

Algebra1, alapszint

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

21. előadás

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti egyhatározatlanú polinomnak nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti egyhatározatlanú polinomnak nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,
ahol $n \geq 0$ egész szám

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti egyhatározatlanú polinomnak nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,
ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$.

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti egyhatározatlanú polinomnak nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$. Ezek halmaza $R[x]$.

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti egyhatározatlanú polinomnak nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$. Ezek halmaza $R[x]$.

Egyenlőség

Két polinom akkor **egyenlő**, ha együtthatóik megegyeznek

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti **egyhatározatlanú polinomnak** nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$. Ezek halmaza $R[x]$.

Egyenlőség

Két polinom akkor **egyenlő**, ha együtthatóik megegyeznek (x^j együtthatója ugyanaz a két polinomban minden $j \geq 0$ -ra).

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti **egyhatározatlanú polinomnak** nevezzük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$. Ezek halmaza $R[x]$.

Egyenlőség

Két polinom akkor **egyenlő**, ha együtthatóik megegyeznek (x^j együtthatója ugyanaz a két polinomban minden $j \geq 0$ -ra).

Nullapolinom

A **nullapolinom** az a polinom, amelynek minden együtthatója nulla.

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti **egyhatározatlanú polinomnak** nevezünk az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$. Ezek halmaza $R[x]$.

Egyenlőség

Két polinom akkor **egyenlő**, ha együtthatóik megegyeznek (x^j együtthatója ugyanaz a két polinomban minden $j \geq 0$ -ra).

Nullapolinom

A **nullapolinom** az a polinom, amelynek minden együtthatója nulla. Ugyanúgy 0 jelöli, mint az R nullelemét.

A polinom definíciója

Polinom

Legyen R kommutatív, egységelemes gyűrű.

R fölötti **egyhatározatlanú polinomnak** nevezük az

$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$ formális kifejezéseket,

ahol $n \geq 0$ egész szám és $a_0, \dots, a_n \in R$. Ezek halmaza $R[x]$.

Egyenlőség

Két polinom akkor **egyenlő**, ha együtthatóik megegyeznek (x^j együtthatója ugyanaz a két polinomban minden $j \geq 0$ -ra).

Nullapolinom

A **nullapolinom** az a polinom, amelynek minden együtthatója nulla. Ugyanúgy 0 jelöli, mint az R nullelemét.

Minden $c \in R$ elemet **konstans** polinomnak tekintünk.

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$a_0 + a_1x + a_2x^2 + \dots + a_nx^n =$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \end{aligned}$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} \end{aligned}$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} \end{aligned}$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} a_0 + a_1x + a_2x^2 + \dots + a_nx^n &= \\ = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Így bármely két polinomot ugyanannyi taggal írhatunk fel.

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Így bármely két polinomot ugyanannyi taggal írhatunk fel.

Összeg és különbség

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Így bármely két polinomot ugyanannyi taggal írhatunk fel.

Összeg és különbség

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Így bármely két polinomot ugyanannyi taggal írhatunk fel.

Összeg és különbség

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

összege és különbsége:

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Így bármely két polinomot ugyanannyi taggal írhatunk fel.

Összeg és különbség

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

összege és különbsége:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n$$

Polinomok összege, különbsége

A nulla együtthatójú tagokat igény szerint írjuk ki:

$$\begin{aligned} & a_0 + a_1x + a_2x^2 + \dots + a_nx^n = \\ & = a_0 + a_1x + a_2x^2 + \dots + a_nx^n + 0 \cdot x^{n+1} + 0 \cdot x^{n+2} + \dots \end{aligned}$$

Megállapodunk abban, hogy $0 = a_{n+1} = a_{n+2} = \dots$

Így bármely két polinomot ugyanannyi taggal írhatunk fel.

Összeg és különbség

$$f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n$$

$$g(x) = b_0 + b_1x + b_2x^2 + \dots + b_nx^n$$

összege és különbsége:

$$(f + g)(x) = (a_0 + b_0) + (a_1 + b_1)x + \dots + (a_n + b_n)x^n$$

$$(f - g)(x) = (a_0 - b_0) + (a_1 - b_1)x + \dots + (a_n - b_n)x^n.$$

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h ,

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$.

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.
Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.
Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje
 $h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n$.

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Szorzat

$(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$ -ben
 x^k együtthatója legyen

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Szorzat

$(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$ -ben

x^k együtthatója legyen $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$.

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Szorzat

$(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$ -ben

x^k együtthatója legyen $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$.

$$\text{Azaz } (fg)(x) = \sum_{k=0}^{m+n} c_k x^k,$$

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Szorzat

$(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$ -ben

x^k együtthatója legyen $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$.

Azaz $(fg)(x) = \sum_{k=0}^{m+n} c_k x^k$, ahol $c_k = \sum_{j=0}^k a_j b_{k-j}$

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Szorzat

$(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$ -ben

x^k együtthatója legyen $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$.

Azaz $(fg)(x) = \sum_{k=0}^{m+n} c_k x^k$, ahol $c_k = \sum_{j=0}^k a_j b_{k-j} = \sum_{j+l=k} a_j b_l$.

Polinomok ellentettje és szorzata

Ellentett

Az $f \in R[x]$ **ellentettje** h , ha $f + h = 0$. Az ellentett jele $h = -f$.

Az $f(x) = a_0 + a_1x + \dots + a_nx^n$ (egyetlen) ellentettje

$$h(x) = (-f)(x) = (-a_0) + (-a_1)x + \dots + (-a_n)x^n.$$

A kivonás az ellentett hozzáadása: $g - f = g + (-f)$.

Szorzat

$(a_0 + a_1x + \dots + a_nx^n)(b_0 + b_1x + \dots + b_mx^m)$ -ben
 x^k együtthatója legyen $c_k = a_0b_k + a_1b_{k-1} + \dots + a_kb_0$.

Azaz $(fg)(x) = \sum_{k=0}^{m+n} c_k x^k$, ahol $c_k = \sum_{j=0}^k a_j b_{k-j} = \sum_{j+l=k} a_j b_l$.

Tétel

$R[x]$ is egységelemes, kommutatív gyűrű ezekre a műveletekre.

Polinom fok

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$,

Polinom fok

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$,

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$,
akkor f **foka** n .

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$.

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Bizonyítás

$$f(x) = a_0 + a_1x + \dots + a_nx^n$$

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Bizonyítás

$f(x) = a_0 + a_1x + \dots + a_nx^n$ és $g(x) = b_0 + b_1x + \dots + b_mx^m$

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Bizonyítás

$f(x) = a_0 + a_1x + \dots + a_nx^n$ és $g(x) = b_0 + b_1x + \dots + b_mx^m$
szorzatában x^{n+m} együtthatója a_nb_m .

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Bizonyítás

$f(x) = a_0 + a_1x + \dots + a_nx^n$ és $g(x) = b_0 + b_1x + \dots + b_mx^m$
szorzatában x^{n+m} együtthatója a_nb_m .

Ez nem nulla, ha a_n és b_m nem nulla, mert R nullosztómentes.

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Bizonyítás

$f(x) = a_0 + a_1x + \dots + a_nx^n$ és $g(x) = b_0 + b_1x + \dots + b_mx^m$
szorzatában x^{n+m} együtthatója a_nb_m .

Ez nem nulla, ha a_n és b_m nem nulla, mert R nullosztómentes.

Megjegyzés: Szorzásnál a főegyütthatók és a konstans tagok is összeszorzódnak,

Polinom foka

Definíció

Ha $f(x) = a_0 + a_1x + \dots + a_nx^n \in R[x]$, ahol $a_n \neq 0$, akkor f **foka** n . Jele: $\text{gr}(f)$. **A nullapolinomnak nincs foka.**

Tétel

Ha R nullosztómentes gyűrű, akkor $\text{gr}(fg) = \text{gr}(f) + \text{gr}(g)$.
Így ha R nullosztómentes, akkor $R[x]$ is az.

Bizonyítás

$f(x) = a_0 + a_1x + \dots + a_nx^n$ és $g(x) = b_0 + b_1x + \dots + b_mx^m$ szorzatában x^{n+m} együtthatója a_nb_m .

Ez nem nulla, ha a_n és b_m nem nulla, mert R nullosztómentes.

Megjegyzés: Szorzásnál a főegyütthatók és a konstans tagok is összeszorzódnak, hiszen fg konstans tagja nyilván a_0b_0 .

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**:

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is:

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**:

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R -ben.

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R -ben.

Bizonyítás

Ha $fg = 1$,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R -ben.

Bizonyítás

Ha $fg = 1$, akkor $\text{gr}(f) + \text{gr}(g) = 0$,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R -ben.

Bizonyítás

Ha $fg = 1$, akkor $\text{gr}(f) + \text{gr}(g) = 0$, így f és g konstans.

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R -ben.

Bizonyítás

Ha $fg = 1$, akkor $\text{gr}(f) + \text{gr}(g) = 0$, így f és g konstans.

Megfordítva, ha $c \in R$ egység,

A polinomgyűrű egységei

Definíció

Legyen R egységelemes gyűrű és $r, s \in R$.

Ha $rs = 1$, akkor r **balinverze** s -nek, s **jobbinverze** r -nek.

(Kétoldali) **inverz**: balinverz és jobbinverz is: $rs = sr = 1$.

Invertálható elem, vagy **egység**: van inverze.

Tétel

Ha R (egységelemes, kommutatív és) nullosztómentes, akkor az $f \in R[x]$ polinom pontosan akkor egység, ha egy olyan konstans polinom, amely egység R -ben.

Bizonyítás

Ha $fg = 1$, akkor $\text{gr}(f) + \text{gr}(g) = 0$, így f és g konstans.

Megfordítva, ha $c \in R$ egység, akkor $1/c \in R[x]$.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Az $f^* : R \mapsto R$ az f -hez tartozó **polinomfüggvény**.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Az $f^* : R \mapsto R$ az f -hez tartozó **polinomfüggvény**.

Az $f^*(b)$ kiszámítása: Horner elrendezéssel.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Az $f^* : R \mapsto R$ az f -hez tartozó **polinomfüggvény**.

Az $f^*(b)$ kiszámítása: Horner elrendezéssel.

A b **gyöke** f -nek, ha $f^*(b) = 0$.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Az $f^* : R \mapsto R$ az f -hez tartozó **polinomfüggvény**.

Az $f^*(b)$ kiszámítása: Horner elrendezéssel.

A b **gyöke** f -nek, ha $f^*(b) = 0$.

A gyöktényező kiemelhetősége

A $b \in R$ akkor és csak akkor gyöke az $f \in R[x]$ -nek,
ha van olyan $q \in R[x]$, hogy

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Az $f^* : R \mapsto R$ az f -hez tartozó **polinomfüggvény**.

Az $f^*(b)$ kiszámítása: Horner elrendezéssel.

A b **gyöke** f -nek, ha $f^*(b) = 0$.

A gyöktényező kiemelhetősége

A $b \in R$ akkor és csak akkor gyöke az $f \in R[x]$ -nek,

ha van olyan $q \in R[x]$, hogy $f(x) = (x - b)q(x)$.

Behelyettesítés polinomba

Polinomfüggvény

Legyen R kommutatív, egységelemes gyűrű és $b \in R$.

Az $f(x) = a_0 + a_1x + a_2x^2 + \dots + a_nx^n \in R[x]$

polinom b helyen felvett helyettesítési értéke

$f^*(b) = a_0 + a_1b + a_2b^2 + \dots + a_nb^n \in R$.

Az $f^* : R \mapsto R$ az f -hez tartozó **polinomfüggvény**.

Az $f^*(b)$ kiszámítása: Horner elrendezéssel.

A b **gyöke** f -nek, ha $f^*(b) = 0$.

A gyöktényező kiemelhetősége

A $b \in R$ akkor és csak akkor gyöke az $f \in R[x]$ -nek,

ha van olyan $q \in R[x]$, hogy $f(x) = (x - b)q(x)$.

Az $x - b$ a b gyökhöz tartozó **gyöktényező**.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban,

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei,

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.
Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$$f(x) = (x - b_1) \dots (x - b_k)q(x),$$

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Valóban, ha $f^*(b) = 0$,

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Valóban, ha $f^*(b) = 0$, akkor $(b - b_1) \dots (b - b_k)q^*(b) = 0$.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Valóban, ha $f^*(b) = 0$, akkor $(b - b_1) \dots (b - b_k)q^*(b) = 0$.

A **nullosztómentesség** miatt valamelyik tényező nulla.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Valóban, ha $f^*(b) = 0$, akkor $(b - b_1) \dots (b - b_k)q^*(b) = 0$.

A **nullosztómentesség** miatt valamelyik tényező nulla.

De $q^*(b) \neq 0$,

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Valóban, ha $f^*(b) = 0$, akkor $(b - b_1) \dots (b - b_k)q^*(b) = 0$.

A **nullosztómentesség** miatt valamelyik tényező nulla.

De $q^*(b) \neq 0$, ezért $b - b_j = 0$ valamelyik j -re.

Több gyöktényező kiemelése

Tétel (Kiss-jegyzet, 2.4.7. Tétel)

Ha R (kommutatív, egységelemes és) **nullosztómentes**, akkor minden $0 \neq f \in R[x]$ fölírható $f(x) = (x - b_1) \dots (x - b_k)q(x)$ alakban, ahol a (nem feltétlenül különböző) $b_1, \dots, b_k \in R$ az f -nek az **összes** R -beli gyökei, és q -nak nincs gyöke R -ben.

A bizonyítás kulcslépése

Addig emelünk ki gyöktényezőket, ameddig lehet.

Legfeljebb $\text{gr}(f)$ lépésben biztosan megállunk:

$f(x) = (x - b_1) \dots (x - b_k)q(x)$, ahol q -nak már nincs gyöke.

Belátjuk, hogy f -nek nincs más gyöke, mint b_1, \dots, b_k .

Valóban, ha $f^*(b) = 0$, akkor $(b - b_1) \dots (b - b_k)q^*(b) = 0$.

A **nullosztómentesség** miatt valamelyik tényező nulla.

De $q^*(b) \neq 0$, ezért $b - b_j = 0$ valamelyik j -re. Azaz $b = b_j$.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.
A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $3^2 - 1$

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1$

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1 = (3 - 1)(3 + 1)$

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1 = (3 - 1)(3 + 1) = 4 *_8 2$.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1 = (3 - 1)(3 + 1) = 4 *_{\mathbb{Z}_8} 2$.

Vagyis a probléma az, hogy \mathbb{Z}_8 nem nullosztómentes.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1 = (3 - 1)(3 + 1) = 4 *_{\mathbb{Z}_8} 2$.

Vagyis a probléma az, hogy \mathbb{Z}_8 nem nullosztómentes.

Ugyanígy $x^2 - 1 = (x - 3)(x + 3)$ is teljesül,

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1 = (3 - 1)(3 + 1) = 4 *_{\mathbb{Z}_8} 2$.

Vagyis a probléma az, hogy \mathbb{Z}_8 nem nullosztómentes.

Ugyanígy $x^2 - 1 = (x - 3)(x + 3)$ is teljesül,

azaz **a gyöktényező alak nem egyértelmű**.

Gyöktényező a nem nullosztómentes esetben

Példa (Kiss-jegyzet, 2.4. Szakasz)

Legyen $R = \mathbb{Z}_8$ és $f(x) = x^2 - 1$ másodfokú polinom.

A \mathbb{Z}_8 gyűrű 8 elemét végigpróbálgatva a gyökök **1, 3, 5, 7**.

(Páratlan szám négyzete nyolccal osztva 1-et ad maradékul.)

Azaz egy **másodfokú** polinomnak **négy** gyöke van.

Magyarázat

$x^2 - 1 = (x - 1)(x + 1)q(x)$, ahol a $q(x) = 1$ -nek nincs gyöke.

$x = 3$ helyettesítéssel $0 = 3^2 - 1 = (3 - 1)(3 + 1) = 4 *_{\mathbb{Z}_8} 2$.

Vagyis a probléma az, hogy \mathbb{Z}_8 nem nullosztómentes.

Ugyanígy $x^2 - 1 = (x - 3)(x + 3)$ is teljesül,

azaz **a gyöktényező alak nem egyértelmű**.

A különböző gyökökhöz tartozó gyöktényezőket **egyszerre** csak nullosztómentes gyűrű fölött lehet kiemelni.

A gyökök száma

A polinomok azonosságai tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

A gyökök száma

A polinomok azonosságai tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.

A gyökök száma

A polinomok azonosságai tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik,

A gyökök száma

A polinomok azonosságai tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).

A gyökök száma

A polinomok azonosságai tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű,

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők,

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységteles és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$.

A gyökök száma

A polinomok azonosságai tétele

Ha R kommutatív, egységteles és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a fok.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$. Ha R **véges**,

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységteles és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$. Ha R **véges**, akkor van két különböző polinom, melyek polinomfüggvénye ugyanaz.

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységteles és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$. Ha R **véges**, akkor van két különböző polinom, melyek polinomfüggvénye ugyanaz.

Bizonyítás

- (1): Egyszerre kiemelhetők a gyöktényezők.

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységteles és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$. Ha R **véges**, akkor van két különböző polinom, melyek polinomfüggvénye ugyanaz.

Bizonyítás

- (1): Egyszerre kiemelhetők a gyöktényezők.
- (2): Alkalmazzuk (1)-et a két polinom különbségére.

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységelemes és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$. Ha R **véges**, akkor van két különböző polinom, melyek polinomfüggvénye ugyanaz.

Bizonyítás

- (1): Egyszerre kiemelhetők a gyöktényezők.
- (2): Alkalmazzuk (1)-et a két polinom különbségére.
- (3): Ha R végtelen, akkor (2)-ben van „elég” elem.

A gyökök száma

A polinomok azonossági tétele

Ha R kommutatív, egységteles és **nullosztómentes**:

- (1) Minden polinomnak legfeljebb annyi gyöke van, mint a foka.
- (2) Ha két, legfeljebb n -edfokú polinom több mint n helyen megegyezik, akkor egyenlők (együtthatóik megegyeznek).
- (3) Ha R **végtelen** gyűrű, és az f^* és g^* polinomfüggvények egyenlők, akkor $f = g$. Ha R **véges**, akkor van két különböző polinom, melyek polinomfüggvénye ugyanaz.

Bizonyítás

- (1): Egyszerre kiemelhetők a gyöktényezők.
- (2): Alkalmazzuk (1)-et a két polinom különbségére.
- (3): Ha R végtelen, akkor (2)-ben van „elég” elem.
Véges gyűrű fölött csak véges sok polinomfüggvény van.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz:

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Valóban: \mathbb{Z}_p test,

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Valóban: \mathbb{Z}_p test, a két oldal különbsége legfeljebb $p - 2$ fokú,

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Valóban: \mathbb{Z}_p test, a két oldal különbsége legfeljebb $p - 2$ fokú, mert x^{p-1} kiesik,

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Valóban: \mathbb{Z}_p test, a két oldal különbsége legfeljebb $p - 2$ fokú, mert x^{p-1} kiesik, de az $1, 2, \dots, p - 1$ helyeken megegyeznek.

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Valóban: \mathbb{Z}_p test, a két oldal különbsége legfeljebb $p - 2$ fokú, mert x^{p-1} kiesik, de az $1, 2, \dots, p - 1$ helyeken megegyeznek.

HF: Lássuk be Wilson tételét:

Véges gyűrű fölötti polinomfüggvények

Példa

Legyen $R = \mathbb{Z}_2$. Ekkor az x^k -hoz tartozó polinomfüggvény minden $k \geq 1$ esetén ugyanaz: az identitás.

Valóban: x^k értéke $x = 0$ -nál 0 és $x = 1$ -nél 1.

Legyen $R = \mathbb{Z}_p$ ahol p prím.

Ekkor az x^p -hez és x -hez tartozó polinomfüggvény ugyanaz.

Valóban: A kis Fermat-tétel szerint $p \mid x^p - x$ minden x egészre.

\mathbb{Z}_p fölött $x^{p-1} - 1 = (x - 1) \dots (x - (p - 1))$.

Valóban: \mathbb{Z}_p test, a két oldal különbsége legfeljebb $p - 2$ fokú, mert x^{p-1} kiesik, de az $1, 2, \dots, p - 1$ helyeken megegyeznek.

HF: Lássuk be Wilson tételét: $p \mid (p - 1)! + 1$, ha p prím.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$.

Ha a $+$ összeadásra van nullelem, akkor legyen $0a = 0$.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$.

Ha a $+$ összeadásra van nullelem, akkor legyen $0a = 0$.

Ha a -nak van egy b inverze, akkor legyen $a^{-n} = b^n$.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$.

Ha a $+$ összeadásra van nullelem, akkor legyen $0a = 0$.

Ha a -nak van egy b inverze, akkor legyen $a^{-n} = b^n$.

Ha a -nak van egy b ellentettje, akkor legyen $(-n)a = nb$.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Ha a $*$ szorzásra van 1 egységelem, akkor legyen $a^0 = 1$.

Ha a $+$ összeadásra van nullelem, akkor legyen $0a = 0$.

Ha a -nak van egy b inverze, akkor legyen $a^{-n} = b^n$.

Ha a -nak van egy b ellentettje, akkor legyen $(-n)a = nb$.

Értelmeztük az **egész kitevőjű** hatvány (többszörös) fogalmát.

Hatvány és többszörös

Definíció (Kiss-jegyzet, 2.2.17. Definíció)

Legyen $*$ asszociatív művelet és n pozitív egész.

Ekkor a^n jelentse az n tényezős $a * a * \dots * a$ szorzatot.

Ez az a elem n -edik **hatványa**.

Ha a művelet jele $+$, akkor a^n helyett na -t írunk.

Ez az a elem n -szerese (**többszörös**).

Ha $a * szorzásra van 1 egységelem, akkor legyen $a^0 = 1$.$

Ha $a + összeadásra van nullelem, akkor legyen $0a = 0$.$

Ha a -nak van egy b inverze, akkor legyen $a^{-n} = b^n$.

Ha a -nak van egy b ellentettje, akkor legyen $(-n)a = nb$.

Értelmeztük az **egész kitevőjű** hatvány (többszörös) fogalmát.
Így minden gyűrű elemeit tudjuk egész számokkal „szorozni”.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív,

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve,

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

(2) $a^m a^n = a^{m+n}$.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

(2) $a^m a^n = a^{m+n}$.

(3) $(a^m)^n = a^{mn}$.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

- (1) a^{-n} az a^n inverze.
- (2) $a^m a^n = a^{m+n}$.
- (3) $(a^m)^n = a^{mn}$.
- (4) Ha a és b **felcserélhetők** ($ab = ba$),

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

- (1) a^{-n} az a^n inverze.
- (2) $a^m a^n = a^{m+n}$.
- (3) $(a^m)^n = a^{mn}$.
- (4) Ha a és b **felcserélhetők** ($ab = ba$), akkor $(ab)^n = a^n b^n$.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

(2) $a^m a^n = a^{m+n}$.

(3) $(a^m)^n = a^{mn}$.

(4) Ha a és b **felcserélhetők** ($ab = ba$), akkor $(ab)^n = a^n b^n$.

Az analóg állítások érvényesek hatvány helyett többszörösre is.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

(2) $a^m a^n = a^{m+n}$.

(3) $(a^m)^n = a^{mn}$.

(4) Ha a és b **felcserélhetők** ($ab = ba$), akkor $(ab)^n = a^n b^n$.

Az analóg állítások érvényesek hatvány helyett többszörösre is.

Bizonyítás

Pozitív kitevőkre egyszerű leszámplálás.

A hatványozás tulajdonságai

Állítás (Kiss-jegyzet, 2.2.18. Gyakorlat)

Legyenek a és b invertálható elemek egy asszociatív, egymás mellé írással jelölt műveletre nézve, és m, n egész számok. Ekkor a következők teljesülnek.

(1) a^{-n} az a^n inverze.

(2) $a^m a^n = a^{m+n}$.

(3) $(a^m)^n = a^{mn}$.

(4) Ha a és b **felcserélhetők** ($ab = ba$), akkor $(ab)^n = a^n b^n$.

Az analóg állítások érvényesek hatvány helyett többszörösre is.

Bizonyítás

Pozitív kitevőkre egyszerű leszámplálás.

A többi esetben esetszétválasztás (HF).

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám,

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$$(r + s)^p = r^p + s^p:$$

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p$

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p$

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p = 1 + 1$

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p = 1 + 1 = 2$.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p = 1 + 1 = 2$. Azaz $p \mid 2^p - 2$.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p = 1 + 1 = 2$. Azaz $p \mid 2^p - 2$.

Ugyanígy $3^p = (1 + 1 + 1)^p$

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p = 1 + 1 = 2$. Azaz $p \mid 2^p - 2$.

Ugyanígy $3^p = (1 + 1 + 1)^p = 1^p + 1^p + 1^p = 3$.

Tagonkénti hatványozás

Állítás (Kiss-jegyzet, 3.3.20. Feladat)

Legyen p prímszám, és R olyan kommutatív gyűrű, amelyben minden elem p -szerese nulla. Ekkor $r, s \in R$ esetén

$(r + s)^p = r^p + s^p$: tagonként lehet p -edik hatványra emelni.

Bizonyítás

A binomiális tétel alkalmazható minden kommutatív gyűrűben. Egyszerű számelméleti megfontolás, hogy a $\binom{p}{j}$ binomiális együttható osztható p -vel, ha $1 \leq j \leq p - 1$.

Alkalmazás

\mathbb{Z}_p -ben $2^p = (1 + 1)^p = 1^p + 1^p = 1 + 1 = 2$. Azaz $p \mid 2^p - 2$.

Ugyanígy $3^p = (1 + 1 + 1)^p = 1^p + 1^p + 1^p = 3$.

HF: belátni a kis Fermat-tételt.