ Y \mapsto Y'$$

rendezésfordító bijekciók (egymás inverzei).
Következésképp L_G izomorf L_M duálisával („fejreállítottjával").

4.49. Megjegyzés.

Mivel L_G és L_M duálisan izomorfak, lehet őket egy Hasse-diagramon ábrázolni úgy, hogy L_G Hasse-diagramjában az $X \in L_G$ halmazt jelképező ponthoz az (X, Y) címkét írjuk, ahol $Y = X'$ (ekkor persze $Y' = X$).

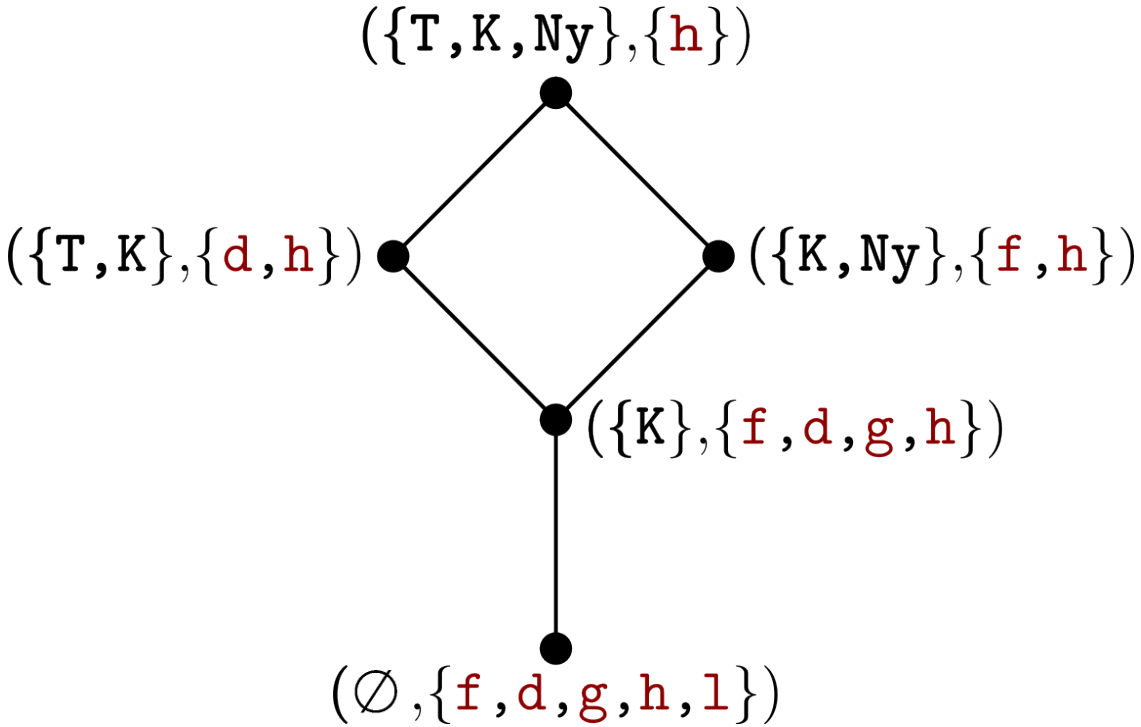
Az ilyen (X, Y) párt **fogalomnak** nevezzük; X a fogalom terjedelme (azon objektumok halmaza, amelyek az adott fogalomhoz tartoznak), Y pedig a fogalom tartalma (a fogalomra jellemző tulajdonságok összessége).

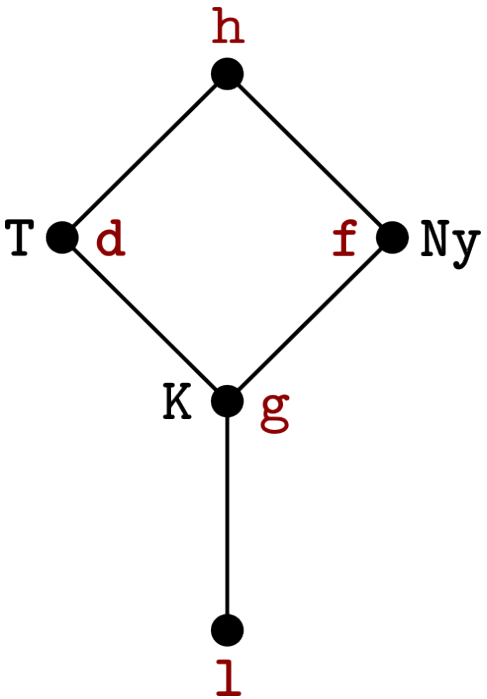
A fogalmak halmazán L_G-ből (és L_M duálisából) adódik rendezés:

$$(X_1, Y_1) \leq (X_2, Y_2) \iff X_1 \subseteq X_2 \,(\iff Y_1 \supseteq Y_2)\,;$$

így kapjuk a (G, M, I) kontextushoz tartozó **fogalomhálót**.

Példa.





4.50. Példa.

Legyen G rögzített típusú algebrák halmaza (pl. grupoidok), M pedig a típusnak megfelelő azonosságok halmaza, és jelentse I azt, hogy az adott algebra teljesíti az adott azonosságot. (Például $(\mathbb{Z}_6, xy = yx) \in I$ és $\left(V, x^2 = y^2\right) \in I$, de $(S_3, xy = yx) \notin I$.)

Ekkor egy X algebrahalmazra X' mindazon azonosságokat tartalmazza, amelyeket X minden eleme kielégít, egy Y azonossághalmaz esetén pedig Y' az Y-beli azonosságokat kielégítő összes algebrák halmaza. Például $\{(xy)\,z = x\,(yz)\,, xy = yx\}'$ a kommutatív félcsportok halmaza, $\{(xy)\,z = x\,(yz)\,, xy = yx\}''$ pedig az összes olyan azonosságot tartalmazza, ami teljesül minden kommutatív félcsoporton, vagyis az asszociativitás és a kommutativitás következményeit (pl. $(xy)\,(xz) = x\,(z\,(yx))$).

Könnyű belátni, hogy minden azonosság „öröklődik" részalgebrákra, faktoralgebrákra és direkt szorzatokra, tehát Y' mindig zárt erre a három konstrukcióra. Birkhoff tétele szerint ennek a megfordítása is igaz: ha egy X algebraosztály zárt a részalgebra, faktoralgebra és direkt szorzat képzésére, akkor definiálható azonosságokkal, azaz Galois-zárt (előáll $X = Y'$ alakban). Az ilyen algebraosztályokat nevezzük varietásoknak. Tehát ebben a kontextusban a zárt algebraosztályok éppen a varietások, a zárt azonossághalmazokat pedig bizonyos logikai dedukciós lépésekre való zártsággal lehet jellemezni (ezeket azonosság-elméleteknek nevezzük).

A Galois-elmélet azt a Galois-kapcsolatot vizsgálja, ahol az „egyik oldalon” egy test elemei vannak, a „másik oldalon” pedig a test automorfizmusai, és az „illeszkedés” azt jelenti, hogy az adott automorfizmus fixen hagyja az adott elemet.
A továbbiakban az egyszerűség kedvéért feltesszük, hogy minden szóba kerülő test számtest, és minden bővítés végesfokú.

4.51. Definíció.

Az $L \mid K$ testbővítés **Galois-csoportja** azon $L \to L$ automorfizmusok csoportja, melyek pontonként fixen hagyják K-t (vagyis az $L \mid K$ bővítést saját magára képező izomorfizmusok csoportja):

$$\mathrm{Gal}\,(L \mid K) = \mathrm{Aut}_K L = \{\sigma \colon L \to L \text{ izomorfizmus, } \sigma|_K = \mathrm{id}_K\}\,.$$

4.52. Definíció.

Az $L \mid K$ testbővítés **közbülső testein** olyan E testeket értünk, amelyekre $K \leq E \leq L$ teljesül. A közbülső testek halmazát $\mathrm{Sub}\,(L \mid K)$ jelöli.

Példa.

Legyen $K = \mathbb{Q}$ és $L = \mathbb{Q}(\vartheta)$, ahol $\vartheta = \sqrt[3]{2}$. Mivel $[L : K] = 3$ (prímszám), nincs L és K között más test: $\mathrm{Sub}\,(L \mid K) = \{K, L\}$.

Ha $\sigma \in \mathrm{Gal}\,(L \mid K)$, akkor $(\vartheta\sigma)^3 = (\vartheta^3)\,\sigma = 2\sigma = 2$ (mert $2 \in K$ és σ fixen hagyja K elemeit). Tehát $\vartheta\sigma = \sqrt[3]{2}$.

Az L test minden α eleme $\alpha = a + b\vartheta + c\vartheta^2$ $(a, b, c \in \mathbb{Q})$ alakban felírható. Számítsuk ki α képét σ mellett:

$$\alpha\sigma = \left(a + b\vartheta + c\vartheta^2\right)\sigma = a\sigma + b\sigma \cdot \vartheta\sigma + c\sigma \cdot (\vartheta\sigma)^2 = a + b \cdot \vartheta + c \cdot \vartheta^2 = \alpha.$$

Azt kaptuk, hogy $\sigma = \mathrm{id}_L$, vagyis $G = \mathrm{Gal}\,(L \mid K) = \{\mathrm{id}_L\}$.

A $\mathrm{Sub}\,(L \mid K)$ háló kételemű, a $\mathrm{Sub}\,(G)$ háló pedig egyelemű, tehát a két háló nem izomorf egymással. Ennek oka az, hogy az $L \mid K$ bővítés nem normális.

4.53. Tétel.

Tetszőleges $L \mid K$ végesfokú bővítés esetén ekvivalensek az alábbiak:

(1) Ha $f \in K[x]$ irreducibilis polinom és f-nek van gyöke L-ben, akkor f elsőfokú polinomok szorzatára bomlik L felett (azaz f „minden gyöke" L-ben van).

(2) Ha egy szám L-ben van, akkor minden konjugáltja is L-ben van (azaz L zárt a „konjugálásra").

(3) Van olyan K feletti polinom, amelynek felbontási teste éppen L.

4.54. Definíció.

A fenti ekvivalens tulajdonságokkal rendelkező testbővítéseket **normális bővítéseknek** nevezzük.

4.55. Állítás.

Minden $L \mid K$ testbővítés kiterjeszthető normális bővítéssé: létezik olyan $N \geq L$ test, amelyre $N \mid K$ normális bővítés. Az ilyen N testek között van egy legszűkebb; ezt nevezzük $L \mid K$ **normális lezártjának**.

4.56. Definíció.

Egy $f \in K[x]$ polinom **Galois-csoportján** a K feletti felbontási testének a Galois-csoportját értjük: $\mathrm{Gal}(f) = \mathrm{Gal}(N \mid K)$, ahol N az f polinom K feletti felbontási teste.

Titkos lemma.

Legyen $L \mid K$ egy testbővítés, $\alpha \in L$, $\sigma \in \mathrm{Gal}(L \mid K)$ és $f \in K[x]$. Ekkor

$$f(\alpha) = 0 \implies f(\alpha\sigma) = 0.$$

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ $(a_i \in K)$, és tegyük fel, hogy $f(\alpha) = 0$.

$$\begin{aligned}
f(\alpha\sigma) &= a_n \cdot (\alpha\sigma)^n + \cdots + a_1 \cdot (\alpha\sigma) + a_0 \\
&= a_n\sigma \cdot (\alpha\sigma)^n + \cdots + a_1\sigma \cdot (\alpha\sigma) + a_0\sigma && (\text{mert } \sigma|_K = \mathrm{id}_K) \\
&= (a_n\alpha^n)\,\sigma + \cdots + (a_1\alpha)\,\sigma + a_0\sigma && (\text{mert } \sigma \text{ felcserélhető a } \cdot\text{-sal}) \\
&= (a_n\alpha^n + \cdots + a_1\alpha + a_0)\,\sigma && (\text{mert } \sigma \text{ felcserélhető az } +\text{-sal}) \\
&= f(\alpha)\,\sigma \\
&= 0\sigma && (\text{mert feltettük, hogy } f(\alpha) = 0) \\
&= 0
\end{aligned}$$

□

4.57. Tétel.

Tetszőleges $N \mid K$ normális bővítés és $\alpha, \beta \in N$ esetén α és β akkor és csak akkor vannak a $\mathrm{Gal}(N \mid K)$ csoport hatása szerint ugyanazon a pályán, ha egymás konjugáltjai K felett:

$$\exists \sigma \in \mathrm{Gal}(N \mid K) : \alpha\sigma = \beta \iff m_{\alpha,K} = m_{\beta,K}.$$

Bizonyítás.

$\Longrightarrow$: Tfh. $\alpha\sigma = \beta$ valamely $\sigma \in \mathrm{Gal}(N \mid K)$ automorfizmusra. Alkalmazzuk a titkos lemmát az $f = m_{\alpha,K}$ polinomra:

$$f(\alpha) = 0 \implies f(\beta) = 0 \overset{f \text{ irr.}}{\implies} m_{\beta,K} = f.$$

$\Longleftarrow$: Tfh. $m_{\alpha,K} = m_{\beta,K} =: m$. Minden egyszerű algebrai bővítést egyértelműen meghatároz (izomorfia erejéig) az adjungált elem minimálpolinomja (4.8. Tétel):

$$K(\alpha) \mid K \cong K[x] / \langle m \rangle \cong K(\beta) \mid K,$$

ezért létezik olyan $\varphi\colon K(\alpha) \to K(\beta)$ izomorfizmus, amelyre $\varphi|_K = \mathrm{id}_K$ és $\alpha\varphi = \beta$. A felbontási test unicitásáról szóló tétel (4.19. Tétel második fele) egy általánosítását használva φ kiterjeszthető egy $\sigma\colon N \to N$ izomorfizmussá. □

4.58. Tétel.

Normális bővítés Galois-csoportjának rendje megegyezik a bővítés fokszámával: ha $N \mid K$ normális bővítés, akkor $|\mathrm{Gal}(N \mid K)| = [N : K]$.

Bizonyítás.

Legyen $[N : K] = n$, és legyen $\vartheta \in N$ egy primitív elem (4.11. Tétel): $N = K(\vartheta)$. Ekkor $m_{\vartheta,K} = (x - \vartheta_1) \cdot \ldots \cdot (x - \vartheta_n)$ alkalmas $\vartheta = \vartheta_1, \ldots, \vartheta_n$ komplex számokra. Mivel $N \mid K$ normális, $\vartheta_1, \ldots, \vartheta_n \in N$, és így $K(\vartheta_i) \subseteq N$, sőt $K(\vartheta_i) = N$, hiszen

$$[K(\vartheta_i) : K] = \deg m_{\vartheta_i,K} = \deg m_{\vartheta,K} = n = [N : K].$$

Az egyszerű algebrai bővítéseket leíró 4.8. Tételt alkalmazva minden i-re kapunk egy $\sigma_i \in \mathrm{Gal}(N \mid K)$ automorfizmust:

$$\begin{array}{rccc} \sigma_i: & K(\vartheta) & \longrightarrow & K(\vartheta_i), \\ & a_0 + a_1\vartheta + \cdots + a_{n-1}\vartheta^{n-1} & \mapsto & a_0 + a_1\vartheta_i + \cdots + a_{n-1}\vartheta_i^{n-1} \quad (a_i \in K). \end{array}$$

Másrészt, a titkos lemma szerint minden $\sigma \in \mathrm{Gal}(N \mid K)$ automorfizmus ϑ-t az $m_{\vartheta,K}$ polinom egy gyökébe viszi, azaz $\vartheta\sigma = \vartheta_i$ valamely i-re. Ez az információ, és az, hogy $\sigma|_K = \mathrm{id}_K$, már egyértelműen meghatározza σ-t: σ nem lehet más, mint a fenti σ_i automorfizmus. Ezzel beláttuk, hogy $\mathrm{Gal}(N \mid K) = \{\sigma_1, \ldots, \sigma_n\}$. □

4.59. Tétel.

Legyen az n-edfokú $f \in K[x]$ polinom felbontási teste N, gyökeinek halmaza pedig Gy. Tegyül fel, hogy f minden gyöke egyszeres (vagyis $|Gy| = n$).
Ekkor minden $\sigma \in \mathrm{Gal}(N \mid K)$ esetén $Gy\sigma = Gy$, így van értelme megszorítani a σ automorfizmust a Gy halmazra. A

$$\varphi\colon\ \mathrm{Gal}(N \mid K) \to S_{Gy},\ \sigma \mapsto \sigma|_{Gy}$$

leképezés beágyazza a $\mathrm{Gal}(N \mid K)$ csoportot az S_{Gy} csoportba, azaz $\mathrm{Gal}(f)$ izomorf S_n egy részcsoportjával.

Bizonyítás.

A titkos lemmából rögtön adódik, hogy $Gy\sigma \subseteq Gy$ minden $\sigma \in \mathrm{Gal}(N \mid K)$ esetén. Mivel Gy véges halmaz és σ bijektív, ezért $Gy\sigma = Gy$. Így megszoríthatjuk σ-t a Gy halmazra. Az világos, hogy a megszorítás felcserélhető a leképezésszorzással: $(\sigma\tau)|_{Gy} = \sigma|_{Gy}\tau|_{Gy}$, vagyis φ homomorfizmus.

Az injektivitáshoz tegyük fel, hogy $\sigma|_{Gy} = \tau|_{Gy}$ $\quad(\sigma, \tau \in \mathrm{Gal}(N \mid K))$.
A Galois-csoport definíciója szerint $\sigma|_K = \tau|_K = \mathrm{id}_K$, tehát σ és τ megegyeznek a $K \cup Gy$ halmazon. Ez a halmaz generálja az N testet (a felbontási test definíciója szerint), így σ és τ az egész N testen megyezik, azaz $\sigma = \tau$.

Ezzel beláttuk, hogy φ beágyazza a $\mathrm{Gal}(N \mid K)$ csoportot az S_{Gy} csoportba.
Mivel $|Gy| = n$, az S_{Gy} csoport izomorf az S_n csoporttal. □

Példa.

Határozzuk meg az $x^3 - 2 \in \mathbb{Q}[x]$ polinom Galois-csoportját. Szereposztás:

- $K = \mathbb{Q}$,
- $Gy = \left\{ \sqrt[3]{2},\ \sqrt[3]{2}\varepsilon,\ \sqrt[3]{2}\varepsilon^2 \right\}$, ahol $\varepsilon = \operatorname{cis} \frac{2\pi}{3}$,
- $N = K(Gy) = K\left(\sqrt[3]{2}, \varepsilon\right)$,
- $[N : K] = 6$.

Az előző két tétel szerint a $G := \operatorname{Gal}(f)$ csoport izomorf S_3 egy 6-elemű részcsoportjával, tehát $G \cong S_3$.

Bármely $\sigma \in G$ automorfizmust egyértelműen meghatározza $\sqrt[3]{2}$ és ε képe. A titkos lemma szerint $\sqrt[3]{2}\sigma$ gyöke az $x^3 - 2$ polinomnak, $\varepsilon\sigma$ pedig gyöke az $x^2 + x + 1$ polinomnak, ezért $\sqrt[3]{2}\sigma \in \left\{ \sqrt[3]{2},\ \sqrt[3]{2}\varepsilon,\ \sqrt[3]{2}\varepsilon^2 \right\}$ és $\varepsilon\sigma \in \left\{ \varepsilon, \varepsilon^2 \right\}$. Így $3 \cdot 2 = 6$ esetet kapunk; foglaljuk ezeket egy táblázatba:

$\sqrt[3]{2}\sigma$	$\sqrt[3]{2}$	$\sqrt[3]{2}\varepsilon$	$\sqrt[3]{2}\varepsilon^2$	$\sqrt[3]{2}$	$\sqrt[3]{2}\varepsilon$	$\sqrt[3]{2}\varepsilon^2$
$\varepsilon\sigma$	ε	ε	ε	ε^2	ε^2	ε^2
	σ_1	σ_2	σ_3	σ_4	σ_5	σ_6

Tehát $G \subseteq \{\sigma_1, \ldots, \sigma_6\}$, és tudjuk, hogy $|G| = 6$, így $G = \{\sigma_1, \ldots, \sigma_6\}$.

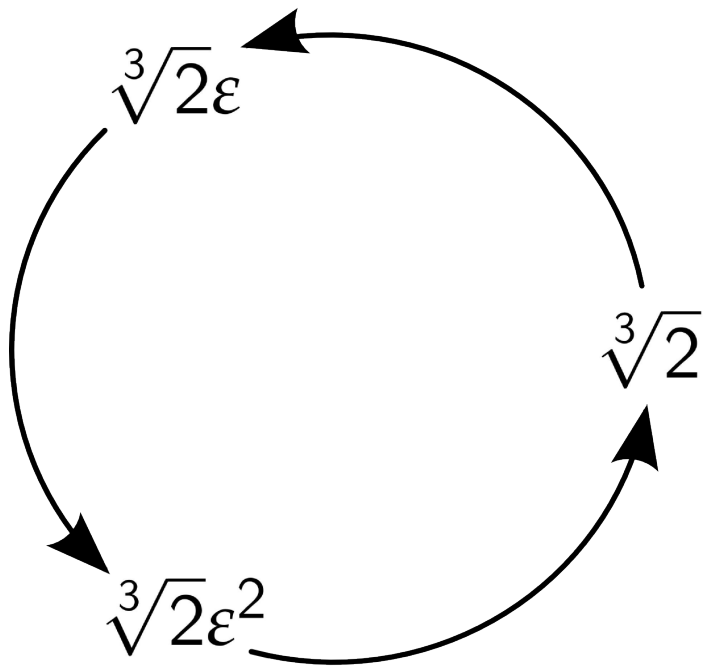
Nézzük, hogyan permutálja σ_2 a Gy halmaz elemeit:

$$\sqrt[3]{2}\sigma_2 = \sqrt[3]{2}\varepsilon$$

$$(\sqrt[3]{2}\varepsilon)\sigma_2 = \sqrt[3]{2}\sigma_2 \cdot \varepsilon\sigma_2 = \sqrt[3]{2}\varepsilon \cdot \varepsilon = \sqrt[3]{2}\varepsilon^2$$

$$(\sqrt[3]{2}\varepsilon^2)\sigma_2 = \sqrt[3]{2}\sigma_2 \cdot \varepsilon\sigma_2 \cdot \varepsilon\sigma_2 = \sqrt[3]{2}\varepsilon \cdot \varepsilon \cdot \varepsilon = \sqrt[3]{2}\varepsilon^3 = \sqrt[3]{2}$$

Tehát $\sigma_2|_{Gy}$ egy három hosszúságú ciklus:



A Galois-csoport többi elemének megfelelő S_{Gy}-beli permutáció hasonlóan felírható.

Ha a $\sqrt[3]{2} \rightsquigarrow 1$, $\sqrt[3]{2}\varepsilon \rightsquigarrow 2$, $\sqrt[3]{2}\varepsilon^2 \rightsquigarrow 3$ átnevezést használjuk, akkor a Galois-csoport elemeinek az alábbi S_3-beli permutációk felelnek meg (HF):

$\sigma_1 \rightsquigarrow \mathrm{id}$

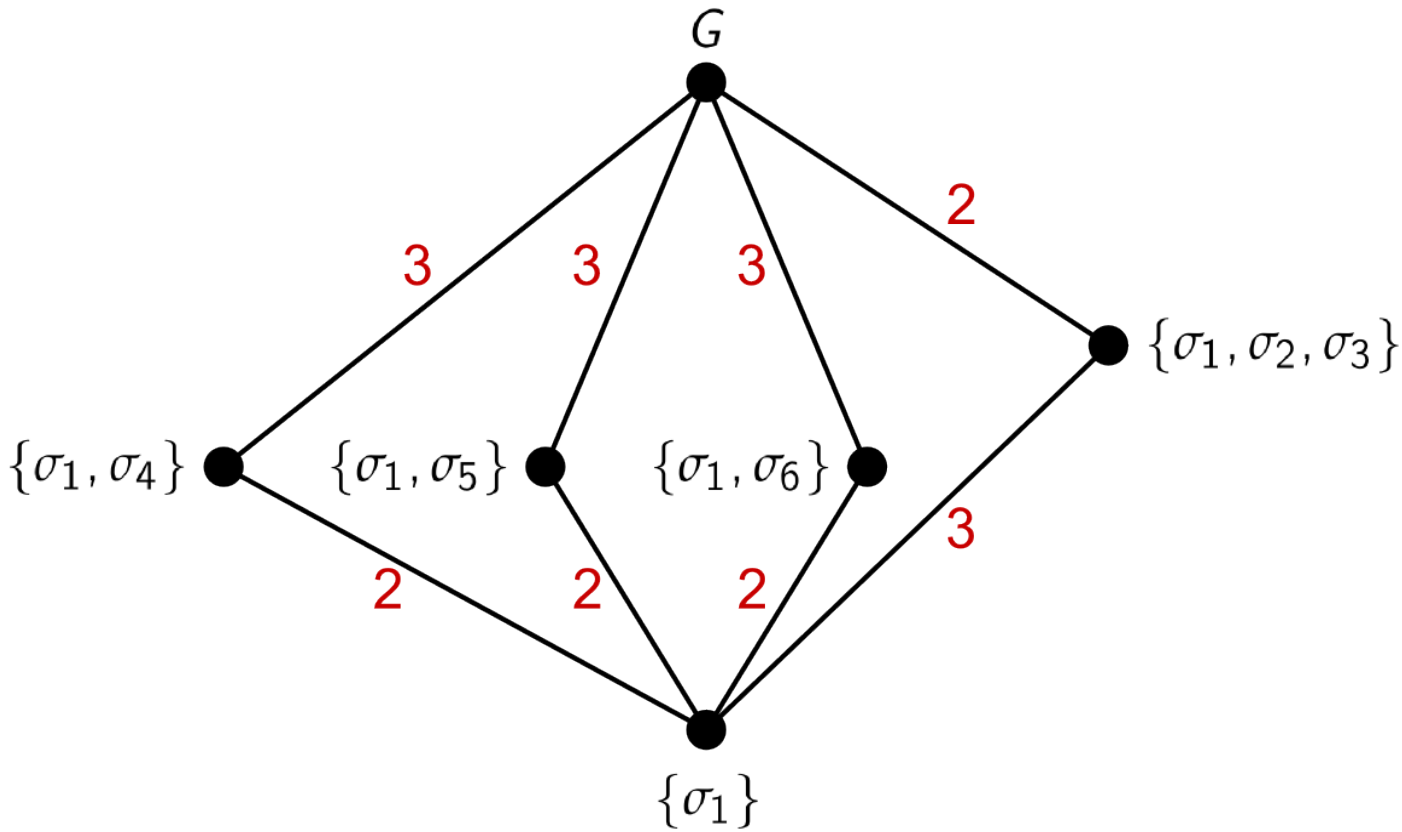
$\sigma_2 \rightsquigarrow (123)$

$\sigma_3 \rightsquigarrow (132)$

$\sigma_4 \rightsquigarrow (23)$

$\sigma_5 \rightsquigarrow (12)$

$\sigma_6 \rightsquigarrow (13)$



$\mathrm{Sub}\,(G)$

Az ${}_K N$ vektortér egy bázisa $1, \sqrt[3]{2}, \sqrt[3]{4}, \varepsilon, \sqrt[3]{2}\varepsilon, \sqrt[3]{4}\varepsilon$, tehát N minden α eleme egyértelműen felírható

$$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\varepsilon + e\sqrt[3]{2}\varepsilon + f\sqrt[3]{4}\varepsilon \quad (a, b, c, d, e, f \in \mathbb{Q})$$

alakban. Nézzük σ_2 hatását a bázis elemein:

$$1\sigma_2 = 1$$

$$\sqrt[3]{2}\sigma_2 = \sqrt[3]{2}\varepsilon$$

$$\sqrt[3]{4}\sigma_2 = \sqrt[3]{2}\sigma_2 \cdot \sqrt[3]{2}\sigma_2 = \sqrt[3]{2}\varepsilon \cdot \sqrt[3]{2}\varepsilon = \sqrt[3]{4}\varepsilon^2 = \sqrt[3]{4}(-\varepsilon - 1) = -\sqrt[3]{4} - \sqrt[3]{4}\varepsilon$$

$$\varepsilon\sigma_2 = \varepsilon$$

$$(\sqrt[3]{2}\varepsilon)\sigma_2 = \sqrt[3]{2}\sigma_2 \cdot \varepsilon\sigma_2 = \sqrt[3]{2}\varepsilon \cdot \varepsilon = \sqrt[3]{2}\varepsilon^2 = \sqrt[3]{2}(-\varepsilon - 1) = -\sqrt[3]{2} - \sqrt[3]{2}\varepsilon$$

$$(\sqrt[3]{4}\varepsilon)\sigma_2 = \sqrt[3]{4}\sigma_2 \cdot \varepsilon\sigma_2 = \sqrt[3]{4}\varepsilon^2 \cdot \varepsilon = \sqrt[3]{4}\varepsilon^3 = \sqrt[3]{4}$$

Ezután már ki tudjuk számítani a fenti α elem képét σ_2 mellett:

$$\begin{aligned}
\alpha\sigma_2 &= a\sigma_2 + b\sigma_2 \cdot \sqrt[3]{2}\sigma_2 + c\sigma_2 \cdot \sqrt[3]{4}\sigma_2 + d\sigma_2 \cdot \varepsilon\sigma_2 + e\sigma_2 \cdot (\sqrt[3]{2}\varepsilon)\sigma_2 + f\sigma_2 \cdot (\sqrt[3]{4}\varepsilon)\sigma_2 \\
&= a + b \cdot \sqrt[3]{2}\sigma_2 + c \cdot \sqrt[3]{4}\sigma_2 + d \cdot \varepsilon\sigma_2 + e \cdot (\sqrt[3]{2}\varepsilon)\sigma_2 + f \cdot (\sqrt[3]{4}\varepsilon)\sigma_2 \\
&= a + b \cdot \sqrt[3]{2}\varepsilon + c \cdot (-\sqrt[3]{4} - \sqrt[3]{4}\varepsilon) + d \cdot \varepsilon + e \cdot (-\sqrt[3]{2} - \sqrt[3]{2}\varepsilon) + f \cdot \sqrt[3]{4} \\
&= a - e \cdot \sqrt[3]{2} + (f - c)\sqrt[3]{4} + d\varepsilon + (b - e)\sqrt[3]{2}\varepsilon - c\sqrt[3]{4}\varepsilon
\end{aligned}$$

4.60. Tétel (a Galois-elmélet főtétele).

Legyen $N \mid K$ normális testbővítés és $G = \operatorname{Gal}(N \mid K) = \operatorname{Aut}_K N$. Tekintsük az $I = \{(\alpha, \sigma) : \alpha\sigma = \alpha\} \subseteq N \times G$ „illeszkedési reláció" által indukált Galois-kapcsolatot:

$$\mathcal{P}(N) \to \mathcal{P}(G), \quad E \mapsto \{\sigma \in G \mid \forall \alpha \in E : \alpha\sigma = \alpha\} = E' = \operatorname{Gal}(N \mid E);$$
$$\mathcal{P}(G) \to \mathcal{P}(N), \quad H \mapsto \{\alpha \in N \mid \forall \sigma \in H : \alpha\sigma = \alpha\} = H' = \operatorname{Fix}(H).$$

Ekkor teljesülnek az alábbiak:

(I) $\forall E \subseteq N: \; E'' = E \iff K \leq E \leq N$ (azaz $E \in \operatorname{Sub}(N \mid K)$).

(II) $\forall H \subseteq G: \; H'' = H \iff H \leq G$ (azaz $H \in \operatorname{Sub} G$).

(III) A $\operatorname{Sub}(N \mid K)$ és $\operatorname{Sub} G$ hálók között duális izomorfizmust létesítenek az

$$E \mapsto E' = \operatorname{Gal}(N \mid E) \quad \text{és} \quad H \mapsto H' = \operatorname{Fix}(H)$$

leképezések (amelyek egymás inverzei).

(IV) Ha $E \in \operatorname{Sub}(N \mid K)$ és $H \in \operatorname{Sub} G$ egymásnak megfelelő résztest és részcsoport, azaz $E = H' = \operatorname{Fix}(H)$ és $H = E' = \operatorname{Gal}(N \mid E)$, akkor

- (a) $[N : E] = |H|$ és $[E : K] = [G : H]$;
- (b) $N \mid E$ normális;
- (c) $E \mid K$ normális $\iff H \lhd G$, és ha ez teljesül, akkor $\operatorname{Gal}(E \mid K) \cong G/H$, azaz

$$\operatorname{Gal}(E \mid K) \cong \operatorname{Gal}(N \mid K) \,/\, \operatorname{Gal}(N \mid E).$$

Példa.

Határozzuk meg a $[\sigma_2] \leq G = \mathrm{Gal}\left(x^3 - 2\right)$ részcsoporthoz tartozó közbülső testet. Ha

$$\alpha = a + b\sqrt[3]{2} + c\sqrt[3]{4} + d\varepsilon + e\sqrt[3]{2}\varepsilon + f\sqrt[3]{4}\varepsilon \ \ (a, b, c, d, e, f \in \mathbb{Q}),$$

akkor

$$\alpha\sigma_2 = a - e \cdot \sqrt[3]{2} + (f - c)\sqrt[3]{4} + d\varepsilon + (b - e)\sqrt[3]{2}\varepsilon - c\sqrt[3]{4}\varepsilon,$$

tehát $\alpha\sigma_2 = \alpha$ akkor és csak akkor teljesül, ha

$$b = -e, \quad c = f - c, \quad e = b - e, \quad f = -c.$$

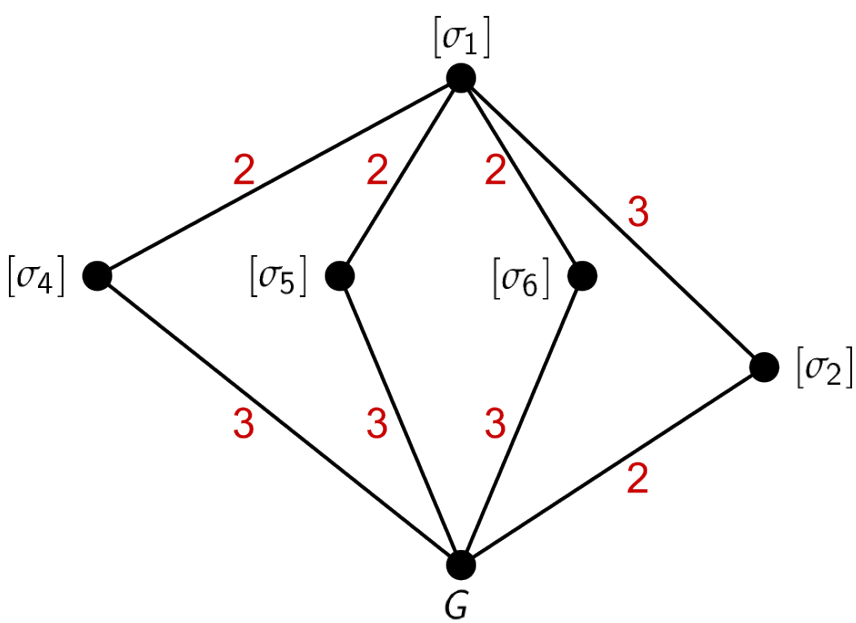
Ez azzal ekvivalens, hogy $b = c = e = f = 0$, tehát

$$\mathrm{Fix}\left([\sigma_2]\right) = \mathrm{Fix}\left(\sigma_2\right) = \left\{a + d\varepsilon : a, d \in \mathbb{Q}\right\} = \mathbb{Q}\left(\varepsilon\right).$$

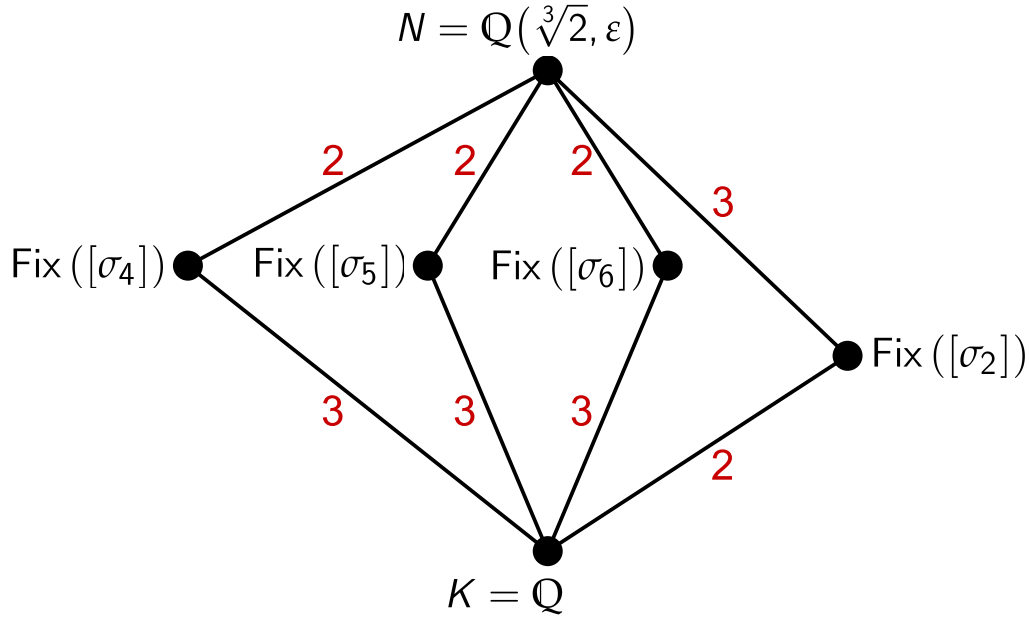
A Galois-elmélet főtételét használva kevesebb számolással is megkaphattuk volna ugyanezt: Az világos, hogy $\varepsilon \in \mathrm{Fix}\left([\sigma_2]\right)$, és így $\mathbb{Q}\left(\varepsilon\right) \subseteq \mathrm{Fix}\left([\sigma_2]\right)$.

Másrészt, a főtételből következik, hogy $\left[\mathrm{Fix}\left([\sigma_2]\right) : \mathbb{Q}\right] = \left[G : [\sigma_2]\right] = 2$.
Mivel $\left[\mathbb{Q}\left(\varepsilon\right) : \mathbb{Q}\right] = 2$ (hiszen $m_{\varepsilon,\mathbb{Q}} = x^2 + x + 1$), látjuk, hogy $\mathbb{Q}\left(\varepsilon\right) = \mathrm{Fix}\left([\sigma_2]\right)$.

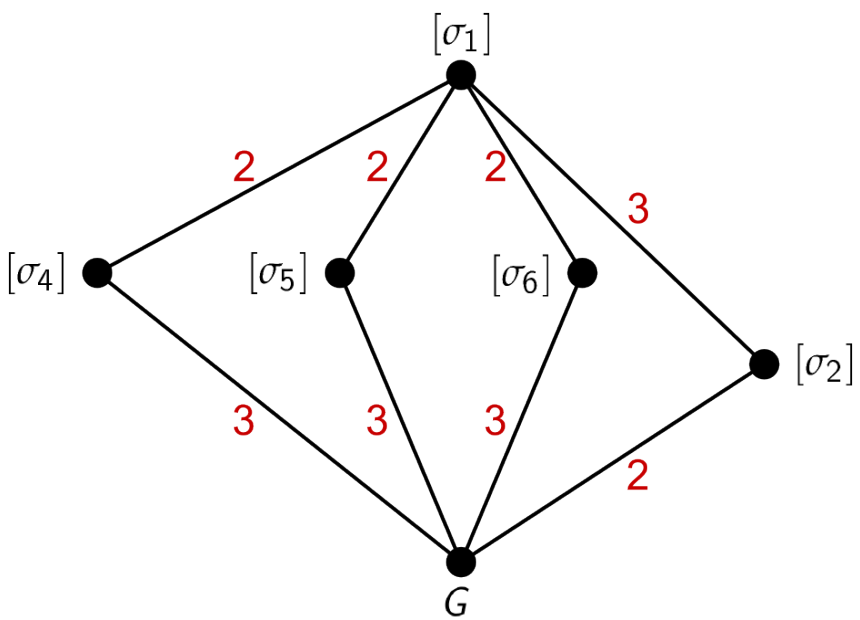
$\mathrm{Sub}\,(G)^d$



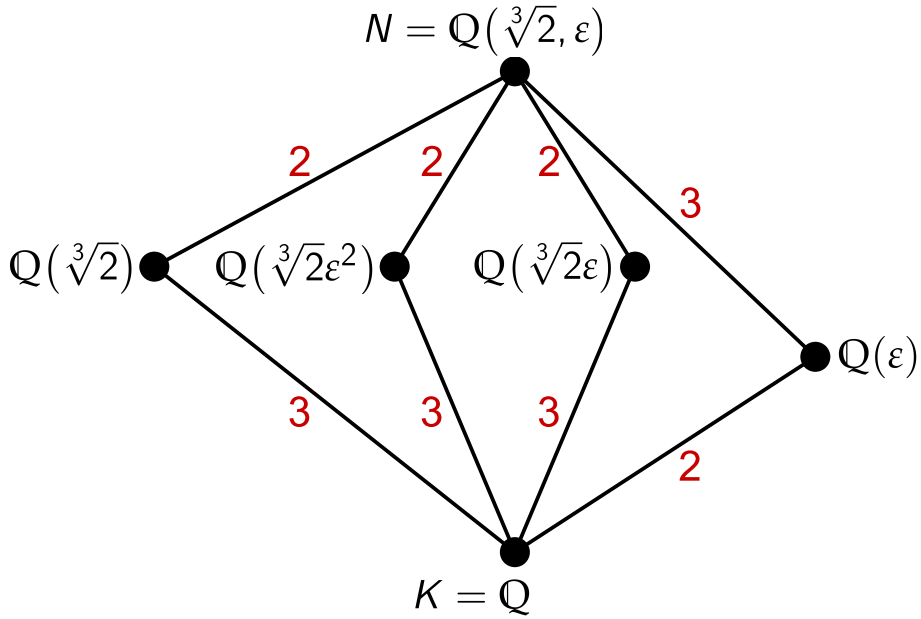
$\mathrm{Sub}\,(N \mid K)$



$\mathrm{Sub}\,(G)^d$



$\mathrm{Sub}\,(N \mid K)$



4.61. Definíció.

Az α komplex számot K feletti **gyökmennyiségnek** nevezzük, ha α megkapható K elemeiből a négy alapművelet és pozitív egész kitevős gyökvonások véges számú alkalmazásával.

4.62. Definíció.

Az $L \mid K$ testbővítés **egyszerű radikálbővítés**, ha $L = K\left(\sqrt[n]{a}\right)$ valamely $a \in K$ elemre és n természetes számra. Az $L \mid K$ testbővítés **radikálbővítés**, ha megkapható véges sok egyszerű radikálbővítés egymásutánjaként:

$$K = T_0 \leq T_1 \leq \cdots \leq T_\ell = L, \text{ ahol } T_{i+1} = T_i\left(\sqrt[n_i]{a_i}\right) \text{ és } a_i \in T_i,\ n_i \in \mathbb{N}.$$

4.63. Tétel.

Tetszőleges α komplex számra az alábbiak ekvivalensek:

(1) α gyökmennyiség K felett;

(2) α benne van K valamely radikálbővítésében;

(3) α benne van K valamely normális radikálbővítésében.

4.64. Következmény.

Ha α gyökmennyiség K felett, akkor α algebrai K felett.

Példa.

Ez a szám gyökmennyiség, és így algebrai $\mathbb{Q}$ felett:

$$\frac{\sqrt[3]{3-\sqrt{\sqrt[4]{2}+\sqrt[5]{\frac{3}{17}}}}+\sqrt[17]{323-\sqrt{2014}}}{\sqrt{2}+\sqrt[3]{3}+\sqrt[5]{5}}.$$

4.65. Definíció.

A G csoport **feloldható**, ha létezik olyan $\{1\} = G_0 \lhd G_1 \lhd \cdots \lhd G_{\ell-1} \lhd G_\ell = G$ *normállánc*, amelynek minden G_{i+1}/G_i faktora Abel-csoport.

4.66. Példa.

Minden Abel-csoport feloldható. A diédercsoportok, valamint az S_3 és S_4 szimmetrikus csoportok feloldhatóak, de $n \geq 5$ esetén S_n már nem feloldható.

4.67. Tétel.

Tetszőleges $f \in K[x]$ polinomra ekvivalensek az alábbiak:

(1) f-nek van olyan gyöke, ami gyökmennyiség K felett;

(2) f minden gyöke gyökmennyiség K felett;

(3) f Galois-csoportja feloldható.

4.68. Tétel.

Az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinom Galois-csoportja S_5. Következésképp f gyökei nem gyökmennyiségek $\mathbb{Q}$ felett (vagyis az $x^5 - 4x + 2 = 0$ egyenlet „nem oldható meg gyökjelekkel”).

4.69. Tétel (Ruffini–Abel-tétel).

Az általános n-edfokú egyenletnek nincs megoldóképlete, azaz nem létezik olyan, az $a_{n-1}, \ldots, a_1, a_0$ szimbólumokból a négy alapművelet és gyökvonások véges számú alkalmazásával felírható képlet, ami minden $a_{n-1}, \ldots, a_1, a_0 \in \mathbb{C}$ komplex értékekre az $x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 = 0$ egyenlet egy megoldását adja.

4.70. Tétel (a casus irreducibilis tétele).

Ha az $f \in \mathbb{Q}[x]$ polinom irreducibilis $\mathbb{Q}$ felett és minden gyöke valós, akkor f gyökei nem fejezhetőek ki $\mathbb{Q}$ feletti *valós* gyökkifejezéssel (azaz nem létezik olyan $L \mid \mathbb{Q}$ radikálbővítés, ami tartalmazza f egyik (minden) gyökét, és $L \subseteq \mathbb{R}$).