

# Lineáris és absztrakt algebra, normál

## ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil

Konzultáció: [ewwkiss@gmail.com](mailto:ewwkiss@gmail.com)

<https://algebra.elte.hu/nyitolap/oktatas-szakdolgozat/linearis-es-absztrakt-algebra/>

17.\* előadás

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi,

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ ,

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$



# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:  $\varphi(k) = |k|$ .

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:  $\varphi(k) = |k|$ .

$T[x]$  euklideszi, ha  $T$  test:

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:  $\varphi(k) = |k|$ .

$T[x]$  euklideszi, ha  $T$  test:  $\varphi(f) = \text{gr}(f)$ .

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:  $\varphi(k) = |k|$ .

$T[x]$  euklideszi, ha  $T$  test:  $\varphi(f) = \text{gr}(f)$ .

**Gauss-egészek:**  $a + bi$  alakú számok, ahol  $a, b \in \mathbb{Z}$ .

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:  $\varphi(k) = |k|$ .

$T[x]$  euklideszi, ha  $T$  test:  $\varphi(f) = \text{gr}(f)$ .

**Gauss-egészek:**  $a + bi$  alakú számok, ahol  $a, b \in \mathbb{Z}$ .

Ez is euklideszi gyűrű:  $\varphi(a + bi) = a^2 + b^2$ .

# Euklideszi gyűrű (lásd Algebra és számelmélet, 22. dia)

## 5.5.1. Definíció

**Euklideszi gyűrű:** „elvégezhető benne a maradékos osztás.”

Az  $R$  szokásos (kommutatív, egységelemes, nullosztómentes) gyűrű euklideszi, ha  $R$  nem nulla elemein értelmezve van egy nemnegatív egész értékű  $\varphi$  függvény úgy, hogy minden  $a, b \in R$ ,  $b \neq 0$  esetén létezik olyan  $q, r \in R$ , hogy  $a = bq + r$ , és  $r = 0$  vagy  $\varphi(r) < \varphi(b)$ .

## Példák

$\mathbb{Z}$  euklideszi:  $\varphi(k) = |k|$ .

$T[x]$  euklideszi, ha  $T$  test:  $\varphi(f) = \text{gr}(f)$ .

**Gauss-egészek:**  $a + bi$  alakú számok, ahol  $a, b \in \mathbb{Z}$ .

Ez is euklideszi gyűrű:  $\varphi(a + bi) = a^2 + b^2$ .

Bizonyítás: Freud Róbert és Gyarmati Edit számelmélet könyve.



# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben,

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű nem nulla eleme.

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű nem nulla eleme. Belátjuk, hogy  $I = (g)$ .

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű nem nulla eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ ,

# Euklideszi gyűrű főideálgűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .



# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ ,

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

## Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

Mivel  $\varphi(g)$  minimális volt,

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

Mivel  $\varphi(g)$  minimális volt, így  $r$  csak nulla lehet.

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

Mivel  $\varphi(g)$  minimális volt, így  $r$  csak nulla lehet.

Tehát  $f \in (g)$ ,

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

Mivel  $\varphi(g)$  minimális volt, így  $r$  csak nulla lehet.

Tehát  $f \in (g)$ , azaz  $I \subseteq (g)$ . □

# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

Mivel  $\varphi(g)$  minimális volt, így  $r$  csak nulla lehet.

Tehát  $f \in (g)$ , azaz  $I \subseteq (g)$ . □

**Főideálgyűrű:** szokásos gyűrű, melynek minden ideálja főideál.



# Euklideszi gyűrű főideálgyűrű

## 5.5.3. Tétel

Minden euklideszi gyűrű minden ideálja főideál.

### Bizonyítás

Legyen  $I$  nem nulla ideál  $R$ -ben, és  $g$  a legkisebb  $\varphi$ -értékű **nem nulla** eleme. Belátjuk, hogy  $I = (g)$ .

Nyilván  $(g) \subseteq I$ , hiszen  $I$  tartalmazza  $g$  többszöröseit.

Legyen  $f \in I$ , ekkor  $f = gq + r$ , ahol  $\varphi(r) < \varphi(g)$  vagy  $r = 0$ .

De  $r = f - gq \in I$ , mert  $I$  zárt a többszörözésre és a kivonásra.

Mivel  $\varphi(g)$  minimális volt, így  $r$  csak nulla lehet.

Tehát  $f \in (g)$ , azaz  $I \subseteq (g)$ . □

**Főideálgyűrű:** szokásos gyűrű, melynek minden ideálja főideál.

Ezekben érvényes a **számelmélet alaptétele**.

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

Szokásos gyűrű:

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív,

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes,

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt.

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.



# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem

egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem

egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:  $\mathbb{Z}$ ,

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem

egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:  $\mathbb{Z}$ ,  $T[x]$  ( $T$  test),



# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem

egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:  $\mathbb{Z}$ ,  $T[x]$  ( $T$  test),  $\mathbb{Z}[x]$ .

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:  $\mathbb{Z}$ ,  $T[x]$  ( $T$  test),  $\mathbb{Z}[x]$ .

**$a, b \in R$  kitüntetett közös osztója  $d$ ,** ha

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:  $\mathbb{Z}$ ,  $T[x]$  ( $T$  test),  $\mathbb{Z}[x]$ .

**$a, b \in R$  kitüntetett közös osztója  $d$ ,** ha

(1)  $d$  közös osztó, azaz  $d \mid a$  és  $d \mid b$ ;

# Számelméleti alapfogalmak (ismétlés)

## Ismétlés (3.1. Szakasz)

**Szokásos gyűrű:** kommutatív, nullosztómentes, egységelemes.

**$r$  osztója  $s$ -nek,** ha van olyan  $t$  a gyűrűben, hogy  $s = tr$ .

**Egység:** mindent oszt. Legyen  $r \in R$  nem nulla, nem egység.

**Triviális felbontás:**  $r = ab$ , ha valamelyik tényező egység.

**$r$  felbonthatatlan:** nincs nemtriviális felbontása szorzatra (azaz minden felbontásában valamelyik tényező egység).

**$r$  prím:** ha  $r \mid ab$ , akkor  $r \mid a$  vagy  $r \mid b$ .

**$R$  alaptételes:** minden nullától és egységtől különböző elem egyértelműen előáll felbonthatatlanok szorzataként.

**Főpéldák** alaptételes gyűrűre:  $\mathbb{Z}$ ,  $T[x]$  ( $T$  test),  $\mathbb{Z}[x]$ .

**$a, b \in R$  kitüntetett közös osztója  $d$ ,** ha

- (1)  $d$  közös osztó, azaz  $d \mid a$  és  $d \mid b$ ;
- (2)  $d$  mindegyik közös osztónak többszöröse.

# Az alapfogalmak összefüggései

## 3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

# Az alapfogalmak összefüggései

## 3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

## 3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel **egyértelműségi** állítása.

# Az alapfogalmak összefüggései

## 3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

## 3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel **egyértelműségi** állítása.

## 3.1.22. és 3.1.26. Gyakorlatok

Alaptételes gyűrűben

# Az alapfogalmak összefüggései

## 3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

## 3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel **egyértelműségi** állítása.

## 3.1.22. és 3.1.26. Gyakorlatok

Alaptételes gyűrűben

(1) bármely két elemnek van kitüntetett közös osztója;



# Az alapfogalmak összefüggései

## 3.1.27. Gyakorlat

Ha bármely két elemnek van kitüntetett közös osztója, akkor minden felbonthatatlan elem prím.

## 3.1.28. Gyakorlat

Ha minden felbonthatatlan elem prím, akkor igaz az alaptétel **egyértelműségi** állítása.

## 3.1.22. és 3.1.26. Gyakorlatok

Alaptételes gyűrűben

- (1) bármely két elemnek van kitüntetett közös osztója;
- (2) minden felbonthatatlan elem prím.

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll:

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”!

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4,

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: főideál.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: főideál.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .



# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például  $2$  kisebb, mint  $4$ , de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: főideál.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

## Bizonyítás

Mivel  $(d) = (a, b) \supseteq (a)$ ,

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

## Bizonyítás

Mivel  $(d) = (a, b) \supseteq (a)$ , ezért  $d \mid a$ ,

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

## Bizonyítás

Mivel  $(d) = (a, b) \supseteq (a)$ , ezért  $d \mid a$ , ugyanígy  $d \mid b$ .

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

## Bizonyítás

Mivel  $(d) = (a, b) \supseteq (a)$ , ezért  $d \mid a$ , ugyanígy  $d \mid b$ .

Ha  $c \mid a$  és  $c \mid b$ ,

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

## Bizonyítás

Mivel  $(d) = (a, b) \supseteq (a)$ , ezért  $d \mid a$ , ugyanígy  $d \mid b$ .

Ha  $c \mid a$  és  $c \mid b$ , akkor  $d = ra + sb$  miatt

# Ideálok és oszthatóság

5.1.10. Definíció:  $(r)$  az  $r$  összes többszöröséből áll: **főideál**.

## 5.5.4. Lemma

$$r \mid s \iff (r) \supseteq (s).$$



„Megfordul”! Például 2 kisebb, mint 4, de  $(2)$  nagyobb, mint  $(4)$ .

## 5.5.5. Lemma

Legyen  $R$  szokásos gyűrű és  $a, b \in R$ .

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  kitüntetett közös osztója.

(A kitüntetett közös osztót is  $(a, b)$  jelölte számelméletben.)

## Bizonyítás

Mivel  $(d) = (a, b) \supseteq (a)$ , ezért  $d \mid a$ , ugyanígy  $d \mid b$ .

Ha  $c \mid a$  és  $c \mid b$ , akkor  $d = ra + sb$  miatt  $c \mid d$ .





# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.  
Ezért főideálgyűrűben

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.  
Ezért főideálgyűrűben (és így euklideszi gyűrűben)

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.  
Ezért főideálgyűrűben (és így euklideszi gyűrűben)  
bármely két elemnek **van** kitüntetett közös osztója.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,



# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ ,

# Euklideszi és főideálgűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgűrű (így minden euklideszi gűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgűrűben (és így euklideszi gűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1, \pm 2$ ,

# Euklideszi és főideálgűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgűrű (így minden euklideszi gűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgűrűben (és így euklideszi gűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  **alptételes** gűrű,  $2$  és  $x$  **kitüntetett közös osztója**  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

Az  $1$  nem ilyen,

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

Az  $1$  nem ilyen, tehát  $(2, x) \neq (1)$ ,

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben) bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

Az  $1$  nem ilyen, tehát  $(2, x) \neq (1)$ , ezért  $(2, x)$  **nem főideál**.

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben)

bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  **alptételes** gyűrű,  $2$  és  $x$  **kitüntetett közös osztója**  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

Az  $1$  nem ilyen, tehát  $(2, x) \neq (1)$ , ezért  $(2, x)$  **nem főideál**. Tehát

$\mathbb{Z}[x]$  **nem főideálgyűrű**,



# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben)

bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

Az  $1$  nem ilyen, tehát  $(2, x) \neq (1)$ , ezért  $(2, x)$  **nem főideál**. Tehát

$\mathbb{Z}[x]$  nem főideálgyűrű, és így nem is euklideszi,

# Euklideszi és főideálgyűrű alaptétele

## Tétel (5.5.9. Következmény)

Minden főideálgyűrű (így minden euklideszi gyűrű) alaptételes.

## Bizonyítás

Ha  $(a, b) = (d)$ , akkor  $d$  az  $a$  és  $b$  **kitüntetett közös osztója**.

Ezért főideálgyűrűben (és így euklideszi gyűrűben)

bármely két elemnek **van** kitüntetett közös osztója.

Így érvényes az alaptétel egyértelműségi állítása.

A felbontás **létezését** nem bizonyítjuk.

$R = \mathbb{Z}[x]$  alaptételes gyűrű,  $2$  és  $x$  kitüntetett közös osztója  $1$ , hiszen  $2$  osztói csak  $\pm 1$ ,  $\pm 2$ , és  $2 \nmid x$ .

$(2, x)$  azokból a polinomokból áll, melyek konstans tagja páros.

Az  $1$  nem ilyen, tehát  $(2, x) \neq (1)$ , ezért  $(2, x)$  **nem főideál**. Tehát

$\mathbb{Z}[x]$  nem főideálgyűrű, és így nem is euklideszi, noha alaptételes.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).  
A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).  
A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.  
A 3 felbonthatatlan, de nem prím.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3$$

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$



# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is,  $2 \pm i\sqrt{5}$  is felbonthatatlan,

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is,  $2 \pm i\sqrt{5}$  is felbonthatatlan, de 3 nem egyszersere

$2 \pm i\sqrt{5}$ -nek,

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is,  $2 \pm i\sqrt{5}$  is felbonthatatlan, de 3 nem egységszerese

$2 \pm i\sqrt{5}$ -nek, így ez a 9-nek két, lényegesen különböző felbontása.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A  $9$ -nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A  $3$  felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt  $3$  is,  $2 \pm i\sqrt{5}$  is felbonthatatlan, de  $3$  nem egységszerese

$2 \pm i\sqrt{5}$ -nek, így ez a  $9$ -nek két, lényegesen különböző felbontása.

Ezért ez a gyűrű nem alaptételes.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A  $9$ -nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A  $3$  felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt  $3$  is,  $2 \pm i\sqrt{5}$  is felbonthatatlan, de  $3$  nem egyszersere

$2 \pm i\sqrt{5}$ -nek, így ez a  $9$ -nek két, lényegesen különböző felbontása.

Ezért ez a gyűrű nem alaptételes.

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is,  $2 \pm i\sqrt{5}$  is felbonthatatlan, de 3 nem egyszersere

$2 \pm i\sqrt{5}$ -nek, így ez a 9-nek két, lényegesen különböző felbontása.

Ezért ez a gyűrű nem alaptételes.

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához. A kiút az, hogy a  $(9, 3(2 + i\sqrt{5}))$  ideál veszi át a hiányzó kitüntetett közös osztó szerepét.

# Példa nem alaptételes gyűrűre

## 3.1.34. Feladat

Legyen  $R$  az  $a + bi\sqrt{5}$  alakú számokból álló gyűrű ( $a, b \in \mathbb{Z}$ ).

A 9-nek és a  $3(2 + i\sqrt{5})$ -nek nincs kitüntetett közös osztója.

A 3 felbonthatatlan, de nem prím.

Az alaptétel egyértelműségi állítása nem igaz:

$$9 = 3 \cdot 3 = (2 + i\sqrt{5})(2 - i\sqrt{5}),$$

itt 3 is,  $2 \pm i\sqrt{5}$  is felbonthatatlan, de 3 nem egységszerese

$2 \pm i\sqrt{5}$ -nek, így ez a 9-nek két, lényegesen különböző felbontása.

Ezért ez a gyűrű nem alaptételes.

Az ilyen gyűrűk is hasznosak számelméleti problémák megoldásához. A kiút az, hogy a  $(9, 3(2 + i\sqrt{5}))$  ideál veszi át a hiányzó kitüntetett közös osztó szerepét.

Ez a témakör az **algebrai számelmélet**.

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ ,



# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2)$$

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

## 5.1.18. Állítás

Ha  $I$  és  $J$  ideálok az  $R$  gyűrűben,



# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

## 5.1.18. Állítás

Ha  $I$  és  $J$  ideálok az  $R$  gyűrűben,  
a csoportelméleti  $I + J$  komplexusösszeg az egész  $R$ ,

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

## 5.1.18. Állítás

Ha  $I$  és  $J$  ideálok az  $R$  gyűrűben,  
a csoportelméleti  $I + J$  komplexusösszeg az egész  $R$ ,  
továbbá  $I \cap J = 0$ ,

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

## 5.1.18. Állítás

Ha  $I$  és  $J$  ideálok az  $R$  gyűrűben, a csoportelméleti  $I + J$  komplexusösszeg az egész  $R$ , továbbá  $I \cap J = 0$ , akkor  $R \cong I \times J$ .

# Direkt szorzat

## 5.1.17. Definíció

Az  $R$  és  $S$  gyűrűk **direkt szorzatának** alaphalmaza  $R \times S$ , ahol a műveleteket **komponensenként** végezzük:

$$(r_1, s_1) + (r_2, s_2) = (r_1 + r_2, s_1 + s_2) \text{ és } (r_1, s_1)(r_2, s_2) = (r_1 r_2, s_1 s_2).$$

**HF:** Ez tényleg gyűrű.

Hasonló a definíció kettőnél több tényező esetében is.

A belső jellemzés mint csoportokra (normálosztó helyett ideál):

## 5.1.18. Állítás

Ha  $I$  és  $J$  ideálok az  $R$  gyűrűben, a csoportelméleti  $I + J$  komplexusösszeg az egész  $R$ , továbbá  $I \cap J = 0$ , akkor  $R \cong I \times J$ .

**A bizonyítás ötlete:** Ha  $I \cap J = 0$ ,  $a \in I$ ,  $b \in J$ , akkor  $ab = 0$ .

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.



# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$  de  $c \neq 0$ ,

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$  de  $c \neq 0$ , akkor  $a = b$ .

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$  (vagy  $ca = cb$ ), de  $c \neq 0$ , akkor  $a = b$ .

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$  (vagy  $ca = cb$ ), de  $c \neq 0$ , akkor  $a = b$ .

**Bizonyítás:** Ha  $ac = bc$ , akkor  $(a - b)c = 0$ .

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$  (vagy  $ca = cb$ ), de  $c \neq 0$ , akkor  $a = b$ .

**Bizonyítás:** Ha  $ac = bc$ , akkor  $(a - b)c = 0$ . Mivel  $c \neq 0$ ,

# Véges nullosztómentes gyűrű test

## 5.3.5. Tétel

Minden véges, nullosztómentes gyűrű test.

## Wedderburn tétele (6.7.13. Tétel, NB)

Minden véges ferdetest kommutatív.

Nehéz tétel, a nagyon szép bizonyítás benne van a jegyzetben.  
Így elég belátni, hogy véges nullosztómentes gyűrű **ferdetest**.

## Emlékeztető (2.2.8. Gyakorlat)

Nullosztómentes gyűrűben érvényes az **egyszerűsítési szabály**:  
ha  $ac = bc$  (vagy  $ca = cb$ ), de  $c \neq 0$ , akkor  $a = b$ .

**Bizonyítás:** Ha  $ac = bc$ , akkor  $(a - b)c = 0$ . Mivel  $c \neq 0$ ,  
a nullosztómentesség miatt  $a - b = 0$ .





# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ ,  
melyre  $er = r$ ,

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ ,

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ .

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ .  
Tehát  $e$  jobboldali egységelem.

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ .

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ .

Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ .

Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is. □

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ . Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ .



# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ . Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ . Ekkor  $r_1r, \dots, r_nr$  a nullosztómentesség miatt csupa különböző elem.

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ . Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ . Ekkor  $r_1r, \dots, r_nr$  a nullosztómentesség miatt csupa különböző elem. Mivel  $R$  véges, minden elemét megkapjuk.

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ .  
Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ .  
Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ . Ekkor  $r_1r, \dots, r_nr$  a nullosztómentesség miatt csupa különböző elem.  
Mivel  $R$  véges, minden elemét megkapjuk.  
Speciálisan  $r = r_jr$  esetén a Lemma miatt  $e = r_j$  egységelem.

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ . Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ . Ekkor  $r_1r, \dots, r_nr$  a nullosztómentesség miatt csupa különböző elem.

Mivel  $R$  véges, minden elemét megkapjuk.

Speciálisan  $r = r_jr$  esetén a Lemma miatt  $e = r_j$  egységelem.

Továbbá  $e = r_jr$  esetén  $r$ -nek balinverze  $r_j$ .

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ . Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ . Ekkor  $r_1r, \dots, r_nr$  a nullosztómentesség miatt csupa különböző elem.

Mivel  $R$  véges, minden elemét megkapjuk.

Speciálisan  $r = r_jr$  esetén a Lemma miatt  $e = r_j$  egységelem.

Továbbá  $e = r_jr$  esetén  $r$ -nek balinverze  $r_j$ . Ugyanígy van jobbinverze is.

# Véges nullosztómentes gyűrűk (bizonyítás)

## 5.3.4. Lemma

Ha  $R$  nullosztómentes,  $e \in R$ , és van olyan  $0 \neq r \in R$ , melyre  $er = r$ , akkor  $e$  egységelem.

**Bizonyítás:** Minden  $t$ -re  $ter = tr$ , az  $r$ -rel egyszerűsítve  $te = t$ . Tehát  $e$  jobboldali egységelem. Speciálisan  $re = r$ . Ugyanezt balról csinálva kapjuk, hogy  $e$  bal egységelem is.  $\square$

## Bizonyítás (véges nullosztómentes gyűrű test)

Legyen  $R = \{r_1, \dots, r_n\}$  és  $0 \neq r$ . Ekkor  $r_1r, \dots, r_nr$  a nullosztómentesség miatt csupa különböző elem.

Mivel  $R$  véges, minden elemét megkapjuk.

Speciálisan  $r = r_jr$  esetén a Lemma miatt  $e = r_j$  egységelem.

Továbbá  $e = r_jr$  esetén  $r$ -nek balinverze  $r_j$ . Ugyanígy van jobbinverze is. Ezek egyenlők (Algebra1, vagy 2.2.10. Feladat).  $\square$

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.



# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ ,

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.  
Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

Tehát minden  $r \in T$ -re  $r = 1r \in I$ .

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

Tehát minden  $r \in T$ -re  $r = 1r \in I$ . Ezért  $I = T$ . □

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

Tehát minden  $r \in T$ -re  $r = 1r \in I$ . Ezért  $I = T$ . □

**HF:** Ferdetestnek minden balideálja és jobbideálja triviális.

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

Tehát minden  $r \in T$ -re  $r = 1r \in I$ . Ezért  $I = T$ . □

**HF:** Ferdetestnek minden balideálja és jobbideálja triviális.

## 5.3.1. Definíció

Az  $R$  egyszerű gyűrű, ha pontosan két ideálja van:  $0$  és  $R$ .

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

Tehát minden  $r \in T$ -re  $r = 1r \in I$ . Ezért  $I = T$ . □

**HF:** Ferdetestnek minden balideálja és jobbideálja triviális.

## 5.3.1. Definíció

Az  $R$  egyszerű gyűrű, ha pontosan két ideálja van:  $0$  és  $R$ .

**Főpélda (5.3.3):** (Ferde)test fölötti teljes mátrixgyűrű egyszerű.

# Testek ideáljai

## 5.3.2. Állítás

Egy testnek csak a triviális ideáljai vannak:  $\{0\}$  és önmaga.

## Bizonyítás

Legyen  $T$  test és  $I$  ideálja  $T$ -nek, amely nem csak a nullából áll.

Ha  $0 \neq s \in I$ , akkor  $1 = ss^{-1} \in I$ , hiszen  $I$  ideál.

Tehát minden  $r \in T$ -re  $r = 1r \in I$ . Ezért  $I = T$ . □

**HF:** Ferdetestnek minden balideálja és jobbideálja triviális.

## 5.3.1. Definíció

Az  $R$  egyszerű gyűrű, ha pontosan két ideálja van:  $0$  és  $R$ .

**Főpélda (5.3.3):** (Ferde)test fölötti teljes mátrixgyűrű egyszerű.

**8.7.10, 8.7.12:** A teljes mátrixgyűrű balideáljainak leírása.



# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ ,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ ,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ .



# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ ,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ .

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ . Tehát az  $s$  elem invertálható,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ . Tehát az  $s$  elem invertálható, és így  $R$  test. □

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ .

Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ .

Tehát az  $s$  elem invertálható, és így  $R$  test. □

## Általánosítás (5.3.8. Tétel, NB)

Legyen  $R$  gyűrű, amelynek csak a két triviális balideálja van.

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ . Tehát az  $s$  elem invertálható, és így  $R$  test. □

## Általánosítás (5.3.8. Tétel, NB)

Legyen  $R$  gyűrű, amelynek csak a két triviális balideálja van. Ekkor  $R$  vagy ferdetest,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ .

Tehát az  $s$  elem invertálható, és így  $R$  test. □

## Általánosítás (5.3.8. Tétel, NB)

Legyen  $R$  gyűrű, amelynek csak a két triviális balideálja van. Ekkor  $R$  vagy ferdetest, vagy olyan prímelemű gyűrű,

# Kommutatív egyszerű gyűrűk

## Tétel (5.3.9. Következmény)

Minden kommutatív, egységelemes, egyszerű gyűrű test.

## Bizonyítás

Ha  $R$  kommutatív, egységelemes, egyszerű gyűrű és  $0 \neq s \in R$ , akkor  $s = 1s \in (s)$  miatt az  $(s)$  ideál nem  $(0)$ , és így  $(s) = R$ . Ezért  $1 \in (s)$ , vagyis van olyan  $r \in R$ , hogy  $sr = 1$ .

Tehát az  $s$  elem invertálható, és így  $R$  test. □

## Általánosítás (5.3.8. Tétel, NB)

Legyen  $R$  gyűrű, amelynek csak a két triviális balideálja van. Ekkor  $R$  vagy ferdetest, vagy olyan prímelemű gyűrű, amelyben bármely két elem szorzata nulla.



# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,  
akkor  $r$  baloldali, **nullosztó**.

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,  
akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,  
akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál,

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,  
akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál,  
**pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,  
akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál,  
**pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ ,

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál, **pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ ,  
akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál,  
**pontatlanul:** az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ ,



# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál, **pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ , akkor pedig  $(sx)r$

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál, **pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ , akkor pedig  $(sx)r = s(xr)$

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál, **pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ , akkor pedig  $(sx)r = s(xr) = s0 = 0$ . □

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál, **pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ , akkor pedig  $(sx)r = s(xr) = s0 = 0$ . □

**Elnevezés**: Ez az  $r$  elem bal oldali **annullátora**.

# Ideálok és nullosztók

## Emlékeztető (2.2.27. Definíció)

Ha  $R$  gyűrű,  $r, s \in R$  egyik sem nulla, de  $rs = 0$ , akkor  $r$  baloldali,  $s$  jobboldali **nullosztó**.

## 5.3.7. Lemma

Legyen  $r \in R$  rögzített. Ekkor  $\{x \in R : xr = 0\}$  balideál, **pontatlanul**: az „ $r$ -hez tartozó” bal nullosztók balideált alkotnak.

## Bizonyítás

Ha  $xr = 0$  és  $yr = 0$ , akkor nyilván  $(x \pm y)r = 0$ .

Ha  $xr = 0$  és  $s \in R$ , akkor pedig  $(sx)r = s(xr) = s0 = 0$ . □

**Elnevezés:** Ez az  $r$  elem bal oldali **annullátora**.

Fontos szerepet játszik a balideálmentes gyűrűk leírásában.

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ ,

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test,

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.



# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ ,

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ .

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ ,  
lesz a nullelem  $R$ -ben.



# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból, melyekre  $g + (f) \in I$ .

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból, melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben,

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból, melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ .

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból,

melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ .

Nyilván  $(f) \subseteq J$ ,

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból, melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ .

Nyilván  $(f) \subseteq J$ , ezért  $h \mid f$ .

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból,

melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ .

Nyilván  $(f) \subseteq J$ , ezért  $h \mid f$ . Mivel  $(f)$  irreducibilis, vagy  $h$  egység, így  $I = R$ ,

# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból,

melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ .

Nyilván  $(f) \subseteq J$ , ezért  $h \mid f$ . Mivel  $(f)$  irreducibilis, vagy  $h$  egység, így  $I = R$ , vagy az  $f$ -nek egységsszerese, és  $I$  az  $R$  nulla ideálja.  $\square$



# A faktorgyűrű mikor test

5.2.9. Állítás: Ha  $T$  test és  $f \in T[x]$ , akkor  $T[x]/(f)$  pontosan akkor test, ha  $f$  irreducibilis  $T$  fölött.

## Második, elegáns (számolásmentes) bizonyítás

Tegyük föl, hogy  $f$  irreducibilis, és legyen  $T = T[x]/(f)$ .

Elég belátni, hogy  $R$  egységelemes, nullosztómentes és egyszerű.

Nyilván  $1 + (f)$  egységelem.

Ha  $(g + (f))(h + (f))$  nulla  $R$ -ben, akkor  $gh \in (f)$ , azaz  $f \mid gh$ .

Mivel  $T[x]$  alaptételes, minden irreducibilis eleme prím.

Ezért vagy  $f \mid g$  vagy  $f \mid h$ . Az első esetben  $g + (f)$ , a másodikban  $h + (f)$  lesz a nullelem  $R$ -ben. Így  $R$  nullosztómentes.

Ha  $I \triangleleft R$ , akkor álljon  $J$  azokból a  $g \in T[x]$  polinomokból,

melyekre  $g + (f) \in I$ . Ez ideál  $T[x]$ -ben, ezért főideál:  $J = (h)$ .

Nyilván  $(f) \subseteq J$ , ezért  $h \mid f$ . Mivel  $(f)$  irreducibilis, vagy  $h$  egység,

így  $I = R$ , vagy az  $f$ -nek egységsszerese, és  $I$  az  $R$  nulla ideálja.  $\square$

( $J$  az  $I$  teljes inverz képe a természetes homomorfizmusnál.)

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni.

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni.  
Ezért bevezettük  $\mathbb{C}$ -t,

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni.  
Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.  
A bevezetés egy lehetséges módja a következő.

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

(1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel,

# Polinomok „nemlétező” gyökei

## Példa

A  $x^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg.

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf részttestet alkotnak,



# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf részttestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) **Definiáljuk**  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek,

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) **Definiáljuk**  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek, és igazoljuk, hogy test.

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) **Definiáljuk**  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek, és igazoljuk, hogy test.
- (3) **Azonosítsuk**  $a \in \mathbb{R}$ -et  $a + (x^2 + 1)$ -gyel,

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) **Definiáljuk**  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek, és igazoljuk, hogy test.
- (3) **Azonosítsuk**  $a \in \mathbb{R}$ -et  $a + (x^2 + 1)$ -gyel, és mutassuk meg, hogy ezek az elemek  $\mathbb{R}$ -rel izomorf résztestet alkotnak.

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) **Definiáljuk**  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek, és igazoljuk, hogy test.
- (3) **Azonosítsuk**  $a \in \mathbb{R}$ -et  $a + (x^2 + 1)$ -gyel, és mutassuk meg, hogy ezek az elemek  $\mathbb{R}$ -rel izomorf résztestet alkotnak.
- (4) **Definiáljuk**  $i$ -t  $x + (x^2 + 1)$ -nek,

# Polinomok „nemlétező” gyökei

## Példa

A  $z^2 + 1$ -nek nincs gyöke  $\mathbb{R}$ -ben, de  $i$ -vel kényelmes számolni. Ezért bevezettük  $\mathbb{C}$ -t, az  $\mathbb{R}$  egy **testbővítését**.

A bevezetés egy lehetséges módja a következő.

- (1) Tudjuk, hogy  $\mathbb{R}[x]/(x^2 + 1)$  izomorf  $\mathbb{C}$ -vel, és  $a + bi$ -nek az  $a + bx + (x^2 + 1)$  mellékosztály felel meg. Így az  $a + (x^2 + 1)$  alakú mellékosztályok  $\mathbb{R}$ -rel izomorf résztestet alkotnak, az  $i$ -nek megfelelő elem  $x + (x^2 + 1)$ .
- (2) **Definiáljuk**  $\mathbb{C}$ -t  $\mathbb{R}[x]/(x^2 + 1)$ -nek, és igazoljuk, hogy test.
- (3) **Azonosítsuk**  $a \in \mathbb{R}$ -et  $a + (x^2 + 1)$ -gyel, és mutassuk meg, hogy ezek az elemek  $\mathbb{R}$ -rel izomorf résztestet alkotnak.
- (4) **Definiáljuk**  $i$ -t  $x + (x^2 + 1)$ -nek, és lássuk be, hogy ez gyöke a  $z^2 + 1$  polinomnak.

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom,



# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest,

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ ,

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.  
A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben.

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben. Végezzük el a  $k = k + (s)$  azonosítást

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben.

Végezzük el a  $k = k + (s)$  azonosítást

(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).



# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben. Végezzük el a  $k = k + (s)$  azonosítást (az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).

Legyen  $\alpha = x + (s) \in L$ .

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben.

Végezzük el a  $k = k + (s)$  azonosítást

(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).

Legyen  $\alpha = x + (s) \in L$ . Be kell látni, hogy  $\alpha$  gyöke  $s$ -nek.

# Testbővítés konstrukciója

## 6.4.3. Tétel

Ha  $K$  test, és  $s$  egy  $K$  fölött irreducibilis polinom, akkor **létezik** olyan  $L$  test, amelyben  $K$  résztest, és amelyben az  $s$  polinomnak már **van gyöke**.

## Bizonyítás

Legyen  $L = K[x]/(s)$ , ez test, mert  $s$  irreducibilis.

A  $k \mapsto k + (s)$  megfeleltetés nyilván művelettartó és injektív.

Ezért a  $k + (s)$  elemek ( $k \in K$ ) a  $K$ -val izomorf résztestet alkotnak  $L$ -ben. Végezzük el a  $k = k + (s)$  azonosítást

(az azonosítás precíz részleteit lásd Kiss-jegyzet, 361. oldal).

Legyen  $\alpha = x + (s) \in L$ . Be kell látni, hogy  $\alpha$  gyöke  $s$ -nek.

Ezzel a bizonyítást be is fejezzük majd.

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ .

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk.

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek. Így  $\alpha = x + (s)$  miatt

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek. Így  $\alpha = x + (s)$  miatt  $s(\alpha) =$



# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk.

Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

Így  $\alpha = x + (s)$  miatt  $s(\alpha) =$

$$= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n =$$

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

Így  $\alpha = x + (s)$  miatt  $s(\alpha) =$   
 $= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n =$   
 $= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s),$   
vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

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

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,



# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a ( $k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,  $B = x + 1 + (x^2 + x + 1)$ .

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a  $(k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,  $B = x + 1 + (x^2 + x + 1)$ .

**Azonosítás:**  $O \leftrightarrow 0$ ,

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a  $(k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,  $B = x + 1 + (x^2 + x + 1)$ .

**Azonosítás:**  $O \leftrightarrow 0$ ,  $E \leftrightarrow 1$ ,

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a  $(k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,  $B = x + 1 + (x^2 + x + 1)$ .

**Azonosítás:**  $0 \leftrightarrow 0$ ,  $E \leftrightarrow 1$ ,  $z^2 + z + 1 \leftrightarrow Ez^2 + Ez + E$ .

# Gyök a bővítésben

## Bizonyítás (folytatás)

Legyen  $s(z) = k_0 + k_1z + \dots + k_nz^n \in K[z]$ . Az  $s$ -et  $L[z]$ -beli polinomnak képzeljük, hogy  $\alpha$ -t helyettesíthessünk. Ezért  $s$  együtthatói a  $(k_j$ -vel azonosított)  $k_j + (s)$  elemek.

$$\begin{aligned} \text{Így } \alpha = x + (s) \text{ miatt } s(\alpha) &= \\ &= (k_0 + (s)) + (k_1 + (s))(x + (s)) + \dots + (k_n + (s))(x + (s))^n = \\ &= k_0 + k_1x + \dots + k_nx^n + (s) = s + (s) = (s), \end{aligned}$$

vagyis a  $K[x]/(s)$  faktorgyűrű nulleleme.

Ezért  $\alpha$  tényleg gyöke az  $s$  polinomnak. □

A  $\mathbb{Z}_2[x]/(x^2 + x + 1)$  négyelemű testben  $E = 1 + (x^2 + x + 1)$ ,  
 $0 = (x^2 + x + 1)$ ,  $A = x + (x^2 + x + 1)$ ,  $B = x + 1 + (x^2 + x + 1)$ .

**Azonosítás:**  $0 \leftrightarrow 0$ ,  $E \leftrightarrow 1$ ,  $z^2 + z + 1 \leftrightarrow Ez^2 + Ez + E$ .

Az  $\alpha = A$  elem tényleg gyöke  $Ez^2 + Ez + E$ -nek.

# Karakterisztika

Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám,

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje



# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás”

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

## 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű.

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

## 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű. Ekkor vagy

(1) van olyan  $p \in \mathbb{Z}$  prímszám, hogy  $pr = 0$  minden  $r \in R$ -re,

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

## 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű. Ekkor vagy

- (1) van olyan  $p \in \mathbb{Z}$  prímszám, hogy  $pr = 0$  minden  $r \in R$ -re, ekkor  $R$  karakterisztikája  $p$ ,

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

## 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű. Ekkor vagy

- (1) van olyan  $p \in \mathbb{Z}$  prímszám, hogy  $pr = 0$  minden  $r \in R$ -re, ekkor  $R$  karakterisztikája  $p$ , vagy
- (2) tetszőleges  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$  esetén  $nr \neq 0$ ,

# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

## 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű. Ekkor vagy

- (1) van olyan  $p \in \mathbb{Z}$  prímszám, hogy  $pr = 0$  minden  $r \in R$ -re, ekkor  $R$  karakterisztikája  $p$ , vagy
- (2) tetszőleges  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$  esetén  $nr \neq 0$ , ekkor  $R$  karakterisztikája  $0$ .



# Karakterisztika

## Emlékeztető (2.2.19, 2.2.37)

Ha  $R$  gyűrű,  $r \in R$  és  $n \geq 0$  egész szám, akkor  $nr$  azt jelenti, hogy  $r$ -nek  $n$  példányát összeadjuk.

Ha  $n < 0$ , akkor  $nr$  a  $(-n)r$  ellentettje (ami  $(-n)(-r)$  is).

Ez  $R$  additív csoportjában a „hatványozás” (többszörös).

## 5.8.1. Állítás, 5.8.2. Definíció

Tegyük föl, hogy  $R$  nullosztómentes gyűrű. Ekkor vagy

- (1) van olyan  $p \in \mathbb{Z}$  prímszám, hogy  $pr = 0$  minden  $r \in R$ -re, ekkor  $R$  karakterisztikája  $p$ , vagy
- (2) tetszőleges  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$  esetén  $nr \neq 0$ , ekkor  $R$  karakterisztikája  $0$ .

Valójában  $R^+$  elemeinek rendjeit írjuk le.

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ ,

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .  
Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek,

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s$



# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ ,

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek.

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együttthátója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r$$



# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együttthátója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel  $R$  nullosztómentes,  $ar = 0$  vagy  $br = 0$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel  $R$  nullosztómentes,  $ar = 0$  vagy  $br = 0$ . Az első esetben

$$m = o(r) \mid a,$$

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel  $R$  nullosztómentes,  $ar = 0$  vagy  $br = 0$ . Az első esetben  $m = o(r) \mid a$ , vagyis  $a \mid m$  miatt  $a = m$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel  $R$  nullosztómentes,  $ar = 0$  vagy  $br = 0$ . Az első esetben

$m = o(r) \mid a$ , vagyis  $a \mid m$  miatt  $a = m$ . A második esetben

ugyanígy kapjuk, hogy  $b = m$ .

# Karakterisztika: bizonyítás

## Bizonyítás

Tegyük föl, hogy  $0 \neq r \in R$  és  $0 \neq n \in \mathbb{Z}$ , melyre  $nr = 0$ .

Az  $R^+$  additív csoportban az elemrend jele  $o(r)$ .

Tehát  $n$  „jó kitevője” (jó együtthatója)  $r$ -nek, és így  $m = o(r) \mid n$ .

Persze  $mr = 0$ . Ha  $s \in R$ , akkor  $0 = (mr)s = r(ms)$ .

Mivel  $R$  nullosztómentes és  $r \neq 0$ , innen  $ms = 0$  adódik.

Tehát  $o(s)$  véges, és osztója  $m = o(r)$ -nek.

Az  $r$  és  $s$  szerepét kicserélve  $s \neq 0$  esetén  $o(s) = o(r) = m$ .

Az (1)-hez már csak azt kell megmutatni, hogy  $m$  prímszám.

Tegyük föl, hogy  $m = ab$ , ahol  $a, b$  pozitív egészek. Ekkor

$$0 = (mr)r = (ar)(br).$$

Mivel  $R$  nullosztómentes,  $ar = 0$  vagy  $br = 0$ . Az első esetben

$m = o(r) \mid a$ , vagyis  $a \mid m$  miatt  $a = m$ . A második esetben

ugyanígy kapjuk, hogy  $b = m$ . Ezért  $m$  tényleg prímszám. □

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:



# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben **tagonként lehet  $p$ -edik hatványra emelni:**

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus**.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus**.

Ugyanez az állítás érvényes  $p$  hatványaira is.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus**.

Ugyanez az állítás érvényes  $p$  hatványaira is.

**Endomorfizmus:** önmagába képző homomorfizmus.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben **tagonként lehet  $p$ -edik hatványra emelni:**

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus.**

Ugyanez az állítás érvényes  $p$  hatványaira is.

**Endomorfizmus:** önmagába képző homomorfizmus.

$\psi$  szorzattartása nyilvánvaló, mert  $R$  kommutatív.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben **tagonként lehet  $p$ -edik hatványra emelni:**

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus.**

Ugyanez az állítás érvényes  $p$  hatványaira is.

**Endomorfizmus:** önmagába képző homomorfizmus.

$\psi$  szorzattartása nyilvánvaló, mert  $R$  kommutatív.

Az összegtartás a **binomiális tételből** következik.

# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus**.

Ugyanez az állítás érvényes  $p$  hatványaira is.

**Endomorfizmus:** önmagába képző homomorfizmus.

$\psi$  szorzattartása nyilvánvaló, mert  $R$  kommutatív.

Az összegtartás a **binomiális tételből** következik.

Elemi számelmélet:  $\binom{p}{j}$  osztható  $p$ -vel, ha  $0 < j < p$ .



# A Frobenius-endomorfizmus

## 5.8.4. Tétel

Legyen  $R$  kommutatív,  $p$  karakterisztikájú gyűrű, ahol  $p$  prím.  
Ekkor  $R$ -ben tagonként lehet  $p$ -edik hatványra emelni:

$$(r + s)^p = r^p + s^p \quad (r, s \in R).$$

Ezért a  $\psi(r) = r^p$  leképezés gyűrűhomomorfizmus  $R$ -ből  $R$ -be.

Neve: **Frobenius-endomorfizmus**.

Ugyanez az állítás érvényes  $p$  hatványaira is.

**Endomorfizmus:** önmagába képző homomorfizmus.

$\psi$  szorzattartása nyilvánvaló, mert  $R$  kommutatív.

Az összegtartás a **binomiális tételből** következik.

Elemi számelmélet:  $\binom{p}{j}$  osztható  $p$ -vel, ha  $0 < j < p$ .

A  $p^k$ -ra emelés  $\psi^k$  ( $k$  tényezős kompozíció). □

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest,

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest,  
amely  $T$  minden résztestének része

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest,  
amely  $T$  minden résztestének része (**legszűkebb résztest**).

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest,  
amely  $T$  minden résztestének része (**legszűkebb résztest**).

A legszűkebb résztest neve:  $P$  a  $T$  **prímteste**.

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem. Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .



# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem. Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .  
Ezért  $P$  részcsoport

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem. Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .

Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem. Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (**legszűkebb résztest**).

A legszűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .

Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

Ez tartja a szorzást is:  $(me)(ne) = (mn)e^2 = (mn)e$ .

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem. Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .

Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

Ez tartja a szorzást is:  $(me)(ne) = (mn)e^2 = (mn)e$ .

**Legsűkebb:** Legyen  $K \leq T$  résztest.

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem. Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest, amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .

Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

Ez tartja a szorzást is:  $(me)(ne) = (mn)e^2 = (mn)e$ .

**Legsűkebb:** Legyen  $K \leq T$  résztest.

Ekkor  $K \neq \{0\}$ , és így  $K^\times$  részcsoportja  $T^\times$ -nek.

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest,  
amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .

Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

Ez tartja a szorzást is:  $(me)(ne) = (mn)e^2 = (mn)e$ .

**Legsűkebb:** Legyen  $K \leq T$  résztest.

Ekkor  $K \neq \{0\}$ , és így  $K^\times$  részcsoportja  $T^\times$ -nek.

Ezért  $T$  egységeleme,  $e \in K$ .

# Prímtest $p$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $p > 0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{0, e, 2e, 3e, \dots, (p-1)e\}$   $\mathbb{Z}_p$ -vel izomorf résztest,  
amely  $T$  minden résztestének része (**legsűkebb résztest**).

A legsűkebb résztest neve:  $P$  a  $T$  **prímteste**.

## Bizonyítás

Mivel  $e \neq 0$  de  $pe = 0$ , az  $e$  elem rendje  $p$ .

Ezért  $P$  részcsoport és  $m \mapsto me$  izomorfizmus  $\mathbb{Z}_p^+$  és  $P^+$  között.

Ez tartja a szorzást is:  $(me)(ne) = (mn)e^2 = (mn)e$ .

**Legsűkebb:** Legyen  $K \leq T$  résztest.

Ekkor  $K \neq \{0\}$ , és így  $K^\times$  részcsoportja  $T^\times$ -nek.

Ezért  $T$  egységeleme,  $e \in K$ . Így  $P \subseteq K$ . □

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,



# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.

Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf résztest,

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.

Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf résztest, amely  $T$  minden résztestének része

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.

Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf résztest, amely  $T$  minden résztestének része (**prímtest**).

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között.

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó**: nyilván.



# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó**: nyilván.  
**Jóldefiniált**:  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó**: nyilván.  
**Jóldefiniált**:  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.  
Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.

Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó**: nyilván.

**Jóldefiniált**:  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.

Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

**Szürjektív**: nyilván.

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (**prímtest**).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.

Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó**: nyilván.

**Jóldefiniált**:  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.

Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

**Szürjektív**: nyilván. **Injektív**: elég, hogy  $\text{Ker}(\psi) = \{0\}$ .

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (prímtest).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.

Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó:** nyilván.

**Jóldefiniált:**  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.

Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

**Szürjektív:** nyilván. **Injektív:** elég, hogy  $\text{Ker}(\psi) = \{0\}$ .

Ha  $(me)/(ne) = 0$  akkor  $me = 0$ ,

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (prímtest).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó:** nyilván.

**Jóldefiniált:**  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.

Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

**Szürjektív:** nyilván. **Injektív:** elég, hogy  $\text{Ker}(\psi) = \{0\}$ .

Ha  $(me)/(ne) = 0$  akkor  $me = 0$ , ezért  $m = 0$  mert  $o(e) = \infty$ .

# Prímtest $0$ karakterisztikában

## 5.8.7. Tétel

Legyen  $T$  egy  $0$  karakterisztikájú test,  $e$  az egységelem.  
Ekkor  $P = \{(me)/(ne) : m, n \in \mathbb{Z}, n \neq 0\}$  egy  $\mathbb{Q}$ -val izomorf  
részttest, amely  $T$  minden részttestének része (prímtest).

## Bizonyítás

Mivel  $e \neq 0$  és a karakterisztika  $0$ , az  $e$  elem rendje végtelen.  
Ellenőrizni kell, hogy  $\psi : m/n \mapsto (me)/(ne)$  jóldefiniált,  
és izomorfizmus  $\mathbb{Q}$  és  $P$  között. **Művelettartó:** nyilván.

**Jóldefiniált:**  $m/n = u/v \implies (me)/(ne) = (ue)(ve)$  HF.

Továbbá  $ne \neq 0$  ha  $n \neq 0$ , mert  $e$  rendje végtelen.

**Szürjektív:** nyilván. **Injektív:** elég, hogy  $\text{Ker}(\psi) = \{0\}$ .

Ha  $(me)/(ne) = 0$  akkor  $me = 0$ , ezért  $m = 0$  mert  $o(e) = \infty$ .

**Legszűkebb:** mint a  $p$  karakterisztikájú esetben. □

# Az algebra fogalma

## 5.10.3. Definíció

$A$  algebra a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött,



# Az algebra fogalma

## 5.10.3. Definíció

**A algebra** a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

# Az algebra fogalma

## 5.10.3. Definíció

$A$  algebra a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .

# Az algebra fogalma

## 5.10.3. Definíció

$A$  algebra a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .  
Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).

# Az algebra fogalma

## 5.10.3. Definíció

$A$  algebra a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .

Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).

(A  $T$  egy elemével, mint skalárral való szorzás az  $R$ -beli szorzás.)

# Az algebra fogalma

## 5.10.3. Definíció

A **algebra** a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .

Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).

(A  $T$  egy elemével, mint skalárral való szorzás az  $R$ -beli szorzás.)

## Példák

- A  $T[x_1, \dots, x_n]$  polinomgyűrű a  $T$  test fölött.

# Az algebra fogalma

## 5.10.3. Definíció

A **algebra** a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .

Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).

(A  $T$  egy elemével, mint skalárral való szorzás az  $R$ -beli szorzás.)

## Példák

- A  $T[x_1, \dots, x_n]$  polinomgyűrű a  $T$  test fölött.
- Ha  $K \leq L$  testbővítés, akkor  $L$  a  $K$  fölött.

# Az algebra fogalma

## 5.10.3. Definíció

A **algebra** a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .

Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).

(A  $T$  egy elemével, mint skalárral való szorzás az  $R$ -beli szorzás.)

## Példák

- A  $T[x_1, \dots, x_n]$  polinomgyűrű a  $T$  test fölött.
- Ha  $K \leq L$  testbővítés, akkor  $L$  a  $K$  fölött.
- A  $T$  test fölötti  $n \times n$ -es mátrixok.

# Az algebra fogalma

## 5.10.3. Definíció

A **algebra** a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .

Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).

(A  $T$  egy elemével, mint skalárral való szorzás az  $R$ -beli szorzás.)

## Példák

- A  $T[x_1, \dots, x_n]$  polinomgyűrű a  $T$  test fölött.
- Ha  $K \leq L$  testbővítés, akkor  $L$  a  $K$  fölött.
- A  $T$  test fölötti  $n \times n$ -es mátrixok.
- A  $T$  test fölötti  $V$  vektortér lineáris transzformációi.



# Az algebra fogalma

## 5.10.3. Definíció

A **algebra** a  $T$  test fölött, ha egyszerre gyűrű, vektortér  $T$  fölött, és  $\lambda(ab) = (\lambda a)b = a(\lambda b)$  minden  $a, b \in A$  és  $\lambda \in T$  esetén.

Legyen  $R$  egységelemes gyűrű,  $T$  részteste  $R$ -nek, és  $1_R = 1_T$ .  
Az  $R$  akkor algebra  $T$  fölött, ha  $\lambda r = r\lambda$  ( $\forall \lambda \in T, \forall r \in R$ ).  
(A  $T$  egy elemével, mint skalárral való szorzás az  $R$ -beli szorzás.)

## Példák

- A  $T[x_1, \dots, x_n]$  polinomgyűrű a  $T$  test fölött.
- Ha  $K \leq L$  testbővítés, akkor  $L$  a  $K$  fölött.
- A  $T$  test fölötti  $n \times n$ -es mátrixok.
- A  $T$  test fölötti  $V$  vektortér lineáris transzformációi.
- A kvaterniók ferdeteste  $\mathbb{R}$  fölött.

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ ,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ .



# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja.

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja.

Ha  $I = \{0\}$ , akkor  $b$  transzcendens,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja.

Ha  $I = \{0\}$ , akkor  $b$  transzcendens, különben algebrai.

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja. Ha  $I = \{0\}$ , akkor  $b$  transzcendens, különben algebrai. Ekkor az  $I$  főideál normált generátoreleme a  $b \in A$  minimálpolinomja,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja. Ha  $I = \{0\}$ , akkor  $b$  transzcendens, különben algebrai. Ekkor az  $I$  főideál normált generátoreleme a  $b \in A$  minimálpolinomja, jele  $m_b$ .

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja. Ha  $I = \{0\}$ , akkor  $b$  transzcendens, különben algebrai. Ekkor az  $I$  főideál normált generátoreleme a  $b \in A$  minimálpolinomja, jele  $m_b$ . Továbbá  $f(b) = 0 \iff m_b \mid f$ .

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha  $A$  algebra a  $T$  test fölött,  $f(x) = a_0 + a_1x + \dots + a_nx^n \in T[x]$  és  $b \in A$ , akkor  $f(b) = a_01_A + a_1b + \dots + a_nb^n$  (behelyettesítés).

Tehát  $f$  konstans tagját  $A$  egységelemével szorozzuk.

5.10.7. Gyakorlat:  $f(a) + g(a) = (f + g)(a)$  és  $(fg)(a) = f(a)g(a)$ .

## 5.10.8, 5.10.11. Definíció

Az  $f \in T[x]$  jó polinomja  $b \in A$ -nak, ha  $f(b) = 0$ . Ezek egy  $I$  ideált alkotnak, ami az  $f \mapsto f(b)$  homomorfizmus magja. Ha  $I = \{0\}$ , akkor  $b$  transzcendens, különben algebrai. Ekkor az  $I$  főideál normált generátoreleme a  $b \in A$  minimálpolinomja, jele  $m_b$ . Továbbá  $f(b) = 0 \iff m_b \mid f$ .

Bizonyítás: mint a testbővítéseknel.



# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha  $\dim_{\mathcal{T}}(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_{\mathcal{T}}(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ .

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_{\mathcal{T}}(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_{\mathcal{T}}(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0,

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_{\mathcal{T}}(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0, és  $b$  gyöke  $f$ -nek.  $\square$

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0, és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.  
Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.



# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált,

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0, és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált, irreducibilis

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.  
Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.  
Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ ,

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.  
Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.  
Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.  
Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.  
Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

**Valóban:** ha  $m_b = gh$ , akkor  $0 = m_b(b) = g(b)h(b)$ .

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

**Valóban:** ha  $m_b = gh$ , akkor  $0 = m_b(b) = g(b)h(b)$ . Ezért vagy  
 $g(b) = 0$

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0, és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

**Valóban:** ha  $m_b = gh$ , akkor  $0 = m_b(b) = g(b)h(b)$ . Ezért vagy  
 $g(b) = 0$  (így  $m_b \mid g$  miatt  $h$  egység),

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem  $0$ , és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

**Valóban:** ha  $m_b = gh$ , akkor  $0 = m_b(b) = g(b)h(b)$ . Ezért vagy  $g(b) = 0$  (így  $m_b \mid g$  miatt  $h$  egység), vagy  $h(b) = 0$  és  $g$  egység.



# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0, és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

**Valóban:** ha  $m_b = gh$ , akkor  $0 = m_b(b) = g(b)h(b)$ . Ezért vagy  
 $g(b) = 0$  (így  $m_b \mid g$  miatt  $h$  egység), vagy  $h(b) = 0$  és  $g$  egység.

**Megfordítva:** ha  $f(b) = 0$ , akkor  $m_b \mid f$ ,

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

**Valóban:** ha  $\dim_T(A) = n$ , akkor  $1, b, \dots, b^n$  már összefügg:  
 $\lambda_0 1 + \lambda_1 b + \dots + \lambda_n b^n = 0$ . Legyen  $f(x) = \lambda_0 + \lambda_1 x + \dots + \lambda_n x^n$ ,  
akkor  $f$  nem 0, és  $b$  gyöke  $f$ -nek.  $\square$

## 5.10.12. Tétel

Legyen  $A$  nullosztómentes algebra és  $b \in A$  algebrai elem.

Ekkor  $b$  minimálpolinomja irreducibilis  $T$  fölött.

Ha  $f \in T[x]$  normált, irreducibilis és  $f(b) = 0$ , akkor  $f = m_b$ .

**Valóban:** ha  $m_b = gh$ , akkor  $0 = m_b(b) = g(b)h(b)$ . Ezért vagy  $g(b) = 0$  (így  $m_b \mid g$  miatt  $h$  egység), vagy  $h(b) = 0$  és  $g$  egység.

**Megfordítva:** ha  $f(b) = 0$ , akkor  $m_b \mid f$ , de mindkettő irreducibilis és normált, ezért egyenlők.  $\square$

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel,



# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,  $\mathbb{R}$  fölötti,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,  $\mathbb{R}$  fölötti, de nem véges dimenziós.



# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,  $\mathbb{R}$  fölötti, de nem véges dimenziós. Sőt,  $\mathbb{R}$  egyszerű transzcendens bővítése még test is.

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,  $\mathbb{R}$  fölötti, de nem véges dimenziós. Sőt,  $\mathbb{R}$  egyszerű transzcendens bővítése még test is.
- $\mathbb{R}^{3 \times 3}$  véges dimenziós,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,  $\mathbb{R}$  fölötti, de nem véges dimenziós. Sőt,  $\mathbb{R}$  egyszerű transzcendens bővítése még test is.
- $\mathbb{R}^{3 \times 3}$  véges dimenziós,  $\mathbb{R}$  fölötti,

# Frobenius tétele

## 5.11.6. Tétel, NB

Ha  $A$  véges dimenziós, nullosztómentes, nem nulla algebra  $\mathbb{R}$  fölött, akkor  $A$  vagy a valós számtesttel, vagy a komplex számtesttel, vagy a kvaterniók ferdetestével izomorf.

Vagyis a számkört nem lehet már tovább bővíteni, ha a nullosztómentességet és az asszociativitást megtartjuk.

## A Frobenius-tétel feltételei szükségesek (5.11.1. Gyakorlat)

- Ha nem  $\mathbb{R}$  fölött vagyunk:  $\mathbb{Q}$  véges bővítései mind nullosztómentesek és véges dimenziósak (pl.  $\mathbb{Q}(\sqrt[n]{2})$ ).
- $\mathbb{R}[x]$  nullosztómentes,  $\mathbb{R}$  fölötti, de nem véges dimenziós. Sőt,  $\mathbb{R}$  egyszerű transzcendens bővítése még test is.
- $\mathbb{R}^{3 \times 3}$  véges dimenziós,  $\mathbb{R}$  fölötti, de nem nullosztómentes.

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van.

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1,

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .



# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

**HF:** Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

**HF:** Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

**HF:** Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

**Valóban,** ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

**Megfordítva:** ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ ,

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ .

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

**HF:** Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

**Valóban,** ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

**Megfordítva:** ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?

Magyarázat:  $x^2 + 1 = (x + i)(x - i)$  a „gyöktényezős alak”.



# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?

Magyarázat:  $x^2 + 1 = (x + i)(x - i)$  a „gyöktényezős alak”.

Ide  $j \in \mathbb{K}$ -t helyettesítve a bal oldal nulla lesz,

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?

Magyarázat:  $x^2 + 1 = (x + i)(x - i)$  a „gyöktényezős alak”.

Ide  $j \in \mathbb{K}$ -t helyettesítve a bal oldal nulla lesz, de a jobb oldal nem:

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?

Magyarázat:  $x^2 + 1 = (x + i)(x - i)$  a „gyöktényezős alak”.

Ide  $j \in \mathbb{K}$ -t helyettesítve a bal oldal nulla lesz, de a jobb oldal nem:

$$(j + i)(j - i) = j^2 + ij - ji - i^2 = ij - ji = 2k \neq 0.$$

# A polinomok azonossági tétele

## 5.11.5. Következmény

Az  $x^2 + 1$  polinomnak a kvaterniók között végtelen sok gyöke van. Ezek pontosan azok, amelyek valós része nulla és normája 1, vagyis a  $qi + rj + sk$  alakú kvaterniók, ahol  $q^2 + r^2 + s^2 = 1$ .

HF: Az  $\alpha = a + bi + cj + dk$  minimálpolinomja  $x^2 - 2ax + N(\alpha)$ .

Valóban, ha  $N(z) = 1$  és  $\bar{z} = -z$ , akkor  $z^2 = -z\bar{z} = -N(z) = -1$ .

Megfordítva: ha  $z^2 = -1$ , akkor  $1 = N(z^2) = N(z)^2$ , így  $N(z) = 1$ .

Ezért  $1 = z\bar{z} = -z^2$ . Innen  $z \neq 0$  miatt  $\bar{z} = -z$ .  $\square$

Hogyan lehet egy másodfokú polinomnak végtelen sok gyöke?

Magyarázat:  $x^2 + 1 = (x + i)(x - i)$  a „gyöktényezős alak”.

Ide  $j \in \mathbb{K}$ -t helyettesítve a bal oldal nulla lesz, de a jobb oldal nem:

$$(j + i)(j - i) = j^2 + ij - ji - i^2 = ij - ji = 2k \neq 0.$$

Mivel  $ij \neq ji$ , nem tudjuk kihasználni, hogy  $\mathbb{K}$  nullosztómentes.

# Kvaterniók és térvektorok

Tiszta kvaternió:  $v = xi + yj + zk$  (valós része nulla).

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort.

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ .



# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat),

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ ,

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ ,

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ ,

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ .

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .



# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .
- Tehát ha  $N(z) = 1$  és  $v \perp w$ , akkor  $zwz^{-1} = z^2w$ .

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .
- Tehát ha  $N(z) = 1$  és  $v \perp w$ , akkor  $zwz^{-1} = z^2w$ . Speciálisan ha  $z = \cos \alpha + v \sin \alpha$ , ahol  $N(v) = 1$ ,

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .
- Tehát ha  $N(z) = 1$  és  $v \perp w$ , akkor  $zwz^{-1} = z^2w$ . Speciálisan ha  $z = \cos \alpha + v \sin \alpha$ , ahol  $N(v) = 1$ , akkor  $v^2 = -1$  (mert  $v$  tiszta),

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .
- Tehát ha  $N(z) = 1$  és  $v \perp w$ , akkor  $zwz^{-1} = z^2w$ . Speciálisan ha  $z = \cos \alpha + v \sin \alpha$ , ahol  $N(v) = 1$ , akkor  $v^2 = -1$  (mert  $v$  tiszta),  $z^2 = \cos(2\alpha) + v \sin(2\alpha)$ ,

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .
- Tehát ha  $N(z) = 1$  és  $v \perp w$ , akkor  $zwz^{-1} = z^2w$ .  
Speciálisan ha  $z = \cos \alpha + v \sin \alpha$ , ahol  $N(v) = 1$ , akkor  $v^2 = -1$  (mert  $v$  tiszta),  $z^2 = \cos(2\alpha) + v \sin(2\alpha)$ , és így  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)vw = \cos(2\alpha)w + \sin(2\alpha)(v \times w)$ .

# Kvaterniók és térvektorok

**Tiszta kvaternió:**  $v = xi + yj + zk$  (valós része nulla). Azonosítsuk ezzel az  $(x, y, z)^T \in \mathbb{R}^3$  vektort. Legyen  $z = r + v$  ( $r \in \mathbb{R}$ ).

- Ha  $N(z) = 1$ , akkor  $z^{-1} = \bar{z}$ . Ha  $z$  tiszta is, akkor  $z^{-1} = -z$ .
- Ha  $v$  és  $w$  tiszta kvaterniók, akkor  $vw = v \times w - \langle v, w \rangle$  (vektoriális, illetve skaláris szorzat), mert  $i^2 = j^2 = k^2 = -1$ , továbbá  $ij = i \times j$ ,  $ji = j \times i$ ,  $jk = j \times k$ , stb.
- Így ha  $v \perp w$ , akkor  $vw = v \times w = -w \times v = -wv$ , ahonnan  $w^{-1}vw = -v$ , és  $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \bar{z}$ . Balról  $zw$ -vel szorozva  $zw\bar{z} = z^2w$ .
- Tehát ha  $N(z) = 1$  és  $v \perp w$ , akkor  $zwz^{-1} = z^2w$ .  
Speciálisan ha  $z = \cos \alpha + v \sin \alpha$ , ahol  $N(v) = 1$ , akkor  $v^2 = -1$  (mert  $v$  tiszta),  $z^2 = \cos(2\alpha) + v \sin(2\alpha)$ , és így  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)vw = \cos(2\alpha)w + \sin(2\alpha)(v \times w)$ .  
Ha  $N(w)$  is 1, akkor  $v$ ,  $w$  és  $v \times w$  ONB a térben. □

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $1$  normájú) kvaterniókkal való konjugálások.

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $1$  normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $v$  egységvektor, akkor a  $z = \cos \alpha + v \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $v$  irányú egyenes körül.



# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $\mathbf{1}$  normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $\mathbf{v}$  egységvektor, akkor a  $\mathbf{z} = \cos \alpha + \mathbf{v} \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $\mathbf{v}$  irányú egyenes körül.

## Bizonyítás

Legyen  $\mathbf{w}$  egy  $\mathbf{v}$ -re merőleges egységvektor. Írjuk föl a  $\mathbf{z}$ -vel való konjugálás mátrixát a  $\mathbf{v}, \mathbf{w}, \mathbf{vw} = \mathbf{v} \times \mathbf{w}$  ONB-ben.

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $\mathbf{1}$  normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $\mathbf{v}$  egységvektor, akkor a  $\mathbf{z} = \cos \alpha + \mathbf{v} \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $\mathbf{v}$  irányú egyenes körül.

## Bizonyítás

Legyen  $\mathbf{w}$  egy  $\mathbf{v}$ -re merőleges egységvektor. Írjuk föl a  $\mathbf{z}$ -vel való konjugálás mátrixát a  $\mathbf{v}, \mathbf{w}, \mathbf{vw} = \mathbf{v} \times \mathbf{w}$  ONB-ben. Nyilván  $\mathbf{z}\mathbf{v}\mathbf{z}^{-1} = \mathbf{v}$

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $\mathbf{1}$  normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $\mathbf{v}$  egységvektor, akkor a  $\mathbf{z} = \cos \alpha + \mathbf{v} \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $\mathbf{v}$  irányú egyenes körül.

## Bizonyítás

Legyen  $\mathbf{w}$  egy  $\mathbf{v}$ -re merőleges egységvektor. Írjuk föl a  $\mathbf{z}$ -vel való konjugálás mátrixát a  $\mathbf{v}, \mathbf{w}, \mathbf{vw} = \mathbf{v} \times \mathbf{w}$  ONB-ben. Nyilván  $\mathbf{zvz}^{-1} = \mathbf{v}$  (hiszen  $\mathbf{zv} = \mathbf{vz}$ ),

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $1$  normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $v$  egységvektor, akkor a  $z = \cos \alpha + v \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $v$  irányú egyenes körül.

## Bizonyítás

Legyen  $w$  egy  $v$ -re merőleges egységvektor. Írjuk föl a  $z$ -vel való konjugálás mátrixát a  $v, w, vw = v \times w$  ONB-ben. Nyilván  $zvz^{-1} = v$  (hiszen  $zv = vz$ ), és az iménti képletek alapján  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$ .

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z 1 normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $v$  egységvektor, akkor a  $z = \cos \alpha + v \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $v$  irányú egyenes körül.

## Bizonyítás

Legyen  $w$  egy  $v$ -re merőleges egységvektor. Írjuk föl a  $z$ -vel való konjugálás mátrixát a  $v, w, vw = v \times w$  ONB-ben. Nyilván  $zvz^{-1} = v$  (hiszen  $zv = vz$ ), és az iménti képletek alapján  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$ . A kettőt összeszorozva  $z(vw)z^{-1} = (zvz^{-1})(zwz^{-1}) = \cos(2\alpha)(vw) + \sin(2\alpha)v(vw)$ ,

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z 1 normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $v$  egységvektor, akkor a  $z = \cos \alpha + v \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $v$  irányú egyenes körül.

## Bizonyítás

Legyen  $w$  egy  $v$ -re merőleges egységvektor. Írjuk föl a  $z$ -vel való konjugálás mátrixát a  $v, w, vw = v \times w$  ONB-ben. Nyilván  $zvz^{-1} = v$  (hiszen  $zv = vz$ ), és az iménti képletek alapján  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$ . A kettőt összeszorozva  $z(vw)z^{-1} = (zvz^{-1})(zwz^{-1}) = \cos(2\alpha)(vw) + \sin(2\alpha)v(vw)$ , ahol  $v(vw) = v^2 w = -w$

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z 1 normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $v$  egységvektor, akkor a  $z = \cos \alpha + v \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $v$  irányú egyenes körül.

## Bizonyítás

Legyen  $w$  egy  $v$ -re merőleges egységvektor. Írjuk föl a  $z$ -vel való konjugálás mátrixát a  $v, w, vw = v \times w$  ONB-ben. Nyilván  $zvz^{-1} = v$  (hiszen  $zv = vz$ ), és az iménti képletek alapján  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$ . A kettőt összeszorozva  $z(vw)z^{-1} = (zvz^{-1})(zwz^{-1}) = \cos(2\alpha)(vw) + \sin(2\alpha)v(vw)$ , ahol  $v(vw) = v^2 w = -w$  (már láttuk, hogy  $v^2 = -1$ ).

# Kvaterniók és forgatások

## Tétel

A térbeli, origón átmenő egyenesek körüli forgatások a(z  $1$  normájú) kvaterniókkal való konjugálások. Pontosabban: ha  $v$  egységvektor, akkor a  $z = \cos \alpha + v \sin \alpha$ -val való konjugálás  $2\alpha$  szögű forgatás a  $v$  irányú egyenes körül.

## Bizonyítás

Legyen  $w$  egy  $v$ -re merőleges egységvektor. Írjuk föl a  $z$ -vel való konjugálás mátrixát a  $v, w, vw = v \times w$  ONB-ben. Nyilván  $zvz^{-1} = v$  (hiszen  $zv = vz$ ), és az iménti képletek alapján  $zwz^{-1} = \cos(2\alpha)w + \sin(2\alpha)(vw)$ . A kettőt összeszorozva  $z(vw)z^{-1} = (zvz^{-1})(zwz^{-1}) = \cos(2\alpha)(vw) + \sin(2\alpha)v(vw)$ , ahol  $v(vw) = v^2 w = -w$  (már láttuk, hogy  $v^2 = -1$ ). Ezért a megfelelő forgatás mátrixát kapjuk. □



# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

Előnyök:

Csak négy paraméter;

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

Előnyök:

Csak négy paraméter; numerikusan stabil;

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

Előnyök:

Csak négy paraméter; numerikusan stabil; effektív.

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

**Előnyök:**

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

**Előnyök:**

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

Navigáció,

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

## Előnyök:

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

Navigáció, aerodinamika,



# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

## Előnyök:

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

Navigáció, aerodinamika, molekuláris dinamika,

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

## Előnyök:

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

Navigáció, aerodinamika, molekuláris dinamika, röntgenkristallográfia.

# Euler-mátrix

Az előző bizonyításban kapott mátrix:

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & \cos(2\alpha) & -\sin(2\alpha) \\ 0 & \sin(2\alpha) & \cos(2\alpha) \end{pmatrix}$$

Az  $i, j, k$  bázisban,  $z = r + xi + yj + zk$  esetén (Euler-mátrix):

$$\begin{pmatrix} r^2 + x^2 - y^2 - z^2 & -2rz + 2xy & 2ry + 2xz \\ 2rz + 2xy & r^2 - x^2 + y^2 - z^2 & -2rx + 2yz \\ -2ry + 2xz & 2rx + 2yz & r^2 - x^2 - y^2 + z^2 \end{pmatrix}$$

## Előnyök:

Csak négy paraméter; numerikusan stabil; effektív.

Forgástengely folytonos változtatása (3D játékok grafikája).

Navigáció, aerodinamika, molekuláris dinamika, röntgenkristallográfia.

Számelméleti alkalmazások.

# A kvaterniók mint transzformációk

A kvaternók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött,

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).  
**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .



# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó.

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje.

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen  $\psi(z) = A_{\bar{z}}$ .

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ ,



# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ ,

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

Végül  $\psi$  injektív:

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

Végül  $\psi$  injektív: ha  $\psi(z) = 0$ , akkor  $0 = \psi(z)(1) = 1\bar{z}$ ,

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

Végül  $\psi$  injektív: ha  $\psi(z) = 0$ , akkor  $0 = \psi(z)(1) = 1\bar{z}$ , így  $z = 0$ .

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

Végül  $\psi$  injektív: ha  $\psi(z) = 0$ , akkor  $0 = \psi(z)(1) = 1\bar{z}$ , így  $z = 0$ .

Tehát a  $\mathbb{K}$  gyűrű izomorf  $\text{Hom}(\mathbb{C}^2)$  egy részgyűrűjével.

# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

Végül  $\psi$  injektív: ha  $\psi(z) = 0$ , akkor  $0 = \psi(z)(1) = 1\bar{z}$ , így  $z = 0$ .

Tehát a  $\mathbb{K}$  gyűrű izomorf  $\text{Hom}(\mathbb{C}^2)$  egy részgyűrűjével.

Ha  $z = p + qi + rj + sk$ , akkor  $\psi(z)$  mátrixa az  $(1, j)$  bázisban

$$\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix} \text{ ahol } v = p + qi \text{ és } w = r + si$$



# A kvaterniók mint transzformációk

A kvaterniók vektortér  $\mathbb{C}$  fölött (a skalárral szorzás balszorzás).

**FIGYELEM:** ez **NEM** algebra  $\mathbb{C}$  fölött, mert  $i(j1) \neq j(i1)$ .

Legyen  $A_z$  a  $z \in \mathbb{K}$ -val való jobbszorzás  $\mathbb{K}$ -n:  $A_z(x) = xz$ .

Ez összegtartó. Skalárszorostartó is az asszociativitás miatt:

$A_z(\lambda x) = (\lambda x)z = \lambda(xz) = \lambda A_z(x)$  (ahol  $\lambda \in \mathbb{C}$  és  $x \in \mathbb{K}$ ).

Továbbá  $A_{z_1 z_2}(x) = x(z_1 z_2) = (x z_1) z_2 = A_{z_2} A_{z_1}(x)$ .

Azaz a  $\psi : z \mapsto A_z$  leképezésre  $\psi(z_1 z_2) = \psi(z_2) \psi(z_1)$ .

**Kellemetlen:** megfordul a szorzás sorrendje. **Megoldás:** legyen

$\psi(z) = A_{\bar{z}}$ . Erre  $\psi(z_1 z_2) = \psi(z_1) \psi(z_2)$ , hiszen  $\overline{z_1 z_2} = \bar{z}_2 \bar{z}_1$ .

Továbbá  $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$ , azaz  $\psi$  gyűrűhomomorfizmus.

Végül  $\psi$  injektív: ha  $\psi(z) = 0$ , akkor  $0 = \psi(z)(1) = 1\bar{z}$ , így  $z = 0$ .

Tehát a  $\mathbb{K}$  gyűrű izomorf  $\text{Hom}(\mathbb{C}^2)$  egy részgyűrűjével.

Ha  $z = p + qi + rj + sk$ , akkor  $\psi(z)$  mátrixa az  $(1, j)$  bázisban

$\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$  ahol  $v = p + qi$  és  $w = r + si$  (így vezettük be  $\mathbb{K}$ -t).

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ .

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ ,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyünk föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ .

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánúsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyünk föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ ,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánúsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyünk föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ .

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ ,



# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .  
Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ ,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .  
Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2), (c_1, c_2)$  ONB.

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2), (c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ .

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2)$ ,  $(c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmas  $|\varepsilon| = 1$ -re  $B$  unitér,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2), (c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmos  $|\varepsilon| = 1$ -re  $B$  unitér, 1 determinánsú



# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2)$ ,  $(c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmasság  $|\varepsilon| = 1$ -re  $B$  unitér, 1 determinánsú és  $B(v) = w$ .  $\square$

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2)$ ,  $(c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmos  $|\varepsilon| = 1$ -re  $B$  unitér, 1 determinánsú és  $B(v) = w$ .  $\square$

Jelölje  $SU(2)$  a  $2 \times 2$ -es, komplex elemű,

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2)$ ,  $(c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmos  $|\varepsilon| = 1$ -re  $B$  unitér, 1 determinánsú és  $B(v) = w$ .  $\square$

Jelölje  $SU(2)$  a  $2 \times 2$ -es, komplex elemű, 1 determinánsú

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2)$ ,  $(c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmos  $|\varepsilon| = 1$ -re  $B$  unitér, 1 determinánsú és  $B(v) = w$ .  $\square$

Jelölje  $SU(2)$  a  $2 \times 2$ -es, komplex elemű, 1 determinánsú unitér mátrixok csoportját a szorzásra (4.1.26. Definíció).

# A speciális unitér csoport

Ha  $0 \neq v, w \in \mathbb{C}^2$  hossza egyenlő, akkor pontosan egy olyan 1 determinánsú, unitér transzformáció van, ami  $v$ -t  $w$ -be viszi.

## Bizonyítás

Tegyük föl, hogy van kettő:  $B(v) = C(v)$ . Legyen  $D = B^{-1}C$ , ekkor  $D(v) = v$ . Ha  $u$  egy  $v$ -re merőleges egységvektor, akkor  $D(u) \perp D(v) = v$ , és így  $D(u) \parallel u$ . A  $(v, u)$  bázisban  $\det(D)$ -t felírva  $D(u) = u$ , azaz  $D$  az identitás, és így  $B = C$ .

Legyen  $b_1 = v/\|v\|$ ,  $c_1 = w/\|w\|$ , és  $(b_1, b_2)$ ,  $(c_1, c_2)$  ONB. Előírhatósági tétel: van  $B$ , melyre  $B(b_1) = c_1$  és  $B(b_2) = \varepsilon c_2$ . Alkalmos  $|\varepsilon| = 1$ -re  $B$  unitér, 1 determinánsú és  $B(v) = w$ .  $\square$

Jelölje  $SU(2)$  a  $2 \times 2$ -es, komplex elemű, 1 determinánsú unitér mátrixok csoportját a szorzásra (4.1.26. Definíció).

Elnevezés:  $SU(2)$  regulárisan hat az egységvektorok halmazán.

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,

# Az egységkvaterniók csoportja

## Tétel

Az 1 normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,  
melynek determinánása  $N(z)$



# Az egységkvaterniók csoportja

## Tétel

Az 1 normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,  
melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

# Az egységkvaterniók csoportja

## Tétel

Az 1 normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,

melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér

# Az egységkvaterniók csoportja

## Tétel

Az 1 normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,

melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánása 1.

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,  
melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánása  $1$ .

**Megfordítás:** Tegyük föl, hogy  $A$  unitér,  $1$  determinánúsú  $\mathbb{K}$ -n.

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,  
melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánása  $1$ .

**Megfordítás:** Tegyük föl, hogy  $A$  unitér,  $1$  determinánúsú  $\mathbb{K}$ -n.

Legyen  $z = \overline{A(1)}$ ,

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ , melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánása  $1$ .

**Megfordítás:** Tegyük föl, hogy  $A$  unitér,  $1$  determinánúsú  $\mathbb{K}$ -n.

Legyen  $z = \overline{A(1)}$ , ekkor  $A(1) = \bar{z} = 1\bar{z} = A_{\bar{z}}(1)$ .

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ ,  
melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánása  $1$ .

**Megfordítás:** Tegyük föl, hogy  $A$  unitér,  $1$  determinánúsú  $\mathbb{K}$ -n.

Legyen  $z = \overline{A(1)}$ , ekkor  $A(1) = \bar{z} = 1\bar{z} = A_{\bar{z}}(1)$ .

Ezért az imént bizonyított állítás miatt  $A = A_{\bar{z}}$ . □

# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ , melynek determinánása  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánása  $1$ .

**Megfordítás:** Tegyük föl, hogy  $A$  unitér,  $1$  determinánúsú  $\mathbb{K}$ -n.

Legyen  $z = \overline{A(1)}$ , ekkor  $A(1) = \bar{z} = 1\bar{z} = A_{\bar{z}}(1)$ .

Ezért az imént bizonyított állítás miatt  $A = A_{\bar{z}}$ . □

Az  $SU(2)$ -t  $Spin(3)$  csoportnak nevezik a kvantumfizikában.



# Az egységkvaterniók csoportja

## Tétel

Az  $1$  normájú kvaterniók multiplikatív csoportja izomorf  $SU(2)$ -vel.

## Bizonyítás

Ha  $z \in \mathbb{K}$ , akkor láttuk, hogy  $\psi(z) = A_{\bar{z}}$  mátrixa  $\begin{pmatrix} v & w \\ -\bar{w} & \bar{v} \end{pmatrix}$ , melynek determinánsa  $N(z)$  és adjungáltja  $A_z$  mátrixa.

Ha  $N(z) = 1$ , akkor tehát  $\psi(z)$  unitér és determinánsa  $1$ .

**Megfordítás:** Tegyük föl, hogy  $A$  unitér,  $1$  determinánsú  $\mathbb{K}$ -n.

Legyen  $z = \overline{A(1)}$ , ekkor  $A(1) = \bar{z} = 1\bar{z} = A_{\bar{z}}(1)$ .

Ezért az imént bizonyított állítás miatt  $A = A_{\bar{z}}$ . □

Az  $SU(2)$ -t  $Spin(3)$  csoportnak nevezik a kvantumfizikában.  
Fermionok (pl. neutron) leírására használják.

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor.

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. **Láttuk:**  
 $F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. **Láttuk:**

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus,

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. Láttuk:

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. Láttuk:  
 $F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.  
Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

Algebrai magyarázat: a  $zwz^{-1} = z^2w$  képlet, ha  $v \perp w$ .

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. Láttuk:

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

**Algebrai magyarázat:** a  $zwz^{-1} = z^2w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.



# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. Láttuk:

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

**Algebrai magyarázat:** a  $zwz^{-1} = z^2w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.

Ezért  $SU(2)$  az  $SO(3)$  minden elemét kétszer „fedi le”.

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. Láttuk:

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

**Algebrai magyarázat:** a  $zwz^{-1} = z^2w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.

Ezért  $SU(2)$  az  $SO(3)$  minden elemét kétszer „fedi le”.

Tekintsük az  $f : \alpha \rightarrow z$  függvényt, miközben  $v$  fix, pl.  $v = i$ .

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. **Láttuk:**

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

**Algebrai magyarázat:** a  $zwz^{-1} = z^2w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.

Ezért  $SU(2)$  az  $SO(3)$  minden elemét kétszer „fedi le”.

Tekintsük az  $f : \alpha \rightarrow z$  függvényt, miközben  $v$  fix, pl.  $v = i$ .

Ha  $0 \leq \alpha \leq 2\pi$ , akkor  $f(\alpha)$  végighalad a komplex egységkörön.

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. **Láttuk:**

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

**Algebrai magyarázat:** a  $zwz^{-1} = z^2w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.

Ezért  $SU(2)$  az  $SO(3)$  minden elemét kétszer „fedi le”.

Tekintsük az  $f : \alpha \rightarrow z$  függvényt, miközben  $v$  fix, pl.  $v = i$ .

Ha  $0 \leq \alpha \leq 2\pi$ , akkor  $f(\alpha)$  végighalad a komplex egységkörön.

De  $\varphi(f(\alpha))$  kétszer halad körbe,

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. **Láttuk:**

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ . □

**Algebrai magyarázat:** a  $zwz^{-1} = z^2 w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.

Ezért  $SU(2)$  az  $SO(3)$  minden elemét kétszer „fedi le”.

Tekintsük az  $f : \alpha \rightarrow z$  függvényt, miközben  $v$  fix, pl.  $v = i$ .

Ha  $0 \leq \alpha \leq 2\pi$ , akkor  $f(\alpha)$  végighalad a komplex egységkörön.

De  $\varphi(f(\alpha))$  kétszer halad körbe, már  $\pi$ -nél az identitás,

# Miért kétszereződik a szög?

## Tétel

$SU(2)/\{1, -1\} \cong SO(3)$  (a térbeli forgatások csoportja).

## Bizonyítás

Legyen  $z = \cos \alpha + v \sin \alpha$ , ahol  $v$  egységvektor. **Láttuk:**

$F_z : w \rightarrow zwz^{-1}$  a  $v$  irányú egyenes körüli  $2\alpha$  szögű forgatás.

Nyilván  $\varphi : z \rightarrow F_z$  homomorfizmus, melynek magja  $\{1, -1\}$ .  $\square$

**Algebrai magyarázat:** a  $zwz^{-1} = z^2 w$  képlet, ha  $v \perp w$ .

**Geometriai magyarázat:** a  $z \mapsto F_z$  homomorfizmus magja kételemű.

Ezért  $SU(2)$  az  $SO(3)$  minden elemét kétszer „fedi le”.

Tekintsük az  $f : \alpha \rightarrow z$  függvényt, miközben  $v$  fix, pl.  $v = i$ .

Ha  $0 \leq \alpha \leq 2\pi$ , akkor  $f(\alpha)$  végighalad a komplex egységkörön.

De  $\varphi(f(\alpha))$  kétszer halad körbe, már  $\pi$ -nél az identitás,

és ezért kétszeres „sebességgel” halad.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata.



# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest,

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra,

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű,

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.



# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

Véges nullosztómentes gyűrű test.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgűrű, főideálgűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

Véges nullosztómentes gyűrű test.

Kommutatív, egységelemes, egyszerű gyűrű test.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

Véges nullosztómentes gyűrű test.

Kommutatív, egységelemes, egyszerű gyűrű test.

Egyszerű testbővítés konstrukciója faktorgyűrűként.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

Véges nullosztómentes gyűrű test.

Kommutatív, egységelemes, egyszerű gyűrű test.

Egyszerű testbővítés konstrukciója faktorgyűrűként.

A prímtestek szerkezete.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

Véges nullosztómentes gyűrű test.

Kommutatív, egységelemes, egyszerű gyűrű test.

Egyszerű testbővítés konstrukciója faktorgyűrűként.

A prímtestek szerkezete.

Frobenius tétele.

# A 17. előadás összefoglalója

## Fogalmak

Főideálgyűrű.

Gyűrűk direkt szorzata. Egyszerű gyűrű.

Karakterisztika, prímtest, Frobenius-endomorfizmus.

Test fölötti algebra, elem minimálpolinomja. Euler-mátrix.

## Tételek

Euklideszi gyűrű főideálgyűrű, főideálgyűrű alaptételes.

Főideálok tartalmazása és oszthatóság.

Véges nullosztómentes gyűrű test.

Kommutatív, egységelemes, egyszerű gyűrű test.

Egyszerű testbővítés konstrukciója faktorgyűrűként.

A prímtestek szerkezete.

Frobenius tétele. Kvaterniók csoportelméleti vonatkozásai.