# Tartalomjegyzék

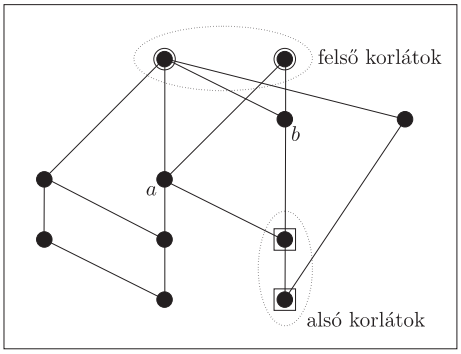
1. Fejezet

# Hálók

## 1.1 Hálószerűen rendezett halmazok

**1.1. Definíció.** *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 $c \leqslant a,b$ $[a,b \leqslant c]$.*

**1.2. Definíció.** *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.*

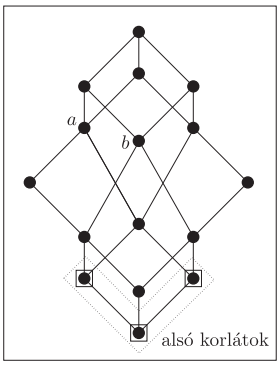



**1. ábra:** Az $a$ és $b$ elemek alsó és felső korlátjai.

**1.3. 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. □

**1.4. Definíció.** *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.

**1.5. 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), |
| $(P(U);\ \subseteq)$ | $X \cap Y$ | $X \cup Y$, |
| $(\mathrm{Sub}({}_K V);\ \subseteq)$ | $U \cap W$ | $U + W$, |
| $(\mathrm{Sub}(G);\ \subseteq)$ | $H \cap K$ | $\langle H \cup K \rangle$, |
| $(\mathrm{SubNorm}(G;\ \subseteq)$ | $M \cap N$ | $M \cdot N$. |

*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;* $\mathrm{Sub}(G)$ *a $G$ csoport részcsoportjainak halmaza, $H$ és $K$ részcsoportjai $G$-nek, $\langle H \cup K \rangle$ pedig az ezen részcsoportok egyesítése által generált részcsoport;* $\mathrm{SubNorm}(G)$ *a $G$ csoport normális részcsoportjainak halmaza, $M$ és $N$ normális részcsoportjai $G$-nek, $M \cdot N$ pedig ezen normális részcsoportok komplexus szorzata.*

## 1.2 Hálók

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

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

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

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

Bizonyítás. Legyenek $a, b, c \in L$ tetszőleges elemek. Példaként igazoljuk, hogy ezen elemekre teljesül az $(a \wedge b) \wedge c = a \wedge (b \wedge c)$ egyenlőség. 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

$$u' \leqslant (a \wedge b) \wedge c = u. \tag{1}$$

Mivel $v \leqslant b \wedge c$ miatt $v \leqslant b, c$, ezért $v \leqslant a, b, c$. Így (1) szerint $v \leqslant u$. Hasonlóan igazolható, hogy $u \leqslant v$ is teljesül, azaz $u = v$. □

**1.8. Definíció.** *Azt mondjuk, hogy az $(L; \wedge, \vee)$ algebra **háló**, ha tetszőleges $a, b, c \in L$ elemekre teljesülnek az 1.7. Állításbeli egyenlőségek.*

**1.9. Tétel.** *Legyen $(L; \leqslant)$ hálószerűen rendezett halmaz. Ekkor $(L; \wedge, \vee)$ háló, ahol $\wedge$ és $\vee$ az 1.6. Definícióbeli műveletek.*

BIZONYÍTÁS. Az 1.7. Állítás következtében nyilvánvaló. □

**1.10. 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

$$\begin{aligned} u &= u \wedge u \\ &= (u \wedge a) \wedge (u \wedge b) \\ &= u \wedge \big(a \wedge (u \wedge b)\big) \\ &= u \wedge \big((a \wedge u) \wedge b\big) \\ &= u \wedge \big((u \wedge a) \wedge b\big) \\ &= u \wedge \big(u \wedge (a \wedge b)\big) \\ &= (u \wedge u) \wedge (a \wedge b) \\ &= u \wedge (a \wedge b), \end{aligned}$$

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

**1.11. Definíció.** *Legyenek $L_1 = (L_1; \wedge_1, \vee_1)$ és $L_2 = (L_2; \wedge_2, \vee_2)$ 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 $a\varphi \leqslant_2 b\varphi$.*

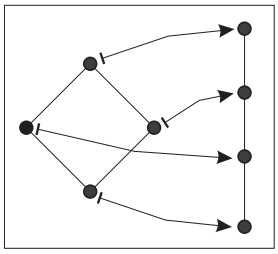
**1.12. Állítás.** *Legyenek $L_1 = (L_1; \wedge_1, \vee_1)$ és $L_2 = (L_2; \wedge_2, \vee_2)$ hálók. Ha a $\varphi\colon L_1 \to L_2$ leképezés homomorfizmus, akkor $\varphi$ rendezéstartó.*

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 leképezés, amely nem homomorfizmus.

Azonban igaz a következő.

**1.13. Tétel.** *Legyenek $L_1 = (L_1; \wedge_1, \vee_1)$ és $L_2 = (L_2; \wedge_2, \vee_2)$ 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.*

**1.14. Tétel.** *Tetszőleges $L = (L; \wedge, \vee)$ 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 $(x \wedge y) \vee z = (x \vee z) \wedge (y \vee z)$.*

**1.15. Definíció.** *Az $L$ háló **disztributív**, ha az 1.14. Tétel (1) pontja teljesül $L$-ben.*

**1.16. Definíció.** *Azt mondjuk, hogy az $L$ háló **moduláris**, ha bármely $x, y, z \in L$-re $x \leqslant z$ esetén $(x \vee y) \wedge z = x \vee (y \wedge z)$.*

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

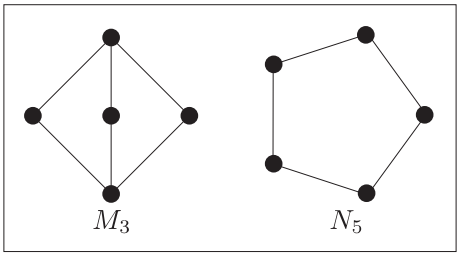
$$(x \wedge z) \vee (y \wedge z) \leqslant (x \vee y) \wedge z,$$
$$(x \wedge y) \vee z \leqslant (x \vee z) \wedge (y \vee z),$$
$$x \vee (y \wedge z) \leqslant (x \vee y) \wedge z.$$

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

*Bizonyítás.* (a) Legyen $V$ a $K$ test feletti vektortér, és legyenek $X, Y, Z$ olyan alterek $V$-ben, amelyekre $X \subseteq Z$ teljesül. Az 1.17. 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 az (a) állítást igazoltuk. A (b) állítás hasonlóan igazolható. □

**1.19. Tétel (Dedekind, 1900).** *Legyen $L$ tetszőleges háló. Az $L$ háló pontosan akkor moduláris, ha nincs az $N_5$ hálóval izomorf részhálója (ld. 4. ábra).*

**1.20. Tétel (Birkhoff).** *Az $L$ moduláris háló pontosan akkor disztributív, ha nincs az $M_3$ hálóval izomorf részhálója (ld. 4. ábra).*




**4. ábra:** Az $M_3$ és $N_5$ hálók.

## 1.3 Boole-algebrák

**1.21. Definíció.** *Az $L$ hálót **korlátosnak** nevezzük, ha van legkisebb és legnagyobb eleme. Az $L$ háló legkisebb elemét $0_L$-lel, legnagyobb elemét $1_L$-lel jelöljük. Ha nem okoz félreértést, akkor az indexet is elhagyjuk.*

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

**1.23. 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 $b = b'$. □

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

**1.25. Definíció.** *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.*

**1.26. 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).*

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

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

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

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

# Testek és bővítéseik

## 2.1 Testbővítések

Legyenek $K$ és $L$ testek. Ha $K$ részteste $L$-nek, akkor azt mondjuk, hogy $L$ **(test)bővítése** $K$-nak, és ezt az $L|K$ szimbólummal jelöljük.

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

A 2.1. Tételt fogjuk felhasználni a testbővítés fokának a definiálására. Az $L|K$ bővítés $[L : K]$ **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 $L|K$ bővítés **véges (dimenziós)**, különben $L|K$ **végtelen (dimenziós)**.

**2.2. Példa.** *A $\mathbb{C}|\mathbb{R}$ bővítés 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 $\mathbb{R}|\mathbb{Q}$ bővítések végtelenek, mivel minden $\mathbb{Q}$ feletti véges dimenziós vektortér megszámlálhatóan végtelen.*

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

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

(b) *Ha az $L|K$ és $M|L$ bővítések végesek, akkor az $M|K$ bővítés 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, $[M : K] = n \in \mathbb{N}$. Megmutatjuk, hogy ekkor $[L : K], [M : L] \leqslant n$ teljesül. Legyenek $\lambda_1, \ldots, \lambda_{n+1}$, illetve $\mu_1, \ldots, \mu_{n+1}$ tetszőleges vektorrendszerek $L$-ben, illetve $M$-ben. Mivel az $M$ vektortér $n$ dimenziós $K$ felett, és a $\lambda_1, \ldots, \lambda_{n+1}$, illetve $\mu_1, \ldots, \mu_{n+1}$ vektorok $M$-beliek, ezért vannak olyan $a_1, \ldots, a_{n+1}$, valamint $b_1, \ldots, b_{n+1}$ $K$-beli skalárok, amelyekre $(a_1, \ldots, a_{n+1}) \neq \mathbf{0}$ és $(b_1, \ldots, b_{n+1}) \neq \mathbf{0}$ teljesül és

$$a_1\lambda_1 + \cdots + a_{n+1}\lambda_{n+1} = 0, \qquad b_1\mu_1 + \cdots + b_{n+1}\mu_{n+1} = 0.$$

Ez pedig éppen azt bizonyítja, hogy a $\lambda_1, \ldots, \lambda_{n+1}$ vektorok lineárisan függők az $L$ (mint $K$ feletti) vektortérben, illetve a $\mu_1, \ldots, \mu_{n+1}$ vektorok lineárisan

függők az $M$ (mint $L$ feletti) vektortérben.

(b) Legyen $[L:K]=m$ és $[M:L]=n$. Válasszunk az $L$, illetve $M$ vektorterekben bázist:

$$\lambda_1,\dots,\lambda_m \quad \text{bázis } L\text{-ben, mint } K \text{ feletti vektortérben,} \tag{2}$$
$$\mu_1,\dots,\mu_n \quad \text{bázis } M\text{-ben, mint } L \text{ feletti vektortérben.} \tag{3}$$

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 (3) miatt vannak olyan $b_1,\dots,b_n\in L$ elemek, amelyekre

$$\mu=b_1\mu_1+\dots+b_n\mu_n.$$

Mivel $b_1,\dots,b_n\in L$, ezért (2) miatt vannak olyan $a_{i,j}\in K$ $(1\leqslant i\leqslant n,\ 1\leqslant j\leqslant m)$ elemek, amelyekre

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

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 (3) miatt $\sum_{j=1}^{m}a_{i,j}\lambda_j=0$ $(1\leqslant i\leqslant n)$. Ekkor (2)-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 $M$, mint $K$ feletti 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. Legyen $n$ természetes szám, és legyenek $K_1,\dots,K_n$ olyan testek, amelyekre $K_{i+1}|K_i$ teljesül tetszőleges $i$-re $(1\leqslant i\leqslant n-1)$. Ekkor

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

## 2.2 Algebrai és transzcendens elemek

Legyen $L$ a $K$ test bővítése, és legyen $A \subseteq L$. 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, és azt mondjuk, hogy a $K(A)|K$ bővítés $K$-nak az $A$ részhalmaz által generált bővítése. 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 $L|K$ bővítés **egyszerű**, ha van olyan $\alpha \in L$, amelyre $L = K(\alpha)$.

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

*Tekintsük a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítést. 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 $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítés egyszerű.*

**2.5. Tétel.** *Legyenek $K$ és $L$ olyan testek, amelyekre $L|K$ teljesül, valamint legyen $\alpha_1, \ldots, \alpha_n \in L$. Ekkor*

$$K(\alpha_1, \ldots, \alpha_n) = \left\{ \frac{f(\alpha_1, \ldots, \alpha_n)}{g(\alpha_1, \ldots, \alpha_n)} \mid f, g \in K[x_1, \ldots, x_n],\ g(\alpha_1, \ldots, \alpha_n) \neq 0 \right\}.$$

Tegyük fel, hogy $L|K$ teljesül, és legyen $\alpha \in L$. Ekkor két eset lehetséges:

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

A két eset szétválasztására az

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

leképezést hívhatjuk segítségül, amint azt a következő tétel mutatja.

**2.6. 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 $K(\alpha)|K$ bővítés végtelen, és az $\alpha$ transzcendens elem $K$ 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.*

Legyenek $K$ és $L$ olyan testek, amelyekre $L|K$ teljesül, valamint $\alpha \in L$ algebrai elem $K$ felett. Ekkor az 2.6. Tétel (b) részében kapott $m_{\alpha,K}$ polinomot az $\alpha$ elem **minimálpolinomjának** nevezzük. Az $\alpha$ **algebrai elem foka** minimálpolinomjának a foka, amit $\mathrm{gr}_K(\alpha)$-val jelölünk.

**2.7. Példa.** *Tekintsük az $\mathbb{R}|\mathbb{Q}$ bővítést. 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 $\mathrm{gr}_{\mathbb{Q}}(\alpha) = 8$.*

**2.8. Tétel.** *Legyen $L|K$ testbővítés, és $\alpha \in L$ algebrai elem $K$ felett, melynek minmálpolinomja $f$. Ekkor tetszőleges $g \in K[x]$, $g \neq 0$ polinomra $g(\alpha) = 0$ pontosan akkor teljesül, ha $f \mid g$.*

**2.9. 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 $[K(\alpha) : K] = \mathrm{gr}_K(\alpha)$. □

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

*Bizonyítás.* A Fokszámtételt (2.3. Tétel) alkalmazva az $K(\alpha)|K$ és $L|K(\alpha)$ bővítésekre azt kapjuk, hogy a $K(\alpha)|K$ bővítés véges, így a 2.9. Tétel szerint $\alpha$ algebrai elem $K$ felett, valamint

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

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

**2.11. Tétel.** *Legyen $L|K$ tetszőleges testbővítés, és $\alpha \in L$ algebrai elem $K$ felett, valamint legyen $k \in \mathbb{N}$. Ekkor $\sqrt[k]{\alpha}$ is algebrai $K$ felett, és $\mathrm{gr}_K(\sqrt[k]{\alpha}) \leqslant k \cdot \mathrm{gr}_K(\alpha)$.*

*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 $f(\sqrt[k]{\alpha}) = 0$, és így a 2.8. Tétel szerint $m_{\sqrt[k]{\alpha},K} \mid f$. Azaz $(m_{\sqrt[k]{\alpha},K})^* \leqslant f^* = k \cdot n = k \cdot (m_{\alpha,K})^* = k \cdot \mathrm{gr}_K(\alpha)$. □

**2.12. Tétel.** *Legyenek $L|K$ és $M|L$ tetszőleges testbővítések, és $\alpha \in M$ algebrai elem $K$ felett. Ekkor $\alpha$ algebrai $L$ 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. □

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

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

**2.14. 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 $\alpha/\beta$ is algebrai elemek $K$ felett, melyek foka legfeljebb* $\mathrm{gr}_K(\alpha) \cdot \mathrm{gr}_K(\beta)$.

Az 2.14. Tétel a Szimmetrikus polinomok Alaptételének segítségével egyszerűen igazolható. A bizonyítást nem végezzük el, de az ötletet egy példán bemutatjuk.

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

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

*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 $x^2 - 2$.

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 $\dfrac{\alpha}{\beta}$ 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 a

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

nevezője már racionális szám.

Legyen $\alpha = 1$ és $\beta = \sqrt{2} + \sqrt[3]{5}$. Ekkor $\beta$ minmálpolinomja $\mathbb{Q}$ 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` utasítással érhetjük el:

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

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

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

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** megmutatja, hogy bizonyos valós számok, amelyeket ma Liouville-számoknak nevezünk, transzcendensek $\mathbb{Q}$ felett. Ilyan szám pl.: $\sum_{n=1}^{\infty} \frac{1}{2^{n!}}$.

- **1873** Charles **Hermite** megmutatja, hogy az $e$ szám transzcendens.
- **1874** George Ferdinand Ludwig **Cantor** 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** igazolja, hogy a $\pi$ szám transzcendens $\mathbb{Q}$ felett.
- **1934** A.J. **Gelfond** 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. (Pl.: $2^{\sqrt{2}}$ transzcendens $\mathbb{Q}$ felett.)

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?

## 2.3 Algebrai testbővítések

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

**2.17. 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 2.9. 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 2.9. Tétel szerint

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

Ekkor az 2.3. Tételt 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. □

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

**2.19. 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 2.17. Tétel szerint a $K(S')$ bővítés algebrai, így $\alpha$ is algebrai elem $K$ felett. Azaz a $K(S)|K$ bővítés algebrai. □

**2.20. 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 2.3. Tétel 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 2.3. Tétel 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. □

**2.21. 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 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 interpolációs tétele[1] 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.*
$\vdots$
*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.*

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

Legyen $D$ integritástartomány[2], 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.

**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

**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 az 3.5. Tétel szerint az $f$ polinom is irreducibilis. A megfelelő eltolt megtalálása azonban nem egyszerű feladat, sőt nem is létezik megfelelő eltolt.

## 3.3 Egyéb tesztek az irreducibilitás eldöntésére

**3.6. 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 $\text{ln.k.o.}(p,q) = 1$, 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.*

**3.7. 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.*

**3.8. 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.*

**3.9. 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.*

[2] Azaz $D$ kommutatív, egységelemes és zérusostómentes.

# Felbontási testek

## 4.1 Felbontási testek

**4.1. Definíció.** *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 $L = K(\alpha_1, \ldots, \alpha_r)$.*

A felbontási test definíciójának közvetlen következménye az alábbi állítás.

**4.2. Állítás.** *Ha $L$ felbontási teste az $f \in K[x]$ polinomnak $K$ felett, akkor az $L|K$ bővítés véges algebrai bővítés.*

**4.3. 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 $1 \leqslant g^* = s,\ h^* = t \leqslant n$. 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 $M$ 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

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

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 $M$ bővítése, 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

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

is teljesül. □

## 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 $K_2$ számtestek, valamint $\eta\colon K_1 \to K_2$ izmorfizmus. 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.

**4.4. 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 $L$ és $L'$ az $f$ és $\eta_f$ 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.*

**4.5. 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.*

*Bizonyítás.* 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 4.4. 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 tényezője $f$-nek. Ekkor $g \mid f$ miatt $\eta_g \mid \eta_f$. 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 4.5. 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 $k[L : M] \leqslant m[L : M] = [L : K]$ 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 4.4. Tételben $K = K'$ teljesül, és $\eta = \mathrm{id}_K$. Ekkor $\eta_f = f$, és a következő tételt kapjuk.

**4.6. 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.*

## 4.3 Polinomok többszörös gyökök

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 $\alpha_1, \ldots, \alpha_r$ 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.

**4.7. Definíció.** *Legyen $K$ tetszőleges test, és legyen $D_x$ a következő leképezés:*

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

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

Az alábbi tétel a formális deriválás tulajdonságait foglalja össze.

**4.8. Állítás.** *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) *$D_x$ **derivváció** 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 $\operatorname{char}(K) = 0$, akkor $\ker(D_x) = K$, és a $D_x$ leképezés szürjektív.*

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

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

*és $D_x$ képterét generálják az $x^k$ 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 $f = h(x^p)$. □

**4.9. Tétel.** *Legyen $f$ a $K$ test feletti polinom, és $\alpha \in L$ az $f$ polinom gyöke a $K$ test valamely $L$ bővítésében. 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 4.8. Állítás (2) szerint

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

Ekkor $x-\alpha$ osztója az $f$ és $D_x(f)$ polinomoknak $L[x]$-ben, és így $x-\alpha \mid$ ln.k.o.$(f, D_x(f))$. Azaz ln.k.o.$(f, D_x(f))$ legalább elsőfokú polinom, melynek gyöke az $\alpha$.

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. □

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

*Bizonyítás.* Mivel $D_x(f)^* = n-1$ és az $f$ polinom irreducibilis, ezért

$$\text{ln.k.o.}(f, D_x(f)) \sim 1,$$

így $f$-nek nem lehet többszörös gyöke $L$-ben. □

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

**4.12. Definíció.** *Legyen $f$ irreducibilis polinom a $K$ test felett ($f^* = n \geqslant 1$). Az $f$ polinom* ***szeparábilis****, ha $f$-nek $n$ különböző gyöke van $L$-ben, ahol $L$ az $f$ polinom felbontási teste $K$ felett.*

**4.13. Definíció.** *Legyen $f$ tetszőleges $K$ test feletti polinom. Az $f$ polinom* ***szeparábilis****, ha $f$ minden irreducibilis tényezője szeparábilis.*

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

**4.15. Példa.** *Ha a $K$ test karakterisztikája 0, akkor $K$ tökéletes.*

*Bizonyítás.* Legyen $f$ tetszőleges $K[x]$-beli irreducibilis polinom. Tegyük fel, hogy $f$-nek van többszörös gyöke. Ekkor ln.k.o.$(f, D_x(f))$ legalább elsőfokú polinom. Mivel $f$ irreducibilis és ln.k.o.$(f, D_x(f)) \mid f$, ezért ln.k.o.$(f, D_x(f)) \sim f$. Így $f \mid D_x(f)$, ami azonban a polinomok fokszámai miatt nem lehetséges. □

# Test algebrai lezártja

## 5.1 Bevezetés

**5.1. 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 $L|K$ algebrai és $L$ algebrailag zárt.*

**5.2. 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.*

**5.3. 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 2.20. 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. □

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

*Bizonyítás.* A 2.19. 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 $L_a(\alpha)|L$ 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. □

## 5.2 Test algebrai lezártjának létezése

**5.5. 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.

**5.6. 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 $\bar{\varphi}\colon K[X] \to H$ leképezéssé. 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, ezér 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 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. □

**5.7. 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 5.4. Tételből adódik. □

## 5.3 Test algebrai lezártjának egyértelműsége

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

**5.8. 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. □

**5.9. 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. □

# Normális bővítések

## 6.1 Alapvető tulajdonságok

Az $L|K$ testbővítés **normális**, ha algebrai bővítés 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.

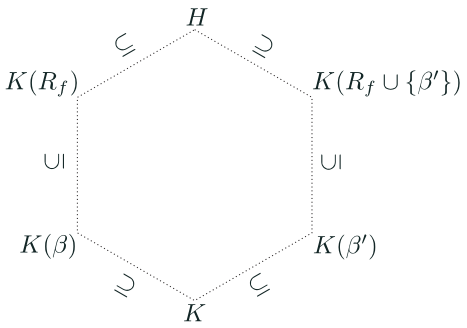
Legyen $K$ tetszőleges test és $S \subseteq K[x]$. Azt mondjuk, hogy a $K$ test $L$ bővítése **felbontási teste az $S$ polinomhalmaznak**, ha $S$ valamennyi eleme elsőfokú tényezők szorzatára bontható $L[x]$-ben, és $L$ a legszűkebb ilyen tulajdonságú test.

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.

**6.1. 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 (2.19. Következmény). Legyen $\beta$ tetszőleges eleme az $L$ testnek. Ekkor vannak olyan $\alpha_1, \dots, \alpha_t \in A$ 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.




**5. 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

$$[K(\beta) : K] = [K(\beta') : K]. \tag{4}$$

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.: 4.5. 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.

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

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

Így a 4.4. Tétel szerint $\vartheta$ 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 (4) 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 $\beta' \in K(R_f)$. □

**6.2. 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 $M = F$.

**6.3. Következmény.** *Ha az $L|K$ 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 $M = F$. □

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

## 6.2 Injektív homomorfizmusok és automorfizmusok

A 6.4. 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

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

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

**6.5. 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 4.5. 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 4.4. 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. □

## 7.1 Fixtestek és Galois-csoportok

Legyen $L|K$ teszőleges testbővítés. Definiáljuk a $\varphi\colon P(\mathrm{Gal}(L|K)) \to P(L)$ és $\gamma\colon P(L) \to P(\mathrm{Gal}(L|K))$ lképezéseket 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 $\mathrm{Gal}(L|K)$ Galois-csoportja részcsoportjai közötti (Galois-)kapcsolat tulajdonságait fogjuk részletesen megvizsgálni.

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

*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. □

**7.2. 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 $\omega(U) = U$.

**7.3. 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

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

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

$$\gamma(M) = \gamma\varphi\gamma(M). \tag{5}$$

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 (5) 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.

**7.4. 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 7.3. 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[3] $L$ felett, ezért $L^G$ a $\varphi(G) \leqslant L$ test felett is vektortér.

**7.5. 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

$$a_1T_{\alpha_1} + \cdots + a_nT_{\alpha_n} = 0. \tag{6}$$

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

$$a_1\sigma(\alpha_1) + \cdots + a_n\sigma(\alpha_n) = 0 \tag{7}$$

[3] $L^G$ 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

$$\tau(a_1)\sigma(\alpha_1) + \cdots + \tau(a_n)\sigma(\alpha_n) = 0. \tag{8}$$

Szorozzuk meg a (6) egyenlőséget $\tau(a_n)$-nel, a (8) 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 (7) 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.

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

**7.7. 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 4.5. 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 6.4. 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 7.6. 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 7.7. Lemma alkalmazható az $\eta$ injektív homomorfizmusra, és a lemma szerint $\eta$ pontosan $[L : K]$-féleképpen terjeszthető ki $L \to L$ injektív homomorfizmussá. Az 2.21. 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. □

**7.8. 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 7.5. 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 4.4. 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 7.6. Tétel szerint az $L|\varphi(G)$ bővítés Galois-bővítés. □

**7.9. 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 7.6. Tétel következménye. A 7.8. 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 7.6. Tétel szerint

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

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

## 7.2 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 7.9. Tételt polinomokra alkalmazva a következőt kapjuk.

**7.10. 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.

**7.11. 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 $\sigma \in \mathrm{Gal}_K(f)$-ra $\sigma|_R \in S_R$, 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.

## 7.3 Egy példa.

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

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

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

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

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

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

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 $G = S_X$.

**7.12. 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

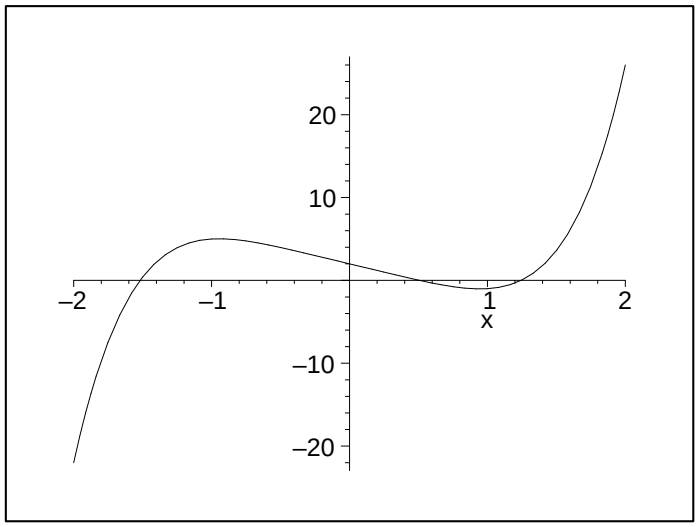
$$\{\sigma|_R \mid \sigma \in \mathrm{Gal}_K(f)\} \leqslant S_R$$

permutációcsoport tranzitív és tartalmaz transzpozíciót. Ekkor az előzőek szerint $\{\sigma|_R \mid \sigma \in \mathrm{Gal}_K(f)\} = S_R$. Továbbá, a 7.11. Tétel szerint,

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

□

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




**7. 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 $\mathrm{Gal}_{\mathbb{Q}}(f) \cong S_5$.

## 7.4 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 7.1. és 7.2. Lemmák, valamint a 7.4. Következmény szerint jóldefiniáltak.

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

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

(b) *Bármely $H_1 \subseteq H_2$ részcsoportjára $\mathrm{Gal}(L|K)$-nak teljesül, hogy $[H_2 : H_1] = [\Phi(H_1) : \Phi(H_2)]$.*

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

(d) *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*

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

**7.14. 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 7.11. 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*

$$1,\ \sqrt[4]{2},\ \sqrt{2},\ (\sqrt[4]{2})^3, i,\ i\sqrt[4]{2},\ i\sqrt{2},\ i(\sqrt[4]{2})^3. \tag{9}$$

*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 (9) 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*

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

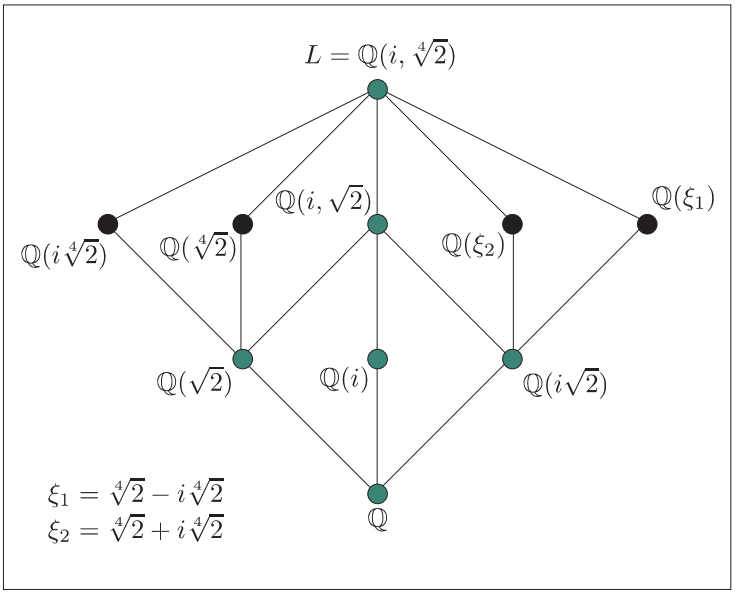
*azaz*

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

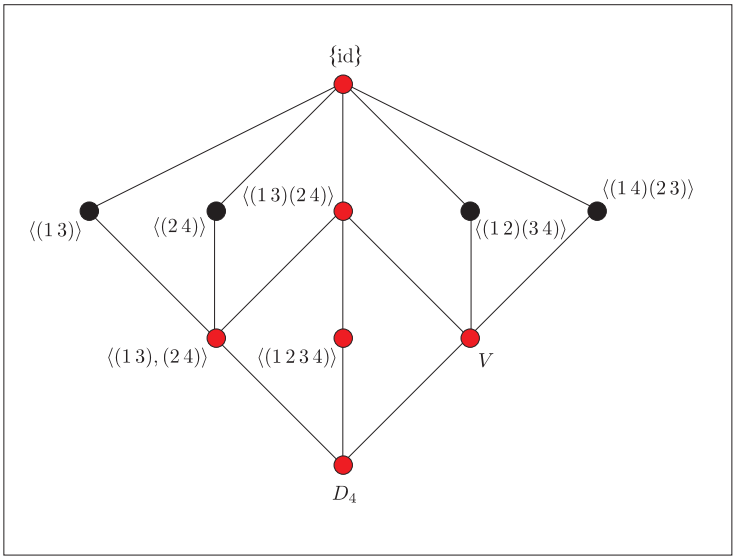
*A fentiek szerint a $H$ részcsoport által fixen hagyott résztest:*

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

*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 8., illetve 9. ábrán láthatók. (A 8. ábrán zölddel jelölt $M$ közbülső testekre az $M|\mathbb{Q}$ bővítés normális, illetve a 9. ábrán pirossal jelölt részcsoportok normálosztók.)*




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




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

**7.15. Tétel.** *Az $L|K$ algebrai bővítés pontosan akkor egyszerű, ha véges sok közbülső teste van.*

**7.16. Tétel.** *Ha az $L|K$ bővítés véges és szeparábilis, akkor egyszerű.*

**7.17. Következmény.** *Ha az $L|K$ bővítés Galois-bővítés, akkor van olyan irreducibilis $f \in K[x]$ polinom, amelynek felbontási teste $L$.*

## 8.1 Bővítés radikálokkal

Tegyük fel, hogy az $L$ és $K$ számtestekre $L|K$ teljesül, és legyen $\beta \in L$. Azt mondjuk, hogy a $\beta$ **radikál** $K$ felett, ha $\beta^n \in K$ valamely $n \in \mathbb{N}_0$-ra. Azt mondjuk, hogy az $L|K$ bővítés **radikálbővítés**, ha vannak az $L|K$ bővítésnek olyan $L_0, \ldots, L_r$ közbülső testei, amelyekre

$$L = L_r|L_{r-1}|\cdots|L_1|L_0 = K$$

teljesül és $L_i = L_{i-1}(\beta_i)$, ahol $\beta_i$ radikál $L_{i-1}$ felett minden $i$-re $(1 \leqslant i \leqslant r)$.

Legyen $f \in K[x]$. Azt mondjuk, hogy $f$ **radikálokkal megoldható**, ha van a $K$ testnek olyan $L$ radikálbővítése, amely felett az $f$ polinom már elsőfokú polinomok szorzatára bontható. Fontos megjegyezni, hogy az $L$ test nem feltétlenül felbontási teste $f$-nek.

## 8.2 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 számolva) az $f$ polinom valamely $L$ felbontási testében, valamint $R = \{\alpha_1, \ldots, \alpha_n\}$. 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

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

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:

1. $\delta = 0$; ekkor az $f$ polinomnak van többszörös gyöke.

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

$$\delta = \sigma(\delta) = (-1)^{\mathrm{sgn}(\sigma)}\delta,$$

   így $\mathrm{sgn}(\sigma) = +1$. Ez pedig azt jelenti, hogy $\mathrm{Gal}_K(f)$ csak páros permutációkat tartalmaz, azaz $\mathrm{Gal}(f|K) \leqslant A_n$.

3. $\delta \notin K$; 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.

**8.1. 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 $\Delta = 0$; ekkor 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 determinánsok kiszámításával kaphatjuk meg:

$$\delta = \begin{vmatrix} 1 & 1 & \cdots & 1 \\ \alpha_1 & \alpha_2 & \cdots & \alpha_n \\ \alpha_1^2 & \alpha_2^2 & \cdots & \alpha_n^2 \\ \vdots & \vdots & \ddots & \vdots \\ \alpha_1^{n-1} & \alpha_2^{n-1} & \cdots & \alpha_n^{n-1} \end{vmatrix}, \quad \Delta = \begin{vmatrix} n & \lambda_1 & \cdots & \lambda_{n-1} \\ \lambda_1 & \lambda_2 & \cdots & \lambda_n \\ \lambda_2 & \lambda_3 & \cdots & \lambda_{n+1} \\ \vdots & \vdots & \ddots & \vdots \\ \lambda_{n-1} & \lambda_n & \cdots & \lambda_{2n-2} \end{vmatrix},$$

ahol $\lambda_j = \alpha_1^j + \cdots + \alpha_n^j$ ($j \in \mathbb{N}$). Ha $f = x^2 + a_1x + a_0$, akkor

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

Ha $f = x^3 + a_2x^2 + a_1x + a_0$, akkor

$$\Delta = \begin{vmatrix} 3 & \lambda_1 & \lambda_2 \\ \lambda_1 & \lambda_2 & \lambda_3 \\ \lambda_2 & \lambda_3 & \lambda_4 \end{vmatrix} = 3\lambda_2\lambda_4 - 3\lambda_3^2 - \lambda_1^2\lambda_4 + 2\lambda_1\lambda_2\lambda_3 - \lambda_2^3.$$

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

$$\begin{aligned}
\lambda_1 &= \sigma_1 = -a_2,\\
\lambda_2 &= \sigma_1^2 - 2\sigma_2 = a_2^2 - 2a_1,\\
\lambda_3 &= \sigma_1^3 - 3\sigma_2\sigma_1 + \sigma_3 = -a_2^3 + 3a_1a_2 - 3a_1,\\
\lambda_4 &= 4\sigma_3\sigma_1 + \sigma_1^4 - 4\sigma_2\sigma_1^2 + 2\sigma_2^2 = a_2^4 - 4a_1a_2^2 + 4a_1a_2 + 2a_1^2,
\end{aligned}$$

és

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

**8.2. 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* $\mathrm{Gal}_{\mathbb{Q}}(g) \cong S_3$*.*

## 8.3 Harmadfokú polinomok

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

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

Tekintsük az $f$ polinom $\frac{a_2}{3}$-eltoltját; legyen

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

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 8.1. Tétel szerint $[L : K(\delta)] = 3$ és $\mathrm{Gal}(L|K(\delta)) \cong A_3$.

Legyen $\varepsilon = -\dfrac{1}{2} + i\dfrac{\sqrt{3}}{2}$ 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 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:

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

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,

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

**8.3. 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.*

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

## 8.4 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

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

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 $H = V \cap G \lhd G$. 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

$$\mu^2 = (\alpha_1 + \alpha_2)^2 = -(\alpha_1 + \alpha_2)(\alpha_3 + \alpha_4),$$
$$\nu^2 = (\alpha_1 + \alpha_3)^2 = -(\alpha_1 + \alpha_3)(\alpha_2 + \alpha_4),$$
$$\xi^2 = (\alpha_1 + \alpha_4)^2 = -(\alpha_1 + \alpha_4)(\alpha_2 + \alpha_3).$$

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:

$$\mu^2 + \nu^2 + \xi^2 = -2p,$$
$$\mu^2\nu^2 + \nu^2\xi^2 + \xi^2\mu^2 = p^2 - 4r,$$
$$\mu\nu\xi = -q.$$

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

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

és $L = K(\mu, \nu, \xi)$.

**8.5. 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.

**8.6. 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.*

**8.7. Példa.** *Tekintsük a 8.5. 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 8.6. Tétel szerint*

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

## 9.1 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 normálláncfaktorainak nevezzük; $n$ a normálláncfossza.

Azt mondjuk, hogy a $G$ csoport **feloldható**, ha $G$-nek van olyan normálláncának, amelynek faktorai Abel-csoportok.

**9.1. Példa.** *Az $S_3$ csoport feloldható, mivel a*

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

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

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

*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.*

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

**9.3. Tétel.** *Legyen $G$ csoport, $H \leqslant G$ és $N \lhd G$. 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.*

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

## 9.2 Polinomok feloldható Galois-csoporttal

**9.5. Tétel.** *Legyen $K$ tetszőleges számtest. Tegyük fel, hogy az $f \in K[x]$ polinom szeparábilis és a $\mathrm{Gal}_K(f)$ Galois-csoport feloldható. Ekkor $f$ radikálokkal megoldható.*

## 9.3 Polinomok, amelyek megoldhatók radikálokkal

**9.6. Tétel.** *Legyen $K$ számtest. Tegyük fel, hogy az $L|K$ bővítés Galois-bővítés. Legyen $\beta$ az $x^n - \vartheta$ polinom egy gyöke, ahol $\vartheta \in L$. Ekkor van olyan $N|L(\beta)$ radikálbővítés, amelyre $N|K$ Galois-bővítés.*

**9.7. Tétel.** *Legyen $K$ számtest. Tegyük fel, hogy az*

$$L = L_r|L_{r-1}|\cdots|L_0 = K$$

*bővítés radikálbővítés, ahol $L_i = L_{i-1}(\beta_i)$ és $\beta_i$ az $x^{n_i} - \vartheta_i$ ($\vartheta_i \in L_{i-1}$) polinom egy gyöke ($n_1, \ldots, n_r \in \mathbb{N}$). Ekkor van olyan $M|L$ bővítés, amelyre az $M|K$ radikálbővítés Galois-bővítés.*

**9.8. Tétel.** *Legyen $K$ számtest. Tegyük fel, hogy az*

$$L = L_r|L_{r-1}|\cdots|L_0 = K$$

*bővítés radikálbővítés, ahol $L_i = L_{i-1}(\beta_i)$ és $\beta_i$ az $x^{n_i} - \vartheta_i$ ($\vartheta_i \in L_{i-1}$) polinom egy gyöke ($n_1, \ldots, n_r \in \mathbb{N}$). Ha az $f \in K[x]$ polinom elsőfokú polinomok szorzatára bontható $L$ felett, akkor a $\mathrm{Gal}(f|K)$ Galois-csoport feloldható.*

## 10.1 Geometriai szerkeszthetőség

### 10.1.1 Szerkesztés körzővel és vonalzóval

A szerkesztéshez használható két legelemibb geometriai eszköz a vonalzó[4] és a körző[5]. 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.

**10.1. Definíció.** *Ha egy szerkesztési feladatot pusztán az* ($E_1$)*–*($E_3$) *lépések véges sokszori alkalmazásával végzünk, akkor a szerkesztést* ***euklideszi szerkesztésnek*** *nevezzük.*

### 10.1.2 Szerkesztés valós alaptest felett

A továbbiakban az euklideszi szerkesztés algebrai leírását szeretnénk megadni valós alaptest felett.

**10.2. 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.*

**10.3. 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 $P = e \cap f$;*

[4] 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.

[5] A körzőnk tetszőlegesen nagy nyílású.

- $\mathcal{E}_2(H)$ *azon* $P$ *pontok halmaza, amelyekhez van olyan* $e$ $H$*-egyenes és* $k$ $H$*-kör, amelyekre* $P = e \cap k$*;*
- $\mathcal{E}_3(H)$ *azon* $P$ *pontok halmaza, amelyekhez vannak olyan különböző* $k_1$ *és* $k_2$ $H$*-körök, amelyekre* $P = k_1 \cap k_2$*.*

*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.*

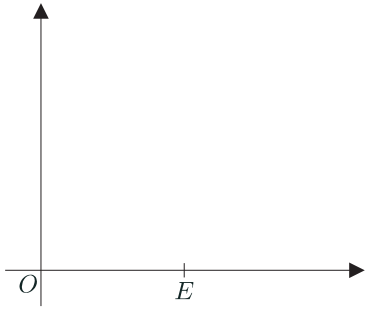
**10.4. Definíció.** *Legyen adott az* $\mathcal{S}$ *sík* $H$ *részhalmaza, amelyből kiindulva definiáljuk a* $H_i$ $(i \in \mathbb{N}_0)$ *halmazokat a következő módon:*

$$H_0 = H,$$
$$H_{i+1} = H_i \cup \mathcal{E}_1(H_i) \cup \mathcal{E}_2(H_i) \cup \mathcal{E}_3(H_i).$$

*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.




**10. ábra:** az $O = (0, 0)$ és $E = (1, 0)$ pontok.

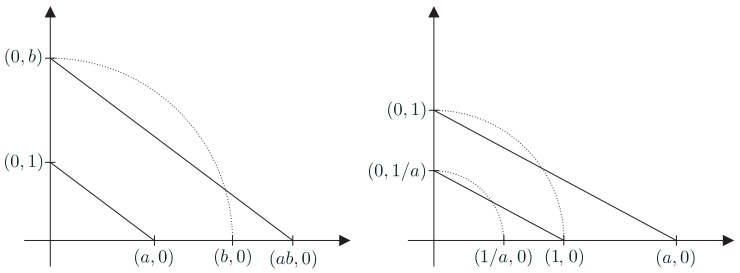
**10.5. Állítás.** (1) *A* $H$*-beli* $O$*,* $E$ *pontokból a két tengely megszerkeszthető.*
(2) *Egy* $(a, b)$ *pont akkor és csak akkor szerkeszthető meg* $H$*-ból, ha* $(a, 0)$ *és* $(b, 0)$ *megszerkeszthető.*
(3) *Valahányszor az* $(a, 0)$*,* $(b, 0)$ *pontok megszerkeszthetők* $H$*-ból, mindannyiszor megszerkeszthetők a következő pontok is:*

(i) $(a + b, 0)$*,* $(-a, 0)$*,*

(ii) $(ab, 0)$*,* $(1/a, 0)$ $(ha\ a \neq 0)$*,*

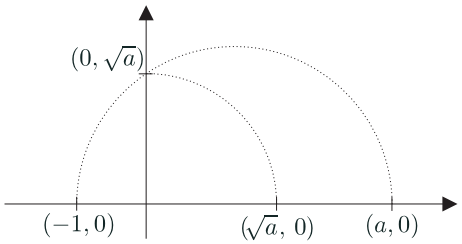
(iii) $(\sqrt{a}, 0)$ $(ha\ a \geqslant 0)$*.*

*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). □




**11. ábra:** az $(ab, 0)$ és $(1/a, 0)$ pontok szerkesztése.

**10.6. Definíció.** *A $(H, P)$ szerkesztési feladat alaptestén a $H$-beli pontok koordinátái által generált valós számtestet értjük.*




**12. ábra:** a $(\sqrt{a}, 0)$ pont szerkesztése.

**10.7. 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 $(c_j \geqslant 0)$.*

**10.8. 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.

**10.9. 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 $\alpha, \beta \in \mathbb{Q}(\sqrt{D})$.*

*10.8. 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 10.9. 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 10.5. 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 10.5. 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 10.8. 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 10.8. Tétel alábbi változata egyenértékű az eredetivel.

**10.10. 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.*

## 10.2 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.

### 10.2.1 A kör négyszögesítése.

A kérdés az, hogy lehetséges-e az egységsugarú körrel azonos területű négyzetet szerkeszteni.[6] Az egységsugarú kör területe $\pi$, így a körrel azonos területű négyzet oldalának a hossza éppen $\sqrt{\pi}$. A kérdés tehát — a 10.25. 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.

**10.11. 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 $f = 0$.*

**10.12. 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.

[6] 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.

### 10.2.2 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 (3.6. Tétel) segítségével gyorsan kideríthető, hogy ez utóbbi polinomnak nincs racionális gyöke, így a 3.8. 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.

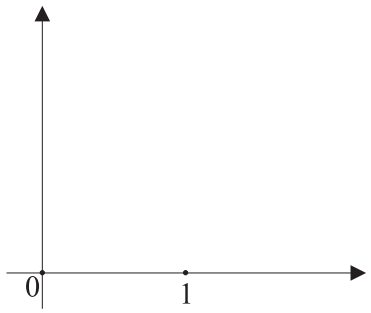
### 10.2.3 Déloszi probléma vagy kockakettőzés.

Olyan kockát kell szerkeszteni, amely kétszer akkora térfogatú mint egy adott kocka.[7] 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 10.25. Következmény szerint.

### 10.2.4 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. 13. ábra).

[7] 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.




**13. ábra:** a 0 és 1 pontok.

**10.13. 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.

**10.14. 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 $(c_j \geqslant 0)$.

**10.15. 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.*

### 10.2.5 Legfeljebb negyedfokú polinom gyökének szerkeszthetősége

**10.16. 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. □

**10.17. 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.*

**10.18. 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.*

## 10.3 Szabályos sokszögek szerkeszthetősége

Egy olyan tétellel kezdjük e részt, amely sok szerkesztési feladat esetén használható a nem-szerkeszthetőség igazolására.

**10.19. 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.

**10.20. 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.

**10.21. 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

$$\chi_p = x^{p-1} + x^{p-2} + \cdots + x + 1 \in \mathbb{Z}[x]$$

polinomot **$p$-edik körosztási polinomnak**,

$$\chi_{p^2} = x^{p(p-1)} + x^{p(p-2)} + \cdots + x^p + 1 \in \mathbb{Z}[x]$$

polinomot pedig **$p^2$-edik körosztási polinomnak** nevezzük.

**10.22. Tétel.** *Tetszőleges $p$ prímre*

(a) *$\varepsilon_p$ gyöke $\chi_p$-nek, $\varepsilon_{p^2}$ pedig $\chi_{p^2}$-nek;*

(b) *a $\chi_p$ és $\chi_{p^2}$ polinomok irreducibilisek $\mathbb{Q}$ 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 10.19. és 10.22 Tételekből közvetlenül adódik az alábbi tétel.

**10.23. 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.*

**10.24. Tétel.** *Ha $p$ Fermat-prím, akkor $\varepsilon_p$ megszerkeszthető.*

## 10.4 A szerkeszthetőség szükséges és elegendő feltétele

A szerkeszthetőség egy szükséges feltétele.

**10.25. 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 2.17. Tétel szerint az $L|K$ testbővítés algebrai, így $u$ algebrai $K$ felett és a 2.10. Állítás következtében $u$ foka is 2-hatvány $K$ felett. □

A szerkeszthetőség egy elegendő feltétele.

**10.26. 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 10.15. Tétel szerint elegendő az alábbi (tisztán algebrai) tételt igazolni.

**10.27. 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.

**10.28. 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.*

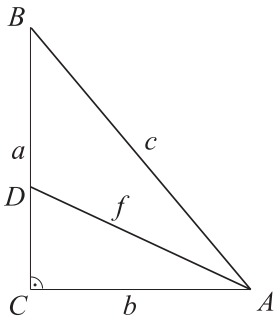
## 10.5 Hétköznapi szerkesztési feladatok

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.

**10.29. 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. 14. ábra). A továbbiakban az $AC$ befogó $b$ hosszára fogunk egy algebrai egyenletet felírni, mivel $b$ ismeretében a háromszög már egyszerűen megszerkeszthető.




**14. 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 10.16. 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

$$b = \frac{f^2 + \sqrt{f^4 + 8f^2c^2}}{4c}.$$

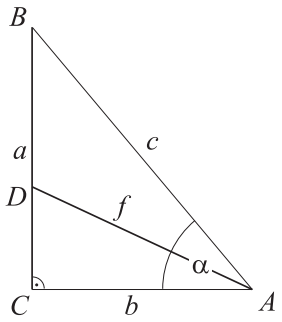
A szerkesztendő háromszög csak akkor létezhet, ha $0 < f < c$. Ezen feltétel teljesülése esetén azonban

$$b < \frac{c^2 + \sqrt{c^4 + 8c^2c^2}}{4c} = c,$$

azaz létezik a $c$ átfogójú, $b$ befogójú derékszögű háromszög.

**10.30. 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. 15. ábra).




**15. 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 $p = 4x^6 + 4(a^2 - f^2)x^4 - 4a^2 f^2 x^2 + a^2 f^4$ 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

$$4x^3 + 4(a^2 - f^2)x^2 - 4a^2 f^2 x + a^2 f^4 \tag{10}$$

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 (10) szerint $b^2$ gyöke a $4x^3 - 4x + 1 \in \mathbb{Q}[x]$ polinomnak. Rolle tételét (3.6. Tétel) alkalmazva azt kapjuk, hogy e polinomnak nincs racionális gyöke. Így a 10.17. Tétel szerint $b^2$ nem szerkeszthető, de a háromszög létezik ($b \approx 0,915$).

# Feladatok

**1.** Legyen $(P;\leqslant)$ részbenrendezett halmaz. Definiáljuk a $<\subset P\times P$ relációt a következőképpen:

$$x<y \iff x\leqslant y,\ x\neq y \quad (x,y\in P).$$

Mutassuk meg, hogy

(a) nincs olyan $x\in P$, amelyre $x<x$ teljesül;

(b) ha $x<y$ és $y<z$, akkor $x<z$ $(x,y,z\in P)$.

**2.** A $P$ halmazon legyen $<\subseteq P\times P$ olyan reláció, amelyre teljesül, hogy

- nincs olyan $x\in P$, amelyre $x<x$ teljesül;
- ha $x<y$ és $y<z$, akkor $x<z$ $(x,y,z\in P)$.

Definiáljuk a $\leqslant\subseteq P\times P$ relációt a következőképpen:

$$x\leqslant y \iff x<y \text{ vagy } x=y \quad (x,y\in P).$$

Mutassuk meg, hogy $\leqslant$ részbenrendezés a $P$ halmazon.

**3.** Tetszőleges $A$ halmazra legyen

$$P=\{\alpha\subseteq A\times A \mid \alpha \text{ részbenrendezés } A\text{-n}\}.$$

A $P$ halmazon definiáljuk a $\leqslant$ relációt a következőképpen:

$$\alpha\leqslant\beta \iff (\forall a,b\in A)(a\,\alpha\,b \Longrightarrow a\,\beta\,b).$$

Igazoljuk, hogy $(P;\leqslant)$ részbenrendezett halmaz.

**4.** Mutassuk meg, hogy a $\leqslant\subseteq A\times A$ reláció részbenrendezés $A$-n.

(a) $A=P(X)$, az $X$ halmaz összes részhalmazainak halmaza, és $X_0\leqslant X_1$ pontosan akkor teljesül, ha $X_0\subseteq X_1$ $(X_0,X_1\in P(X))$.

(b) $A$ az összes az $X$ halmazból $\mathbb{R}$-be menő leképezések halmaza, és $f\leqslant g$ pontosan akkor teljesül, ha $f(x)\leqslant g(x)$ minden $x\in\mathbb{R}$-re $(f,g\in A)$.

(c) $A$ az emberek halmaza, és $a\leqslant b$ pontosan akkor teljesül, ha $a$ őse $b$-nek vagy $a=b$ $(a,b\in A)$.

(d) $A=\mathbb{N}$ és $m\leqslant n$ pontosan akkor teljesül, ha $m\mid n$ $(m,n\in A)$.

**5.** Legyen $A$ egy $k$-elemű halmaz, ahol $1 \leqslant k \leqslant 6$. Adjuk meg Hasse-diagrammal az összes részberendezést $A$-n. Döntsük el, hogy mely $\leqslant$ részbenrendezésekre lesz $(A; \leqslant)$ háló, moduláris háló, illetve disztributív háló.

**6.** Legyen $\mathbb{Z}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Z}\}$ és $\mathbb{Q}[\xi] = \{a + b\xi \mid a, b \in \mathbb{Q}\}$, ahol $\xi \in \mathbb{C} \setminus \mathbb{Q}$ egy másodfokú valós együtthatós polinom egyik gyöke. A másik gyököt jelölje $\xi'$. Mutassuk meg, hogy

(a) $\mathbb{Z}[\xi]$ gyűrű a szokásos összeadásra és szorzásra;

(b) $\mathbb{Q}[\xi]$ számtest;

(c) $\mathbb{Z}[\xi]$ elemeinek $a + b\xi$ $(a, b \in \mathbb{Z})$ alakban való előállítása egyértelmű;

(d) $\mathbb{Q}[\xi]$ elemeinek $a + b\xi$ $(a, b \in \mathbb{Q})$ alakban való előállítása egyértelmű;

(e) $\mathbb{Z}[\xi] = \mathbb{Z}[\xi']$;

(f) $\mathbb{Q}[\xi] = \mathbb{Q}[\xi']$.

**7.** Legyen $p$ prímszám. Mutassuk meg, hogy $[\mathbb{Q}(\sqrt{p}) : \mathbb{Q}] = 2$.

**8.** Határozzuk meg a $\mathbb{Q}(\sqrt{2}, \sqrt{3})|\mathbb{Q}$ bővítés fokát.

**9.** Legyen $p$ és $q$ különböző prímszámok. Határozzuk meg a $\mathbb{Q}(\sqrt{p}, \sqrt{q})|\mathbb{Q}(\sqrt{p})$ bővítés fokát.

**10.** Legyenek $p_1, \ldots, p_n$ páronként különböző prímszámok. Mutassuk meg, hogy $\sqrt{p_n} \notin \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})$. Így $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_{n-1}})] = 2$ és $[\mathbb{Q}(\sqrt{p_1}, \ldots, \sqrt{p_n}) : \mathbb{Q}] = 2^n$.

**11.** Legyenek $K$ és $L$ olyan számtestek, amelyekre $L|K$ teljesül. Legyen $u$ $v$ az $L$ test olyan elemei, amelyekre $u^2$ és $v^2$ a $K$ test különböző elemei. Mutassuk meg, hogy $K(u, v) = K(u + v)$.

**12.** Tegyük fel, hogy $[L : K]$ prímszám. Mik lesznek az $L|K$ bővítés közbülső testei?

**13.** Tegyük fel, hogy $K_1$ és $K_2$ az $L|K$ bővítés olyan közbülső testei, amelyekre $L = K(K_1, K_2)$. Mutassuk meg, hogy $[L : K] \leqslant [K_1 : K] \cdot [K_2 : K]$.

**14.** Mutassuk meg, hogy az $f = x^3 + 3x + 1$ polinom irreducibilis $\mathbb{Q}[x]$-ben. Legyen $\alpha \in \mathbb{C}$ az $f$ polinom gyöke. Fejezzük ki az $\alpha^{-1}$ és $(1 + \alpha)^{-1}$ elemeket az 1, $\alpha$ és $\alpha^2$ elemeknek racionális együtthatós lineáris kombinációjaként.

**15.** Tegyük fel, hogy $L(\alpha)|L$, $L|K$ teljesül és $[K(\alpha) : K]$, $[L : K]$ relatív prímek. Mutassuk meg, hogy $m_{\alpha,L} \in K[x]$.

**16.** Bizonyítsuk be, hogy ha $[L : K]$ prímszám, akkor az $L|K$ bővítés egyszerű.

**17.** Legyen $K$ megszámlálhatóan végtelen test és $L|K$ algebrai bővítés. Mutassuk meg, hogy $|L|$ is megszámlálhatóan végtelen. Mutassuk meg, hogy vannak olyan valós számok, amelyek transzcendensek a racionális számok teste felett.

**18.** Legyen $L|K$ bővítés, $\alpha \in L$ transzcendens elem $K$ felett és $f \in K[x]$ nem konstans polinom. Mutassuk meg, hogy

(a) $f(\alpha)$ transzcendens $K$ felett;

(b) ha $\beta \in L$-re $f(\beta) = \alpha$ teljesül, akkor $\beta$ is transzcendens $K$ felett.

**19.** Legyenek $a$ és $b$ olyan komplex számok, amely transzcendensek $\mathbb{Q}$ felett. Igaz-e, hogy $a^b$ is transzcendens $\mathbb{Q}$ felett?

**20.** Tegyük fel, hogy $K(\alpha, \beta)|K$ olyan bővítést, ahol $\alpha \notin K$ algebrai elem $K$ felett, míg $\beta$ transzcendens. Mutassuk meg, hogy $K(\alpha, \beta)|K$ nem egyszerű.

**21.** Tegyük fel, hogy $L|K$ algebrai bővítés, és legyen $\tau\colon L \to L$ olyan injektív homomorfizmus, amelyre $\tau(\alpha) = \alpha$ teljesül tetszőleges $\alpha \in K$ esetén. Mutassuk meg, hogy $\tau$ izomorfizmus.

**22.** Tegyük fel, hogy $\alpha$ transzcendens elem $K$ felett. Mutassuk meg, hogy ha $\beta \in K(\alpha) \setminus K$, akkor $K(\alpha)|K(\beta)$ bővítés véges és $\beta$ transzcendens $K$ felett. Ha $\beta = f(\alpha)/g(\alpha)$ $(f, g \in K[x]$, ln.k.o.$(f, g) \sim 1)$, akkor $[K(\alpha) : K(\beta)] = \max(f^*, g^*)$.

**23.** Legyenek $K$ és $L$ olyan számtestek, amelyekre $[L : K] = 2$ teljesül, továbbá legyen

$$S(L) = \left\{a \in L^\times \mid a \text{ egy } L\text{-beli elem négyzete}\right\}.$$

Mutassuk meg, hogy $S(L)$ részcsoport $L^\times$-ban.[8]

**24.** Legyenek $L, L'$ és $K$ olyan számtestek, amelyekre $[L : K] = [L' : K] = 2$ teljesül. Mutassuk meg, hogy pontosan akkor van olyan $\varphi\colon L \to L'$ izomorfizmus, amely fixen hagyja $K$ elemeit, ha $S(L) = S(L')$.

**25.** 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 $p \mid a_1, \ldots, a_n$, de $p \nmid a_0$ és $p^2 \nmid a_n$, akkor $f$ irreducibilis $\mathbb{Z}$ felett.

**26.** Mutassuk meg, hogy van olyan $f \in \mathbb{Z}[x]$ irreducibilis főpolinom, hogy az $f_{\to s}$ polinomok $(s \in \mathbb{Z})$ egyikére sem alkalmazható a Schönemann–Eisenstein-tétel (3.4. Tétel).

**27.** Mutassuk meg, hogy tetszőleges $p$ prímszámra az $x^n - p$ polinom irreducibilis $\mathbb{Q}[x]$-ben.

**28.** Bizonyítsuk be, hogy $[\mathbb{A} \cap \mathbb{R} : \mathbb{Q}] = \infty$.

**29.** Legyen $H = \left\{\sqrt[p]{2} \mid p \text{ prímszám}\right\}$. Mutassuk meg, hogy ha $H'$ véges részhalmaza $H$-nak, akkor a $H'$-beli elemek lineárisan függetlenek $\mathbb{Q}$ felett.

**30.** Igazoljuk, hogy az

(a) $x^5 - 4x + 2$,

(b) $x^4 - 4x + 2$

polinomok irreducibilisek $\mathbb{Q}(i)$ felett.

**31.** Legyen $p$ tetszőleges prímszám. Mutassuk meg, hogy az $x^p + x^{p-1} + \cdots + x + 1$ polinom irreducibilis $\mathbb{Q}$ felett.

[8] Tetszőleges $L$ testre $L^\times$ jelöli a test multiplikatív csoportját, azaz $L^\times = (L \setminus \{0\}; \cdot)$.

**32.** Legyen $\vartheta = \dfrac{2\pi}{7}$. Határozzuk meg a $\cos\vartheta + i\sin\vartheta$ és a $2\cos\vartheta$ komplex számok minimálpolinomját $\mathbb{Q}$ felett.

**33.** Ha egy $n$-edfokú $f \in \mathbb{Z}[x]$ polinom ($n \geqslant 1$) legalább $2\left[\dfrac{n}{2}\right] + 1$ egész helyen $\pm 1$ értéket vesz fel, akkor $f$ irreducibilis $\mathbb{Z}$ (s így $\mathbb{Q}$) felett.

**34.** Igazoljuk, hogy az

(a) $x^5 + 9x^4 + 30x^3 + 2x + 3$,

(b) $x^n - px + p^2$ ($p$ prímszám, $n > 3$)

polinomok irreducibilisek $\mathbb{Q}$ felett.

**35.** Legyen $n$ természetes szám. Mutassuk meg, hogy a $\sum_{k=0}^{n} \dfrac{x^k}{k!} \in \mathbb{Q}[x]$ polinom irreducibilis.

**36.** Legyen $p$ prímszám és $a$ olyan egész szám, amely nem osztható $p$-vel. Mutassuk meg, hogy az $x^p - x + a$ polinom irreducibilis $\mathbb{Z}$ felett.

**37.** Legyenek $a$ és $b$ tetszőleges egész számok. Ekkor az $f = x^4 + \overline{a}x^2 + \overline{b}^2$ polinom nem irreducibilis $\mathbb{Z}_p$ felett ($p$ tetszőleges prímszám).

**38.** Legyen $g \in \mathbb{Z}[x]$ tetszőleges $k$-adfokú polinom ($k \in \mathbb{N}$), és legyenek $d_0 < d_1 < \cdots < d_k$ egészek. Igazoljuk, hogy van olyan $i \in \{0, 1, \ldots, k\}$, amelyre $|g(d_i)| \geqslant k!/2^k$.

**39.** Legyen $f \in \mathbb{Z}[x]$ tetszőleges $n$-edfokú polinom ($n \in \mathbb{N}$), és legyen $m = [(n+1)/2]$. Tegyük fel, hogy vannak olyan különböző $a_1, \ldots, a_n$ egészek, amelyekre $0 < |f(a_i)| < m!/2^m$. Ekkor az $f$ polinom irreducibilis.

**40.** Legyen $f = x^n + a_{n-1}x^{n-1} + \cdots + a_1 x + \varepsilon p \in \mathbb{Z}[x]$, ahol $\varepsilon \in \{-1, 1\}$ és $p$ prímszám. Ha $p > 1 + |a_1| + \cdots + |a_{n-1}|$, akkor $f$ irreducibilis.

**41.** Az $i\sqrt{3}$ és $1+i\sqrt{3}$ komplex számok gyökei az $f = x^- 2x^3 + 7x^2 - 6x + 12 \in \mathbb{Q}[x]$ polinomnak. Van-e olyan $\sigma$ automorfizmusa az $f$ polinom $\mathbb{Q}$ feletti felbontási testének, amelyre $\sigma(i\sqrt{3}) = 1 + i\sqrt{3}$ teljesül?

**42.** Határozzuk meg az alábbi polinomok $F \leqslant \mathbb{C}$ felbontási testét $\mathbb{Q}$ felett:

(a) $p_1 = x^4 - x^2 + 1$;

(b) $p_2 = x^6 - 2$;

(c) $p_3 = x^4 + 2$;

(d) $p_4 = x^4 + 5x^3 + 10x^2 + 10x + 5$.

**43.** Mutassuk meg, hogy az alábbi bővítések egyszerűek. Határozzuk meg a generáló elem minimálpolinomját is $\mathbb{Q}$ felett.

(a) $\mathbb{Q}(\sqrt{5}, \sqrt{10})|\mathbb{Q}$;

(b) $\mathbb{Q}(\sqrt{2}, i)|\mathbb{Q}$;

(c) $\mathbb{Q}(\sqrt{3}, i)|\mathbb{Q}$;

(d) $\mathbb{Q}(\sqrt[4]{3}, i)|\mathbb{Q}$;

(e) $\mathbb{Q}(\sqrt{2}, \sqrt{3}, \sqrt{5})|\mathbb{Q}$.

**44.** Legyen $p$ tetszőleges prímszám, és legyen $f = x^p - 2 \in \mathbb{Q}[x]$. Bizonyítsuk be, hogy ha $L$ az $f$ polinom felbontási teste $\mathbb{Q}$ felett, akkor $[L : \mathbb{Q}] = p(p-1)$.

**45.** Legyen $\varepsilon = -\frac{1}{2} + i\frac{\sqrt{3}}{2}$. Mutassuk meg, hogy $\mathbb{Q}(\varepsilon)$ felbontási teste az $x^6 - 1 \in \mathbb{Q}[x]$ polinomnak. Határozzuk meg a $\mathbb{Q}(\varepsilon)|\mathbb{Q}$ bővítés fokát.

**46.** Legyenek $L|K$ és $M|L$ testbővítések. Tegyük fel, hogy $\alpha \in M$ algebrai elem $K$ felett. Igaz-e, hogy $[L(\alpha) : L] \mid [K(\alpha) : K]$ mindig teljesül?

**47.** Legyen $f \in \mathbb{Q}[x]$. Határozzuk meg az $f$ polinom egy $L$ felbontási testét, valamint az $L|\mathbb{Q}$ bővítés fokát. Keressünk olyan $\alpha \in L$ elemet, amelyre $L = \mathbb{Q}(\alpha)$ teljesül:

(a) $f = x^4 - 5x^2 + 6$;

(b) $f = x^4 + 5x^2 + 6$;

(c) $f = x^4 - 5$.

**48.** Legyen $K$ számtest, és $f$ tetszőleges $K[x]$-beli $n$-edfokú polinom ($n \in \mathbb{N}_0$). Tegyük fel, hogy $\alpha \in K$. Mutassuk meg, hogy

$$f = f(\alpha) + \sum_{k=1}^{n} \frac{D_x^{(k)}(\alpha)}{k!}(x - \alpha)^k,$$

ahol $D_x^{(1)} = D_x$ és $D_x^{(k)} = D_x \circ D_x^{(k-1)}$ $(k \geqslant 2)$.

**49.** Tegyük fel, hogy $L|K$ Galois-bővítés, melynek Galois-csoportja $G$, és legyen $\alpha \in L$. Igazoljuk, hogy $L = K(\alpha)$ pontosan akkor teljesül, ha bármely $\sigma, \sigma' \in G$-re $\sigma \neq \sigma'$ esetén $\sigma(\alpha) \neq \sigma'(\alpha)$.

**50.** Határozzuk meg az $S_n$ $n$-edfokú szimmetrikus csoport tranzitív részcsoportjait, ha $n \in \{3, 4, 5\}$.

**51.** Legyen $K$ számtest, $f \in K[x]$. Az $f$ polinom valamely $L$ felbontási testében $f$ gyökei legyenek $\alpha_1, \ldots, \alpha_n$. Mutassuk meg, hogy

$$\Delta = \eta_n \prod_{j=1}^{n} D_x(f)(\alpha_j),$$

ahol $\eta_n = \begin{cases} 1, & \text{ha } 4 \mid n \text{ vagy } 4 \mid n-1, \\ -1, & \text{különben.} \end{cases}$

**52.** Legyen $K$ számtest, $f = x^n + px + q \in K[x]$. Az $f$ polinom valamely $L$ felbontási testében $f$ gyökei legyenek $\alpha_1, \ldots, \alpha_n$. Legyen $\lambda_k = \alpha_1^k + \cdots + \alpha_n^k$ $(k \in \mathbb{N})$. Mutassuk meg, hogy

$$\lambda_k = \begin{cases} 0, & \text{ha } 1 \leqslant k \leqslant n-2 \text{ vagy } n+1 \leqslant k \leqslant 2n-3, \\ -(n-1)p, & \text{ha } k = n-1, \\ -nq, & \text{ha } k = n, \\ (n-1)^p, & \text{ha } k = 2n-2, \end{cases}$$

és az $f$ polinom $\Delta$ diszkriminánsa:

$$\Delta = \eta_{n+1} n^n q^{n-1} - \eta_n (n-1)^{n-1} p^n,$$

ahol $\eta_n = \begin{cases} 1, & \text{ha } 4 \mid n \text{ vagy } 4 \mid n-1, \\ -1, & \text{különben.} \end{cases}$

**53.** Legyen $f = x^3 + px + q \in \mathbb{Q}[x]$, $\alpha$ az $f$ polinom gyöke valamely $\mathbb{Q}$ feletti felbontási testében. Legyen $g = 3x^2 - 3\alpha x - p \in \mathbb{Q}(\alpha)[x]$, és legyen $\beta$ a $g$ polinom gyöke valamely $\mathbb{Q}(\alpha)$ feletti felbontási testében. Mutassuk meg, hogy $\beta$ gyöke az $27x^6 + 27q^3 - p^3 \in \mathbb{Q}[x]$ polinomnak, valamint $\alpha = \beta - \dfrac{p}{3\beta}$, ahol $\beta = -\frac{q}{2} + \delta$ és $\delta^2 = \dfrac{q^2}{4} + \dfrac{p^3}{27}$.

**54.** Mutassuk meg, hogy $S_4$ tranzitív részcsoportjai a következők: $S_4$, $A_4$, $V$ (Viergruppe), $D_4$ és a 4-rendű ciklikus részcsoportok.

**55.** Legyen az $x^3 - 7 \in \mathbb{Q}[x]$ polinom felbontási teste $\mathbb{Q}$ felett $F$. Mutassuk meg, hogy $\mathrm{Gal}_{\mathbb{Q}}(x^3 - 7) \cong S_3$, és határozzuk meg az $F|\mathbb{Q}$ bővítés közbülső testeit.

**56.** Határozzuk meg az $x^5 - 2 \in \mathbb{Q}[x]$ polinom $G$ Galois-csoportját $Q$ felett. Döntsük el, hogy $G$ Abel-csoport-e, illetve feloldható-e.

**57.** Határozzuk meg az alábbi $\mathbb{Q}[x]$-beli polinomok Galois-csoportját $\mathbb{Q}$ felett.

(a) $x^4 + 4x + 2$;

(b) $x^4 + 8x - 12$;

(c) $x^4 + 1$;

(d) $x^4 + x^3 + x^2 + x + 1$;

(e) $x^4 - 2$.

**58.** Tetszőleges $n$ természetes számra legyen

$$P_n = \left\{ \varepsilon \in \mathbb{C} \mid \varepsilon^n = 1 \text{ és } \varepsilon^k \neq 1 \ (1 \leqslant k < n) \right\}.$$

Mutassuk meg az alábbiakat.

(a) Tetszőleges $\omega \in \mathbb{C}$-re $\omega \in P_n$ pontosan akkor teljesül, ha $\omega = \cos \dfrac{2k\pi}{n} + i \sin \dfrac{2k\pi}{n}$, ahol ln.k.o.$(k, n) = 1$.

(b) $|P_n| = \varphi(n)$, ahol $\varphi$ az Euler-féle függvény.

(c) $\prod_{\varepsilon \in P_n} \varepsilon = 1$, ha $n \geqslant 3$.

(d) $\sum_{\varepsilon \in P_n} \varepsilon = \mu(n)$, ahol $\mu$ a Möbius-függvény.

**59.** Tetszőleges $n$ természetes számra legyen

$$\chi_n = \prod_{\varepsilon \in P_n} (x - \varepsilon).$$

A $\chi_n$ polinomot az $n$-edik körosztási polinomnak nevezzük.

(a) Írjuk fel a $\chi_n$ polinomokat $n \in \{1, 2, 3, 4, 5, 6\}$ esetén.

(b) Mutassuk meg, hogy $\prod_{d|n} \chi_d = x^n - 1$.

(c) Igazoljuk, hogy $\chi_n \in \mathbb{Z}[x]$.

(d) Bizonyítsuk be, hogy tetszőleges $n > 1$ páratlan számra és tetszőleges $z$ komplex számra $\chi_{2n}(z) = \chi_n(-z)$ teljesül.

(e) Mutassuk meg, hogy tetszőleges $p$ prímszámra a $\chi_p$ polinom irreducibilis $\mathbb{Q}$ felett.

(f) Mutassuk meg, hogy tetszőleges $n$ természetes számra a $\chi_n$ polinom irreducibilis $\mathbb{Q}$ felett.

**60.** Az alábbi szerkesztési feladatok mindegyikében határozzuk meg a szerkesztés $K$ alaptestét, a szerkesztendő szám által generált bővítés fokát $K$ felett, és döntsük el, hogy a szerkesztés elvégezhető-e.

(a) Adott az egységszakasz, szerkesztendő $\alpha = \sqrt[5]{2}$.

(b) Adott az egységszakasz, szerkesztendő $\alpha = \sqrt[4]{2}$.

(c) Adott az egységszakasz és egy $\sqrt[3]{2}$ hosszú szakasz, szerkesztendő $\alpha = \sqrt[6]{2}$.

(d) Adott az egységszakasz és egy $\sqrt[3]{2}$ hosszú szakasz, szerkesztendő $\alpha = \sqrt[5]{2}$.

(e) Adott $(0, 0)$, $(0, 1)$, $(0, \pi)$, az egységsugarú kört kell négyszögesíteni,

(f) Adott egy szabályos 9-szög, szerkesztendő egy szabályos 18-szög

**61.** Szerkeszthető-e a háromszög két oldalából, és az egyikhez tartozó szögfelezőből? (A szakaszok hossza adott.)

**62.** Mutassuk meg, hogy nem szerkeszthető egyenlő szárú háromszög a szárából és a beírt kör sugarából.

**63.** Mely $n$ egészekre szerkeszthető $n$-fokos szög.

**64.** Határozzuk meg $\cos \dfrac{2\pi}{n}$ fokát $\mathbb{Q}$ felett.

# 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).