# Algebra3, alkalmazott matematikus

## ELTE Algebra és Számelmélet Tanszék

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

9/11. előadás

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$,

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban,

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis $T$-ben $P$ fölött,

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis $T$-ben $P$ fölött, és $\lambda_1, \ldots, \lambda_n \in P$.

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis $T$-ben $P$ fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik $\lambda_i$ skalár $|P| = p$-féle lehet,

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis $T$-ben $P$ fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik $\lambda_i$ skalár $|P| = p$-féle lehet, így $|T| = p^n$. □

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis $T$-ben $P$ fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik $\lambda_i$ skalár $|P| = p$-féle lehet, így $|T| = p^n$. □

## Megjegyzés

A $\lambda_1 b_1 + \ldots + \lambda_n b_n \mapsto (\lambda_1, \ldots, \lambda_n)$ megfeleltetés nyilván összegtartó.

# Véges test elemszáma

## 6.7.2. Következmény

Minden véges test elemszáma prímhatvány.

## Bizonyítás

Legyen $T$ karakterisztikája $p$, prímteste $P$, és $|T : P| = n$.
Ekkor $T$ elemei egyértelműen írhatók $\lambda_1 b_1 + \ldots + \lambda_n b_n$ alakban, ahol $b_1, \ldots, b_n$ bázis $T$-ben $P$ fölött, és $\lambda_1, \ldots, \lambda_n \in P$.
Mindegyik $\lambda_i$ skalár $|P| = p$-féle lehet, így $|T| = p^n$. □

## Megjegyzés

A $\lambda_1 b_1 + \ldots + \lambda_n b_n \mapsto (\lambda_1, \ldots, \lambda_n)$ megfeleltetés nyilván összegtartó. Ezért $T$ additív csoportja izomorf a $\mathbb{Z}_p^+ \times \ldots \times \mathbb{Z}_p^+$ $n$-tényezős direkt szorzattal.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$,

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$,

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.
Vagyis a $d$ rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.
Vagyis a $d$ rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs $d$ rendű elem Lagrange tétele miatt.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.
Vagyis a $d$ rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs $d$ rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.
Vagyis a $d$ rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs $d$ rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.
Ez csak úgy lehet, ha minden $d \mid k$-ra van $d$ rendű elem!

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.
Vagyis a $d$ rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs $d$ rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.
Ez csak úgy lehet, ha minden $d \mid k$-ra van $d$ rendű elem!
Speciálisan van $k$ rendű elem,

# Véges test multiplikatív csoportja

## 4.3.22. Tétel

Minden véges test multiplikatív csoportja ciklikus.

## Bizonyítás

Legyen $T$ elemszáma $k+1$, azaz $|T^\times| = |T - \{0\}| = k$.
Az $x^d - 1$ polinomnak legfeljebb $d$ gyöke van $T$-ben.
Így ha $g \in T^\times$ rendje $d$, akkor e gyökök éppen $g$ hatványai.
Speciálisan minden $d$ rendű elem $g$-nek hatványa!
A $\langle g \rangle$ ciklikus részcsoportban $\varphi(d)$ darab $d$ rendű elem van.
Vagyis a $d$ rendű elemek száma $T^\times$-ben $\varphi(d)$ vagy 0.
Ha $d \nmid k$, akkor nincs $d$ rendű elem Lagrange tétele miatt.
Az $x^k - 1 = \prod_{d|k} \Phi_d(x)$-ben a fokokat véve $\sum_{d|k} \varphi(d) = k$.
Ez csak úgy lehet, ha minden $d \mid k$-ra van $d$ rendű elem!
Speciálisan van $k$ rendű elem, azaz $T^\times$ ciklikus. □

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test,

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.
Mivel $K$ összes eleme generálja $K$-t,

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.
Mivel $K$ összes eleme generálja $K$-t,
ezért $K$ az $x^q - x$ felbontási teste $P$ fölött.

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.
Mivel $K$ összes eleme generálja $K$-t,
ezért $K$ az $x^q - x$ felbontási teste $P$ fölött.
A felbontási test egyértelmű (6.4.9. Következmény),

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.
Mivel $K$ összes eleme generálja $K$-t,
ezért $K$ az $x^q - x$ felbontási teste $P$ fölött.
A felbontási test egyértelmű (6.4.9. Következmény),
és így bármely két $q$ elemű test izomorf. □

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.
Mivel $K$ összes eleme generálja $K$-t,
ezért $K$ az $x^q - x$ felbontási teste $P$ fölött.
A felbontási test egyértelmű (6.4.9. Következmény),
és így bármely két $q$ elemű test izomorf. □

Megjegyzés: $q = p$ esetén a kis Fermat-tételt kaptuk:

# Véges test egyértelműsége

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig legfeljebb egy darab $q$ elemű test létezik.

## Bizonyítás

Legyen $K$ egy $q$ elemű test, prímteste $P \cong \mathbb{Z}_p$.
Nyilván $K^\times$ elemszáma $q - 1$.
Lagrange tétele miatt így $g \neq 0$ esetén $g^{q-1} = 1$.
Ezért $K$ minden eleme gyöke $x^q - x \in P[x]$-nek.
Mivel $K$ összes eleme generálja $K$-t,
ezért $K$ az $x^q - x$ felbontási teste $P$ fölött.
A felbontási test egyértelmű (6.4.9. Következmény),
és így bármely két $q$ elemű test izomorf. □

Megjegyzés: $q = p$ esetén a kis Fermat-tételt kaptuk: $x^p \equiv x\ (p)$.

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke ($k \geq 1$),

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke ($k \geq 1$), akkor $b$ az $f'$ deriváltnak legalább $k-1$-szeres gyöke.

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke ($k \geq 1$), akkor $b$ az $f'$ deriváltnak legalább $k-1$-szeres gyöke.

## Bizonyítás

$$f(x) = (x-b)^k g(x) \implies f'(x) = (x-b)^{k-1}[kg(x) + (x-b)g'(x)].$$

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke ($k \geq 1$), akkor $b$ az $f'$ deriváltnak legalább $k-1$-szeres gyöke.

## Bizonyítás

$f(x) = (x-b)^k g(x) \implies f'(x) = (x-b)^{k-1}[kg(x) + (x-b)g'(x)]$.
Megjegyezzük, hogy ha $b$ pontosan $k$-szoros gyöke $f$-nek,

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$ (formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke ($k \geq 1$), akkor $b$ az $f'$ deriváltnak legalább $k-1$-szeres gyöke.

## Bizonyítás

$f(x) = (x-b)^k g(x) \implies f'(x) = (x-b)^{k-1}[kg(x) + (x-b)g'(x)]$.
Megjegyezzük, hogy ha $b$ pontosan $k$-szoros gyöke $f$-nek, akkor pontosan $k-1$-szeres gyöke $f'$-nek,

# Többszörös gyökök és a derivált

## 3.6.1. Definíció

Ha $R$ szokásos gyűrű, akkor $f(x) = a_0 + \ldots + a_n x^n \in R[x]$
(formális) deriváltja $f'(x) = a_1 + 2a_2 x + \ldots + n a_n x^{n-1}$.

HF: Érvényesek a deriválás szokásos azonosságai.

## 3.6.3. Állítás

Ha $f \in R[x]$-nek $b \in R$ legalább $k$-szoros gyöke ($k \geq 1$),
akkor $b$ az $f'$ deriváltnak legalább $k-1$-szeres gyöke.

## Bizonyítás

$f(x) = (x-b)^k g(x) \implies f'(x) = (x-b)^{k-1}[kg(x)+(x-b)g'(x)]$.
Megjegyezzük, hogy ha $b$ pontosan $k$-szoros gyöke $f$-nek,
akkor pontosan $k-1$-szeres gyöke $f'$-nek, kivéve ha $kg(b) = 0$. □

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik.

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest,

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).
Az $L$ elemszáma $q$,

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).
Az $L$ elemszáma $q$, mert $x^q - x$-nek nincs többszörös gyöke.

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).
Az $L$ elemszáma $q$, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).
Az $L$ elemszáma $q$, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.
De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$,

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).
Az $L$ elemszáma $q$, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.
De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$, hiszen $p \mid q$.

# Véges test konstrukciója

## 6.7.5. Tétel

Minden $q = p^k$ prímhatványra izomorfia erejéig pontosan egy darab $q$ elemű test létezik. Jele $\mathbb{F}_q$.

## Bizonyítás

Legyen $K$ az $x^q - x$ felbontási teste $\mathbb{Z}_p$ fölött (ez létezik a 6.4.5. Következmény miatt).
Jelölje $L$ az $x^q - x$ gyökeinek halmazát $K$-ban.
Ez résztest, mert $(a+b)^q = a^q + b^q$ és $(ab)^q = a^q b^q$ a $K$-ban (hiszen $x \to x^q$ a Frobenius-endomorfizmus $k$-adik hatványa).
Az $L$ elemszáma $q$, mert $x^q - x$-nek nincs többszörös gyöke.
Ha ugyanis lenne, akkor az gyöke lenne a deriváltjának is.
De $x^q - x \in \mathbb{Z}_p[x]$ deriváltja $qx^{q-1} - 1 = -1$, hiszen $p \mid q$.
A $-1$ konstans polinomnak pedig nincs gyöke $K$-ban. □

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van,

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Láttuk, hogy $K$ elemei pontosan az $x^{p^k} - x$ gyökei.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Láttuk, hogy $K$ elemei pontosan az $x^{p^k} - x$ gyökei.
Ezért $K$ az egyetlen $p^k$ elemű résztest.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Láttuk, hogy $K$ elemei pontosan az $x^{p^k} - x$ gyökei.
Ezért $K$ az egyetlen $p^k$ elemű résztest.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Láttuk, hogy $K$ elemei pontosan az $x^{p^k} - x$ gyökei.
Ezért $K$ az egyetlen $p^k$ elemű résztest.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.
Mivel $L^\times$ ciklikus,

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Láttuk, hogy $K$ elemei pontosan az $x^{p^k} - x$ gyökei.
Ezért $K$ az egyetlen $p^k$ elemű résztest.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.
Mivel $L^\times$ ciklikus, $x^{p^k-1} - 1$-nek $p^k - 1$ gyöke van $L$-ben.

# Véges test résztestei

## 6.7.8. Tétel

Ha $K \leq L$ véges testek, akkor ez a bővítés normális.
A $q = p^n$ elemű $\mathbb{F}_q$ testnek minden $k \mid n$ esetén egyetlen $\mathbb{F}_{p^k}$-val izomorf részteste van, más részteste pedig nincs.
Ez a résztest az $x^{p^k} - x$ polinom összes gyökéből áll.

## Bizonyítás

Ha $L = \mathbb{F}_q$, akkor $L$ az $x^q - x$ felbontási teste $K$ fölött is.
A szorzástétel miatt $k = |K : \mathbb{Z}_p|$ osztója $n = |\mathbb{F}_q : \mathbb{Z}_p|$-nek.
Láttuk, hogy $K$ elemei pontosan az $x^{p^k} - x$ gyökei.
Ezért $K$ az egyetlen $p^k$ elemű résztest.
Megfordítva, $k \mid n$ esetén $p^k - 1 \mid p^n - 1 = |\mathbb{F}_q^\times|$.
Mivel $L^\times$ ciklikus, $x^{p^k-1} - 1$-nek $p^k - 1$ gyöke van $L$-ben.
Ezek a nullával együtt $p^k$ elemű résztestet alkotnak. □

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste,

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus,

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$,

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik. Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével:

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével: $K = \mathbb{Z}_p(\beta)$

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével: $K = \mathbb{Z}_p(\beta)$ és $|K| = p^n$.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével: $K = \mathbb{Z}_p(\beta)$ és $|K| = p^n$.
Mivel $\mathbb{Z}_p \leq K$ normális, a $K$ az $f$ felbontási teste $\mathbb{Z}_p$ fölött.

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével: $K = \mathbb{Z}_p(\beta)$ és $|K| = p^n$.
Mivel $\mathbb{Z}_p \leq K$ normális, a $K$ az $f$ felbontási teste $\mathbb{Z}_p$ fölött.
A $\beta$ közös gyöke $f$-nek és $x^{p^n} - x$-nek,

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével: $K = \mathbb{Z}_p(\beta)$ és $|K| = p^n$.
Mivel $\mathbb{Z}_p \leq K$ normális, a $K$ az $f$ felbontási teste $\mathbb{Z}_p$ fölött.
A $\beta$ közös gyöke $f$-nek és $x^{p^n} - x$-nek, így $f(x) \mid x^{p^n} - x$

# Véges test, mint egyszerű bővítés

## Állítás (6.7.9, 6.7.10)

Minden $p$ prímszámra és minden $n > 0$ egészre létezik $\mathbb{Z}_p$ fölött irreducibilis $n$-edfokú $f$ polinom. Minden ilyen $f$ polinomnak $\mathbb{F}_{p^n}$ a felbontási teste, és $f(x) \mid x^{p^n} - x$.

## Bizonyítás

Mivel $\mathbb{F}_{p^n}^{\times}$ ciklikus, van $p^n - 1$ rendű $\alpha$ eleme. Ekkor $\mathbb{Z}_p(\alpha) = \mathbb{F}_{p^n}$, hiszen csak szorzással is minden nem nulla elem generálódik.
Ezért az irreducibilis $m_\alpha$ foka $|\,\mathbb{F}_{p^n} : \mathbb{Z}_p\,| = n$.
Ha $f \in \mathbb{Z}_p[x]$ egy $n$-edfokú, irreducibilis polinom, akkor bővítsünk ennek egy $\beta$ gyökével: $K = \mathbb{Z}_p(\beta)$ és $|K| = p^n$.
Mivel $\mathbb{Z}_p \leq K$ normális, a $K$ az $f$ felbontási teste $\mathbb{Z}_p$ fölött.
A $\beta$ közös gyöke $f$-nek és $x^{p^n} - x$-nek, így $f(x) \mid x^{p^n} - x$ (hiszen $f$ a $\beta$ minimálpolinomja $\mathbb{Z}_p$ fölött). □

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.

Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.

Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.

Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.

A $0$ és az $1$ minimálpolinomja $x$ és $x - 1$.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x - 1$. Három elem minimálpolinomja $x^3 + x + 1$, a másik háromé $x^3 + x^2 + 1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0, 1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$;

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0 + (x^3+x+1)$ és $E = 1 + (x^3+x+1)$; ekkor $\{O, E\}$ a prímtest.
$A = x + (x^3+x+1)$ gyöke $Ex^3 + Ex + E$-nek. A másik két gyök $A^2 = x^2 + (x^3+x+1)$

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0+(x^3+x+1)$ és $E = 1+(x^3+x+1)$; ekkor $\{O,E\}$ a prímtest.
$A = x+(x^3+x+1)$ gyöke $Ex^3+Ex+E$-nek. A másik két gyök $A^2 = x^2+(x^3+x+1)$ és $A^4 = x^2+x+(x^3+x+1)$.

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0+(x^3+x+1)$ és $E = 1+(x^3+x+1)$; ekkor $\{O,E\}$ a prímtest.
$A = x+(x^3+x+1)$ gyöke $Ex^3+Ex+E$-nek. A másik két gyök $A^2 = x^2+(x^3+x+1)$ és $A^4 = x^2+x+(x^3+x+1)$.
A maradék három elem $Ex^3+Ex^2+E$-nek lesz gyöke,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0+(x^3+x+1)$ és $E = 1+(x^3+x+1)$; ekkor $\{O,E\}$ a prímtest.
$A = x+(x^3+x+1)$ gyöke $Ex^3+Ex+E$-nek. A másik két gyök $A^2 = x^2+(x^3+x+1)$ és $A^4 = x^2+x+(x^3+x+1)$.
A maradék három elem $Ex^3+Ex^2+E$-nek lesz gyöke, ezek $A+E$,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0+(x^3+x+1)$ és $E = 1+(x^3+x+1)$; ekkor $\{O,E\}$ a prímtest.
$A = x+(x^3+x+1)$ gyöke $Ex^3+Ex+E$-nek. A másik két gyök $A^2 = x^2+(x^3+x+1)$ és $A^4 = x^2+x+(x^3+x+1)$.
A maradék három elem $Ex^3+Ex^2+E$-nek lesz gyöke, ezek $A+E$, $A^2+E$,

# A nyolcelemű test példája

$\mathbb{Z}_2$ fölött $x^8 - x = x(x+1)(x^3+x+1)(x^3+x^2+1)$.
Ezek irreducibilisek $\mathbb{Z}_2$ fölött, ezért

$$\mathbb{F}_8 \cong \mathbb{Z}_2[x]/(x^3+x+1) \cong \mathbb{Z}_2[x]/(x^3+x^2+1).$$

Az $\mathbb{F}_8$ elemei az $x^8 - x$ polinom összes gyökei.
Az egyetlen valódi résztest a prímtest: $\{0,1\}$.
A $0$ és az $1$ minimálpolinomja $x$ és $x-1$. Három elem minimálpolinomja $x^3+x+1$, a másik háromé $x^3+x^2+1$.
A $\psi : z \mapsto z^2$ Frobenius-endomorfizmus bijektív, mert magja $\{0\}$.
Ez permutálja $x^3+x+1$ és $x^3+x^2+1$ gyökeit is.

Legyen $K = \mathbb{Z}_2[x]/(x^3+x+1)$, $O = 0+(x^3+x+1)$ és $E = 1+(x^3+x+1)$; ekkor $\{O,E\}$ a prímtest.
$A = x+(x^3+x+1)$ gyöke $Ex^3+Ex+E$-nek. A másik két gyök $A^2 = x^2+(x^3+x+1)$ és $A^4 = x^2+x+(x^3+x+1)$.
A maradék három elem $Ex^3+Ex^2+E$-nek lesz gyöke, ezek $A+E$, $A^2+E$, $A^2+A+E$.

# Primitív polinomok

## 6.7.11. Definíció

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját.

# Primitív polinomok

## 6.7.11. Definíció

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$,

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$,

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$,

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke,

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$,

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$, melynek többi gyöke $g^2$, $g^4$ és $g^8$.

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$, melynek többi gyöke $g^2$, $g^4$ és $g^8$.

A másik két negyedfokú irreducibilis gyökei a 15 rendű elemek,

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$, melynek többi gyöke $g^2$, $g^4$ és $g^8$.

A másik két negyedfokú irreducibilis gyökei a 15 rendű elemek, ezek primitív polinomok:

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$, melynek többi gyöke $g^2$, $g^4$ és $g^8$.

A másik két negyedfokú irreducibilis gyökei a 15 rendű elemek, ezek primitív polinomok: $x^4 + x + 1$

# Primitív polinomok

**6.7.11. Definíció**

Ha $K$ véges test, akkor egy irreducibilis $f \in K[x]$ primitív polinom, ha mindegyik gyöke generálja a felbontási testének multiplikatív csoportját. (NEM azonos fogalom a $\mathbb{Z}[x]$-beli primitív polinommal!)

9.3.9. Példa: Legyen $K = \mathbb{F}_{16}$, elemei $x^{16} - x$ gyökei.
$|K : \mathbb{Z}_2| = 4$, az egyetlen valódi résztest $\mathbb{F}_4$, ez $x^4 - x$ gyökeiből áll.
Ezért a harmadrendű elemek közös minimálpolinomja $x^2 + x + 1$.
Ha $g \notin \mathbb{F}_4$, akkor $\mathbb{Z}_2(g) = K$, és ezért $\mathrm{gr}(m_g) = 4$.

Ha $g$ ötödrendű, akkor $x^5 - 1$-nek is gyöke, így minimálpolinomja $x^4 + x^3 + x^2 + x + 1$, melynek többi gyöke $g^2$, $g^4$ és $g^8$.

A másik két negyedfokú irreducibilis gyökei a 15 rendű elemek, ezek primitív polinomok: $x^4 + x + 1$ és $x^4 + x^3 + 1$.

# 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 $T[x_1, \ldots, x_n]$ 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 $T[x_1, \ldots, x_n]$ 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 $T[x_1, \ldots, x_n]$ 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 $T[x_1, \ldots, x_n]$ 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 $T[x_1, \ldots, x_n]$ 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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1 x + \ldots + a_n x^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (behelyettesítés).

# Algebra elemének minimálpolinomja

**5.10.6. Definíció**

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (behelyettesítés).

Tehát $f$ konstans tagját $A$ egységelemével szorozzuk.

# Algebra elemének minimálpolinomja

**5.10.6. Definíció**

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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 $I$ normált generátoreleme a $b \in A$ minimálpolinomja,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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 $I$ normált generátoreleme a $b \in A$ minimálpolinomja, jele $m_b$.

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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 $I$ normált generátoreleme a $b \in A$ minimálpolinomja, jele $m_b$.

Az $m_b$ létezik, mert $T[x]$ euklideszi,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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 $I$ normált generátoreleme a $b \in A$ minimálpolinomja, jele $m_b$.

Az $m_b$ létezik, mert $T[x]$ euklideszi, és így főideálgyűrű.

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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 $I$ normált generátoreleme a $b \in A$ minimálpolinomja, jele $m_b$.

Az $m_b$ létezik, mert $T[x]$ euklideszi, és így főideálgyűrű. Nyilván $f(b) = 0 \iff m_b \mid f$,

# Algebra elemének minimálpolinomja

## 5.10.6. Definíció

Ha $A$ algebra a $T$ test fölött, $f(x) = a_0 + a_1x + \ldots + a_nx^n \in T[x]$ és $b \in A$, akkor $f(b) = a_0 1_A + a_1 b + \ldots + a_n b^n$ (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 $I$ normált generátoreleme a $b \in A$ minimálpolinomja, jele $m_b$.

Az $m_b$ létezik, mert $T[x]$ euklideszi, és így főideálgyűrű. Nyilván $f(b) = 0 \iff m_b \mid f$, vagyis a jó polinomok a minimálpolinom többszörösei.

# 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 $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg:

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$.

# A minimálpolinom irreducibilitása

**5.10.9. Állítás**

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$,

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem $0$,

# A minimálpolinom irreducibilitása

**5.10.9. Állítás**

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ fölött.

# A minimálpolinom irreducibilitása

## 5.10.9. Állítás

Véges dimenziós algebra minden eleme algebrai.

Valóban: ha $\dim_T(A) = n$, akkor $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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 $1, b, \ldots, b^n$ már összefügg: $\lambda_0 1 + \lambda_1 b + \ldots + \lambda_n b^n = 0$. Legyen $f(x) = \lambda_0 + \lambda_1 x + \ldots + \lambda_n x^n$, ekkor $f$ nem 0, és $b$ gyöke $f$-nek. □

## 5.10.12. Tétel

Legyen $A$ nullosztómentes algebra és $b \in A$ algebrai elem.
Ekkor $b$ minimálpolinomja irreduciblis $T$ 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. □

# 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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
Magyarázat: $x^2 + 1 = (x + i)(x - i)$ a „gyöktényezős alak”.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j + i)(j - i) = j^2 + ij - ji - i^2 = ij - ji = 2k \neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

## 5.11.5. Következmény

Az $x^2+1$ polinomnak a kvaterniók között végtelen sok gyöke van.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

## 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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

## 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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

## 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

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

### 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 $q^2+r^2+s^2=1$.

Valóban, ha $N(z)=1$ és $\overline{z}=-z$, akkor $z^2=-z\overline{z}=-N(z)=-1$.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

### 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 $q^2+r^2+s^2=1$.

Valóban, ha $N(z)=1$ és $\overline{z}=-z$, akkor $z^2=-z\overline{z}=-N(z)=-1$.
Megfordítva: ha $z^2=-1$, akkor $1=N(z^2)=N(z)^2$,

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

### 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 $q^2+r^2+s^2=1$.

Valóban, ha $N(z)=1$ és $\overline{z}=-z$, akkor $z^2=-z\overline{z}=-N(z)=-1$.
Megfordítva: ha $z^2=-1$, akkor $1=N(z^2)=N(z)^2$, így $N(z)=1$.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

### 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 $q^2+r^2+s^2=1$.

Valóban, ha $N(z)=1$ és $\overline{z}=-z$, akkor $z^2=-z\overline{z}=-N(z)=-1$.
Megfordítva: ha $z^2=-1$, akkor $1=N(z^2)=N(z)^2$, így $N(z)=1$.
Ezért $1=z\overline{z}=-z^2$.

# A polinomok azonossági tétele

Ha a kommutativitás feltételét elhagyjuk, akkor egy polinomnak már lehet több gyöke, mint a foka (a nullosztómentesség ellenére)!
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:
$(j+i)(j-i)=j^2+ij-ji-i^2=ij-ji=2k\neq 0$.
Az a gond, hogy $i$ és $j$ nem felcserélhetők.
Nem tudjuk így kihasználni, hogy $\mathbb{K}$ nullosztómentes.

### 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 $q^2+r^2+s^2=1$.

Valóban, ha $N(z)=1$ és $\overline{z}=-z$, akkor $z^2=-z\overline{z}=-N(z)=-1$.
Megfordítva: ha $z^2=-1$, akkor $1=N(z^2)=N(z)^2$, így $N(z)=1$.
Ezért $1=z\overline{z}=-z^2$. Innen $z\neq 0$ miatt $\overline{z}=-z$. □

# 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 $z^{-1} = \overline{z}$.

# 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 $z^{-1} = \overline{z}$. 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 $z^{-1} = \overline{z}$. 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 $z^{-1} = \overline{z}$. 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 $z^{-1} = \overline{z}$. 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 $z^{-1} = \overline{z}$. 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 $z^{-1} = \overline{z}$. 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$.

# 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.

# 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$.

# 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$. 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$. 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$. 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$. 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 $z^{-1} = \overline{z}$. 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 $w^{-1}zw = w^{-1}rw + w^{-1}vw = r - v = \overline{z}$. Balról $zw$-vel szorozva $zw\overline{z} = z^2 w$.
- Tehát ha $N(z) = 1$ és $v \perp w$, akkor $zwz^{-1} = z^2 w$. 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 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.

# 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 $zvz^{-1} = v$

# 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 $zv = vz$),

# 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 $v(vw) = v^2w = -w$

# 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 $v(vw) = v^2w = -w$ (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 $v(vw) = v^2w = -w$ (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 kvaternók vektortér $\mathbb{C}$ fölött (a skalárral szorzás balszorzás).
FIGYELEM: ez NEM algebra $\mathbb{C}$ fölött,

# A kvaterniók mint transzformációk

A kvaternók 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 kvaternók 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 kvaternók 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 kvaternók 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 kvaternók 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 kvaternók 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 kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
Azaz a $\psi : z \mapsto A_z$ leképezésre $\psi(z_1 z_2) = \psi(z_2)\psi(z_1)$.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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 kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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 $\psi(z) = A_{\overline{z}}$.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$,

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$,

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.
Végül $\psi$ injektív:

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.
Végül $\psi$ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\overline{z}$,

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.
Végül $\psi$ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\overline{z}$, így $z = 0$.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.
Végül $\psi$ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\overline{z}$, így $z = 0$.
Tehát a $\mathbb{K}$ gyűrű izomorf $\mathrm{Hom}(\mathbb{C}^2)$ egy részgyűrűjével.

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.
Végül $\psi$ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\overline{z}$, így $z = 0$.
Tehát a $\mathbb{K}$ gyűrű izomorf $\mathrm{Hom}(\mathbb{C}^2)$ egy részgyűrűjével.

Ha $z = p + qi + rj + sk$, akkor $\psi(z)$ mátrixa az $(1, j)$ bázisban
$\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$ ahol $v = p + qi$ és $w = r + si$

# A kvaterniók mint transzformációk

A kvaternók 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 $A_{z_1 z_2}(x) = x(z_1 z_2) = (xz_1)z_2 = A_{z_2} A_{z_1}(x)$.
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
$\psi(z) = A_{\overline{z}}$. Erre $\psi(z_1 z_2) = \psi(z_1)\psi(z_2)$, hiszen $\overline{z_1 z_2} = \overline{z_2}\ \overline{z_1}$.
Továbbá $\psi(z_1 + z_2) = \psi(z_1) + \psi(z_2)$, azaz $\psi$ gyűrűhomomorfizmus.
Végül $\psi$ injektív: ha $\psi(z) = 0$, akkor $0 = \psi(z)(1) = 1\overline{z}$, így $z = 0$.
Tehát a $\mathbb{K}$ gyűrű izomorf $\mathrm{Hom}(\mathbb{C}^2)$ egy részgyűrűjével.

Ha $z = p + qi + rj + sk$, akkor $\psi(z)$ mátrixa az $(1, j)$ bázisban
$\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$ 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

Tegyük 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 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 $D(u) \perp D(v) = v$,

# 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 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 $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-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 $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-re $B$ unitér, 1 determinánsú és $B(v) = w$. □

# 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.
Előírhatósági tétel: van $B$, melyre $B(b_1) = c_1$ és $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-re $B$ unitér, 1 determinánsú és $B(v) = w$. □

Jelölje $\mathrm{SU}(2)$ 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 $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-re $B$ unitér, $1$ determinánsú és $B(v) = w$. □

Jelölje $\mathrm{SU}(2)$ 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 $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-re $B$ unitér, $1$ determinánsú és $B(v) = w$. □

Jelölje $\mathrm{SU}(2)$ 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 $B(b_2) = \varepsilon c_2$.
Alkalmas $|\varepsilon| = 1$-re $B$ unitér, $1$ determinánsú és $B(v) = w$. □

Jelölje $\mathrm{SU}(2)$ a $2 \times 2$-es, komplex elemű, $1$ determinánsú unitér mátrixok csoportját a szorzásra (4.1.26. Definíció).
Elnevezés: $\mathrm{SU}(2)$ regulárisan hat az egységvektorok halmazán.

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

# Az egységkvaterniók csoportja

## Tétel

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

## Bizonyítás

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,

# Az egységkvaterniók csoportja

## Tétel

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

## Bizonyítás

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,

melynek determinánsa $N(z)$

# Az egységkvaterniók csoportja

## Tétel

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

## Bizonyítás

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,

melynek determinánsa $N(z)$ és adjungáltja $A_z$ mátrixa.

# Az egységkvaterniók csoportja

## Tétel

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

## Bizonyítás

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,

melynek determinánsa $N(z)$ 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 $\mathrm{SU}(2)$-vel.

## Bizonyítás

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,

melynek determinánsa $N(z)$ és adjungáltja $A_z$ mátrixa.
Ha $N(z) = 1$, akkor tehát $\psi(z)$ unitér és determinánsa $1$.

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

**Bizonyítás**

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,
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.

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

**Bizonyítás**

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,
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 $z = \overline{A(1)}$,

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

**Bizonyítás**

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,
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 $A(1) = \overline{z} = 1\overline{z} = A_{\overline{z}}(1)$.

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

**Bizonyítás**

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,
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 $A(1) = \overline{z} = 1\overline{z} = A_{\overline{z}}(1)$.
Ezért az imént bizonyított állítás miatt $A = A_{\overline{z}}$. □

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

**Bizonyítás**

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,
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 $A(1) = \overline{z} = 1\overline{z} = A_{\overline{z}}(1)$.
Ezért az imént bizonyított állítás miatt $A = A_{\overline{z}}$. □

Az $\mathrm{SU}(2)$-t $\mathrm{Spin}(3)$ csoportnak nevezik a kvantumfizikában.

# Az egységkvaterniók csoportja

**Tétel**

Az $1$ normájú kvaterniók multiplikatív csoportja izomorf $\mathrm{SU}(2)$-vel.

**Bizonyítás**

Ha $z \in \mathbb{K}$, akkor láttuk, hogy $\psi(z) = A_{\overline{z}}$ mátrixa $\begin{pmatrix} v & w \\ -\overline{w} & \overline{v} \end{pmatrix}$,
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 $A(1) = \overline{z} = 1\overline{z} = A_{\overline{z}}(1)$.
Ezért az imént bizonyított állítás miatt $A = A_{\overline{z}}$. □

Az $\mathrm{SU}(2)$-t $\mathrm{Spin}(3)$ csoportnak nevezik a kvantumfizikában.
Fermionok (pl. neutron) leírására használják.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ homomorfizmus,

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ homomorfizmus, melynek magja $\{1,-1\}$. □

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ homomorfizmus, melynek magja $\{1,-1\}$. □

Algebrai magyarázat: a $zwz^{-1} = z^2 w$ képlet, ha $v \perp w$.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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 $\mathrm{SU}(2)$ az $\mathrm{SO}(3)$ minden elemét kétszer „fedi le”.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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 $\mathrm{SU}(2)$ az $\mathrm{SO}(3)$ minden elemét kétszer „fedi le”.
Tekintsük az $f : \alpha \to z$ függvényt, miközben $v$ fix, pl. $v = i$.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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 $\mathrm{SU}(2)$ az $\mathrm{SO}(3)$ minden elemét kétszer „fedi le”.
Tekintsük az $f : \alpha \to z$ függvényt, miközben $v$ fix, pl. $v = i$.
Ha $0 \le \alpha \le 2\pi$, akkor $f(\alpha)$ végighalad a komplex egységkörön.

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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 $\mathrm{SU}(2)$ az $\mathrm{SO}(3)$ minden elemét kétszer „fedi le".
Tekintsük az $f : \alpha \to z$ függvényt, miközben $v$ fix, pl. $v = i$.
Ha $0 \le \alpha \le 2\pi$, akkor $f(\alpha)$ végighalad a komplex egységkörön.
De $\varphi\big(f(\alpha)\big)$ kétszer halad körbe,

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v\sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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 $\mathrm{SU}(2)$ az $\mathrm{SO}(3)$ minden elemét kétszer „fedi le".
Tekintsük az $f : \alpha \to z$ függvényt, miközben $v$ fix, pl. $v = i$.
Ha $0 \le \alpha \le 2\pi$, akkor $f(\alpha)$ végighalad a komplex egységkörön.
De $\varphi\big(f(\alpha)\big)$ kétszer halad körbe, már $\pi$-nél az identititás,

# Miért kétszereződik a szög?

**Tétel**

$\mathrm{SU}(2)/\{1,-1\} \cong \mathrm{SO}(3)$ (a térbeli forgatások csoportja).

**Bizonyítás**

Legyen $z = \cos\alpha + v \sin\alpha$, ahol $v$ egységvektor. Láttuk:
$F_z : w \to zwz^{-1}$ a $v$ irányú egyenes körüli $2\alpha$ szögű forgatás.
Nyilván $\varphi : z \to F_z$ 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 $\mathrm{SU}(2)$ az $\mathrm{SO}(3)$ minden elemét kétszer „fedi le".
Tekintsük az $f : \alpha \to z$ függvényt, miközben $v$ fix, pl. $v = i$.
Ha $0 \le \alpha \le 2\pi$, akkor $f(\alpha)$ végighalad a komplex egységkörön.
De $\varphi\big(f(\alpha)\big)$ kétszer halad körbe, már $\pi$-nél az identititás,
és ezért kétszeres „sebességgel" halad.