Algebra3, alkalmazott matematikus

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
http://ewkiss.web.elte.hu/wp/wordpress
ewwkiss@gmail.com

8/11. előadás

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés,

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}$,

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek. Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}),$

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$.

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$.

$1, \sqrt{2}$ bázis L-ben K fölött

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$.
$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3}).$

$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).

$1, \sqrt{3}$ bázis M-ben L fölött

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$.
$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).
$1, \sqrt{3}$ bázis M-ben L fölött (mert $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: HF).

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \le L \le M$ testbővítések, akkor $K \le M$ pontosan akkor véges bővítés, ha $K \le L$ és $L \le M$ mindketten végesek.
Ilyenkor $|M:K| = |M:L| \cdot |L:K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}$, $\quad L = \mathbb{Q}(\sqrt{2})$, $\quad M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$.
$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).
$1, \sqrt{3}$ bázis M-ben L fölött (mert $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: HF).
Láttuk: az $M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$ általános eleme felírható
$\alpha + \gamma\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alakban,

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek. Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}, \quad L = \mathbb{Q}(\sqrt{2}), \quad M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$.

$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).

$1, \sqrt{3}$ bázis M-ben L fölött (mert $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: HF).

Láttuk: az $M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$ általános eleme felírható

$\alpha + \gamma\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alakban,

ahol $\alpha = a + b\sqrt{2}$

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \leq L \leq M$ testbővítések, akkor $K \leq M$ pontosan akkor véges bővítés, ha $K \leq L$ és $L \leq M$ mindketten végesek.
Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}$, $\quad L = \mathbb{Q}(\sqrt{2})$, $\quad M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$.
$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).
$1, \sqrt{3}$ bázis M-ben L fölött (mert $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: HF).
Láttuk: az $M = \left(\mathbb{Q}(\sqrt{2})\right)(\sqrt{3})$ általános eleme felírható
$\alpha + \gamma\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alakban,
ahol $\alpha = a + b\sqrt{2}$ és $\gamma = c + d\sqrt{3}$.

A szorzástétel

Tétel (6.2.3. Következmény)

Ha $K \le L \le M$ testbővítések, akkor $K \le M$ pontosan akkor véges bővítés, ha $K \le L$ és $L \le M$ mindketten végesek. Ilyenkor $|M : K| = |M : L| \cdot |L : K|$.

A bizonyítás gondolata egy példán

$K = \mathbb{Q}$, $\quad L = \mathbb{Q}(\sqrt{2})$, $\quad M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$.
$1, \sqrt{2}$ bázis L-ben K fölött (mert $\sqrt{2} \notin \mathbb{Q}$).
$1, \sqrt{3}$ bázis M-ben L fölött (mert $\sqrt{3} \notin \mathbb{Q}(\sqrt{2})$: HF).
Láttuk: az $M = \big(\mathbb{Q}(\sqrt{2})\big)(\sqrt{3})$ általános eleme felírható
$\alpha + \gamma\sqrt{3} = a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}$ alakban,
ahol $\alpha = a + b\sqrt{2}$ és $\gamma = c + d\sqrt{3}$.
Ekkor $1, \sqrt{2}, \sqrt{3}, \sqrt{2}\sqrt{3} = \sqrt{6}$ bázis lesz az $L \le M$ bővítésben.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \dots, u_m$ bázis M-ben L fölött, $v_1, \dots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \dots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \dots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \dots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A szorzástétel bizonyítása

Legyenek $K \le L \le M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött, mindegyik $\alpha_i = 0$.

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött, mindegyik $\alpha_i = 0$.
Mivel $v_1, \ldots, v_n$ független K fölött,

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött, mindegyik $\alpha_i = 0$.
Mivel $v_1, \ldots, v_n$ független K fölött, $a_{ij} = 0$ minden i, j-re.

A szorzástétel bizonyítása

Legyenek $K \le L \le M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött, mindegyik $\alpha_i = 0$.
Mivel $v_1, \ldots, v_n$ független K fölött, $a_{ij} = 0$ minden i, j-re.
Ezért $v_i u_j$ tényleg független rendszer. $\square$

A szorzástétel bizonyítása

Legyenek $K \leq L \leq M$ testbővítések,
$u_1, \ldots, u_m$ bázis M-ben L fölött, $v_1, \ldots, v_n$ bázis L-ben K fölött.
Elég belátni: az nm darab $v_i u_j$ szorzat bázis M-ben K fölött.

M elemei $\alpha_1 u_1 + \ldots + \alpha_m u_m$ alakúak, ahol $\alpha_1, \ldots, \alpha_m \in L$.
Mindegyik $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$, ahol $a_{ij} \in K$.
Behelyettesítve $\sum a_{ij} v_i u_j$ adódik, így $v_i u_j$ generátorrendszer.

A függetlenséghez tegyük föl, hogy $\sum a_{ij} v_i u_j = 0$.
Legyen $\alpha_i = a_{i1} v_1 + \ldots + a_{in} v_n$. Ekkor $\alpha_1 u_1 + \ldots + \alpha_m u_m = 0$.
Mivel $u_1, \ldots, u_m$ független L fölött, mindegyik $\alpha_i = 0$.
Mivel $v_1, \ldots, v_n$ független K fölött, $a_{ij} = 0$ minden i, j-re.
Ezért $v_i u_j$ tényleg független rendszer. $\square$

A bővítések végességéről szóló állítás HF.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:

Ha $K \leq L$ véges bővítés és $\alpha \in L$,

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött,

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós,

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges. Így α algebrai K fölött,

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött,
és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós,
ezért $|K(\alpha) : K|$ véges. Így α algebrai K fölött,
és $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges. Így α algebrai K fölött, és $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$. A szorzástételt alkalmazzuk a

$$K \leq K(\alpha) \leq L$$

testláncra.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges. Így α algebrai K fölött, és $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$. A szorzástételt alkalmazzuk a

$$K \leq K(\alpha) \leq L$$

testláncra. Azt kapjuk, hogy $|L : K| = |L : K(\alpha)| \cdot \mathrm{gr}_K(\alpha)$.

A szorzástétel első következménye

6.2.4. Állítás

Elem foka osztója a bővítés fokának. Pontosabban:
Ha $K \leq L$ véges bővítés és $\alpha \in L$, akkor α algebrai K fölött, és $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak.

Bizonyítás

Mivel $\alpha \in L$, a generált résztest definíciója miatt $K(\alpha) \subseteq L$.
Véges dimenziós vektortér altere is véges dimenziós, ezért $|K(\alpha) : K|$ véges. Így α algebrai K fölött, és $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$. A szorzástételt alkalmazzuk a

$$K \leq K(\alpha) \leq L$$

testláncra. Azt kapjuk, hogy $|L : K| = |L : K(\alpha)| \cdot \mathrm{gr}_K(\alpha)$.
Ezért $\mathrm{gr}_K(\alpha)$ osztója $|L : K|$-nak. $\square$

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$. Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$. Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$,

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött,

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,
és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,
és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$.

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,|$-nak.

.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött, és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,|$-nak.
Ezért $7 \mid 6k$, .

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,
és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}|$-nak.
Ezért $7 \mid 6k$, ahonnan $(7, 6) = 1$ miatt $7 \mid k$.

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,
és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,|$-nak.
Ezért $7 \mid 6k$, ahonnan $(7, 6) = 1$ miatt $7 \mid k$.
Így $k = 7$,

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,
és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,|$-nak.
Ezért $7 \mid 6k$, ahonnan $(7, 6) = 1$ miatt $7 \mid k$.
Így $k = 7$, és az is kijött, hogy $x^7 - 7 = m(x)$,

Példa a szorzástétel alkalmazására

Határozzuk meg $\sqrt[7]{6}$ fokát $\mathbb{Q}(\sqrt[6]{7})$ fölött.

$x^7 - 6$ a Schönemann-Eisenstein miatt irreducibilis $\mathbb{Q}$ fölött,
és ezért ez a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}$ fölött. Így $\mathrm{gr}_{\mathbb{Q}}(\sqrt[7]{6}) = 7$.
Hasonlóan $\mathrm{gr}_{\mathbb{Q}}(\sqrt[6]{7}) = 6$ és $|\,\mathbb{Q}(\sqrt[6]{7}) : \mathbb{Q}\,| = 6$.
Legyen $m(x)$ a $\sqrt[7]{6}$ minimálpolinomja $\mathbb{Q}(\sqrt[6]{7})$ fölött.
Mivel $x^7 - 6 \in \mathbb{Q}(\sqrt[6]{7})[x]$-nek gyöke $\sqrt[7]{6}$, ezért $m(x) \mid x^7 - 6$.
Legyen $k = \mathrm{gr}(m)$ a $\sqrt[7]{6}$ foka $\mathbb{Q}(\sqrt[6]{7})$ fölött, ekkor $k \leq 7$.
$\mathbb{Q} \leq \mathbb{Q}(\sqrt[6]{7}) \leq \mathbb{Q}(\sqrt[6]{7})(\sqrt[7]{6})$ miatt $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,| = 6k$.
De $\sqrt[7]{6} \in \mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6})$ miatt 7 osztója $|\,\mathbb{Q}(\sqrt[6]{7}, \sqrt[7]{6}) : \mathbb{Q}\,|$-nak.
Ezért $7 \mid 6k$, ahonnan $(7,6) = 1$ miatt $7 \mid k$.
Így $k = 7$, és az is kijött, hogy $x^7 - 7 = m(x)$,
vagyis $x^7 - 6$ irreducibilis $\mathbb{Q}(\sqrt[6]{7})$ fölött.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges,

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.

A $K \leq L$ véges bővítés, ha $|L : K|$ véges.

Ekkor L minden eleme algebrai K fölött.

A $K \leq L$ algebrai bővítés, ha L minden eleme algebrai K fölött.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.
A $K \leq L$ algebrai bővítés, ha L minden eleme algebrai K fölött.
Tehát minden véges bővítés algebrai.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.
A $K \leq L$ algebrai bővítés, ha L minden eleme algebrai K fölött.
Tehát minden véges bővítés algebrai.

6.2.12. Tétel

Az L-nek a K fölött algebrai elemei résztestet alkotnak.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.
A $K \leq L$ algebrai bővítés, ha L minden eleme algebrai K fölött.
Tehát minden véges bővítés algebrai.

6.2.12. Tétel

Az L-nek a K fölött algebrai elemei résztestet alkotnak.

Speciálisan az algebrai számok $\mathbb{A}$ halmaza résztest $\mathbb{C}$-ben.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \le L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \le L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.
A $K \le L$ algebrai bővítés, ha L minden eleme algebrai K fölött.
Tehát minden véges bővítés algebrai.

6.2.12. Tétel

Az L-nek a K fölött algebrai elemei résztestet alkotnak.

Speciálisan az algebrai számok $\mathbb{A}$ halmaza résztest $\mathbb{C}$-ben.
Ez tehát az algebrai számok teste.

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.
A $K \leq L$ algebrai bővítés, ha L minden eleme algebrai K fölött.
Tehát minden véges bővítés algebrai.

6.2.12. Tétel

Az L-nek a K fölött algebrai elemei résztestet alkotnak.

Speciálisan az algebrai számok $\mathbb{A}$ halmaza résztest $\mathbb{C}$-ben.
Ez tehát az algebrai számok teste.
A $\mathbb{Q} \leq \mathbb{A}$ bővítés algebrai (nyilván),

Véges és algebrai bővítés

Ismétlés (6.1.20, 6.2.4, 6.1.11)

Legyen $K \leq L$ testbővítés, $\alpha \in L$. Ekkor $\mathrm{gr}_K(\alpha) = |K(\alpha) : K|$ akkor és csak akkor véges, ha α algebrai K fölött.
A $K \leq L$ véges bővítés, ha $|L : K|$ véges.
Ekkor L minden eleme algebrai K fölött.
A $K \leq L$ algebrai bővítés, ha L minden eleme algebrai K fölött.
Tehát minden véges bővítés algebrai.

6.2.12. Tétel

Az L-nek a K fölött algebrai elemei résztestet alkotnak.

Speciálisan az algebrai számok $\mathbb{A}$ halmaza résztest $\mathbb{C}$-ben.
Ez tehát az algebrai számok teste.
A $\mathbb{Q} \leq \mathbb{A}$ bővítés algebrai (nyilván), de nem véges (HF).

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$,

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$.

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$.
Ekkor $\sqrt[k]{\alpha}$ gyöke

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$. Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. □

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$. Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. □

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$.
Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. $\square$

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.
Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$.
Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. $\square$

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.
Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az α minimálpolinomja K, illetve L fölött,

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$. Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. $\square$

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.
Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az α minimálpolinomja K, illetve L fölött, akkor

$$t \mid s.$$

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$.
Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. $\square$

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.
Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az α minimálpolinomja K, illetve L fölött,
akkor $s \in L[x]$ $t \mid s$.

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$. Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. $\square$

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.
Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az α minimálpolinomja K, illetve L fölött, akkor $s \in L[x]$ és $s(\alpha) = 0$ miatt $t \mid s$.

Fok bővebb test fölött

6.2.5. Állítás

Algebrai elem k-adik gyöke is algebrai.

Legyen $K \leq L$, $\alpha \in L$ és $0 \neq s(x) \in K[x]$, melyre $s(\alpha) = 0$.
Ekkor $\sqrt[k]{\alpha}$ gyöke az $s(x^k) \in K[x]$ nem nulla polinomnak. $\square$

6.2.8. Lemma

Elem foka nagyobb test fölött nem nőhet.
Vagyis $K \leq L \leq M$, $\alpha \in M$ esetén $\mathrm{gr}_L(\alpha) \leq \mathrm{gr}_K(\alpha)$.

Ha $s(x)$, illetve $t(x)$ az α minimálpolinomja K, illetve L fölött,
akkor $s \in L[x]$ és $s(\alpha) = 0$ miatt $t \mid s$.
Így $\mathrm{gr}_L(\alpha) = \mathrm{gr}(t) \leq \mathrm{gr}(s) = \mathrm{gr}_K(\alpha)$. $\square$

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$,

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött, és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \leq K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \leq \mathrm{gr}_K(\beta)$.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött. Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött, és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt $|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \leq K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \leq \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \le L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \le K(\alpha) \le K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \le K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \le \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \le \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.
De $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$,

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \leq K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \leq \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.
De $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$, így fokuk $\leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$. $\square$

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \le L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \le K(\alpha) \le K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \le K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \le \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \le \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.
De $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$, így fokuk $\le \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$. $\square$

Így például $\sqrt[7]{3 - \sqrt[5]{23}} - \sqrt[4]{5 + i\sqrt{7 + \sqrt[6]{3}}}$ is algebrai szám.

Összeg és szorzat foka

6.2.10. Következmény

Legyen $K \leq L$ testbővítés, $\alpha, \beta \in L$ algebrai K fölött.
Ekkor $\alpha \pm \beta$, $\alpha\beta$ és $\beta \neq 0$ esetén α/β is algebrai K fölött,
és fokuk legfeljebb $\mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.

Bizonyítás

$K \leq K(\alpha) \leq K(\alpha)(\beta)$ testlánc. A szorzástétel miatt
$|K(\alpha)(\beta) : K| = \mathrm{gr}_K(\alpha)\mathrm{gr}_{K(\alpha)}(\beta)$.
Láttuk, hogy $K \leq K(\alpha)$ miatt $\mathrm{gr}_{K(\alpha)}(\beta) \leq \mathrm{gr}_K(\beta)$.
Ezért $|K(\alpha)(\beta) : K| \leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$.
De $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in K(\alpha)(\beta)$, így fokuk $\leq \mathrm{gr}_K(\alpha)\mathrm{gr}_K(\beta)$. $\square$

Így például $\sqrt[7]{3 - \sqrt[5]{23}} - \sqrt[4]{5 + i\sqrt{7 + \sqrt[6]{3}}}$ is algebrai szám.
Foka legfeljebb $7 \cdot 5 \cdot 4 \cdot 2 \cdot 2 \cdot 6$.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt,

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.
Sem a $\mathbb{Q}$ véges bővítései,

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.
Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.
Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak.

6.4.6, NB

Minden testnek van algebrailag zárt bővítése.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.
Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak.

6.4.6, NB

Minden testnek van algebrailag zárt bővítése.

Ezért minden polinomnak számolhatunk formálisan a gyökeivel!

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.
Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak.

6.4.6, NB

Minden testnek van algebrailag zárt bővítése.

Ezért minden polinomnak számolhatunk formálisan a gyökeivel!
Ez az algebrailag zárt bővítés analízis nélkül is megkonstruálható.

Algebrailag zárt testek

Emlékeztető (2.5.3. Definíció)

Egy T test algebrailag zárt, ha minden nem konstans polinom gyöktényezőkre bomlik T fölött.

2.5.4, 2.5.18, 6.2.20, HF

Tudjuk analízisből, hogy $\mathbb{C}$ algebrailag zárt.
Sem a $\mathbb{Q}$ véges bővítései, sem a véges testek nem algebrailag zártak.

6.4.6, NB

Minden testnek van algebrailag zárt bővítése.

Ezért minden polinomnak számolhatunk formálisan a gyökeivel!
Ez az algebrailag zárt bővítés analízis nélkül is megkonstruálható.
Halmazelméleti (transzfinit) módszereket igényel.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám. Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is. Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1x + \ldots + a_kx^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám. Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is. Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$,

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$
és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben
véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.
Beláttuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének,

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1x + \ldots + a_kx^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.
Belláttuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének, így algebrai szám.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$
és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben
véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.
Beláttuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének, így algebrai szám.
Tehát minden $f \in \mathbb{A}[x]$ komplex gyökei algebrai számok.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1x + \ldots + a_kx^k \in \mathbb{A}[x]$
és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben
véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.
Belátuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének, így algebrai szám.
Tehát minden $f \in \mathbb{A}[x]$ komplex gyökei algebrai számok.
Mivel $\mathbb{C}$ algebrailag zárt, f gyöktényezőkre bomlik $\mathbb{C}$ fölött.

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1x + \ldots + a_kx^k \in \mathbb{A}[x]$
és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben
véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.
Beláttuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének, így algebrai szám.
Tehát minden $f \in \mathbb{A}[x]$ komplex gyökei algebrai számok.
Mivel $\mathbb{C}$ algebrailag zárt, f gyöktényezőkre bomlik $\mathbb{C}$ fölött.
De minden gyöke $\mathbb{A}$-beli, és így $\mathbb{A}$ fölött is. $\square$

$\mathbb{A}$ algebrailag zárt

6.2.13. Tétel

Az algebrai számok $\mathbb{A}$ teste algebrailag zárt.

Bizonyítás: Legyen $0 \neq f(x) = a_0 + a_1 x + \ldots + a_k x^k \in \mathbb{A}[x]$ és $\alpha \in \mathbb{C}$ gyöke f-nek. Belátjuk, hogy α algebrai szám.
Mivel a_j algebrai $\mathbb{Q}$ fölött, algebrai minden bővebb test fölött is.
Ezért az a_j elemekkel sorban bővítve mindegyik lépésben véges bővítést kapunk. Így $|\mathbb{Q}(a_0, \ldots, a_k) : \mathbb{Q}|$ véges.
De $f(x) \in \mathbb{Q}(a_0, \ldots, a_k)[x]$, ezért α algebrai $\mathbb{Q}(a_0, \ldots, a_k)$ fölött.
Tehát $|\mathbb{Q}(a_0, \ldots, a_k)(\alpha) : \mathbb{Q}|$ is véges.
Beláttuk, hogy α eleme $\mathbb{Q}$ egy véges bővítésének, így algebrai szám.
Tehát minden $f \in \mathbb{A}[x]$ komplex gyökei algebrai számok.
Mivel $\mathbb{C}$ algebrailag zárt, f gyöktényezőkre bomlik $\mathbb{C}$ fölött.
De minden gyöke $\mathbb{A}$-beli, és így $\mathbb{A}$ fölött is. $\square$

A bizonyításban kihasználtuk, hogy $\mathbb{C}$ algebrailag zárt!

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg,

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály,

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes” gyökével bővíteni.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$,

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.
Ezért az „összes" gyök helyett gyöktényezős alakról beszélünk.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.
Ezért az „összes" gyök helyett gyöktényezős alakról beszélünk.

6.3.2. Definíció

Legyen $K \leq L$ testbővítés, ahol L tartalmazza $0 \neq f \in K[x]$ összes gyökét:

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes” gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.
Ezért az „összes” gyök helyett gyöktényezős alakról beszélünk.

6.3.2. Definíció

Legyen $K \leq L$ testbővítés, ahol L tartalmazza $0 \neq f \in K[x]$ összes gyökét: $f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$,

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.
Ezért az „összes" gyök helyett gyöktényezős alakról beszélünk.

6.3.2. Definíció

Legyen $K \leq L$ testbővítés, ahol L tartalmazza $0 \neq f \in K[x]$ összes gyökét: $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$, ahol $\alpha_i \in L$

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes” gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.
Ezért az „összes” gyök helyett gyöktényezős alakról beszélünk.

6.3.2. Definíció

Legyen $K \leq L$ testbővítés, ahol L tartalmazza $0 \neq f \in K[x]$ összes gyökét: $f(x) = c(x - \alpha_1)\dots(x - \alpha_n)$, ahol $\alpha_i \in L$ és $c \in K$.

Felbontási test

Ismétlés

Legyen K test és $f \in K[x]$ irreducibilis polinom.
Ekkor van olyan $L \supseteq K$ test, melyben f-nek van egy α gyöke.
Az L-et a $K[x]/(f)$ faktorgyűrűként kaptuk meg, ekkor $L = K(\alpha)$.
α az $x + (f)$ mellékosztály, és $k \in K$-t azonosítottuk $k + (f)$-fel.

Szeretnénk f „összes" gyökével bővíteni. Ez értelmetlen:
például $x^2 + 1$ gyökei nemcsak $\pm i$, hanem sok mátrix is.
Ezért az „összes" gyök helyett gyöktényezős alakról beszélünk.

6.3.2. Definíció

Legyen $K \leq L$ testbővítés, ahol L tartalmazza $0 \neq f \in K[x]$ összes gyökét: $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$, ahol $\alpha_i \in L$ és $c \in K$.
Ekkor $K(\alpha_1, \ldots, \alpha_n)$ az f polinom felbontási teste K fölött.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló:

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke. Legyen $f(x) = (x - \alpha_1)g(x)$, ahol $g \in L_1[x]$.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke. Legyen $f(x) = (x - \alpha_1)g(x)$, ahol $g \in L_1[x]$. Van $L_1 \subseteq L_2$ bővítés, melyben g-nek van gyöke.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke. Legyen $f(x) = (x - \alpha_1)g(x)$, ahol $g \in L_1[x]$. Van $L_1 \subseteq L_2$ bővítés, melyben g-nek van gyöke. Legfeljebb $\mathrm{gr}(f)$ lépésben egy olyan $K \leq L$ bővítést kapunk, amelyben f már gyöktényezőkre bomlik.

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke. Legyen $f(x) = (x - \alpha_1)g(x)$, ahol $g \in L_1[x]$. Van $L_1 \subseteq L_2$ bővítés, melyben g-nek van gyöke. Legfeljebb $\mathrm{gr}(f)$ lépésben egy olyan $K \leq L$ bővítést kapunk, amelyben f már gyöktényezőkre bomlik.
Ebben az f gyökei és a K által generált résztest megfelelő lesz. $\square$

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke. Legyen $f(x) = (x - \alpha_1)g(x)$, ahol $g \in L_1[x]$. Van $L_1 \subseteq L_2$ bővítés, melyben g-nek van gyöke. Legfeljebb $\mathrm{gr}(f)$ lépésben egy olyan $K \leq L$ bővítést kapunk, amelyben f már gyöktényezőkre bomlik.
Ebben az f gyökei és a K által generált résztest megfelelő lesz. $\square$

Ha ezt végtelen sok lépésben (azaz transzfinit módon) elvégezzük sorban minden polinomra,

Felbontási test létezése

6.4.5. Következmény

Minden nem nulla polinomnak van felbontási teste.

Ha az alaptest $\mathbb{C}$-nek részteste, akkor ez nyilvánvaló: bővíthetünk a polinom összes komplex gyökével.

Bizonyítás

Ha $0 \neq f \in K[x]$, akkor van olyan $K \leq L_1$ bővítés, melyben f-nek van egy α_1 gyöke. Legyen $f(x) = (x - \alpha_1)g(x)$, ahol $g \in L_1[x]$. Van $L_1 \subseteq L_2$ bővítés, melyben g-nek van gyöke. Legfeljebb $\mathrm{gr}(f)$ lépésben egy olyan $K \leq L$ bővítést kapunk, amelyben f már gyöktényezőkre bomlik.
Ebben az f gyökei és a K által generált résztest megfelelő lesz. $\square$

Ha ezt végtelen sok lépésben (azaz transzfinit módon) elvégezzük sorban minden polinomra, akkor algebrailag zárt testet kapunk.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött,

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött,

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ és $L = K(\alpha_1, \ldots, \alpha_n)$.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött,
akkor bármely $g \in K[x]$ irreducibilis polinom vagy
gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ és $L = K(\alpha_1, \ldots, \alpha_n)$.
Ekkor L elemei $p(\alpha_1, \ldots, \alpha_n)$ alakúak, ahol $p \in K[x_1, \ldots, x_n]$.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ és $L = K(\alpha_1, \ldots, \alpha_n)$.
Ekkor L elemei $p(\alpha_1, \ldots, \alpha_n)$ alakúak, ahol $p \in K[x_1, \ldots, x_n]$.
Legyen $\beta \in L$ gyöke g-nek, $\beta = p(\alpha_1, \ldots, \alpha_n)$.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ és $L = K(\alpha_1, \ldots, \alpha_n)$.
Ekkor L elemei $p(\alpha_1, \ldots, \alpha_n)$ alakúak, ahol $p \in K[x_1, \ldots, x_n]$.
Legyen $\beta \in L$ gyöke g-nek, $\beta = p(\alpha_1, \ldots, \alpha_n)$.
Belátjuk, hogy g összes gyökét megkaphatjuk úgy, hogy p-be $\alpha_1, \ldots, \alpha_n$-et alkalmas sorrendben írjuk be.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$ és $L = K(\alpha_1, \dots, \alpha_n)$.
Ekkor L elemei $p(\alpha_1, \dots, \alpha_n)$ alakúak, ahol $p \in K[x_1, \dots, x_n]$.
Legyen $\beta \in L$ gyöke g-nek, $\beta = p(\alpha_1, \dots, \alpha_n)$.
Belátjuk, hogy g összes gyökét megkaphatjuk úgy, hogy p-be $\alpha_1, \dots, \alpha_n$-et alkalmas sorrendben írjuk be. Ha $\sigma \in S_n$, akkor legyen $\alpha_\sigma = p(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \dots (x - \alpha_n)$ és $L = K(\alpha_1, \dots, \alpha_n)$.
Ekkor L elemei $p(\alpha_1, \dots, \alpha_n)$ alakúak, ahol $p \in K[x_1, \dots, x_n]$.
Legyen $\beta \in L$ gyöke g-nek, $\beta = p(\alpha_1, \dots, \alpha_n)$.
Belátjuk, hogy g összes gyökét megkaphatjuk úgy, hogy p-be $\alpha_1, \dots, \alpha_n$-et alkalmas sorrendben írjuk be. Ha $\sigma \in S_n$, akkor legyen $\alpha_\sigma = p(\alpha_{\sigma(1)}, \dots, \alpha_{\sigma(n)})$ és $h(x) = \prod_{\sigma \in S_n} (x - \alpha_\sigma)$.

A felbontási test meglepő tulajdonsága

6.3.4. Tétel

Ha $K \leq L$ egy $f \in K[x]$ felbontási teste L fölött, akkor bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Bizonyítás

Legyen $f(x) = c(x - \alpha_1) \ldots (x - \alpha_n)$ és $L = K(\alpha_1, \ldots, \alpha_n)$.
Ekkor L elemei $p(\alpha_1, \ldots, \alpha_n)$ alakúak, ahol $p \in K[x_1, \ldots, x_n]$.
Legyen $\beta \in L$ gyöke g-nek, $\beta = p(\alpha_1, \ldots, \alpha_n)$.
Belátjuk, hogy g összes gyökét megkaphatjuk úgy, hogy p-be $\alpha_1, \ldots, \alpha_n$-et alkalmas sorrendben írjuk be. Ha $\sigma \in S_n$, akkor legyen $\alpha_\sigma = p(\alpha_{\sigma(1)}, \ldots, \alpha_{\sigma(n)})$ és $h(x) = \prod_{\sigma \in S_n} (x - \alpha_\sigma)$.
Az Algebra1-ben tanult (de nem bizonyított) szimmetrikus polinomok alaptétele (2.7.3. Tétel) miatt $h \in K[x]$.

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja,

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás),

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás), és ezért $g \mid h$.

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás), és ezért $g \mid h$.
Mivel h gyöktényezőkre bomlik L fölött, ezért g is. $\square$

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás), és ezért $g \mid h$.
Mivel h gyöktényezőkre bomlik L fölött, ezért g is. $\square$

6.3.5. Definíció

A $K \leq L$ algebrai bővítés normális,

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás), és ezért $g \mid h$.
Mivel h gyöktényezőkre bomlik L fölött, ezért g is. □

6.3.5. Definíció

A $K \leq L$ algebrai bővítés **normális**, ha bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött,

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás), és ezért $g \mid h$.
Mivel h gyöktényezőkre bomlik L fölött, ezért g is. $\square$

6.3.5. Definíció

A $K \leq L$ algebrai bővítés **normális**, ha bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

A bizonyítás folytatása

A gyökök és együtthatók összefüggése miatt h minden együtthatója $\alpha_1, \ldots, \alpha_n$ szimmetrikus polinomja, és ezért az elemi szimmetrikus polinomokkal, azaz f együtthatóival kifejezhető
(a részletesebb magyarázatot lásd a könyvben).
Mivel g irreducibilis, β minimálpolinomja g (normálva).
De $h(\beta) = 0$ (legyen σ az identitás), és ezért $g \mid h$.
Mivel h gyöktényezőkre bomlik L fölött, ezért g is. □

6.3.5. Definíció

A $K \leq L$ algebrai bővítés **normális**, ha bármely $g \in K[x]$ irreducibilis polinom vagy gyöktényezőkre bomlik L fölött, vagy egyáltalán nincs gyöke L-ben.

Így minden nem nulla polinom felbontási teste normális bővítést eredményez.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L:K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L:K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális,

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert $x^3 - 2$-nek egy gyöke van benne.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert $x^3 - 2$-nek egy gyöke van benne.

6.3.7. Feladat

Ha $K \leq L$ véges és normális, akkor egy polinom felbontási teste.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert $x^3 - 2$-nek egy gyöke van benne.

6.3.7. Feladat

Ha $K \leq L$ véges és normális, akkor egy polinom felbontási teste.

Útmutatás: Ha $\alpha \in L$, akkor m_α összes gyöke L-ben van.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert $x^3 - 2$-nek egy gyöke van benne.

6.3.7. Feladat

Ha $K \leq L$ véges és normális, akkor egy polinom felbontási teste.

Útmutatás: Ha $\alpha \in L$, akkor m_α összes gyöke L-ben van.
Bővítsük ezekkel K-t.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L:K|=2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x)=x^2+ax+b$, akkor m_α másik gyöke $-a-\alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert x^3-2-nek egy gyöke van benne.

6.3.7. Feladat

Ha $K \leq L$ véges és normális, akkor egy polinom felbontási teste.

Útmutatás: Ha $\alpha \in L$, akkor m_α összes gyöke L-ben van.
Bővítsük ezekkel K-t. Ha ez még nem L, akkor ismételjük az eljárást.

Példák normális és nem normális bővítésre

6.3.15. Feladat

Minden másodfokú bővítés normális.

Valóban, ha $|L : K| = 2$, akkor legyen $\alpha \in L$, $\alpha \notin K$.
Ha $m_\alpha(x) = x^2 + ax + b$, akkor m_α másik gyöke $-a - \alpha \in L$.
Ezért L az m_α felbontási teste.

$\mathbb{Q} \leq \mathbb{Q}(\sqrt[3]{2})$ nem normális, mert $x^3 - 2$-nek egy gyöke van benne.

6.3.7. Feladat

Ha $K \leq L$ véges és normális, akkor egy polinom felbontási teste.

Útmutatás: Ha $\alpha \in L$, akkor m_α összes gyöke L-ben van.
Bővítsük ezekkel K-t. Ha ez még nem L, akkor ismételjük az eljárást. A kapott polinomok szorzatának L felbontási teste lesz.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste,

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$,

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus,

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, melyre $\psi(\alpha) = \beta$

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, melyre $\psi(\alpha) = \beta$ és $\psi(k) = k$ minden $k \in K$ esetén.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, melyre $\psi(\alpha) = \beta$ és $\psi(k) = k$ minden $k \in K$ esetén.

Valóban, $K(\alpha) \cong K[x]/(f) \cong K(\beta)$.

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \le L$ és $K \le N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \le L$ és $K \le N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, melyre $\psi(\alpha) = \beta$ és $\psi(k) = k$ minden $k \in K$ esetén.

Valóban, $K(\alpha) \cong K[x]/(f) \cong K(\beta)$. A két izomorfizmus egymásutánja megfelelő,

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, melyre $\psi(\alpha) = \beta$ és $\psi(k) = k$ minden $k \in K$ esetén.

Valóban, $K(\alpha) \cong K[x]/(f) \cong K(\beta)$. A két izomorfizmus egymásutánja megfelelő, hiszen $\alpha \mapsto x + (f) \mapsto \beta$

A felbontási test egyértelmű

6.4.9. Következmény

Ha $f \in K[x]$, és f-nek $K \leq L$ és $K \leq N$ is felbontási teste, akkor $L \cong N$, sőt van közöttük olyan izomorfizmus is, ami K elemeit fixen hagyja.

Az alábbi állítás az indukció alapja, részletek a jegyzetben.

Tétel (vö. 6.4.10. Következmény)

Legyen $f \in K[x]$ irreducibilis, $K \leq L$ és $K \leq N$ testbővítések. Tegyük föl, hogy $\alpha \in L$, illetve $\beta \in N$ gyökei f-nek. Ekkor van olyan $\psi : K(\alpha) \to K(\beta)$ izomorfizmus, melyre $\psi(\alpha) = \beta$ és $\psi(k) = k$ minden $k \in K$ esetén.

Valóban, $K(\alpha) \cong K[x]/(f) \cong K(\beta)$. A két izomorfizmus egymásutánja megfelelő, hiszen $\alpha \mapsto x + (f) \mapsto \beta$ és $k \mapsto k + (f) \mapsto k$.

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok

A négyzetrács csúcspontjai.

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok

A négyzetrács csúcspontjai.

Megengedett lépések

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok

A négyzetrács csúcspontjai.

Megengedett lépések

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.

(2) Két megszerkesztett egyenes metszéspontjának kijelölése.

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok

A négyzetrács csúcspontjai.

Megengedett lépések

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.

(2) Két megszerkesztett egyenes metszéspontjának kijelölése.

Ezt a kétféle lépést véges sokszor szabad alkalmazni.

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok

A négyzetrács csúcspontjai.

Megengedett lépések

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.

(2) Két megszerkesztett egyenes metszéspontjának kijelölése.

Ezt a kétféle lépést véges sokszor szabad alkalmazni.
A végén a keresett pontot kell megkapnunk

Szerkeszthetetlenség csak vonalzóval

6.8.1. Állítás

Kockás papíron csak vonalzóval nem tudjuk megszerkeszteni az egyik kis négyzetoldalra támaszkodó szabályos háromszög harmadik csúcsát.

Kiinduló adatok

A négyzetrács csúcspontjai.

Megengedett lépések

(1) Két adott vagy megszerkesztett ponton át egyenes húzása.

(2) Két megszerkesztett egyenes metszéspontjának kijelölése.

Ezt a kétféle lépést véges sokszor szabad alkalmazni.
A végén a keresett pontot kell megkapnunk (2) típusú lépéssel.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert: $(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak,

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert: $(0, 0)$ és $(1, 0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p, q) pontját racionálisnak, ha $p, q \in \mathbb{Q}$.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax + by + c = 0,$$

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert: $(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$ax + by + c = 0$, ahol a,b,c valós számok.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax+by+c=0, \text{ ahol } a,b,c \text{ valós számok.}$$

Hívjunk egy egyenest racionálisnak,

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax + by + c = 0, \text{ ahol } a, b, c \text{ valós számok.}$$

Hívjunk egy egyenest racionálisnak, ha $a, b, c \in \mathbb{Q}$-val felírható.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$ax + by + c = 0$, ahol a,b,c valós számok.

Hívjunk egy egyenest racionálisnak, ha $a,b,c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz,

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax + by + c = 0, \text{ ahol } a, b, c \text{ valós számok.}$$

Hívjunk egy egyenest racionálisnak, ha $a,b,c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz,
a (2) lépésben két racionális egyenesből racionális pont lesz,

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$ax + by + c = 0$, ahol a, b, c valós számok.

Hívjunk egy egyenest racionálisnak, ha $a, b, c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz,
a (2) lépésben két racionális egyenesből racionális pont lesz,
mert mindkétszer lineáris egyenletrendszert kell megoldani.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax + by + c = 0, \text{ ahol } a, b, c \text{ valós számok.}$$

Hívjunk egy egyenest racionálisnak, ha $a,b,c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz,
a (2) lépésben két racionális egyenesből racionális pont lesz,
mert mindkétszer lineáris egyenletrendszert kell megoldani.
Ezért az eljárásban végig minden egyenes és pont racionális.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax + by + c = 0, \text{ ahol } a, b, c \text{ valós számok.}$$

Hívjunk egy egyenest racionálisnak, ha $a,b,c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz,
a (2) lépésben két racionális egyenesből racionális pont lesz,
mert mindkétszer lineáris egyenletrendszert kell megoldani.
Ezért az eljárásban végig minden egyenes és pont racionális.
Azaz csak racionális pont lehet szerkeszthető.

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0, 0)$ és $(1, 0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p, q) pontját racionálisnak, ha $p, q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$ax + by + c = 0$, ahol a, b, c valós számok.

Hívjunk egy egyenest racionálisnak, ha $a, b, c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz,
a (2) lépésben két racionális egyenesből racionális pont lesz,
mert mindkétszer lineáris egyenletrendszert kell megoldani.
Ezért az eljárásban végig minden egyenes és pont racionális.
Azaz csak racionális pont lehet szerkeszthető. A keresett
$(1/2, \sqrt{3}/2)$ nem racionális pont,

A feladat algebraizálása

A négyzetrács ad egy természetes koordinátarendszert:
$(0,0)$ és $(1,0)$ egy kis négyzet két szomszédos csúcsa.

Hívjuk a sík (p,q) pontját racionálisnak, ha $p,q \in \mathbb{Q}$.
Minden egyenest megadhatunk egyenlettel:

$$ax + by + c = 0, \text{ ahol } a,b,c \text{ valós számok.}$$

Hívjunk egy egyenest racionálisnak, ha $a,b,c \in \mathbb{Q}$-val felírható.

Az (1) lépésben két racionális pontból racionális egyenes lesz, a (2) lépésben két racionális egyenesből racionális pont lesz, mert mindkétszer lineáris egyenletrendszert kell megoldani.
Ezért az eljárásban végig minden egyenes és pont racionális.
Azaz csak racionális pont lehet szerkeszthető. A keresett $(1/2, \sqrt{3}/2)$ nem racionális pont, így nem szerkeszthető. $\square$

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF).

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez,

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF).
Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re.
Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF).
Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez,
ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re.
Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány.
Így K_n elemei algebraiak K_0 fölött,

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében,

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében, akkor a szerkesztés elvégezhető.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében, akkor a szerkesztés elvégezhető.

Oka: Véges 2-csoport feloldható;

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében, akkor a szerkesztés elvégezhető.

Oka: Véges 2-csoport feloldható; részcsoportok $\rightarrow$ közbülső testek.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében, akkor a szerkesztés elvégezhető.

Oka: Véges 2-csoport feloldható; részcsoportok $\to$ közbülső testek. A csoport a bővítés „szimmetriáiból áll”:

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében, akkor a szerkesztés elvégezhető.

Oka: Véges 2-csoport feloldható; részcsoportok $\to$ közbülső testek. A csoport a bővítés „szimmetriáiból áll”: Galois-csoport.

Az euklideszi szerkesztés algebraizálása

6.8.3. Lemma, 6.8.15. Tétel, NB

Ha körzőt is használhatunk, akkor minden szerkesztési lépésnél első vagy másodfokú egyenleteket kell megoldanunk (HF). Ezért az alapadatok által generált K_0 test minden lépés során bővülhet egy elem négyzetgyökével. Így a szerkesztés egy $\mathbb{Q} \leq K_0 \leq K_1 \leq \ldots \leq K_n \leq \mathbb{R}$ testláncot eredményez, ahol K_{i+1} megkapható $K_i(\sqrt{d})$ alakban alkalmas $0 < d \in K_i$-re. Speciálisan $K_i \leq K_{i+1}$ foka 1 vagy 2 és $|K_n : K_0|$ 2-hatvány. Így K_n elemei algebraiak K_0 fölött, és fokuk 2-hatvány. Megfordítva, ha a szerkesztendő alakzat adatai benne vannak az alapadatok által generált test egy 2-hatvány fokú normális bővítésében, akkor a szerkesztés elvégezhető.

Oka: Véges 2-csoport feloldható; részcsoportok $\rightarrow$ közbülső testek. A csoport a bővítés „szimmetriáiból áll”: Galois-csoport. Például $x^4 + 2x + 2$ gyökei nem szerkeszthetők (6.10.10. Gyakorlat).

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza,

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3,

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Nem szerkeszthető, mert $\sqrt{\pi}$ transzcendens szám.

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Nem szerkeszthető, mert $\sqrt{\pi}$ transzcendens szám.

6.8.8. Szögharmadolás

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Nem szerkeszthető, mert $\sqrt{\pi}$ transzcendens szám.

6.8.8. Szögharmadolás

Szerkesszük meg egy adott szög harmadát.

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata
egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel
egyenlő területű négyzetet (illetve ennek az oldalát).

Nem szerkeszthető, mert $\sqrt{\pi}$ transzcendens szám.

6.8.8. Szögharmadolás

Szerkesszük meg egy adott szög harmadát.

Nem harmadolható már 60° sem,

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Nem szerkeszthető, mert $\sqrt{\pi}$ transzcendens szám.

6.8.8. Szögharmadolás

Szerkesszük meg egy adott szög harmadát.

Nem harmadolható már 60° sem, mert $\cos 20^\circ$ foka $\mathbb{Q}$ fölött 3,

Kockakettőzés, körnégyszögesítés, szögharmadolás

6.8.6. Kockakettőzés, vagy Déloszi Probléma

Szerkesztendő egy olyan kocka élhossza, aminek térfogata egy adott élhosszúságú kocka térfogatának kétszerese.

Nem szerkeszthető, mert $\sqrt[3]{2}$ foka $\mathbb{Q}$ fölött 3, ami nem 2-hatvány.

6.8.7. Körnégyszögesítés

Szerkesszünk egy megadott sugarú körrel egyenlő területű négyzetet (illetve ennek az oldalát).

Nem szerkeszthető, mert $\sqrt{\pi}$ transzcendens szám.

6.8.8. Szögharmadolás

Szerkesszük meg egy adott szög harmadát.

Nem harmadolható már 60° sem, mert $\cos 20^\circ$ foka $\mathbb{Q}$ fölött 3, minimálpolinomja $x^3 - (3/4)x - (1/8)$.

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög,

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány.

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$,

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

A Fermat-prímes jellemzés elemi számelméleti gondolatmenet.

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

A Fermat-prímes jellemzés elemi számelméleti gondolatmenet.

6.8.10. Állítás

Ha $n \geq 1$, akkor $\mathrm{gr}_{\mathbb{Q}}\big(\cos(2\pi/n)\big)$ értéke $\varphi(n)$, vagy $\varphi(n)/2$.

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

A Fermat-prímes jellemzés elemi számelméleti gondolatmenet.

6.8.10. Állítás

Ha $n \geq 1$, akkor $\mathrm{gr}_{\mathbb{Q}}\big(\cos(2\pi/n)\big)$ értéke $\varphi(n)$, vagy $\varphi(n)/2$.

A pontos érték a 6.8.24. Feladatban olvasható.

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \ldots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

A Fermat-prímes jellemzés elemi számelméleti gondolatmenet.

6.8.10. Állítás

Ha $n \geq 1$, akkor $\mathrm{gr}_{\mathbb{Q}}\big(\cos(2\pi/n)\big)$ értéke $\varphi(n)$, vagy $\varphi(n)/2$.

A pontos érték a 6.8.24. Feladatban olvasható.
A bizonyítás körosztási polinomok segítségével,

Szabályos sokszögek szerkeszthetősége

6.8.11. Tétel, NB

Akkor és csak akkor szerkeszthető szabályos n-szög, ha a $\varphi(n)$ szám 2-hatvány. Ez akkor és csak akkor igaz, ha $n = 2^m p_1 p_2 \dots p_r$, ahol $m \geq 0$ és a p_i számok páronként különböző Fermat-prímek (vagyis $2^{2^k} + 1$ alakú prímszámok).

A Fermat-prímes jellemzés elemi számelméleti gondolatmenet.

6.8.10. Állítás

Ha $n \geq 1$, akkor $\mathrm{gr}_{\mathbb{Q}}\big(\cos(2\pi/n)\big)$ értéke $\varphi(n)$, vagy $\varphi(n)/2$.

A pontos érték a 6.8.24. Feladatban olvasható.
A bizonyítás körosztási polinomok segítségével, a $\mathbb{Q} \leq \mathbb{Q}\big(\cos(2\pi/n)\big) \leq \mathbb{Q}(\varepsilon)$ vizsgálatával, ahol ε primitív n-edik egységgyök.