# Magasabb fokú egyenletek és geometriai szerkeszthetőség

2009/2010. őszi félév

# Jelölések

**Halmazok, számhalmazok**

$P(X)$ $\rightsquigarrow$ az $X$ halmaz részhalmazainak halmaza, azaz az $X$ halmaz **hatványhalmaza**

$\mathbb{N}$ $\rightsquigarrow$ a természetes számok halmaza, $\mathbb{N} = \{1, 2, \dots\}$

$\mathbb{Z}$ $\rightsquigarrow$ az egész számok halmaza, $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$

$\mathbb{Q}$ $\rightsquigarrow$ a racionális számok halmaza

$\mathbb{R}$ $\rightsquigarrow$ a valós számok halmaza

$\mathbb{C}$ $\rightsquigarrow$ a komplex számok halmaza

$\mathbb{A}$ $\rightsquigarrow$ a racionális számtest felett algebrai komplex számok halmaza

**Relációk**

$0_A$ $\rightsquigarrow$ $\{(a, a) \mid a \in A\}$ — az egyenlőségreláció az $A$ halmazon

$1_A$ $\rightsquigarrow$ $A \times A$ — a teljesreláció az $A$ halmazon

**Mátrixok**

$K^{n\times n}$ $\rightsquigarrow$ a $K$ test feletti $n \times n$-es **mátrix**ok halmaza

$\det(A)$ $\rightsquigarrow$ az $A$ négyzetes mátrix **determináns**a

$A^T$ $\rightsquigarrow$ az $A$ mátrix **transzponált**ja

$\mathfrak{V}(\alpha_1, \dots, \alpha_n)$ $\rightsquigarrow$ az $\alpha_1, \dots, \alpha_n$ elemekhez tartozó **Vandermonde-mátrix**

$V(\alpha_1, \dots, \alpha_n)$ $\rightsquigarrow$ az $\alpha_1, \dots, \alpha_n$ elemekhez tartozó **Vandermonde-determináns**

**Csoportok, permutációcsoportok**

$\langle X \rangle$ $\rightsquigarrow$ a $\mathbb{G}$ csoport $X \subseteq G$ részhalmaz által generált részcsoportja

$S_H$ $\rightsquigarrow$ a **szimmetrikus csoport** a $H$ halmazon[1]

$A_H$ $\rightsquigarrow$ az **alternáló csoport** a $H$ halmazon[2]

$D_n$ $\rightsquigarrow$ az $n$-edfokú **diédercsoport**

$Q_8$ $\rightsquigarrow$ a **kvaterniócsoport**

$[G, G]$ $\rightsquigarrow$ a $G$ csoport **kommutátor részcsoport**ja

$\mathbb{A} \hookrightarrow \mathbb{B}$ $\rightsquigarrow$ injektív homomorfizmus $\mathbb{A}$-ból $\mathbb{B}$-be.

**Polinomok**

$K[x]$ $\rightsquigarrow$ a $K$ test feletti $x$-határozatlanú **polinomgyűrű**

$f^*$ $\rightsquigarrow$ az $f \in K[x]$ **polinom fokszáma**

$K(x)$ $\rightsquigarrow$ az $x$ határozatlan **racionális kifejezés**einek halmaza a $K$ test felett, azaz $Q_{K[x]}$

$D_x(f)$ $\rightsquigarrow$ az $f$ polinom $x$ határozatlan szerinti **formális deriváltj**a

**Gyűrűk, testek és vektorterek**

$a \sim b$ $\rightsquigarrow$ az $a$ és $b$ elemek **asszociált**ak, azaz $a \mid b$ és $b \mid a$

---

[1] $S_H = \{\pi \colon H \to H \mid \pi \text{ permutáció}\}$, ha $H$ véges ($|H| = n \in \mathbb{N}$), akkor $|S_H| = n!$. Amennyiben $H = \{1, 2, \dots, n\}$, akkor $S_H$ helyett szokás az $S_n$ jelölést használni.

[2] $A_H = \{\pi \colon H \to H \mid \pi \text{ páros permutáció}\}$, ha $H$ véges ($|H| = n \in \mathbb{N}$), akkor $|A_H| = \frac{n!}{2}$. Amennyiben $H = \{1, 2, \dots, n\}$, akkor $A_H$ helyett szokás az $A_n$ jelölést használni.

$Q_D$ $\rightsquigarrow$ a $D$ integritástartomány **hányadostest**e
$\mathrm{char}(K)$ $\rightsquigarrow$ a $K$ test **karakterisztká**ja[3]
$\dim_K V$ $\rightsquigarrow$ a $K$ test feletti $V$ vektortér **dimenzió**ja

**Testbővítések**

$L : K$ $\rightsquigarrow$ az $L$ test a $K$ test **testbővítés**e
$[L : K]$ $\rightsquigarrow$ az $L : K$ **testbővítés foka**
$m_{\alpha,K}$ $\rightsquigarrow$ az $\alpha$ elem **minimálpolinom**ja a $K$ test felett
$\mathrm{gr}_K(\alpha)$ $\rightsquigarrow$ az $\alpha$ **elem foka** a $K$ test felett
$\mathrm{Aut}(K)$ $\rightsquigarrow$ a $K$ test **automorfizmus**ainak halmaza
$\mathrm{Aut}_K(L)$ $\rightsquigarrow$ a $L$ test $K$ fixen hagyó **automorfizmus**ainak halmaza, azaz az $L : K$ testbővítés Galois-csoportja
$\mathrm{Gal}(L : K)$ $\rightsquigarrow$ az $L : K$ **testbővítés Galois-csoportja**
$\mathrm{Gal}_K(f)$ $\rightsquigarrow$ az $f \in K[x]$ **polinom Galois-csoportja**
$\mathfrak{F}$ $\rightsquigarrow$ a **Frobenius-endomorfizmus**
$L^\times$ $\rightsquigarrow$ az $L$ **test multiplikatív csoportja**, azaz $L^\times = (L \setminus \{0\}; \cdot)$.

[3] a $K$ test karakterisztikája 0 vagy prímszám.

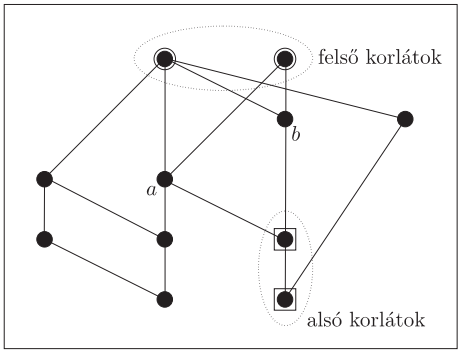
# Tartalomjegyzék

# Hálók

## 1.1 Hálószerűen rendezett halmazok

Legyen $(A;\leqslant)$ részbenrendezett halmaz és $a,b,c \in A$. Azt mondjuk, hogy $c$ **alsó korlátja** [**felső korlátja**] $a$-nak és $b$-nek, ha $c \leqslant a,b$ $[a,b \leqslant c]$.

Legyen $(A;\leqslant)$ részbenrendezett halmaz és $a,b,c_0 \in A$. Azt mondjuk, hogy $c_0$ **legnagyobb alsó korlátja** [**legkisebb felső korlátja**] $a$-nak és $b$-nek, ha $c_0 \leqslant a,b$ $[a,b \leqslant c_0]$ és $a,b$ bármely $c$ alsó korlátjára [felső korlátjára] $c \leqslant c_0$ $[c_0 \leqslant c]$ teljesül.

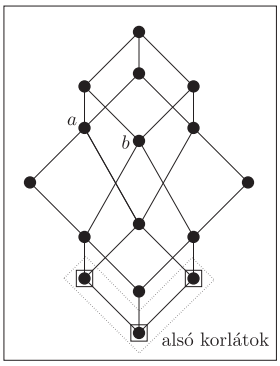



**1. ábra:** Az $a$ és $b$ elemek alsó és felső korlátjai.

**1.1. Állítás.** *Legyen $(A;\leqslant)$ részbenrendezett halmaz és $a,b \in A$. Ha az $a$ és $b$ elemeknek van legnagyobb alsó korlátja [legkisebb felső lorlátja], akkor az egyértelműen meghatározott.*

*Bizonyítás.* Tegyük fel, hogy $c,c' \in A$ legnagyobb alsó korlátja az $a,b \in A$ elemeknek. Ekkor $c$ és $c'$ alsó korlátja is $a$-nak és $b$-nek. Ezért $c' \leqslant c$, mivel $c$ legnagyobb alsó korlát, illetve $c \leqslant c'$, mivel $c'$ legnagyobb alsó korlát. Így a $\leqslant$ reláció antiszimmetriája miatt $c' = c$. A legkisebb felső korlát esetére a bizonyítás hasonlóképpen végezhető el. □

Az $(A;\leqslant)$ részbenrendezett halmazt **hálószerűen rendezett halmaznak** hívjuk, ha az $A$ halmaz bármely $a$ és $b$ elemének létezik legnagyobb alsó, illetve legkisebb felső korlátja.




**2. ábra:** Az $a$ és $b$ elemeknek nincs legnagyobb alsó korlátja.

**1.2. Példa.** *Az alábbiakban néhány példát mutatunk hálószerűen rendezett halmazokra.*

| *részbenrendezett halmaz* | *legnagyobb alsó korlát* | *legkisebb felső korlát* |
|---|---|---|
| $(\mathbb{N};\ \vert\ )$ | ln.k.o.(a, b) | lk.k.t.(a, b), |
| $(P(U);\ \subseteq\ )$ | $X \cap Y$ | $X \cup Y$, |
| $(\mathrm{Sub}({}_K V);\ \subseteq\ )$ | $U \cap W$ | $U + W$, |
| $(\mathrm{Sub}(\mathbb{G});\ \subseteq\ )$ | $H \cap K$ | $\langle H \cup K \rangle$, |
| $(\mathrm{SubNorm}(\mathbb{G};\ \subseteq\ )$ | $M \cap N$ | $M \cdot N$. |

*A táblázatban $U$ tetszőleges halmazt jelöl, $X, Y \subseteq U$; $\mathrm{Sub}({}_K V)$ a $K$ test feletti ${}_K V$ vektortér altereinek halmaza, $U$ és $W$ alterei ${}_K V$-nek, $U + W$ ezen alterek komplexus összege;* $\mathrm{Sub}(\mathbb{G})$ *a $\mathbb{G}$ csoport részcsoportjainak halmaza, $H$ és $K$ részcsoportjai $\mathbb{G}$-nek, $\langle H \cup K \rangle$ pedig az ezen részcsoportok egyesítése által generált részcsoport;* $\mathrm{SubNorm}(\mathbb{G})$ *a $\mathbb{G}$ csoport normális részcsoportjainak halmaza, $M$ és $N$ normális részcsoportjai $\mathbb{G}$-nek, $M \cdot N$ pedig ezen normális részcsoportok komplexus szorzata.*

## 1.2 Hálók

Legyen $(L; \leqslant)$ hálószerűen rendezett halmaz. Az $L$ halmazon definiáljuk a $\wedge$ (metszet) és $\vee$ (egyesítés) műveleteket az alábbi módon:

$$\wedge\colon L \times L \to L,\ (a, b) \mapsto a \text{ és } b \text{ legnagyobb alsó korlátja}, \tag{1}$$

$$\vee\colon L \times L \to L,\ (a, b) \mapsto a \text{ és } b \text{ legkisebb felső korlátja}. \tag{2}$$

**1.3. Állítás.** *Bármely $(L; \leqslant)$ hálószerűen rendezett halmaz tetszőleges $a, b, c$ elemeire teljesülnek az alábbiak:*

$$\begin{array}{ccc}
a \wedge a = a, & a \vee a = a & (\textit{idempotencia}),\\
a \wedge b = b \wedge a, & a \vee b = b \vee a & (\textit{kommutativitás}),\\
(a \wedge b) \wedge c = a \wedge (b \wedge c), & (a \vee b) \vee c = a \vee (b \vee c) & (\textit{asszociativitás}),\\
(a \wedge b) \vee b = b, & (a \vee b) \wedge b = b & (\textit{(abszorptivitás}).
\end{array}$$

*Bizonyítás.* A $\wedge$ és $\vee$ műveletek idempotenciája és kommutativitása nyilvánvaló, ezért csak e műveletek asszociativitását és abszorptivitását igazoljuk. Legyenek $a, b, c \in L$ tetszőleges elemek.

A $\wedge$ művelet asszociativitása. Legyen $u = (a \wedge b) \wedge c$ és $v = a \wedge (b \wedge c)$. Ekkor $a \wedge b \leqslant a, b$ és $u \leqslant a \wedge b, c$ miatt $u \leqslant a, b, c$. Tegyük fel, hogy az $u' \in L$ elemre $u' \leqslant a, b, c$ teljesül. Ekkor $u' \leqslant a \wedge b$ és $u' \leqslant c$ következtében

$$u' \leqslant (a \wedge b) \wedge c = u. \tag{3}$$

Mivel $v \leqslant b \wedge c$ miatt $v \leqslant b, c$, ezért $v \leqslant a, b, c$. Így (3) szerint $v \leqslant u$. Hasonlóan igazolható, hogy $v \leqslant u$ is teljesül, azaz $u = v$.

A $\vee$ művelet asszociativitása. Legyen $u = (a \vee b) \vee c$ és $v = a \vee (b \vee c)$. Ekkor $a, b \leqslant a \vee b$ és $a \vee b, c \leqslant u$ miatt $a, b, c \leqslant$. Tegyük fel, hogy az $u' \in L$ elemre $a, b, c \leqslant u'$ teljesül. Ekkor $a \vee b \leqslant u'$ és $c \leqslant u'$ következtében

$$u = (a \vee b) \vee c \leqslant u. \tag{4}$$

Mivel $b \vee c \leqslant v$ miatt $b, c \leqslant v$, ezért $a, b, c \leqslant v$. Így (4) szerint $u \leqslant v$. Hasonlóan igazolható, hogy $v \leqslant u$ is teljesül, azaz $u = v$.

Az abszorptivitás igazolásához először azt gondoljuk meg, hogy ha $s \leqslant t$ $(s, t \in L)$, akkor $s \wedge t = s$ és $s \vee t = t$. Az $s$ elem nyilván alsó korlátja $s, t$-nek, így $s \leqslant s \wedge t$. Továbbá, ha $s'$ alsó korlátja $s, t$-nek, akkor $s' \leqslant s, t$. Így $s$ az $s$ és $t$ elemek legnagyobb alsó korlátja, azaz $s = s \wedge t$. Másrészt, a $t$ elem nyilván felső korlátja $s, t$-nek, így $s \vee t \leqslant t$. Továbbá, ha $t'$ felső korlátja $s, t$-nek, akkor $s, t \leqslant t'$. Így $t$ az $s$ és $t$ elemek legkisebb felső korlátja, azaz $t = s \vee t$.

Ekkor $a \wedge b \leqslant b$ miatt $(a \wedge b) \vee b = b$, és $b \leqslant a \vee b$ miatt $(a \vee b) \wedge b = b$. □

Azt mondjuk, hogy az $(L; \wedge, \vee)$ algebra **háló**, ha tetszőleges $a, b, c \in L$ elemekre teljesülnek az 1.3. Állításbeli egyenlőségek.

**1.4. Tétel.** *Legyen $(L; \leqslant)$ hálószerűen rendezett halmaz. Ekkor $(L; \wedge, \vee)$ háló, ahol $\wedge$ és $\vee$ az (1) és (2) műveletek.*

*Bizonyítás.* Az 1.3. Állítás következtében nyilvánvaló. □

**1.5. Tétel.** *Legyen $(L; \wedge, \vee)$ háló. Ekkor $(L; \leqslant)$ hálószerűen rendezett halmaz, ahol $\leqslant$ a következő reláció az $L$ halmazon:*

$$a \leqslant b \Longleftrightarrow a \wedge b = a \quad (\Longleftrightarrow a \vee b = b).$$

*Bizonyítás.* Legyenek $a, b, c \in L$ tetszőleges elemek. Először azt igazoljuk, hogy $\leqslant$ részbenrendezés. Mivel a $\wedge$ művelet idempotens, ezért $a \wedge a = a$, azaz $a \leqslant a$. Tegyük fel, hogy $a \leqslant b$ és $b \leqslant a$. Ekkor $a = a \wedge b = b \wedge a = b$, azaz $\leqslant$ antiszimmetrikus. Végül, tegyük fel, hogy $a \leqslant b$ és $b \leqslant c$. Ekkor $a = a \wedge b$ és $b = b \wedge c$ miatt

$$a = a \wedge b = a \wedge (b \wedge c) = (a \wedge b) \wedge c = a \wedge c,$$

azaz $a \leqslant c$. Ezzel igazoltuk, hogy $\leqslant$ részbenrendezés.

Megmutatjuk, hogy $(L; \leqslant)$ hálószerűen rendezett halmaz. Tegyük fel, hogy

$u \in L$ alsó korlátja $a$-nak és $b$-nek. Ekkor $u \leqslant a, b$, azaz $u = u \wedge a = u \wedge b$, és így

$$\begin{aligned}
u &= u \wedge u && (\wedge \text{ idempotens}) \\
&= (u \wedge a) \wedge (u \wedge b) && (u = u \wedge a \text{ és } u = u \wedge b) \\
&= u \wedge \big(a \wedge (u \wedge b)\big) && (\wedge \text{ asszociatív}) \\
&= u \wedge \big((a \wedge u) \wedge b\big) && (\wedge \text{ asszociatív}) \\
&= u \wedge \big((u \wedge a) \wedge b\big) && (\wedge \text{ kommutatív}) \\
&= u \wedge \big(u \wedge (a \wedge b)\big) && (\wedge \text{ asszociatív}) \\
&= (u \wedge u) \wedge (a \wedge b) && (\wedge \text{ asszociatív}) \\
&= u \wedge (a \wedge b), && (\wedge \text{ idempotens})
\end{aligned}$$

azaz $u \leqslant a \wedge b$. Ezzel igazoltuk, hogy az $L$ halmaz bármely két elemének van legnagyobb alsó korlátja, ami éppen a két elem metszete. Hasonlóan mutatható meg az, hogy bármely két elemnek van legkisebb felső korlátja, nevezetesen a két elem egyesítése. A bizonyítást ezzel befejeztük. □

Legyenek $\mathbb{L}_1 = (L_1; \wedge_1, \vee_1)$ és $\mathbb{L}_2 = (L_2; \wedge_2, \vee_2)$ hálók, a hozzájuk tartozó hálószerűen rendezett halmazok legyenek rendre $(L_1; \leqslant_1)$ és $(L_2; \leqslant_2)$, valamint $\varphi\colon L_1 \to L_2$ tetszőleges leképezés. Azt mondjuk, hogy a $\varphi$ leképezés **rendezéstartó**, ha tetszőleges $a, b \in L_1$-re $a \leqslant_1 b$ esetén $a\varphi \leqslant_2 b\varphi$.

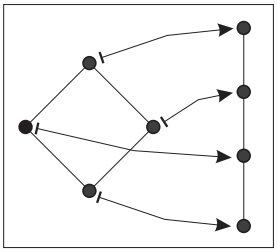
**1.6. Állítás.** *Legyenek $\mathbb{L}_1 = (L_1; \wedge_1, \vee_1)$ és $\mathbb{L}_2 = (L_2; \wedge_2, \vee_2)$ hálók. Ha a $\varphi\colon L_1 \to L_2$ leképezés homomorfizmus, akkor $\varphi$ rendezéstartó.*

*Bizonyítás.* Tegyük fel $a \leqslant_1 b$ $(a, b \in L_1)$. Ekkor $a = a \wedge_1 b$ miatt

$$a\varphi = (a \wedge_1 b)\varphi = a\varphi \wedge_2 b\varphi,$$

azaz $a\varphi \leqslant_2 b\varphi$. □

Az előző állítás megfordítása nem igaz, azaz rendezéstartó leképezés nem feltétlenül homomorfizmus (ld. 3. ábra).



**3. ábra:** Rendezéstartó bijektív leképezés, amely nem izomorfizmus.

Azonban igaz a következő.

**1.7. Tétel.** *Legyenek $\mathbb{L}_1 = (L_1; \wedge_1, \vee_1)$ és $\mathbb{L}_2 = (L_2; \wedge_2, \vee_2)$ hálók, valamint $\varphi\colon L_1 \to L_2$ bijektív leképezés. Ekkor $\varphi$ pontosan akkor izomorfizmus, ha a $\varphi$ és $\varphi^{-1}$ leképezések mindegyike rendezéstartó.*

*Bizonyítás.* Tegyük fel, hogy $\varphi$ izomorfizmus. Ekkor az 1.6. Állítás szerint $\varphi$ rendezéstartó. Legyen $a_2$ és $b_2$ olyan $L_2$-beli elemek, amelyekre $a_2 \leqslant_2 b_2$ teljesül. Mivel $\varphi$ bijekció, ezért vannak olyan $a_1, b_1 \in L_1$ elemek, hogy $a_2 = a_1\varphi$ és $b_2 = b_1\varphi$. Ekkor

$$\begin{aligned} a_2 \leqslant_2 b_2 &\iff a_2 = a_2 \wedge_2 b_2 \\ &\iff a_1\varphi = a_1\varphi \wedge_2 b_1\varphi \\ &\iff a_1\varphi = (a_1 \wedge_1 b_1)\varphi \\ &\iff a_1 = a_1 \wedge_1 b_1 \\ &\iff a_1 \leqslant_1 b_1, \end{aligned}$$

azaz $a_2 \leqslant_2 b_2 \iff a_2\varphi^{-1} \leqslant_1 b_2\varphi^{-1}$. Ez pedig éppen azt jelenti, hogy $\varphi^{-1}$ is rendezéstartó.

Tegyük fel, hogy $\varphi$ és $\varphi^{-1}$ is rendezéstartó leképezés. Mivel $\varphi$ bijektív, ezért elegendő azt igazolni, hogy $\varphi$ homomorfizmus. Legyenek $a, b \in L_1$ tetszőleges elemek. Ekkor igazak a következők:

$$\begin{aligned} a \wedge_1 b \leqslant_1 a, b &\Longrightarrow (a \wedge_1 b)\varphi \leqslant_2 a\varphi, b\varphi && (\varphi \text{ rendezéstartó}) \\ &\Longrightarrow (a \wedge_1 b)\varphi \leqslant_2 a\varphi \wedge_2 b\varphi \\ a\varphi \wedge_2 b\varphi \leqslant_2 a\varphi, b\varphi &\Longrightarrow (a\varphi \wedge_2 b\varphi)\varphi^{-1} \leqslant_1 a, b && (\varphi^{-1} \text{ rendezéstartó}) \\ &\Longrightarrow (a\varphi \wedge_2 b\varphi)\varphi^{-1} \leqslant_1 a \wedge b \\ &\Longrightarrow a\varphi \wedge_2 b\varphi \leqslant_2 (a \wedge_1 b)\varphi, && (\varphi \text{ rendezéstartó}) \end{aligned}$$

azaz $(a \wedge_1 b)\varphi = a\varphi \wedge_2 b\varphi$. Továbbá,

$$\begin{aligned} a, b \leqslant_1 a \vee_1 b &\Longrightarrow a\varphi, b\varphi \leqslant_2 (a \vee_1 b)\varphi && (\varphi \text{ rendezéstartó}) \\ &\Longrightarrow a\varphi \vee_2 b\varphi \leqslant_2 (a \vee_1 b)\varphi \\ a\varphi, b\varphi \leqslant_2 a\varphi \vee_2 b\varphi &\Longrightarrow a, b \leqslant_1 (a\varphi \vee_2 b\varphi)\varphi^{-1} && (\varphi^{-1} \text{ rendezéstartó}) \\ &\Longrightarrow a \vee_1 b \leqslant_1 (a\varphi \vee_2 b\varphi)\varphi^{-1} \\ &\Longrightarrow (a \vee_1 b)\varphi \leqslant_2 a\varphi \wedge_2 b\varphi, && (\varphi \text{ rendezéstartó}) \end{aligned}$$

azaz $(a \vee_1 b)\varphi = a\varphi \vee_2 b\varphi$. Ezzel igazoltuk, hogy $\varphi$ homomorfizmus. □

A továbbiakban a disztributív és moduláris hálókkal ismerkedünk meg.

**1.8. Tétel.** *Tetszőleges $(L; \wedge, \vee)$ hálóban ekvivalensek a következők:*

(1) *bármely $x, y, z \in L$-re $(x \vee y) \wedge z = (x \wedge z) \vee (y \wedge z)$,*

(2) *bármely $x, y, z \in L$-re $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$.*

Az $\mathbb{L}$ háló **disztributív**, ha az 1.8. Tétel (1) pontja teljesül $\mathbb{L}$-ben. Az $\mathbb{L}$ hálót **modulárisnak** nevezzük, ha bármely $x, y, z \in L$ elemekre $x \leqslant z$ esetén $(x \vee y) \wedge z = x \vee (y \wedge z)$ teljesül.

**1.9. Megjegyzés.** *Tetszőleges hálóban igazak az alábbi egyenlőtlenségek:*

$$\begin{aligned} (x \wedge z) \vee (y \wedge z) &\leqslant (x \vee y) \wedge z, \\ (x \wedge y) \vee z &\leqslant (x \vee z) \wedge (y \vee z), \\ x \vee (y \wedge z) &\leqslant (x \vee y) \wedge z, \ \textit{ha } x \leqslant z. \end{aligned}$$

**1.10. Tétel.** (a) *Bármely csoport normális részcsoportjainak hálója moduláris háló.*
(b) *Bármely vektortér altérhálója moduláris háló.*

*Bizonyítás.* (a) Legyen $G$ tetszőleges csoport, valamint legyen $L, M$ és $N$ olyan normális részcsoportjai, amelyekre $L \leqslant N$ teljesül. Az 1.9. Megjegyzés szerint elég azt igazolni, hogy $(LM) \cap N \subseteq L(M \cap N)$. Tegyük fel, hogy $g \in (LM) \cap N$. Ekkor $g \in N$, és vannak olyan $l \in L$, $m \in M$ elemek, amelyekre $g = lm$ teljesül. Így $m = l^{-1}g \in N$, mivel $l \in L \subseteq N$, aminek következtében $m \in M \cap N$. Azaz $g = lm \in L(M \cap N)$.

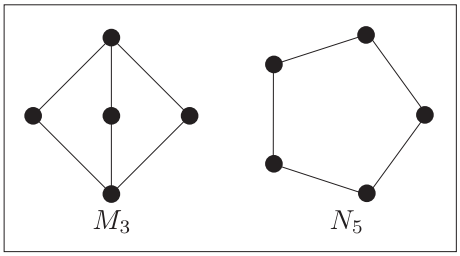
(b) Legyen $V$ a $K$ test feletti vektortér, és legyenek $X, Y, Z$ olyan alterek $V$-ben, amelyekre $X \subseteq Z$ teljesül. Az 1.9. Megjegyzés szerint elég azt igazolni, hogy $(X+Y) \cap Z \subseteq X + (Y \cap Z)$. Legyen $v$ tetszőleges $(X+Y) \cap Z$-beli vektor. Ekkor vannak olyan $x \in X$ és $y \in Y$ vektorok, amelyekre $v = x + y \in Z$ teljesül. Mivel $X \subseteq Z$ következtében $x \in Z$, ezért $y = v - x \in Z$. Azaz $y \in Y \cap Z$, és így $v = x + y \in X + (Y \cap Z)$.

Ezzel igazoltuk a tétel állításait. □

Hálók modularitása és a disztributivitása is jellemezhető bizonyos típusú részhálók hiányával, amint azt az alábbi, Richard Dedekind-től[4] és Garrett Birkhoff-tól[5] származó tételek mutatják.

**1.11. Tétel (Richard Dedekind, 1900).** *Legyen $\mathbb{L}$ tetszőleges háló. Az $\mathbb{L}$ háló pontosan akkor moduláris, ha nincs az $\mathbb{N}_5$ hálóval izomorf részhálója (ld. 4. ábra).*

**1.12. Tétel (Garrett Birkhoff).** *Az $\mathbb{L}$ moduláris háló pontosan akkor disztributív, ha nincs az $\mathbb{M}_3$ hálóval izomorf részhálója (ld. 4. ábra).*




**4. ábra:** Az $M_3$ és $N_5$ hálók.

## 1.3 Boole-algebrák

Az $\mathbb{L}$ hálót **korlátosnak** nevezzük, ha van legkisebb és legnagyobb eleme. Az $\mathbb{L}$ háló legkisebb elemét $0_{\mathbb{L}}$-lel, legnagyobb elemét $1_{\mathbb{L}}$-lel jelöljük. Ha nem okoz félreértést, akkor az indexet is elhagyjuk.

Legyen $\mathbb{L}$ korlátos háló, $a \in L$. A $b \in L$ elemet az $a$ elem **komplementumának** nevezzük, ha $a \wedge b = 0_L$ és $a \vee b = 1_L$.

[4] Julius Wilhelm Richard **Dedekind** (1831. október 6., Braunschweig - 1916. február 12., Braunschweig) német matematikus, kiemelkedő a munkássága az absztrakt algebra, valamint az algebrai számelmélet területén és a valós számok elméleti megalapozásában.

[5] Garrett **Birkhoff** (1911. január 19., Princeton, New Jersey – 1996. november 22., Water Mill, New York) amerikai matematikus.

**1.13. Állítás.** *Korlátos disztributív háló bármely elemének legfeljebb egy komplementuma van.*

*Bizonyítás.* Legyen $L$ korlátos disztributív háló. Tegyük fel, hogy az $a \in L$ elemnek $b$ és $b'$ is komplementuma. Ekkor az

$$b = 1_L \wedge b \overset{a\vee b'=1_L}{=} (a \vee b') \wedge b \overset{L \text{ diszt.}}{=} (a \wedge b) \vee (b' \wedge b) \overset{a\wedge b=0_L}{=} b' \wedge b,$$
$$b' = 1_L \wedge b' \overset{a\vee b=1_L}{=} (a \vee b) \wedge b' \overset{L \text{ diszt.}}{=} (a \wedge b') \vee (b \wedge b') \overset{a\wedge b'=0_L}{=} b \wedge b',$$

egyenlőségek következtében $b \leqslant b'$ és $b' \leqslant b$ teljesül, azaz $b = b'$. □

Azokat a korlátos disztributív hálókat, amelyekben minden elemnek pontosan egy komplementuma van **komplementumos disztributív hálóknak** vagy **Boole-hálóknak** nevezzük.

A $(B; \wedge, \vee, ', 0, 1)$ algebrát ($\wedge$ és $\vee$ kétváltozós, $'$ egyváltozós, 0 és 1 pedig nullaváltozós műveletek) **Boole-algebrának** nevezzük, ha

(1) $(B; \wedge, \vee)$ disztributív háló,

(2) $x \wedge 0 = 0$, $x \vee 1 = 1$ teljesül bármely $x \in B$-re,

(3) $x \wedge x' = 0$, $x \vee x' = 1$ teljesül bármely $x \in B$-re.

**1.14. Állítás.** *Legyen $(B; \wedge, \vee, ', 0, 1)$ Boole-algebra. Ekkor tetszőleges $a, b, c \in B$ elemekre teljesülnek a következők:*

(a) *ha $a \wedge c = 0$ és $a \vee c = 1$, akkor $c = a'$;*

(b) $(a')' = a$;

(c) $(a \wedge b)' = a' \vee b' \quad$ *és* $\quad (a \vee b)' = a' \wedge b'$ *(De Morgan-azonosságok).*

*Bizonyítás.* (a) Tegyük fel, hogy az $a, b, c \in B$ elemekre $a \wedge c = 0$ és $a \vee c = 1$ teljesül. Ekkor $c$ komplementuma $a$-nak. Mivel a $(B; \wedge, \vee)$ háló disztributív és $a'$ is komplementuma $a$-nak, ezért $c = a'$.

(b) Mivel $a' \wedge a = 0$ és $a' \vee a = 1$, ezért (a) szerint $a = (a')'$.

(c) Legyenek $a$ és $b$ tetszőleges elemei $B$-nek, ekkor

$$\begin{aligned}
(a \wedge b) \wedge (a' \vee b') &\overset{\wedge \text{ asszoc.}}{=} a \wedge (b \wedge (a' \vee b')) \\
&\overset{\text{diszt.}}{=} a \wedge ((b \wedge a') \vee (b \wedge b')) \\
&\overset{b\wedge b'=0}{=} a \wedge (b \wedge a') \\
&\overset{\wedge \text{ komm.}}{=} a \wedge (a' \wedge b) \\
&\overset{\wedge \text{ asszoc.}}{=} (a \wedge a') \wedge b \\
&\overset{a\wedge a'=0}{=} 0,
\end{aligned}$$

másrészt

$$\begin{aligned}
(a \wedge b) \vee (a' \vee b') &\overset{\vee \text{ asszoc.}}{=} ((a \wedge b) \vee a') \vee b' \\
&\overset{\text{diszt.}}{=} ((a \vee a') \wedge (b \vee a')) \vee b' \\
&\overset{a\vee a'=1}{=} (b \vee a') \vee b' \\
&\overset{\vee \text{ komm.}}{=} (a' \vee b) \vee b' \\
&\overset{\vee \text{ asszoc.}}{=} a' \vee (b \vee b') \\
&\overset{b\vee b'=1}{=} 1.
\end{aligned}$$

Így az (a) állítás szerint $(a \wedge b)' = a' \vee b'$. Az $(a \vee b)' = a' \wedge b'$ egyenlőség hasonlóan igazolható. □

**1.15. Példa.** *Tetszőleges $U$ nemüres halmazra a $(P(U); \cap, \cup, {}^-, \emptyset, U)$ algebra Boole-algebra.*

Az alábbi tétel Garrett Birkhoff 1937-ben felfedezett tételének véges Boole-algebrákra vonatkozó változata. Az eredeti tétel a véges disztributív hálókat jellemzi.

**1.16. Tétel (Véges Boole-algebrák reprezentációtétele).** *Bármely véges $\mathbb{B}$ Boole-algebrához létezik olyan $\mathcal{A}$ véges halmaz, amelyre*

$$\mathbb{B} \cong (P(\mathcal{A}); \cap, \cup, {}^-, \emptyset, \mathcal{A}).$$

**1.17. Megjegyzés.** *Az $\mathcal{A}$ halmaz választható a $(B; \wedge, \vee)$ háló atomjai halmazának. A bizonyítás egy lényeges lépése annak megmutatása, hogy $b < c$ $(b, c \in B)$ esetén van olyan $a$ atom, amelyre $a \leqslant c$, $a \not\leqslant b$ teljesül.*

Legyen $\mathcal{A}$ véges halmaz. A $H \in P(\mathcal{A})$ halmaz **karakterisztikus leképezésének** nevezzük a

$$\chi_H \colon \mathcal{A} \to \{0,1\},\ \chi(a) = \begin{cases} 1, & \text{ha } a \in \mathcal{A}, \\ 0, & \text{ha } a \notin \mathcal{A} \end{cases}$$

leképezést. Egyszerűen igazolható, hogy a

$$P(\mathcal{A}) \to \{0,1\}^{|\mathcal{A}|},\ H \mapsto (\chi_H(a))_{a \in \mathcal{A}}$$

leképezés izomorfizmus a $(P(\mathcal{A}); \cap, \cup, {}^-, \emptyset, \mathcal{A})$ és $(\{0,1\}; \wedge, \vee, {}', 0, 1)^{|\mathcal{A}|}$ Boole-algebrák között.

**1.18. Következmény.** *Minden véges Boole-algebra izomorf a 2-elemű Boole-algebra egy véges direkt hatványával.*

# Testek és bővítéseik

A Galois-elmélet egyik fontos része a polinom egyenletek vizsgálata. Mielőtt belemerülnénk a részletekbe, először néhány egyszerű és — már bizonyára — jólismert példát szeretnénk bemutatni.

A polinomok összeadására és szorozására gondolva természetes módon vetődik fel, hogy olyan polinomhalmazokkal foglalkozzunk, amelyek együtthatói valamely $R$ gyűrűből valók. Már a legegyszerűbb esetben is, amikor $R = \mathbb{Z}$ és $f$ egész együtthatós elsőfokú polinom, nehézségeink támadhatnak, hiszen például a $2x + 3 = 0$ egyenletnek nincs egész megoldása.

Ha $R$ integritástartomány, akkor a a hányadostest konstrukció kínál megoldást ezen problémára. A fenti egyenlet esetében, ha a 2-t és 3-at mint $\mathbb{Q}$-beli elemeket tekintjük, akkor az egyenletnek már lesz megoldása: $x = -2/3 \in \mathbb{Q}$.[6]

Tekintsük az $x^2 - 2x - 1 = 0$ egyenletet a racionális számtest felett. Teljesnégyzetté kiegészítve azt kapjuk, hogy egyenletünk ekvivalens az $(x-1)^2 = 2$ egyenlettel. Mivel nincs olyan raconális $r$ szám, amelyre $r^2 = 2$ teljesülne, ezért egyenletünk nem oldható meg a racionális számok körében. Kézenfekvő ötlet, hogy az $x^2 - 2x - 1$ polinomot valós együtthatós polinomnak tekintsük. Ekkor egyenletünk $(x - 1 + \sqrt{2})(x - 1 - \sqrt{2}) = 0$ alakban írható, és így van (valós) megoldásunk: $1 \pm \sqrt{2}$.

A kérdés most már csak az, hogy $\mathbb{Q}$ helyett $\mathbb{R}$-et véve gazdaságosan jártunk-e el: vajon van-e olyan $\mathbb{Q}$-t tartalmazó $\mathbb{R}$-nél szűkebb test, amely szintén tartalmazza ezeket a megoldásokat. Egyszerűen igazolható, hogy az $a+b\sqrt{2}$ $(a, b \in \mathbb{Q})$ alakú valós számok $H$ halmaza testet alkot, és $\mathbb{Q} \subsetneq H \subsetneq \mathbb{R}$.[7] Ha az $x^2 - 2x - 1$ polinomot $H$ feletti polinomnak tekintjük, akkor a fentiek azt mondják e polinomnak van gyöke $H$-ban.

A fentiek az algebra nyelvén a következőképpen mondhatók el. Az $x^2 - 2x - 1 \in \mathbb{Q}[x]$ polinom irreducibilis, de $H[x]$-beli polinomként tekintve már nem irreducibilis, sőt lneáris tényezők szorzatára bontható $H$ felett.

A feladatunk most már egyszerűen mefogalmazható: adott $f \in K[x]$ ($K$ test) polinom esetén található-e olyan $K$-t tartalmazó $L$ test, hogy $f$-et $L$ feletti polinomnak tekintve már lineáris tényezőkre bomlik.

## 2.1 Testbővítések

Legyenek $K$ és $L$ testek. Ha $K$ részteste $L$-nek, akkor azt mondjuk, hogy $L$ **testbővítése** $K$-nak, és ezt az $L : K$ szimbólummal jelöljük.

[6] Ha $R$ integritástartomány, akkor az $ax + b = c$ alakú polinomegyenletek mindig megoldhatók $Q_R$-ben $(a, b, c \in R,\ a \neq 0)$, ahol $Q_R$ az $R$ integritástartomány hányadosteste. Például: $Q_{\mathbb{Z}} = \mathbb{Q}$.

[7] Valójában $H$ inkább $\mathbb{Q}$-hoz áll közelebb, mivel $|H| = |\mathbb{Q}| < |\mathbb{R}|$.

**2.1. Tétel.** *Ha az $L$ test bővítése a $K$ testnek, akkor $L$ vektortér $K$ felett az*

$$\oplus\colon L \times L \to L,\ u \oplus v = u + v,$$
$$f_\lambda\colon L \to L,\ uf_\lambda = \lambda u\ (\lambda \in K)$$

*műveletekkel.*

Az 2.1. Tételt fogjuk felhasználni testbővítés fokának a definiálására. Az $L : K$ testbővítés $[L : K]$ **foka** az $L$ testnek, mint $K$ feletti vektortérnek a dimenziója, azaz $[L : K] = \dim_K L$. Ha $[L : K] < \infty$, akkor azt mondjuk, hogy az $L : K$ testbővítés **véges (dimenziós)**, különben $L : K$ **végtelen (dimenziós)**.

**2.2. Példa.** *A $\mathbb{C} : \mathbb{R}$ testbővítés 2-fokú, mivel $\mathbb{C}$ 2-dimenziós vektortér $\mathbb{R}$ felett; az $1, i \in \mathbb{C}$ vektorok bázist alkotnak. Azonban a $\mathbb{C} : \mathbb{Q}$ és $\mathbb{R} : \mathbb{Q}$ testbővítések végtelenek, mivel minden $\mathbb{Q}$ felett véges dimenziós vektortér megszámlálhatóan végtelen.*

**2.3. Tétel (Fokszámtétel).** *Legyenek $K$, $L$ és $M$ olyan testek, amelyekre $L : K$, $M : L$ teljesül.*

(a) *Ha az $L : K$ és $M : L$ testbővítések valamelyike végtelen, akkor $M : K$ is az.*

(b) *Ha az $L : K$ és $M : L$ testbővítések végesek, akkor az $M : K$ testbővítés is az, és fennáll az*
$$[M : K] = [M : L] \cdot [L : K]$$
*egyenlőség.*

*Bizonyítás.* (a) Az állítást kontrapozicióval igazoljuk. Tegyük fel, hogy $M : K$ véges, $[M : K] = n \in \mathbb{N}$. Mivel $L$ altér $M$-ben, ezért

$$[L : K] = \dim_K L \leqslant \dim_K M = n.$$

Megmutatjuk, hogy $[M : L] \leqslant n$ is teljesül. Legyen $\mu_1, \ldots, \mu_{n+1}$ tetszőleges vektorrendszer $M$-ben. Mivel az $M$ vektortér $n$-dimenziós $K$ felett, és a $\mu_1, \ldots, \mu_{n+1}$ vektorok $M$-beliek, ezért vannak olyan $b_1, \ldots, b_{n+1}$ $K$-beli skalárok, amelyekre $(b_1, \ldots, b_{n+1}) \neq \mathbf{0}$ teljesül és

$$b_1\mu_1 + \cdots + b_{n+1}\mu_{n+1} = 0.$$

Ez pedig éppen azt bizonyítja, hogy a $\mu_1, \ldots, \mu_{n+1}$ vektorok lineárisan függőek az $M$ (mint $L$ feletti) vektortérben.

(b) Tegyük fel, hogy az $L : K$ és $M : L$ testbővítések is végesek, legyen $[L : K] = m$ és $[M : L] = n$ $(m, n \in \mathbb{N})$. Válasszunk az $L$ és az $M$ vektortérben is egy-egy bázist:

$$\lambda_1, \ldots, \lambda_m \quad \text{bázis } L\text{-ben, mint } K \text{ feletti vektortérben,} \tag{5}$$
$$\mu_1, \ldots, \mu_n \quad \text{bázis } M\text{-ben, mint } L \text{ feletti vektortérben.} \tag{6}$$

Megmutatjuk, hogy a $\mu_i\lambda_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ vektorrendszer bázis $M$-ben, mint $K$ feletti vektortérben. Legyen $\mu$ tetszőleges $M$-beli vektor. Ekkor (6) miatt vannak olyan $b_1, \ldots, b_n \in L$ skalárok, amelyekre

$$\mu = b_1\mu_1 + \cdots + b_n\mu_n$$

teljesül. Mivel $b_1, \ldots, b_n \in L$, ezért (5) miatt vannak olyan $a_{i,j} \in K$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ skalárok, amelyekre

$$b_i = a_{i,1}\lambda_1 + \cdots + a_{i,m}\lambda_m \quad (1 \leqslant i \leqslant n)$$

teljesül. Így

$$\mu = \sum_{i=1}^{n} b_i\mu_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} a_{i,j}\lambda_j \right) \mu_i = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\lambda_j\mu_i,$$

azaz a $\mu_i\lambda_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ vektorrendszer generátorrendszer. Tegyük fel, hogy

$$\sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\lambda_j\mu_i = 0.$$

Ekkor

$$0 = \sum_{i=1}^{n}\sum_{j=1}^{m} a_{i,j}\lambda_j\mu_i = \sum_{i=1}^{n} \left( \sum_{j=1}^{m} a_{i,j}\lambda_j \right) \mu_i$$

és (6) miatt $\sum_{j=1}^{m} a_{i,j}\lambda_j = 0$ $(1 \leqslant i \leqslant n)$. Ekkor (5)-et ismét felhasználva azt kapjuk, hogy $a_{i,j} = 0$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$, azaz a $\mu_i\lambda_j$ $(1 \leqslant i \leqslant n,\ 1 \leqslant j \leqslant m)$ vektorrendszer lineárisan független, így bázisa az $M$ vektortérnek. Mindezeket figyelembevéve azt kapjuk, hogy

$$[L : K] \cdot [M : L] = m \cdot n = \dim_K M = [M : L].$$

Ezzel az állítást igazoltuk. □

A 2.3. Tétel állítása teljes indukcióval egyszerűen kiterjeszthető bővítések egymásutánjaira is.

**2.4. Következmény.** *Legyenek $K_1, \ldots, K_n$ olyan testek $(n \in \mathbb{N})$, amelyekre a $K_{i+1} : K_i$ testbővítések minden $i$-re $(1 \leqslant i \leqslant n-1)$ végesek. Ekkor a $K_n : K_1$ testbővítés is véges és*

$$[K_n : K_1] = [K_2 : K_1] \cdots [K_n : K_{n-1}].$$

## 2.2 Algebrai és transzcendens elemek

Legyen $L$ a $K$ test testbővítése, és $A$ tetszőleges részhalmaza $L$-nek. Ekkor $K(A)$-val jelöljük, és a $K \cup A$ részhalmaz által **generált résztestnek** nevezzük az $L$ test $K \cup A$ részhalmazát tartalmazó legszűkebb résztestét. Azt mondjuk, hogy a $K(A) : K$ testbővítés $K$-nak az $A$ részhalmaz által generált testbővítése. Ha $A$ véges részhalmaza $L$-nek, pl. $A = \{\alpha_1, \ldots, \alpha_n\}$, akkor $K(A)$ helyett $K(\alpha_1, \ldots, \alpha_n)$-et írunk. Azt mondjuk, hogy az $L : K$ testbővítés **egyszerű**, ha van olyan $\alpha \in L$, amelyre $L = K(\alpha)$ teljesül.

**2.5. Példa.** *A $\mathbb{C} : \mathbb{R}$ bővítés egyszerű, mivel $\mathbb{C} = \mathbb{R}(i)$. Az $\mathbb{R} : \mathbb{Q}$ testbővítés azonban nem egyszerű.*

*Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ testbővítést. Mivel $\sqrt{2} + \sqrt{3} \in \mathbb{Q}(\sqrt{2}, \sqrt{3})$, ezért $\mathbb{Q}(\sqrt{2} + \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2}, \sqrt{3})$. Másrészt, az*

$$\sqrt{2} = \frac{1}{2} \cdot \big((\sqrt{2} + \sqrt{3})^3 - 9 \cdot (\sqrt{2} + \sqrt{3})\big),$$
$$\sqrt{3} = (\sqrt{2} + \sqrt{3}) - \sqrt{2}$$

*egyenlőségek következtében $\sqrt{2}, \sqrt{3} \in \mathbb{Q}(\sqrt{2} + \sqrt{3})$, azaz $\mathbb{Q}(\sqrt{2}, \sqrt{3}) \subseteq \mathbb{Q}(\sqrt{2} + \sqrt{3})$. Így azt kapjuk, hogy $\mathbb{Q}(\sqrt{2}, \sqrt{3}) = \mathbb{Q}(\sqrt{2} + \sqrt{3})$, azaz a $\mathbb{Q}(\sqrt{2}, \sqrt{3}) : \mathbb{Q}$ testbővítés egyszerű.*

**2.6. Tétel.** *Legyenek $K$ és $L$ olyan testek, amelyekre $L : K$ teljesül, valamint legyen $\alpha_1, \ldots, \alpha_n \in L$. Ekkor $K(\alpha_1, \ldots, \alpha_n)$ megegyezik az*

$$\left\{ f(\alpha_1, \ldots, \alpha_n) \cdot g(\alpha_1, \ldots, \alpha_n)^{-1} \;\middle|\; f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}. \tag{7}$$

*halmazzal.*

*Bizonyítás.* Legyen $M$ az $L$ test $K \cup \{\alpha_1, \ldots, \alpha_n\}$ részhalmazát tartalmazó legszűkebb részteste. Mivel $K \cup \{\alpha_1, \ldots, \alpha_n\} \subseteq M$, ezért tetszőleges $f \in K[x_1, \ldots, x_n]$-re $f(\alpha_1, \ldots, \alpha_n) \in M$, mivel $M$ zárt az

$$+ \colon L \times L \to L, (x, y) \mapsto x + y,$$
$$\cdot \colon L \times L \to L, (x, y) \mapsto x \cdot y,$$
$$- \colon L \times L \to L, (x, y) \mapsto x + (-y)$$

műveletek mindegyikére. Ha a $g \in K[x_1, \ldots, x_n]$ polinomra $g(\alpha_1, \ldots, \alpha_n) \neq 0$ teljesül, akkor $f(\alpha_1, \ldots, \alpha_n) \cdot g(\alpha_1, \ldots, \alpha_n)^{-1} \in M$ is teljesül, mivel $M^\times$ zárt az $L^\times \times L^\times \to L^\times$, $(x, y) \mapsto x \cdot y^{-1}$ műveletre. Mindezek után elegendő belátni, hogy (7) részteste $L$-nek. Ennek bizonyítását a kedves olvasóra bízzuk. □

Tegyük fel, hogy a $K$ és $L$ testekre $L : K$ teljesül, és legyen $\alpha \in L$. Ekkor az alábbi állítások közül pontosan az egyik teljesül:

- Van olyan $f \in K[x] \setminus \{0\}$ polinom, amelynek $\alpha$ gyöke, azaz $f(\alpha) = 0$; ekkor azt mondjuk, hogy $\alpha$ **algebrai elem a $K$ test felett**.
- Nincs olyan $f \in K[x] \setminus \{0\}$ polinom, amelynek $\alpha$ gyöke. Ebben az esetben azt mondjuk, hogy $\alpha$ **transzcendens elem a $K$ test felett**.

Annak eldöntésére, hogy melyik állítás teljesül az

$$\varepsilon_\alpha \colon K[x] \to K(\alpha),\ f \mapsto f(\alpha)$$

leképezést hívhatjuk segítségül, amint azt a következő tétel mutatja.

**2.7. Tétel.** *Legyenek $K$ és $L$ olyan testek, amelyekre $L : K$ teljesül, valamint legyen $\alpha \in L$. Ekkor az alábbi két állítás közül pontosan az egyik teljesül.*

(a) *Az $\varepsilon_\alpha$ leképezés injektív homomorfizmus, és $\varepsilon_\alpha$-t kiterjesztve $K[x]$ hányadostestére, a kapott*

$$\widetilde{\varepsilon_\alpha}\colon K(x) \to K(\alpha)$$

*leképezés izomorfizmus. Ekkor a $K(\alpha) : K$ testbővítés végtelen, és az $\alpha$ elem transzcendens $K$ felett.*

(b) *Az $\varepsilon_\alpha$ leképezés homomorfizmus, amely nem injektív, így magja* $\ker(\varepsilon_\alpha) \neq \{0\}$. *Ekkor* $\ker(\varepsilon_\alpha) = (m_{\alpha,K})$ *teljesül valamely egyértelműen meghatározott $m_{\alpha,K} \in K[x]$ irreducibilis főpolinomra, és az*

$$\widehat{\varepsilon_\alpha}\colon K[x]/(m_{\alpha,K}) \to K(\alpha)$$

*homomorfizmus izomorfizmus. Ekkor $K(\alpha) : K$ véges, és az $\alpha$ elem algebrai $K$ felett.*

*Bizonyítás.* (a) Tegyük fel, hogy az $\varepsilon_\alpha$ leképezés injektív homomorfizmus. Ekkor $f(\alpha) = 0$ pontosan akkor teljesül, ha $f = 0$, így az $\alpha$ elem transzcendens $K$ felett és a $K(\alpha) : K$ testbővítés végtelen. Az $\varepsilon_\alpha$ leképezés kiterjeszthetősége korábbi tételből következik,[8] a szürjektivitás pedig abból, hogy $K \cup \{\alpha\}$ generálja $K(\alpha)$-át.

(b) Tegyük fel, hogy az $\varepsilon_\alpha$ leképezés nem injektív homomorfizmus. Ekkor $\ker(\varepsilon_\alpha)$ ideál a $K[x]$ polinomgyűrűben, ami főideálgyűrű, mivel $K$ test. Ezért van olyan $f \in K[x]$ polinom, amelyre $\ker(\varepsilon_\alpha) = (f)$ teljesül. Legyen $m_{\alpha,K} = a^{-1}f$, ahol $a \in K \setminus \{0\}$ az $f$ polinom főegyütthatója. Mivel $f \sim a^{-1}f$, ezért $\ker(\varepsilon_\alpha) = (f) = (m_{\alpha,K})$. Tegyük fel, hogy $m_{\alpha,K}$ nem irreducibilis, azaz vannak olyan $g, h \in K[x]$ polinomok, amelyekre $m_{\alpha,K} = gh$ és $1 \leqslant g^*, h^* < m^*_{\alpha,K}$ teljesül. Ekkor $g, h \notin (m_{\alpha,K})$, de $g(\alpha) = 0$ vagy $h(\alpha) = 0$, ellentmondás. Így azt kaptuk, hogy $m_{\alpha,K}$ valóban irreducibilis főpolinom, amelynek gyöke $\alpha$. Ekkor $K(\alpha) : K$ véges testbővítés, és az $\alpha$ elem algebrai $K$ felett. Egyszerűen ellenőrizhető, hogy a

$$K[x]/(m_{\alpha,K}) \to K(\alpha),\ p + (m_{\alpha,K}) \mapsto p(\alpha)$$

leképezés izomorfizmus. □

Legyenek $K$ és $L$ olyan testek, amelyekre $L : K$ teljesül, valamint $\alpha \in L$ algebrai elem $K$ felett. Ekkor az 2.7. Tétel (b) részében kapott $m_{\alpha,K}$ polinomot az $\alpha$ elem **($K$ feletti) minimálpolinomjának** nevezzük. Az $\alpha$ **algebrai elem foka** minimálpolinomjának a foka, amit $\mathrm{gr}_K(\alpha)$-val jelölünk.

**2.8. Példa.** (a) *Legyen $\alpha = \sqrt[4]{2}$. Ekkor $\alpha$ gyöke az $x^4 - 2 \in \mathbb{Q}[x]$ polinomnak. Mivel az $x^4 - 2$ főpolinom irreducibilis $\mathbb{Q}$ felett, ezért $m_{\alpha,\mathbb{Q}} = x^4 - 2$. A $\mathbb{Q}(\sqrt{2})$ test felett azonban az $x^4 - 2$ polinom már nem irreducibilis, irreducibilis felbontása $\mathbb{Q}(\sqrt{2})[x]$-ben:*

$$x^4 - 2 = (x^2 - \sqrt{2}) \cdot (x^2 + \sqrt{2}).$$

*Ezért $m_{\alpha,\mathbb{Q}(\sqrt{2})} = x^2 - \sqrt{2}$.*

(b) Tekintsük az $\mathbb{R} : \mathbb{Q}$ testbővítést. Legyen $\alpha = \sqrt{2} + \sqrt{3} + \sqrt{5}$. Ekkor $m_{\alpha,\mathbb{Q}} = x^8 - 40x^6 + 352x^4 - 960x^2 + 576$. Így az $\alpha$ elem 8-adfokú $\mathbb{Q}$ felett, azaz $\mathrm{gr}_{\mathbb{Q}}(\alpha) = m^*_{\alpha,\mathbb{Q}} = 8$.

[8] **Tétel.** Legyen $D$ legalább kételemű integritástartomány és $K$ test. Ekkor bármely $\varphi\colon D \to K$ injektív (gyűrű) homomorfizmus egyértelműen kiterjeszthető egy $Q_D \to K$ injektív homomorfizmussá.

**2.9. Tétel.** *Legyen $L : K$ testbővítés, és $\alpha \in L$ algebrai elem $K$ felett. Ekkor tetszőleges $g \in K[x]$, $g \neq 0$ polinomra $g(\alpha) = 0$ pontosan akkor teljesül, ha $m_{\alpha,K} \mid g$ ($K[x]$-ben).*

*Bizonyítás.* Tegyük fel, hogy $m_{\alpha,K} \mid g$. Ekkor $g = m_{\alpha,K} \cdot h$ teljesül alkalmas $h \in K[x]$ polinomra. Így $g(\alpha) = m_{\alpha,K}(\alpha) \cdot h(\alpha) = 0$.

Tegyük fel, hogy $g(\alpha) = 0$. Ekkor $g \in \ker(\varepsilon_\alpha) = (m_{\alpha,K})$ miatt $m_{\alpha,K} \mid g$. Ezzel a tételt igazoltuk. □

**2.10. Tétel.** *Legyen $L : K$ testbővítés, és $\alpha \in L$. Ekkor az $\alpha$ elem pontosan akkor algebrai $K$ felett, ha $[K(\alpha) : K] < \infty$. Ha $\alpha$ algebrai elem $K$ felett, akkor $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$.*

*Bizonyítás.* Tegyük fel, hogy a $K(\alpha) : K$ testbővítés véges, azaz $[K(\alpha) : K] = n$ teljesül valamely $n$ természetes számra. Az $1, \alpha, \ldots, \alpha^n \in K(\alpha)$ vektorok lineárisan függő vektorrendszert alkotnak, mivel számuk $n + 1 > \dim_K K(\alpha) = n$. Így vannak olyan $a_0, \ldots, a_n \in K$ skalárok, amelyek nem mind 0-ák és amelyekre $a_n\alpha^n + \cdots + a_1\alpha + a_0 = 0$ teljesül. Ekkor $\alpha$ gyöke az $f = a_nx^n + \cdots + a_1x + a_0$ polinomnak. Mivel $f \neq 0$, ezért $\alpha$ algebrai elem $K$ felett.

Tegyük fel, hogy $\alpha$ algebrai elem $K$ felett. Ekkor az

$$\widehat{\varepsilon_\alpha} \colon K[x]/(m_{\alpha,K}) \to K(\alpha),\ f + (m_{\alpha,K}) \mapsto f(\alpha)$$

homomorfizmus izomorfizmus. Mivel tetszőleges $f \in K[x]$ polinomhoz pontosan egy olyan $h \in K[x]$, $h^* < (m_{\alpha,K})^*$ polinom van, amelyre $f + (m_{\alpha,K}) = h + (m_{\alpha,K})$, ezért $K(\alpha)$ tetszőleges eleme egyértelműen írható fel $h(\alpha)$ alakban, ahol $h^* < (m_{\alpha,K})^*$. Ez pedig azt jelenti, hogy a $K(\alpha)$ (mint $K$ feletti) vektortérnek bázisa az $1, \alpha, \ldots, \alpha^{n-1}$ vektorrendszer, ahol $n = (m_{\alpha,K})^*$. Azaz $[K(\alpha) : K]$ véges és $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$. □

**2.11. Tétel.** *Ha $L : K$ véges testbővítés és $\alpha \in L$, akkor $\alpha$ algebrai elem $K$ felett, és $\mathrm{gr}_K(\alpha)$ osztója $[L : K]$-nak.*

*Bizonyítás.* A Fokszámtételt (2.3. Tételt) alkalmazva a $K(\alpha) : K$, $L : K(\alpha)$ és $L : K$ testbővítésekre azt kapjuk, hogy a $K(\alpha) : K$ testbővítés véges, így a 2.10. Tétel szerint $\alpha$ algebrai elem $K$ felett, valamint

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K(\alpha)] \cdot \mathrm{gr}_K(\alpha),$$

azaz $\mathrm{gr}_K(\alpha) \mid [L : K]$. □

**2.12. Tétel.** *Legyen $L : K$ tetszőleges testbővítés, és $\alpha \in L$ algebrai elem $K$ felett, valamint legyen $k \in \mathbb{N}$. Ha a $\beta \in L$ elemre $\beta^k = \alpha$ teljesül, akkor $\beta$ is algebrai elem $K$ felett, és $\mathrm{gr}_K(\beta) \leqslant k \cdot \mathrm{gr}_K(\alpha)$.*

*Bizonyítás.* Legyen $m_{\alpha,K} = \sum_{t=0}^{n} a_t x^t \in K[x]$, és legyen $f = \sum_{k=0}^{n} a_t x^{kt}$. Ekkor $f(\beta) = 0$, és így a 2.9. Tétel szerint $m_{\beta,K} \mid f$. Azaz $m^*_{\beta,K} \leqslant f^* = k \cdot n = k \cdot m^*_{\alpha,K} = k \cdot \mathrm{gr}_K(\alpha)$. □

**2.13. Tétel.** *Legyenek $L : K$ és $M : L$ tetszőleges testbővítések, valamint legyen $\alpha \in M$ algebrai elem $K$ felett. Ekkor $\alpha$ algebrai elem $L$ felett is, és $\mathrm{gr}_L(\alpha) \leqslant \mathrm{gr}_K(\alpha)$.*

*Bizonyítás.* Mivel $m_{\alpha,K} \in K[x] \subseteq L[x]$, ezért az állítás nyilvánvalóan teljesül. □

**2.14. Tétel.** *Legyenek $K$ és $L$ olyan testek, amelyekre $L : K$ teljesül, valamint legyen $\alpha, \beta \in L$. Ekkor*

$$K(\alpha)(\beta) = K(\beta)(\alpha) = K(\alpha, \beta).$$

*Bizonyítás.* Mivel $\alpha, \beta \in K(\alpha)(\beta)$, ezért $K(\alpha, \beta) \subseteq K(\alpha)(\beta)$. A fordított irányú tartalmazás igazolásához válasszunk egy tetszőleges $\gamma$ elemet $K(\alpha)(\beta)$-ból. Ekkor az 2.6. Tétel szerint

$$\gamma = f(\beta) \cdot g(\beta)^{-1},$$

ahol $f, g \in K(\alpha)[x]$ és $g(\beta) \neq 0$, és így $f(\beta), g(\beta) \in K(\alpha, \beta)$ miatt $\gamma \in K(\alpha, \beta)$. Ezzel igazoltuk, hogy $K(\alpha)(\beta) \subseteq K(\alpha, \beta)$. Aminek következtében megkapjuk a hőn áhított $K(\alpha)(\beta) = K(\alpha, \beta)$ egyenlőséget. Az $\alpha$ és $\beta$ elemek szerepének felcserélésével a másik egyenlőséget is megkaphatjuk. □

**2.15. Tétel.** *Legyen $L : K$ tetszőleges testbővítés, és $\alpha, \beta \in L$ algebrai elemek $K$ felett. Ekkor $\alpha \pm \beta$, $\alpha\beta$, valamint $\beta \neq 0$ esetén $\alpha \cdot \beta^{-1}$ is algebrai elemek $K$ felett, melyek foka legfeljebb $\mathrm{gr}_K(\alpha) \cdot \mathrm{gr}_K(\beta)$.*

**2.16. Következmény.** *Legyen $L : K$ tetszőleges testbővítés. Ekkor az $L$ test $K$ felett algebrai elemei $L$ egy résztestét alkotják.*

Az 2.15. Tétel a több határozatlanrendszerre nézve szimmetrikus polinomok alaptételének segítségével egyszerűen igazolható.[9] A bizonyítást nem végezzük el, de az ötletet egy példán bemutatjuk.

**2.17. Példa.** *Legyen $\alpha_1 = \sqrt{2} + 1$ és $\beta_1 = \sqrt[3]{3}$. Ekkor legyen*

$$f = m_{\alpha_1,\mathbb{Q}} = x^2 - 2x - 1,$$
$$g = m_{\beta_1,\mathbb{Q}} = x^3 - 3.$$

*Az $f$ polinom másik gyöke $\alpha_2 = 1 - \sqrt{2}$, illetve a $g$ polinom másik két gyöke*

[9] Legyen $R$ tetszőleges egységelemes gyűrű, $f \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$ $(m, n \in \mathbb{N})$. Azt mondjuk, hogy az $f$ polinom szimmetrikus az $x_1, \ldots, x_m$ és $y_1, \ldots, y_n$ határozatlanrendszerekre, ha tetszőleges $\alpha \in S_m$, $\beta \in S_n$ permutációkra

$$f = f(x_{1\alpha}, \ldots, x_{m\alpha}, y_{1\beta}, \ldots, y_{n\beta}).$$

teljesül. Legyenek $\sigma_k^{(1)}$ $(k = 1, \ldots, m)$, illetve $\sigma_l^{(2)}$ $(l = 1, \ldots, n)$ az elemi szimmetrikus polinomok az $x_1, \ldots, x_m$, illetve $y_1, \ldots, y_n$ határozatlanrendszerekre vonatkozóan.

**Tétel.** *Ha az $f \in R[x_1, \ldots, x_m, y_1, \ldots, y_n]$ polinom szimmetrikus az $x_1, \ldots, x_m$ és $y_1, \ldots, y_n$ határozatlanrendszerekre vonatkozóan, akkor van olyan $h \in R[x_1, \ldots, x_m$ és $y_1, \ldots, y_n]$ polinom, hogy $f = h(\sigma_1^{(1)}, \ldots, \sigma_m^{(1)}, \sigma_1^{(2)}, \ldots, \sigma_n^{(2)})$.*

$\beta_2 = -\frac{\sqrt[3]{3}}{2} + i\frac{\sqrt[6]{3^5}}{2}$ *és* $\beta_3 = -\frac{\sqrt[3]{3}}{2} - i\frac{\sqrt[6]{3^5}}{2}$. *Legyen*

$$m_{\alpha_1+\beta_1} = \prod_{1\leqslant s\leqslant 2,\ 1\leqslant t\leqslant 3} (x - \alpha_s - \beta_t),$$

$$m_{\alpha_1\beta_1} = \prod_{1\leqslant s\leqslant 2,\ 1\leqslant t\leqslant 3} (x - \alpha_s\beta_t),$$

$$m_{\alpha_1/\beta_1} = \prod_{1\leqslant s\leqslant 2,\ 1\leqslant t\leqslant 3} (x - \alpha_s/\beta_t).$$

*Ekkor*

$$\begin{aligned} m_{\alpha_1+\beta_1} &= x^6 - 6x^5 + 9x^4 - 2x^3 + 9x^2 - 60x + 50 \in \mathbb{Q}[x], \\ m_{\alpha_1\beta_1} &= x^6 - 42x^3 - 9 \in \mathbb{Q}[x], \\ m_{\alpha_1/\beta_1} &= x^6 - \frac{14}{3}x^3 - \frac{1}{9} \in \mathbb{Q}[x]. \end{aligned}$$

*és az* $\alpha_1 + \beta_1$, $\alpha_1\beta_1$, $\alpha_1/\beta_1$ *számok rendre gyökei az* $m_{\alpha_1+\beta_1}$, $m_{\alpha_1\beta_1}$, $m_{\alpha_1/\beta_1}$ *polinomoknak, azaz mindegyik legfeljebb* 6*-odfokú algebrai elem* $\mathbb{Q}$ *felett.*

Tekintsük az $L : K$ testbővítést, és legyenek $\alpha, \beta \in L$ algebrai elemek $K$ felett. Azt mondjuk, hogy az $\alpha$ és $\beta$ elemek **konjugáltak**, ha $m_{\alpha,K} = m_{\beta,K}$.

Például a $\sqrt{2}$ és $-\sqrt{2}$ valós számok konjugáltak $\mathbb{Q}$ felett, mivel minimálpolinomjuk megegyezik ($m_{\sqrt{2},\mathbb{Q}} = m_{-\sqrt{2},\mathbb{Q}} = x^2 - 2$).

Most pedig vizsgáljuk meg, hogy hogyan lehet a minimálpolinomot törtek gyöktelenítésére felhasználni. Legyenek $\alpha, \beta \in \mathbb{C}$ algebrai elemek $\mathbb{Q}$ felett, ahol $\beta \neq 0$. Tekintsük az $\frac{\alpha}{\beta}$ törtet. Legyenek $m_{\beta,\mathbb{Q}}$ gyökei (multiplicitással): $\beta = \beta_1, \beta_2, \ldots, \beta_n$, ahol $n = (m_{\beta,\mathbb{Q}})^*$. Ekkor $\{\beta_1, \ldots, \beta_n\}$ éppen $\beta$ konjugáltjainak halmaza. Mivel $\beta_1 \cdots \beta_n$ éppen $m_{\beta,\mathbb{Q}}$ konstans tagja, ezért racionális szám. Így az

$$\frac{\alpha}{\beta} = \frac{\alpha\beta_2 \cdots \beta_n}{\beta_1 \cdots \beta_n}$$

tört nevezője már racionális szám.

Legyen $\alpha = 1$ és $\beta = \sqrt{2} + \sqrt[3]{5}$. Ekkor $\beta$ minimálpolinomja $\mathbb{Q}$ felett $m_{\beta,\mathbb{Q}} = x^6 - 6x^4 - 10x^3 + 12x^2 - 60x + 17$, melynek gyökei:

$$\begin{aligned} \beta_1 &= \sqrt{2} + \sqrt[3]{5}, \\ \beta_2 &= -\sqrt{2} + \sqrt[3]{5}, \\ \beta_3 &= \sqrt{2} - \frac{1}{2}\sqrt[3]{5} - \frac{1}{2}i\sqrt{3}\sqrt[3]{5}, \\ \beta_4 &= \sqrt{2} - \frac{1}{2}\sqrt[3]{5} + \frac{1}{2}i\sqrt{3}\sqrt[3]{5}, \\ \beta_5 &= -\sqrt{2} - \frac{1}{2}\sqrt[3]{5} - \frac{1}{2}i\sqrt{3}\sqrt[3]{5}, \\ \beta_6 &= -\sqrt{2} - \frac{1}{2}\sqrt[3]{5} + \frac{1}{2}i\sqrt{3}\sqrt[3]{5}. \end{aligned}$$

Így $\beta_1 \cdots \beta_6 = 17$,

$$\alpha\beta_2 \cdots \beta_6 = -2\sqrt{2}\sqrt[3]{5^2} + 10 - 5\sqrt{2}\sqrt[3]{5} + 5\sqrt[3]{5^2} - 4\sqrt{2} + 4\sqrt[3]{5}.$$

és

$$\frac{\alpha}{\beta} = \frac{-2\sqrt{2}\sqrt[3]{5^2} + 10 - 5\sqrt{2}\sqrt[3]{5} + 5\sqrt[3]{5^2} - 4\sqrt{2} + 4\sqrt[3]{5}}{17}.$$

A fenti példa mutatja, hogy a módszer csak elvileg egyszerű.

Maple-ben mindezt a `factor` vagy `rationalize` utasítással érhetjük el:

```
> restart:
> alpha:=1:  beta:=sqrt(2)+root[3](5):
> factor(alpha/beta);
```

$$\frac{5\,5^{(2/3)}}{17} - \frac{2\sqrt{2}\,5^{(2/3)}}{17} - \frac{5\,5^{(1/3)}\sqrt{2}}{17} + \frac{4\,5^{(1/3)}}{17} + \frac{10}{17} - \frac{4\sqrt{2}}{17}.$$

`> rationalize(`$\alpha/\beta$`);`

$$\frac{(5^{(1/3)} - \sqrt{2})(4 + 2\,5^{(2/3)} + 5\,5^{(1/3)})}{17}$$

A $z$ komplex számot **algebrai számnak** nevezzük, ha $z$ algebrai $\mathbb{Q}$ felett. A 2.16. Tétel szerint az algebrai számok a komplex számtest egy résztestét alkotják, melyet $\mathbb{A}$-val jelölünk.

Az alábbiakban az $\mathbb{R} : \mathbb{Q}$ bővítés transzcendens elemeinek történetét tekintjük át röviden.

- **1844** Joseph **Liouville**[10] megmutatja, hogy bizonyos valós számok, amelyeket ma Liouville-számoknak nevezünk, transzcendensek $\mathbb{Q}$ felett. Ilyen szám, például a $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$ összeg értéke.
- **1873** Charles **Hermite**[11] megmutatja, hogy az $e$ szám transzcendens.
- **1874** George **Cantor**[12] bebizonyítja, hogy azon valós számok halmazának számossága, amelyek algebraiak $\mathbb{Q}$ felett megszámlálhatóan végtelen. Mivel a valós számok halmaza nem megszámlálható, ezért a valós számok többsége transzcendens $\mathbb{Q}$ felett.
- **1882** Ferdinand **Lindemann**[13] igazolja, hogy a $\pi$ szám transzcendens $\mathbb{Q}$ felett.
- **1934** A. O. **Gelfond**[14] igazolja, hogy ha $\alpha, \beta \in \mathbb{R}$ olyan algebrai elemek $\mathbb{Q}$ felett, amelyekre $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ teljesül, akkor az $\alpha^{\beta}$ valós szám transzcendens $\mathbb{Q}$ felett. Tőle függetlenül 1935-ben Theodor Schneider is igazolja ugyanezt a tételt, amely így Gelfond–Schneder-tételként vonul be a matematikatörténetbe. (Például a $2^{\sqrt{2}}$ valós szám —az ún. Gelfond–Schneider konstans— transzcendens $\mathbb{Q}$ felett.)

[10] Joseph **Liuville** francia matematikus (1809. március 24., Saint-Omer – 1882. szeptember 8., Párizs). A matematika számos területén alkotott. Érdemes megjegyezni, hogy 1846-ban Liuville publikálta először Évariste Galois kéziratát, halála után 14 évvel.

[11] Charles **Hermite** francia matematikus (1822. december 24., Dieuze – 1901. január 14., Párizs)

[12] George Ferdinand Ludwig **Cantor** német matematikus (1845. március 3., Szentpétervár – 1918. január 6., Halle)

[13] Ferdinand von **Lindemann** német matematikus (1852. április 12., Hannover – 1939. március 1., München) A Hermite által kifejlesztett módszerekre alapozva bizonyította a $\pi$ valós szám transzcendens voltát, ezen eredményét 1882-ben az *Über die Zahl* $\pi$ cikkben publikálta.

[14] Alexander Osipovich **Gelfond** orosz matematikus (1906. október 24., Szentpétervár – 1968. november 7., Moszkva)

Azt eldönteni, hogy egy adott valós szám transzcendens-e, általában nagyon bonyolult, amint azt a következő problémák is mutatják.

- Igaz-e, hogy $e + \pi$ transzcendens $\mathbb{Q}$ felett?
- Igaz-e, hogy a $\gamma = \lim_{n\to\infty} \left(\sum_{k=1}^{n} \frac{1}{k} - \ln n\right) \approx 0.577215664901$ transzcendens $\mathbb{Q}$ felett?
- Igaz-e, hogy $\zeta(3) = \sum_{n=1}^{\infty} \frac{1}{n^3}$ transzcendens $\mathbb{Q}$ felett? Roger **Apéry**[15] 1978-ban bizonyította be, hogy $\zeta(3)$ irracionális.

## 2.3 Algebrai testbővítések

Azt mondjuk, hogy az $L : K$ testbővítés **algebrai testbővítés**, ha $L$ minden eleme algebrai $K$ felett.

**2.18. Tétel.** *Legyen $L : K$ tetszőleges testbővítés. Ekkor a következők ekvivalensek:*

(1) $[L : K] < \infty$*;*

(2) *az $L : K$ bővítés algebrai, és $L$ végesen generált $K$ felett;*

(3) $L = K(\alpha_1, \ldots, \alpha_n)$*, ahol $\alpha_1, \ldots, \alpha_n \in L$ algebrai elemek $K$ felett.*

*Bizonyítás.* (1) $\Longrightarrow$ (2): legyen $[L : K] = n$, és $\alpha_1, \ldots, \alpha_n \in L$ az $L$ vektortér bázisa. Ekkor $L = [\alpha_1, \ldots, \alpha_n]$ miatt $L = K(\alpha_1, \ldots, \alpha_n)$, azaz $L$ végesen generált. Legyen $\alpha$ az $L$ test tetszőleges eleme. Ekkor a 2.3. Tétel szerint a $K(\alpha) : K$ testbővítés végesfokú, így a 2.10. Tétel következtében $\alpha$ algebrai elem $K$ felett. Ezért az $L : K$ testbővítés algebrai.

(2) $\Longrightarrow$ (3): Az állítás triviálisan teljesül.

(3) $\Longrightarrow$ (1): Definiáljuk az $L_0$ $(1 \leqslant i \leqslant n)$ testeseket a következőképpen:

$$L_0 = K, \qquad L_i = L_{i-1}(\alpha_i) \quad (1 \leqslant i \leqslant n).$$

Mivel $\alpha_i \in L$ algebrai elem $K$ felett, ezért $\alpha_i$ algebrai elem $L_{i-1}$ felett is, így a 2.10. Tétel szerint

$$[L_i : L_{i-1}] = [L_{i-1}(\alpha_i) : L_{i-1}] < \infty.$$

Ekkor az 2.4. Következményt alkalmazva azt kapjuk, hogy

$$[L : K] = [L_n : L_0] = \prod_{i=1}^{n} [L_i : L_{i-1}] < \infty.$$

Ezzel a tétel bizonyítását befejeztük. □

**2.19. Következmény.** *Ha $\alpha \in L$ az $L : K$ bővítés algebrai eleme, akkor a $K(\alpha) : K$ bővítés algebrai.*

[15] Roger **Apéry** francia matematikus (1916. november 14., Rouen – 1994. december 18., Caen)

**2.20. Következmény.** *Legyen $L : K$ testbővítés, és $S \subseteq L$. Ha $S$ minden eleme algebrai $K$ felett, akkor a $K(S) : K$ bővítés algebrai.*

*Bizonyítás.* Legyen $\alpha$ tetszőleges eleme a $K(S)$ testnek. Ekkor van olyan véges $S'$ részhalmaza $S$-nek, amelyre $\alpha \in K(S')$ teljesül. Ekkor a 2.18. Tétel szerint a $K(S')$ bővítés algebrai, így $\alpha$ is algebrai elem $K$ felett. Azaz a $K(S) : K$ bővítés algebrai. □

**2.21. Tétel.** *Ha az $M : L$ és $L : K$ testbővítések algebraiak, akkor az $M : K$ bővítés is algebrai.*

*Bizonyítás.* Legyen $\alpha$ tetszőleges eleme $M$-nek. Mivel az $M : L$ bővítés algebrai, ezért $\alpha$ algebrai elem $L$ felett. Legyen $m_{\alpha,L} = \sum_{i=0}^{n} \lambda_i x^i$. Definiáljuk a $K_0, \ldots, K_n$ testeket a következő módon:

$$K_0 = K, \qquad K_i = K_{i-1}(\lambda_i) \quad (1 \leqslant i \leqslant n).$$

Mivel $\lambda_i$ algebrai elem $K$ felett, ezért a $K_i : K_{i-1}$ bővítések végesek $(1 \leqslant i \leqslant n)$. Így a 2.4. Következmény szerint a $K_n : K$ bővítés is véges. Tekintsük a $K_n(\alpha) : K$ bővítést. Mivel $\alpha$ algebrai elem $K_n$ felett $(f \in K_n[x])$, ezért $K_n(\alpha) : K_n$ véges. Így ismét a Fokszámtételt alkalmazva, azt kapjuk, hogy

$$[K_n(\alpha) : K] = [K_n(\alpha) : K_n] \cdot [K_n : K] < \infty,$$

azaz $\alpha$ a $K$ test felett is algebrai elem. □

**2.22. Tétel.** *Legyen $L : K$ algebrai bővítés, és legyen $\tau \colon L \to L$ olyan injektív homomorfizmus, amelyre $\tau(a) = a$ teljesül minden $a \in K$-ra. Ekkor $\tau$ izomorfizmus.*

*Bizonyítás.* Mivel $\tau$ homomorfizmus, ezért $\tau(0) = 0$. Legyen $\alpha \neq 0$ tetszőleges eleme $L$-nek, és legyen $R$ az $m_{\alpha,K}$ polinom $L$-beli gyökeinek halmaza. Ekkor tetszőleges $\beta \in R$-re

$$m_{\alpha,K}(\tau(\beta)) = \tau(m_{\alpha,K}(\beta)) = \tau(0) = 0,$$

azaz $\tau(R) \subseteq R$. Mivel $\tau$ injektív és $R$ véges, ezért $\tau(R) = R$. Így van olyan $\beta \in R$, amelyre $\tau(\beta) = \alpha$ teljesül. Azaz $\tau$ szürjektív is. □

# Polinomok irreducibilitása

## 3.1 Irreducibilis polinomok

**3.1. Tétel (L. Kronecker).** *Tetszőleges egész együtthatós polinom véges sok lépésben felbontható $\mathbb{Z}$ felett irreducibilis polinomok szorzatára.*

Kronecker[16] tételét nem bizonyítjuk, de az alábbi példa segítségével a bizonyítás és az algoritmus is könnyen kitalálható.

**3.2. Példa.** *Legyen $f = x^5 - x^4 + 8x^3 + 12x + 16$. Ha $f$ nem irreducibilis $\mathbb{Z}[x]$-ben, akkor vannak olyan $g, h \in \mathbb{Z}[x]$ polinomok, amelyekre $f = gh$ teljesül és $1 \leqslant g^* \leqslant h^* < 4$. Ekkor természetesen $g^* \leqslant 2$ is teljesül, azaz $f$-nek legfeljebb másodfokú osztója is van. Rögzítsük az $a_1 = -1$, $a_2 = 0$ és $a_3 = 1$ értékeket. Mivel $f(a_k) = g(a_k)h(a_k)$, ezért $g(a_k) \mid f(a_k)$ teljesül minden $k$-ra $(k = 1, 2, 3)$, azaz $g(-1) \mid f(-1) = -6$, $g(0) \mid f(0) = 16$ és $g(1) \mid f(1) = 36$. Így*

$$\begin{aligned} g(-1) &\in \{\pm 6, \pm 3, \pm 2, \pm 1\}, \\ g(0) &\in \{\pm 16, \pm 8, \pm 4, \pm 2, \pm 1\}, \\ g(1) &\in \{\pm 36, \pm 18, \pm 12, \pm 9, \pm 6, \pm 4, \pm 3, \pm 2, \pm 1\}, \end{aligned}$$

*azaz a $(g(-1), g(0), g(1)) \in \mathbb{Z}^3$ hármasokra csak véges sok lehetőség van. Mivel $g$ legfeljebb másodfokú, ezért Lagrange[17] interpolációs tétele[18] szerint három különböző helyen felvett értéke már meghatározza (mint $\mathbb{Q} \to \mathbb{Q}$ leképezést).*
*1. eset: $g(-1) = -3$, $g(0) = -4$ és $g(1) = -9$. Ekkor $g = -2x^2 - 3x - 4 \in \mathbb{Z}[x]$, de $g \nmid f$.*

$\vdots$

*17. eset: $g(-1) = -6$, $g(0) = -4$ és $g(1) = 1$. Ekkor $g = \frac{3}{2}x^2 + \frac{7}{2}x - 4 \notin \mathbb{Z}[x]$, így $g \mid f$ biztosan nem teljesülhet.*

$\vdots$

*571. eset: $g(-1) = 1$, $g(0) = -4$ és $g(1) = -9$. Ekkor $g = -5x - 4 \in \mathbb{Z}[x]$, de $g \mid f$ nem teljesül.*

$\vdots$

[16] Leopold **Kronecker** német matematikus (1823. december 7., Liegnitz – 1891. december 29., Berlin) „Die ganzen Zahlen hat der liebe Gott gemacht, alles andere ist Menschenwerk.", azaz „Isten teremtette az egész számokat; minden egyéb az ember műve."

[17] (gróf) Joseph-Luis **Lagrange** olasz születésű francia matematikus (1736. január 25., Torinó – 1813. április 10, Párizs), eredeti olasz neve Giuseppe Luigi Lagrangia.

[18] **Lagrange interpolációs tétele**. Legyen $K$ számtest, $n$ természetes szám, valamint $a_1, \ldots, a_{n+1}$ páronként különböző és $b_1, \ldots, b_{n+1}$ tetszőleges $K$-beli elemek. Ekkor pontosan egy olyan legfeljebb $n$-edfokú $K$ feletti $f$ polinom létezik, amelyre $f(a_k) = b_k$ teljesül minden $k$-ra $(1 \leqslant k \leqslant n + 1)$.

*1440. eset:* $g(-1) = 6$, $g(0) = 4$ *és* $g(1) = 4$. *Ekkor* $g = x^2 - x + 4 \in \mathbb{Z}[x]$ *és végre* $g \mid f$ *is teljesül:* $f = (x^2 - x + 4)(x^3 + 4x + 4)$.
*Most már csak azt kell megvizsgálni, hogy a kapott polinomok tovább bonthatók-e.*

Legyen $D$ integritástartomány[19], valamint $f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$ tetszőleges polinom. Azt mondjuk, hogy az $f$ polinom **primitív**, ha az $a_0, \ldots, a_n$ együtthatók relatív prímek. Nagyon érdekes az alábbi Gauss-tól[20] származó tétel.

**3.3. Tétel (C. F. Gauss).** *Legyen* $f$ *legalább elsőfokú, egész együtthatós primitív polinom. Az* $f$ *polinom akkor és csak akkor irreducibilis* $\mathbb{Z}$ *felett, ha irreducibilis* $\mathbb{Q}$ *felett.*

## 3.2 A Schönemann–Eisenstein-féle kritérium

Polinomok irreducibilitásának vizsgálata nehezen képzelhető el Schönemann[21] és Eisenstein[22] alábbi tétele nélkül.

**3.4. Tétel (Schönemann–Eisenstein-tétel).** *Legyen*

$$f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$$

*legalább elsőfokú primitív polinom. Ha létezik olyan* $p$ *prímszám, amelyre* $p \mid a_0, \ldots, a_{n-1}$, *de* $p \nmid a_n$ *és* $p^2 \nmid a_0$, *akkor* $f$ *irreducibilis* $\mathbb{Z}$ *felett.*

Számos esetben jól alkalmazható tesztet kapunk, ha nem csak az $f$ polinomot, de annak az „eltoltjait" is vizsgáljuk. Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ekkor tetszőleges $s$ egész számra az $f_{\to s} = a_n(x-s)^n + \cdots + a_1(x-s) + a_0$ polinomot az $f$ polinom **$s$-eltoltjának** nevezzük.

**3.5. Tétel.** *Legyen* $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$, *és* $s \in \mathbb{Z}$. *Ekkor az* $f$ *polinom pontosan akkor irreducibilis* $\mathbb{Z}$ *felett, ha* $f_{\to s}$ *az.*

Tekintsük az $f = x^5 - 7x^4 + 24x^3 - 42x^2 + 39x - 25 \in \mathbb{Z}[x]$ polinomot. Erre a polinomra nem alkalmazható a Schönemann–Eisenstein-tétel. Tekintsük azonban az

$$\begin{aligned} f_{\to -1} &= (x+1)^5 - 7(x+1)^4 + 24(x+1)^3 - 42(x+1)^2 + 39(x+1) - 25 \\ &= x^5 - 2x^4 + 6x^3 - 2x^2 + 4x - 10 \end{aligned}$$

polinomot. Ez a polinom primitív, és a Schönemann–Eisenstein-tételt a $p = 2$ választással alkalmazva kapjuk, hogy irreducibilis. Így a 3.5. Tétel szerint az $f$ polinom is irreducibilis. A megfelelő eltolt megtalálása azonban nem egyszerű feladat, sőt nem is létezik megfelelő eltolt.

A 3.4. Tétel általánosabban is megfogalmazható, amint azt az alábbi tétel mutatja.

[19] Azaz $D$ kommutatív, egységelemes és zérusosztómentes.
[20] Carl Friedrich **Gauss** német matematikus (1777. április 30., Braunschweig – 1855. február 23., Göttingen) A matematikusok „fejedelme".
[21] T. **Schönemann** (1812-1868) brandenburgi gimnáziumi tanár volt.
[22] Ferdinand Gotthold Max **Eisenstein** német matematikus (1823. április 16., Berlin – 1852. október 11., Berlin)

**3.6. Tétel.** *Legyen $D$ integritástartomány és*

$$f = a_n x^n + \cdots + a_1 x + a_0 \in D[x]$$

*legalább elsőfokú primitív polinom. Ha létezik olyan $p \in D$ prímelem, amelyre $p \mid a_0, \ldots, a_{n-1}$, de $p \nmid a_n$ és $p^2 \nmid a_0$, akkor $f$ irreducibilis $D[x]$-ben.*

## 3.3 Egyéb tesztek az irreducibilitás eldöntésére

Michael Rolle[23] alábbi tétele szerint egy egész együtthatós polinom racionális gyökeit mindig megtalákhatjuk véges sok lépésben.

**3.7. Tétel (Rolle-tétel).** *Legyen $f = \sum_{k=0}^{n} a_k x^k \in \mathbb{Z}[x]$ tetszőleges polinom. Ha $\frac{p}{q} \in \mathbb{Q}$ tört, ahol* ln.k.o.$(p, q) = 1$, *gyöke $f$-nek, akkor $q \mid a_n$ és $p \mid a_0$. Továbbá bármely $m$ egész számra $p + mq \mid f(-m)$ is teljesül.*

**3.8. Következmény.** (a) *Az $f \in \mathbb{Z}[x]$ polinom racionális gyökei véges sok lépésben megtalálhatók.*
(b) *Ha az $f \in \mathbb{Z}[x]$ polinom főegyütthatója 1, akkor $f$ minden racionális gyöke egész szám.*

**3.9. Tétel.** *Legyen $K$ test, és $f \in K[x]$ másod- vagy harmadfokú polinom. Ekkor $f$ pontosan akkor irreducibilis $K$ felett, ha nincs gyöke $K$-ban.*

**3.10. Tétel.** *Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ olyan egész együtthatós primitív polinom. Legyen $p$ olyan prímszám, amely nem osztja $a_n$-et. Ha $\overline{f} = \overline{a_n} x^n + \cdots + \overline{a_1} x + \overline{a_0} \in \mathbb{Z}_p[x]$ irreducibilis $\mathbb{Z}_p$ felett, akkor $f$ irreducibilis $\mathbb{Z}$ felett.*

[23] Michael **Rolle** (1652. április 21., Ambert, Bass-Auvergne, Franciaország – 1719. november 8., Párizs) francia matematikus. Nevét elsősorban az analízisbeli Rolle-tétel őrizte meg, de azt is meg kell jegyezni, hogy Rolle vezette be az $\sqrt[n]{x}$ jelölést is.

# Polinomok felbontási teste

Ezen fejezet célja annak megmutatása, hogy tetszőleges $K$ test feletti $f$ polinom esetén van olyan $L$ testbővítése $K$-nak, amely felett már $f$ elsőfokú polinomok szorzatára bontható. Megmutatjuk, hogy az ilyen tulajdonságú testek lényegében egyértelműek.

## 4.1 Polinomok felbontási teste

Legyen $K$ test, és $f \in K[x]$ tetszőleges polinom. Azt mondjuk, hogy a $K$ test $L$ bővítése **felbontási teste $f$-nek $K$ felett**, ha $f$ elsőfokú tényezők szorzatára bontható $L$ felett, azaz vannak olyan $\alpha_1, \ldots, \alpha_r \in L$ és $\lambda \in K$ elemek, amelyekre

$$f = \lambda(x - \alpha_1) \cdots (x - \alpha_r)$$

teljesül $L[x]$-ben, és $L = K(\alpha_1, \ldots, \alpha_r)$.

Legyen $K_0 = K$ és $K_i = K(\alpha_1, \ldots, \alpha_i)$ $(i = 1, \ldots, r)$. Ekkor a $K_{i+1} : K_i$ testbővítések minden $i \in \{1, \ldots, r-1\}$-re végesek (legfeljebb $n$-edfokúak), így a $K_r : K_0 = L : K$ testbővítés is véges. Azaz, ha $L$ felbontási teste az $f \in K[x]$ polinomnak a $K$ test felett, akkor az $L : K$ testbővítés véges algebrai bővítés.

A következő tétel pedig éppen az állítja, hogy a felbontási test mindig létezik.[24]

**4.1. Tétel.** *Legyen $K$ test, és $f$ $n$-edfokú $(n \in \mathbb{N})$ polinom $K$ felett. Ekkor $f$-nek van felbontási teste $K$ felett, és az $f$ polinom tetszőleges $K$ feletti $L$ felbontási testére $[L : K] \leqslant n!$ teljesül.*

*Bizonyítás.* Az állítást az $f$ polinom fokszáma szerinti indukcióval bizonyítjuk. Ha $f^* \leqslant 1$, akkor az állítás nyilvánvalóan teljesül. Tegyük fel, hogy az állítás igaz tetszőleges $K$ testre és tetszőleges $K$ feletti legfeljebb $(n-1)$-edfokú polinomra. Legyen $f$ egy $n$-edfokú polinom. A továbbiakban a bizonyítás két esetre bomlik aszerint, hogy $f$ reducibilis vagy irreducibilis $K$ felett.

*1. eset.* Ha $f$ reducibilis $K[x]$-ben, akkor $f = gh$ teljesül valamely $g, h \in K[x]$ polinomokra, ahol $1 \leqslant g^* = s$, $h^* = t \leqslant n-1$. Az indukciós feltevés szerint van a $K$ testnek egy olyan $L$ bővítése, amely felbontási teste az $g$ polinomnak és $[L : K] \leqslant s!$. Ekkor

$$g = \lambda(x - \alpha_1) \cdots (x - \alpha_s),$$

ahol $\alpha_1, \ldots, \alpha_s \in L$, $\lambda \in K$ és $L = K(\alpha_1, \ldots, \alpha_s)$. Tekintsük a $h \in K[x] \subseteq L[x]$ polinomot. Szintén az indukciós feltevés szerint van az $L$ testnek egy olyan $M$

[24] Amennyiben $K$ számtest, azaz $K \leqslant \mathbb{C}$, akkor a felbontási test létezése következik az Algebra Alaptételéből. Ha $f \in K[x]$, akkor az Algebra Alaptétele szerint $f$-nek (multiplicitással számolva) pontosan $f^*$ darab gyöke van $\mathbb{C}$-ben, ha $f$ gyökei $\alpha_1, \ldots, \alpha_n \in \mathbb{C}$, akkor $K(\alpha_1, \ldots, \alpha_n) \leqslant \mathbb{C}$ felbontási teste az $f$ polinomnak a $K$ test felett.

Az Algebra Alaptétele azt állítja, hogy tetszőleges $f \in \mathbb{C}[x]$ polinomnak van komplex gyöke.

bővítése, amely felbontási teste a $h$ polinomnak az $L$ test felett és $[M : L] \leqslant t!$. Ekkor

$$h = \mu(x - \beta_1) \cdots (x - \beta_t),$$

ahol $\beta_1, \ldots, \beta_t \in M$, $\mu \in L$ és $M = L(\beta_1, \ldots, \beta_t)$. Ekkor

$$f = gh = \lambda\mu(x - \alpha_1) \cdots (x - \alpha_s)(x - \beta_1) \cdots (x - \beta_t)$$

miatt $\lambda\mu \in K$, továbbá $M = K(\alpha_1, \ldots, \alpha_s, \beta_1, \ldots, \beta_t)$, azaz $M$ felbontási teste $f$-nek $K$ felett. Valamint, a Fokszámtétel (2.3. Tétel) miatt az

$$[M : K] = [M : L] \cdot [L : K] \leqslant t!s! \leqslant (s + t)! \leqslant n!$$

egyenlőtlenség is teljesül.

*2. eset.* Ha $f$ irreducibilis $K$ felett, akkor tekintsük a $K$ test $L = K[x]/(f)$ bővítését. Tudjuk, hogy $\alpha = x + (f) \in L$ gyöke $f$-nek, $L = K(\alpha)$ és $[L : K] = n$. A Bézout-tétel szerint $f = (x - \alpha)h$ teljesül valamely $(n - 1)$-edfokú $h \in L[x]$ polinomra. Alkalmazzuk az indukciós feltevést $h$-ra: az $L$ testnek van egy olyan $M$ testbővítése, mely felbontási teste $h$-nak $L$ felett és $[M : L] \leqslant (n-1)!$. Ekkor

$$h = \mu(x - \beta_1) \cdots (x - \beta_{n-1}),$$

ahol $\beta_1, \ldots, \beta_{n-1} \in M$, $\mu \in L$ és $M = L(\beta_1, \ldots, \beta_{n-1})$. Ezért azt kapjuk, hogy

$$f = \mu(x - \alpha)(x - \beta_1) \cdots (x - \beta_{n-1})$$

miatt $\mu \in K$, továbbá $M = L(\beta_1, \ldots, \beta_{n-1}) = K(\alpha, \beta_1, \ldots, \beta_{n-1})$, azaz $M$ felbontási teste $f$-nek $K$ felett. Végül a Fokszámtétel következtében

$$[M : K] = [M : L] \cdot [L : K] \leqslant (n - 1)! \cdot n = n!$$

is teljesül.

Ezzel a tétel bizonyítását befejeztük. □

**4.2. Példa.** *Legyen $f = x^4 + 2x^2 + 2 \in \mathbb{Q}[x]$ polinomot. Az $f$ polinom a Schönemann–Eisenstein-tétel következtében irreducibilis $\mathbb{Q}$ felett. Az $f$ polinom gyökei $\mathbb{C}$-ben:*

$$\mu\alpha + \nu i\beta,$$

*ahol $\alpha = \dfrac{\sqrt{-2 + 2\sqrt{2}}}{2}$, $\beta = \dfrac{\sqrt{2 + 2\sqrt{2}}}{2}$ és $\mu, \nu \in \{-1, 1\}$. Így az $f$ polinom felbontási teste*

$$\begin{aligned} L &= \mathbb{Q}(\alpha + i\beta, \alpha - i\beta, -\alpha + i\beta, -\alpha - i\beta) \\ &= \mathbb{Q}(\alpha, \beta, i). \end{aligned}$$

*Sőt, az is igaz, hogy $L = \mathbb{Q}(\alpha + i)$.*

## 4.2 Injektív homomorfizmusok kiterjesztése

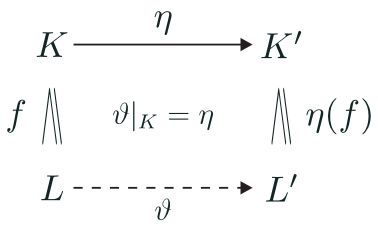
Most pedig azt mutatjuk meg, hogy a felbontási test lényegében egyértelmű, azaz ha $L$ és $L'$ is felbontás teste az $f \in K[x]$ polinomnak, akkor van olyan $L \to L'$ izomorfizmus, amely $K$ elemeit fixen hagyja.

Legyenek $K_1$ és $K_2$ testek, valamint $\eta\colon K_1 \to K_2$ izomorfizmus. Tetszőleges $f = \sum_{i=0}^{n} a_i x^i \in K_1[x]$ polinomra legyen

$$\eta(f) = \sum_{i=0}^{n} (a_i\eta) x^i \in K_2[x].$$

Egyszerűen igazolható, hogy a $K_1[x] \to K_2[x],\ f \mapsto \eta(f)$ leképezés izomorfizmus.

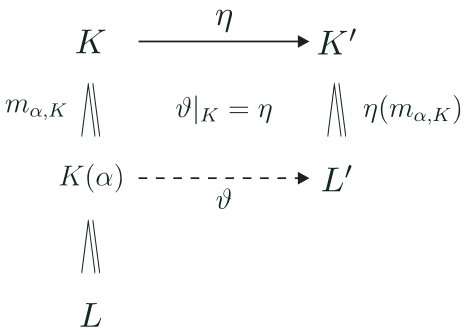
**4.3. Tétel.** *Legyenek $K, K'$ testek, $\eta\colon K \to K'$ izomorfizmus, és $f \in K[x]$ egy $n$-edfokú polinom ($n \geqslant 1$). Legyenek továbbá rendre $L$, illetve $L'$ az $f$, illetve $\eta_f$ polinomok felbontási testei a $K$, illetve $K'$ testek felett. Ekkor $\eta$ kiterjeszthető egy $L \to L'$ izomorfizmussá. Továbbá, az $\eta$ izomorfizmust legfeljebb $[L : K]$ féleképpen tudjuk kiterjeszteni; a kiterjesztések száma pontosan $[L : K]$, ha $\eta(f)$ gyökei páronként különbözőek $L'$-ben.*




**5. ábra:** Az $\eta$ izomorfizmus kiterjesztése izomorfizmussá.

A 4.3. Tétel bizonyításához az alábbi lemmát fogjuk felhasználni.

**4.4. Lemma (Kiterjesztési Lemma).** *Legyenek $K$ és $K'$ testek, $\eta\colon K \to K'$ izomorfizmus, amelyekre $L : K$, $L' : K'$ teljesül. Tegyük fel, hogy az $\alpha \in L$ elem algebrai $K$ felett, és legyen $f = m_{\alpha,K} \in K[x]$. Ekkor $\eta$ pontosan akkor terjeszthető ki egy $\vartheta\colon K(\alpha) \to L'$ injektív homomorfizmussá, ha $\eta(f)$-nek van gyöke $L'$-ben, és ebben az esetben $\eta$-t annyiféleképpen tudjuk kiterjeszteni ahány gyöke van $\eta(f)$-nek $L'$-ben.*




**6. ábra:** Az $\eta$ izomorfizmus kiterjesztése injektív homomorfizmussá.

*A 4.4. Lemma bizonyítása.* Tegyük fel, hogy $\vartheta\colon K(\alpha) \to L$ injektív homomorfizmus, amely kiterjesztése $\eta$-nak. Ekkor

$$\eta(f)(\vartheta(\alpha)) = \vartheta(f(\alpha)) = \vartheta(0) = 0,$$

azaz $\vartheta(\alpha) \in L'$ gyöke $\eta(f)$-nek.

Tegyük fel, hogy $\omega \in L'$ gyöke $\eta(f)$-nek. Tekintsük a

$$\kappa\colon K[x] \to L',\ h \mapsto \eta(h)(\omega)$$

homomorfizmust. Mivel $\kappa(f) = \eta(f)(\omega) = 0$, ezért $(f) \subseteq \ker(\kappa)$, és így $\kappa$ indukál egy

$$\widehat{\kappa}\colon K[x]/(f) \to L',\ h + (f) \mapsto \eta(h)(\omega)$$

homomorfizmust. Mivel $K[x]/(f)$ test ($f$ irreducibilis), ezért $\widehat{\kappa}$ injektív homomorfizmus. Legyen

$$\vartheta = \widehat{\kappa} \circ (\widehat{\varepsilon_\alpha})^{-1}\colon K(\alpha) \to L',\ h(\alpha) \mapsto \eta(h)(\omega).$$

Ekkor $\vartheta$ injektív homomorfizmus, valamint tetszőleges $u \in K$-ra

$$\vartheta(u) = \widehat{\kappa}((\widehat{\varepsilon_\alpha})^{-1}(u)) = \widehat{\kappa}(u + (f)) = \eta(u)(\omega) = \eta(u),$$

azaz $\vartheta$ kiterjesztése $\eta$-nak. Abból a tényből, hogy $K \cup \{\alpha\}$ generálja a $K(\alpha)$ testet következik, hogy a fent definiált $\vartheta$ az egyetlen olyan injektív homomorfizmus, amelyre $\vartheta(\alpha) = \omega$ teljesül. Így már az is világos, hogy $\eta$ annyiféleképpen terjeszthető ki injektív homomorfizmussá, ahány gyöke van $\eta(f)$-nek $L'$-ben. □

*A 4.3. Tétel bizonyítása.* Az állítást $[L : K]$-ra vonatkozó indukcióval bizonyítjuk. Ha $[L : K] = 1$, akkor $L = K$ és $f = \lambda(x - \alpha_1) \cdots (x - \alpha_n)$, ahol $\lambda, \alpha_1, \ldots, \alpha_n \in K$. Ekkor $\eta(f) = \eta(\lambda)(x - \eta(\alpha_1)) \cdots (x - \eta(\alpha_n))$ teljesül $K'[x]$-ben, így $L' = K'$ és $\eta$-nak pontosan egy kiterjesztése van.

Tegyük fel, hogy $[L : K] > 1$, azaz $f$ nem bomlik fel lineáris tényezők szorzatára $K$ felett. Legyen $g$ egy legalább elsőfokú irreducibilis főpolinom, amely osztója $f$-nek $K[x]$-ben. Ekkor $g \mid f$ miatt $\eta(g)$ osztója $\eta(f)$-nek. Az általánosság megszorítása nélkül feltehető, hogy

$$\begin{aligned} f &= \lambda(x - \alpha_1) \cdots (x - \alpha_n), \\ \eta(f) &= \kappa(x - \omega_1) \cdots (x - \omega_n), \\ g &= \mu(x - \alpha_1) \cdots (x - \alpha_m), \\ \eta(g) &= \nu(x - \omega_1) \cdots (x - \omega_m). \end{aligned}$$

Legyen $M = K(\alpha_1)$. Mivel $g$ irreducibilis $K$ felett, ezért $m_{\alpha_1,K} = g$, és $[M : K] = g^* = m$. A 4.4. Lemma szerint $\eta$-nak pontosan $k$ kiterjesztése van $M \to L'$ injektív homomorfizmussá: $\vartheta_1, \ldots, \vartheta_k$, ahol $k = |\{\omega_1, \ldots, \omega_m\}|$. Világos, hogy $L$ felbontási teste $M$ felett az $f \in M[x]$ polinomnak és $L'$ felbontási teste a $\vartheta_i(M)$ test felett az $\eta(f)$ polinomnak ($1 \leqslant i \leqslant k$). Mivel $[L : M] = [L : K]/[M : K] = [L : K]/m < [L : K]$, ezért az indukciós feltevés alkalmazva azt kapjuk, hogy $\vartheta_i$ kiterjeszthető egy $L \to L'$ izomorfizmussá, és ezen kiterjesztések száma $\leqslant [L : M]$ (egyenlőség pontosan akkor van, ha $\eta(f)$ gyökei páronként különbözők $L'$-ben). Mivel ezen izomorfizmusok mindegyike az $\eta$-nak is kiterjesztése, ezért ezen a módon $\eta$-nak legfeljebb $k \cdot [L : M] \leqslant m \cdot [L : M] = [L : K]$ kiterjesztését kapjuk (pontosan $[L : K]$ kiterjesztést kapunk, ha $\eta(f)$ gyökei páronként különbözők). A bizonyítás befejezéséhez csak azt kell meggondolnunk, hogy $\eta$-nak más kiterjesztései nem is lehetnek. Tegyük fel, hogy a $\vartheta\colon L \to L'$ izomorfizmus kiterjesztése $\eta$-nak. Ekkor $\vartheta|_M$ egy $M \to L'$ injektív homomorfizmus, azaz $\vartheta = \vartheta_i$ valamely $i$-re ($1 \leqslant i \leqslant k$), és így a $\vartheta$ izomorfizmus is a fenti módon keletkezik. □

Vizsgáljuk meg azt az esetet, amikor a 4.3. Tételben $K = K'$ teljesül, és $\eta = \mathrm{id}_K$. Ekkor $\eta(f) = f$, és a következő tételt kapjuk.

**4.5. Tétel.** *Legyen $K$ tetszőleges test, $f \in K[x]$, és $L, L'$ az $f$ polinom felbontási testei. Ekkor az $L$ és $L'$ testek izomorfak, sőt olyan $L \to L'$ izomorfizmus is van, amely a $K(\subseteq L, L')$ test elemeit fixen hagyja. Továbbá, pontosan annyi a $K$ test elemeit fixen hagyó $L \to L'$ izomorfizmus van ahány különböző gyöke van $f$-nek $L$-ben.*

# Szeparábilitás

Bizonyos testek esetén előfordulhat, hogy van olyan a test felett irreducibilis polinom, amelyeknek van többszörös gyöke a test feletti felbontási testében, azaz a polinom nem szeparábilis. Ezen fejezetet a szeparábilitás vizsgálatának szenteljük.

Testbővítések egyik fontos tulajdonsága —a később sorra kerülő normalitás mellett— a szeparábilitás. E tulajdonság hiányában számos technikai nehézséggel kerülhetünk szembe. Azonban meg kell jegyezni, hogy nem is olyan egyszerű nem szeparábilis polinomra példát mutatni. A későbbiekben látni fogjuk, hogy számtestek (általában 0 karakterisztikájú testek) minden testbővítése szeparábilis.

## 5.1 Alapvető fogalmak

Legyenek $K$ és $L$ olyan testek, amelyre $L : K$ teljesül. Az $f \in K[x]$ irreducibilis polinom **szeparábilis**, ha $f$-nek $f^*$ különböző gyöke van bármely ($K$ feletti) felbontási testében, azaz $f$ valamennyi gyöke egyszeres. Az $f$ polinomot **inszeparábilis** polinomnak nevezzük, ha nem szeparábilis. Az $\alpha \in L$ **elem szeparábilis $K$ felett**, ha $\alpha$ algebrai $K$ felett és $m_{\alpha,K}$ szeparábilis. Az $L : K$ **bővítés szeparábilis**, ha $L$ minden eleme szeparábilis $K$ felett.

Az $g \in K[x]$ polinom **szeparábilis**, ha $g$ minden irreducibilis tényezője szeparábilis.

A $K$ testet **tökéletesnek** nevezzük, ha minden $K[x]$-beli polinom szeparábilis, ami ekvivalens azzal, hogy minden $K[x]$-beli irreducibilis polinom szeparábilis.

**5.1. Tétel.** *Legyen $M$ az $L : K$ szeparábilis testbővítés közbülső teste. Ekkor az $L : M$ és $M : K$ testbővítések is szeparábilisak.*

*Bizonyítás.* Legyen $\alpha$ az $L$ test tetszőleges eleme. Mivel az $L : K$ bővítés szeparábilis, ezért az $\alpha$ elem algebrai $K$ felett, ezért $M$ felett is algebrai, valamint az is teljesül, hogy $m_{\alpha,M} \mid m_{\alpha,K}$. Legyen $N$ az $m_{\alpha,K} \in M[x]$ polinom egy felbontási teste $M$ felett. Ekkor $N[x]$-ben

$$m_{\alpha,K} = (x - \alpha_1) \cdots (x - \alpha_n)$$

teljesül, ahol $\alpha_1, \ldots, \alpha_n \in N$ páronként különböző elemek. Így $m_{\alpha,M} \mid m_{\alpha,K}$ miatt

$$m_{\alpha,M} = (x - \alpha_{i_1}) \cdots (x - \alpha_{i_m})$$

teljesül valamely $1 \leqslant i_1 < \cdots < i_m \leqslant n$ indexekre. Azaz $m_{\alpha,M}$ is szeparábilis.

Az $M : K$ bővítés szeparábilitása nyilvánvaló. □

## 5.2 Injektív homomorfizmusok és automorfizmusok

**5.2. Tétel.** *Legyen a $K(\alpha):K$ testbővítés $d$-edfokú egyszerű bővítés, és legyen $\mathrm{j}\colon K\to L$ a $K$ test injektív homomorfizmusa az $L$ testbe. Ha $\alpha$ szeparábilis a $K$ test felett és $\mathrm{j}_{m_{\alpha,K}}$ elsőfokú polinomok szorzatára bomlik $L$ felett, akkor pontosan $d$ darab olyan injektív homomorfizmus van $K$-ból $L$-be, amely kiterjesztése* j*-nek; különben pedig $d$-nél kevesebb.*

*Bizonyítás.* Alkalmazzuk a Kiterjesztési Lemmát (4.4. Lemma) a $K'=\mathrm{j}(K)$ és $\eta\colon K\to K',\ k\mapsto \mathrm{j}(k)$ választással. Ekkor $\eta$ kiterjesztéseinek száma

$$|\left\{\beta\in L\mid\ \beta \text{ gyöke } \mathrm{j}_{m_{\alpha,K}}\text{-nak}\right\}|=\mathrm{j}^*_{m_{\alpha,K}}=m^*_{\alpha,K}=d,$$

mivel $\alpha$ pontosan akkor szeparábilis $K$ felett, ha $\mathrm{j}_{m_{\alpha,K}}$ szeparábilis $\mathrm{j}(K)$ felett. □

## 5.3 Polinomok többszörös gyökei

Legyen $f$ legalább elsőfokú polinom a $K$ test felett, és legyen $L$ az $f$ polinom felbontási teste. Ekkor az $f$ polinom felírható

$$f=\lambda(x-\alpha_1)^{\ell_1}\cdots(x-\alpha_r)^{\ell_r}$$

alakban, ahol $\alpha_1,\dots,\alpha_r$ az $f$ polinom páronként különböző gyökei $L$-ben. Az $\ell_i\in\mathbb{N}$ egészet az $\alpha_i$ gyök multiplicitásának nevezzük. Ha $\ell_i=1$, akkor $\alpha_i$ **egyszeres gyök**, különben pedig **többszörös gyök**. Megjegyezzük, hogy az $f$ polinom gyökeinek multiplicitása független a felbontási test választásától.

Legyen $K$ tetszőleges test, és legyen $D_x$ a következő leképezés:

$$D_x\colon K[x]\to K[x],\ \sum_{k=0}^{n}a_kx^k\mapsto\begin{cases}0, & \text{ha } f\in K,\\ \sum_{k=0}^{n-1}(k+1)a_{k+1}x^k, & \text{ha } f^*=n\geqslant 1.\end{cases}$$

A $D_x$ leképezést **(formális) driválásnak** nevezzük a $K[x]$ halmazon.

Az alábbi tétel a formális deriválás tulajdonságait foglalja össze.

**5.3. Tétel.** *Legyen $K$ tetszőleges test, ekkor a $D_x$ formális deriválásra teljesülnek a következők.*

(1) *$D_x$ lineáris transzformációja a $K[x]$ (mint $K$ feletti) vektortérnek.*

(2) *$D_x$ **derivációja** a $K[x]$ halmazon, azaz tetszőleges $f,g\in K[x]$-re $D_x(fg)=D_x(f)g+fD_x(g)$ teljesül.*

(3) *Ha $\mathrm{char}(K)=0$, akkor $\ker(D_x)=K$, és a $D_x$ leképezés szürjektív.*

(4) *Ha $\mathrm{char}(K)=p$ prímszám, akkor*

$$\ker(D_x)=\{h(x^p)\mid h\in K[x]\},$$

*és $D_x$ képterét generálják az $x^k$ alakú monomok, ahol $p\nmid k+1$.*

*Bizonyítás.* Az (1)–(3) állításokat a definíció alapján egyszerűen igazolhatjuk. Így csak utolsó állítással kell foglalkoznunk.

(4) Legyen $f = \sum_{k=0}^{n} a_k x^k$ olyan $n$-edfokú ($n \geqslant 1$) $K$ feletti polinom, amelynek formális deriváltja 0, azaz

$$D_x(f) = \sum_{k=0}^{n-1} (k+1) a_{k+1} x^k = 0.$$

Ekkor $ka_k = 0$ minden $k$-ra ($1 \leqslant k \leqslant n$). Ez pedig pontosan azt jelenti, hogy $p \nmid k$ esetén $a_k = 0$ teljesül, azaz $f = \sum_{k=0}^{[n/p]} a_{kp} x^{kp}$. Ekkor a $h = \sum_{k=0}^{[n/p]} a_{kp} x^k \in K[x]$ polinomra $f = h(x^p)$. □

**5.4. Tétel.** *Legyen $K$ test, $f \in K[x]$ és $\alpha \in L$ az $f$ polinom gyöke a $K$ test valamely $L$ testbővítésében. Ekkor $\alpha$ pontosan akkor többszörös gyöke $f$-nek, ha* ln.k.o.$(f, D_x(f))$ *legalább elsőfokú polinom, amelynek gyöke $\alpha$.*

*Bizonyítás.* Tegyük fel, hogy $\alpha \in L$ többszörös gyöke $f$-nek a $K$ test $L$ bővítésében. Ekkor $f = (x-\alpha)^\ell g$, ahol $\ell \geqslant 2$ és $g \in L[x]$. Így az 5.3. Tétel (2) pontja szerint

$$D_x(f) = \ell(x-\alpha)^{\ell-1} g + (x-\alpha)^\ell D_x(g) = (x-\alpha)^{\ell-1} \left(\ell g + (x-\alpha) D_x(g)\right).$$

Ekkor $x - \alpha$ osztója az $f$ és $D_x(f)$ polinomoknak $L[x]$-ben, és így

$$x - \alpha \mid \text{ln.k.o.}(f, D_x(f)).$$

Azaz, ln.k.o.$(f, D_x(f))$ legalább elsőfokú polinom, melynek gyöke $\alpha$.

Tegyük fel, hogy az $f \in K[x]$ polinomnak ($f^* = n \in \mathbb{N}$) nincs többszörös gyöke a $K$ test $L$ bővítésében. Legyen $f = g_1 \cdots g_t$ az $f$ polinom irreducibilis felbontása $L$ felett, valamint legyen $M$ az $f$ polinom felbontási teste $L$ felett:

$$f = \lambda(x-\alpha_1)^{\ell_1} \cdots (x-\alpha_s)^{\ell_s},$$

ahol $\lambda \in K$, $\alpha_1, \ldots, \alpha_s \in M$ páronként különböző elemek és $\ell_1 + \cdots + \ell_s = n$. Ekkor

$$D_x(f) = D_x(g_1) \cdot g_2 \cdots g_t + \cdots + g_1 \cdots g_{t-1} \cdot D_x(g_t).$$

Ha $\alpha_1, \ldots, \alpha_s \notin L$, akkor ln.k.o.$(f, D_x(f))$-nek sem lehet gyöke $L$-ben. Tegyük fel, hogy valamely $i \in \{1, \ldots, s\}$-re $\alpha_i \in L$. Ekkor $g_j = x - \alpha_i$ irreducibilis tényezője $f$-nek, és $(x-\alpha_i)$-től különböző irreducibilis tényezőnek nem gyöke $\alpha_i$. Így $D_x(f)(\alpha_i) = g_1(\alpha_i) \cdots g_{j-1}(\alpha_i) \cdot D_x(x-\alpha_i)(\alpha_i) \cdot g_{j+1}(\alpha_i) \cdots g_t(\alpha_i) \neq 0$ miatt $\alpha_i$ nem lehet gyöke ln.k.o.$(f, D_x(f))$-nek sem. □

**5.5. Következmény.** *Legyen $K$ 0-karakterisztikájú test (pl. számtest), $f$ irreducibilis polinom $K$ felett, melynek felbontási teste $L$. Ekkor az $f$ polinom valamennyi gyöke egyszeres $L$-ben.*

*Bizonyítás.* Mivel $\text{char}(K) = 0$, ezért $D_x(f)^* = f^* - 1$. A legnagyobb közös osztó definíciójából következik, hogy ln.k.o.$(f, D_x(f)) \mid f$. Így $f$ irreducibilitásának következtében ln.k.o.$(f, D_x(f)) \sim 1$ vagy ln.k.o.$(f, D_x(f)) \sim f$ teljesül. Mivel

$$\text{ln.k.o.}(f, D_x(f)) \sim f \iff f \mid D_x(f),$$

ezért ez a fokszámok miatt nem fordulhat elő. Ekkor ln.k.o.$(f, D_x(f)) \sim 1$, aminek következtében $f$-nek nem lehet többszörös gyöke $L$-ben. □

**5.6. Példa.** *Legyen* $f = \sum_{j=0}^{n} \frac{x^j}{j!} \in \mathbb{Q}[x]$ *(*$n \geqslant 1$*). Ekkor* $D_x(f) = \sum_{j=0}^{n-1} \frac{x^j}{j!}$. *Mivel* $\text{ln.k.o.}(f, D_x(f)) \mid f, D_x(f)$, *ezért* $\text{ln.k.o.}(f, D_x(f)) \mid f - D_x(f) = \frac{x^n}{n!}$. *Így* $\text{ln.k.o.}(f, D_x(f))$*-nek legfeljebb egy gyöke van* $\mathbb{C}$*-ben, a 0, ami azonban nem gyöke* $f$*-nek. Azaz* $f$*-nek nincs többszörös gyöke.*

A 5.5. Következmény állításának egyszerű újrafogalmazása az alábbi tétel.

**5.7. Tétel.** *Ha a* $K$ *test karakterisztikája* 0*, akkor* $K$ *tökéletes.*

Ez a tétel nagy jelentőséggel bír számunkra, mivel azt is állítja, hogy minden számtest feletti polinom szeparábilis.

**5.8. Tétel.** *Tegyük fel, hogy a* $K$ *testre* $\text{char}(K) = p > 0$ *teljesül. Ekkor a* $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ *leképezés injektív homomorfizmus, valamint az* $\alpha \in K$ *elemre pontosan akkor teljesül, hogy* $\mathfrak{F}(\alpha) = \alpha$*, ha* $\alpha$ *a* $K$ *test prímtestében van.*

*Bizonyítás.* A bizonyítás alapját az az észrevétel alkotja, hogy tetszőleges $a, b \in K$-ra

$$(a+b)^p = \sum_{k=0}^{p} \binom{p}{k} a^k b^{p-k} = a^p + b^p, \tag{8}$$

mivel $p \mid \binom{p}{k}$, ha $1 \leqslant k \leqslant p-1$ egész szám.

Legyenek $a$ és $b$ tetszőleges $K$-beli elemek. Ekkor a szorzás művelet kommutativitása miatt

$$\mathfrak{F}(a \cdot b) = (a \cdot b)^p = a^p \cdot b^p = \mathfrak{F}(a) \cdot \mathfrak{F}(b),$$

valamint (8) miatt

$$\mathfrak{F}(a+b) = (a+b)^p = a^p + b^p = \mathfrak{F}(a) + \mathfrak{F}(b).$$

teljesül, azaz $\mathfrak{F}$ homomorfizmus. Az $\mathfrak{F}$ homomorfizmus injektivitása szintén (8) következménye, mivel

$$\mathfrak{F}(a) = \mathfrak{F}(b) \Longleftrightarrow a^p = b^p \Longleftrightarrow a^p - b^p = 0 \Longleftrightarrow (a-b)^p = 0 \Longleftrightarrow a = b.$$

Mivel tetszőleges $a \in K$-ra

$$\begin{aligned} a \in \mathbb{Z}_p &\Longleftrightarrow a \text{ gyöke az } x^p - x \in \mathbb{Z}_p[x] \text{ polinomnak} \\ &\Longleftrightarrow a^p - a = 0 \\ &\Longleftrightarrow a^p = a \\ &\Longleftrightarrow \mathfrak{F}(\alpha) = \alpha, \end{aligned}$$

ezért $\mathfrak{F}$ fixpontjai éppen a $\mathbb{Z}_p$ test elemei. □

A fenti $\mathfrak{F}\colon K \to K,\ \alpha \mapsto \alpha^p$ leképezést **Frobenius-endomorfizmusnak**[25] nevezzük.

Az 5.8. és 2.22. Tételekből adódik az alábbi állítás.

**5.9. Következmény.** *Legyen* $K$ *test. Ha* $\text{char}(K) = p > 0$ *és* $K$ *algebrai testbővítése a prímtestének, akkor a Frobenius-endomorfizmus automorfizmus.*

[25] Ferdinand Georg **Frobenius** (1849. október 26., Charlottenburg – 1917. augusztus 3., Berlin) német matematikus, legismertebb eredményeit a differenciálegyeneletek és a csoportok elméletében érte el.

## 5.4 Inszeparábilis polinomok

**5.10. Tétel.** *Legyen $K$ test. Tegyük fel, hogy* $\mathrm{char}(K) = p > 0$ *és legyen*

$$f = x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1x^p + a_0 \in K[x].$$

*Ekkor az $f$ polinom pontosan akkor irreducibilis $K$ felett, ha a*

$$g = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$$

*polinom irreducibilis $K[x]$-ben és van olyan $i \in \{1, \ldots, n-1\}$ index, amelyre $a_i$ nem $p$-hatvány $K$-ban.*

Amennyiben a $p$ karakterisztikájú $K$ test algebrai testbővítése prímtestének, akkor az 5.9. Következmény szerint a $K$ test Frobenius-endomorfizmusa automorfizmus, azaz $K$ minden eleme $p$-hatvány. Így $x^{np} + a_{n-1}x^{(n-1)p} + \cdots + a_1x^p + a_0$ alakú polinom nem lehet irreducibilis $K[x]$-ben. Ez pedig a következőt jelenti.

**5.11. Tétel.** *Ha a $p$ karakterisztikájú $K$ test algebrai testbővítése prímtestének, akkor minden $K$ feletti polinom szeparábilis.*

Mivel minden véges test a prímtestének véges testbővítése —így algebrai testbővítése is—, ezért igaz az alábbi állítás.

**5.12. Következmény.** *Minden véges test tökéletes.*

# Test algebrai lezártja

## 6.1 Bevezetés

**6.1. Definíció.** *Azt mondjuk, hogy az $L$ test* ***algebrailag zárt****, ha bármely $f \in L[x]$ polinomnak van gyöke $L$-ben.*

*A $K$ test $L$ testbővítése $K$* ***algebrai lezártja****, ha az $L : K$ testbővítés algebrai és az $L$ test algebrailag zárt.*

**6.2. Példa.** *Az Algebra Alaptétele éppen azt állítja, hogy a komlex számok $\mathbb{C}$ teste algebrailag zárt, azonban $\mathbb{C}$ nem algebrai lezártja $\mathbb{Q}$-nak, mivel $\mathbb{C}$ nem minden eleme algebrai $\mathbb{Q}$ felett (pl. $e$ és $\pi$ nem algebrai elemek $\mathbb{Q}$ felett).*

**6.3. Tétel.** *Tetszőleges $L : K$ testbővítésre ekvivalensek az alábbi állítások.*

(1) *$L$ algebrai lezártja $K$-nak.*

(2) *az $L : K$ bővítés algebrai és minden irreducibilis $K[x]$-beli polinom elsőfokú polinomok szorzatára bomlik $L[x]$-ben.*

(3) *az $L : K$ bővítés algebrai, és tetszőleges $L'$ testre, ha a $L' : L$ testbővítés algebrai, akkor $L' = L$.*

*Bizonyítás.* (1) $\Longrightarrow$ (2): az $f$ irreducibilis polinom fokszámára vonatkozó indukcióval az állítás egyszerűen belátható.

(2) $\Longrightarrow$ (3): legyen $\alpha$ az $L'$ test tetszőleges eleme. Mivel az $L : K$ és $L' : L$ bővítések is algebraiak, ezért a 2.21. Tétel szerint az $L' : K$ bővítés is algebrai, így $\alpha$ algebrai elem $K$ felett, melynek minimálpolinomja $m_{\alpha,K}$ irreducibilis polinom $K[x]$-ben. Ekkor a (2) pont következtében $m_{\alpha,K}$ lineáris tényezőkre bomlik $L$ felett:

$$m_{\alpha,K} = \lambda(x - \alpha_1) \cdots (x - \alpha_n),$$

ahol $n = \mathrm{gr}_K(\alpha)$, $\lambda \in K$ és $\alpha_1, \ldots, \alpha_n \in L$. Mivel $\alpha$ is gyöke $m_{\alpha,K}$-nak, ezért valamely $i$-re $(1 \leqslant i \leqslant n)$ $\alpha = \alpha_i \in L$. Azaz $L' = L$.

(3) $\Longrightarrow$ (1): csak azt kell megmutatni, hogy $L$ algebrailag zárt. Legyen $f \in L[x]$ tetszőleges legalább elsőfokú polinom, és legyen $f_1$ az $f$ polinom egy irreducibilis tényezője. Tekintsük az $L$ test $L' = L[x]/(f_1)$ bővítését. Az $L'$ testben $f_1$-nek, és így $f$-nek is van gyöke $(\alpha = x + (f_1))$. Mivel az $L' : L$ bővítés algebrai, ezért a (3) pont szerint $L' = L$, ami éppen azt jelenti, hogy $f$-nek $L$-ben is van gyöke. □

**6.4. Következmény.** *Legyen $L$ algebrailag zárt test, és $L : K$ tetszőleges testbővítés. Legyen $L_a$ mindazon $L$-beli elemek halmaza, amelyek algebraiak $K$ felett. Ekkor $L_a$ algebrai lezártja $K$-nak.*

*Bizonyítás.* A 2.20. Tétel szerint az $L_a : K$ bővítés algebrai. Legyen $f \in L_a[x]$ tetszőleges irreducibilis polinom. Mivel $f \in L_a[x] \subseteq L[x]$ és $L$ algebrailag zárt, ezért $f$-nek van egy $\alpha$ gyöke $L$-ben. Mivel az $L_a(\alpha) : L_a$ és $L_a : K$ bővítések is algebraiak, ezért az $L_a(\alpha) : K$ bővítés is algebrai, azaz $\alpha \in L$ algebrai elem $K$ felett, így $\alpha \in L_a$. Azaz $f$ elsőfokú polinom kell legyen. Ez pedig azt jelenti, hogy az $L_a$ test algebrailag zárt, és így a $K$ test algebrai lezártja. □

## 6.2 Test algebrai lezártjának létezése

**6.5. Lemma (Zorn-lemma).** *Legyen $P = (P; \leqslant)$ tetszőleges részbenrendezett halmaz. Ha bármely $C \subseteq P$ láncnak van felső korlátja $P$-ben, akkor $P$-ben van maximális.*

A Zorn-lemma egyik fontos következménye, hogy egy egységelemes gyűrű tetszőleges valódi ideálja mindig része a gyűrű egy maximális ideáljának.

**6.6. Tétel.** *Legyen $K$ test. Ekkor van olyan algebrailag zárt $L$ test, amely tartalmazza $K$-t.*

*Bizonyítás.* Legyen $X = \{x_f \mid f \in K[x] \text{ legalább elsőfokú főpolinom}\}$, és legyen $I$ az $\{f(x_f) \mid f \in K[X] \text{ legalább elsőfokú főpolinom}\}$ halmaz által generált ideálja a $K[X]$ gyűrűnek. Először megmutatjuk, hogy $I$ valódi ideál.

Tegyük fel, hogy $I = K[X]$. Ekkor $1 \in I$ miatt van olyan $n$ természetes szám, $f_1, \dots, f_n \in K[X]$ legalább elsőfokú főpolinomok, valamint $g_1, \dots, g_n \in K[x]$ elemek, amelyekre

$$1 = \sum_{i=0}^{n} g_i f_i(x_{f_i}).$$

Legyen $M$ olyan testbővítése $K$-nak, amely tartalmazza az $f_1, \dots, f_n$ polinomok egy-egy gyökét ($\alpha_i \in M$ gyöke $f_i$-nek, $i = 1, \dots, n$). A

$$\varphi\colon X \to H,\ x_f \mapsto \begin{cases} \alpha_i, & \text{ha } f = f_i\ (i = 1, \dots, n), \\ 0, & \text{különben} \end{cases}$$

leképezés egyértelműen kiterjeszthető egy $\bar{\varphi}\colon K[X] \to H$ homomorfizmussá. Ekkor $f_i(\alpha_i) = 0$ miatt az $1 = \bar{\varphi}(g_1 f_1(x_{f_1}) + \dots + g_n f_n(x_{f_n})) = 0$ ellentmondást kapjuk.

Azaz $I$ valódi ideálja $K[X]$-nek. Legyen $J$ az $R$ gyűrű $I$-t tartalmazó maximális ideáljainak valamelyike (a Zorn-lemma miatt van ilyen maximális ideál). Legyen $F(K) = K[X]/J$, mivel $J$ maximális ideál $K[X]$-ben, ezért az $F(K)$ faktorgyűrű test, és a $\pi\colon K \to F(K),\ k \mapsto k + J$ leképezés injektív homomorfizmus, mivel $J \cap K = \{0\}$. A $k$ és $k + J$ elemek ($k \in K$) azonosítása után úgy tekintjük, hogy $K \subseteq F(K)$.

Legyen $f$ tetszőleges $K[X]$-beli legalább elsőfokú polinom. Mivel $f(x_f) \in I \subseteq J$, ezért $f(x_f + J) = 0$, és így $x_f + J \in F(K)$ gyöke $f$-nek.

Definiáljuk a $(K_i)_{i \in \mathbb{N}_0}$ testsorozatot a következőképpen:

$$K_0 = K, \quad K_i = F(K_{i-1}) \quad (i \in \mathbb{N}),$$

és legyen $L = \bigcup_{i=0}^{\infty} K_i$. Az $L$ halmazon definiáljuk az összeadás ($+$) és szorzás ($\cdot$) műveleteket az alábbi módon: legyen $a, b \in L$, ekkor van olyan $n \in \mathbb{N}_0$,

amelyre $a, b \in K_n$. Legyen $a + b = a +_{K_n} b$ és $a \cdot_{K_n} b$, ahol $+_{K_n}$, illetve $\cdot_{K_n}$ a $K_n$ testbeli összeadás, illetve szorzás. Egyszerűen igazolható, hogy az $(L; +, \cdot)$ algebra test.

Azt állítjuk, hogy az $L$ test algebrailag zárt. Legyen $f \in L[x]$ tetszőleges irreducibilis polinom. Legyen $n$ olyan természetes azám, amelyre $K_n$ az $f$ polinom valamennyi együtthatóját tartalmazza. Ekkor $f \in K_n[X]$, és így $f$-nek van gyöke $K_{n+1} \subseteq K$-ban. Mivel $f$ irreducibilis ez éppen azt jelenti, hogy $f$ elsőfokú.

Ezzel a tétel bizonyítását befejeztük. □

**6.7. Tétel.** *Legyen $K$ test. Ekkor van olyan $L$ bővítése a $K$ testnek, amelyre $L$ algebrai lezártja $K$-nak.*

*Bizonyítás.* A tétel állítása az előző tételből és a 6.4. Tételből adódik. □

## 6.3 Test algebrai lezártjának egyértelműsége

Ezen fejezetet annak igazolásával zárjuk, hogy az algebrai lezárt izomorfiától eltekintve egyértelmű.

**6.8. Tétel.** *Tegyük fel, hogy a $K$ és $K'$ testek izomorfak, $\eta\colon K \to K'$ izomorfizmus. Legyenek $L$, illetve $L'$ a $K$, illetve $K'$ testek algebrai lezártjai. Ekkor van olyan $\psi\colon L \to L'$ izomorfizmus, amely kiterjesztése $\eta$-nek, azaz $\psi|_K = \eta$.*

*Bizonyítás.* Az $(E, \chi, E')$ hármas jelölje azt, hogy az $E$ és $E'$ testek izomorfak, és $\chi\colon E \to E'$ izomorfizmus. Tekintsük a

$$P = \{(E, \chi, E') \mid K \subseteq E \subseteq L, K' \subseteq E' \subseteq L',\ \text{és } \chi|_K = \eta\}$$

halmazt, amely nem üres, mivel $(K, \eta, K') \in P$. A $P$ halmazon a

$$(E, \chi, E') \leqslant (F, \xi, F') \Longleftrightarrow E \subseteq E',\ F \subseteq F',\ \chi \subseteq \xi$$

reláció parciális rendezés. Legyen $C = \{(E_\delta, \chi_\delta, E'_\delta) \mid \delta \in H\}$ $P$-beli lánc, valamint legyen $E = \cup_{\delta\in H} E_\delta$, $E' = \cup_{\delta\in H} E'_\delta$ és $\chi = \cup_{\delta\in H} \chi_\delta$. Ekkor $(E, \chi, E') \in P$ és nyilván felső korlátja $C$-nek, és a Zorn-lemma szerint $P$-ben van maximális elem: $(M, \psi, M')$. Tegyük fel, hogy $M \neq L$, és legyen $\alpha \in L \setminus M$. Mivel az $L : K$ bővítés algebrai, ezért $\alpha$ algebrai elem $K$ felett. Legyen $f = m_{\alpha,K}$. Mivel $L'$ algerai lezártja $K'$-nek, ezért az $\eta_f \in K'[x]$ polinomnak van olyan $\alpha' \in L'$ gyöke, amely nincs $M'$-ben (ugyanis, ha $\eta_f$ valamennyi gyöke $M'$-ban volna, akkor $f$ gyökei $M$-ben lennének, azonban $\alpha \notin M$). Legyen $\psi\colon M \to M'$ izomorfizmus egyértelmű kiterjesztése $\bar\psi\colon M(\alpha) \to M'(\alpha')$. Ekkor $(M(\alpha), \bar\psi, M'(\alpha')) \in P$ és $(M, \psi, M') < (M(\alpha), \bar\psi, M'(\alpha'))$ ellentmondva $(M, \psi, M')$ maximalitásának. Azaz $M = L$, hasonlóan igazolható, hogy $M' = L'$. Ezzel a tétel állítását igazoltuk. □

**6.9. Következmény.** *Legyen $K$ tetszőleges test. Ha $L$ és $L'$ is a $K$ test algebrai lezártja, akkor van olyan $\psi\colon L \to L'$ izomorfizmus, amely kiterjesztése $K$ elemeit fixen hagyja.*

*Bizonyítás.* Alkalmazzuk az előző tételt a $K = K'$, $\eta = \mathrm{id}_K$ esetben. □

## 7.1 Alapvető tulajdonságok

Az $L : K$ testbővítés **normális**, ha algebrai testbővítés és valahányszor $f \in K[x]$ irreducibilis polinom, mindannyiszor vagy $f$ elsőfokú tényezők szorzatára bomlik $L$ felett, vagy $f$-nek nincs gyöke $L$-ben.

Nyilvánvaló, hogy az $L : K$ algebrai bővítés pontosan akkor normális, ha bármely $\alpha \in L$-re $m_{\alpha,K}$ elsőfokú tényezők szorzatára bontható $L[x]$-ben.

A normális bővítések leírásához ki kell terjesztenünk a felbontási test fogalmát egyetlen polinomról polinomok halmazaira.

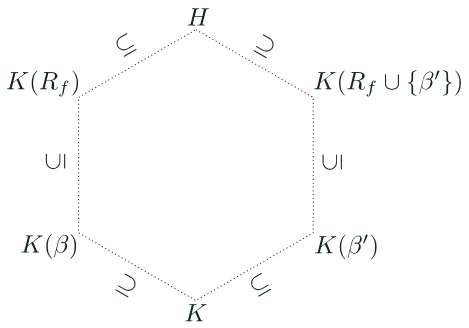
Legyen $K$ tetszőleges test és $S \subseteq K[x]$. Azt mondjuk, hogy a $K$ test $L$ bővítése **felbontási teste az $S$ polinomhalmaznak**, ha $S$ valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben, és $L$ a legszűkebb ilyen tulajdonságú test.

Ha az $S$ halmaz véges, $S = \{f_1, \dots, f_n\}$, akkor $S$ felbontási teste megegyezik az $f = f_1 \cdots f_n$ polinom felbontási testével.

**7.1. Tétel.** *Az $L : K$ testbővítés pontosan akkor normális, ha $L$ valamely $S \subseteq K[x]$ polinomhalmaz felbontási teste.*

*Bizonyítás.* Tegyük fel, hogy $L : K$ normális, és legyen $S = \{m_{\alpha,K} \mid \alpha \in L\}$. Ekkor $S$ valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben. Továbbá ezzel a tulajdonsággal nyilván nem rendelkezik $L$ egyetlen valódi részteste sem.

Tegyük fel, hogy $L$ felbontási teste az $S \subseteq K[x]$ polinomhalmaznak. Legyen $R$ az $S$-beli polinomok gyökeinek halmaza. Ekkor $L = K(R)$ és az $L : K$ bővítés algebrai, mivel $R$ minden eleme algebrai $K$ felett (2.20. Következmény). Legyen $\beta$ tetszőleges eleme az $L$ testnek. Ekkor vannak olyan $\alpha_1, \dots, \alpha_t \in R$ elemek, amelyekre $\beta \in K(\alpha_1, \dots, \alpha_t)$. Minden $i$-re $(1 \leqslant i \leqslant t)$ válasszunk egy $f_i \in S$ polinomot, amelynek gyöke $\alpha_i$, és legyen $f = f_1 \cdots f_t$. Jelölje $R_f$ az $f$ polinom gyökeinek a halmazát $L$-ben. Ekkor $K(R_f)$ felbontási teste az $f$ polinomnak $K$ felett. Legyen az $m_{\beta,K}$ polinom felbontási teste $K(R_f)$ felett $H$. Tekintsük $m_{\beta,K}$ egy $\beta' \neq \beta$ gyökét $H$-ban. Meg fogjuk mutatni, hogy $\beta' \in K(R_f) \subseteq L$. A $K, \dots, H$ testek egymáshoz való viszonya az alábbi ábrán látható.




**7. ábra:** a $K, \dots, H$ testek egymáshoz való viszonya.

Mivel $m_{\beta,K}$ a $\beta$ és $\beta'$ elemeknek is minimálpolinomja a $K$ test felett, ezért

$$[K(\beta) : K] = [K(\beta') : K]. \tag{9}$$

Legyen $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$ és $\eta$ kiterjeszthető egy olyan $\vartheta\colon K(\beta) \to K(\beta')$ injektív homomorfizmussá, amelyre $\vartheta(\beta) = \beta'$ teljesül (vö.: 4.4. Lemma). Mivel a $K(\beta')$ testet generálja $K \cup \{\beta'\}$, ezért $\vartheta$ izomorfizmus. A $K(R_f)$ test felbontási teste $f$-nek $K(\beta)$ felett és $K(R_f \cup \{\beta'\})$ felbontási teste $\vartheta_f = f$-nek $K(\beta')$ felett.

$$\begin{array}{ccc} K(R_f) & \xrightarrow[\tau|_{K(\beta)}=\vartheta]{\tau} & K(R_f \cup \{\beta'\}) \\ \cup\mathrm{I} & & \cup\mathrm{I} \\ K(\beta) & \xrightarrow[\vartheta|_K=\eta]{\vartheta} & K(\beta') \\ \cup\mathrm{I} & & \cup\mathrm{I} \\ K & \xrightarrow[\eta = \mathrm{id}_K]{} & K \end{array}$$

**8. ábra:** az $\eta$ izomorfizmus és kiterjesztése.

Így a 4.3. Tétel szerint van olyan $\tau\colon K(R_f) \to K(R_f \cup \{\beta'\})$ izomorfizmus, amelyre $\tau|_{K(\beta)} = \vartheta$. Ez pedig azt jelenti, hogy

$$[K(R_f) : K(\beta)] = [K(R_f \cup \{\beta'\}) : K(\beta')],$$

és így a Fokszámtétel és (9) szerint

$$\begin{aligned} [K(R_f) : K] &= [K(R_f) : K(\beta)][K(\beta) : K] \\ &= [K(R_f \cup \{\beta'\}) : K(\beta)][K(\beta') : K] \\ &= [K(R_f \cup \{\beta'\}) : K]. \end{aligned}$$

Mivel $K(R_f) \subseteq K(R_f \cup \{\beta'\})$, ezért $K(R_f) = K(R_f \cup \{\beta'\})$. Ebből pedig már következik, hogy $\beta' \in K(R_f)$. □

**7.2. Következmény.** *Az $L : K$ véges testbővítés pontosan akkor normális, ha $L$ valamely $f \in K[x]$ polinom felbontási teste.*

*Bizonyítás.* Ha $L$ valamely $f \in K[x]$ polinom felbontási teste, akkor az előző tétel szerint az $L : K$ bővítés normális.

Tegyük fel, hogy $L : K$ véges és normális. Legyen $[L : K] = k$ és $\alpha_1, \dots, \alpha_k \in L$ az $L$, mint $K$ feletti vektortér, bázisa. Ekkor $L$ éppen az

$$f = m_{\alpha_1,K} \cdots m_{\alpha_k,K} \in K[x]$$

polinom felbontási teste. □

Tegyük fel, hogy az $L : K$ bővítés normális. Az $F : L$ testbővítés az $L : K$ bővítés **normális lezártja**, ha valahányszor $L \leqslant M \leqslant F$ és $M : K$ normális, mindannyiszor $M = F$.

**7.3. Következmény.** *Ha $L : K$ véges testbővítés, akkor van olyan $F : L$ véges bővítés, amely normális lezártja $L : K$-nak.*

*Bizonyítás.* Tegyük fel, hogy $L : K$ véges, $[L : K] = k$ és $\alpha_1, \ldots, \alpha_k \in L$ az $L$, mint $K$ feletti vektortér, bázisa. Legyen $F$ az $f = m_{\alpha_1,K} \cdots m_{\alpha_k,K} \in L[x]$ polinom felbontási teste $L$ felett. Ekkor az $F : K$ bővítés normális, mivel $F$ a $K$ test felett is felbontási teste $f$-nek. Tegyük fel, hogy $L \leqslant M \leqslant F$ és $M : K$ normális bővítés. Ekkor $M$ tartalmazza az $m_{\alpha_i,K}$ polinomok $(i = 1, \ldots, k)$ valamennyi gyökét, így $f$ lineáris tényezőkre bomlik $M[x]$-ben. Ez pedig $M \leqslant F$ miatt éppen azt jelenti, hogy $M = F$. □

**7.4. Következmény.** *Ha az $L : K$ bővítés normális és $M$ közbülső teste a bővítésnek, akkor az $L : M$ bővítés is normális.*

## 7.2 Injektív homomorfizmusok és automorfizmusok

A 7.4. Következmény szerint, ha az $L : K$ testbővítés normális, akkor az $L : M$ testbővítés is normális, ahol $K \leqslant M \leqslant L$. Vajon mi a helyzet az $M : K$ bővítéssel? Például legyen $\omega$ egy komplex harmadik egységgyök. Ekkor a $\mathbb{Q}(\sqrt[3]{2}, \omega) : \mathbb{Q}$ bővítés normális, mivel $\mathbb{Q}(\sqrt[3]{2}, \omega)$ az $f = x^3 - 2$ polinom felbontási teste. Azonban a $\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}$ bővítés nem normális, mivel $f$-nek van gyöke a $\mathbb{Q}(\sqrt[3]{2})$ testben, de $f$ nem bomlik fel elsőfokú polinomok szorzatára $\mathbb{Q}(\sqrt[3]{2})[x]$-ben.

Legyenek $K$ és $L$ testek úgy, hogy $K \leqslant L$. Ekkor $\mathrm{Aut}(L)$-lel jelöljük az $L$ test automorfizmusainak csoportját, valamint legyen

$$\mathrm{Aut}_K(L) = \{\sigma \in \mathrm{Aut}(L) \mid \sigma(k) = k \text{ minden } k \in K\text{-ra}\}.$$

Nyilvánvaló, hogy $\mathrm{Aut}_K(L)$ részcsoportja $\mathrm{Aut}(L)$-nek. Az $\mathrm{Aut}_K(L)$ csoportot **az $L : K$ testbővítés Galois-csoportjának**[26] nevezzük, és $\mathrm{Gal}(L : K)$-val jelöljük.

[26] Évariste **Galois** (1811. október 25., Bourg-la-Rein – 1832. március 31., Párizs) francia matematikus. Tragikus sorsú tudós, a csoportelmélet megalapozója. Élete még Abelénél is rövidebb és tragikusabb. Egy Párizs melletti kisváros polgármesterének fia volt. Tizenkét éves koráig anyja tanította, aki igen művelt hölgy volt. Ezután került egy híres párizsi gimnáziumba. Itt kezdte el tanulmányozni Abel, Legendre és Jacobi műveit, nemsokára pedig már önálló eredményeket is produkált. Felvételi dolgozatát az École Polytechnique-be azonban kétszer is elutasították. Harmadszorra eljutott a szóbeliig, de az botrányba fulladt. Galois a levezetéseit nem értő bizottsághoz hajította szivacsát és elrohant. Az akadémiához beküldött dolgozatai sem találtak több megértésre. Egyiküket Cauchy egyszerűen elvesztette. Végül 1829-ben beiratkozott a tanárképző intézetbe. Részt vett az 1830-as forradalomban, ezért kicsapták az iskolából és több hónapi börtönre ítélték. Kiszabadulása után egy talán provokált párbajba keveredett egy rosszhírű nő miatt és a párbajban halálos lövést kapott. Halála előtti éjszakáján vetette papírra matematikai felfedezéseit. Ezt a tudományos végrendeletet barátjának címezte ezekkel a sorokkal: „Nyilvánosan kérdezd meg Jacobit vagy Gausst, mi a véleménye nem a tételek igazságáról, hanem fontosságáról. Utána remélem akadnak emberek, akik érdemesnek tartják ennek a zagyvaléknak a kisilabizálását." Ez a „zagyvalék" a Galois-elmélet volt, ami lezárta a magasabbfokú egyenletek algebrai megoldhatóságának több évszázados problémáját és megnyitotta a kaput az absztrakt algebra kialakulása felé. A mű

**7.5. Tétel.** *Tegyük fel, hogy az $L : K$ testbővítés véges és normális, és legyen $K \leqslant M \leqslant L$. Ekkor a következők ekvivalensek:*

(1) *az $M : K$ bővítés normális;*

(2) *ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) \subseteq M$;*

(3) *ha $\sigma \in \mathrm{Aut}_K(L)$, akkor $\sigma(M) = M$.*

*Bizonyítás.* (1)$\Longrightarrow$(2): Tegyük fel, hogy az $M : K$ bővítés normális, és legyen $\sigma \in \mathrm{Aut}_K(L)$. Legyen $\alpha$ az $M$ test tetszőleges eleme, melynek minimálpolinomja $f = m_{\alpha,K} \in K[x]$. Ekkor $f(\sigma(\alpha)) = \sigma(f(\alpha)) = 0$, azaz $\sigma(\alpha)$ is gyöke $f$-nek. Mivel $f$ lineáris tényezőkre bomlik $M[x]$-ben, ezért $\sigma(\alpha) \in M$. Így $\sigma(M) \subseteq M$.

(2)$\Longrightarrow$(3): Az állítás következik abból, hogy $\sigma^{-1} \in \mathrm{Aut}_K(L)$.

(3)$\Longrightarrow$(1): Tegyük fel, hogy tetszőleges $\sigma \in \mathrm{Aut}_K(L)$-ra $\sigma(M) = M$ teljesül. Legyen $\alpha$ az $M$ test tetszőleges eleme, melynek minimálpolinomja $f = m_{\alpha,K} \in K[x]$. Legyen $\beta$ az $f$ polinom $\alpha$-tól különböző gyöke $L$-ben (mivel az $L : K$ bővítés normális, ezért $f$ valamennyi gyöke $L$-ben van). Azt kell igazolnunk, hogy $\beta \in M$. A 4.4. Lemma szerint az $\eta = \mathrm{id}_K$ izomorfizmus kiterjeszthető egy $\vartheta\colon K(\alpha) \to K(\beta)$ injektív homomorfizmussá, amelyre $\vartheta(\alpha) = \beta$ is teljesül.

Mivel $L : K$ véges és normális bővítés, ezért $L$ valamely $g \in K[x]$ polinom felbontási testével egyezik meg. Az $L$ test a $\vartheta_g = g$ polinom felbontási teste mind a $K(\alpha)$, mind a $K(\beta)$ testek felett, ezért a 4.3. Tétel szerint $\vartheta$ kiterjeszthető egy $\sigma\colon L \to L$ izomorfizmussá. Ekkor $\sigma \in \mathrm{Aut}_K(L)$, és így (3) miatt $\sigma(M) = M$. Ebből pedig azt kapjuk, hogy $\beta = \vartheta(\alpha) = \sigma(\alpha) \in M$. Ezzel a bizonyítást befejeztük. □

megmentése Liouville érdeme, aki Galois halála után 14 évvel leközölte azt lapjában. Galois tragikus életéről Leopold Infeld írt regényt *Whom the Gods Love: The Story of Evariste Galois* (*Akit az istenek szeretnek*) címmel, utalva ezzel arra a régi görög mondásra, hogy akit az istenek szeretnek, korán hal meg.

## 8.1 Fixtestek és Galois-csoportok

Legyen $L : K$ teszőleges testbővítés. Definiáljuk a $\varphi\colon P(\mathrm{Gal}(L : K)) \to P(L)$ és $\gamma\colon P(L) \to P(\mathrm{Gal}(L : K))$ leképezéseket az alábbi módon:

$$\varphi\colon A \mapsto \{\alpha \in L \mid \sigma(\alpha) = \alpha \text{ minden } \sigma \in A\text{-ra}\} \quad (A \subseteq \mathrm{Gal}(L : K)),$$
$$\gamma\colon M \mapsto \{\sigma \in \mathrm{Gal}(L : K) \mid \sigma(\alpha) = \alpha \text{ minden } \alpha \in M\text{-re}\} \quad (M \subseteq L).$$

A $(\varphi, \gamma)$ leképezéspárt a $P(\mathrm{Gal}(L : K))$ és $P(L)$ halmazok közötti **Galois-kapcsolatnak** nevezzük.

Ebben a fejezetben az $L : K$ testbővítés közbülső testei és a $\mathrm{Gal}(L : K)$ Galois-csoport részcsoportjai közötti (Galois-)kapcsolat tulajdonságait fogjuk részletesen megvizsgálni.

**8.1. Lemma.** *Tetszőleges $A \subseteq \mathrm{Gal}(L : K)$-ra $\varphi(A)$ a $K$ testet tartalmazó részteste $L$-nek, azaz közbülső teste az $L : K$ testbővítésnek.*

*Bizonyítás.* Legyenek $\alpha, \beta \in \varphi(A)$ és $\sigma \in A$ tetszőleges elemek. Ekkor $\sigma(a) = a$ $(a \in K)$ és

$$\sigma(\alpha + \beta) = \sigma(\alpha) + \sigma(\beta) = \alpha + \beta,$$
$$\sigma(\alpha\beta) = \sigma(\alpha)\sigma(\beta) = \alpha\beta.$$

Azaz $\varphi(A)$ részgyűrűje $L$-nek. Mivel $\alpha \in L \setminus \{0\}$ esetén $\sigma(\alpha^{-1}) = \sigma(\alpha)^{-1} = \alpha^{-1}$ is teljesül, ezért $\varphi(A)$ részteste $L$-nek, amely tartalmazza $K$-t. □

**8.2. Lemma.** *Tetszőleges $M \subseteq L$-re $\gamma(M)$ az $L : K$ bővítés Galois-csoportjának részcsoportja.*

*Bizonyítás.* Legyenek $\sigma, \tau \in \gamma(M)$ és $\alpha \in M$ tetszőleges elemek. Nyilvánvaló, hogy $\mathrm{id}_L \in \gamma(M)$. Valamint teljesülnek a következők:

$$(\sigma\tau)(\alpha) = \sigma(\tau(\alpha)) \overset{\tau \in \gamma(M)}{=} \sigma(\alpha) \overset{\sigma \in \gamma(M)}{=} \alpha,$$
$$(\sigma^{-1})(\alpha) = \sigma^{-1}(\sigma(\alpha)) = (\sigma^{-1}\sigma)(\alpha) = \alpha,$$

Azaz $\gamma(M)$ részcsoportja $\mathrm{Gal}(L : K)$-nak. □

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

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

- 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 $\omega$-ra vonatkozóan**, ha $\omega(U) = U$.

**8.3. Tétel.** *Legyen $L : K$ teszőleges testbővítés, $A \subseteq \mathrm{Gal}(L : K)$ és $M \subseteq L$. Ekkor teljesülnek a következők.*

(1) *A $\varphi$ és $\gamma$ leképezések antimonotonok.*

(2) *A $\varphi\gamma$, illetve a $\gamma\varphi$ leképezés polaritás az $L$, illetve az $\mathrm{Gal}(L : K)$ halmazon.*

(3) *Az $A \subseteq \mathrm{Gal}(L : K)$ halmaz pontosan akkor zárt $\gamma\varphi$-re vonatkozóan, ha van olyan $M \subseteq L$, amelyre $A = \gamma(M)$.*

*Bizonyítás.* (1) Az állítás nyilvánvaló.

(2) Az állítást $\varphi\gamma$-ra igazoljuk, $\gamma\varphi$-re az állítás hasonlóan igazolható. Legyen $M, M' \subseteq L$, $M \subseteq M'$. Ekkor (1) felhasználva azt kapjuk, hogy $\gamma(M') \subseteq \gamma(M)$, és így szintén (1) szerint:

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

azaz $\varphi\gamma$ monoton ($\gamma\varphi$ monoton).

Legyen $M$ tetszőleges részhalmaza $L$-nek. Tegyük fel, hogy van olyan $\alpha \in M$, amely nem eleme $\varphi\gamma(M)$-nek. Ekkor

$$\alpha \notin \varphi\gamma(M) \Longleftrightarrow \text{van olyan } \sigma \in \gamma(M), \text{ amelyre } \sigma(\alpha) \neq \alpha,$$

azonban $\gamma$ definíciója miatt azt kapjuk, hogy

$$\sigma \in \gamma(M) \Longrightarrow \text{minden } \beta \in M\text{-re}, \sigma(\beta) = \beta,$$

ami $\beta = \alpha$ esetben ellentmond az előzőeknek. Ezzel igazoltuk, hogy $\varphi\gamma$ extenzív ($\gamma\varphi$ extenzív).

Legyen $M$ tetszőleges részhalmaza $L$-nek. Ekkor $\varphi\gamma$ extenzivitása miatt $M \subseteq \varphi\gamma(M)$, és így felhasználva, hogy $\gamma$ antimonoton azt kapjuk, hogy $\gamma(M) \supseteq \gamma(\varphi\gamma(M)) = \gamma\varphi\gamma(M)$. Másrészt, $\gamma\varphi$ extenzitvitása miatt $\gamma(M) \subseteq \gamma\varphi(\gamma(M)) = \gamma\varphi\gamma(M)$, így azt kapjuk, hogy

$$\gamma(M) = \gamma\varphi\gamma(M). \tag{10}$$

Ebből pedig már következik, hogy

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

azaz $\varphi\gamma$ idempotens ($\gamma\varphi$ idempotens). Ezzel igazoltuk, hogy a $\varphi\gamma$ és $\gamma\varphi$ leképezések polaritások.

(3) Tegyük fel, hogy $A \subseteq \mathrm{Gal}(L : K)$ zárt $\gamma\varphi$-re vonatkozóan, azaz $\gamma\varphi(A) = A$. Ekkor $M = \varphi(A) \subseteq L$-re teljesül, hogy $A = \gamma\varphi(A) = \gamma(\varphi(A)) = \gamma(M)$. Fordítva, tegyük fel, hogy $A = \gamma(M)$ valamely $M \subseteq L$-re. Ekkor (10) miatt

$$A = \gamma(M) = \gamma\varphi\gamma(M) = \gamma\varphi(\gamma(M)) = \gamma\varphi(A),$$

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

A továbbiakban rögzítsük az $L : K$ testbővítést és a $(\varphi, \gamma)$ Galois-kapcsolatot.

**8.4. Következmény.** *Tetszőleges $A \subseteq \mathrm{Gal}(L : K)$-ra $\varphi(A) = \varphi(\langle A \rangle)$.*

*Bizonyítás.* Mivel $A \subseteq \langle A \rangle$, ezért $\varphi$ antimonotonitása miatt $\varphi(\langle A \rangle) \subseteq \varphi(A)$. Felhasználva, hogy $\gamma\varphi(A)$ olyan részcsoportja $\mathrm{Gal}(L : K)$-nak, amely tartalmazza $A$-t, azt kapjuk, hogy $A \subseteq \langle A \rangle \subseteq \gamma\varphi(A)$. A 8.3. Tétel alkalmazva azt kapjuk, hogy

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

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

A fenti következmény szerint elegendő csupán $\mathrm{Gal}(L : K)$ részcsoportjaival foglalkozni. Legyen $G$ részcsoportja $\mathrm{Gal}(L : K)$-nak. Tetszőleges $\alpha \in L$-re definiáljuk a $T_\alpha \colon G \to L \in L^G$ leképezést az alábbi módon:

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

Mivel $L^G$ vektortér[27] $L$ felett, ezért $L^G$ a $\varphi(G) \leqslant L$ test felett is vektortér.

**8.5. Tétel.** *Legyen $G$ részcsoportja $\mathrm{Gal}(L : K)$-nak, és legyen $M \subseteq L$. Ekkor a következő állítások ekvivalensek:*

(1) *$M$ lineárisan független $\varphi(G)$ felett;*

(2) *$\{T_\alpha \mid \alpha \in M\}$ lineárisan független $\varphi(G)$ felett;*

(3) *$\{T_\alpha \mid \alpha \in M\}$ lineárisan független $L$ felett.*

*Bizonyítás.* (3)$\Longrightarrow$(2): Mivel $\varphi(G) \leqslant L$, ezért az állítás nyilvánvaló.

(2)$\Longrightarrow$(1): Tegyük fel, hogy $M$ nem lineárisan független $\varphi(G)$ felett. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_n \in M$ vektorok és $a_1, \ldots, a_n \in \varphi(G)$ skalárok, amelyek nem mind 0-ák, és amelyekre

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

Ekkor tetszőleges $\sigma \in G$-re

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

azaz $a_1T_{\alpha_1} + \cdots + a_nT_{\alpha_n} = 0$. Így a $\{T_\alpha \mid \alpha \in M\}$ vektorrendszer lineárisan független $\varphi(G)$ felett.

(1)$\Longrightarrow$(3): Tegyük fel, hogy a $\{T_\alpha \mid \alpha \in M\}$ vektorrendszer nem lineárisan független $L$ felett. Ekkor vannak olyan $\alpha_1, \ldots, \alpha_n \in M$ elemek és $a_1, \ldots, a_n \in L$ skalárok, amelyekre

$$a_1T_{\alpha_1} + \cdots + a_nT_{\alpha_n} = 0. \tag{11}$$

Tegyük fel, hogy az $\alpha_1, \ldots, \alpha_n \in M$ és $a_1, \ldots, a_n \in L$ elemeket úgy választottuk meg, hogy $n$ minimális. A (11) formulából következik, hogy tetszőleges $\sigma \in G$-re

$$a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_n) = 0 \tag{12}$$

[27] $L^G$ jelöli a $G$-ből $L$-be menő leképezések halmazát.

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

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

egyenlőség, azaz $\tau$-t alkalmazva mindkét oldalra azt kapjuk, hogy a $G$ csoport bármely $\sigma$ elemére

$$\tau(a_1)\sigma(\alpha_1) + \cdots + \tau(a_n)\sigma(\alpha_n) = 0. \tag{13}$$

Szorozzuk meg a (11) egyenlőséget $\tau(a_n)$-nel, a (13) egyenlőséget pedig $a_n$-nel, 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, 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 (12) 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 $M$ nem lineárisan független $\varphi(G)$ felett. Ezzel a tételt igazoltuk. □

Legyen $L : K$ testbővítés. Azt mondjuk, hogy **az** $\alpha \in L$ **elem szeparábilis** ($K$ felett), ha $m_{\alpha,K}$ szeparábilis $K$ felett, illetve azt mondjuk, hogy **az** $L : K$ **bővítés szeparábilis** ($K$ felett), ha minden $\alpha \in L$ elem szeparábilis.

Az $L : K$ testbővítést **Galois-bővítésnek** hívjuk, ha véges, normális és szeparábilis.

**8.6. Tétel.** *Tegyük fel, hogy $L : K$ véges testbővítés. Ekkor az $L : K$ bővítés pontosan akkor Galois-bővítés, ha $|\mathrm{Aut}_K(L)| = [L : K]$.*

**8.7. Lemma.** *Legyenek $K, L$ és $L'$ testek. Tegyük fel, hogy az $L : K$ bővítés $d$-edfokú és $\eta\colon K \to L'$ injektív homomorfizmus. Ha $L : K$ szeparábilis, és tetszőleges $\alpha \in L$-re $\eta_{m_{\alpha,K}}$ lineáris tényezőkre bomlik $L'$ felett, akkor pontosan $d$ darab injektív $L \to L'$ homomorfizmus van, amely kiterjesztése $\eta$-nak; ellenkező esetben $d$-nél kevesebb kiterjesztése van.*

*Bizonyítás.* Az állítást $d$-re vonatkozó teljes indukcióval igazoljuk. Ha $d = 1$, akkor az állítás nyilván teljesül. Tegyük fel, hogy az állítás minden olyan bővítésre igaz, amelynek fokszáma kisebb, mint $d$, és legyen $[L : K] = d \geqslant 2$.

Tegyük fel, hogy $L : K$ szeparábilis, és tetszőleges $\alpha \in L$-re $\eta_{m_{\alpha,K}}$ lineáris tényezőkre bomlik $L'$ felett. Legyen $\alpha \in L \setminus K$. Ekkor a 4.4. Lemma szerint $\eta$ pontosan $r$-féleképpen terjeszthető ki $K(\alpha) \to L'$ injektív homomorfizmussá, ahol $r$ az $\eta_{m_{\alpha,K}}$ polinom különböző gyökeinek a száma $L'$-ben. Mivel $\alpha$ szeparábilis $K$ felett, ezért $\eta_{m_{\alpha,K}}$ szeparábilis $\eta(K)$ felett. A feltétel szerint $\eta_{m_{\alpha,K}}$ lineáris tényezőkre bomlik $L'$ felett, így $\eta_{m_{\alpha,K}}$-nak pontosan $[K(\alpha) : K]$ darab

különböző gyöke van $L'$-ben. Azaz $\eta$ ennyiféleképpen terjeszthető ki $K(\alpha) \to L'$ injektív homomorfizmussá.

Legyen $\vartheta\colon K(\alpha) \to L'$ egy injektív homomorfizmus, mely kiterjesztése $\eta$-nak. Tekintsük az $L : K(\alpha)$ testbővítést. A Fokszámtétel miatt $[L : K(\alpha)] = \dfrac{[L : K]}{[K(\alpha) : K]} < d$, a 7.4. Következmény szerint pedig az $L : K(\alpha)$ bővítés normális. Legyen $\beta$ tetszőleges $L$-beli elem. Ekkor $m_{\beta,K(\alpha)} \mid m_{\beta,K}$ teljesül $K(\alpha)[x]$-ben. Így $\vartheta_{m_{\beta,K(\alpha)}} \mid \vartheta_{m_{\beta,K}}$ teljesül az $L'[x]$ polinomgyűrűben. Ezért $\vartheta_{m_{\beta,K(\alpha)}}$ lineáris tényezőkre bomlik $L'$ felett. Az indukciós feltevés szerint $\vartheta$ $[L : K(\alpha)]$-féleképpen terjeszthető ki $L \to L'$ injektív homomorfizmussá. Így ismét a Fokszámtétel alkalmazva azt kapjuk, hogy $\eta$-nak pontosan $[L : K]$ darab kiterjesztése van $L \to L'$ injektív homomorfizmussá.

Tegyük fel, hogy a lemma feltételei nem teljesülnek, azaz vagy $L : K$ nem szeparábilis vagy van olyan $\alpha \in L$, amelyre $\eta_{m_{\alpha,K}}$ nem bomlik lineáris tényezőkre $L'$ felett. Ekkor van olyan $\alpha \in L$, amelyre az $\eta_{m_{\alpha,K}}$ polinomnak kevesebb mint $[K(\alpha) : K]$ gyöke van, és így $\eta$ legfeljebb $[K(\alpha) : K]$-féleképpen terjeszthető ki $K(\alpha) \to K$ injektív homomorfizmussá. Az indukciós feltevés szerint minden ilyen injektív homomorfizmus legfeljebb $[L : K(\alpha)]$-féleképpen terjeszthető ki $L \to L'$ injektív homomorfizmussá. Így $\eta$-nak kevesebb mint $d$ kiterjesztése van. Ezzel a lemmát igazoltuk. □

*A 8.6. Tétel bizonyítása.* Tekintsük az $\eta\colon K \to L,\ k \mapsto k$ injektív homomorfizmust.

Tegyük fel, hogy az $L : K$ bővítés Galois-bővítés. Ekkor a 8.7. Lemma alkalmazható az $\eta$ injektív homomorfizmusra, és a lemma szerint $\eta$ pontosan $[L : K]$-féleképpen terjeszthető ki $L \to L$ injektív homomorfizmussá. Az 2.22. Tétel pedig éppen azt állítja, hogy ezek az injektív homomorfizmusok izomorfizmusok. Azaz $|\mathrm{Aut}_K(L)| = [L : K]$.

Tegyük fel, hogy $|\mathrm{Aut}_K(L)| = [L : K]$. Mivel az $\mathrm{Aut}_K(L)$-beli izomorfizmusok mindegyike kiterjesztése $\eta$-nak, ezért az $L : K$ bővítés szeparábilis és minden $\alpha \in L$-re $\eta_{m_{\alpha,K}} = m_{\alpha,K}$ lineáris tényezőkre bomlik $L$ felett, azaz $L : K$ normális is. Ennek következtében az $L : K$ bővítés Galois-bővítés.

Ezzel a tétel állítását igazoltuk. □

**8.8. Tétel.** *Legyen $G$ véges részcsoportja $\mathrm{Aut}(L)$-nek. Ekkor $[L : \varphi(G)] = |G|$, és így az $L : \varphi(G)$ testbővítés Galois-bővítés.*

*Bizonyítás.* Legyen $M \subseteq L$ lineárisan független vektorrendszer $\varphi(G)$ felett. Ekkor a 8.5. Tétel szerint a $\{T_\alpha \mid \alpha \in M\}$ vektorrendszer lineárisan független az $L$ feletti $L^G$ vektortérben, melynek dimenziója $|G|$. Így azt kapjuk, hogy

$$[L : \varphi(G)] = |M| \leqslant |G|.$$

A 4.3. Tétel szerint $|\gamma\varphi(G)| \leqslant [L : \varphi(G)]$, azaz $G \subseteq \gamma\varphi(G)$ miatt $[L : \varphi(G)] = |G|$ és $G = \gamma\varphi(G)$. Mivel $\gamma\varphi(G) = \mathrm{Aut}_{\varphi(G)}(L)$, ezért $|\mathrm{Aut}_{\varphi(G)}(L)| = |G| = [L : \varphi(G)]$, és így a 8.6. Tétel szerint az $L : \varphi(G)$ bővítés Galois-bővítés. □

**8.9. Tétel.** *Ha az $L : K$ testbővítés 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.* Mivel $\gamma(K) = \mathrm{Aut}_K(L)$, ezért a $|\gamma(K)| = [L : K]$ egyenlőség a 8.6. Tétel következménye. A 8.8. Tétel szerint $|\gamma(K)| = [L : \varphi\gamma(K)]$ is teljesül, mivel $\gamma(K)$ véges részcsoportja $\mathrm{Aut}(L)$-nek. A fentiekből már következik, hogy $K = \varphi\gamma(K)$, mivel $K \subseteq \varphi\gamma(K)$.

Ha az $L : K$ bővítés nem Galois-bővítés, akkor a 8.6. Tétel szerint

$$|\gamma(K)| = |\mathrm{Aut}_K(L)| < [L : K],$$

és így $K$ valódi részteste $\varphi\gamma(K)$-nak. □

## 8.2 Polinom Galois-csoportja

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

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.

A 8.9. Tételt polinomokra alkalmazva a következőt kapjuk.

**8.10. 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 $\sigma$ eleme az $L$ test automorfizmusa. Számunkra a legfontosabb az lesz, hogy $\sigma$ hogyan hat az $f$ polinom gyökeinek halmazán. A következő tétel szerint nem vesztünk információt, ha csak ezt a hatást vizsgáljuk.

**8.11. 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 $\sigma \in \mathrm{Gal}_K(f)$-re $\sigma|_R \in S_R$, és a*

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

*leképezés injektív homomorfizmus, azaz $\mathrm{Gal}_K(f)$ izomorf $S_{|R|}$ egy részcsoportjával.*

Ha $f$ irreducibilis, akkor $\mathrm{Gal}_K(f)$ tranzitívan hat $f$ gyökeinek halmazán, azaz ha $\alpha$ és $\beta$ 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 $\alpha$ 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.

## 8.3 Egy példa.

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

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

A $\leftrightsquigarrow \subseteq X \times X$ reláció nyilván reflexív és szimmetrikus. Tegyük fel, hogy az $x, y, z \in X$ elemekre teljesül, hogy $x \leftrightsquigarrow y$ és $y \leftrightsquigarrow z$. 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 $x \leftrightsquigarrow z$. Ezzel igazoltuk, hogy $\leftrightsquigarrow$ 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 $x \leftrightsquigarrow x'$ 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.

Így abban a speciális esetben, 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 $G = S_X$.

**8.12. 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

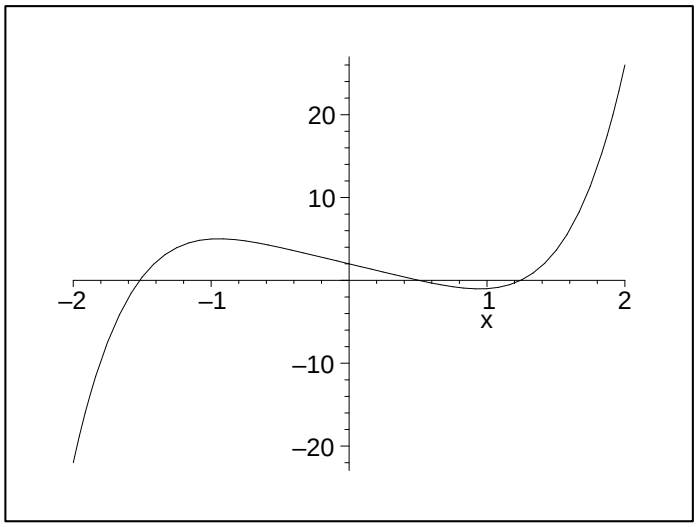
$$\{\sigma|_R \mid \sigma \in \mathrm{Gal}_K(f)\} \leqslant S_R$$

permutációcsoport tranzitív és tartalmaz transzpozíciót. Ekkor az előzőek szerint $\{\sigma|_R \mid \sigma \in \mathrm{Gal}_K(f)\} = S_R$. Továbbá, a 8.11. Tétel szerint,

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

Ezzel a bizonyítást befejeztük. □

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




**9. ábra:** Az $f = x^5 - 4x + 2 \in \mathbb{Q}[x]$ polinom grafikonja.

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

## 8.4 A Galois-elmélet főtétele és alkalmazásai

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

Az $L : K$ véges testbővítésre legyen

$$\mathcal{S}(L:K) = \{H \mid H \leqslant \mathrm{Gal}(L:K)\},$$
$$\mathcal{F}(L:K) = \{M \mid K \leqslant M \leqslant L\}.$$

Ekkor $(\mathcal{S}(L:K);\ \subseteq\ )$ és $(\mathcal{F}(L:K); \subseteq)$ részbenrendezett halmazok. Definiáljuk a $\Phi$ és $\Gamma$ leképezéseket a következőképpen:

$$\Phi\colon \mathcal{S}(L:K) \to \mathcal{F}(L:K),\ H \mapsto \varphi(H),$$
$$\Gamma\colon \mathcal{F}(L:K) \to \mathcal{S}(L:K),\ M \mapsto \gamma(M).$$

A $\Phi$ és $\Gamma$ leképezések a 8.1. és 8.2. Lemmák, valamint a 8.4. Következmény szerint jóldefiniáltak.

**8.13. Tétel (A Galois-elmélet Főtétele).** *Legyen az $L : K$ testbővítés véges Galois-bővítés. Ekkor teljesülnek a következők.*

(i) *A $\Phi$ és $\Gamma$ leképezések rendezésfordító bijekciók, melyek egymás inverzei.*

(ii) *A $\mathrm{Gal}(L : K)$ csoport bármely $H_1 \subseteq H_2$ részcsoportjára $[H_2 : H_1] = [\Phi(H_1) : \Phi(H_2)]$ teljesül.*

(iii) *Az $N \leqslant \mathrm{Gal}(L : K)$ részcsoport pontosan akkor normális, ha a $\varphi(N) : K$ bővítés normális.*

(iv) *Tegyük fel, hogy $N$ normális részcsoport az $L : K$ bővítés Galois-csoportjában, és legyen $\sigma \in \mathrm{Gal}(L : K)$. Ekkor $\sigma|_{\varphi(N)} \in \mathrm{Gal}(\varphi(N) : K)$, és a*

$$\mathrm{Gal}(L:K) \to \mathrm{Gal}(\varphi(N):K),\ \sigma \mapsto \sigma|_{\varphi(N)}$$

*leképezés szürjektív homomorfizmus, melynek magja $N$. Így*

$$\mathrm{Gal}(\varphi(N) : K) \cong G/N.$$

*Bizonyítás.* (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 $\varphi$ szürjektív is, melynek inverze $\gamma|_{\{M|K_0\leqslant M\leqslant L\}}$.

(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 $\gamma(\sigma(M)) = \sigma(\gamma(M))\sigma^{-1}$. Tegyük fel, hogy $H \lhd G$. 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.

(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 $\sigma\colon L \to L$ automorfizmus, amely kiterjesztése $\xi$-nek. Azaz a leképezés szürjektív. A fennmaradó állítás a homomorfia-tétel következménye. Ezzel igazoltuk a Galois-elmélet főtételét. □

**8.14. Példa.** *Legyen $L = \mathbb{Q}(\sqrt[4]{2}, i)$, és tekintsük a $\mathbb{Q}(\sqrt[4]{2}, i) : \mathbb{Q}$ bővítést. Mivel $L$ az $x^4-2$ polinom felbontási teste $\mathbb{Q}$ felett, ezért az $L : \mathbb{Q}$ bővítés Galois-bővítés. Felhasználva, hogy $L = \mathbb{Q}(\sqrt[4]{2} + i)$ és $m_{\sqrt[4]{2}+i,\mathbb{Q}} = x^8 + 4x^6 + 2x^4 + 28x^2 + 1$, az adódik, hogy $|\mathrm{Gal}(L : \mathbb{Q})| = [L : \mathbb{Q}] = 8$. A 8.11. Tétel szerint*

$$\mathrm{Gal}(L : \mathbb{Q}) \cong \mathrm{Gal}(L : \mathbb{Q})|_R \leqslant S_4,$$

*ahol $R = \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\}$ az $x^4 - 2$ polinom (komplex) gyökeinek halmaza. Legyen $\sigma \in \mathrm{Gal}(L : \mathbb{Q})$. Ekkor*

$$\sigma(\sqrt[4]{2}) \in \{\sqrt[4]{2}, -\sqrt[4]{2}, i\sqrt[4]{2}, -i\sqrt[4]{2}\} \text{ és } \sigma(i) \in \{i, -i\},$$

*mivel a Galois-csoport tetszőleges eleme a $\sqrt[4]{2}$ és $i$ (generáló) elemeket minimálpolinomjuk egy-egy gyökébe viszi.*

*Tekintsük a Galois-csoport azon $\sigma, \tau$ elemeit, amelyekre*

$$\sigma(\sqrt[4]{2}) = i\sqrt[4]{2}, \qquad \sigma(i) = i,$$
$$\tau(\sqrt[4]{2}) = i\sqrt[4]{2}, \qquad \tau(i) = -i$$

*teljesül. Ekkor*

$$\sigma(i\sqrt[4]{2}) = -\sqrt[4]{2}, \quad \sigma(-\sqrt[4]{2}) = -i\sqrt[4]{2}, \quad \sigma(-i\sqrt[4]{2}) = \sqrt[4]{2},$$

*és*

$$\tau(i\sqrt[4]{2}) = \sqrt[4]{2}, \quad \tau(-\sqrt[4]{2}) = -i\sqrt[4]{2}, \quad \tau(-i\sqrt[4]{2}) = -\sqrt[4]{2}.$$

*Azonosítsuk a $\sqrt[4]{2}$, $i\sqrt[4]{2}$, $-\sqrt[4]{2}$, $-i\sqrt[4]{2}$ gyököket rendre az $1, 2, 3, 4$ egészekkel. Ekkor $\sigma|_R = (1\,2\,3\,4)$, $\tau|_R = (1\,2)(3\,4)$, és*

$$\langle \sigma|_R, \tau|_R \rangle = \{\mathrm{id}, (1\,2\,3\,4), (1\,3)(2\,4), (1\,4\,3\,2), (1\,2)(3\,4), (2\,4), (1\,4)(2\,3), (1\,3)\}.$$

*Azaz $|\langle \sigma|_R, \tau|_R \rangle| = 8$ miatt*

$$\mathrm{Gal}_{\mathbb{Q}}(x^4 - 2) = \mathrm{Gal}(L : \mathbb{Q}) \cong \langle \sigma|_R, \tau|_R \rangle \cong D_4,$$

*ahol $D_4$ a négyzet szimmetriacsoportja.*

*Keressünk bázist $L$-ben a $\mathbb{Q}(\sqrt[4]{2}) : \mathbb{Q}$ negyedfokú és $L : \mathbb{Q}(\sqrt[4]{2})$ másodfokú bővítések felhasználásával. A $\mathbb{Q}$ feletti $\mathbb{Q}(\sqrt[4]{2})$ vektortérnek bázisa az*

$$1,\ \sqrt[4]{2},\ (\sqrt[4]{2})^2 = \sqrt{2},\ (\sqrt[4]{2})^3$$

*vektorrendszer. A $\mathbb{Q}(\sqrt[4]{2})$ feletti $L$ vektortérnek pedig bázisa az*

$$1,\ i$$

*vektorrendszer. Így a Fokszámtétel bizonyításában látottak szerint $L$-nek mint $\mathbb{Q}$ feletti vektortérnek bázisa az*

$$1,\ \sqrt[4]{2},\ \sqrt{2},\ (\sqrt[4]{2})^3, i,\ i\sqrt[4]{2},\ i\sqrt{2},\ i(\sqrt[4]{2})^3. \tag{14}$$

*vektorrendszer. Határozzuk meg a Galois-csoport $H = \langle \tau \rangle = \{\mathrm{id}, \tau\}$ részcsoportjához tartozó fixtestet, azaz $\Phi(H)$-t. Legyen $\alpha$ az $L$ test tetszőleges eleme, és írjuk fel az $\alpha$ elemet a (14) bázisban:*

$$\alpha = a + b\sqrt[4]{2} + c\sqrt{2} + d(\sqrt[4]{2})^3 + ei + fi\sqrt[4]{2} + gi\sqrt{2} + hi(\sqrt[4]{2})^3,$$

*ahol* $a, b, c, d, e, f, g, h \in \mathbb{Q}$. *Ekkor*

$$\tau(\alpha) = a + f\sqrt[4]{2} - c\sqrt{2} - h(\sqrt[4]{2})^3 - ei + bi\sqrt[4]{2} + gi\sqrt{2} - di(\sqrt[4]{2})^3.$$

*Így* $\tau(\alpha) = \alpha$ *pontosan akkor teljesül, ha*

$$\begin{aligned} a &= a, & b &= f, & c &= -c, & d &= -h, \\ e &= -e, & f &= b, & g &= g, & h &= -d, \end{aligned}$$

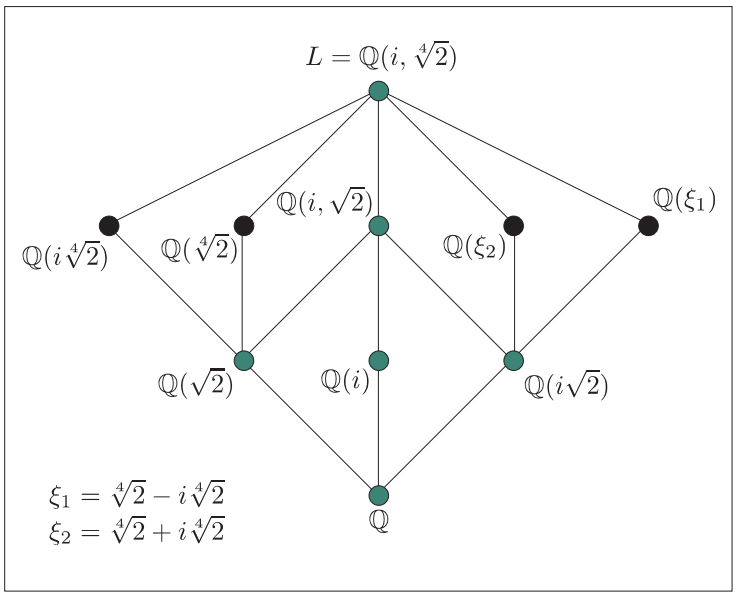
*azaz*

$$\begin{aligned} \alpha &= a + b\sqrt[4]{2} + a(\sqrt[4]{2})^3 + bi\sqrt[4]{2} + gi\sqrt{2} - ai(\sqrt[4]{2})^3 \\ &= a + b(1+i)\sqrt[4]{2} + d(1-i)(\sqrt[4]{2})^3 + gi\sqrt{2}. \end{aligned}$$

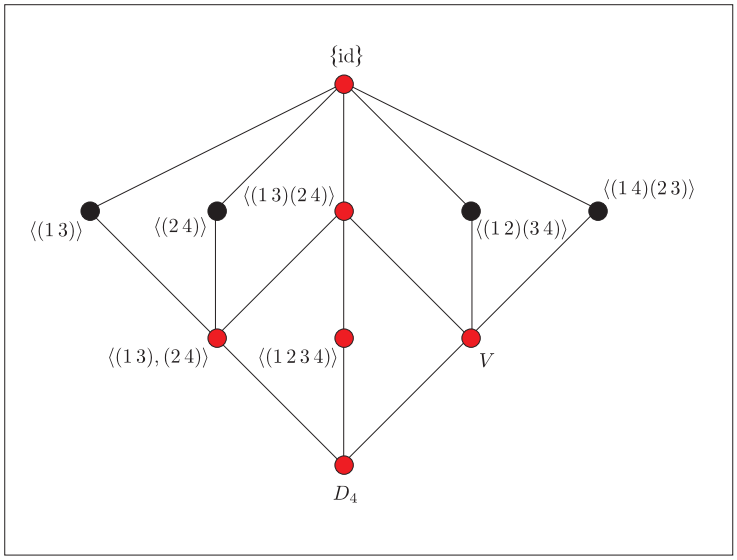
*A fentiek szerint a* $H$ *részcsoport által fixen hagyott résztest:*

$$\begin{aligned} \Phi(H) &= \left\{ a + b(1+i)\sqrt[4]{2} + ci(\sqrt[4]{2})^2 + d(1-i)(\sqrt[4]{2})^3 \mid a, b, c, d \in \mathbb{Q} \right\} \\ &= \mathbb{Q}((1+i)\sqrt[4]{2}, i(\sqrt[4]{2})^2, (1-i)(\sqrt[4]{2})^3) \\ &= \mathbb{Q}(\sqrt[4]{2} + i\sqrt[4]{2}), \end{aligned}$$

*mivel* $(1-i)\sqrt[4]{2} = \dfrac{4}{\sqrt[4]{2} + i\sqrt[4]{2}}$ *és* $i(\sqrt[4]{2})^2 = \dfrac{(\sqrt[4]{2} + i\sqrt[4]{2})^2}{2}$. *A* $L : \mathbb{Q}$ *bővítés közbülső testei és a* $\mathrm{Gal}(L : \mathbb{Q})$ *Galois-csoport részcsoportjai hálója a 4., illetve 5. ábrán láthatók. (A 4. ábrán zölddel jelölt* $M$ *közbülső testekre az* $M : \mathbb{Q}$ *bővítés normális, illetve a 5. ábrán pirossal jelölt részcsoportok normálosztók.)*




**10. ábra:** A $\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}$ bővítés közbülső testei.




**11. ábra:** A $\mathbb{Q}(i, \sqrt[4]{2}) : \mathbb{Q}$ bővítés Galois-csoportjának részcsoportjai.

## 8.5 Az egyszerűség jellemzés közbülső testekkel

**8.15. Tétel.** *Az $L : K$ algebrai bővítés pontosan akkor egyszerű, ha az $L : K$ bővítés közbülső testeinek száma véges.*

*Bizonyítás.* Tegyük fel, hogy az $L : K$ testbővítés közbülső testeinek a száma véges. Ekkor $L$ végesen generált $K$ felett. Ha $K$ is véges, akkor $L : K$ is véges. A továbbiakban tegyük fel, hogy $K$ végtelen. Tegyük fel, hogy $r = \min\{|A| \mid L = K(A)\} \geqslant 2$ és $L = K(\alpha_1, \ldots, \alpha_r)$. Legyen $M = K(\alpha_1, \alpha_2)$ és tetszőleges $\omega \in K$-ra legyen $F_\omega = K(\alpha_1 + \omega\alpha_2)$. Ekkor vannak olyan $K$-beli $\beta$ és $\gamma$ elemek, amelyekre $\beta \neq \gamma$ és $F_\beta = F_\gamma$ teljesül. Ekkor

$$\alpha_2 = (\beta - \gamma)^{-1}\big((\alpha_1 + \beta\alpha_2) - (\alpha_1 + \gamma\alpha_2)\big) \in F_\beta.$$

Valamint $\alpha_1 = (\alpha_1 + \beta\alpha_2) - \beta\alpha_2 \in F_\beta$ is teljesül, így $L = K(\alpha_1 + \beta\alpha_2, \alpha_3, \ldots, \alpha_r)$ ellentmondva az $r$-re vonatkozó feltevésnek.

Tegyük fel, hogy $L = K(\alpha)$ egyszerű algebrai bővítése $K$-nak. Legyen $m = m_{\alpha,K}$. Legyenek a $d_1, \ldots, d_k$ főpolinomok az $m$ polinom irreducibilis osztói $L[x]$-ben. Tegyük fel, hogy $K \leqslant F \leqslant L$, és legyen $m_F = m_{\alpha,F}$. Ekkor $m_F = d_i$ teljesül valamely $i \in \{1, \ldots, k\}$-ra. Legyen $m_F = a_0 + a_1x + \cdots + a_rx^r$, valamint legyen $E = K(a_0, \ldots, a_r)$. Ekkor $E \leqslant F$ és $m_F$ irreducibilis $E$ felett. Mivel $L = E(\alpha)$, ezért $[L : E] = m_F^* = [L : F]$. Azaz $F = E$. □

## 8.6 Tétel a primitív elemekről

**8.16. Tétel.** *Ha az $L : K$ testbővítés véges és szeparábilis, akkor egyszerű.*

*Bizonyítás.* Tegyük fel, hogy $L = K(\alpha_1, \ldots, \alpha_n)$ és legyen $g = m_{\alpha_1,K} \cdots m_{\alpha_n,K}$. Legyen $N$ a $g$ polinom felbontási teste $L$ felett. Ekkor $N$ a $K$ test felett is

felbontási teste $g$-nek. Így az $N : K$ bővítés Galois-bővítés és $K = \varphi(\mathrm{Gal}(N : K))$. Mivel $\mathrm{Gal}(N : K)$ véges, ezért véges sok részcsoportja van, ami a Galois-elmélet Főtétele szerint azt jelenti, hogy az $N : K$ testbővítés közbülső testeinek a száma is véges. Így az előző tétel szerint $L : K$ egyszerű. □

# Véges testek

E fejezetben az eddig kifejlesztett eszközeink egy alkalmazását mutatjuk be.

## 9.1 Véges testek leírása.

Legyen $K$ véges test. Ekkor $\mathrm{char}(K) = p > 0$ ($p$ prímszám) és $K$ prímtestét azonosítjuk $\mathbb{Z}_p$-vel. Mivel $K$ véges, ezért $[K : \mathbb{Z}_p]$ is véges. Ha $[K : \mathbb{Z}_p] = n$, akkor $K$ $n$-dimenziós vektortér a $\mathbb{Z}_p$ test felett, és így $K \cong (\mathbb{Z}_p)^k$. Ezzel az alábbi állítást kaptuk.

**9.1. Tétel.** *Minden véges test elemszáma prímhatvány.*

Most pedig azt mutatjuk meg, hogy tetszőleges $p$ prímszámra és $n$ természetes számra lényegében egy test van, amelynek elemszáma $p^n$.

**9.2. 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 $L \cong K$. □

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

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

## 9.2 Véges testek multiplikatív csoportja.

Ebben a részben a $K$ véges test $K^\times$ multiplikatív csoportját vizsgáljuk részletesebben. Már tudjuk, hogy $(K^\times; \cdot)$ Abel-csoport, azonban szerkezetének további tanulmányozásához szükségünk lesz az alábbi csoportelméleti eredményekre.

**9.5. Tétel.** *Tetszőleges $(G; +)$ véges Abel-csoport izomorf ciklikus csoportok direkt szorzatával:*

$$G \cong_\varphi \mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_s}.$$

*A $\varphi$ izomorfizmust úgy is meg tudjuk választani, hogy $d_j \mid d_k$ teljesüljön minden $1 \leqslant j < k \leqslant s$-re, valamint $s$-et az a tulajdonság határozza meg, hogy $G$ generálható $s$ elemmel, de kevesebbel nem.*

A $G$ véges csoport $e(G)$ **exponense** az a legkisebb pozitív $k$ egész, amelyre $g^k = 1$ teljesül minden $g \in G$-re. Például az $S_3$ csoport exponense $e(S_3) = |S_3| = 6$, míg $e(S_6) = |S_6|/12 = 60$.

**9.6. Következmény.** *Ha $G$ véges Abel-csoport, akkor van olyan $g \in G$ elem, amelynek rendje $e(G)$.*

**9.7. 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. □

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

**9.9. Következmény.** *Ha az $L$ test véges, akkor az $L : K$ testbővítés egyszerű.*

## 9.3 Véges testek automorfizmus-csoportja.

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

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

Ebben a fejezetben azt vizsgáljuk meg, hogy az előző fejezetekben leírt eszközök miként kapcsolódnak a harmad- és negyedfokú polinomegyenletek megoldásához.

## 10.1 A diszkrimináns

Legyen $f$ egy harmadfokú szeparábilis irreducibilis főpolinom a $K$ számtest felett. Ekkor az $f$ polinom $\mathrm{Gal}_K(f)$ Galois-csoportja tranztívan hat a polinom gyökeinek halmazán (az $f$ polinom valamely felbontási testében). Így $\mathrm{Gal}_K(f)$ izomorf az $A_3$ vagy $S_3$ csoportok valamelyikével. Vajon hogyan tudnánk eldönteni, hogy melyikkel?

A fenti problémát először általánosabban vizsgáljuk meg. Legyen $f$ egy $K$ feletti polinom, melynek gyökei $\alpha_1, \ldots, \alpha_n$ (multiplicitással) az $f$ polinom valamely $L$ felbontási testében, valamint legyen $R = \{\alpha_1, \ldots, \alpha_n\}$. Legyen

$$\delta = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i).$$

Ha $f$-nek van többszörös gyöke, akkor $\delta = 0$, különben az $f$ polinom szeparábilis és $\delta \neq 0$. Ha $\sigma \in \mathrm{Gal}_K(f)$, akkor

$$\sigma(\delta) = \prod_{1 \leqslant i < j \leqslant n} (\sigma(\alpha_j) - \sigma(\alpha_i)) = \mathrm{sgn}(\sigma)\delta,$$

ahol $\mathrm{sgn}(\sigma)$ a $\sigma$ permutáció paritása:

$$\mathrm{sgn}(\sigma) = \begin{cases} +1, & \text{ha } \sigma \text{ páros,} \\ -1, & \text{ha } \sigma \text{ páratlan.} \end{cases}$$

A következő esetek lehetségesek:

- $\delta = 0$; ekkor az $f$ polinomnak van többszörös gyöke.
- $\delta \in K \setminus \{0\}$; ekkor $\delta$ az $f$ polinom Galois-csoportjának fixtestében van, azaz tetszőleges $\sigma \in \mathrm{Gal}_K(f)$-ra

  $$\delta = \sigma(\delta) = \mathrm{sgn}(\sigma)\delta,$$

  így $\mathrm{sgn}(\sigma) = +1$. Ez pedig azt jelenti, hogy $\mathrm{Gal}_K(f)$ csak páros permutációkat tartalmaz, azaz $\mathrm{Gal}(f : K) \leqslant A_n$.
- $\delta \notin K$; ekkor $\delta$ nincs az $f$ polinom Galois-csoportjának fixtestében, így $\mathrm{Gal}_K(f) \not\subseteq A_n$. Másrészt, a $\Delta = \delta^2$ elemet $\mathrm{Gal}_K(f)$ minden eleme fixen

hagyja, így $x^2 - \Delta$ a $\delta$ elem $K$ feletti minimálpolinomja és $[K(\delta) : K] = 2$. Ekkor a $\mathrm{Gal}_K(f) \cap A_n$ részcsoport indexe 2 a $\mathrm{Gal}_K(f)$ csoportban, mivel

$$\mathrm{Gal}_K(f)/(\mathrm{Gal}_K(f) \cap A_n) \cong (\mathrm{Gal}_K(f)A_n)/A_n = S_n/A_n \cong C_2.$$

Így a Galois-elmélet Főtétele szerint $K(\delta)$ éppen a $\mathrm{Gal}_K(f) \cap A_n$ részcsoport fixteste, és $\mathrm{Gal}_K(f) \cap A_n = \mathrm{Gal}(L : K(\delta))$.

A $\Delta = \delta^2$ elemet az $f$ polinom **diszkriminánsának** nevezzük. Megjegyezzük, hogy $\delta$ függ a gyökök címkézésétől, de $\Delta$ nem. A fentieket összefoglalva az alábbi tételt kapjuk.

**10.1. Tétel.** *Legyen $f$ a $K$ számtest feletti polinom, és legyen $\Delta$ az $f$ polinom diszkriminánsa, valamint $L$ az $f$ polinom valamely felbontási teste.*

(a) *Ha $\Delta = 0$, akkor az $f$ polinomnak van többszörös gyöke.*

(b) *Ha $\Delta \neq 0$ és $\Delta$-nak van négyzetgyöke $K$-ban, akkor $\mathrm{Gal}_K(f) \leqslant A_n$.*

(c) *Ha $\Delta$-nak nincs négyzetgyöke $K$-ban; akkor van egy $\delta$ négyzetgyöke $L$-ben. $\mathrm{Gal}_K(f) \not\subseteq A_n$, és $K(\delta)$ a $\mathrm{Gal}_K(f) \cap A_n$ részcsoport fixteste.*

A gyakorlatban $\delta$ és $\Delta$ értékét az alábbi módon kaphatjuk meg (a gyökök ismeret nélkül). Legyen $L$ tetszőleges test, $\alpha_1, \ldots, \alpha_n \in L$. Ekkor az $\alpha_1, \ldots, \alpha_n$ elemekhez tartozó $\mathfrak{V}(\alpha_1, \ldots, \alpha_n)$ Vandermonde-mátrix az alábbi $L$ feletti $n \times n$-es mátrix:

$$\mathfrak{V}(\alpha_1, \ldots, \alpha_n) = \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}.$$

Korábbi tanulmányainkból jól ismert, hogy

$$V(\alpha_1, \ldots, \alpha_n) = \det(\mathfrak{V}(\alpha_1, \ldots, \alpha_n)) = \prod_{1 \leqslant i < j \leqslant n} (\alpha_j - \alpha_i).$$

Ekkor

$$\delta = V(\alpha_1, \ldots, \alpha_n) = \det \begin{pmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{pmatrix}, \text{ valamint}$$

$$\Delta = \delta^2 = \det(\mathfrak{V}(\alpha_1, \ldots, \alpha_n) \cdot \mathfrak{V}(\alpha_1, \ldots, \alpha_n)^T)$$

$$= \det \begin{pmatrix} n & \lambda_1 & \cdots & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_2 & \lambda_3 & \cdots & \lambda_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \lambda_n & \cdots & \lambda_{2n-2} \end{pmatrix},$$

ahol $\lambda_j = \alpha_1^j + \cdots + \alpha_n^j$ $(j \in \mathbb{N})$. Ha $f = x^2 + a_1 x + a_0$, akkor

$$\delta = \det \begin{pmatrix} 1 & 1 \\ \alpha_1 & \alpha_2 \end{pmatrix} = \alpha_2 - \alpha_1,$$
$$\Delta = (\alpha_2 - \alpha_1)^2 = (\alpha_1 + \alpha_2)^2 - 4\alpha_1\alpha_2 = a_1^2 - 4a_0.$$

Ha $f = x^3 + a_2 x^2 + a_1 x + a_0$, akkor

$$\delta = \det \begin{pmatrix} 1 & 1 & 1 \\ \alpha_1 & \alpha_2 & \alpha_3 \\ \alpha_1^2 & \alpha_2^2 & \alpha_3^2 \end{pmatrix} = \alpha_2\alpha_3^2 - \alpha_3\alpha_2^2 - \alpha_1\alpha_3^2 + \alpha_1\alpha_2^2 + \alpha_1^2\alpha_3 - \alpha_1^2\alpha_2,$$
$$\Delta = \det \begin{pmatrix} 3 & \lambda_1 & \lambda_2 \\ \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_2 & \lambda_3 & \lambda_4 \end{pmatrix} = 3\lambda_2\lambda_4 - 3\lambda_3^2 - \lambda_1^2\lambda_4 + 2\lambda_1\lambda_2\lambda_3 - \lambda_2^3.$$

Legyen $\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3$, $\sigma_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1$ és $\sigma_3 = \alpha_1\alpha_2\alpha_3$. Ekkor a Viète-formulák szerint: $\sigma_1 = -a_2$, $\sigma_2 = a_1$ és $\sigma_3 = -a_0$. Így

$$\lambda_1 = \sigma_1 = -a_2,$$
$$\lambda_2 = \sigma_1^2 - 2\sigma_2 = a_2^2 - 2a_1,$$
$$\lambda_3 = \sigma_1^3 - 3\sigma_2\sigma_1 + \sigma_3 = -a_2^3 + 3a_1a_2 - 3a_1,$$
$$\lambda_4 = 4\sigma_3\sigma_1 + \sigma_1^4 - 4\sigma_2\sigma_1^2 + 2\sigma_2^2 = a_2^4 - 4a_1a_2^2 + 4a_1a_2 + 2a_1^2,$$

és

$$\Delta = -4a_2^3a_0 + a_2^2a_1^2 + 18a_2a_1a_0 - 4a_1^3 - 27a_0^2.$$

**10.2. Példa.** *Tekintsük az $f = x^3 - 4x^2 + 3x + 1$ és $g = x^3 - 7x^2 + 3x + 1$ $\mathbb{Q}[x]$-beli polinomokat. Mivel az $f$ és $g$ polinomnak nincs racionális gyöke, ezért irreducibilisek $\mathbb{Q}$ felett. Az $f$ polinom diszkriminánsa* 49*, ami négyzetelem $\mathbb{Q}$-ban, így* $\mathrm{Gal}_{\mathbb{Q}}(f) \cong A_3$*. A $g$ polinom diszkriminánsa* 1300*, ami nem négyzetelem $\mathbb{Q}$-ban, így* $\mathrm{Gal}_{\mathbb{Q}}(g) \cong S_3$*.*

## 10.2 Harmadfokú polinomok

Legyen $f$ egy harmadfokú irreducibilis főpolinom a $K$ számtest felett:

$$f = x^3 + a_2x^2 + a_1x + a_0.$$

Legyen $g$ az $f$ polinom $\frac{a_2}{3}$-eltoltja:

$$g = f_{\to a_2/3} = (x - a_2/3)^3 + a_2\,(x - a_2/3)^2 + a_1\,(x - a_2/3) + a_0$$
$$= x^3 + \left(a_1 - \frac{1}{3}a_2^2\right)x + a_0 - \frac{1}{3}a_1a_2 + \frac{2}{27}a_2^3.$$

A $p = a_1 - \frac{1}{3}a_2^2$ és $q = a_0 - \frac{1}{3}a_1a_2 + \frac{2}{27}a_2^3$ jelöléseket bevezetve azt kapjuk, hogy

$$g = x^3 + px + q,$$

ahol a $g \in K[x]$ polinom is irreducibilis főpolinom. Legyen $L$ a $g \in K[x]$ polinom egy felbontási teste $K$ felett, és legyenek $\alpha_1, \alpha_2, \alpha_3$ a $g$ polinom gyökei $L$-ben.

A $g$ polinom diszkriminánsa $\Delta = -4p^3 - 27q^2$. Ekkor a 10.1. Tétel szerint $[L : K(\delta)] = 3$ és $\mathrm{Gal}(L : K(\delta)) \cong A_3$.

Legyen $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$ primitív harmadik egységgyök, és bővítsük az $L$ testet $\varepsilon$-nal. Az $L(\varepsilon)$ testben tekintsük a

$$\beta = \alpha_1 + \varepsilon\alpha_2 + \varepsilon^2\alpha_3, \qquad \gamma = \alpha_1 + \varepsilon^2\alpha_2 + \varepsilon\alpha_3$$

elemeket. Ekkor az $\varepsilon^3 = 1$ és $\varepsilon + \varepsilon^2 = -1$ egyenlőségeket és a Viète-formulákat ($\sigma_1 = \alpha_1 + \alpha_2 + \alpha_3 = 0$, $\sigma_2 = \alpha_1\alpha_2 + \alpha_2\alpha_3 + \alpha_3\alpha_1 = p$ és $\sigma_3 = \alpha_1\alpha_2\alpha_3 = -q$) felhasználva azt kapjuk, hogy teljesülnek a következők:

$$\begin{aligned}\beta^3\gamma^3 &= (\sigma_1^2 - 3\sigma_2)^3\\ &= -3p,\\ \beta^3 + \gamma^3 &= 2\sigma_1^3 - 9\sigma_2\sigma_1 + 27\sigma_3\\ &= -27q.\end{aligned}$$

Ezért $\beta^3$ és $\gamma^3$ gyökei az $x^2 + 27qx - 27p^3$ polinomnak, melynek gyökei

$$\begin{aligned}\frac{-27q \pm \sqrt{729q^2 + 108p^3}}{2} &= -\frac{27q}{2} \pm \frac{\sqrt{-27(-4p^3 - 27q^2)}}{2}\\ &= -\frac{27q}{2} \pm \frac{3}{2}(2\varepsilon + 1)\sqrt{\Delta}\\ &= -\frac{27q}{2} \pm \frac{3}{2}(2\varepsilon + 1)\delta,\end{aligned}$$

azaz $\beta^3, \gamma^3 \in K(\varepsilon, \delta)$. Így $\beta, \gamma \in K(\varepsilon, \delta, \beta)$, mivel $\gamma = -3p/\beta$. Végül,

$$\begin{aligned}\frac{1}{3}(\beta + \gamma) &= \frac{1}{3}\big(2\alpha_1 + \overbrace{(\varepsilon + \varepsilon^2)}^{-1}(\alpha_2 + \alpha_3)\big) = \alpha_1,\\ \frac{1}{3}(\varepsilon^2\beta + \varepsilon\gamma) &= \frac{1}{3}\big(2\alpha_2 + (\varepsilon + \varepsilon^2)(\alpha_1 + \alpha_3)\big) = \alpha_2,\\ \frac{1}{3}(\varepsilon\beta + \varepsilon^2\gamma) &= \frac{1}{3}\big(2\alpha_3 + (\varepsilon + \varepsilon^2)(\alpha_2 + \alpha_3)\big) = \alpha_3.\end{aligned}$$

**10.3. Példa.** *Legyen $f = x^3 + 9x^2 + 33x + 47 \in \mathbb{Q}[x]$. Ekkor $f$ irreducibilis és*

$$f_{\to 3} = (x-3)^3 + 9(x-3)^2 + 33(x-3) + 47 = x^3 + 6x + 2.$$

*Legyen $g = x^3 + 6x + 2$. Ekkor $\Delta = -972 = -2^2 \cdot 3^5$ és $\beta^3$, $\gamma^3$ az $x^2 + 54x - 5832$ polinom gyökei, melyek $54$ és $-108$. Legyen $\beta = \sqrt[3]{54} = 3\sqrt[3]{2}$. Ekkor $\gamma = -3 \cdot 6/\beta = -3\sqrt[3]{4}$, és a $g$ polinom gyökei:*

$$\begin{aligned}\frac{1}{3}(\beta + \gamma) &= \sqrt[3]{2} - \sqrt[3]{4},\\ \frac{1}{3}(\varepsilon^2\beta + \varepsilon\gamma) &= \frac{\sqrt[3]{4} - \sqrt[3]{2}}{2} - \frac{\sqrt{3}}{2}(\sqrt[3]{2} + \sqrt[3]{4})i,\\ \frac{1}{3}(\varepsilon\beta + \varepsilon^2\gamma) &= \frac{\sqrt[3]{4} - \sqrt[3]{2}}{2} + \frac{\sqrt{3}}{2}(\sqrt[3]{2} + \sqrt[3]{4})i.\end{aligned}$$

*Így az $f$ polinom gyökei:*

$$\sqrt[3]{2} - \sqrt[3]{4} - 3, \quad \frac{\sqrt[3]{4} - \sqrt[3]{2}}{2} - 3 \pm \frac{\sqrt{3}}{2}(\sqrt[3]{2} + \sqrt[3]{4})i.$$

*Az $f$ polinom Galois-csoportja $S_3$-mal izomorf.*

**10.4. Tétel (Casus Irreducibilis).** *Legyen $f \in \mathbb{Q}[x]$ olyan irreducibilis harmadfokú polinom, amelynek minden gyöke valós. Ekkor $f$ egyik gyöke sem írható fel olyan gyökkifejezésekkel, amelyeknél mindegyik gyökvonás a valós számtestben marad.*

## 10.3 Negyedfokú polinomok

Legyen $f$ egy negyedfokú irreducibilis főpolinom a $K$ számtest felett:

$$f = x^4 + a_3x^3 + a_2x^2 + a_1x + a_0.$$

Tekintsük az $f$ polinom $\frac{a_3}{4}$-eltoltját; legyen

$$g = f_{\to a_3/4} = x^4 + px^2 + qx + r \in K[x],$$

ahol

$$\begin{aligned} p &= a_2 - \frac{3}{8}a_3^2, \\ q &= -\frac{1}{2}a_2a_3 + a_1 + \frac{1}{8}a_3^3, \\ r &= a_0 + \frac{1}{16}a_2a_3^2 - \frac{1}{4}a_1a_3 - \frac{3}{256}a_3^4. \end{aligned}$$

A $g \in K[x]$ polinom is irreducibilis főpolinom. Legyen $L$ a $g \in K[x]$ polinom egy felbontási teste $K$ felett, és legyenek $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ a $g$ polinom gyökei $L$-ben. A $g$ polinom diszkriminánsa:

$$\Delta = 16p^4r - 4p^3q^2 - 128p^2r^2 + 144pq^2r - 27q^4 + 256r^3.$$

Legyen $G \leqslant S_4$ az $f$ polinom Galois-csoportja. Mivel az

$$V = \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$$

részcsoport normális részcsoportja $S_4$-nek, ezért $H = V \cap G \triangleleft G$. Legyen $M = \Phi(H)$.

Először az $M$ testet határozzuk meg. Legyen

$$\mu = \alpha_1 + \alpha_2, \quad \nu = \alpha_1 + \alpha_3, \quad \xi = \alpha_1 + \alpha_4.$$

Az $\alpha_1 + \alpha_2 + \alpha_3 + \alpha_4 = 0$ összefüggés felhasználásával adódik, hogy

$$\begin{aligned} \mu^2 &= (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4), \\ \nu^2 &= (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4), \\ \xi^2 &= (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3). \end{aligned}$$

A fentiek szerint $\mu^2, \nu^2, \xi^2 \in M$, és így $K(\mu^2, \nu^2, \xi^2) \subseteq M$. Másrészt, ha $\sigma$ olyan permutációja az $\alpha_1, \alpha_2, \alpha_3, \alpha_4$ gyököknek, amely fixen hagyja a $\mu^2, \nu^2$ és $\xi^2$ elemeket, akkor $\sigma \in N$. Ezért

$$\mathrm{Gal}(L : K(\mu^2, \nu^2, \xi^2)) \subseteq H = \mathrm{Gal}(L : M),$$

aminek következtében $M \subseteq K(\mu^2, \nu^2, \xi^2)$. Azaz $M = K(\mu^2, \nu^2, \xi^2)$. Egyszerű számolással adódnak a következő egyenlőségek:

$$\begin{aligned} \mu^2 + \nu^2 + \xi^2 &= -2p, \\ \mu^2\nu^2 + \nu^2\xi^2 + \xi^2\mu^2 &= p^2 - 4r, \\ \mu\nu\xi &= -q. \end{aligned}$$

Ekkor a Viète-formulák szerint $\mu^2, \nu^2, \xi^2$ az

$$x^3 + 2px^2 + (p^2 - 4r)x - q^2$$

polinom gyökei, amelyet a $g$ polinom **harmadfokú rezolvensének** vagy **köbös rezolvensének** nevezünk. Így

$$\begin{aligned} \alpha_1 &= \frac{1}{2}(\mu + \nu + \xi), \qquad \alpha_2 = \frac{1}{2}(\mu - \nu - \xi), \\ \alpha_3 &= \frac{1}{2}(-\mu + \nu - \xi), \quad \alpha_4 = \frac{1}{2}(-\mu - \nu + \xi), \end{aligned}$$

és $L = K(\mu, \nu, \xi)$.

**10.5. Példa.** *Legyen $f = x^4 - x^3 - 4x^2 + 4x + 1 \in \mathbb{Q}[x]$. Tegyük fel, hogy vannak olyan legalább elsőfokú $u, v \in \mathbb{Q}[x]$ polinomok, amelyekre $f = u \cdot v$ teljesül. Mivel $f$-nek nincs racionális gyöke, ezért $u^* = v^* = 2$. Az $f(0) = f(1) = f(2) = 1$ egyenlőségek következtében $u(\kappa) = v(\kappa)$, ha $\kappa \in \{0, 1, 2\}$. Így a Lagrange-féle intrpolációs tétel miatt $u = v$. Ez pedig nem lehetséges. Azaz az $f$ polinom irreducibilis.*

*Legyen $g = f_{\to -\frac{1}{4}} = x^4 - \frac{35}{8}x^2 + \frac{15}{8}x + \frac{445}{256}$. A $g$ polinom köbös rezolvense:*

$$x^3 - \frac{35}{4}x^2 + \frac{195}{16}x - \frac{225}{64},$$

*melynek gyökei: $\mu^2 = \frac{5}{4}$, $\nu^2 = \frac{15}{4} + \frac{3\sqrt{5}}{2}$, $\xi^2 = \frac{15}{4} - \frac{3\sqrt{5}}{2}$. A $\mu$, $\nu$ és $\xi$ elemeket úgy válasszuk meg, hogy $\mu\nu\xi = -\frac{15}{8}$ is teljesüljön, pl.*

$$\mu = \frac{\sqrt{5}}{2}, \quad \nu = \sqrt{\frac{15}{4} + \frac{3\sqrt{5}}{2}}, \quad \xi = -\sqrt{\frac{15}{4} - \frac{3\sqrt{5}}{2}}.$$

*Ekkor a $f$ polinom gyökei:*

$$\begin{aligned} \alpha_1 &= \frac{1}{2}(\mu + \nu + \xi) + \frac{1}{4}, \\ \alpha_2 &= \frac{1}{2}(\mu - \nu - \xi) + \frac{1}{4}, \\ \alpha_3 &= \frac{1}{2}(-\mu + \nu - \xi) + \frac{1}{4}, \\ \alpha_4 &= \frac{1}{2}(-\mu - \nu + \xi) + \frac{1}{4}. \end{aligned}$$

*Valamint, az $f$ polinom Galois-csoportja izomorf $C_4$-gyel.*

Legyen $K$ tetszőleges számtest. Bármely $f = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ negyedfokú főpolinomra az

$$y^3 - by^2 + (ac - 4d)y - c^2 - a^2d + 4bd \in K[y]$$

polinomot $f$ **köbös rezolvensének** vagy **harmadfokú rezolvensének** nevezzük.

**10.6. Tétel.** *Legyen $K$ tetszőleges számtest, $f = x^4 + ax^3 + bx^2 + cx + d \in K[x]$ pedig tetszőleges negyedfokú főpolinom. Ha az $s$ szám gyöke $f$ köbös rezolvensének, akkor $f$ előáll*

$$f = \left(x^2 + \left(\frac{a}{2} + q\right)x + \frac{s}{2} + r\right)\left(x^2 + \left(\frac{a}{2} - q\right)x + \frac{s}{2} - r\right)$$

*alakban, ahol a $q$ és $r$ számokat az alábbi feltételek határozzák meg:*

$$q^2 = \frac{a^2}{4} + s - b, \qquad r^2 = \frac{s^2}{4} - d,$$

*és $q, r$ előjele úgy választandó, hogy $2qr = \frac{a}{2}s - c$ teljesüljön.*

**10.7. Példa.** *Tekintsük a 10.5. Példában látott $f = x^4 - x^3 - 4x^2 + 4x + 1 \in \mathbb{Q}[x]$ polinomot. Az $f$ polinom köbös rezolvense:*

$$x^3 + 4x^2 - 8x - 33,$$

*melynek gyökei: $-3$, $-\frac{1}{2} \pm \frac{3\sqrt{5}}{2}$. Legyen $s = -3$. Ekkor a 10.6. Tétel szerint*

$$f = \left(x^2 - \frac{1 + \sqrt{5}}{2}x + \frac{\sqrt{5} - 3}{2}\right) \cdot \left(x^2 - \frac{1 - \sqrt{5}}{2}x - \frac{\sqrt{5} + 3}{2}\right).$$

# Egyenletek megoldása radikálokkal

## 11.1 Feloldható csoportok

A $G$ csoport **normálláncának** nevezzük $G$ részcsoportjainak egy $G_0, \dots, G_n$ 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 normálsorozata, amelynek faktorai Abel-csoportok.[28]

**11.1. Példa.** (a) *Az $S_3$ csoport feloldható, mivel a*

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

*normállánc faktorai Abel-csoportok, sőt ciklikus csoportok:*

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

(b) *Az $S_4$ csoport is feloldható, az*

$$\{\mathrm{id}\} \lhd \{\mathrm{id}, (1\,2)(3\,4)\} \lhd \{\mathrm{id}, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \lhd A_4 \lhd S_4$$

*normállánc faktorai Abel-csoportok.*

(c) *Legyen $G$ végesen generált Abel-csoport, pl. $G = \langle g_1, \dots, g_n \rangle$ ($n \in \mathbb{N}$, $g_1, \dots, g_n \in G$). Legyen $G_j = \langle g_1, \dots, g_{n-j} \rangle$ ($0 \leqslant j \leqslant n$). Ekkor $G_0 = G$ és $G_j \lhd G_{j-1}$ teljesül minden $j$-re ($1 \leqslant j \leqslant n$), sőt a $G_{j-1}/G_j$ csoport ciklikus, mivel $G_{j-1}/G_j = \langle g_{n-j+1} + G_j \rangle$. Így a $G$ csoport feloldható.*

[28] Niels Henrik **Abel** (1802. augusztus 5., Findø-szigetén (Stavanger közelében), Norvégia – 1829. április 6., Froland, Norvégia) norvég matematikus. Abel a teológus és filológus Soren Georg Abelnek, és Ane Marie Simonsonnak a fia. Hat lánytestvére volt. Abel 1821-ben ösztöndíjjal beiratkozott Christiania (ma Oslo) egyetemére, amit 1822-ben el is végzett. 1825-től 1827-ig külföldön dolgozott, főként Párizsban, Berlinben és Göttingenben. Visszatérése után docens lett a Christianiai Egyetemen és Mérnökiskolában. 1829-ben tuberkulózisban halt meg. Kutatásai:

- 1821-ben úgy vélte, megtalálta az ötödfokú egyenletek gyökképletét és cikket nyújtott be a dán Ferdinand Degenhez, a Royal Society of Copenhagen folyóiratában való közlésre. Miután Degen numerikus példákat kért, Abel felismerte eljárásának hibáját.
- 1824-ben már az ötödfokú egyenlet megoldhatatlanságát publikálta egy tömör, hatoldalas cikkben.
- Az elliptikus függvényekkel is foglalkozott, ezen a területen Carl Gustav Jacob Jacobival dolgozott együtt.

Abelről nevezték el az Abel-csoportot és az Abel-díjat.

Az $A_n$ ($n \geqslant 5$) permutációcsoport egyszerűségére vonatkozó tételt bizonyítás nélkül közöljük, a tétel bizonyítása megtalálható Kiss E. [4]-ben (4.12.31. Tétel, 249–251. old.).

**11.2. Tétel.** *Az $A_n$ alternáló csoport $n \geqslant 5$ esetén egyszerű.*

Mivel $A_n$ nem Abel-csoport, ha $n \geqslant 5$, ezért feloldható sem lesz.

**11.3. 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.*

**11.4. Lemma.** *Legyenek $G$ és $K$ csoportok. Legyen $H$ részcsoport $G$-ben, valamint $M$ és $N$ olyan normális részcsoportok $G$-ben, amelyekre $M \subseteq N$ teljesül. Legyen továbbá $\varphi\colon G \to K$ szürjektív homomorfizmus. Ekkor igazak a következők.*

(a) $\ker(\varphi) \triangleleft G$ *és* $G/\ker(\varphi) \cong K$;

(b) $N \cap H \triangleleft H$, $N \triangleleft NH$ *és* $NH/N \cong H/(N \cap H)$;

(c) $M \triangleleft N$, $N/M \triangleleft G/M$ *és* $(G/M)/(N/M) \cong G/N$.

A 11.4. Lemma bizonyítása megtalálható [2]-ben és [4]-ben is. Az (a) állítás Homomorfia-tétel, a (b) állítás I. Izomorfia-tétel, végül a (c) állítás pedig II. izomorfia-tétel néven ismeretes.

*A 11.3. Tétel bizonyítása.* (a) Tegyük fel, hogy $G$ feloldható. Legyen

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

olyan normálllánca $G$-nek, melynek faktorai Abel-csoportok. Ekkor

$$\{1\} = H \cap G_0 \triangleleft H \cap G_1 \triangleleft \cdots \triangleleft H \cap G_{n-1} \triangleleft H \cap G_n = H$$

normálllánca $H$-nak, melynek faktorai:

$$\begin{aligned}(H \cap G_i)/(H \cap G_{i-1}) &= (H \cap G_i)/((H \cap G_i) \cap G_{i-1}) && (G_{i-1} \subseteq G_i)\\ &\cong ((H \cap G_i)G_{i-1})/G_{i-1} && (11.4.(b))\\ &\leqslant G_i/G_{i-1}\end{aligned}$$

maitt Abel-csoportok. Azaz $H$ is feloldható.

(b) Tegyük fel, hogy $G$ feloldható és $N \triangleleft G$. Legyen

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

olyan normálllánca $G$-nek, melynek faktorai Abel-csoportok. Mivel $N$ részcsoportja is $G$-nek, ezért az (a) állítás szerint $N$ feloldható. Mivel $N$ normális részcsoport, $G_i$ pedig részcsoport $G$-ben, ezért $N \triangleleft NG_i$; legyen $N_i = (NG_i)/N$. Tekintsük a

$$\begin{aligned}q&\colon G \to G/N,\ g \mapsto Ng,\\ q_i&\colon N_i \to N_i/N_{i-1},\ n \mapsto N_{i-1}n\end{aligned}$$

természetes homomorfizmusokat. Ekkor $q(G_i) = \{Ng \mid g \in G_i\} = N_i$ miatt a $(qq_i)|_{G_i}$ leképezés létezik és szürjektív homomorfizmus. Továbbá, tetszőleges $g \in G_i$ elemre

$$g \in \ker\left((qq_i)|_{G_i}\right) \Longleftrightarrow Ng \in NG_{i-1} \Longleftrightarrow g \in NG_{i-1},$$

azaz $\ker\left((qq_i)|_{G_i}\right) = NG_{i-1} \cap G_i$. Így

$$\begin{aligned} N_i/N_{i-1} &\cong G_i/(NG_{i-1} \cap G_i) && \text{(11.4.(a))} \\ &\cong (G_i/G_{i-1})/((NG_{i-1} \cap G_i)/G_{i-1}), && \text{(11.4.(c))} \end{aligned}$$

azaz $N_i/N_{i-1}$ izomorf a $G_i/G_{i-1}$ Abel-csoport egy faktorcsoportjával, így maga is Abel-csoport. Ezzel igazoltuk, hogy $G/N$ is feloldható.

Tegyük fel, hogy $N \lhd G$-re $N$ és $G/N$ is feloldható. Legyenek

$$\begin{aligned} \{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_{s-1} \lhd N_s = N, \text{ illetve} \\ N/N = N_s/N \lhd N_{s+1}/N \lhd \cdots \lhd N_{s+t-1}/N \lhd N_{s+t}/N = G/N \end{aligned}$$

olyan normálláncok $N$-ben, illetve $G/N$-ben, amelyek faktorai Abel-csoportok. Ekkor $G$ is feloldható, mivel az

$$\{1\} = N_0 \lhd N_1 \lhd \cdots \lhd N_{s-1} \lhd N_s = N = N_s \lhd N_{s+1} \lhd \cdots \lhd N_{s+t-1} \lhd N_{s+t} = G$$

normállánc faktorai Abel-csoportok. □

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

*Bizonyítás.* Mivel $n \geqslant 5$ esetén $S_n$-nek pontosan három darab normális részcsoportja van: $\{\mathrm{id}\}$, $A_n$, $S_n$ és a $A_n$ nem feloldható, ezért a 11.3. Tétel miatt $S_n$ sem feloldható. □

## 11.2 Polinomok feloldható Galois-csoporttal

Legyen $L : K$ tetszőleges testbővítés, $\beta \in L$. Azt mondjuk, hogy $\beta$ **radikál** $K$ felett, ha $\beta^n \in K$ teljesül valamely $n \in \mathbb{N}$-re.

Az $L : K$ testbővítés **radikálbővítés**, ha van az $L : K$ testbővítés közbülső testeinek olyan $L_0, \ldots, L_r$ sorozata, amelyre teljesülnek a következők:

(1) $L_0 = K$, $L_r = L$,

(2) $L_j = L_{j-1}(\beta_i)$, ahol $\beta_i \in L$ radikál $L_{i-1}$ felett.

Legyen $f$ tetszőleges polinom a $K$ test felett. Azt mondjuk, hogy az $f$ polinom **radikálokkal megoldható**, ha van olyan $L$ test, amelyre az $L : K$ testbővítés olyan radikálbővítés, amely felett $f$ elsőfokú polinomok szorzatára bontható. Fontos megjegyezni, hogy az $L$ test nem feltétlenül felbontási teste $f$-nek.

**11.6. Tétel.** *Legyen $K$ tetszőleges test. Tegyük fel, hogy az $f \in K[x]$ polinom szeparábilis és Galois-csoportja feloldható, valamint* $\mathrm{char}(K) \nmid |\mathrm{Gal}_K(f)|$. *Ekkor az $f$ polinom radikálokkal megoldható.*

*Bizonyítás.* Legyen $d = |\mathrm{Gal}_K(f)|$, $\varepsilon$ $d$-edik primitív egységgyök és $L = K(\varepsilon)$. Mivel $\mathrm{char}(K) \nmid d$, ezért $L$ pontosan $d$ darab $d$-edik egységgyököt tartalmaz. Legyen $N$ az $f$ polinom felbontási teste $L$ felett, az $N$ testben $f$ gyökei legyenek $\alpha_1, \ldots, \alpha_n$, valamint legyen $M = K(\alpha_1, \ldots, \alpha_n)$. Mivel az $N : L$ testbővítés Galois-bővítés, ezért $\mathrm{Gal}_L(f) = \mathrm{Gal}(N : L)$ fixteste $L$.

Legyen $\sigma \in \mathrm{Gal}_L(f)$. Ekkor $\sigma(M) = M$ miatt $\sigma|_M \in \mathrm{Gal}(M : L \cap M)$. Továbbá, a

$$\varrho\colon \mathrm{Gal}_L(f) \to \mathrm{Gal}(M : L \cap M),\ \sigma \mapsto \sigma|_M$$

leképezés homomorfizmus. Ha $\sigma|_M = \mathrm{id}_M$, akkor $\sigma = \mathrm{id}_N$, mivel

$$N = L(\alpha_1, \ldots, \alpha_n),$$

azaz $\varrho$ injektív homomorfizmus. Ekkor

$$\mathrm{Gal}_L(f) \underset{\varrho}{\hookrightarrow} \mathrm{Gal}(M : L \cap M) \leqslant \mathrm{Gal}(M : K) \cong \mathrm{Gal}_K(f)$$

következtében $\mathrm{Gal}_L(f)$ is feloldható, így van olyan

$$\{\mathrm{id}_N\} = G_0 \triangleleft G_1 \triangleleft \cdots \triangleleft G_r = \mathrm{Gal}_L(f)$$

normállánca, melynek faktorai ciklikus csoportok.

A Galois-elmélet Főtétele szerint a $G_i \leqslant \mathrm{Gal}_L(f)$ részcsoportnak megfelelő résztest legyen $L_i$ $(0 \leqslant i \leqslant r)$. Ekkor $L = L_r \leqslant L_{r-1} \leqslant \cdots \leqslant L_1 \leqslant L_0 = N$ és tetszőleges $j \in \{1, \ldots, r\}$-re teljesülnek a következők:

$$L_0 : L_r \text{ Galois-bővítés} \quad \Rightarrow \quad L_0 : L_j \text{ Galois-bővítés}$$

$$\Downarrow \text{ (a Galois-elmélet Főtétele)}$$

$$L_j = \varphi(G_j) \text{ és } \mathrm{Gal}(L_0 : L_j) = \gamma(L_j) = G_j,$$

valamint

$$L_0 : L_j \text{ Galois-bővítés és } G_{j-1} \triangleleft G_j = \mathrm{Gal}(L_0 : L_j)$$

$$\Downarrow \text{ (a Galois-elmélet Főtétele)}$$

$$\varphi(G_{j-1}) : L_j \text{ normális bővítés és } \mathrm{Gal}(L_{j-1} : L_j) \cong G_j/G_{j-1}.$$

Mivel $G_j/G_{j-1}$ ciklikus, ezért az $L_{j-1} : L_j$ tesbővítés is ciklikus és $[L_{j-1} : L_j] = |G_j/G_{j-1}|$. Így $\mathrm{char}(K) \nmid [L_{j-1} : L_j]$, mivel $d \mid |G_j/G_{j-1}|$, és van olyan $\beta_j \in L_{j-1}$ radikál $L_j$ felett, amelyre $L_{j-1} = L_j(\beta)$. Így az $N : L$ bővítés radikálbővítés, aminek következtében az $N : K$ bővítés is az. Az $f$ polinom $N$ felett elsőfokú tényezőkre bomlik, ezért $f$ megoldható radikálokkal. □

Ha a $K$ test karakterisztikája 0, akkor a 11.6. Tétel sokkal egyszerűbbé válik.

**11.7. Következmény.** *Legyen $K$ test, melynek karakterisztikája 0. Ha az $f \in K[x]$ polinom Galois-csoportja feloldható, akkor az $f$ polinom radikálokkal megoldható.*

## 11.3 Radikálokkal megoldható polinomok

**11.8. Tétel.** *Tegyük fel, hogy az $L : K$ testbővítés Galois-bővítés, $M = L(\beta)$, ahol $\beta$ gyöke az $x^n - \vartheta \in L[x]$ polinomnak, és* $\mathrm{char}(K) \nmid n$. *Ekkor van olyan $N : M$ testbővítés, amely radikálbővítés és $N : K$ Galois-bővítés.*

*Bizonyítás.* Legyen $\varepsilon$ primitív $n$-edik gyök. Ekkor $M(\varepsilon)[x]$-ben

$$x^n - \vartheta = \prod_{k=0}^{n-1} (x - \varepsilon^k \beta),$$

azaz $M(\varepsilon)$ felbontási teste az $x^n - \vartheta$ polinomnak $L$ felett, amelynek $n$ különböző gyöke van $M(\varepsilon)$-ban, ezért $M(\varepsilon) : L$ Galois-bővítés (és radikál bővítés is). Legyen $f = \prod_{\sigma \in \mathrm{Gal}(L:K)} (x^n - \sigma(\vartheta))$, amelynek felbontási teste $M(\varepsilon)$ felett legyen $N$. Ha $\gamma \in N$ gyöke $x^n - \sigma(\vartheta)$, akkor

$$x^n - \sigma(\vartheta) = \prod_{k=0}^{n-1} (x - \varepsilon^k \gamma),$$

azaz $N$ felbontási teste $f$-nek $K$ felett is, és $f$ szeparábilis $M(\varepsilon)$ felett. Ezért az $N : K$ bővítés is szeparábilis. Mivel tetszőleges $\tau \in \mathrm{Gal}(L : K)$-ra $\tau_f = f$, ezért $f \in K[x]$. Legyen $g \in K[x]$ olyan polinom, amelynek felbontási teste $K$ felett $L$. Ekkor $N$ az $fg$ polinom felbontási teste $K$ felett, így az $N : K$ bővítés normális, valamint radikálbővítés is. □

**11.9. Tétel.** *Tegyük fel, hogy az $L = L_r \colon L_{r-1} \colon \ldots \colon L_0 \colon K$ , testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$ és $\beta_i$ az $x^{n_i} - \vartheta_i \in L_{i-1}$ polinom gyöke $(i = 1, \ldots, r)$. Ha* $\mathrm{char}(K) \nmid n_1 \cdots n_r$, *akkor van olyan $M : L$ testbővítés, amelyre $M : K$ Galois-bővítés és radikálbővítés.*

*Bizonyítás.* Teljes indukcióval igazoljuk az állítást ($r$-re vonatkozó). Ha $r = 1$, akkor $M = L(\varepsilon)$-ra teljesül az állítás, ahol $\varepsilon$ primitív $n_1$-edik egységgyök. Tegyük fel, hogy $r-1$ ($\geqslant 1$)-re teljesül az állítás, legyen $M_{r-1} : L_{r-1}$ olyan testbővítés, amelyre $M_{r-1} : K$ Galois- és radikálbővítés. Legyen $m_r = m_{\beta_r, L_{r-1}}$, és legyen $l_r$ irreducibilis osztója az $m_r \in M_{r-1}[x]$ polinomnak. Legyen $\gamma$ az $l_r$ polinom gyöke (valamely felbontási testében). Tekintsük az $\mathfrak{i} \colon L_{r-1} \to M_{r-1}$, $\alpha \mapsto \alpha$ injektív homomorfizmust. Mivel $\mathfrak{i}_{m_r}(\gamma) = m_r(\gamma) = 0$, ezért van olyan $\mathfrak{j} \colon L_{r-1}(\beta_r) \to M_{r-1}(\gamma)$ injektív homomorfzmus, amely kiterjesztése $\mathfrak{i}$-nek. Feltehető, hogy $L \leqslant M_{r-1}(\beta)$. Legyen $M = M_{r-1}(\beta_r)$. Ekkor $M_{r-1} : K$ Galois bővítés, $\beta_r$ gyöke az $x^{n_r} - \vartheta_r \in M_{r-1}[x]$ polinomnak és $\mathrm{char}(K) \nmid n_r$. Így van olyan $M_r : M_{r-1}(\beta_r)$ radikálbővítés, amelyre $M_r : K$ Galois-bővítés. Az

$$M_r \colon M_{r-1}(\beta_r) \colon M_{r-1} \colon K$$

testláncot tanulmányozva kapjuk, hogy $M_r : K$ radikálbővítés. □

**11.10. Tétel.** *Tegyük fel, hogy az $L = L_r \colon L_{r-1} \colon \ldots \colon L_0 \colon K$ , testbővítéseknek olyan sorozata, ahol $L_i = L_{i-1}(\beta_i)$, $\beta_i$ az $x^{n_i} - \vartheta_i \in L_{i-1}[x]$ polinom gyöke $(i = 1, \ldots, r)$ és* $\mathrm{char}(K) \nmid n_1 \cdots n_r$. *Ha az $f \in K[x]$ polinom $L$ felett elsőfokú polinomok szorzatára bontható, akkor* $\mathrm{Gal}_K(f)$ *feloldható.*

*Bizonyítás.* Feltehető, hogy $L : K$ Galois-bővítés. Ekkor $L : L_i$ is Galois-bővítés minden $i$-re $(1 \leqslant i \leqslant r)$, továbbá az $x^{n_i} - \vartheta_i$ polinomnak van gyöke $L$-ben, ezért elsőfokú polinomok szorzatára bomlik $L$ felett. Ez pedig biztosítja, hogy $L$ tartalmaz primitív $n_i$-edik egységgyököket. Legyen $n = \text{lk.k.t.}(n_1, \ldots, n_r)$ és $\varepsilon$ legyen egy $n$-edik primitív egységgyök. Legyen $L'_i = L_i(\varepsilon)$ és $G_i = \text{Gal}(L : L'_i)$ $(i = 0, 1 \ldots, r)$. Mivel $L'_i : L'_{i-1}$ az $x^{n_i} - \vartheta_i \in L'_{i-1}[x]$ polinom felbontási teste, ezért az $L'_i : L'_{i-1}$ bővítés ciklikus. Így $G_i \triangleleft G_{i-1}$ és $G_{i-1}/G_i \cong \text{Gal}(L'_i : L'_{i-1})$. Ezért a $G_0 = \text{Gal}(L : L'_0) = \text{Gal}(L : K(\varepsilon))$ Galois-csoport feloldható. A $K(\varepsilon)$ test az $x^n - 1 \in K[x]$ polinom felbontási teste, ezért $\text{Gal}(K(\varepsilon) : K)$ Abel-csoport, és emiatt feloldható:

$$\text{Gal}(K(\varepsilon) : K) \cong \text{Gal}(L : K)/\text{Gal}(L : K(\varepsilon)) = \text{Gal}(L : K)/G_0$$

ezért $\text{Gal}(L : K)/G_0$ is feloldható. Ez pedig azt jelenti, hogy $\text{Gal}(L : K)$ is feloldható. Legyen $N \leqslant L$ az $f$ polinom felbontási teste. A Galois-elmélet Főtétele szerint:

$$\text{Gal}_K(f) \cong \text{Gal}(N : K) \cong \text{Gal}(L : K)/\text{Gal}(L : N),$$

azaz $\text{Gal}_K(f)$ is feloldható. □

Ha a $K$ test karakterisztikája 0, akkor a 11.10. Tétel állítása az alábbi módon fogalmazható meg.

**11.11. Következmény.** *Tegyük fel, hogy az* $L = L_r : L_{r-1} : \ldots : L_0 : K$ *, testbővítéseknek olyan sorozata, ahol* $L_i = L_{i-1}(\beta_i)$*,* $\beta_i$ *az* $x^{n_i} - \vartheta_i \in L_{i-1}[x]$ *polinom gyöke* $(i = 1, \ldots, r)$*. Ha az* $f \in K[x]$ *polinom* $L$ *felett elsőfokú polinomok szorzatára bontható, akkor* $\text{Gal}_K(f)$ *feloldható.*

# Geometriai szerkeszthetőség

## 12.1 Szerkesztés körzővel és vonalzóval

A szerkesztéshez használható két legelemibb geometriai eszköz a vonalzó[29] és a körző[30]. A legegyszerűbb lépések, amelyeket ezekkel az eszközökkel megtehetünk, a következők:

- A vonalzót két adott ponthoz illesztve megrajzolhatjuk a két ponton áthaladó egyenest.
- Két adott pont távolságát körzőnyílásba vehetjük.
- Adott pont körül adott körzőnyílással kört rajzolhatunk.

Új pontokat pedig a következőképpen kaphatunk:

($E_1$) Két metsző egyenes metszéspontját megkereshetjük.

($E_2$) Egy kör és az azt metsző egyenes metszéspontjait megkereshetjük.

($E_3$) Két egymást metsző kör metszéspontjait megkereshetjük.

**12.1. Definíció.** *Ha egy szerkesztési feladatot pusztán az* ($E_1$)–($E_3$) *lépések véges sokszori alkalmazásával végzünk, akkor a szerkesztést* ***euklideszi szerkesztésnek*** *nevezzük.*

## 12.2 Szerkesztés valós alaptest felett

A továbbiakban az euklideszi szerkesztés algebrai leírását szeretnénk megadni valós alaptest felett.

**12.2. Definíció.** *Legyen $H$ az $\mathcal{S}$ sík tetszőleges részhalmaza. Az $e \subseteq \mathcal{S}$ egyenest* ***$H$-egyenesnek*** *nevezzük, ha $e$ legalább két különböző $S$-beli pontot tartalmaz. A $k = k(O, r) \subseteq \mathcal{S}$ kör(vonala)t* ***$H$-körnek*** *nevezzük, ha a $k$ kör $O$ középpontja $H$-ban van, és $r$ sugara megegyezik két $H$-beli pont távolságával.*

**12.3. Definíció.** *Legyen $H$ az $\mathcal{S}$ sík tetszőleges részhalmaza. Definiáljuk a $\mathcal{E}_1(H)$, $\mathcal{E}_2(H)$ és $\mathcal{E}_3(H)$ halmazokat a következőképpen:*

- *$\mathcal{E}_1(H)$ azon $P$ pontok halmaza, amelyekhez vannak olyan különböző $e$ és $f$ $H$-egyenesek, amelyekre $P = e \cap f$;*

[29] Fontos, hogy a vonalzó nem a hétköznapi értelemben vett vonalzó, hanem egy végtelen, egyélű és beosztás nélküli szerkezet, amellyel bármely két adott ponton át egyenes húzható.

[30] A körzőnk tetszőlegesen nagy nyílású.

- $\mathcal{E}_2(H)$ *azon* $P$ *pontok halmaza, amelyekhez van olyan* $e$ $H$*-egyenes és* $k$ $H$*-kör, amelyekre* $P \in e \cap k$*;*
- $\mathcal{E}_3(H)$ *azon* $P$ *pontok halmaza, amelyekhez vannak olyan különböző* $k_1$ *és* $k_2$ $H$*-körök, amelyekre* $P \in k_1 \cap k_2$*.*

*A* $H \cup \mathcal{E}_1(H) \cup \mathcal{E}_2(H) \cup \mathcal{E}_3(H)$ *halmaz elemei éppen azok a pontok, amelyek az* $(E_1)$—$(E_3)$ *elemi szerkesztési lépések egyszeri végrehajtásával adódnak.*

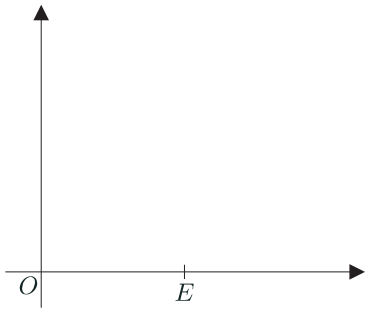
**12.4. Definíció.** *Legyen adott az* $\mathcal{S}$ *sík* $H$ *részhalmaza, amelyből kiindulva definiáljuk a* $H_i$ $(i \in \mathbb{N}_0)$ *halmazokat a következő módon:*

$$H_0 = H,$$
$$H_{i+1} = H_i \cup \mathcal{E}_1(H_i) \cup \mathcal{E}_2(H_i) \cup \mathcal{E}_3(H_i).$$

*Valamint legyen* $\mathcal{E}(H) = \cup_{i=0}^{\infty} H_i$*. Azt mondjuk, hogy* ***a*** $P \in \mathcal{S}$ ***pont euklideszi módon (körzővel és vonalzóval) megszerkeszthető a*** $H$ ***ponthalmazból****, ha* $P \in \mathcal{E}(H)$*.*

Ha $|H| \leqslant 1$, akkor $H$-ból új pontot nem tudunk szerkeszteni. Ezért a továbbiakban feltesszük, hogy $H$ legalább két pontot tartalmaz. A $(H, P)$ párt, ahol $H$ az adott ponthalmaz, $P$ pedig a megszerkesztendő pont, **szerkesztési feladatnak** nevezzük.

A geometriai problémát a koordináta-geometria segítségével fogjuk algebrai problémává átfogalmazni. Ennek egyik kézenfekvő módja, ha felveszünk egy Descartes-féle koordináta-rendszert: az adott $H$ ponthalmazból kiválasztunk két különböző pontot, amelyeket a továbbiakban $O$, illetve $E$ jelöl, és a koordináta-rendszer tengelyeit úgy vesszük fel, hogy $O$ az origó, $E$ pedig az $(1, 0)$ pont legyen.




**12. ábra:** az $O = (0, 0)$ és $E = (1, 0)$ pontok.

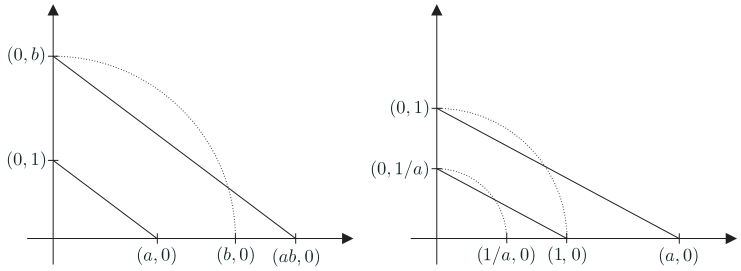
**12.5. Állítás.** (1) *A* $H$*-beli* $O$*,* $E$ *pontokból a két tengely megszerkeszthető.*
(2) *Egy* $(a, b)$ *pont akkor és csak akkor szerkeszethető meg* $H$*-ból, ha* $(a, 0)$ *és* $(b, 0)$ *megszerkeszthető.*
(3) *Valahányszor az* $(a, 0)$*,* $(b, 0)$ *pontok megszerkeszthetők* $H$*-ból, mindannyiszor megszerkeszthetők a következő pontok is:*

(i) $(a + b, 0)$*,* $(-a, 0)$*,*

(ii) $(ab, 0)$*,* $(1/a, 0)$ $(ha\ a \neq 0)$*,*

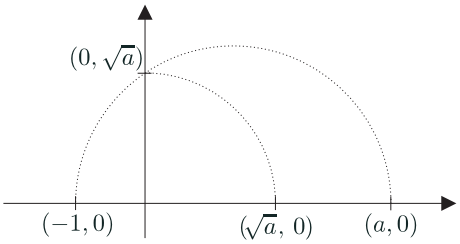
(iii) $(\sqrt{a}, 0)$ $(ha\ a \geqslant 0)$*.*

*Bizonyítás.* Az állítás (1) és (2) pontjában szereplő szerkesztések nyilvánvalóak. A szerkesztés a (3)(ii) esetben hasonlósággal, a (3)(iii) esetben pedig Thalesszkörrel egyszerűen elvégezhető (ld. 2. és 3. ábra). □




**13. ábra:** az $(ab, 0)$ és $(1/a, 0)$ pontok szerkesztése.

**12.6. Definíció.** *A $(H, P)$ szerkesztési feladat alaptestén a $H$-beli pontok koordinátái által generált valós számtestet értjük.*




**14. ábra:** a $(\sqrt{a}, 0)$ pont szerkesztése.

**12.7. Definíció.** *Legyen $K$ tetszőleges számtest. Az $L$ testet **egyszerű négyzetgyökbővítésnek** hívjuk, ha $L = K(\sqrt{c})$ valamely nemnegatív $c \in K$ számra. Az $L$ testet **négyzetgyökbővítésnek** nevezzük, ha van $K$ bővítéseinek egy olyan*

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = L$$

*sorozata, hogy minden $j$-re $(1 \leqslant j \leqslant t)$ a $K_j$ test egyszerű négyzetgyök bővítése $K_{j-1}$-nek, azaz $K_j = K_{j-1}(\sqrt{c_j})$ valamely $c_j \in K_{j-1}$-re $(c_j \geqslant 0)$.*

**12.8. Tétel.** *Legyen $(H, P)$ tetszőleges szerkesztési feladat, melynek alapteste $K$. Ekkor ekvivalensek az alábbi feltételek:*

(1) *$P$ megszerkeszthető $H$-ból;*

(2) *$K$-nak van olyan $L$ négyzetgyökbővítése, amely $P$ mindkét koordinátáját tartalmazza;*

(3) *$K$-nak van olyan $L'$, illetve $L''$ négyzetgyökbővítése, amely $P$ első, illetve második koordinátáját tartalmazza.*

A tétel igazolásához szükségünk lesz az alábbi egyszerű lemmára.

**12.9. Lemma.** *Legyen $f = ax^2 + bx + c \in \mathbb{R}[x]$ tetszőleges másodfokú polinom, melynek diszkriminánsa $D = b^2 - 4ac$. Ha az $f$ polinom gyökei $\alpha$ és $\beta$, akkor $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.*

*12.8. Tétel bizonyítása.* (1)$\Longrightarrow$(2): Mivel a szerkesztés véges sok közvetlen szerkesztés egymás utáni végrehajtása, ezért az alábbi tényt belátva már adódik a bizonyítandó állítás:
*Ha egy $P$ pont a $H$ ponthalmazból közvetlenül szerkeszthető, s a $H$-beli pontok koordinátái által generált számtest $K$, akkor a $H \cup \{P\}$ ponthalmazbeli pontok koordinátái által generált számtest vagy $K$, vagy egyszerű négyzetgyökbővítése $K$-nak.*
Tegyük fel, hogy $P$ közvetlenül szerkeszthető $H$-ból, azaz $P \in H \cup \mathcal{E}_1(H) \cup \mathcal{E}_2(H) \cup \mathcal{E}_3(H)$. Koordináta-geometriából jól ismert, hogy a $H$-egyenesek, illetve $H$-körök egyenletének alakja:

$$ax + by = c, \text{ illetve}$$
$$(x - v)^2 + (y - w)^2 = r^2,$$

ahol $a, b, c, v, w, r^2 \in K$. A $P$ pont koordinátái két fenti alakú egyenletrendszer megoldásaként adódnak. Ha mindkét egyenlet egyenes egyenlete, akkor $P$ koordinátái szintén $K$-ban lesznek, míg a többi esetben az egyenletrendszer megoldása $K$-beli együtthatós másodfokú egyenletre vezet; ha e másodfokú egyenlet diszkriminánsa $D$ ($D \in K$), akkor a 12.9. Lemma szerint $P$ mindkét koordinátája a $K(\sqrt{D})$ test eleme.

(2)$\Longrightarrow$(3): nyilvánvaló.

(3)$\Longrightarrow$(1): Tegyük fel, hogy $u$, illetve $v$ benne van a $K$ test egy $L'$, illetve $L''$ négyzetgyökbővítésében. Legyen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = L',$$

ahol $K_j = K_{j-1}(\sqrt{c_j})$ ($c_j \in K_{j-1},\ c_j \geqslant 0$) minden $j$-re ($1 \leqslant j \leqslant t$). Az állítást $j$ szerinti teljes indukcióval bizonyítjuk, azaz belátjuk, hogy tetszőleges $j$-re ($0 \leqslant j \leqslant t$) bármely $K_j$-beli valós szám megszerkeszthető $H$-ból. Amiből már következik, hogy $u \in L' = K_t$ is megszerkeszthető $H$-ból. Hasonló meggondolással kapjuk, hogy $v \in L''$ is megszerkeszthető $H$-ból, és így a $P = (u, v)$ pont is megszerkeszthető $H$-ból.
A 12.5. Állítás (3)(i) és (3)(ii) részéből következik, hogy $H$-ból a $K = K_0$ test megszerkeszthető. Tegyük fel, hogy valamely $j$-re ($1 \leqslant j \leqslant t$) a $K_{j-1}$ test elemei megszerkeszthetők $H$-ból. A 12.5. Állítás (3)(iii) részéből az is következik, hogy $\sqrt{c_j}$ megszerkeszthető $H$-ból, így a $K_{j-1} \cup \{\sqrt{c_j}\}$ által generált $K_j = K_{j-1}(\sqrt{c_j})$ test elemei is megszerkeszthetők $H$-ból.
Ezzel a tétel állítását bebizonyítottuk. □

Tetszőleges $u$ valós szám esetén a $(H, u)$ szerkesztési feladaton a $(H, (u, 0))$ szerkesztési feladatot értjük.

A 12.8. Tételben a (2) és (3) feltételek ekvivalenciája mutatja, hogy a szerkeszthetőségre kapott algebrai feltételnél is mindegy, hogy a megfelelő négyzetgyökbővítés létezését a $P$ pontra (azaz mindkét koordinátájára egyidejüleg) vagy a koordinátákra külön-külön követeljük meg. Ezért a 12.8. Tétel alábbi változata egyenértékű az eredetivel.

**12.10. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste $K$. Ekkor ekvivalensek az alábbi feltételek:*

(1) *$u$ megszerkeszthető $H$-ból;*

(2) *$K$-nak van olyan $L$ négyzetgyökbővítése, amely tartalmazza $u$-t.*

## 12.3 Nevezetes szerkesztési feladatok

A mai értelemben vett matematikával az ókori görögök kezdtek foglalkozni az i.e. VI. században (Thalész és Püthagorász). A matematikának azt a formáját, ahogy ma is ismerjük és műveljük, az i.e. V. században alakították ki. Ebben az időben fogalmazták meg a három klasszikus geometriai problémát, amelyek sok évszázadon át lázban tartották a matematikusokat. Mind a három probléma a geometriai szerkeszthetőségre vonatkozott (körző és (jelöletlen) egyenes vonalzó segítségével).

Az eddig felhalmozott ismereteink segítségével már egyszerűen megmutathatjuk, hogy az alábbi nevezetes geometriai problémák mindegyike megoldhatatlan euklideszi szerkesztéssel.

### 12.3.1 A kör négyszögesítése.

A kérdés az, hogy lehetséges-e az egységsugarú körrel azonos területű négyzetet szerkeszteni.[31] Az egységsugarú kör területe $\pi$, így a körrel azonos területű négyzet oldalának a hossza éppen $\sqrt{\pi}$. A kérdés tehát — a 12.26. Következményt felhasználva — az algebra nyelvén úgy fogalmazható meg, hogy a $\sqrt{\pi}$ szám foka 2-hatvány-e a a szerkesztés alapteste, azaz $K = \mathbb{Q}$ felett, ami ekvivalens azzal, hogy a $\pi$ szám foka 2-hatvány-e a a szerkesztés alapteste, azaz $K = \mathbb{Q}$ felett. Azonban a $\pi$ szám még csak nem is végesfokú, azaz transzcendens, $\mathbb{Q}$ felett, így a kör négyszögesítése euklideszi módon nem végezhető el. A $\pi$ szám transzcendenciája következik például az alábbi tételből.

**12.11. Definíció.** *Azt mondjuk, hogy az $u_1, \dots, u_r$ komplex számok **algebrailag függetlenek** a racionális számtest felett, ha tetszőleges $f \in \mathbb{Q}[x_1, \dots, x_r]$ polinomra $f(u_1, \dots, u_r) = 0$ pontosan akkor teljesül, ha $f = 0$.*

**12.12. Tétel (Lindemann–Weierstrass-tétel).** *Legyenek $u_1, \dots, u_r \in \mathbb{C}$ algebrai számok $\mathbb{Q}$ felett. Ha $u_1, \dots, u_r$ lineárisan függetlenek $\mathbb{Q}$ felett, akkor az $e^{u_1}, \dots, e^{u_r}$ komplex számok algebrailag függetlenek az algebrai számok teste felett, így $\mathbb{Q}$ felett is.*

Ha $r = 1$, akkor a Lindemann–Weierstrass-tétel alkalmazva azt kapjuk, hogy ha $u \neq 0$ algebrai szám, akkor $e^u$ transzcendens. Mivel $e^{i\pi} = -1$ algebrai szám, ezért $i\pi$ nem lehet algebrai szám, azaz $i\pi$ transzcendens. Mivel $i$ algebrai, ezért $\pi$ transzcendens.

[31] A kérdés az i.e. V. század második felében olyan népszerű volt, hogy Arisztophanész a Madarakban (i.e. 414) már gúnyolódik a körnégyszögesítőkön. A probléma mindig is a köztudatban maradt. Még Thomas Mann A varázshegyében című művében is van egy szereplő (Paravant államügyész), aki megszállottan keresi a megoldást.

### 12.3.2 Szögharmadolás.

Lehetséges-e egy adott szög egyharmadát megszerkeszteni? A válasz általában az, hogy nem. Megmutatjuk, hogy 60°-os szöget nem lehet harmadolni, azaz nem lehet 20°-os szöget szerkeszteni. A 20°-os szerkesztése azt jelenti, hogy a $P = (\cos 20°, \sin 20°)$ pont szerkeszthető a $O = (0,0)$, $E = (1,0)$, $P = (\cos 60°, \sin 60°) = (\frac{1}{2}, \frac{\sqrt{3}}{2})$ pontokból. Ekkor a $Q = (\cos 20°, 0)$ is szerkeszthető, mivel $Q$ nem más mint a $P$ pontból az $OE$ szakaszra állított merőleges talppontja. Mivel a szerkesztés alapteste $K = \mathbb{Q}(\sqrt{3})$ és $[K : \mathbb{Q}] = 2$, ezért elegendő azt megmutatni, hogy $\cos 20°$ foka 2-hatvány $\mathbb{Q}$ felett. Legyen $\alpha = \cos 20°$, ekkor — felhasználva a $\cos 3x = 4\cos^3 x - 3\cos x$ azonosságot — azt kapjuk, hogy $\alpha$ eleget tesz az $\frac{1}{2} = 4x^3 - 3x$ egyenletnek, azaz gyöke a $4x^3 - 3x - \frac{1}{2} \in \mathbb{Q}[x]$ polinomnak. Tekintsük a $2(4x^3 - 3x - \frac{1}{2}) = 8x^3 - 6x - 1 \in \mathbb{Z}[x]$ polinomot. A Rolle-tétel (3.7. Tétel) segítségével gyorsan kideríthető, hogy ez utóbbi polinomnak nincs racionális gyöke, így a 3.9. Állítás szerint irreducibilis $\mathbb{Q}$ felett, így a $4x^3 - 3x - \frac{1}{2}$ polinom is irreducibilis $\mathbb{Q}$ felett. Ez azt jelenti, hogy $m_{\cos 20°, \mathbb{Q}} = 4x^3 - 3x - \frac{1}{2}$, azaz $\cos 20°$ foka $\mathbb{Q}$ felett 3, ami nem 2-hatvány. Így a 60°-os szög nem harmadolható euklideszi módon.

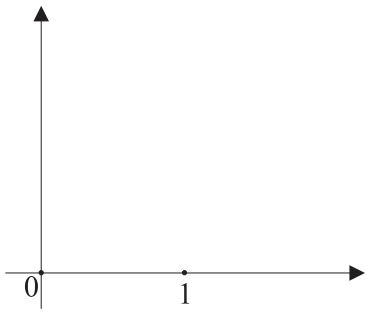
### 12.3.3 Déloszi probléma vagy kockakettőzés.

Olyan kockát kell szerkeszteni, amely kétszer akkora térfogatú mint egy adott kocka.[32] Legyen az adott kocka élhossza 1 méter, ekkor térfogata 1 $m^3$. Feladatunk egy 2 $m^3$-es kocka élének, azaz az $\alpha = \sqrt[3]{2}$ valós számnak a szerkesztése a $H = \{O, E\}$ halmazból. Mivel a $(H, \sqrt[3]{2})$ szerkesztési feladat alapteste $\mathbb{Q}$ és $\alpha$ minimálpolinomja $\mathbb{Q}$ felett a (3.4. Tétel szerint irreducibilis) $x^3 - 2$ polinom, ezért $\alpha$ foka 3 a racionális számtest felett, így nem szerkeszthető a 12.26. Következmény szerint.

## 12.4 Szerkesztés komplex alaptest felett

Ha a sík pontjait (a Gauss-féle számsíkon nekik megfeleltetett) komplex számokkal adjuk meg, akkor a valós alaptest feletti szerkesztéstől eltérő — bár azzal sok rokonságot mutató — lehetőség adódik a szerkeszthetőség problémájának algebrai tárgyalására. Ennél a megközelítésnél bármely $(H, u)$ szerkesztési feladat esetén a valós és a képzetes tengelyt úgy vesszük fel, hogy a $0, 1$ számoknak megfelelő pontok $H$-ban legyenek, és ezek után úgy tekintjük, hogy $H \subseteq \mathbb{C}$ és $u \in \mathbb{C}$ (ld. 15. ábra).

[32] Egy ókori legenda szerint a délosziak azt a jóslatot kapták, hogy csak akkor háríthatják el a pestisjárványt, ha Apollón templomában a kocka alakú oltár helyett kétszer akkorát állítanak.




**15. ábra:** a 0 és 1 pontok.

**12.13. Állítás.** (1) *0-ból és 1-ből (ahol $0, 1 \in H$) megszerkeszthető $i$.*
(2) *$a+bi$ akkor és csak akkor szerkeszethető meg $H$-ból, ha $a$ és $b$ megszerkeszthető.*
(3) *Valahányszor az $z, w \in \mathbb{C}$ megszerkeszthetők $H$-ból, mindannyiszor megszerkeszthetők a következő pontok is:*

(i) $z + w$, $-z$,

(ii) $zw$, $1/z$ (*ha* $z \neq 0$),

(iii) $\pm\sqrt{z}$.

A $(H, P)$ **szerkesztési feladat alaptestén** a $H$-beli komplex számok és konjugáltjaik által generált számtestet értjük.

**12.14. Tétel.** *A szerkesztési feladat alapteste független a Gauss-féle számsík választásától.*

Legyen $K \subseteq \mathbb{C}$ tetszőleges számtest. Az $L$ testet **egyszerű négyzetgyökbővítésnek** hívjuk, ha $L = K(\sqrt{c})$ valamely nemnegatív $c \in K$ számra. Az $L$ testet **négyzetgyökbővítésnek** nevezzük, ha van $K$ bővítéseinek egy olyan

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = L$$

sorozata, hogy minden $j$-re $(1 \leqslant j \leqslant t)$ a $K_j$ test egyszerű négyzetgyök bővítése $K_{j-1}$-nek, azaz $K_j = K_{j-1}(\sqrt{c_j})$ valamely $c_j \in K_{j-1}$-re $(c_j \geqslant 0)$.

**12.15. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste $K$. Ekkor ekvivalensek az alábbi feltételek:*

(a) *$u$ megszerkeszthető $H$-ból;*

(b) *$K$-nak van olyan $L$ négyzetgyökbővítése, amely tartalmazza $u$-t.*

## 12.5 Legfeljebb negyedfokú polinom gyökének szerkeszthetősége

**12.16. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste legyen $K$. Ha $u$ gyöke egy $K$ feletti másodfokú polinomnak, akkor $u$ megszerkeszthető.*

*Bizonyítás.* A másodfokú polinom gyökképlete alapján $u \in K(\sqrt{c})$ valamely $c \in K$-ra. Így $u$ szerkeszthető. □

**12.17. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste legyen $K$. Ha $u$ gyöke egy $K$ feletti harmadfokú polinomnak, akkor az alábbi három feltétel ekvivalens egymással:*

(a) *$u$ megszerkeszthető,*

(b) *$f$ minden olyan gyöke megszerkeszthető, amely a szerkesztés szempontjából szóba jöhet,*

(c) *$f$-nek van gyöke $K$-ban.*

**12.18. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste legyen $K$. Ha $u$ gyöke egy olyan $K$ feletti negyedfokú polinomnak, amelynek nincs gyöke $K$-ban, akkor az alábbi három feltétel ekvivalens egymással:*

(a) *$u$ megszerkeszthető,*

(b) *$f$ minden olyan gyöke megszerkeszthető, amely a szerkesztés szempontjából szóba jöhet,*

(c) *$f$ köbös rezolvensének van gyöke $K$-ban.*

## 12.6 Szabályos sokszögek szerkeszthetősége

Egy olyan tétellel kezdjük e részt, amely sok szerkesztési feladat esetén használható a nem-szerkeszthetőség igazolására.

**12.19. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste legyen $K$. Legyen $f \in K[x]$ olyan $K$ felett irreducibilis polinom, amelynek $u$ gyöke. Ha az $u$ pont megszerkeszthető, akkor $f$ fokszáma 2-hatvány.*

A szabályos sokszögek szerkeszthetősége is klasszikus szerkesztési feladat. A kérdés az, hogy milyen $n > 2$ egészek esetén szerkeszhető (adott körbe) szabályon $n$-szög. A választ az alábbi Gausstól és Wanzeltól származó tétel adja meg.

**12.20. Tétel.** *Szabályos $n$-szög $(n > 2)$ akkor és csak akkor szerkeszthető, ha $n$ prímtényezős felbontása*

$$n = 2^k p_1 \cdots p_r \quad (k, r \geqslant 0),$$

*ahol $p_1, \ldots, p_r$ páronként különböző prímek, és $p_1 - 1, \ldots, p_r - 1$ mindegyike 2-hatvány.*

Az általánosság megszorítása nélkül feltehető, hogy a kör, melybe a szabályos sokszöget szerkesztjük, egységnyi sugarú, s a 0 középpontjával és az 1 pontjával van megadva. Így a szerkesztés alapteste $\mathbb{Q}$. E körbe szabályos $n$-szög pontosan akkor szerkeszthető, ha az a szabályos $n$-szög megszerkeszthető, amelynek egyik csúcsa az 1 pont. Ezen szabályos $n$-szög megszerkeszthetősége pedig ekvivalens az

$$\varepsilon_n = \cos\frac{2\pi}{n} + i \sin\frac{2\pi}{n}$$

csúcs megszerkesztésével. Az $n$-szög $n$ csúcsa a következő:

$$\varepsilon_n^k = \cos\frac{2k\pi}{n} + i\sin\frac{2k\pi}{n} \quad (k = 0, 1, \ldots, n-1).$$

Egyszerű észrevétel, hogy tetszőleges $n$-re a szabályos $n$-szög szerkesztése visszavezethető prímhatvány oldalú szabályos sokszögek szerkesztésére.

**12.21. Tétel.** (1) *Bármely $m, n > 1$ egymáshoz relatív prím egészekre, $\varepsilon_{mn}$ akkor és csak akkor szerkeszthető meg, ha $\varepsilon_m$ és $\varepsilon_n$ is megszerkeszthető.*

(2) *Bármely $n = p_1^{k_1} \cdots p_t^{k_t}$ egész számra, ahol $p_1, \ldots, p_t$ páronként különböző prímek, $\varepsilon_n$ akkor és csak akkor szerkeszthető meg, ha $\varepsilon_{p_j^{k_j}}$ $(j = 1, \ldots, t)$ mindegyike megszerkeszthető.*

Tetszőleges $p$ prímre a

$$\Phi_p = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

polinomot **$p$-edik körosztási polinomnak**,

$$\Phi_{p^2} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1 \in \mathbb{Z}[x]$$

polinomot pedig **$p^2$-edik körosztási polinomnak** nevezzük.

**12.22. Tétel.** *Tetszőleges $p$ prímre*

(a) *$\varepsilon_p$ gyöke $\Phi_p$-nek, $\varepsilon_{p^2}$ pedig $\Phi_{p^2}$-nek;*

(b) *a $\Phi_p$ és $\Phi_{p^2}$ polinomok irreducibilisek $\mathbb{Q}$ felett.*

A tétel bizonyításához szükségünk lesz az alábbi számelméleti eredményekre.

**12.23. Lemma.** *Legyen $p$ páratlan prímszám. Ekkor igazak a következők.*

(a) *Ha $1 \leqslant k \leqslant p-1$, $1 \leqslant j < pk$ és $p \nmid j$, akkor $\binom{pk}{j} \equiv 0 \pmod{p}$.*

(b) *Ha $1 \leqslant j \leqslant k \leqslant p-1$, akkor $\binom{pk}{pj} \equiv \binom{k}{j} \pmod{p}$.*

*A 12.22. Tétel bizonyítása.* (a) Ha $p = 2$, akkor $\varepsilon_2 = -1$, $\varepsilon_4 = i$ és $\Phi_2 = x + 1$, $\Phi_4 = x^2 + 1$. Így ebben az esetben (a) nyilván teljesül.

Tegyük fel, hogy $p$ páratlan prímszám. Ekkor $\varepsilon_p, \varepsilon_{p^2}^p \neq 1$ miatt

$$\Phi_p(\varepsilon_p) = \varepsilon_p^{p-1} + \varepsilon_p^{p-2} + \cdots + \varepsilon_p + 1 = \frac{\varepsilon_p^p - 1}{\varepsilon_p - 1} = 0,$$

$$\Phi_{p^2}(\varepsilon_{p^2}) = \varepsilon_{p^2}^{p(p-1)} + \varepsilon_{p^2}^{p(p-2)} + \cdots + \varepsilon_{p^2}^p + 1 = \frac{\varepsilon_{p^2}^{p^2} - 1}{\varepsilon_{p^2}^p - 1} = 0.$$

(b) A $\Phi_p$ polinom irreducibilitása. Tekintsük a $(\Phi_p)_{\to -1}$ polinomot:

$$(\Phi_p)_{\to -1} = \sum_{k=0}^{p-1} (x+1)^k = x^{p-1} + \sum_{k=1}^{p-1} \binom{p}{k} x^{k-1}.$$

Mivel a 12.23. Lemma (a) állítása miatt $p \mid \binom{p}{k}$, ha $1 \leqslant k \leqslant p-1$, és $p^2 \nmid \binom{p}{1} = p$, ezért a Schönemann–Eisenstein-Tétel szerint $(\Phi_p)_{\to -1}$ irreducibilis $\mathbb{Q}$ felett, így a 3.5. Tétel következtében $\Phi_p$ is irreducibilis $\mathbb{Q}$ felett is.

A $\Phi_{p^2}$ polinom irreducibilitása. Tekintsük a $\left(\Phi_{p^2}\right)_{\to -1}$ polinomot:

$$\left(\Phi_{p^2}\right)_{\to -1} = \sum_{k=0}^{p-1}(x+1)^{pk} = \sum_{k=0}^{p-1}\sum_{j=0}^{pk}\binom{pk}{j}x^j = \sum_{j=0}^{p(p-1)}\left(\sum_{k=0}^{p-1}\binom{pk}{j}\right)x^j.$$

Legyen $a_j = \sum_{k=0}^{p-1}\binom{pk}{j}$ $(1 \leqslant j < p(p-1))$. Ha $p \nmid j$, akkor 12.23. Lemma (a) következtében $p \mid a_j$. Ha $p \mid j$, pl. $j = pu$ $(u \in \mathbb{N})$, akkor

$$a_j = a_{pu} = \sum_{k=u}^{p-1}\binom{pk}{pu} \equiv \sum_{k=u}^{p-1}\binom{k}{u} = \binom{p}{u+1}.$$

Így —szintén a 12.23. Lemma (a) állításának a következtében— azt kapjuk, hogy $p \mid a_j$, mivel $u+1 \leqslant p-1$. Ezért a Schönemann–Eisenstein-Tétel szerint $\left(\Phi_{p^2}\right)_{\to -1}$ irreducibilis $\mathbb{Q}$ felett, így a 3.5. Tétel következtében $\Phi_{p^2}$ is irreducibilis $\mathbb{Q}$ felett. □

A $2^{2^n}+1$ alakú prímszámokat **Fermat-prímeknek** nevezzük. Az első öt ilyen szám,

$$2^{2^0}+1 = 3,\ 2^{2^1}+1 = 5,\ 2^{2^2}+1 = 17,\ 2^{2^3}+1 = 257,\ 2^{2^4}+1 = 65537$$

mind prímszám, $2^{2^5}+1 = 641 \cdot 6700417$ azonban nem prím. A felsoroltakon kívül más Fermat-prím nem ismeretes, de az sem eldöntött kérdés, hogy a Fermat-prímek száma véges vagy végtelen.

A 12.19. és 12.22. Tételekből közvetlenül adódik az alábbi tétel.

**12.24. Tétel.** *Legyen $p$ tetszőleges páratlan prímszám.*

(1) *$\varepsilon_{p^2}$ nem szerkeszthető meg.*

(2) *Ha $p$ nem Fermat-prím, akkor $\varepsilon_p$ sem szerkeszthető meg.*

*Bizonyítás.* Legyen $n = p^b$ $(b \in \mathbb{N})$, és tegyük fel, hogy szabályos $n$-szög szerkeszthető. Legyen $x_n = \cos\dfrac{2\pi}{n}$, $y_n = \sin 2\pi n$. Ekkor az $(x_n, y_n)$ pont is szerkeszthető, így van olyan $r \in \mathbb{N}_0$, amelyre $[\mathbb{Q}(x_n, y_n) : \mathbb{Q}] = 2^r$ teljesül. A Fokszámtétel szerint pedig:

$$[\mathbb{Q}(x_n, y_n, i) : \mathbb{Q}] = [\mathbb{Q}(x_n, y_n, i) : \mathbb{Q}(x_n, y_n)] \cdot [\mathbb{Q}(x_n, y_n) : \mathbb{Q}] = 2^{r+1}.$$

Mivel $\varepsilon_n = x_n + iy_n \in \mathbb{Q}(x_n, y_n, i)$, ezért

$$[\mathbb{Q}(\varepsilon_n) : \mathbb{Q}] = 2^s \text{ alkalmas } s \in \mathbb{N}\text{-re.} \tag{15}$$

Tegyük fel, hogy $b \geqslant 2$. Ekkor szabályos $p^2$-szög is szerkeszthető. Mivel $m_{\varepsilon_{p^2},\mathbb{Q}} = \Phi_{p^2}$, ezért (15) miatt

$$2^s = [\mathbb{Q}(\varepsilon_{p^2}) : \mathbb{Q}] = m^*_{\varepsilon_{p^2},\mathbb{Q}} = \Phi^*_{p^2} = p(p-1).$$

Ez azonban nem lehetséges, így ellentmondásra jutottunk. Ezzel igazoltuk az (1) állítást.

Tegyük fel, hogy $b = 1$. Mivel $m_{\varepsilon_p,\mathbb{Q}} = \Phi_p$, ezért (15) miatt

$$2^s = [\mathbb{Q}(\varepsilon_p) : \mathbb{Q}] = m^*_{\varepsilon_p,\mathbb{Q}} = \Phi^*_p = p - 1,$$

azaz $p$ Fermat-prím. Ezzel igazoltuk a (2) állítást. □

**12.25. Tétel.** *Ha $p$ Fermat-prím, akkor $\varepsilon_p$ megszerkeszthető.*

*Bizonyítás.* Legyen $p = 2^s + 1$ Fermat-féle prímszám. Ekkor

$$[\mathbb{Q}(\varepsilon_p) : \mathbb{Q}] = \Phi^*_p = p - 1 = 2^s,$$

$\mathbb{Q}(\varepsilon_p)$ felbontási teste a $\Phi_p$ polinomnak $\mathbb{Q}$ felett. Legyen $G$ az $\Phi_p$ polinom Galois-csoportja, azaz

$$G = \mathrm{Gal}_{\mathbb{Q}}(\Phi_p) \cong \mathrm{Gal}(\mathbb{Q}(\varepsilon_p) : \mathbb{Q}).$$

Állítás. *$G$ ciklikus csoport.*

Legyen $\sigma$ tetszőleges eleme a $G$ csoportnak, továbbá legyen $\varepsilon = \varepsilon_p$. Ekkor $\Phi_p$ gyökei pontosan a primitív $p$-edik egységgyökök, azaz $\varepsilon, \varepsilon^2, \ldots, \varepsilon^{p-1}$. Így a $\sigma$ automorfizmust egyértelműen meghatározza $\varepsilon\sigma$, ha $\varepsilon\sigma = \varepsilon^{k_\sigma}$ teljesül valamely $k_\sigma$-ra ($k_\sigma \in \{1, 2, \ldots, p-1\}$), akkor tetszőleges $t \in \{1, 2, \ldots, p-1\}$-re $\varepsilon^t\sigma = \varepsilon^{tk_\sigma}$. Tekintsük az

$$\omega\colon G \to R_p,\ \sigma \mapsto \overline{k_\sigma}$$

leképezést. Legyen $\alpha$ és $\beta$ tetszőleges eleme $G$-nek. Mivel tetszőleges $t$-re ($t \in \{1, 2, \ldots, p-1\}$) teljesül, hogy

$$\varepsilon^t(\alpha\beta) = (\varepsilon^t\alpha)\beta = \varepsilon^{tk_\alpha}\beta = \varepsilon^{tk_\alpha k_\beta},$$

ezért $k_{\alpha\beta} = k_\alpha k_\beta$, azaz $\omega$ homomorfizmus. Az $\omega$ leképezés injektív is, mivel

$$\sigma\omega = \overline{1} \iff \varepsilon\sigma = \varepsilon \iff \sigma = \mathrm{id}.$$

Azaz $\omega$ injektív homomorfizmus, így $G$ izomorf $R_p$-vel. Mivel $R_p$ ciklikus, így $G$ is az. Ezzel az állítást igazoltuk.

Legyen $\sigma$ a $G$ csoport egy generátora, és tetszőleges $t$-re ($t \in \{0, 1, \ldots, s\}$) legyen $G_{s-t} = \left\langle \sigma^{2^{s-t}} \right\rangle$. Ekkor $|G_{s-t}| = 2^t$. Jelölje $L_j$ a $G_j$ részcsoport fixtestét ($j \in \{0, 1, \ldots, s\}$). Mivel

$$\{\mathrm{id}\} = G_s \leqslant G_{s-1} \leqslant \cdots \leqslant G_0 = G \quad \text{és} \quad |G_{j-1}/G_j| = 2\ (1 \leqslant j \leqslant s),$$

ezért a Galois-elmélet Főtétele szerint

$$\mathbb{Q}(\varepsilon) = L_s \geqslant L_{s-1} \geqslant \cdots \geqslant L_0 = \mathbb{Q} \quad \text{és} \quad [L_j : L_{j-1}] = 2\ (1 \leqslant j \leqslant s),$$

Állítás. *Ha $z \in \mathbb{Q}(\varepsilon_p)$ és $z = x + iy$, akkor $(x, y)$ szerkeszthető.*

Az állítást teljes indukcióval igazoljuk, megmutatjuk, hogy ha $z \in L_j$ ($j \in \{0, 1, \ldots, s\}$) és $z = x + iy$, akkor $(x, y)$ szerkeszthető. Az állítás $j = 0$-ra nyilván teljesül. Tegyük fel, hogy $(j-1)$-re igaz az állítás, és legyen $\alpha = \alpha_1 + i\alpha_2 \in L_j \setminus L_{j-1}$. Ekkor $m_{\alpha,L_{j-1}} = x^2 + 2bx + c \in L_{j-1}[x]$, valamint $\alpha = -b + \nu$, ahol $\nu^2 = \mu = b^2 - c \in L_{j-1}$. Legyen $b = b_1 + ib_2$,

$\nu = \nu_1 + i\nu_2$ és $\mu = \mu_1 + i\mu_2 = r(\cos\vartheta + i\sin\vartheta)$. Mivel $\mu \in L_{j-1}$, az indukciós hipotézis szerint $(\mu_1, \mu_2)$ szerkeszthető, így szerkeszthetők az $(r, 0)$, $(\sqrt{r}, 0)$ és $(\pm\sqrt{r}\cos(\vartheta/2), \pm\sqrt{r}\sin(\vartheta/2))$ pontok is. Felhasználva, hogy $b \in L_{j-1}$ miatt $(b_1, b_2)$ is szerkeszthető az indukciós hipotézis szerint, végül azt kapjuk, hogy $(\alpha_1, \alpha_2)$ is szerkeszthető. Ezzel az állítást bizonyítottuk.

Mivel $\varepsilon_p \in \mathbb{Q}(\varepsilon_p)$, ezért az $(x_p, y_p)$ szerkeszthető, azaz szabályos $p$-szög is szerkeszthető. □

## 12.7 A szerkeszthetőség szükséges és elegendő feltétele

A szerkeszthetőség egy szükséges feltétele.

**12.26. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste $K$. Ha $u$ megszerkeszthető $H$-ból, akkor $u$ algebrai $K$ felett, melynek foka 2-hatvány.*

*Bizonyítás.* Tegyük fel, hogy $u \in \mathbb{R}$ szerkeszthető $H$-ból. Ekkor $u$ benne van a $K$ test egy $L$ négyzetgyökbővítésében. Legyen

$$K = K_0 \subseteq K_1 \subseteq \cdots \subseteq K_{t-1} \subseteq K_t = L,$$

ahol $K_j = K_{j-1}(\sqrt{c_j})$ $(c_j \in K_{j-1},\ c_j \geqslant 0)$ minden $j$-re $(1 \leqslant j \leqslant t)$. Mivel tetszőleges $j$-re $(1 \leqslant j \leqslant t)$ a $K_j : K_{j-1} = K_{j-1}(\sqrt{c_j}) : K_{j-1}$ bővítés első- vagy másodfokú, ezért a Fokszámtétel (2.3. Tétel) szerint

$$[L : K] = [K_t : K_0] = \prod_{j=1}^{t} [K_j : K_{j-1}] = 2^s$$

valamely $s \in \mathbb{N}_0$-ra. Ekkor a 2.18. Tétel szerint az $L : K$ testbővítés algebrai, így $u$ algebrai $K$ felett és a 2.11. Állítás következtében $u$ foka is 2-hatvány $K$ felett. □

A szerkeszthetőség egy elegendő feltétele.

**12.27. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste $K$. Ha $u$ algebrai $K$ felett és $u$ ($K$ feletti) minimálpolinomjának a foka 2-hatvány, továbbá $K(u)$ ezen polinom minden (komplex) gyökét tartalmazza, akkor az $u$ pont megszerkeszthető $H$-ból.*

Az előbbi tétel feltétele távolról sem szükséges feltétele a szerkeszthetőségnek. Ha például $\mathbb{Q}$ az alaptest, akkor $u = \sqrt[4]{2}$ megszerkeszthető, de $\mathbb{Q}(u)$ nem tartalmazza az $m_{\sqrt[4]{2},\mathbb{Q}} = x^4 - 2$ minimálpolinomjának összes gyökét.

A 12.15. Tétel szerint elegendő az alábbi (tisztán algebrai) tételt igazolni.

**12.28. Tétel.** *Legyen $K$ tetszőleges számtest, $u \in \mathbb{C}$ pedig tetszőleges komplex szám. Ha $u$ algebrai $K$ felett és $u$ ($K$ feletti) minimálpolinomjának a fokszáma 2-hatvány, továbbá $K(u)$ ezen polinom minden (komplex) gyökét tartalmazza, akkor $K(u)$ négyzetgyökbővítése $K$-nak.*

Végül, a szerkeszthetőség szükséges és elegendő feltétele.

**12.29. Tétel.** *Legyen $(H, u)$ tetszőleges szerkesztési feladat, melynek alapteste $K$. Az $u$ pont akkor és csak akkor szerkeszthető meg, $u$ algebrai $K$ felett, és $u$ $K$ feletti minimálpolinomjának $K$ feletti felbontási teste $K$-nak 2-hatvány fokú bővítése.*

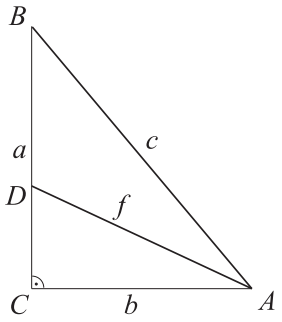
## 12.8 Hétköznapi szerkesztési feladatok

A szerkesztési problémák esetében többnyire van a megszerkesztendő alakzatnak olyan adata, amelynek segítségével az alakzat már könnyen megszerkeszthető. A célunk az lesz, hogy erre az adatra a megadott adatok segítségével alkalmas algebrai egyenletet állítsunk fel. A szerkeszthetőség kivitelezhetőségét pedig ezen polinom vizsgálatával döntjük el.

A fenti eljárást néhány példán mutatjuk be.

**12.30. Feladat.** *Megszerkeszthető-e az $ABC$ derékszögű háromszög, ha adott az $AB$ átfogójának és az $A$ csúcsból kiinduló szögfelezőjének a hossza?*

Az átfogó és az $A$ csúcsból kiinduló szögfelező hosszát jelölje rendre $c$ és $f$, a szögfelező talppontja legyen $D$ (ld. 16. ábra). A továbbiakban az $AC$ befogó $b$ hosszára fogunk egy algebrai egyenletet felírni, mivel $b$ ismeretében a háromszög már egyszerűen megszerkeszthető.




**16. ábra.**

A Szögfelező-tétel szerint $\overline{BD} : \overline{DC} = c : b$. Mivel $\overline{DC} = a - \overline{BD}$, ezért

$$\overline{DC} = \frac{b}{b+c}a.$$

Alkalmazzuk Pithagorasz tételét az $ABC$ és $ADC$ háromszögekre:

$$a^2 + b^2 = c^2,$$

$$\overline{DC}^2 + b^2 = f^2 \Longleftrightarrow \left(\frac{b}{b+c}a\right)^2 + b^2 = f^2.$$

A fenti egyenlőségek felhasználásával azt kapjuk, hogy $b$ gyöke a

$$p = (2c)x^2 - f^2x - f^2c$$

polinomnak. Válasszuk a $c$ hosszúságot egységnyinek. Ekkor a szerkesztés $K$ alapteste az $f$ által generált számtest, a szerkesztendő $b$ pont pedig a $p \in K[x]$ másodfokú polinom gyöke. A 12.16. Tétel szerint $b$ — és így az $ABC$ háromszög is — szerkeszthető.

A $p$ polinom gyökei:

$$\frac{f^2 \pm \sqrt{f^4 + 8f^2c^2}}{4c}.$$

Mivel a gyökök közül nyilván csak a poztív jöhet szóba, ezért

$$b = \frac{f^2 + \sqrt{f^4 + 8f^2c^2}}{4c}.$$

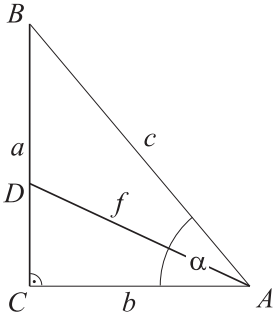
A szerkesztendő háromszög csak akkor létezhet, ha $0 < f < c$. Ezen feltétel teljesülése esetén azonban

$$b < \frac{c^2 + \sqrt{c^4 + 8c^2c^2}}{4c} = c,$$

azaz létezik a $c$ átfogójú, $b$ befogójú derékszögű háromszög.

**12.31. Feladat.** *Megszerkeszthető-e az $ABC$ derékszögű háromszög, ha adott az $BC$ befogójának és az $A$ csúcsból kiinduló szögfelezőjének a hossza?*

Az előző feladat jelöléseit fogjuk használni, továbbá az $A$ csúcsnál lévő szöget jelölje $\alpha$ (ld. 17. ábra).




**17. ábra.**

Ismét $b$-t szeretnénk megszerkeszteni, mivel $b$ ismeretében már az $ABC$ háromszög is megszerkeszthető. Keressünk olyan polinomot, amelynek együtthatói a szerkesztés alaptestében vannak.

Felhasználva, hogy az $\alpha$ szöghöz tartozó szögfelező hossza

$$f = \frac{2bc}{b+c}\cos\frac{\alpha}{2},$$

valamint $c^2 = a^2 - b^2$ (Pithagorasz-tétel) és $\cos\frac{\alpha}{2} = \frac{b}{f}$, azt kapjuk, hogy

$$\begin{aligned} f = \frac{2}{\frac{1}{b}+\frac{1}{c}}\frac{b}{f} &\iff \frac{2b}{f^2} - \frac{1}{b} = \frac{1}{c} \\ &\iff c(2b^2 - f^2) = f^2 b \\ &\iff c^2(2b^2 - f^2)^2 = f^4 b^2 \\ &\iff (a^2+b^2)(2b^2 - f^2)^2 = f^4 b^2, \end{aligned}$$

azaz $b$ gyöke a $p = 4x^6 + 4(a^2 - f^2)x^4 - 4a^2f^2x^2 + a^2f^4$ polinomnak. Mivel $b$ pontosan akkor szerkeszthető, ha $b^2$ szerkeszthető, ezért jelen esetben érdemesebb $b^2$-et választani szerkesztendő adatnak, mivel $b^2$ a harmadfokú

$$4x^3 + 4(a^2 - f^2)x^2 - 4a^2f^2x + a^2f^4 \tag{16}$$

polinomnak gyöke.

Megmutatjuk, hogy az $a$ és $f$ hosszúságok alkalmas választása esetén az $ABC$ háromszög létezik, de nem szerkeszthető meg.

Legyen $a = f = 1$, ekkor a szerkesztés alapteste $\mathbb{Q}$, és (16) szerint $b^2$ gyöke a $4x^3 - 4x + 1 \in \mathbb{Q}[x]$ polinomnak. Rolle tételét (3.7. Tétel) alkalmazva azt kapjuk, hogy e polinomnak nincs racionális gyöke. Így a 12.17. Tétel szerint $b^2$ nem szerkeszthető, de a háromszög létezik ($b \approx 0,915$).

# Irodalomjegyzék


[1] **Bálintné Szendrei Mária, Czédli Gábor, Szendrei Ágnes**, *Absztrakt algebrai feladatok*, POLYGON (Szeged, 2005).

[2] **Csákány Béla**, *Algebra*, Nemzeti Tankönyvkiadó (1995).

[3] **Czédli Gábor, Szendrei Ágnes**, *Geometriai szerkeszthetőség*, POLYGON (Szeged, 1997).

[4] **Kiss Emil**, *Bevezetés az algebrába*, TYPOTEX (Budapest, 2007).

# Maple, pontosabban Maple 8

Ezen fejezetben azt szeretnénk bemutatni (a teljesség igénye nélkül), hogy milyen módon használhatjuk fel a számítógépes algebrai rendszerek nyújtotta lehetőségeket. A példákban a Maple programcsomag utasításai szerepelnek, ezért azokban —többnyire— a Maple szintaxisát használjuk.

## 13.1 Polinomok irreducibilitása

A feladatok megoldása során gyakran kerülünk szembe olyan probléma melynek során valamely $\mathbb{Z}$ vagy $K$ feletti ($K$ test) polinomról kell eldöntenünk, hogy irreducibilis-e. A Maple-ben két irányból is közelíthetünk a probléma felé, az **irreduc**, illetve a **factor** utasítások alkalmazásával.

`irreduc(f)` *az $f \in \mathbb{Q}[x]$ polinom irreducibilitásának ellenőrzése, visszatérési érték:* `true`*, ha az $f$ polinom irreducibilis, illetve* `false`*, ha nem irreducibilis.*

**1. Példa.**

```
> irreduc(x^4 + 1);
```

$$true$$

```
> irreduc(x^7 - 4*x^6 + 6*x^5 - 5*x^4 - 3*x^3 + 4*x^2 - x - 1);
```

$$false$$

A második esetben azonkívül, hogy az $f$ polinom nem irreducibilis sajnos más információt nem kaptunk. Ezen a hiányosságon fog segíteni a `factor` utasítás.

`factor(f)` *az $f \in \mathbb{Q}[x]$ polinom felbontása irreducibilis tényezők szorzatára, visszatérési érték: az $f$ polinom irreducibilis felbontása.*

**2. Példa.**

```
> factor(x^8 + 1);
```

$$x^8 + 1$$

```
> factor(x^8 - 7*x^7 + 15*x^6 - 5*x^5 - 14*x^4 + 7*x^3 + 3*x^2 - 3*x - 1);
```

$$(x^4 - 3x^3 + x^2 + x - 1)(x^2 - 2x - 1)^2$$

Így az $x^8+1$ polinom irreducibilis $\mathbb{Q}$ felett, mivel az utasítás visszatérései értéke önmaga, az $x^8 - 7x^7 + 15x^6 - 5x^5 - 14x^4 + 7x^3 + 3x^2 - 3x - 1$ polinom azonban nem irreducibilis.

Mindkét utasítás esetében igaz, hogy nem csak $\mathbb{Q}$ felett, hanem $\mathbb{Q}$ véges fokú algebrai bővítéseiben is működnek. Példaként tekintsük a $\mathbb{Q}$ felett irreducibilis $f = x^8 + 1$ polinomot. Vajon irreducibilis-e a $\mathbb{Q}(\sqrt{2})$ test felett az $f$ polinom? A $\sqrt{2}$ valós algebrai számot a minimálpolinomjával `RootOf(x^2 - 2)` alakban adhatjuk meg.

**3. Példa.**

```
> f := x^8 + 1;
> irreduc(f, RootOf(x^2 - 2));
```

$$false$$

Azaz $\mathbb{Q}(\sqrt{2})[x]$-ben az $f$ polinom már nem irreducibilis. Állítsuk elő az irreducibilis felbontsát is!

**4. Példa.**

```
> restar;
> f := x^8 + 1;
> factor(f, {RootOf(x^2 - 2)});
```

$$(x^4 + x^2\text{RootOf}(\_Z^2 - 2) + 1)(x^4 - x^2\text{RootOf}(\_Z^2 - 2) + 1)$$

Egy kicsit szebbé tehetjük, ha a „RootOf"-os kifejezést helyettesítjük.

```
> alias(alpha = RootOf(x^2 - 1)) :
> factor(f, {alpha};
```

$$(x^4 + x^2\alpha + 1)(x^4 - x^2\alpha + 1)$$

Most próbálkozzunk a $\mathbb{Q}(\sqrt{2}, i)$ testtel. A célunk az, hogy első fokú polinom szorzatára bontsuk $f$-et.

**5. Példa.**

```
> restar;
> f := x^8 + 1;
> alias(alpha = RootOf(x^2 - 1),  beta = RootOf(x^2 + 1)) :
> factor(f, {alpha, beta};
```

$$\frac{(2x^2 + \alpha - \beta\alpha)(2x^2 + \alpha + \beta\alpha)(2x^2 - \alpha + \beta\alpha)(2x^2 - \alpha - \beta\alpha)}{16}$$

Ez már majdnem jó — legalábbis a polinom gyökeit már könnyen megkaphatjuk —, de még nem tökéletes.

```
> alias(epsilon = RootOf(x^8 + 1)) :
> factor(f, {epsilon};
```

$$(x + \varepsilon^5)(-x + \varepsilon^5)(-x + \varepsilon^3)(-x + \varepsilon^7)(x + \varepsilon^3)(x + \varepsilon^7)(x + \varepsilon)(-x + \varepsilon)$$

Ez már tökéletes. Így az $f$ polinom felbontási teste $\mathbb{Q}(\varepsilon)$

Azt fontos megjegyezni, hogy a `RootOf` utasítás argumentuma irreducibilis kell legyen.

## 13.2 Minimálpolinomok meghatározása

Ez már egy kicsit bonyolultabb feladat. A Maple egy érdekes eljárást kínál e probléma „közelítő" megoldására.

`MinimalPolynomial(r,n)` *az eljárás egy legfeljebb $n$-edfokú egész együtthatós polinomot ad visszatérési értékül, amelynek az $r$ algebrai szám közelítése gyöke.*

Azaz nem feltétlenül az $r$ algebrai szám minimálpolinomját kapjuk meg!!! Első példánkban a $\sqrt{2}$ (2-fokú) algebrai szám minimálpolinomját határozzuk meg.

**6. Példa.**

```
> restart :
> with(PolinomialTools) :
> r := sqrt(2);
> mp[1] := MinimalPolynomial(r, 1) :
```

$$mp_1 := -8119 + 5741 * \_X$$

```
> mp[2] := MinimalPolynomial(r, 2) :
```

$$mp_2 := -2 + \_X^2$$

Az $mp[1]$ polinomnak biztosan nem gyöke a $\sqrt{2}$, de a polinom egyetlen gyöke jól közelíti $\sqrt{2}$-t. A második esetben már egy $\mathbb{Q}$ feletti irreducibilis polinomot kaptunk, amelynek $\sqrt{2}$ gyöke, így $mp_2$ a minimálpolinom, azaz $mp_2 = m_{\sqrt{2},\mathbb{Q}}$.

Most már bátran nekivághatunk valami bonyolultabbnak is, például az $r = \sqrt{2} + \sqrt{3} + \sqrt{5}$ algebrai szám minimálpolinomja meghatározásának. Vigyázat, „a nemzetközi helyzet egyre fokozódik": ezen a ponton egy a számítógépével kevésbé baráti viszonyt ápoló „Homo sapiens sapiens" esetleg már megriadhat.

**7. Példa.**

```
> restart :
> with(PolinomialTools) :
> r := sqrt(2) + sqrt(3) + sqrt(5);
```

$$r := \sqrt{2} + \sqrt{3} + \sqrt{5};$$

Egyszerre több polinomot is ki fogunk iratni egy ún. for-ciklussal:

```
> for n from 1 to 8 do mp[n] := MinimalPolynomial(r, n) od;
```

$$mp_1 := -15415 + 2864\_X$$
$$mp_2 := 117 - 673\_X + 121\_X^2$$
$$mp_3 := 237 + 50\_X - 39\_X^2 + 4\_X^3$$
$$mp_4 := -26 + 46\_X - \_X^2 - 12\_X^3 + 2\_X^4$$
$$mp_5 := -26 + 46\_X - \_X^2 - 12\_X^3 + 2\_X^4$$
$$mp_6 := -7 + 18\_X - 21\_X^2 + 10\_X^3 + 10\_X^4 - 29\_X^5 + 5\_X^6$$
$$mp_7 := 23 - 6\_X + 4\_X^2 - 17\_X^3 + 7\_X^4 - 21\_X^5 - 7\_X^6 + 2\_X^7$$
$$mp_8 := 23 - 6\_X + 4\_X^2 - 17\_X^3 + 7\_X^4 - 21\_X^5 - 7\_X^6 + 2\_X^7$$

Sajnos, ezen polinom egyikének sem gyöke $r$. Növeljük a számítások pontosságát. Mostantól számoljunk 30 értékes jegyre pontosan (ezt a `Digits` paraméter értékének beállításával fogjuk elérni).

```
> Digits := 30 :
> for n from 1 to 8 do mp[n] := MinimalPolynomial(r, n) od;
```

$$mp_1 := -32078891133454 + 5960035364353\_X$$
$$mp_2 := -1643893970 - 1838934657\_X + 398406975\_X^2$$
$$mp_3 := 2087394 - 28718181\_X - 1983070\_X^2 + 1346378\_X^3$$
$$mp_4 := 48001 + 934452\_X + 204309\_X^2 - 172777\_X^3 + 18998\_X^4$$
$$mp_5 := 23336 + 78529\_X - 73162\_X^2 + 29751\_X^3 - 70156\_X^4 + 12378\_X^5$$
$$mp_6 := 8009 + 10231\_X - 27737\_X^2 - 8069\_X^3 + 19675\_X^4 - 8337\_X^5 + \cdots$$
$$mp_7 := -1033 + 7130\_X + 6309\_X^2 + 989\_X^3 + 1463\_X^4 - 3046\_X^5 + \ldots$$
$$mp_8 := 576 - 960\_X^2 + 352\_X^4 - 40\_X^6 + \_X^8$$

Az $mp_8$ polinomnak gyöke $r$. Mivel ezen polinom irreducibilis is, ezért megvan a minimálpolinomunk: $m_{\sqrt{2}+\sqrt{3}+\sqrt{5},\mathbb{Q}} = 576 - 960x^2 + 352x^4 - 40x^6 + x^8$.

A következő példa azt mutatja, hogy hasznos, ha tudunk valamilyen infromációt az algebrai szám fokszámáról. Határozzuk meg az $r = 1 + \sqrt[3]{2} + \sqrt[4]{5}$ algebrai

szám minimálpolinomját $\mathbb{Q}$ felett. Azt már tudjuk, hogy $r$ foka legfeljebb 12. Így csak a számítás pontosságát fogjuk változtatni.

**8. Példa.**

```
> restart :
> with(PolinomialTools) :
> r := 1 + root[3](2) + root[4](5);
```

$$r := 1 + 2^{(1/3)} + 5^{(1/4)};$$

```
> Digits := 20 : mp[20] := MinimalPolynomial(r, 12);
```

$$mp_{20} := 33 - 5\_X - 15\_X^2 - 111\_X^3 + 24\_X^4 + 11\_X^5 + \cdots$$

```
> Digits := 30 : mp[30] := MinimalPolynomial(r, 12);
```

$$mp_{30} := 309 - 332\_X + 5\_X^2 + 133\_X^3 - 313\_X^4 + 230\_X^5 + \cdots$$

```
> Digits := 40 : mp[40] := MinimalPolynomial(r, 12);
```

$$mp_{40} := 1382 + 52\_X + 128\_X^2 + 3225\_X^3 - 505\_X^4 + 2067\_X^5 + \cdots$$

```
> Digits := 50 : mp[50] := MinimalPolynomial(r, 12);
```

$$mp_{50} := 496 - 2304\_X + 5040\_X^2 - 5664\_X^3 + 3288\_X^4 - 1584\_X^5 + \cdots$$

```
> irreduc(mp[50]);
```

$$true$$

Az $mp_{20}, mp_{30}, mp_{40}$ polinomoknak nem gyöke $r$, de az $mp_{50}$ ireducibilis polinomnak már igen. Így

$$\begin{aligned} m_{1+\sqrt[3]{2}+\sqrt[4]{5},\mathbb{Q}} = 496 &- 2304\_X + 5040\_X^2 - 5664\_X^3 + 3288\_X^4 \\ &- 1584\_X^5 + 1200\_X^6 - 960\_X^7 + 552\_X^8 \\ &- 228\_X^9 + 66\_X^{10} - 12\_X^{11} + \_X^{12} \end{aligned}$$

## 13.3 Galois-csoport meghatározása

Ez egy nagyon egyszerű feladat a Maple-nek, de ...

`galois(f)` *az $f$ irreduciblis polinom Galois-csoportját határozza meg, sajnos csak $f^* \leqslant 9$ esetén. Az eljárás visszatérési értéke az alábbi elemekből áll:*

1. *A Galois-csoportot leíró név G. Butler és J. McKay "The Transitive Groups of Degree up to Eleven" című cikke alapján, amely (Communications in Algebra, 11(8) 1983). Például "8T24" jelöli a 24-dik csoportot a listában, amely egy 8-adfokú tranzitív permutációcsoport.*

2. *Egy másik név J. H. Conway, A. Hulpke és J. McKay "On Transitive Permutation Groups" című cikke alapján (London Mathematical Society Journal of Computation and Mathematics).*

3. *Egy karakter, amely a permutációcsoport paritását jelöli ("+" a páros csoportokra, azaz az alternáló csoport részcsoportjaira, és "−" a többire).*

4. *A Galois-csoport rendje.*

5. *A Galois-csoporttal izomorf permutációcsoport generátorai.*

*A jelölések megértéséhez nyújthat még segítséget a Maple „Help"-jében a Mathematics/Discrete Mathematics/Combinatorics/Permutations/transgrp helyen található leírás.*

**9. Példa.**

```
> restart :
> galois(x^4 + x^3 + x^2 + x + 1);
```

$$"4T1", \{"C(4)"\}, " - ", 4, \{"(1\,2\,3\,4)"\}$$

Az $x^4 + x^3 + x^2 + x + 1 \in \mathbb{Q}[x]$ polinom Galois-csoportja izomorf $C(4)$-gyel.[33]

```
> galois(x^4 + x^3 + 5 * x^2 + 8 * x + 4);
```

$$"4T2", \{"E(4)", "2[\times]2"\}, " + ", 4, \{"(1\,4)(2\,3)", "(1\,2)(3\,4)"\}$$

Az $x^4 + x^3 + 5x^2 + 8x + 4 \in \mathbb{Q}[x]$ polinom Galois-csoportja izomorf $E(4)$-gyel.[34]

```
> galois(x^4 + x^3 + x^2 + 2 * x + 4);
```

$$"4T3", \{"D(4)"\}, " - ", 8, \{"(1\,2\,3\,4)", "(1\,3)"\}$$

Az $x^4 + x^3 + x^2 + 2x + 4 \in \mathbb{Q}[x]$ polinom Galois-csoportja izomorf $D(4)$-gyel.[35]

```
> galois(x^4 + x^3 + 4 * x^2 + 7 * x + 8);
```

$$"4T4", \{"A(4)"\}, " + ", 12, \{"(2\,3\,4)", "(1\,2\,4)"\}$$

Az $x^4 + x^3 + 4x^2 + 7x + 8 \in \mathbb{Q}[x]$ polinom Galois-csoportja izomorf $A(4)$-gyel.[36]

```
> galois(x^4 + x^3 + x^2 + x + 2);
```

$$"4T5", \{"S(4)"\}, " - ", 24, \{"(1\,4)", "(3\,4)", "(2\,4)"\}$$

Az $x^4 + x^3 + x^2 + x + 2 \in \mathbb{Q}[x]$ polinom Galois-csoportja izomorf $S(4)$-gyel.[37]

[33] Azaz a négyelemű ciklikus csoporttal ($\mathbb{Z}_4$).
[34] Azaz a Klein-csoporttal ($V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$).
[35] Azaz a 4-edfokú diédercsoporttal ($D_4$).
[36] Azaz a 4-edfokú alternáló csoporttal ($A_4$).
[37] Azaz a 4-edfokú szimmetrikus csoporttal ($S_4$).

# Kis fokszámú polinomok Galois-csoportjai

Legyen $\mathcal{P}_{n,k}$ ($n \in \mathbb{N}$) az alábbi polinom halmaz:

$$\mathcal{P}_{n,k} = \left\{ x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + a_0 \in \mathbb{Z}[x] \mid \max\{a_{n-1}, \ldots, a_1, a_0\} \leqslant k \right\}.$$

Ebben a fejezetben a $\mathcal{P}_{n,4}$-beli irreducibilis polinomok Galois-csoportját vizsgáljuk meg $n \in \{2,3,4,5,6\}$-ra. A továbbiakban $s_k$ jelöli az

$$\{f \in \mathcal{P}_{4,k} \mid \mathrm{Gal}_{\mathbb{Q}}(f) \cong G\}$$

halmaz elemszámát.

## 13.1 Harmadfokú irreducibilis főpolinomok

A $\mathcal{P}_{3,7}$ polinom halmaz elemszáma $15^3 = 3375$. Ebből az irreducibilis polinomok száma 2718. A Galois-csoportjuk szerinti megoszlásuk pedig a következő:

| $G$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ | $s_5$ | $s_6$ | $s_7$ |
|---|---|---|---|---|---|---|---|
| $A_3$ | 0 | 4 | 10 | 18 | 25 | 36 | 48 |
| $S_3$ | 12 | 68 | 216 | 496 | 976 | 1668 | 2670 |

## 13.2 Negyedfokú irreducibilis főpolinomok

A $\mathcal{P}_{4,4}$ polinom halmaz elemszáma $9^4 = 6561$. Ebből az irreducibilis polinomok száma 4712. A Galois-csoportjuk szerinti megoszlásuk pedig a következő:

| $G$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ |
|---|---|---|---|---|
| $\mathbb{Z}_4$ | 2 | 2 | 4 | 20 |
| $V_4$ | 2 | 6 | 9 | 32 |
| $D_4$ | 10 | 70 | 188 | 444 |
| $A_4$ | 0 | 2 | 8 | 12 |
| $S_4$ | 20 | 274 | 1382 | 4204 |

Néhány $\mathcal{P}_{4,3}$-beli polinom, melynek Galois-csoportja izomorf $\mathbb{Z}_4$-gyel:

$$x^4 + x^3 + x^2 + x + 1, \qquad x^4 + 3x^3 - x^2 - 3x + 1.$$

Néhány $\mathcal{P}_{4,3}$-beli polinom, melynek Galois-csoportja izomorf $V_4$-gyel:

$$x^4 - x^2 + 1, \qquad x^4 + 1,$$
$$x^4 + 3x^2 + 1, \qquad x^4 + x^3 + 2x^2 - x + 1,$$
$$x^4 + 2x^3 + 2x^2 - 2x + 1, \qquad x^4 + 3x^3 + 2x^2 - 3x + 1.$$

Néhány $\mathcal{P}_{4,1}$-beli polinom, melynek Galois-csoportja izomorf $D_4$-gyel:

$$x^4 - x^2 - 1, \qquad x^4 + x^2 - 1,$$
$$x^4 + x^3 - x^2 - x + 1, \qquad x^4 + x^3 - x^2 + x + 1,$$
$$x^4 + x^3 - x + 1, \qquad x^4 + x^3 + x^2 - x + 1.$$

Néhány $\mathcal{P}_{4,3}$-beli polinom, melynek Galois-csoportja izomorf $A_4$-gyel:

$$x^4 + 2x^3 + 2x^2 + 2, \qquad x^4 + 2x^3 + 2x^2 + 2x + 3,$$
$$x^4 + 2x^3 + 3x^2 - 3x + 1, \qquad x^4 + 3x^3 + 3x^2 - 2x + 1.$$

Néhány $\mathcal{P}_{4,1}$-beli polinom, melynek Galois-csoportja izomorf $S_4$-gyel:

$$x^4 + x - 1, \qquad x^4 + x + 1,$$
$$x^4 + x^2 + x + 1, \qquad x^4 + x^3 - x^2 - x - 1,$$
$$x^4 + x^3 - x^2 + x - 1, \qquad x^4 + x^3 - 1,$$
$$x^4 + x^3 + 1, \qquad x^4 + x^3 + x^2 - x - 1,$$
$$x^4 + x^3 + x^2 + 1, \qquad x^4 + x^3 + x^2 + x - 1.$$

## 13.3 Ötödfokú irreducibilis főpolinomok

A $\mathcal{P}_{5,4}$ polinom halmaz elemszáma $9^5 = 59049$. Ebből az irreducibilis polinomok száma 43684. A Galois-csoportjuk szerinti megoszlásuk pedig a következő:

| $G$ | $s_1$ | $s_2$ | $s_3$ | $s_4$ |
|---|---|---|---|---|
| $\mathbb{Z}_5$ | 0 | 0 | 0 | 4 |
| $D_5$ | 0 | 10 | 78 | 116 |
| $F_5$ | 0 | 4 | 14 | 44 |
| $A_5$ | 0 | 8 | 32 | 56 |
| $S_5$ | 104 | 1790 | 11324 | 43464 |

$\mathbb{Z}_5$: $x^5 \pm 3x^4 - 3x^3 \pm 4x^2 + x \pm 1$, $x^5 \pm x^4 - 4x^3 \pm 3x^2 + 3x \pm 1$

$D_5$: $x^5 \pm 2x^4 + x^3 \pm x^2 - x \pm 1$, $x^5 \pm x^4 + x^3 \pm x^2 - 2x \pm 1$,
$x^5 \pm 2x^4 + 2x^3 \pm x^2 \pm 1$, $x^5 \pm x^4 + 2x^3 \pm x^2 + 2x \pm 2$

$F_5$: $x^5 \pm 2x^4 - 2x^3 - x \pm 2$, $x^5 \pm 2$

$A_5$: $x^5 \pm x^4 - 2x^3 + x \pm 1$, $x^5 \pm x^4 + x^3 \mp 2x^2 + x \pm 1$
$x^5 + 2x^3 \pm 2x^2 - x \mp 2$, $x^5 \pm x^4 \mp 2x^2 - 2x \mp 2$

$S_5$: $x^5 - x^3 \pm 1$, $x^5 - x^2 \pm 1$
$x^5 - x^4 - x^3 - x^2 \pm x - 1$, $x^5 \pm x^4 \mp 2x^2 - 2x \mp 2$

## 13.4 Hatodfokú irreducibilis főpolinomok

A $\mathcal{P}_{6,3}$ polinom halmaz elemszáma $7^6 = 117649$. Ebből az irreducibilis polinomok száma 81940. A Galois-csoportjuk szerinti megoszlásuk pedig a következő:

| $G$ | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|
| $6T1$ | 4 | 4 | 4 |
| $6T2$ | 0 | 0 | 10 |
| $6T3$ | 2 | 46 | 108 |
| $6T4$ | 0 | 2 | 6 |
| $6T5$ | 0 | 12 | 28 |
| $6T6$ | 0 | 8 | 48 |
| $6T7$ | 20 | 54 | 136 |
| $6T8$ | 0 | 5 | 19 |

| $G$ | $s_1$ | $s_2$ | $s_3$ |
|---|---|---|---|
| $6T9$ | 0 | 8 | 36 |
| $6T10$ | 0 | 0 | 0 |
| $6T11$ | 18 | 167 | 819 |
| $6T12$ | 0 | 4 | 22 |
| $6T13$ | 8 | 278 | 1056 |
| $6T14$ | 0 | 0 | 6 |
| $6T15$ | 0 | 4 | 46 |
| $6T16$ | 240 | 8672 | 79596 |

$6T1$: $x^6+x^5+x^4+x^3+x^2+x+1$
$6T2$: $x^6+3x^5+x^4-3x^3+x^2+3x+1$,
$x^6+3x^5+2x^4-x^3+2x^2+3x+1$,
$x^6+3x^5+3x^4+x^3+3x^2+3x+1$
$6T3$: $x^6+x^3-1$
$6T4$: $x^6+x^4-2x^2-1$
$6T5$: $x^6+x^4-2x^3+x^2+2x+1$
$6T6$: $x^6-x^4-2x^2+1$
$6T7$: $x^6+x^2-1$
$6T8$: $x^6-x^4+2x^2+2$
$6T9$: $x^6+x^3+2$
$6T10$: $x^6-6x^5+8x^4+x^3+3x^2+x+1$,
$x^6+5x^5+6x^4+2x^3+4x^2+x+1$
$6T11$: $x^6+x^2+1$
$6T12$: $x^6+x^5-x^4+x^3-2x^2-2$
$6T13$: $x^6+x^2+2x+1$
$6T14$: $x^6+2x^5+3x^4+x^3+2x^2-3x-1$,
$x^6+3x^5-2x^4-x^3-3x^2-2x-1$
$6T15$: $x^6-2x^4+x^2-2x-1$
$6T16$: $x^6+x+1$

A $6Tk$ $(k=1,2,\ldots,16)$ csoportok a következők:

| $6Tk$ | $\mathbb{G}$ | $\lvert\mathbb{G}\rvert$ | generátorok |
|---|---|---|---|
| $6T1$ | $C_6$ | 6 | (1 2 3 4 5 6) |
| $6T2$ | $D_6(6)$ | 6 | (1 3 5)(2 4 6), (1 4)(2 3)(5 6) |
| $6T3$ | $D(6)$ | 12 | (1 2 3 4 5 6), (1 4)(2 3)(5 6) |
| $6T4$ | $A_4(6)$ | 12 | (1 3 5)(2 4 6), (1 4)(2 5) |
| $6T5$ | $F_{18}(6)$ | 18 | (2 4 6), (1 4)(2 5)(3 6) |
| $6T6$ | $2A_4(6)$ | 24 | (1 3 5)(2 4 6), (3 6) |
| $6T7$ | $S_4(6d)$ | 24 | (1 3 5)(2 4 6), (1 4)(2 5), (1 5)(2 4) |
| $6T8$ | $S_4(6c)$ | 24 | (1 3 5)(2 4 6), (1 4)(2 5), (1 5)(2 4)(3 6) |
| $6T9$ | $F_{18}(6):2$ | 36 | (2 4 6), (1 5)(2 4), (1 4)(2 5)(3 6) |
| $6T10$ | $F_{36}(6)$ | 36 | (1 4 5 2)(3 6), (2 4 6), (1 5)(2 4) |
| $6T11$ | $2S_4(6)$ | 48 | (1 3 5)(2 4 6), (1 5)(2 4), (3 6) |
| $6T12$ | $A_5(6)$ | 60 | (1 2 3 4 6), (1 4)(5 6) |
| $6T13$ | $F_{36}(6):2$ | 72 | (2 4 6), (1 4)(2 5)(3 6), (2 4) |
| $6T14$ | $S_5(6)$ | 120 | (1 2 3 4 6), (1 2)(3 4)(5 6) |
| $6T15$ | $A(6)$ | 360 | (1 2 6), (2 3 6), (3 4 6), (4 5 6) |
| $6T16$ | $S(6)$ | 720 | (1 2), (1 3), (1 4), (1 5), (1 6) |

A jelölések az alábbi cikkekből, címekről ismerhetők meg:


- Butler, G. and McKay, J., *The Transitive Groups of Degree up to Eleven*, Communications in Algebra, 11(8) 1983.
- Conway, J.H., Hulpke, A. and McKay, J., *On Transitive Permutation Groups*, London Mathematical Society Journal of Computation and Mathema-

tics, 1. (1998) (http://www.lms.ac.uk/jcm/1/lms1996-001/sub/lms1996-001.pdf).

- http://www.math.uni-duesseldorf.de/ klueners/minimum/minimum.html
- Maple (8) Help: Transitive Groups Naming Scheme.