

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.*
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .*
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).*

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong$

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Ha G véges, akkor $G \cong$

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Ha G véges, akkor $G \cong \mathbb{Z}_n$ valamely $n \geq 2$ természetes számra.

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Ha G véges, akkor $G \cong \mathbb{Z}_n$ valamely $n \geq 2$ természetes számra.

A \mathbb{Z}_n csoportnak annyi részcsoporthja van, ahány

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Ha G véges, akkor $G \cong \mathbb{Z}_n$ valamely $n \geq 2$ természetes számra.

A \mathbb{Z}_n csoportnak annyi részcsoporthja van, ahány osztója n -nek,

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $\langle g \rangle = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Ha G véges, akkor $G \cong \mathbb{Z}_n$ valamely $n \geq 2$ természetes számra. A \mathbb{Z}_n csoportnak annyi részcsoporthja van, ahány osztója n -nek, ezért n csak prím lehet.

Tétel

Bármely legalább kételemű G csoport esetén az alábbiak ekvivalensek:

- (1) G egyszerű Abel-csoport.
- (2) G -nek csak két részcsoporthja van: $\{1\}$ és G .
- (3) G prímszámú ciklikus csoport (azaz $G \cong \mathbb{Z}_p$ valamely p prímszámra).

Biz.

(1) \implies (2): Világos.

(2) \implies (3): Tetszőleges $1 \neq g \in G$ esetén $[g] = G$, tehát G ciklikus.

Ha G végtelen, akkor $G \cong \mathbb{Z}$, de ennek vannak nemtriviális valódi részcsoporthjai.

Ha G véges, akkor $G \cong \mathbb{Z}_n$ valamely $n \geq 2$ természetes számra. A \mathbb{Z}_n csoportnak annyi részcsoporthja van, ahány osztója n -nek, ezért n csak prím lehet.

(3) \implies (1): Világos.



Testek

2013 május 10.

1. Faktortest

2. Hányadostest

3. Karakterisztika, prímtest

4. Testbővítések

1. Faktortest

2. Hányadostest

3. Karakterisztika, prímtest

4. Testbővítések

Ez a rész a tankönyvekben a [Sz] XIII/2 és az [F] VI/4 fejezetben található (+ előismeretek!).

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

$\mathbb{C}, \mathbb{R}, \mathbb{Q}$

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

$\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Q}(\sqrt{2})$

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

\mathbb{C} , \mathbb{R} , \mathbb{Q} , $\mathbb{Q}(\sqrt{2})$, \mathbb{Z}_p (p prímszám)

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

\mathbb{C} , \mathbb{R} , \mathbb{Q} , $\mathbb{Q}(\sqrt{2})$, \mathbb{Z}_p (p prímszám)

Definíció

Az $S \subseteq T$ halmaz **részteste** a T testnek, ha S testet alkot a T -től „örökölt” műveletekkel.

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

\mathbb{C} , \mathbb{R} , \mathbb{Q} , $\mathbb{Q}(\sqrt{2})$, \mathbb{Z}_p (p prímszám)

Definíció

Az $S \subseteq T$ halmaz **részteste** a T testnek, ha S testet alkot a T -től „örökölt” műveletekkel.

Állítás

Egy $S \subseteq T$ halmaz pontosan akkor alkot résztestet a T testben, ha tartalmazza T additív és multiplikatív egységelemét (0 és 1) és zárt a négy alpműveletre (+, -, ·, /).

Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

\mathbb{C} , \mathbb{R} , \mathbb{Q} , $\mathbb{Q}(\sqrt{2})$, \mathbb{Z}_p (p prímszám)

Definíció

Az $S \subseteq T$ halmaz **részteste** a T testnek, ha S testet alkot a T -től „örökölt” műveletekkel.

Állítás

Egy $S \subseteq T$ halmaz pontosan akkor alkot résztestet a T testben, ha tartalmazza T additív és multiplikatív egységelemét (0 és 1) és zárt a négy alpműveletre (+, -, ·, /).

Biz.

HF



Definíció

A $T = (T; +, \cdot)$ gyűrűt **testnek** nevezzük, ha

- ▶ legalább két eleme van;
- ▶ kommutatív és egységelemes;
- ▶ minden nemnulla elemének van multiplikatív inverze: $T^* = T \setminus \{0\}$.

Példa

$\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Q}(\sqrt{2}), \mathbb{Z}_p$ (p prímszám)

Definíció

Az $S \subseteq T$ halmaz **részteste** a T testnek, ha S testet alkot a T -től „örökölt” műveletekkel.

Állítás

Egy $S \subseteq T$ halmaz pontosan akkor alkot résztestet a T testben, ha tartalmazza T additív és multiplikatív egységelemét (0 és 1) és zárt a négy alpműveletre (+, -, ·, /).

Biz.

HF



Példa

A komplex számok testének részteste \mathbb{R} és \mathbb{Q} , de \mathbb{Z} **csak** részgyűrű.

Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.*
- (2) R test vagy prímrendű zérógyűrű.*

Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.
- (2) R test vagy prírendű zérógyűrű.

Biz.

A táblán.



Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.
- (2) R test vagy prímrendű zérógyűrű.

Biz.

A táblán.



Következmény

Bármely legalább kételemű **egységelemes** kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.

Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.
- (2) R test vagy prímrendű zérógyűrű.

Biz.

A táblán.



Következmény

Bármely legalább kételemű **egységelemes** kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.
- (2) R test.

Tétel

Bármely legalább kételemű kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.
- (2) R test vagy prímrendű zérógyűrű.

Biz.

A táblán.



Következmény

Bármely legalább kételemű **egységelemes** kommutatív R gyűrű esetén az alábbiak ekvivalensek:

- (1) R egyszerű gyűrű.
- (2) R test.

Természetesen következik az előző tételből, de íme egy közvetlen bizonyítás:

Biz.

R egyszerű $\implies R$ test:

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze.

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) =$

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$.

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

R test $\implies R$ egyszerű:

Legyen $\{0\} \neq I \triangleleft R$ és $0 \neq a \in I$.

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

R test $\implies R$ egyszerű:

Legyen $\{0\} \neq I \triangleleft R$ és $0 \neq a \in I$. A szívó tulajdonság miatt minden $r \in R$ esetén $r = (ra^{-1}) a \in I$

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

R test $\implies R$ egyszerű:

Legyen $\{0\} \neq I \triangleleft R$ és $0 \neq a \in I$. A szívó tulajdonság miatt minden $r \in R$ esetén $r = (ra^{-1})a \in I$, tehát $I = R$. □

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

R test $\implies R$ egyszerű:

Legyen $\{0\} \neq I \triangleleft R$ és $0 \neq a \in I$. A szívó tulajdonság miatt minden $r \in R$ esetén $r = (ra^{-1})a \in I$, tehát $I = R$. □

Következmény

Legyen R kommutatív egységelemes gyűrű és $I \triangleleft R$. Ekkor az alábbiak ekvivalensek:

- (1) I **maximális ideál** (azaz $\nexists J \triangleleft R : I \subset J \subset R$).
- (2) Az R/I faktorgyűrű test.

Biz.

R egyszerű $\implies R$ test:

Csak azt kell belátni, hogy R minden nemnulla elemének van multiplikatív inverze. Tetszőleges $a \in T \setminus \{0\}$ esetén $\{0\} \neq (a) \triangleleft R$, ezért R egyszerűsége miatt $(a) = R$. Ebből következik, hogy $1 \in (a)$, azaz $\exists b \in R : ab = 1$.

R test $\implies R$ egyszerű:

Legyen $\{0\} \neq I \triangleleft R$ és $0 \neq a \in I$. A szívó tulajdonság miatt minden $r \in R$ esetén $r = (ra^{-1})a \in I$, tehát $I = R$. □

Következmény

Legyen R kommutatív egységelemes gyűrű és $I \triangleleft R$. Ekkor az alábbiak ekvivalensek:

- (1) I **maximális ideál** (azaz $\nexists J \triangleleft R : I \subset J \subset R$).
- (2) Az R/I faktorgyűrű test.

Biz.

A megfeleltetési tétel szerint I pontosan akkor maximális ideál, ha R/I egyszerű gyűrű, vagyis – az előző tétel szerint – test. □

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következésképp az (m) ideál akkor és csak akkor maximális, ha m -nek asszociáltság erejéig pontosan két osztója van: 1 és maga m .

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következésképp az (m) ideál akkor és csak akkor maximális, ha m -nek asszociáltság erejéig pontosan két osztója van: 1 és maga m .

Ezek éppen az irreducibilis elemek, kivéve ha

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következésképp az (m) ideál akkor és csak akkor maximális, ha m -nek asszociáltság erejéig pontosan két osztója van: 1 és maga m .

Ezek éppen az irreducibilis elemek, kivéve ha $m = 0$.

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következésképp az (m) ideál akkor és csak akkor maximális, ha m -nek asszociáltság erejéig pontosan két osztója van: 1 és maga m .

Ezek éppen az irreducibilis elemek, kivéve ha $m = 0$. Utóbbi csak akkor fordulhatna elő, ha

Következmény

Legyen R főideálgyűrű de nem test, és legyen $m \in R$. Ekkor az alábbiak ekvivalensek:

- (1) Az $m \in R$ elem irreducibilis.
- (2) Az $R/(m)$ faktorgyűrű test.

Biz.

Az oszthatóság és az asszociáltság szoros kapcsolatban van a főideálokkal:

$$\forall a, b \in R : a \mid b \iff (a) \supseteq (b)$$

$$\forall a, b \in R : a \sim b \iff (a) = (b)$$

Emiatt m valódi osztói megfelelnek az (m) „fölötti” (fő)ideáloknak.

Következésképp az (m) ideál akkor és csak akkor maximális, ha m -nek asszociáltság erejéig pontosan két osztója van: 1 és maga m .

Ezek éppen az irreducibilis elemek, kivéve ha $m = 0$. Utóbbi csak akkor fordulhatna elő, ha R test lenne (miért)? □

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} =$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} =$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} =$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} =$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} =$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} =$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

$$\overline{12}^{-1} = \overline{u} \iff$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

$$\overline{12}^{-1} = \overline{u} \iff \overline{12} \cdot \overline{u} = \overline{1}$$
$$\iff$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

$$\begin{aligned}\overline{12}^{-1} = \overline{u} &\iff \overline{12} \cdot \overline{u} = \overline{1} \\ &\iff 12u \equiv 1 \pmod{17} \\ &\iff\end{aligned}$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

$$\overline{12}^{-1} = \overline{u} \iff \overline{12} \cdot \overline{u} = \overline{1}$$

$$\iff 12u \equiv 1 \pmod{17}$$

$$\iff \exists v \in \mathbb{Z} : 12u = 1 + 17v$$

$$\iff$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

$$\overline{12}^{-1} = \overline{u} \iff \overline{12} \cdot \overline{u} = \overline{1}$$

$$\iff 12u \equiv 1 \pmod{17}$$

$$\iff \exists v \in \mathbb{Z} : 12u = 1 + 17v$$

$$\iff u \equiv 10 \pmod{17}$$

$$\iff$$

Következmény

\mathbb{Z}_m test $\iff m$ prímszám

- ▶ elemek: $\mathbb{Z}_p = \{\overline{0}, \overline{1}, \dots, \overline{p-1}\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo p kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy diofantoszi egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Példa

Számoljunk \mathbb{Z}_{17} -ben.

$$\overline{12} + \overline{13} = \overline{25} = \overline{8}$$

$$-\overline{12} = \overline{-12} = \overline{5}$$

$$\overline{12} \cdot \overline{13} = \overline{156} = \overline{3}$$

$$\overline{12}^{-1} = \overline{u} \iff \overline{12} \cdot \overline{u} = \overline{1}$$

$$\iff 12u \equiv 1 \pmod{17}$$

$$\iff \exists v \in \mathbb{Z} : 12u = 1 + 17v$$

$$\iff u \equiv 10 \pmod{17}$$

$$\iff \overline{u} = \overline{10}$$

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

- ▶ elemek: $T[x]/(f) = \{\bar{g} : g \in T[x], \deg g \leq n-1\} =$
 $= \left\{ \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} : a_0, a_1, \dots, a_{n-1} \in T \right\}$

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

- ▶ elemek: $T[x]/(f) = \{\bar{g} : g \in T[x], \deg g \leq n-1\} =$
 $= \left\{ \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} : a_0, a_1, \dots, a_{n-1} \in T \right\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo f kell számolni

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

- ▶ elemek: $T[x]/(f) = \{\bar{g} : g \in T[x], \deg g \leq n-1\} =$
 $= \left\{ \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} : a_0, a_1, \dots, a_{n-1} \in T \right\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo f kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy „diofantoszi” egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

- ▶ elemek: $T[x]/(f) = \{\bar{g} : g \in T[x], \deg g \leq n-1\} =$
 $= \left\{ \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} : a_0, a_1, \dots, a_{n-1} \in T \right\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo f kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy „diofantoszi” egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Következmény

Ha $f \in \mathbb{Z}_p[x]$ egy n -edfokú irreducibilis polinom, akkor $\mathbb{Z}_p[x]/(f)$ egy p^n elemszámú test.

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

- ▶ elemek: $T[x]/(f) = \{\bar{g} : g \in T[x], \deg g \leq n-1\} =$
 $= \left\{ \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} : a_0, a_1, \dots, a_{n-1} \in T \right\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo f kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy „diofantoszi” egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Következmény

Ha $f \in \mathbb{Z}_p[x]$ egy n -edfokú irreducibilis polinom, akkor $\mathbb{Z}_p[x]/(f)$ egy p^n elemszámú test.

Megjegyzés

Meg lehet mutatni, hogy minden p prímszám és n természetes szám esetén létezik n -edfokú irreducibilis polinom \mathbb{Z}_p felett.

Következmény

Tetszőleges T test és n -edfokú $f \in T[x]$ esetén

$T[x]/(f)$ test $\iff f$ irreducibilis T felett.

- ▶ elemek: $T[x]/(f) = \{\bar{g} : g \in T[x], \deg g \leq n-1\} =$
 $= \left\{ \overline{a_{n-1}x^{n-1} + \dots + a_1x + a_0} : a_0, a_1, \dots, a_{n-1} \in T \right\}$
- ▶ számolás:
 - ▶ összeadás, additív inverz (kivonás), szorzás: egyszerű, csak modulo f kell számolni
 - ▶ multiplikatív inverz (osztás): lineáris kongruenciát vagy „diofantoszi” egyenletet kell megoldani (ha másképp nem megy, akkor euklideszi algoritmussal)

Következmény

Ha $f \in \mathbb{Z}_p[x]$ egy n -edfokú irreducibilis polinom, akkor $\mathbb{Z}_p[x]/(f)$ egy p^n elemszámú test.

Megjegyzés

Meg lehet mutatni, hogy minden p prímszám és n természetes szám esetén létezik n -edfokú irreducibilis polinom \mathbb{Z}_p felett. Következésképp minden q prímszámra létezik q -elemű test.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.
- ▶ $\mathbb{C}[x] / (x^2 + 1)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.
- ▶ $\mathbb{C}[x] / (x^2 + 1)$: nem,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.
- ▶ $\mathbb{C}[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x - i)(x + i)$.

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.
- ▶ $\mathbb{C}[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x - i)(x + i)$.
- ▶ $\mathbb{Q}[x] / (x^4 + 4x^3 + 6x^2 + 8x + 10)$:

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.
- ▶ $\mathbb{C}[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x - i)(x + i)$.
- ▶ $\mathbb{Q}[x] / (x^4 + 4x^3 + 6x^2 + 8x + 10)$: igen,
mert

Példa

Melyek testek az alábbi faktorgyűrűk közül?

- ▶ $\mathbb{Z}_2[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x + 1)^2$.
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_3 -ban.
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1)$: igen,
mert $x^2 + x + 1$ csak másodfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1)$: igen,
mert $x^3 + x + 1$ csak harmadfokú, és nincs gyöke \mathbb{Z}_2 -ben.
- ▶ $\mathbb{Z}_2[x] / (x^4 + x^2 + 1)$: nem,
mert $x^4 + x^2 + 1 = (x^2 + x + 1)^2$.
- ▶ $\mathbb{R}[x] / (x^2 + 1)$: igen,
mert $x^2 + 1$ csak másodfokú, és nincs valós gyöke.
- ▶ $\mathbb{C}[x] / (x^2 + 1)$: nem,
mert $x^2 + 1 = (x - i)(x + i)$.
- ▶ $\mathbb{Q}[x] / (x^4 + 4x^3 + 6x^2 + 8x + 10)$: igen,
mert $x^4 + 4x^3 + 6x^2 + 8x + 10$ irreducibilis \mathbb{Q} felett (miért?).

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\overline{2-x}^{-1} = \bar{u} \iff$$

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned} \overline{2-x}^{-1} = \bar{u} &\iff \overline{2-x} \cdot \bar{u} = \bar{1} \\ &\iff \end{aligned}$$

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned}\overline{2-x}^{-1} = \bar{u} &\iff \overline{2-x} \cdot \bar{u} = \bar{1} \\ &\iff (2-x)u \equiv 1 \pmod{x^3-7} \\ &\iff\end{aligned}$$

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\overline{2-x}^{-1} = \bar{u} \iff \overline{2-x} \cdot \bar{u} = \bar{1}$$

$$\iff (2-x)u \equiv 1 \pmod{x^3-7}$$

$$\iff \exists v \in \mathbb{Q}[x] : (2-x)u = 1 + (x^3-7)v$$

$$\iff$$

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned}\overline{2-x}^{-1} = \bar{u} &\iff \overline{2-x} \cdot \bar{u} = \bar{1} \\ &\iff (2-x)u \equiv 1 \pmod{x^3-7} \\ &\iff \exists v \in \mathbb{Q}[x] : (2-x)u = 1 + (x^3-7)v \\ &\iff u \equiv x^2 + 2x + 4 \pmod{x^3-7} \\ &\iff\end{aligned}$$

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned}\overline{2-x}^{-1} = \bar{u} &\iff \overline{2-x} \cdot \bar{u} = \bar{1} \\ &\iff (2-x)u \equiv 1 \pmod{x^3-7} \\ &\iff \exists v \in \mathbb{Q}[x] : (2-x)u = 1 + (x^3-7)v \\ &\iff u \equiv x^2 + 2x + 4 \pmod{x^3-7} \\ &\iff \bar{u} = \overline{x^2 + 2x + 4}\end{aligned}$$

Példa

Határozzuk meg a $K = \mathbb{Q}[x] / (x^3 - 7)$ testben a $\overline{2-x}$ elem multiplikatív inverzét.

K elemei $\overline{ax^2 + bx + c}$ ($a, b, c \in \mathbb{Q}$) alakúak, ilyen alakban szeretnénk az $\bar{u} = \overline{2-x}^{-1}$ elemet is megkapni.

$$\begin{aligned}\overline{2-x}^{-1} = \bar{u} &\iff \overline{2-x} \cdot \bar{u} = \bar{1} \\ &\iff (2-x)u \equiv 1 \pmod{x^3-7} \\ &\iff \exists v \in \mathbb{Q}[x] : (2-x)u = 1 + (x^3-7)v \\ &\iff u \equiv x^2 + 2x + 4 \pmod{x^3-7} \\ &\iff \bar{u} = \overline{x^2 + 2x + 4}\end{aligned}$$

Tehát $\overline{2-x}^{-1} = \overline{x^2 + 2x + 4}$.

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} =$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} =$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} =$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1}$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

$$\overline{x+1}^{-1} = \bar{u} \iff$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

$$\overline{x+1}^{-1} = \bar{u} \iff \overline{x+1} \cdot \bar{u} = \bar{1}$$
$$\iff$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

$$\overline{x+1}^{-1} = \bar{u} \iff \overline{x+1} \cdot \bar{u} = \bar{1}$$

$$\iff (x+1)u \equiv 1 \pmod{x^2+x+1}$$

$$\iff$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

$$\overline{x+1}^{-1} = \bar{u} \iff \overline{x+1} \cdot \bar{u} = \bar{1}$$

$$\iff (x+1)u \equiv 1 \pmod{x^2+x+1}$$

$$\iff \exists v \in \mathbb{Z}_2[x] : (x+1)u = 1 + (x^2+x+1)v$$

$$\iff$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

$$\overline{x+1}^{-1} = \bar{u} \iff \overline{x+1} \cdot \bar{u} = \bar{1}$$

$$\iff (x+1)u \equiv 1 \pmod{x^2+x+1}$$

$$\iff \exists v \in \mathbb{Z}_2[x] : (x+1)u = 1 + (x^2+x+1)v$$

$$\iff u \equiv x \pmod{x^2+x+1}$$

$$\iff$$

Példa

Számoljunk a $\mathbb{Z}_2[x] / (x^2 + x + 1)$ négyelemű testben.

$$\mathbb{Z}_2[x] / (x^2 + x + 1) = \{\bar{0}, \bar{1}, \bar{x}, \overline{x+1}\}$$

$$\overline{x+1} + \bar{1} = \bar{x}$$

$$-\overline{x+1} = \overline{x+1}$$

$$\overline{x+1} \cdot \overline{x+1} = \overline{x^2+1} = \bar{x}$$

$$\overline{x+1}^{-1} = \bar{u} \iff \overline{x+1} \cdot \bar{u} = \bar{1}$$

$$\iff (x+1)u \equiv 1 \pmod{x^2+x+1}$$

$$\iff \exists v \in \mathbb{Z}_2[x] : (x+1)u = 1 + (x^2+x+1)v$$

$$\iff u \equiv x \pmod{x^2+x+1}$$

$$\iff \bar{u} = \bar{x}$$

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test művelet táblázatai:

+	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$

·	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test művelet táblázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test műveletábrázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test művelet táblázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test művelet táblázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;
- ▶ $\alpha = \bar{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test művelet táblázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;
- ▶ $\alpha = \bar{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:
 $f(\alpha) = \alpha^2 + \alpha + 1 =$

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test művelet táblázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;
- ▶ $\alpha = \bar{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:
 $f(\alpha) = \alpha^2 + \alpha + 1 = \bar{x}^2 + \bar{x} + \bar{1} =$

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test műveletábrázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;
- ▶ $\alpha = \bar{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:
 $f(\alpha) = \alpha^2 + \alpha + 1 = \overline{x^2 + x + 1} = \overline{x^2 + x + 1} =$

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test műveletábrázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;
- ▶ $\alpha = \bar{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:
 $f(\alpha) = \alpha^2 + \alpha + 1 = \bar{x}^2 + \bar{x} + \bar{1} = \overline{x^2 + x + 1} = \bar{0} =$

A négyelemű $K := \mathbb{Z}_2[x] / (x^2 + x + 1)$ test műveletábrázatai:

$+$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	\cdot	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\overline{x+1}$
\bar{x}	\bar{x}	$\overline{x+1}$	$\bar{0}$	$\bar{1}$	\bar{x}	$\bar{0}$	\bar{x}	$\overline{x+1}$	$\bar{1}$
$\overline{x+1}$	$\overline{x+1}$	\bar{x}	$\bar{1}$	$\bar{0}$	$\overline{x+1}$	$\bar{0}$	$\overline{x+1}$	$\bar{1}$	\bar{x}

Ugyanez tömörebben, a $0 := \bar{0}$, $1 := \bar{1}$, $\alpha := \bar{x}$, $\beta := \overline{x+1}$ jelöléssel:

$+$	0	1	α	β	\cdot	0	1	α	β
0	0	1	α	β	0	0	0	0	0
1	1	0	β	α	1	0	1	α	β
α	α	β	0	1	α	0	α	β	1
β	β	α	1	0	β	0	β	1	α

Figyeljük meg, hogy

- ▶ $\{0, 1\} = \{\bar{0}, \bar{1}\}$ egy \mathbb{Z}_2 -vel izomorf résztestet alkot K -ban;
- ▶ $\alpha = \bar{x}$ gyöke az $x^2 + x + 1 \in K[x]$ polinomnak:
 $f(\alpha) = \alpha^2 + \alpha + 1 = \overline{x^2 + x + 1} = \overline{x^2 + x + 1} = \bar{0} = 0.$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

- ▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

- ▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)
- ▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

▶ elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$)

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

▶ elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$)

▶ számolási szabály: $\alpha^2 + 1 = \bar{x}^2 + \bar{1} = \overline{x^2 + 1} = \bar{0} = 0$, azaz $\alpha^2 = -1$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

▶ elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$)

▶ számolási szabály: $\alpha^2 + 1 = \bar{x^2 + 1} = \bar{0} = 0$, azaz $\alpha^2 = -1$

▶ összeadás: $(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

▶ elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$)

▶ számolási szabály: $\alpha^2 + 1 = \bar{x^2 + 1} = \bar{0} = 0$, azaz $\alpha^2 = -1$

▶ összeadás: $(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$

▶ szorzás: $(a + b\alpha) \cdot (c + d\alpha) = (ac - bd) + (ad + bc)\alpha$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

- ▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)
- ▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$
- ▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

- ▶ elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$)
- ▶ számolási szabály: $\alpha^2 + 1 = \bar{x}^2 + \bar{1} = \overline{x^2 + 1} = \bar{0} = 0$, azaz $\alpha^2 = -1$
- ▶ összeadás: $(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$
- ▶ szorzás: $(a + b\alpha) \cdot (c + d\alpha) = (ac - bd) + (ad + bc)\alpha$

Ha α helyett az i betűt használjuk, akkor világos, hogy

$$\mathbb{R}[x] / (x^2 + 1) \cong$$

Példa

Számoljunk az $\mathbb{R}[x] / (x^2 + 1)$ testben

▶ elemek: $\overline{a + bx}$ ($a, b \in \mathbb{R}$)

▶ összeadás: $\overline{a + bx} + \overline{c + dx} = \overline{(a + c) + (b + d)x}$

▶ szorzás:

$$\overline{a + bx} \cdot \overline{c + dx} = \overline{ac + (ad + bc)x + bdx^2} = \overline{(ac - bd) + (ad + bc)x}$$

Használjuk az $a := \bar{a}$ ($a \in \mathbb{R}$) és $\alpha := \bar{x}$ rövidítéseket:

▶ elemek: $a + b\alpha$ ($a, b \in \mathbb{R}$)

▶ számolási szabály: $\alpha^2 + 1 = \bar{x}^2 + \bar{1} = \overline{x^2 + 1} = \bar{0} = 0$, azaz $\alpha^2 = -1$

▶ összeadás: $(a + b\alpha) + (c + d\alpha) = (a + c) + (b + d)\alpha$

▶ szorzás: $(a + b\alpha) \cdot (c + d\alpha) = (ac - bd) + (ad + bc)\alpha$

Ha α helyett az i betűt használjuk, akkor világos, hogy

$$\mathbb{R}[x] / (x^2 + 1) \cong \mathbb{C}.$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az $\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x]$ polinommal.

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az

$$\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x] \text{ polinommal.}$$

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$f(\alpha) = a_n \cdot \alpha^n + \dots + a_1 \cdot \alpha + a_0 =$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az

$$\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x] \text{ polinommal.}$$

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$\begin{aligned} f(\alpha) &= a_n \cdot \alpha^n + \dots + a_1 \cdot \alpha + a_0 = \bar{a}_n \cdot \bar{x}^n + \dots + \bar{a}_1 \cdot \bar{x} + \bar{a}_0 \\ &= \end{aligned}$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az $\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x]$ polinommal.

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$\begin{aligned} f(\alpha) &= a_n \cdot \alpha^n + \dots + a_1 \cdot \alpha + a_0 = \bar{a}_n \cdot \bar{x}^n + \dots + \bar{a}_1 \cdot \bar{x} + \bar{a}_0 \\ &= \overline{a_n x^n + \dots + a_1 x + a_0} \\ &= \end{aligned}$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az

$$\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x] \text{ polinommal.}$$

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$\begin{aligned} f(\alpha) &= a_n \cdot \alpha^n + \dots + a_1 \cdot \alpha + a_0 = \bar{a}_n \cdot \bar{x}^n + \dots + \bar{a}_1 \cdot \bar{x} + \bar{a}_0 \\ &= \overline{a_n x^n + \dots + a_1 x + a_0} \\ &= \bar{f} = \end{aligned}$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, \quad a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az

$$\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x] \text{ polinommal.}$$

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$\begin{aligned} f(\alpha) &= a_n \cdot \alpha^n + \dots + a_1 \cdot \alpha + a_0 = \bar{a}_n \cdot \bar{x}^n + \dots + \bar{a}_1 \cdot \bar{x} + \bar{a}_0 \\ &= \overline{a_n x^n + \dots + a_1 x + a_0} \\ &= \bar{f} = \bar{0} = \end{aligned}$$

Tétel

Ha $f \in T[x]$ irreducibilis polinom, akkor a $K := T[x]/(f)$ faktortestben

$$T_1 := \{\bar{a} : a \in T\}$$

egy T -vel izomorf résztestet alkot, továbbá $\alpha := \bar{x} \in K$ gyöke az $f \in K[x]$ polinomnak.

Biz.

Az alábbi leképezés izomorfizmus T és T_1 között:

$$\varphi: T \rightarrow T_1 \leq K, a \mapsto \bar{a}.$$

Általában nem is különböztetjük meg az \bar{a} és a ($a \in T$) elemeket egymástól, így T részteste lesz K -nak.

Ezzel az $f = a_n x^n + \dots + a_1 x + a_0 \in T[x]$ polinomot is azonosítottuk az $\bar{a}_n x^n + \dots + \bar{a}_1 x + \bar{a}_0 \in T_1[x] \leq K[x]$ polinommal.

Így már van értelme kiszámítani $f(\alpha)$ értékét:

$$\begin{aligned} f(\alpha) &= a_n \cdot \alpha^n + \dots + a_1 \cdot \alpha + a_0 = \bar{a}_n \cdot \bar{x}^n + \dots + \bar{a}_1 \cdot \bar{x} + \bar{a}_0 \\ &= \overline{a_n x^n + \dots + a_1 x + a_0} \\ &= \bar{f} = \bar{0} = 0. \quad \square \end{aligned}$$

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében.

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében.
(Ha f nem irreducibilis, akkor

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- ▶ Az eljárást ismételve olyan test is konstruálható, amelyben már f -nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f **felbontási teste**).

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- ▶ Az eljárást ismételve olyan test is konstruálható, amelyben már f -nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f **felbontási teste**).
- ▶ Transzfinit indukcióval igazolható olyan \bar{T} test létezése is, amelyben már nem csak egy kiválasztott $f \in T[x]$ polinom bomlik lineáris tényezők szorzatára, hanem minden T feletti polinom (a \bar{T} testet a T test **algebrai lezártjának** nevezzük).

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- ▶ Az eljárást ismételve olyan test is konstruálható, amelyben már f -nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f **felbontási teste**).
- ▶ Transzfinit indukcióval igazolható olyan \bar{T} test létezése is, amelyben már nem csak egy kiválasztott $f \in T[x]$ polinom bomlik lineáris tényezők szorzatára, hanem minden T feletti polinom (a \bar{T} testet a T test **algebrai lezártjának** nevezzük).
- ▶ Az algebra alaptétele szerint a komplex számok teste algebrailag zárt ($\bar{\mathbb{C}} = \mathbb{C}$)

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- ▶ Az eljárást ismételve olyan test is konstruálható, amelyben már f -nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f **felbontási teste**).
- ▶ Transzfinit indukcióval igazolható olyan \bar{T} test létezése is, amelyben már nem csak egy kiválasztott $f \in T[x]$ polinom bomlik lineáris tényezők szorzatára, hanem minden T feletti polinom (a \bar{T} testet a T test **algebrai lezártjának** nevezzük).
- ▶ Az algebra alaptétele szerint a komplex számok teste algebrailag zárt ($\bar{\mathbb{C}} = \mathbb{C}$), ez a valós számtest algebrai lezártja is ($\bar{\mathbb{R}} = \mathbb{C}$).

Megjegyzés

- ▶ Az előbbi konstrukcióval bármely $f \in T[x]$ polinomnak lehet „gyököt csinálni” az alaptest egy megfelelő K kibővítésében. (Ha f nem irreducibilis, akkor dolgozzunk egy irreducibilis osztójával.)
- ▶ Az eljárást ismételve olyan test is konstruálható, amelyben már f -nek annyi gyöke van, amennyi a fokszáma, azaz f elsőfokú polinomok (gyöktényezők) szorzatára bomlik (f **felbontási teste**).
- ▶ Transzfinit indukcióval igazolható olyan \bar{T} test létezése is, amelyben már nem csak egy kiválasztott $f \in T[x]$ polinom bomlik lineáris tényezők szorzatára, hanem minden T feletti polinom (a \bar{T} testet a T test **algebrai lezártjának** nevezzük).
- ▶ Az algebra alaptétele szerint a komplex számok teste algebrailag zárt ($\bar{\mathbb{C}} = \mathbb{C}$), ez a valós számtest algebrai lezártja is ($\bar{\mathbb{R}} = \mathbb{C}$).
- ▶ A racionális számtest algebrai lezártja az **algebrai számok** teste.

1. Faktortest

2. Hányadostest

3. Karakterisztika, prímtest

4. Testbővítések

Ez a rész a tankönyvekben az [F] III/8 fejezetben található.

Tétel

Minden integritástartomány beágyazható testbe.

Tétel

Minden integritástartomány beágyazható testbe.

Biz.

Legyen R integritástartomány, és értelmezzünk az $R \times (R \setminus \{0\})$ halmazon két műveletet a következőképpen:

$$(a, b) + (c, d) = (ad + bc, bd),$$

$$(a, b) \cdot (c, d) = (ac, bd).$$

Tétel

Minden integritástartomány beágyazható testbe.

Biz.

Legyen R integritástartomány, és értelmezzünk az $R \times (R \setminus \{0\})$ halmazon két műveletet a következőképpen:

$$(a, b) + (c, d) = (ad + bc, bd),$$

$$(a, b) \cdot (c, d) = (ac, bd).$$

Mindkét művelet asszociatív és kommutatív

Tétel

Minden integritástartomány beágyazható testbe.

Biz.

Legyen R integritástartomány, és értelmezzünk az $R \times (R \setminus \{0\})$ halmazon két műveletet a következőképpen:

$$(a, b) + (c, d) = (ad + bc, bd),$$

$$(a, b) \cdot (c, d) = (ac, bd).$$

Mindkét művelet asszociatív és kommutatív, viszont a szorzás sajnos nem disztributív az összeadásra:

$$((a, b) + (c, d)) \cdot (e, f) = (ade + bce, bdf),$$

$$(a, b) \cdot (e, f) + (c, d) \cdot (e, f) = (adef + bcef, bdf^2).$$

Tétel

Minden integritástartomány beágyazható testbe.

Biz.

Legyen R integritástartomány, és értelmezzünk az $R \times (R \setminus \{0\})$ halmazon két műveletet a következőképpen:

$$(a, b) + (c, d) = (ad + bc, bd),$$

$$(a, b) \cdot (c, d) = (ac, bd).$$

Mindkét művelet asszociatív és kommutatív, viszont a szorzás sajnos nem disztributív az összeadásra:

$$((a, b) + (c, d)) \cdot (e, f) = (ade + bce, bdf),$$

$$(a, b) \cdot (e, f) + (c, d) \cdot (e, f) = (adef + bcef, bdf^2).$$

Vezessünk be egy \sim relációt az $R \times (R \setminus \{0\})$ halmazon:

$$(a, b) \sim (c, d) \stackrel{\text{def}}{\iff} ad = bc.$$

Tétel

Minden integritástartomány beágyazható testbe.

Biz.

Legyen R integritástartomány, és értelmezzünk az $R \times (R \setminus \{0\})$ halmazon két műveletet a következőképpen:

$$(a, b) + (c, d) = (ad + bc, bd),$$

$$(a, b) \cdot (c, d) = (ac, bd).$$

Mindkét művelet asszociatív és kommutatív, viszont a szorzás sajnos nem disztributív az összeadásra:

$$((a, b) + (c, d)) \cdot (e, f) = (ade + bce, bdf),$$

$$(a, b) \cdot (e, f) + (c, d) \cdot (e, f) = (adef + bcef, bdf^2).$$

Vezessünk be egy \sim relációt az $R \times (R \setminus \{0\})$ halmazon:

$$(a, b) \sim (c, d) \stackrel{\text{def}}{\iff} ad = bc.$$

Ez egy ekvivalenciareláció, ami kompatibilis a fenti műveletekkel, vagyis kongruenciája az $(R \times (R \setminus \{0\}); +, \cdot)$ algebrának.

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el).

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem:

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el).

Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el).

Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze:

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el).

Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el).

Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el).

Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem:

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem: $\overline{(1, 1)}$

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem: $\overline{(1, 1)}$
- ▶ $\overline{(a, b)} \approx \overline{(0, 1)}$ multiplikatív inverze:

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem: $\overline{(1, 1)}$
- ▶ $\overline{(a, b)} \approx \overline{(0, 1)}$ multiplikatív inverze: $\overline{(b, a)}$

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem: $\overline{(1, 1)}$
- ▶ $\overline{(a, b)} \approx \overline{(0, 1)}$ multiplikatív inverze: $\overline{(b, a)}$

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$$

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem: $\overline{(1, 1)}$
- ▶ $\overline{(a, b)} \approx \overline{(0, 1)}$ multiplikatív inverze: $\overline{(b, a)}$

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$$

Tehát T test.

Biz. (folyt.)

A $T := (R \times (R \setminus \{0\}); +, \cdot) / \sim$ faktoralgebrában már teljesül a disztributivitás (és az asszociativitás meg a kommutativitás se romlik el). Jelölje az $(a, b) \in R \times (R \setminus \{0\})$ elem \sim szerinti osztályát $\overline{(a, b)}$.

- ▶ additív egységelem: $\overline{(0, 1)}$
- ▶ $\overline{(a, b)}$ additív inverze: $\overline{(-a, b)}$

$$\overline{(a, b)} + \overline{(-a, b)} = \overline{(0, b^2)} = \overline{(0, 1)}$$

- ▶ multiplikatív egységelem: $\overline{(1, 1)}$
- ▶ $\overline{(a, b)} \approx \overline{(0, 1)}$ multiplikatív inverze: $\overline{(b, a)}$

$$\overline{(a, b)} \cdot \overline{(b, a)} = \overline{(ab, ba)} = \overline{(1, 1)}$$

Tehát T test.

Az $\overline{(a, 1)}$ alakú elemek egy R -rel izomorf részgyűrűt alkotnak T -ben, hiszen könnyű ellenőrizni, hogy

$$\varphi: R \rightarrow T, a \mapsto \overline{(a, 1)}$$

injektív homomorfizmus (vagyis beágyazás).



Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel).

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$.

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a **a** legszűkebb test, ami tartalmazza R -et.

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

▶ $Q_{\mathbb{Z}} \cong$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

► $Q_{\mathbb{Z}} \cong \mathbb{Q}$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

► $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

► $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

► $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

► $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

- ▶ $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- ▶ Ha K test, akkor $Q_K \cong$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a **a** legszűkebb test, ami tartalmazza R -et.

Példa

- ▶ $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- ▶ Ha K test, akkor $Q_K \cong K$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

- ▶ $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- ▶ Ha K test, akkor $Q_K \cong K$, hiszen $\overline{(a, b)} =$

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

- ▶ $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- ▶ Ha K test, akkor $Q_K \cong K$, hiszen $\overline{(a, b)} = \overline{(ab^{-1}, 1)}$.

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a **a** legszűkebb test, ami tartalmazza R -et.

Példa

- ▶ $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- ▶ Ha K test, akkor $Q_K \cong K$, hiszen $\overline{(a, b)} = \overline{(ab^{-1}, 1)}$.
- ▶ Ha K test, akkor $Q_{K[x]} = K(x) = \left\{ \frac{f}{g} : f, g \in K[x], g \neq 0 \right\}$; ez a K feletti **racionális törtek** teste.

Megjegyzés

Mivel T tartalmaz R -rel izomorf részgyűrűt, tekinthetjük úgy, hogy R részgyűrűje T -nek (az $\overline{(a, 1)} \in T$ elemet azonosítjuk az $a \in R$ elemmel). Ekkor a T test bármely eleme előáll két R -beli elem hányadosaként:

$$\overline{(a, b)} = \overline{(a, 1)} \cdot \overline{(1, b)} = \overline{(a, 1)} \cdot \overline{(b, 1)}^{-1} = a \cdot b^{-1}.$$

Ezért a T testet az R integritástartomány **hányadostestének** nevezzük. Jelölése: $T = Q_R$. Ez a legszűkebb test, ami tartalmazza R -et.

Példa

- ▶ $Q_{\mathbb{Z}} \cong \mathbb{Q}$, $Q_{\mathbb{Z}[i]} \cong \mathbb{Q}(i)$, $Q_{\mathbb{Z}[\sqrt{2}]} \cong \mathbb{Q}(\sqrt{2})$
- ▶ Ha K test, akkor $Q_K \cong K$, hiszen $\overline{(a, b)} = \overline{(ab^{-1}, 1)}$.
- ▶ Ha K test, akkor $Q_{K[x]} = K(x) = \left\{ \frac{f}{g} : f, g \in K[x], g \neq 0 \right\}$;
ez a K feletti **racionális törtek** teste.
(Nem keverendő a racionális törtfüggvényekkel, ahogy a polinomok se keverendők a polinomfüggvényekkel!)

Tétel

Izomorf integritástományok hányadostestei is izomorfak.

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi: R \rightarrow S$ izomorfizmus; ekkor

$$\hat{\varphi}: Q_R \rightarrow Q_S, \overline{(a, b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely **kiterjesztése** φ -nek (azaz $\hat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi: R \rightarrow S$ izomorfizmus; ekkor

$$\hat{\varphi}: Q_R \rightarrow Q_S, \overline{(a, b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely **kiterjesztése** φ -nek (azaz $\hat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Ha K olyan test, ami részgyűrűként tartalmazza az R integritástartományt, akkor K résztestként tartalmazza Q_R egy izomorf példányát.

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi: R \rightarrow S$ izomorfizmus; ekkor

$$\hat{\varphi}: Q_R \rightarrow Q_S, \overline{(a, b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely **kiterjesztése** φ -nek (azaz $\hat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Ha K olyan test, ami részgyűrűként tartalmazza az R integritástartományt, akkor K résztestként tartalmazza Q_R egy izomorf példányát.

Biz.

Definiáljuk az alábbi φ leképezést:

$$\varphi: R \times (R \setminus \{0\}) \rightarrow K, (a, b) \mapsto ab^{-1}.$$

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi: R \rightarrow S$ izomorfizmus; ekkor

$$\hat{\varphi}: Q_R \rightarrow Q_S, \overline{(a, b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely **kiterjesztése** φ -nek (azaz $\hat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Ha K olyan test, ami részgyűrűként tartalmazza az R integritástartományt, akkor K résztestként tartalmazza Q_R egy izomorf példányát.

Biz.

Definiáljuk az alábbi φ leképezést:

$$\varphi: R \times (R \setminus \{0\}) \rightarrow K, (a, b) \mapsto ab^{-1}.$$

Ez a leképezés felcserélhető az összeadással és a szorzással is, és magja éppen

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi: R \rightarrow S$ izomorfizmus; ekkor

$$\hat{\varphi}: Q_R \rightarrow Q_S, \overline{(a, b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely **kiterjesztése** φ -nek (azaz $\hat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Ha K olyan test, ami részgyűrűként tartalmazza az R integritástartományt, akkor K résztestként tartalmazza Q_R egy izomorf példányát.

Biz.

Definiáljuk az alábbi φ leképezést:

$$\varphi: R \times (R \setminus \{0\}) \rightarrow K, (a, b) \mapsto ab^{-1}.$$

Ez a leképezés felcserélhető az összeadással és a szorzással is, és magja éppen a \sim reláció.

Tétel

Izomorf integritástartományok hányadostestei is izomorfak.

Biz.

Legyen $\varphi: R \rightarrow S$ izomorfizmus; ekkor

$$\hat{\varphi}: Q_R \rightarrow Q_S, \overline{(a, b)} \mapsto \overline{(a\varphi, b\varphi)}$$

izomorfizmus, amely **kiterjesztése** φ -nek (azaz $\hat{\varphi}$ megszorítása az $R \leq Q_R$ részgyűrűre éppen φ). □

Tétel

Ha K olyan test, ami részgyűrűként tartalmazza az R integritástartományt, akkor K résztestként tartalmazza Q_R egy izomorf példányát.

Biz.

Definiáljuk az alábbi φ leképezést:

$$\varphi: R \times (R \setminus \{0\}) \rightarrow K, (a, b) \mapsto ab^{-1}.$$

Ez a leképezés felcserélhető az összeadással és a szorzással is, és magja éppen a \sim reláció. A homomorfia-tételt alkalmazva kapjuk, hogy

$$Q_R = R \times (R \setminus \{0\}) / \sim \cong \varphi \text{ értékészlete} \leq K. \quad \square$$

Következmény

Legyen K *minimális* olyan test, ami részgyűrűként tartalmazza az R integritástartományt (azaz K -nak nincs olyan valódi részteste, ami tartalmazza R -et). Ekkor $K \cong Q_R$.

Következmény

Legyen K *minimális* olyan test, ami részgyűrűként tartalmazza az R integritástartományt (azaz K -nak nincs olyan valódi részteste, ami tartalmazza R -et). Ekkor $K \cong Q_R$.

Biz.

Az előző tételt alkalmazva kapjuk, hogy K tartalmaz Q_R -rel izomorf résztestet.

Következmény

Legyen K *minimális* olyan test, ami részgyűrűként tartalmazza az R integritástartományt (azaz K -nak nincs olyan valódi részteste, ami tartalmazza R -et). Ekkor $K \cong Q_R$.

Biz.

Az előző tételt alkalmazva kapjuk, hogy K tartalmaz Q_R -rel izomorf résztestet. A minimalitás miatt ez a résztest csak maga K lehet. □

1. Faktortest
2. Hányadostest
3. Karakterisztika, prímtest
4. Testbővítések

Ez a rész a tankönyvekben az [F] III/9 fejezetben található.

Definíció

Az R gyűrű **karaktisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla.

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Példa

► $\text{char } \mathbb{C} = \text{char } \mathbb{R} = \text{char } \mathbb{Q} = \text{char } \mathbb{Z} =$

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Példa

- ▶ $\text{char } \mathbb{C} = \text{char } \mathbb{R} = \text{char } \mathbb{Q} = \text{char } \mathbb{Z} = 0$

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \cdots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Példa

- ▶ $\text{char } \mathbb{C} = \text{char } \mathbb{R} = \text{char } \mathbb{Q} = \text{char } \mathbb{Z} = 0$
- ▶ $\text{char } \mathbb{Z}_n =$

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Példa

- ▶ $\text{char } \mathbb{C} = \text{char } \mathbb{R} = \text{char } \mathbb{Q} = \text{char } \mathbb{Z} = 0$
- ▶ $\text{char } \mathbb{Z}_n = n$

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Példa

- ▶ $\text{char } \mathbb{C} = \text{char } \mathbb{R} = \text{char } \mathbb{Q} = \text{char } \mathbb{Z} = 0$
- ▶ $\text{char } \mathbb{Z}_n = n$
- ▶ $\text{char } R[x] = \text{char } R$

Definíció

Az R gyűrű **karakterisztikáján** a legkisebb olyan n pozitív egész számot értjük, amelyre

$$\forall a \in R : na = \underbrace{a + \dots + a}_n = 0.$$

Ha nincs ilyen n , akkor azt mondjuk, hogy R karakterisztikája végtelen nulla. Jelölés: $\text{char } R$.

Megjegyzés

A karakterisztika (ha véges), nem más, mint a gyűrűelemek **additív rendjeinek** legkisebb közös felső korlátja.

Példa

- ▶ $\text{char } \mathbb{C} = \text{char } \mathbb{R} = \text{char } \mathbb{Q} = \text{char } \mathbb{Z} = 0$
- ▶ $\text{char } \mathbb{Z}_n = n$
- ▶ $\text{char } R[x] = \text{char } R$
- ▶ $\text{char } R^{n \times n} = \text{char } R$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me =$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m =$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} =$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne =$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\ell a = a + \cdots + a =$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\ell a = a + \cdots + a = e \cdot a + \cdots + e \cdot a =$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\begin{aligned} \ell a &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= \end{aligned}$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $l \in \mathbb{N}$ esetén

$$\begin{aligned} la &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= le \cdot a \end{aligned}$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\begin{aligned} \ell a &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= \ell e \cdot a = 0 \iff \end{aligned}$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\begin{aligned} \ell a &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= \ell e \cdot a = 0 \iff \ell e = 0, \end{aligned}$$

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R,+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\begin{aligned} \ell a &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= \ell e \cdot a = 0 \iff \ell e = 0, \end{aligned}$$

tehát $o_{(R,+)}(a) = n$.

Tétel

Integritástartomány karakterisztikája megegyezik multiplikatív egységelemének additív rendjével, és a karakterisztika értéke csak nulla vagy prímszám lehet.

Biz.

Legyen $e \in R$ a multiplikatív egységelem, és legyen $n = o_{(R;+)}(e)$.

Tegyük fel, hogy n nem nulla és nem prím: $n = km$ ($1 < k, m < n$).

Ekkor $ke \neq 0$ és $me \neq 0$, viszont

$$ke \cdot me = \underbrace{(e + \cdots + e)}_k \cdot \underbrace{(e + \cdots + e)}_m = \underbrace{(e \cdot e + \cdots + e \cdot e)}_{km} = ne = 0,$$

ami ellentmond a zérusosztómentességnek.

Tetszőleges $0 \neq a \in R$ és $\ell \in \mathbb{N}$ esetén

$$\begin{aligned} \ell a &= a + \cdots + a = e \cdot a + \cdots + e \cdot a = (e + \cdots + e) \cdot a \\ &= \ell e \cdot a = 0 \iff \ell e = 0, \end{aligned}$$

tehát $o_{(R;+)}(a) = n$. Ebből rögtön következik, hogy $\text{char } R = n$. □

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Biz.

Trivi. (HF)



Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Biz.

Trivi. (HF)



Tétel

Ha a T test karakterisztikája p , akkor prímteste izomorf \mathbb{Z}_p -vel.

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Biz.

Trivi. (HF)



Tétel

Ha a T test karakterisztikája p , akkor prímteste izomorf \mathbb{Z}_p -vel.

Ha a T test karakterisztikája 0 , akkor prímteste izomorf \mathbb{Q} -val.

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Biz.

Trivi. (HF)



Tétel

Ha a T test karakterisztikája p , akkor prímteste izomorf \mathbb{Z}_p -vel.

Ha a T test karakterisztikája 0 , akkor prímteste izomorf \mathbb{Q} -val.

Biz.

A $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ leképezés gyűrűhomomorfizmus (itt $e \in T$ a multiplikatív egységelem):

Definíció

Az olyan testet, amelynek nincs valódi részteste **prímtestnek** nevezzük.

Állítás

Bármely T testben a multiplikatív egységelem által generált résztest prímtest, amelyet T prímtestének nevezünk. Ez a T test legszűkebb részteste.

Biz.

Trivi. (HF)



Tétel

Ha a T test karakterisztikája p , akkor prímteste izomorf \mathbb{Z}_p -vel.

Ha a T test karakterisztikája 0 , akkor prímteste izomorf \mathbb{Q} -val.

Biz.

A $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ leképezés gyűrűhomomorfizmus
(itt $e \in T$ a multiplikatív egységelem):

$$k\varphi + l\varphi = ke + le = (k+l)e = (k+l)\varphi;$$

$$k\varphi \cdot l\varphi = ke \cdot le = (k \cdot l)e = (k \cdot l)\varphi.$$

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi =$$

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} =$$

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi =$$

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\}$$

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

Biz. (folyt.)

Alkalmazzuk a homomorfizátételet a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_t T$.

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_t T$.

Ekkor T prímteste $\{0, e, 2e, \dots, (p-1)e\} \cong \mathbb{Z}_p$.

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_{\text{t}} T$.
Ekkor T prímteste $\{0, e, 2e, \dots, (p-1)e\} \cong \mathbb{Z}_p$.
- ▶ Ha $\text{char } T = 0$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(0) \cong \mathbb{Z}\varphi \leq_{\text{gy}} T$.

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_t T$.
Ekkor T prímteste $\{0, e, 2e, \dots, (p-1)e\} \cong \mathbb{Z}_p$.
- ▶ Ha $\text{char } T = 0$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(0) \cong \mathbb{Z}\varphi \leq_{\text{gy}} T$.
Nyilván $\mathbb{Z}/(0) \cong$

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z} : ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_t T$.

Ekkor T prímteste $\{0, e, 2e, \dots, (p-1)e\} \cong \mathbb{Z}_p$.

- ▶ Ha $\text{char } T = 0$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(0) \cong \mathbb{Z}\varphi \leq_{\text{gy}} T$.

Nyilván $\mathbb{Z}/(0) \cong \mathbb{Z}$, tehát T tartalmazza részgyűrűként \mathbb{Z} egy izomorf példányát

Biz. (folyt.)

Alkalmazzuk a homomorfizmatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z}: ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_t T$.

Ekkor T prímteste $\{0, e, 2e, \dots, (p-1)e\} \cong \mathbb{Z}_p$.

- ▶ Ha $\text{char } T = 0$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(0) \cong \mathbb{Z}\varphi \leq_{\text{gy}} T$.

Nyilván $\mathbb{Z}/(0) \cong \mathbb{Z}$, tehát T tartalmazza részgyűrűként \mathbb{Z} egy izomorf példányát, és így \mathbb{Z} hányadosteste, vagyis \mathbb{Q} egy izomorf példányát is.

Biz. (folyt.)

Alkalmazzuk a homomorfiatételt a $\varphi: \mathbb{Z} \rightarrow T, k \mapsto ke$ gyűrű-homomorfizmusra.

$$\ker \varphi = \{k \in \mathbb{Z} : ke = 0\} = (\text{char } T)$$

$$\mathbb{Z}\varphi = \{\dots, -2e, -e, 0, e, 2e, 3e, \dots\} \leq_{\text{gy}} T$$

- ▶ Ha $\text{char } T = p$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(p) \cong \mathbb{Z}\varphi \leq_t T$.

Ekkor T prímteste $\{0, e, 2e, \dots, (p-1)e\} \cong \mathbb{Z}_p$.

- ▶ Ha $\text{char } T = 0$, akkor $\mathbb{Z}/\ker \varphi = \mathbb{Z}/(0) \cong \mathbb{Z}\varphi \leq_{\text{gy}} T$.

Nyilván $\mathbb{Z}/(0) \cong \mathbb{Z}$, tehát T tartalmazza részgyűrűként \mathbb{Z} egy izomorf példányát, és így \mathbb{Z} hányadosteste, vagyis \mathbb{Q} egy izomorf példányát is.

Ekkor T prímteste $\left\{ \frac{ke}{me} : k, m \in \mathbb{Z}, m \neq 0 \right\} \cong \mathbb{Q}$.



1. Faktortest
2. Hányadostest
3. Karakterisztika, prímtest
4. Testbővítések

Ez a rész a tankönyvekben az [F] VI/1-5 fejezetekben található.

Definíció

- ▶ Az L testet a K test **bővítésének** nevezzük, ha K részteste L -nek.
Jelölés: $L | K$.

Definíció

- ▶ Az L testet a K test **bővítésének** nevezzük, ha K részteste L -nek.
Jelölés: $L | K$.
- ▶ Ha létezik véges sok $\alpha_1, \dots, \alpha_k$ elem úgy, hogy L megegyezik a $K \cup \{\alpha_1, \dots, \alpha_k\}$ halmaz által generált testtel, akkor azt mondjuk, hogy az $L | K$ bővítés **végesen generált**.
Jelölés: $L = K(\alpha_1, \dots, \alpha_n)$.

Definíció

- ▶ Az L testet a K test **bővítésének** nevezzük, ha K részteste L -nek.
Jelölés: $L | K$.
- ▶ Ha létezik véges sok $\alpha_1, \dots, \alpha_k$ elem úgy, hogy L megegyezik a $K \cup \{\alpha_1, \dots, \alpha_k\}$ halmaz által generált testtel, akkor azt mondjuk, hogy az $L | K$ bővítés **végeesen generált**.
Jelölés: $L = K(\alpha_1, \dots, \alpha_n)$.
- ▶ Ha létezik $\alpha \in L$ úgy, hogy $L = K(\alpha)$, akkor azt mondjuk, hogy $L | K$ **egyszerű bővítés**.

Definíció

- ▶ Az L testet a K test **bővítésének** nevezzük, ha K részteste L -nek.
Jelölés: $L | K$.
- ▶ Ha létezik véges sok $\alpha_1, \dots, \alpha_k$ elem úgy, hogy L megegyezik a $K \cup \{\alpha_1, \dots, \alpha_k\}$ halmaz által generált testtel, akkor azt mondjuk, hogy az $L | K$ bővítés **végeesen generált**.
Jelölés: $L = K(\alpha_1, \dots, \alpha_n)$.
- ▶ Ha létezik $\alpha \in L$ úgy, hogy $L = K(\alpha)$, akkor azt mondjuk, hogy $L | K$ **egyszerű bővítés**.
- ▶ Az $L_1 | K$ és $L_2 | K$ testbővítések közötti **izomorfizmuson** olyan $\varphi: L_1 \rightarrow L_2$ leképezést értünk, amelyre
 - ▶ $\varphi: L_1 \rightarrow L_2$ testizomorfizmus

Definíció

- ▶ Az L testet a K test **bővítésének** nevezzük, ha K részteste L -nek.
Jelölés: $L | K$.
- ▶ Ha létezik véges sok $\alpha_1, \dots, \alpha_k$ elem úgy, hogy L megegyezik a $K \cup \{\alpha_1, \dots, \alpha_k\}$ halmaz által generált testtel, akkor azt mondjuk, hogy az $L | K$ bővítés **végeesen generált**.
Jelölés: $L = K(\alpha_1, \dots, \alpha_n)$.
- ▶ Ha létezik $\alpha \in L$ úgy, hogy $L = K(\alpha)$, akkor azt mondjuk, hogy $L | K$ **egyszerű bővítés**.
- ▶ Az $L_1 | K$ és $L_2 | K$ testbővítések közötti **izomorfizmuson** olyan $\varphi: L_1 \rightarrow L_2$ leképezést értünk, amelyre
 - ▶ $\varphi: L_1 \rightarrow L_2$ testizomorfizmus
 - ▶ $\varphi|_K = \text{id}_K$, azaz minden $a \in K$ esetén $a\varphi = a$.

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF).



Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] =$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis:

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] =$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; egy bázis:

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; egy bázis: $1, \sqrt{2}$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; egy bázis: $1, \sqrt{2}$
- ▶ $[\mathbb{R} : \mathbb{Q}] =$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; egy bázis: $1, \sqrt{2}$
- ▶ $[\mathbb{R} : \mathbb{Q}] = \infty$

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; egy bázis: $1, \sqrt{2}$
- ▶ $[\mathbb{R} : \mathbb{Q}] = \infty$; egy lineárisan független rendszer:

Állítás

Ha $L \mid K$ testbővítés, akkor L vektorteret alkot K felett.

Biz.

Az L test műveletei adják a ${}_K L$ vektortér műveleteit:

- ▶ az $\alpha, \beta \in L$ vektorok összege: $\alpha + \beta \in L$;
- ▶ az $\alpha \in L$ vektornak a $c \in K$ skalárral való szorzata: $c\alpha \in L$.

Könnyű ellenőrizni, hogy a testaxiómákból következnek a vektortér-axiómák (HF). □

Definíció

Az ${}_K L$ vektortér dimenzióját az $L \mid K$ testbővítés **fokszámának** nevezzük. Jelölés: $[L : K] := \dim_K L$.

Példa

- ▶ $[\mathbb{C} : \mathbb{R}] = 2$; egy bázis: $1, i$
- ▶ $[\mathbb{Q}(\sqrt{2}) : \mathbb{Q}] = 2$; egy bázis: $1, \sqrt{2}$
- ▶ $[\mathbb{R} : \mathbb{Q}] = \infty$; egy lineárisan független rendszer: $1, \pi, \pi^2, \pi^3, \dots$

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek.

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek.

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Az ${}_K L$ vektortér egy bázisa: $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. (világos)

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Az ${}_K L$ vektortér egy bázisa: $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. (világos)

Az ${}_L M$ vektortér egy bázisa: $\beta_1 = 1$, $\beta_2 = i$. (majd később világos lesz)

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Az ${}_K L$ vektortér egy bázisa: $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. (világos)

Az ${}_L M$ vektortér egy bázisa: $\beta_1 = 1$, $\beta_2 = i$. (majd később világos lesz)

Az ${}_K M$ vektortér egy bázisa:

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Az ${}_K L$ vektortér egy bázisa: $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. (világos)

Az ${}_L M$ vektortér egy bázisa: $\beta_1 = 1$, $\beta_2 = i$. (majd később világos lesz)

Az ${}_K M$ vektortér egy bázisa:

$$\alpha_1 \beta_1 = 1, \alpha_2 \beta_1 = \sqrt{2}, \alpha_1 \beta_2 = i, \alpha_2 \beta_2 = \sqrt{2}i.$$

Tétel (fokszámtétel)

Bármely $K \leq L \leq M$ testtoronyra $[M : K] = [M : L] \cdot [L : K]$.

Biz. (csak véges fokszámokra).

Legyen $\alpha_1, \dots, \alpha_n$ bázisa az ${}_K L$ vektortérnek és β_1, \dots, β_m bázisa az ${}_L M$ vektortérnek. Ekkor $\alpha_i \beta_j$ ($i = 1, \dots, n; j = 1, \dots, m$) bázisa az ${}_K M$ vektortérnek. (HF [F] VI/1.) □

Példa

Legyen $K = \mathbb{Q}$, $L = \mathbb{Q}(\sqrt{2})$, $M = L(i) = \mathbb{Q}(\sqrt{2}, i)$.

Az ${}_K L$ vektortér egy bázisa: $\alpha_1 = 1$, $\alpha_2 = \sqrt{2}$. (világos)

Az ${}_L M$ vektortér egy bázisa: $\beta_1 = 1$, $\beta_2 = i$. (majd később világos lesz)

Az ${}_K M$ vektortér egy bázisa:

$$\alpha_1 \beta_1 = 1, \alpha_2 \beta_1 = \sqrt{2}, \alpha_1 \beta_2 = i, \alpha_2 \beta_2 = \sqrt{2}i.$$

Az ${}_K M$ vektortér egy tetszőleges elemének felírása ebben a bázisban:

$$a + b\sqrt{2} + ci + d\sqrt{2}i \quad (a, b, c, d \in \mathbb{Q})$$

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét.

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong$

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p =$

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.
Ekkor T végesdimenziós vektortér K felett.

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Tétel

Ha T véges test, akkor T elemszáma prímszám.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$.



Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámúra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámúra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

▶ $\mathbb{Z}_p \cong$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámra létezik q elemszámú test, és ez a test izomorfiá erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámú testre létezik q elemszámú test, és ez a test izomorfiá erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$,
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1) \cong$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámúra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$,
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1) \cong \text{GF}(4)$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámúra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$,
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1) \cong \text{GF}(4)$,
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1) \cong$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámúra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$,
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1) \cong \text{GF}(4)$,
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1) \cong \text{GF}(8)$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$,
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1) \cong \text{GF}(4)$,
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1) \cong \text{GF}(8)$,
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1) \cong$

Tétel

Ha T véges test, akkor T elemszáma prímszámú.

Biz.

Jelölje K a T test prímtestét. Mivel T véges, $K \cong \mathbb{Z}_p$, ahol $p = \text{char } T$.

Ekkor T végesdimenziós vektortér K felett. Ha $\dim_K T = n$, akkor T izomorf a \mathbb{Z}_p feletti elem n -esek vektorterével (az izomorfizmust egy rögzített bázisbeli koordinátasorok adják).

Következésképp $|T| = p^n$. □

Megjegyzés

Minden q prímszámúra létezik q elemszámú test, és ez a test izomorfia erejéig egyértelműen meghatározott. Jelölés: $\text{GF}(q)$.

Például

- ▶ $\mathbb{Z}_p \cong \text{GF}(p)$,
- ▶ $\mathbb{Z}_2[x] / (x^2 + x + 1) \cong \text{GF}(4)$,
- ▶ $\mathbb{Z}_2[x] / (x^3 + x + 1) \cong \text{GF}(8)$,
- ▶ $\mathbb{Z}_3[x] / (x^2 + 1) \cong \text{GF}(9)$, stb.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\}$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\}$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\}$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Biz.

1. Az világos, hogy minden $f(\alpha)$ ($f \in K[x]$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alapművelettel.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Biz.

1. Az világos, hogy minden $f(\alpha)$ ($f \in K[x]$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt az első három alpműveletre,

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Biz.

1. Az világos, hogy minden $f(\alpha)$ ($f \in K[x]$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt az első három alpműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált részgyűrű.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Biz.

1. Az világos, hogy minden $f(\alpha)$ ($f \in K[x]$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt az első három alpműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált részgyűrű.

2. Az világos, hogy minden $t(\alpha)$ ($t \in K(x)$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból a négy alpművelettel.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Biz.

1. Az világos, hogy minden $f(\alpha)$ ($f \in K[x]$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt az első három alpműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált részgyűrű.

2. Az világos, hogy minden $t(\alpha)$ ($t \in K(x)$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból a négy alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt a négy alpműveletre,

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén

1. A $K \cup \{\alpha\}$ halmaz által generált részgyűrű:

$$\{f(\alpha) : f \in K[x]\} =: K[\alpha].$$

2. A $K \cup \{\alpha\}$ halmaz által generált résztest:

$$\left\{ \frac{f(\alpha)}{g(\alpha)} : f, g \in K[x], g(\alpha) \neq 0 \right\} = \{t(\alpha) : t \in K(x)\} =: K(\alpha).$$

Biz.

1. Az világos, hogy minden $f(\alpha)$ ($f \in K[x]$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból az első három alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt az első három alpműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált részgyűrű.

2. Az világos, hogy minden $t(\alpha)$ ($t \in K(x)$) alakú elem előállítható a $K \cup \{\alpha\}$ halmazból a négy alpművelettel.

Másrészt az is világos, hogy ezen elemek halmaza már zárt a négy alpműveletre, tehát ez lesz a $K \cup \{\alpha\}$ halmaz által generált résztest.



Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $G_{\alpha} := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $G_{y_\alpha} := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $G_{\alpha} := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $G_{\alpha} \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

(1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(1) \implies (2): Tegyük fel, hogy $(f) = Gy_\alpha$.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(1) \implies (2): Tegyük fel, hogy $(f) = Gy_\alpha$. Ekkor nyilván $f(\alpha) = 0$.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(1) \implies (2): Tegyük fel, hogy $(f) = Gy_\alpha$. Ekkor nyilván $f(\alpha) = 0$.

Ha $0 \neq g \in K[x]$ és $g(\alpha) = 0$, akkor

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(1) \implies (2): Tegyük fel, hogy $(f) = Gy_\alpha$. Ekkor nyilván $f(\alpha) = 0$.

Ha $0 \neq g \in K[x]$ és $g(\alpha) = 0$, akkor

$$g \in Gy_\alpha \implies f \mid g \implies \deg f \leq \deg g,$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(1) \implies (2): Tegyük fel, hogy $(f) = Gy_\alpha$. Ekkor nyilván $f(\alpha) = 0$.

Ha $0 \neq g \in K[x]$ és $g(\alpha) = 0$, akkor

$$g \in Gy_\alpha \implies f \mid g \implies \deg f \leq \deg g,$$

tehát f fokszáma valóban minimális.



Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(2) \implies (3): Tegyük fel, hogy f minimális fokszámú, de nem irreducibilis:

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(2) \implies (3): Tegyük fel, hogy f minimális fokszámú, de nem irreducibilis: $f = gh$ ($\deg g, \deg h < \deg f$).

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(2) \implies (3): Tegyük fel, hogy f minimális fokszámú, de nem irreducibilis: $f = gh$ ($\deg g, \deg h < \deg f$). Ekkor

$$f(\alpha) = g(\alpha)h(\alpha) = 0 \implies g(\alpha) = 0 \text{ vagy } h(\alpha) = 0,$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(2) \implies (3): Tegyük fel, hogy f minimális fokszámú, de nem irreducibilis: $f = gh$ ($\deg g, \deg h < \deg f$). Ekkor

$$f(\alpha) = g(\alpha)h(\alpha) = 0 \implies g(\alpha) = 0 \text{ vagy } h(\alpha) = 0,$$

ami ellentmond

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(2) \implies (3): Tegyük fel, hogy f minimális fokszámú, de nem irreducibilis: $f = gh$ ($\deg g, \deg h < \deg f$). Ekkor

$$f(\alpha) = g(\alpha)h(\alpha) = 0 \implies g(\alpha) = 0 \text{ vagy } h(\alpha) = 0,$$

ami ellentmond $\deg f$ minimalitásának.



Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(3) \implies (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(3) \implies (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

$$f(\alpha) = 0 \implies (f) \subseteq Gy_\alpha$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(3) \implies (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

$$f(\alpha) = 0 \implies (f) \subseteq Gy_\alpha$$

$$f \text{ irred.} \implies$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(3) \implies (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

$$f(\alpha) = 0 \implies (f) \subseteq Gy_\alpha$$

$$f \text{ irred.} \implies (f) \text{ max. ideál}$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(3) \implies (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

$$\left. \begin{array}{l} f(\alpha) = 0 \implies (f) \subseteq Gy_\alpha \\ f \text{ irred.} \implies (f) \text{ max. ideál} \end{array} \right\} \implies$$

Állítás

Tetszőleges $\alpha \in L \mid K$ esetén $Gy_\alpha := \{f \in K[x] : f(\alpha) = 0\} \triangleleft K[x]$.

Biz.

HF



Állítás

Legyen $\alpha \in L \mid K$ és tegyük fel, hogy $Gy_\alpha \neq \{0\}$. Ekkor bármely $f \in K[x]$ polinomra az alábbi három állítás ekvivalens.

- (1) Az f polinom generálja a Gy_α ideált: $(f) = Gy_\alpha$.
- (2) Az f polinom minimális fokszámú azon nemnulla polinomok között, amelyeknek α gyöke.
- (3) Az f polinom irreducibilis K felett, és α gyöke f -nek.

Biz.

(3) \implies (1): Tegyük fel, hogy $f(\alpha) = 0$ és f irreducibilis.

$$\left. \begin{array}{l} f(\alpha) = 0 \implies (f) \subseteq Gy_\alpha \\ f \text{ irred.} \implies (f) \text{ max. ideál} \end{array} \right\} \implies (f) = Gy_\alpha \text{ vagy } Gy_\alpha = K[x]. \quad \square$$

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.

A Gy_α ideált generáló **fő**polinomot (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.

A Gy_α ideált generáló **fő**polinomot (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **fő**polinomot (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **fő**polinomot (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} =$

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $G_{y_\alpha} \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A G_{y_α} ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $G_{y_\alpha} = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} =$

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.
- ▶ $i \in \mathbb{C} \mid \mathbb{Q}(\sqrt{2})$

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.
- ▶ $i \in \mathbb{C} \mid \mathbb{Q}(\sqrt{2})$ másodfokú algebrai elem: $m_{i,\mathbb{Q}(\sqrt{2})} = x^2 + 1$.

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.
- ▶ $i \in \mathbb{C} \mid \mathbb{Q}(\sqrt{2})$ másodfokú algebrai elem: $m_{i,\mathbb{Q}(\sqrt{2})} = x^2 + 1$.
- ▶ Ha $z \in \mathbb{C} \setminus \mathbb{R}$, akkor z

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.
- ▶ $i \in \mathbb{C} \mid \mathbb{Q}(\sqrt{2})$ másodfokú algebrai elem: $m_{i,\mathbb{Q}(\sqrt{2})} = x^2 + 1$.
- ▶ Ha $z \in \mathbb{C} \setminus \mathbb{R}$, akkor z másodfokú algebrai elem \mathbb{R} felett:
 $m_{z,\mathbb{R}} =$

Definíció

Legyen $\alpha \in L \mid K$.

- ▶ Ha $Gy_\alpha \neq \{0\}$, akkor azt mondjuk, hogy α **algebrai** K felett.
A Gy_α ideált generáló **főpolinomot** (mely egyértelműen meghatározott), az α elem K feletti **minimálpolinomjának** nevezzük. Jelölés: $m_{\alpha,K}$. Az $m_{\alpha,K}$ polinom fokszámát az α **algebrai elem fokszámának** nevezzük.
- ▶ Ha $Gy_\alpha = \{0\}$, akkor azt mondjuk, hogy α **transzcendens** K felett.
- ▶ A $\mathbb{C} \mid \mathbb{Q}$ testbővítés algebrai illetve transzcendens elemeit **algebrai számoknak** illetve **transzcendens számoknak** nevezzük.

Példa

- ▶ Ha $\alpha \in K$, akkor (és csak akkor) α elsőfokú algebrai elem:
 $m_{\alpha,K} = x - \alpha$.
- ▶ $i \in \mathbb{C} \mid \mathbb{R}$ másodfokú algebrai elem: $m_{i,\mathbb{R}} = x^2 + 1$.
- ▶ $i \in \mathbb{C} \mid \mathbb{Q}(\sqrt{2})$ másodfokú algebrai elem: $m_{i,\mathbb{Q}(\sqrt{2})} = x^2 + 1$.
- ▶ Ha $z \in \mathbb{C} \setminus \mathbb{R}$, akkor z másodfokú algebrai elem \mathbb{R} felett:
 $m_{z,\mathbb{R}} = x^2 - 2 \operatorname{Re} z \cdot x + |z|^2$.

Példa

▶ $\sqrt{2}$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2}, \mathbb{Q}} =$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2}, \mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} =$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám.

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} =$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$
- ▶ $\alpha \in \mathbb{R} \implies m_{\alpha,\mathbb{R}} =$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$
- ▶ $\alpha \in \mathbb{R} \implies m_{\alpha,\mathbb{R}} = x - \alpha$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$
- ▶ $\alpha \in \mathbb{R} \implies m_{\alpha,\mathbb{R}} = x - \alpha$
- ▶ $(\alpha - 4)^2 = 3$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2}, \mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2}, \mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$
- ▶ $\alpha \in \mathbb{R} \implies m_{\alpha, \mathbb{R}} = x - \alpha$
- ▶ $(\alpha - 4)^2 = 3 \implies \alpha^2 - 8\alpha + 13 = 0$

Példa

- ▶ $\sqrt{2}$ másodfokú algebrai szám: $m_{\sqrt{2},\mathbb{Q}} = x^2 - 2$.
- ▶ $\sqrt[n]{2}$ n -edfokú algebrai szám: $m_{\sqrt[n]{2},\mathbb{Q}} = x^n - 2$ (miért irreducibilis?).
- ▶ π és e transzcendens számok.
- ▶ A Liouville-féle $\sum \frac{1}{10^{n!}}$ konstans transzcendens szám.
- ▶ Ha $\alpha \neq 0, 1$ és $\beta \notin \mathbb{Q}$ algebrai számok, akkor α^β transzcendens szám. Például $2^{\sqrt{2}}$, $\sqrt{2}^{\sqrt{2}}$ és $e^{-\pi/2} = i^i$ transzcendens számok.

Példa

Határozzuk meg $\alpha = 4 - \sqrt{3}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha,\mathbb{C}} = x - \alpha$
- ▶ $\alpha \in \mathbb{R} \implies m_{\alpha,\mathbb{R}} = x - \alpha$
- ▶ $(\alpha - 4)^2 = 3 \implies \alpha^2 - 8\alpha + 13 = 0 \implies m_{\alpha,\mathbb{Q}} = x^2 - 8x + 13$
(miért irreducibilis?)

Példa

Határozzuk meg $\alpha = i\sqrt{2} - \sqrt{2}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

Példa

Határozzuk meg $\alpha = i\sqrt{2} - \sqrt{2}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

► $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$

Példa

Határozzuk meg $\alpha = i\sqrt{2 - \sqrt{2}}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$

▶ $\alpha^2 = -(2 - \sqrt{2})$

Példa

Határozzuk meg $\alpha = i\sqrt{2 - \sqrt{2}}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$

▶ $\alpha^2 = -(2 - \sqrt{2}) \implies \alpha^2 + 2 - \sqrt{2} = 0$

Példa

Határozzuk meg $\alpha = i\sqrt{2 - \sqrt{2}}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$

▶ $\alpha^2 = -(2 - \sqrt{2}) \implies \alpha^2 + 2 - \sqrt{2} = 0 \implies m_{\alpha, \mathbb{R}} = x^2 + 2 - \sqrt{2}$
(miért irreducibilis?)

Példa

Határozzuk meg $\alpha = i\sqrt{2 - \sqrt{2}}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$
- ▶ $\alpha^2 = -(2 - \sqrt{2}) \implies \alpha^2 + 2 - \sqrt{2} = 0 \implies m_{\alpha, \mathbb{R}} = x^2 + 2 - \sqrt{2}$
(miért irreducibilis?)
- ▶ $(\alpha^2 + 2)^2 = 2$

Példa

Határozzuk meg $\alpha = i\sqrt{2 - \sqrt{2}}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$
- ▶ $\alpha^2 = -(2 - \sqrt{2}) \implies \alpha^2 + 2 - \sqrt{2} = 0 \implies m_{\alpha, \mathbb{R}} = x^2 + 2 - \sqrt{2}$
(miért irreducibilis?)
- ▶ $(\alpha^2 + 2)^2 = 2 \implies \alpha^4 + 4\alpha^2 + 2 = 0$

Példa

Határozzuk meg $\alpha = i\sqrt{2 - \sqrt{2}}$ minimálpolinomját \mathbb{C} , \mathbb{R} és \mathbb{Q} felett.

- ▶ $\alpha \in \mathbb{C} \implies m_{\alpha, \mathbb{C}} = x - \alpha$
- ▶ $\alpha^2 = -(2 - \sqrt{2}) \implies \alpha^2 + 2 - \sqrt{2} = 0 \implies m_{\alpha, \mathbb{R}} = x^2 + 2 - \sqrt{2}$
(miért irreducibilis?)
- ▶ $(\alpha^2 + 2)^2 = 2 \implies \alpha^4 + 4\alpha^2 + 2 = 0 \implies m_{\alpha, \mathbb{Q}} = x^4 + 4x^2 + 2$
(miért irreducibilis?)

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i$$

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8$$

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak.

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \quad \bar{\alpha} = \sqrt{2} - i, \quad -\alpha = -\sqrt{2} - i, \quad -\bar{\alpha} = -\sqrt{2} + i;$$

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \quad \bar{\alpha} = \sqrt{2} - i, \quad -\alpha = -\sqrt{2} - i, \quad -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \bar{\alpha} = \sqrt{2} - i, -\alpha = -\sqrt{2} - i, -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja:

$$(x - \alpha)(x - \bar{\alpha}) \cdot (x + \alpha)(x + \bar{\alpha});$$

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \bar{\alpha} = \sqrt{2} - i, -\alpha = -\sqrt{2} - i, -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja:

$$(x - \alpha)(x - \bar{\alpha}) \cdot (x + \alpha)(x + \bar{\alpha});$$

- ▶ \mathbb{R} feletti irreducibilis faktorizációja:

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \bar{\alpha} = \sqrt{2} - i, -\alpha = -\sqrt{2} - i, -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja:

$$(x - \alpha)(x - \bar{\alpha}) \cdot (x + \alpha)(x + \bar{\alpha});$$

- ▶ \mathbb{R} feletti irreducibilis faktorizációja:

$$(x^2 - 2\sqrt{2}x + 3) \cdot (x^2 + 2\sqrt{2}x + 3);$$

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \bar{\alpha} = \sqrt{2} - i, -\alpha = -\sqrt{2} - i, -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja:

$$(x - \alpha)(x - \bar{\alpha}) \cdot (x + \alpha)(x + \bar{\alpha});$$

- ▶ \mathbb{R} feletti irreducibilis faktorizációja:

$$(x^2 - 2\sqrt{2}x + 3) \cdot (x^2 + 2\sqrt{2}x + 3);$$

- ▶ \mathbb{Q} feletti irreducibilis faktorizációja:

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \bar{\alpha} = \sqrt{2} - i, -\alpha = -\sqrt{2} - i, -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja:

$$(x - \alpha)(x - \bar{\alpha}) \cdot (x + \alpha)(x + \bar{\alpha});$$

- ▶ \mathbb{R} feletti irreducibilis faktorizációja:

$$(x^2 - 2\sqrt{2}x + 3) \cdot (x^2 + 2\sqrt{2}x + 3);$$

- ▶ \mathbb{Q} feletti irreducibilis faktorizációja: $x^4 - 2x^2 + 9$.

Példa

Határozzuk meg az $\alpha = \sqrt{2} + i$ algebrai szám \mathbb{Q} feletti minimálpolinomját.

$$\alpha^2 = 1 + 2\sqrt{2}i \implies (\alpha^2 - 1)^2 = -8 \implies \alpha^4 - 2\alpha^2 + 9 = 0$$

Tehát α gyöke az $x^4 - 2x^2 + 9$ polinomnak. Ez irreducibilis \mathbb{Q} felett?

Az $x^4 - 2x^2 + 9$ polinom

- ▶ komplex gyökei:

$$\alpha = \sqrt{2} + i, \bar{\alpha} = \sqrt{2} - i, -\alpha = -\sqrt{2} - i, -\bar{\alpha} = -\sqrt{2} + i;$$

- ▶ \mathbb{C} feletti irreducibilis faktorizációja:

$$(x - \alpha)(x - \bar{\alpha}) \cdot (x + \alpha)(x + \bar{\alpha});$$

- ▶ \mathbb{R} feletti irreducibilis faktorizációja:

$$(x^2 - 2\sqrt{2}x + 3) \cdot (x^2 + 2\sqrt{2}x + 3);$$

- ▶ \mathbb{Q} feletti irreducibilis faktorizációja: $x^4 - 2x^2 + 9$.

Tehát $m_{\alpha, \mathbb{Q}} = x^4 - 2x^2 + 9$.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$, értékkészlete pedig $K(\alpha)$.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$, értékkészlete pedig $K(\alpha)$. A homomorfizmatétel szerint $K(x) \cong K(x) / (0) \cong K(\alpha)$

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$, értékkészlete pedig $K(\alpha)$.

A homomorfiatétel szerint $K(x) \cong K(x) / (0) \cong K(\alpha)$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$, értékkészlete pedig $K(\alpha)$.

A homomorfizmatétel szerint $K(x) \cong K(x) / (0) \cong K(\alpha)$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Minden $c \in K$ esetén $c\varphi = c(\alpha) = c$

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(1): Ha $t = \frac{f}{g} \in K(x)$, akkor $t(\alpha)$ értelmezett, mert α transzcendenciája miatt $g(\alpha) \neq 0$. Így definiálhatjuk a

$$\psi: K(x) \rightarrow L, t \mapsto t(\alpha)$$

homomorfizmust. Ennek magja $\{0\}$, értékkészlete pedig $K(\alpha)$.

A homomorfizmatétel szerint $K(x) \cong K(x)/(0) \cong K(\alpha)$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Minden $c \in K$ esetén $c\varphi = c(\alpha) = c$, tehát φ nem csak a $K(x)$ és $K(\alpha)$ testek, de a $K(x) \mid K$ és $K(\alpha) \mid K$ testbővítések között is izomorfizmust létesít.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2):

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tehát $[K(\alpha) : K] = \infty$.

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tehát $[K(\alpha) : K] = \infty$.

Konkrétabban:

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tehát $[K(\alpha) : K] = \infty$.

Konkrétabban: ha $1, \alpha, \alpha^2, \alpha^3, \dots$ lineárisan összefüggő lenne, akkor

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tehát $[K(\alpha) : K] = \infty$.

Konkrétabban: ha $1, \alpha, \alpha^2, \alpha^3, \dots$ lineárisan összefüggő lenne, akkor valamelyik tagja előállna az őt megelőző tagok lineáris kombinációjaként:

$$\alpha^{k+1} = c_k \alpha^k + \dots + c_1 \alpha + c_0 1 \quad (c_0, c_1, \dots, c_k \in K).$$

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tehát $[K(\alpha) : K] = \infty$.

Konkrétabban: ha $1, \alpha, \alpha^2, \alpha^3, \dots$ lineárisan összefüggő lenne, akkor valamelyik tagja előállna az öt megelőző tagok lineáris kombinációjaként:

$$\alpha^{k+1} = c_k \alpha^k + \dots + c_1 \alpha + c_0 \mathbf{1} \quad (c_0, c_1, \dots, c_k \in K).$$

Ekkor α gyöke lenne a nemzéró $x^{k+1} - c_k x^k - \dots - c_1 x - c_0 \in K[x]$ polinomnak

Tétel

Ha $\alpha \in L \mid K$ transzcendens K felett, akkor

(1) $K(\alpha) \mid K \cong K(x) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(x) \rightarrow K(\alpha), t \mapsto t(\alpha);$$

(2) $[K(\alpha) : K] = \infty$.

Biz.

(2): Az $1, x, x^2, x^3, \dots$ vektorrendszer lineárisan független a ${}_K K(x)$ vektortérben, ezért ennek φ melletti képe, azaz $1, \alpha, \alpha^2, \alpha^3, \dots$ is lineárisan független vektorrendszer a ${}_K K(\alpha)$ vektortérben.

Tehát $[K(\alpha) : K] = \infty$.

Konkrétabban: ha $1, \alpha, \alpha^2, \alpha^3, \dots$ lineárisan összefüggő lenne, akkor valamelyik tagja előállna az öt megelőző tagok lineáris kombinációjaként:

$$\alpha^{k+1} = c_k \alpha^k + \dots + c_1 \alpha + c_0 \mathbf{1} \quad (c_0, c_1, \dots, c_k \in K).$$

Ekkor α gyöke lenne a nemzéró $x^{k+1} - c_k x^k - \dots - c_1 x - c_0 \in K[x]$ polinomnak, ami ellentmond α transzcendenciájának. □

Következmény

Test egyszerű transzcendens bővítése izomorfia erejéig egyértelműen meghatározott.

Ha $K(\alpha) \mid K$ és $K(\beta) \mid K$ egyszerű transzcendens bővítések, akkor $K(\alpha) \mid K \cong K(\beta) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(\alpha) \rightarrow K(\beta), t(\alpha) \mapsto t(\beta) \quad (t \in K(x)).$$

Következmény

Test egyszerű transzcendens bővítése izomorfia erejéig egyértelműen meghatározott.

Ha $K(\alpha) | K$ és $K(\beta) | K$ egyszerű transzcendens bővítések, akkor $K(\alpha) | K \cong K(\beta) | K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(\alpha) \rightarrow K(\beta), t(\alpha) \mapsto t(\beta) \quad (t \in K(x)).$$

Biz.

Tudjuk, hogy $K(\alpha) | K \cong K(x) | K \cong K(\beta) | K$:

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\sigma} & K(x) & \xrightarrow{\tau} & K(\beta) \\ t(\alpha) & \longleftarrow & t & \longrightarrow & t(\beta) \end{array}$$

Következmény

Test egyszerű transzcendens bővítése izomorfia erejéig egyértelműen meghatározott.

Ha $K(\alpha) | K$ és $K(\beta) | K$ egyszerű transzcendens bővítések, akkor $K(\alpha) | K \cong K(\beta) | K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(\alpha) \rightarrow K(\beta), t(\alpha) \mapsto t(\beta) \quad (t \in K(x)).$$

Biz.

Tudjuk, hogy $K(\alpha) | K \cong K(x) | K \cong K(\beta) | K$:

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\sigma} & K(x) & \xrightarrow{\tau} & K(\beta) \\ t(\alpha) & \longleftarrow & t & \longmapsto & t(\beta) \end{array}$$

A két izomorfizmust „összevarrva” kapjuk a $\varphi = \sigma^{-1}\tau$ izomorfizmust:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sigma^{-1}\tau} & K(\beta) \\ t(\alpha) & \longmapsto & t(\beta) \end{array}$$



Következmény

Minden K testnek létezik egyszerű transzcendens bővítése, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Következmény

Minden K testnek létezik egyszerű transzcendens bővítése, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk

Következmény

Minden K testnek létezik egyszerű transzcendens bővítése, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk
- ▶ egzisztencia:

Következmény

Minden K testnek létezik egyszerű transzcendens bővítése, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk
- ▶ egzisztencia: $K(x)$



Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(0) & (1):

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha,K})$

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) \quad K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) \quad [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $G_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) \quad K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) \quad [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$.

A homomorfiatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$. A homomorfiatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$.

A homomorfiatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha, K}$ irreducibilis, $K[x] / (m_{\alpha, K})$

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) \quad K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) \quad [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$.

A homomorfiatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha, K}$ irreducibilis, $K[x] / (m_{\alpha, K})$ test

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) \quad K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) \quad [K(\alpha) : K] = \deg m_{\alpha,K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha,K})$, értékkészlete pedig $K[\alpha]$.

A homomorfiatétel szerint $K[x] / (m_{\alpha,K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha,K}$ irreducibilis, $K[x] / (m_{\alpha,K})$ test, így $K[\alpha]$ is az.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$. A homomorfiatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha, K}$ irreducibilis, $K[x] / (m_{\alpha, K})$ test, így $K[\alpha]$ is az. Következésképp $K[\alpha] = K(\alpha)$.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$. A homomorfiatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha, K}$ irreducibilis, $K[x] / (m_{\alpha, K})$ test, így $K[\alpha]$ is az. Következésképp $K[\alpha] = K(\alpha)$.

Minden $c \in K$ esetén $\bar{c}\varphi = c(\alpha) = c$

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(0) & (1): Tekintsük a

$$\psi: K[x] \rightarrow L, f \mapsto f(\alpha)$$

homomorfizmust. Ennek magja $Gy_{\alpha} = (m_{\alpha, K})$, értékkészlete pedig $K[\alpha]$. A homomorfizmatétel szerint $K[x] / (m_{\alpha, K}) \cong K[\alpha]$; a megfelelő izomorfizmus éppen a fenti φ leképezés.

Mivel $m_{\alpha, K}$ irreducibilis, $K[x] / (m_{\alpha, K})$ test, így $K[\alpha]$ is az. Következésképp $K[\alpha] = K(\alpha)$.

Minden $c \in K$ esetén $\bar{c}\varphi = c(\alpha) = c$, tehát φ a megfelelő testbővítések között is izomorfizmust létesít.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha, K}$.

Biz.

(2):

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x]/(m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x]/(m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(2): Legyen $n = \deg m_{\alpha,K}$.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

(0) $K(\alpha) = K[\alpha]$

(1) $K(\alpha) \mid K \cong K[x]/(m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x]/(m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

(2) $[K(\alpha) : K] = \deg m_{\alpha,K}$.

Biz.

(2): Legyen $n = \deg m_{\alpha,K}$. A $K[x]/(m_{\alpha,K})$ test elemei egyértelműen előállnak

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = a_{n-1}\bar{x}^{n-1} + \cdots + a_1\bar{x} + a_0 \quad (a_0, a_1, \dots, a_{n-1} \in K)$$

alakban.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) \quad K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x]/(m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x]/(m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) \quad [K(\alpha) : K] = \deg m_{\alpha,K}.$$

Biz.

(2): Legyen $n = \deg m_{\alpha,K}$. A $K[x]/(m_{\alpha,K})$ test elemei egyértelműen előállnak

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = a_{n-1}\bar{x}^{n-1} + \cdots + a_1\bar{x} + a_0 \quad (a_0, a_1, \dots, a_{n-1} \in K)$$

alakban.

Ez azt jelenti, hogy $1, \bar{x}, \dots, \bar{x}^{n-1}$ bázisa a K feletti $K[x]/(m_{\alpha,K})$ vektortérnek.

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x]/(m_{\alpha,K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x]/(m_{\alpha,K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha,K}.$$

Biz.

(2): Legyen $n = \deg m_{\alpha,K}$. A $K[x]/(m_{\alpha,K})$ test elemei egyértelműen előállnak

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = a_{n-1}\bar{x}^{n-1} + \cdots + a_1\bar{x} + a_0 \quad (a_0, a_1, \dots, a_{n-1} \in K)$$

alakban.

Ez azt jelenti, hogy $1, \bar{x}, \dots, \bar{x}^{n-1}$ bázisa a K feletti $K[x]/(m_{\alpha,K})$ vektortérnek. Ezen bázis φ melletti képe, azaz

Tétel

Ha $\alpha \in L \mid K$ algebrai K felett, akkor

$$(0) K(\alpha) = K[\alpha]$$

(1) $K(\alpha) \mid K \cong K[x] / (m_{\alpha, K}) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K[x] / (m_{\alpha, K}) \rightarrow K(\alpha), \bar{f} \mapsto f(\alpha);$$

$$(2) [K(\alpha) : K] = \deg m_{\alpha, K}.$$

Biz.

(2): Legyen $n = \deg m_{\alpha, K}$. A $K[x] / (m_{\alpha, K})$ test elemei egyértelműen előállnak

$$\overline{a_{n-1}x^{n-1} + \cdots + a_1x + a_0} = a_{n-1}\bar{x}^{n-1} + \cdots + a_1\bar{x} + a_0 \quad (a_0, a_1, \dots, a_{n-1} \in K)$$

alakban.

Ez azt jelenti, hogy $1, \bar{x}, \dots, \bar{x}^{n-1}$ bázisa a K feletti $K[x] / (m_{\alpha, K})$ vektortérnek. Ezen bázis φ melletti képe, azaz $1, \alpha, \dots, \alpha^{n-1}$ bázisa a ${}_K K(\alpha)$ vektortérnek. □

Következmény

Test egyszerű algebrai bővítését izomorfia erejéig egyértelműen meghatározza az adjungált elem minimálpolinomja.

Ha $K(\alpha) \mid K$ és $K(\beta) \mid K$ egyszerű algebrai bővítések és $m_{\alpha,K} = m_{\beta,K} = m \in K[x]$, akkor $K(\alpha) \mid K \cong K(\beta) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(\alpha) \rightarrow K(\beta), f(\alpha) \mapsto f(\beta) \quad (f \in K[x], \deg f \leq n-1).$$

Következmény

Test egyszerű algebrai bővítését izomorfia erejéig egyértelműen meghatározza az adjungált elem minimálpolinomja.

Ha $K(\alpha) | K$ és $K(\beta) | K$ egyszerű algebrai bővítések és $m_{\alpha,K} = m_{\beta,K} = m \in K[x]$, akkor $K(\alpha) | K \cong K(\beta) | K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(\alpha) \rightarrow K(\beta), f(\alpha) \mapsto f(\beta) \quad (f \in K[x], \deg f \leq n-1).$$

Biz.

Tudjuk, hogy $K(\alpha) | K \cong K[x]/(m) | K \cong K(\beta) | K$:

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\sigma} & K[x]/(m) | K & \xrightarrow{\tau} & K(\beta) \\ f(\alpha) & \longleftarrow & f & \longmapsto & f(\beta) \end{array}$$

Következmény

Test egyszerű algebrai bővítését izomorfia erejéig egyértelműen meghatározza az adjungált elem minimálpolinomja.

Ha $K(\alpha) \mid K$ és $K(\beta) \mid K$ egyszerű algebrai bővítések és $m_{\alpha,K} = m_{\beta,K} = m \in K[x]$, akkor $K(\alpha) \mid K \cong K(\beta) \mid K$ az alábbi φ izomorfizmus mellett:

$$\varphi: K(\alpha) \rightarrow K(\beta), f(\alpha) \mapsto f(\beta) \quad (f \in K[x], \deg f \leq n-1).$$

Biz.

Tudjuk, hogy $K(\alpha) \mid K \cong K[x]/(m) \mid K \cong K(\beta) \mid K$:

$$\begin{array}{ccccc} K(\alpha) & \xleftarrow{\sigma} & K[x]/(m) \mid K & \xrightarrow{\tau} & K(\beta) \\ f(\alpha) & \longleftarrow & f & \longmapsto & f(\beta) \end{array}$$

A két izomorfizmust „összevarrva” kapjuk a $\varphi = \sigma^{-1}\tau$ izomorfizmust:

$$\begin{array}{ccc} K(\alpha) & \xrightarrow{\sigma^{-1}\tau} & K(\beta) \\ f(\alpha) & \longmapsto & f(\beta) \end{array}$$



Következmény

Tetszőleges K test és $f \in K[x]$ irreducibilis polinom esetén létezik olyan $K(\alpha)$ egyszerű algebrai bővítés, ahol $m_{\alpha, K} = f$, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Következmény

Tetszőleges K test és $f \in K[x]$ irreducibilis polinom esetén létezik olyan $K(\alpha)$ egyszerű algebrai bővítés, ahol $m_{\alpha, K} = f$, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk

Következmény

Tetszőleges K test és $f \in K[x]$ irreducibilis polinom esetén létezik olyan $K(\alpha)$ egyszerű algebrai bővítés, ahol $m_{\alpha, K} = f$, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk
- ▶ egzisztencia:

Következmény

Tetszőleges K test és $f \in K[x]$ irreducibilis polinom esetén létezik olyan $K(\alpha)$ egyszerű algebrai bővítés, ahol $m_{\alpha, K} = f$, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk
- ▶ egzisztencia: $K[x]/(f) = K(\alpha)$, ahol $\alpha =$

Következmény

Tetszőleges K test és $f \in K[x]$ irreducibilis polinom esetén létezik olyan $K(\alpha)$ egyszerű algebrai bővítés, ahol $m_{\alpha, K} = f$, és ez a bővítés izomorfia erejéig egyértelműen meghatározott.

Biz.

- ▶ unicitás: most láttuk
- ▶ egzisztencia: $K[x]/(f) = K(\alpha)$, ahol $\alpha = \bar{x}$



Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Példa

A $\mathbb{Q}(\sqrt[3]{2}) | \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis:

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$.

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2}$ ($a, b \in \mathbb{Q}$) alakú számok?

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2}$ ($a, b \in \mathbb{Q}$) alakú számok?

Mert ez a halmaz nem zárt a szorzásra, például $\sqrt[3]{4}$ nem áll elő $a + b\sqrt[3]{2}$ alakban.

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2}$ ($a, b \in \mathbb{Q}$) alakú számok?

Mert ez a halmaz nem zárt a szorzásra, például $\sqrt[3]{4}$ nem áll elő $a + b\sqrt[3]{2}$ alakban.

Ha előállna, akkor $\sqrt[3]{4} - b\sqrt[3]{2} - a = 0$ lenne,

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2}$ ($a, b \in \mathbb{Q}$) alakú számok?

Mert ez a halmaz nem zárt a szorzásra, például $\sqrt[3]{4}$ nem áll elő $a + b\sqrt[3]{2}$ alakban.

Ha előállna, akkor $\sqrt[3]{4} - b\sqrt[3]{2} - a = 0$ lenne, azaz $\sqrt[3]{2}$ gyöke lenne az $x^2 - bx - a \in \mathbb{Q}[x]$ polinomnak.

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2}$ ($a, b \in \mathbb{Q}$) alakú számok?

Mert ez a halmaz nem zárt a szorzásra, például $\sqrt[3]{4}$ nem áll elő $a + b\sqrt[3]{2}$ alakban.

Ha előállna, akkor $\sqrt[3]{4} - b\sqrt[3]{2} - a = 0$ lenne, azaz $\sqrt[3]{2}$ gyöke lenne az $x^2 - bx - a \in \mathbb{Q}[x]$ polinomnak. Ez lehetetlen, mert

Példa

A $\mathbb{Q}(\sqrt[3]{2}) \mid \mathbb{Q}$ bővítés harmadfokú, mert $m_{\sqrt[3]{2}, \mathbb{Q}} = x^3 - 2$.

Egy bázis: $1, \sqrt[3]{2}, \sqrt[3]{4}$. Tehát $\mathbb{Q}(\sqrt[3]{2})$ elemei egyértelműen előállnak

$$a + b\sqrt[3]{2} + c\sqrt[3]{4} \quad (a, b, c \in \mathbb{Q})$$

alakban.

(Miért nem alkotnak testet az $a + b\sqrt[3]{2}$ ($a, b \in \mathbb{Q}$) alakú számok?

Mert ez a halmaz nem zárt a szorzásra, például $\sqrt[3]{4}$ nem áll elő $a + b\sqrt[3]{2}$ alakban.

Ha előállna, akkor $\sqrt[3]{4} - b\sqrt[3]{2} - a = 0$ lenne, azaz $\sqrt[3]{2}$ gyöke lenne az $x^2 - bx - a \in \mathbb{Q}[x]$ polinomnak. Ez lehetetlen, mert $\sqrt[3]{2}$ minimálpolinomja harmadfokú.)

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) =$$

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= \end{aligned}$$

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= \end{aligned}$$

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

$$(2 - \alpha)^{-1} = ?$$

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

$$(2 - \alpha)^{-1} = ?$$

A $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x] / (x^3 - 7)$ izomorfiát használva, a $\overline{2 - x}^{-1}$ elemet kell kiszámolni.

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

$$(2 - \alpha)^{-1} = ?$$

A $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x] / (x^3 - 7)$ izomorfiát használva, a $\overline{2 - x}^{-1}$ elemet kell kiszámolni. Ezt korábban már kiszámoltuk: $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

$$(2 - \alpha)^{-1} = ?$$

A $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x] / (x^3 - 7)$ izomorfiát használva, a $\overline{2 - x}^{-1}$ elemet kell kiszámolni. Ezt korábban már kiszámoltuk: $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$.
Tehát $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$

Példa

Számoljunk a $\mathbb{Q}(\alpha)$ testben, ahol $\alpha = \sqrt[3]{7}$.

- ▶ elemek: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = 7$ (mert $m_{\sqrt[3]{7}, \mathbb{Q}} = x^3 - 7$)

$$\begin{aligned}(\alpha^2 + \alpha + 1) \cdot (3\alpha^2 - \alpha + 2) &= 3\alpha^4 + 2\alpha^3 + 4\alpha^2 + \alpha + 2 \\ &= 3\alpha \cdot 7 + 2 \cdot 7 + 4\alpha^2 + \alpha + 2 \\ &= 4\alpha^2 + 22\alpha + 16\end{aligned}$$

(Vagy a $3x^4 + 2x^3 + 4x^2 + x + 2$ polinomot maradékosan osztva az $x^3 - 7$ polinommal kapjuk a $4x^2 + 22x + 16$ maradékot.)

$$(2 - \alpha)^{-1} = ?$$

A $\mathbb{Q}(\alpha) \cong \mathbb{Q}[x] / (x^3 - 7)$ izomorfiát használva, a $\overline{2 - x}^{-1}$ elemet kell kiszámolni. Ezt korábban már kiszámoltuk: $\overline{2 - x}^{-1} = \overline{x^2 + 2x + 4}$. Tehát $(2 - \alpha)^{-1} = \alpha^2 + 2\alpha + 4$, vagyis

$$\frac{1}{2 - \sqrt[3]{7}} = \sqrt[3]{49} + 2\sqrt[3]{7} + 4.$$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály:

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 =$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 =$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 =$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:

$$\alpha^2 \cdot (\alpha^2 - \alpha + 1) =$$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:

$$\alpha^2 \cdot (\alpha^2 - \alpha + 1) = \alpha^4 - \alpha^3 + \alpha^2 =$$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:

$$\alpha^2 \cdot (\alpha^2 - \alpha + 1) = \alpha^4 - \alpha^3 + \alpha^2 = \alpha(-\alpha - 1) - (-\alpha - 1) + \alpha^2 =$$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:

$$\alpha^2 \cdot (\alpha^2 - \alpha + 1) = \alpha^4 - \alpha^3 + \alpha^2 = \alpha(-\alpha - 1) - (-\alpha - 1) + \alpha^2 = 1.$$

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:

$$\alpha^2 \cdot (\alpha^2 - \alpha + 1) = \alpha^4 - \alpha^3 + \alpha^2 = \alpha(-\alpha - 1) - (-\alpha - 1) + \alpha^2 = 1.$$

Ugyanez megy \mathbb{Z}_2 felett.

Példa

Legyen α gyöke az $x^3 + x + 1$ polinomnak. Határozzuk meg az α^{-2} szám „kanonikus alakját”.

- ▶ $\mathbb{Q}(\alpha)$ elemei: $a\alpha^2 + b\alpha + c$ ($a, b, c \in \mathbb{Q}$)
- ▶ számolási szabály: $\alpha^3 = -\alpha - 1$ (mert $m_{\alpha, \mathbb{Q}} = x^3 + x + 1$)

Az $x^2 \cdot u \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása: $u \equiv x^2 - x + 1$.
Tehát $\alpha^{-2} = \alpha^2 - \alpha + 1$.

Másik lehetőség: az $x \cdot v \equiv 1 \pmod{x^3 + x + 1}$ kongruencia megoldása:
 $v \equiv -x^2 - 1$. Tehát $\alpha^{-1} = -\alpha^2 - 1$, és így
 $\alpha^{-2} = (-\alpha^2 - 1)^2 = \alpha^4 + 2\alpha^2 + 1 = \alpha(-\alpha - 1) + 2\alpha^2 + 1 = \alpha^2 - \alpha + 1$.

Harmadik lehetőség: $1 = -\alpha^3 - \alpha = \alpha \cdot (-\alpha^2 - 1)$, ezért
 $\alpha^{-1} = -\alpha^2 - 1$.

Ellenőrzés:

$$\alpha^2 \cdot (\alpha^2 - \alpha + 1) = \alpha^4 - \alpha^3 + \alpha^2 = \alpha(-\alpha - 1) - (-\alpha - 1) + \alpha^2 = 1.$$

Ugyanez megy \mathbb{Z}_2 felett. És \mathbb{Z}_3 felett?

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$.

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \dots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \dots + c_1 \alpha + c_0 1 = 0.$$

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \dots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \dots + c_1 \alpha + c_0 1 = 0.$$

Ez azt jelenti, hogy α gyöke a nemnulla $c_n x^n + \dots + c_1 x + c_0 \in K[x]$ polinomnak. □

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \dots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \dots + c_1 \alpha + c_0 1 = 0.$$

Ez azt jelenti, hogy α gyöke a nemnulla $c_n x^n + \dots + c_1 x + c_0 \in K[x]$ polinomnak. □

Tétel

Ha $L \mid K$ végesfokú bővítés, akkor minden $\alpha \in L$ esetén

$$\deg m_{\alpha, K} \mid [L : K].$$

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \dots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \dots + c_1 \alpha + c_0 1 = 0.$$

Ez azt jelenti, hogy α gyöke a nemnulla $c_n x^n + \dots + c_1 x + c_0 \in K[x]$ polinomnak. □

Tétel

Ha $L \mid K$ végesfokú bővítés, akkor minden $\alpha \in L$ esetén

$$\deg m_{\alpha, K} \mid [L : K].$$

Biz.

Alkalmazzuk a torony-törvényt a $K \leq K(\alpha) \leq L$ toronyra:

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \dots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \dots + c_1 \alpha + c_0 1 = 0.$$

Ez azt jelenti, hogy α gyöke a nemnulla $c_n x^n + \dots + c_1 x + c_0 \in K[x]$ polinomnak. □

Tétel

Ha $L \mid K$ végesfokú bővítés, akkor minden $\alpha \in L$ esetén

$$\deg m_{\alpha, K} \mid [L : K].$$

Biz.

Alkalmazzuk a torony-törvényt a $K \leq K(\alpha) \leq L$ toronyra:

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K]$$

Definíció

Ha minden $\alpha \in L \mid K$ algebrai K felett, akkor azt mondjuk, hogy $L \mid K$ **algebrai bővítés**.

Tétel

Minden végesfokú bővítés algebrai.

Biz.

Legyen $[L : K] = n$ és $\alpha \in L$. Az $1, \alpha, \alpha^2, \dots, \alpha^n$ vektorrendszer lineárisan függő az ${}_K L$ vektortérben, ezért vannak olyan $c_0, \dots, c_n \in K$ skalárok (nem mind nulla), hogy

$$c_n \alpha^n + \dots + c_1 \alpha + c_0 1 = 0.$$

Ez azt jelenti, hogy α gyöke a nemnulla $c_n x^n + \dots + c_1 x + c_0 \in K[x]$ polinomnak. □

Tétel

Ha $L \mid K$ végesfokú bővítés, akkor minden $\alpha \in L$ esetén

$$\deg m_{\alpha, K} \mid [L : K].$$

Biz.

Alkalmazzuk a torony-törvényt a $K \leq K(\alpha) \leq L$ toronyra:

$$[L : K] = [L : K(\alpha)] \cdot [K(\alpha) : K] = [L : K(\alpha)] \cdot \deg m_{\alpha, K}. \quad \square$$

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$:

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$:

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$:

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
 - ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
 - ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.
- $\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies$

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.

$$\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\alpha) \implies$$

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.

$\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\alpha)$,
mert

Példa

Legyen $\alpha = i\sqrt{2} - \sqrt{2}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.

$\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\alpha)$,
mert mindkettő negyedfokú bővítése \mathbb{Q} -nak.

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.

$\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\alpha)$,
mert mindkettő negyedfokú bővítése \mathbb{Q} -nak.

Ez viszont lehetetlen, hiszen

Példa

Legyen $\alpha = i\sqrt{2 - \sqrt{2}}$. Benne vannak-e a $\sqrt{2}$, $\sqrt[3]{2}$, $\sqrt[4]{2}$ számok a $\mathbb{Q}(\alpha)$ testben?

- ▶ $\sqrt{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: igen, mert $\sqrt{2} = \alpha^2 + 2$.
- ▶ $\sqrt[3]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem, mert $\deg m_{\sqrt[3]{2}, \mathbb{Q}} = 3 \nmid [\mathbb{Q}(\alpha) : \mathbb{Q}] = 4$.
- ▶ $\sqrt[4]{2} \stackrel{?}{\in} \mathbb{Q}(\alpha)$: nem.

$$\sqrt[4]{2} \in \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) \subseteq \mathbb{Q}(\alpha) \implies \mathbb{Q}(\sqrt[4]{2}) = \mathbb{Q}(\alpha),$$

mert mindkettő negyedfokú bővítése \mathbb{Q} -nak.

Ez viszont lehetetlen, hiszen $\alpha \notin \mathbb{Q}(\sqrt[4]{2})$.

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett.

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) | K$ bővítés fokszámát:

Tétel

Tetszőleges $L \mid K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) \mid K$ bővítés fokszámát:

$$[K(\alpha, \beta) : K] = [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K]$$

Tétel

Tetszőleges $L \mid K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) \mid K$ bővítés fokszámát:

$$\begin{aligned} [K(\alpha, \beta) : K] &= [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \\ &= \deg m_{\beta, K(\alpha)} \cdot \deg m_{\alpha, K} \end{aligned}$$

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) | K$ bővítés fokszámát:

$$\begin{aligned} [K(\alpha, \beta) : K] &= [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \\ &= \deg m_{\beta, K(\alpha)} \cdot \deg m_{\alpha, K} \\ &\leq \deg m_{\beta, K} \cdot \deg m_{\alpha, K}. \end{aligned}$$

Tétel

Tetszőleges $L \mid K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) \mid K$ bővítés fokszámát:

$$\begin{aligned} [K(\alpha, \beta) : K] &= [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \\ &= \deg m_{\beta, K(\alpha)} \cdot \deg m_{\alpha, K} \\ &\leq \deg m_{\beta, K} \cdot \deg m_{\alpha, K}. \end{aligned}$$

Tehát $K(\alpha, \beta) \mid K$ végesfokú, ezért minden eleme algebrai K felett.

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) | K$ bővítés fokszámát:

$$\begin{aligned} [K(\alpha, \beta) : K] &= [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \\ &= \deg m_{\beta, K(\alpha)} \cdot \deg m_{\alpha, K} \\ &\leq \deg m_{\beta, K} \cdot \deg m_{\alpha, K}. \end{aligned}$$

Tehát $K(\alpha, \beta) | K$ végesfokú, ezért minden eleme algebrai K felett. Speciálisan $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, α/β (ha $\beta \neq 0$) is algebraiak K felett.

Tétel

Tetszőleges $L | K$ testbővítésben a K felett algebrai elemek résztestet alkotnak.

Biz.

Legyenek $\alpha, \beta \in L$ algebraiak K felett. Ekkor β algebrai $K(\alpha)$ felett is, és a fokszámtétel segítségével megbecsülhetjük a $K(\alpha, \beta) | K$ bővítés fokszámát:

$$\begin{aligned} [K(\alpha, \beta) : K] &= [K(\alpha)(\beta) : K(\alpha)] \cdot [K(\alpha) : K] \\ &= \deg m_{\beta, K(\alpha)} \cdot \deg m_{\alpha, K} \\ &\leq \deg m_{\beta, K} \cdot \deg m_{\alpha, K}. \end{aligned}$$

Tehát $K(\alpha, \beta) | K$ végesfokú, ezért minden eleme algebrai K felett. Speciálisan $\alpha + \beta$, $\alpha - \beta$, $\alpha \cdot \beta$, α/β (ha $\beta \neq 0$) is algebraiak K felett. □

Következmény

Az algebrai számok testet alkotnak.

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Biz.

Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke a

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Biz.

Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke a $g(x) = f(x^n) \in \mathbb{Q}[x]$ polinomnak. □

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Biz.

Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke a $g(x) = f(x^n) \in \mathbb{Q}[x]$ polinomnak. □

Következmény

A **gyökmennyiségek**, azaz a racionális számokból a négy alapművelet és gyökvonások véges számú alkalmazásával megkapható számok mind algebraiak.

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Biz.

Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke a $g(x) = f(x^n) \in \mathbb{Q}[x]$ polinomnak. □

Következmény

A **gyökmennyiségek**, azaz a racionális számokból a négy alapművelet és gyökvonások véges számú alkalmazásával megkapható számok mind algebraiak.

Biz.

A racionális számok (elsőfokú) algebrai számok, és az algebrai számok halmaza zárt a négy alapműveletre és a gyökvonásokra. □

Tétel

Ha α algebrai szám, akkor $\sqrt[n]{\alpha}$ is algebrai (a gyöknek mind az n értékére).

Biz.

Ha α gyöke az $f \in \mathbb{Q}[x]$ polinomnak, akkor $\sqrt[n]{\alpha}$ gyöke a $g(x) = f(x^n) \in \mathbb{Q}[x]$ polinomnak. □

Következmény

A **gyökmennyiségek**, azaz a racionális számokból a négy alapművelet és gyökvonások véges számú alkalmazásával megkapható számok mind algebraiak.

Biz.

A racionális számok (elsőfokú) algebrai számok, és az algebrai számok halmaza zárt a négy alapműveletre és a gyökvonásokra. □

Tétel

Van olyan algebrai szám, ami nem gyökmennyiség.