

# Algebra1, normál

## ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil  
ewwkiss@gmail.com

11. előadás

# Hatvány és többszörös

## Definíció (K2.2.19)

Legyen  $*$  asszociatív művelet és  $n$  pozitív egész.

# Hatvány és többszörös

## Definíció (K2.2.19)

Legyen  $*$  asszociatív művelet és  $n$  pozitív egész.

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

# Hatvány és többszörös

## Definíció (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.19)

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 (K2.2.20)

Legyenek  $a$  és  $b$  invertálható elemek egy asszociatív,

# A hatványozás tulajdonságai

## Állítás (K2.2.20)

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

# A hatványozás tulajdonságai

## Állítás (K2.2.20)

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

# A hatványozás tulajdonságai

## Állítás (K2.2.20)

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 (K2.2.20)

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 (K2.2.20)

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 (K2.2.20)

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 (K2.2.20)

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 (K2.2.20)

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 (K2.2.20)

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 (K2.2.20)

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 leszámlálás.

# A hatványozás tulajdonságai

## Állítás (K2.2.20)

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 leszámlálás.

A többi esetben esetszétválasztás (HF).



# Tagonkénti hatványozás

Állítás (K3.3.22)

Legyen  $p$  prímszám,

# Tagonkénti hatványozás

## Állítás (K3.3.22)

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

# Tagonkénti hatványozás

## Állítás (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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 (K3.3.22)

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.

# A polinom definíciója

## Polinom (K2.1. szakasz)

Legyen  $R$  kommutatív, egységelemes gyűrű.

# A polinom definíciója

## Polinom (K2.1. szakasz)

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 (K2.1. szakasz)

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 (K2.1. szakasz)

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 (K2.1. szakasz)

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 (K2.1. szakasz)

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 (K2.1.1)

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

# A polinom definíciója

## Polinom (K2.1. szakasz)

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 (K2.1.1)

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

# A polinom definíciója

## Polinom (K2.1. szakasz)

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 (K2.1.1)

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 (K2.1. szakasz)

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 (K2.1.1)

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 (K2.1. szakasz)

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 (K2.1.1)

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 (K2.1.6, K2.3.2)

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

# Polinom foka

## Definíció

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

# Polinom foka

## 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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.1.5, K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.3.2)

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 (K2.4.1)

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

# Behelyettesítés polinomba

## Polinomfüggvény (K2.4.1)

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 (K2.4.1)

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 (K2.4.1)

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 (K2.4.1)

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 (K2.4.1)

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 (K2.4.1)

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 (K2.4.6)

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 (K2.4.1)

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 (K2.4.6)

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 (K2.4.1)

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 (K2.4.6)

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.

# Behelyettesítés polinomba

## Polinomfüggvény (K2.4.1)

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 (K2.4.6)

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.

**Bizonyítás:** Horner-elrendezéssel.

# Több gyöktényező kiemelése

## Tétel (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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  $gr(f)$  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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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 (K2.4.7)

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  $gr(f)$  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 (K2.4.7)

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 (K, 57. oldal)

Legyen  $R = \mathbb{Z}_8$

# Gyöktényező a nem nullosztómentes esetben

Példa (K, 57. oldal)

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

# Gyöktényező a nem nullosztómentes esetben

Példa (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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 (K, 57. oldal)

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

# Gyöktényező a nem nullosztómentes esetben

## Példa (K, 57. oldal)

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

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

# Gyöktényező a nem nullosztómentes esetben

## Példa (K, 57. oldal)

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

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 (K, 57. oldal)

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

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 (K, 57. oldal)

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

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 azonossági tétele (K2.4.10, K2.4.11)

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

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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

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

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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 azonossági tétele (K2.4.10, K2.4.11)

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 azonossági tétele (K2.4.10, K2.4.11)

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 (K2.4.10, K2.4.11)

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 (K2.4.10, K2.4.11)

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  $f = g$ .

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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**,

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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.

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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.

## A bizonyítások megjegyzendő fő gondolatai:

- (1): Egyszerre kiemelhetők a gyöktényezők.

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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.

## A bizonyítások megjegyzendő fő gondolatai:

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

# A gyökök száma

## A polinomok azonossági tétele (K2.4.10, K2.4.11)

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.

## A bizonyítások megjegyzendő fő gondolatai:

- (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 (K2.4.10, K2.4.11)

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.

## A bizonyítások megjegyzendő fő gondolatai:

- (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  $x$  egészszre.

# 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  $x$  egészszre.

$\mathbb{Z}_p$  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  $x$  egészszre.

$\mathbb{Z}_p$  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  $x$  egészszre.

$\mathbb{Z}_p$  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  $x$  egészszre.

$\mathbb{Z}_p$  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  $x$  egészszre.

$\mathbb{Z}_p$  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 ebből 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 ebből Wilson tételét:  $p \mid (p - 1)! + 1$ , ha  $p$  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.

**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 ebből Wilson tételét:  $p \mid (p - 1)! + 1$ , ha  $p$  prím.

**Ötlet:**  $x = 0$  helyettesítés.

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha



# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív,

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes,

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes.

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük.

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük.

Ha  $r, s \in R$ ,

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek),

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ .



# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben,

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

(1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ ,

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ , sőt  $rt \mid st$ .

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ , sőt  $rt \mid st$ . Megfordítva, ha  $t \neq 0$ , akkor  $rt \mid st$ -ből  $r \mid s$  következik

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ , sőt  $rt \mid st$ . Megfordítva, ha  $t \neq 0$ , akkor  $rt \mid st$ -ből  $r \mid s$  következik ( $R$  nullosztómentes!).



# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ , sőt  $rt \mid st$ . Megfordítva, ha  $t \neq 0$ , akkor  $rt \mid st$ -ből  $r \mid s$  következik ( $R$  nullosztómentes!).
- (3) **Tranzitivitás:** ha  $r \mid s$  és  $s \mid t$ , akkor  $r \mid t$ .

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ , sőt  $rt \mid st$ . Megfordítva, ha  $t \neq 0$ , akkor  $rt \mid st$ -ből  $r \mid s$  következik ( $R$  nullosztómentes!).
- (3) **Tranzitivitás:** ha  $r \mid s$  és  $s \mid t$ , akkor  $r \mid t$ .
- (4) **Reflexivitás:**  $r \mid r$  minden  $r \in R$  esetén

# Oszthatóság

## Definíció (K3.1.3)

Az  $R$  szokásos gyűrű, ha kommutatív, egységelemes, nullosztómentes. Számelméleti vizsgálatokban ezt feltesszük. Ha  $r, s \in R$ , akkor  $r$  osztója  $s$ -nek ( $s$  többszöröse  $r$ -nek), ha van olyan  $t \in R$ , hogy  $rt = s$ . Jele:  $r \mid s$ .

Példa:  $2x \mid 3x^2$  igaz  $\mathbb{R}[x]$ -ben, nem igaz  $\mathbb{Z}[x]$ -ben.

## Tulajdonságok (K3.1.4)

- (1) Ha  $r \mid s$  és  $r \mid t$ , akkor  $r \mid s \pm t$ .
- (2) Ha  $r \mid s$ , akkor  $r \mid st$ , sőt  $rt \mid st$ . Megfordítva, ha  $t \neq 0$ , akkor  $rt \mid st$ -ből  $r \mid s$  következik ( $R$  nullosztómentes!).
- (3) **Tranzitivitás:** ha  $r \mid s$  és  $s \mid t$ , akkor  $r \mid t$ .
- (4) **Reflexivitás:**  $r \mid r$  minden  $r \in R$  esetén ( $R$  egységelemes!).

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  egység, ha  $e \mid 1$ .

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem.

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ .

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .



# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói?

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása,

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis),

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység,

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

**Ekvivalens:**  $p$  minden osztója egység, vagy  $p$  egységszerese.



# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

**Ekvivalens:**  $p$  minden osztója egység, vagy  $p$  egységszerese.

**Példa:** A  $23$  felbonthatatlan  $\mathbb{Z}$ -ben,

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

**Ekvivalens:**  $p$  minden osztója egység, vagy  $p$  egységszerese.

**Példa:** A  $23$  felbonthatatlan  $\mathbb{Z}$ -ben, mert nem nulla, nem  $\pm 1$ ,

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

**Ekvivalens:**  $p$  minden osztója egység, vagy  $p$  egységszerese.

**Példa:** A  $23$  felbonthatatlan  $\mathbb{Z}$ -ben, mert nem nulla, nem  $\pm 1$ , és osztói csak  $\pm 1$  és  $\pm 23$ .

# Felbonthatatlan elem

## Emlékeztető (K3.1.9)

Az  $e \in R$  **egység**, ha  $e \mid 1$ . Ez ugyanaz, mint az invertálható elem. Minden egység osztója  $R$  minden elemének.

**Példa:** A  $\mathbb{Z}$  gyűrű egységei  $\pm 1$ . Az egység**elem**e az  $1$ .

**HF:** Mik a  $0$  osztói? Mely elemeknek osztója a  $0$ ?

## Definíció (K3.1.12, K3.1.13, K3.1.14)

A  $b = cd$  a  $b$ -nek **triviális** felbontása, ha  $c$  és  $d$  egyike egység.

A  $p \in R$  **felbonthatatlan** (irreducibilis), ha nem nulla, nem egység, és **nincs nemtriviális felbontása**.

**Ekvivalens:**  $p$  minden osztója egység, vagy  $p$  egységszerese.

**Példa:** A  $23$  felbonthatatlan  $\mathbb{Z}$ -ben, mert nem nulla, nem  $\pm 1$ , és osztói csak  $\pm 1$  és  $\pm 23$ . Az összes felbontása:

$$23 = 1 \cdot 23 = 23 \cdot 1 = (-1)(-23) = (-23)(-1).$$

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele,**

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**,  
ha  $R$  minden nem nulla és nem egység eleme

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**,  
ha  $R$  minden nem nulla és nem egység eleme  
a sorrendtől és az egységszerestől eltekintve **egyértelműen**  
felbontható



# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára.

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ ,

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ ,

alaptételes.

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ , és minden  $T[x]$  polinomgyűrű, ahol  $T$  test, alaptételes.

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ , és minden  $T[x]$  polinomgyűrű, ahol  $T$  test, alaptételes.

- elvégezhető a maradékos osztás, ezért

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ , és minden  $T[x]$  polinomgyűrű, ahol  $T$  test, alaptételes.

- elvégezhető a maradékos osztás, ezért
- létezik „legnagyobb” közös osztó, ezért

# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ , és minden  $T[x]$  polinomgyűrű, ahol  $T$  test, alaptételes.

- elvégezhető a maradékos osztás, ezért
- létezik „legnagyobb” közös osztó, ezért
- a felbonthatatlan elemek ugyanazok, mint a prímek, ezért



# Alaptételes gyűrű

## Definíció (K3.1.15)

Az  $R$  gyűrűben **érvényes a számelmélet alaptétele**, ha  $R$  minden nem nulla és nem egység eleme a sorrendtől és az egységszerestől eltekintve **egyértelműen** felbontható felbonthatatlan elemek szorzatára. Az ilyen gyűrűt **alaptételes** gyűrűnek nevezzük.

## Tétel (K3.2.12)

A  $\mathbb{Z}$ , és minden  $T[x]$  polinomgyűrű, ahol  $T$  test, alaptételes.

- elvégezhető a maradékos osztás, ezért
- létezik „legnagyobb” közös osztó, ezért
- a felbonthatatlan elemek ugyanazok, mint a prímek, ezért
- egyértelmű a felbontás.

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és **23**-mal osztható számot kapott.

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben,

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység,

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik,

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik, hogy  $p \mid b$  vagy  $p \mid c$ .

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik, hogy  $p \mid b$  vagy  $p \mid c$ .

## Tétel (K3.1.26, K3.1.27, K3.2.13, K3.2.14)

A  $\mathbb{Z}$  gyűrűben,



# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik, hogy  $p \mid b$  vagy  $p \mid c$ .

## Tétel (K3.1.26, K3.1.27, K3.2.13, K3.2.14)

A  $\mathbb{Z}$  gyűrűben,

**a felbonthatatlan elemek ugyanazok, mint a prímelek.**

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik, hogy  $p \mid b$  vagy  $p \mid c$ .

## Tétel (K3.1.26, K3.1.27, K3.2.13, K3.2.14)

A  $\mathbb{Z}$  gyűrűben, továbbá a  $T[x]$  polinomgyűrűben, ahol  $T$  test, **a felbonthatatlan elemek ugyanazok, mint a prímek.**

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik, hogy  $p \mid b$  vagy  $p \mid c$ .

## Tétel (K3.1.26, K3.1.27, K3.2.13, K3.2.14)

A  $\mathbb{Z}$  gyűrűben, továbbá a  $T[x]$  polinomgyűrűben, ahol  $T$  test, **a felbonthatatlan elemek ugyanazok, mint a prímek.**

**Oka:** létezik „legnagyobb” közös osztó.

# Prímtulajdonságú elem

## Feladat

Pistike megszámolta a kockás füzetlapján a négyzetek számát, és 23-mal osztható számot kapott. Igazoljuk, hogy a lap valamelyik oldalán 23-mal osztható számú kis négyzet van.

## Definíció (K3.1.25)

A  $p \in R$  **prím**  $R$ -ben, ha nem nulla, nem egység, és tetszőleges  $b, c \in R$  esetén  $p \mid bc$ -ből következik, hogy  $p \mid b$  vagy  $p \mid c$ .

## Tétel (K3.1.26, K3.1.27, K3.2.13, K3.2.14)

A  $\mathbb{Z}$  gyűrűben, továbbá a  $T[x]$  polinomgyűrűben, ahol  $T$  test, **a felbonthatatlan elemek ugyanazok, mint a prímek.**

**Oka:** létezik „legnagyobb” közös osztó.

**HF:** Minden szokásos gyűrűben minden prím felbonthatatlan.

# Maradékös osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű.

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**,

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

# Maradékös osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékösan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok,



# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ ,

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ ,

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra.

# Maradékös osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékösan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra.

A tétel magában foglalja azt is, hogy  $q$  és  $r$  együtthatói az  $f$  és  $g$  együtthatóiból a négy alpművelettel kaphatók:

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra.

A tétel magában foglalja azt is, hogy  $q$  és  $r$  együtthatói az  $f$  és  $g$  együtthatóiból a négy alpművelettel kaphatók:

## Emlékeztető (K3.2.2)

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra.

A tétel magában foglalja azt is, hogy  $q$  és  $r$  együtthatói az  $f$  és  $g$  együtthatóiból a négy alpművelettel kaphatók:

## Emlékeztető (K3.2.2)

Ha  $g \mid f$  a  $\mathbb{C}[x]$ -ben,



# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra.

A tétel magában foglalja azt is, hogy  $q$  és  $r$  együtthatói az  $f$  és  $g$  együtthatóiból a négy alpművelettel kaphatók:

## Emlékeztető (K3.2.2)

Ha  $g \mid f$  a  $\mathbb{C}[x]$ -ben, és  $f, g \in \mathbb{R}[x]$ ,

# Maradékos osztás

## Tétel (K3.2.1)

Legyen  $R$  szokásos gyűrű. Ekkor az  $R[x]$  polinomgyűrűben minden olyan  $g \in R[x]$  polinommal lehet **maradékosan osztani**, amelynek **főegyütthatója invertálható** (azaz egység).

Ez azt jelenti, hogy tetszőleges  $f \in R[x]$  polinomhoz léteznek olyan  $q, r \in R[x]$  polinomok, melyekre  $f = gq + r$ , és vagy  $r = 0$ , vagy  $r$  foka kisebb  $g$  fokánál.

A  $q$  és  $r$  polinomok **egyértelműen** meghatározottak.

A bizonyítás ugyanaz mint komplex együtthatós polinomokra.

A tétel magában foglalja azt is, hogy  $q$  és  $r$  együtthatói az  $f$  és  $g$  együtthatóiból a négy alpművelettel kaphatók:

## Emlékeztető (K3.2.2)

Ha  $g \mid f$  a  $\mathbb{C}[x]$ -ben, és  $f, g \in \mathbb{R}[x]$ , akkor  $g \mid f$  az  $\mathbb{R}[x]$ -ben is.

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

(1) közös osztó,

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

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

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c$

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .



# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .

## Állítás (K3.1.27)

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója,

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .

## Állítás (K3.1.27)

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímek.

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .

## Állítás (K3.1.27)

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímek.

## Tétel (K5.5.9)

Ha egy  $R$  szokásos gyűrűben „**elvégezhető a maradékos osztás**”,

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .

## Állítás (K3.1.27)

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímek.

## Tétel (K5.5.9)

Ha egy  $R$  szokásos gyűrűben „**elvégezhető a maradékos osztás**”, akkor az euklideszi algoritmus miatt,

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .

## Állítás (K3.1.27)

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímek.

## Tétel (K5.5.9)

Ha egy  $R$  szokásos gyűrűben „**elvégezhető a maradékos osztás**”, akkor az euklideszi algoritmus miatt, bármely két elemnek van kitüntetett közös osztója,

# Kitüntetett közös osztó

## Definíció (K3.1.19)

A  $b$  és  $c$  elemeknek  $d$  **kitüntetett közös osztója**, ha

- (1) közös osztó, azaz  $d \mid b$  és  $d \mid c$ ;
- (2) minden közös osztónak többsége:  $d' \mid b$  és  $d' \mid c \implies d' \mid d$ .

## Állítás (K3.1.27)

Ha egy szokásos gyűrűben bármely két elemnek van kitüntetett közös osztója, akkor a felbonthatatlanok prímek.

## Tétel (K5.5.9)

Ha egy  $R$  szokásos gyűrűben „**elvégezhető a maradékos osztás**”, akkor az euklideszi algoritmus miatt, bármely két elemnek van kitüntetett közös osztója, ezért  $R$  **alaptételes**.

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  kanonikus alakja  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ,

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,



# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  
 $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok,

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,  
ahol a  $c$  a főegyüttható

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,  
ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,  
ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

Ez a gyöktényezős alak,

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,  
ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

Ez a gyöktényezős alak, a  $k_i$  a  $b_i$  gyök multiplicitása.



# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,

ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

Ez a gyöktényezős alak, a  $k_i$  a  $b_i$  gyök multiplicitása.

Az **osztók száma**,

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,  
ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

Ez a gyöktényezős alak, a  $k_i$  a  $b_i$  gyök multiplicitása.

Az **osztók száma**, a **kitüntetett közös osztó**,

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,

ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

Ez a gyöktényező-s alak, a  $k_i$  a  $b_i$  gyök multiplicitása.

Az **osztók száma**, a **kitüntetett közös osztó**, és a kitüntetett közös többszörös

# Kanonikus alak

## Definíció (K3.1.16)

A  $0 \neq r$  **kanonikus alakja**  $r = ep_1^{\alpha_1} p_2^{\alpha_2} \dots p_k^{\alpha_k}$ , ahol  $e$  egység,  $p_1, p_2, \dots, p_k$  pedig felbonthatatlanok, amelyek páronként nem egységszeresei egymásnak.

## Példák

$\mathbb{Z}$ -ben  $-36 = (-1)2^2 3^2$ .

$\mathbb{C}[x]$ -ben  $f(x) = c(x - b_1)^{k_1} (x - b_2)^{k_2} \dots (x - b_m)^{k_m}$ ,  
ahol a  $c$  a főegyütthető (nem nulla konstans, így egység).

Ez a gyöktényezős alak, a  $k_i$  a  $b_i$  gyök multiplicitása.

Az **osztók száma**, a **kitüntetett közös osztó**, és a kitüntetett közös többszörös hasonló képletekkel kapható a kanonikus alakból, mint az egész számok számelméletében.

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

(1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött,

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans,

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.



# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben,

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.
- (4) **Legalább negyedfokú** polinom,

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.
- (4) **Legalább negyedfokú** polinom, **HA** van gyöke  $T$ -ben,

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.
- (4) **Legalább negyedfokú** polinom, **HA** van gyöke  $T$ -ben, akkor biztosan **NEM** irreducibilis  $T[x]$ -ben.

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.
- (4) **Legalább negyedfokú** polinom, **HA** van gyöke  $T$ -ben, akkor biztosan **NEM** irreducibilis  $T[x]$ -ben. **Ha nincs gyöke, attól még lehet reducibilis!**

# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.
- (4) **Legalább negyedfokú** polinom, **HA** van gyöke  $T$ -ben, akkor biztosan **NEM** irreducibilis  $T[x]$ -ben. **Ha nincs gyöke, attól még lehet reducibilis!** Példa:  $\mathbb{Q}[x]$ -ben  $(x^2 + 1)^2$ .



# Gyökök és irreducibilitás

## Tétel (K3.3. szakasz)

Legyen  $T$  test.

- (1) Az  $f \in T[x]$  akkor és csak akkor irreducibilis  $T$  fölött, ha nem konstans, és nem bontható  $T[x]$ -ben **alacsonyabb fokú** polinomok szorzatára.
- (2) **Elsőfokú** polinom mindig irreducibilis  $T[x]$ -ben.
- (3) **Másod- és harmadfokú** polinom akkor és csak akkor irreducibilis  $T[x]$ -ben, ha **nincs gyöke**  $T$ -ben.
- (4) **Legalább negyedfokú** polinom, **HA** van gyöke  $T$ -ben, akkor biztosan **NEM** irreducibilis  $T[x]$ -ben. **Ha nincs gyöke, attól még lehet reducibilis!** Példa:  $\mathbb{Q}[x]$ -ben  $(x^2 + 1)^2$ .
- (5) Gyök létezése **elsőfokú** irreducibilis tényezőnek felel meg.

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval) értelmezzük:

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ ,

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ ,

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ , az együtthatók a már definiált  $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ , az együtthatók a már definiált  $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

## Előny

Mivel  $S = R[x_1, \dots, x_{n-1}]$  is kommutatív, egységelemes gyűrű,



# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ , az együtthatók a már definiált  $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

## Előny

Mivel  $S = R[x_1, \dots, x_{n-1}]$  is kommutatív, egységelemes gyűrű, az  $R[x_1, \dots, x_n] = S[x_n]$  is az.

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ , az együtthatók a már definiált  $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

## Előny

Mivel  $S = R[x_1, \dots, x_{n-1}]$  is kommutatív, egységelemes gyűrű, az  $R[x_1, \dots, x_n] = S[x_n]$  is az.

A tulajdonságokat nem kell külön ellenőrizni.

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ , az együtthatók a már definiált  $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

## Előny

Mivel  $S = R[x_1, \dots, x_{n-1}]$  is kommutatív, egységelemes gyűrű,  
az  $R[x_1, \dots, x_n] = S[x_n]$  is az.

**A tulajdonságokat nem kell külön ellenőrizni.**

**Példa:** Ha  $R$  nullosztómentes,

# Rekurzív definíció

## Definíció (K2.6.1)

Legyen  $R$  kommutatív, egységelemes gyűrű.

Ekkor  $R[x_1, \dots, x_n]$ -et  $n$  szerinti indukcióval (rekurzióval)

értelmezzük:  $R[x_1, x_2] = (R[x_1])[x_2]$ , és így tovább,

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n].$$

Vagyis a határozatlan  $x_n$ , az együtthatók a már definiált  $n - 1$ -határozatlanú polinomok gyűrűjének elemei.

## Előny

Mivel  $S = R[x_1, \dots, x_{n-1}]$  is kommutatív, egységelemes gyűrű, az  $R[x_1, \dots, x_n] = S[x_n]$  is az.

**A tulajdonságokat nem kell külön ellenőrizni.**

**Példa:** Ha  $R$  nullosztómentes, akkor indukcióval világos, hogy  $R[x_1, \dots, x_n]$  is nullosztómentes.

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 =$

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ .

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  
 $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ ,

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .



# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .  
Tehát  $s_2$  az elemi szimmetrikus polinomok **polinomja**.

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .  
Tehát  $s_2$  az elemi szimmetrikus polinomok **polinomja**.

## Tétel (K2.7.3)

Legyen  $R$  szokásos gyűrű.

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .  
Tehát  $s_2$  az elemi szimmetrikus polinomok **polinomja**.

## Tétel (K2.7.3)

Legyen  $R$  szokásos gyűrű. Ekkor minden  $f \in R[x_1, \dots, x_n]$  szimmetrikus polinom **egyértelműen** fölírható

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .  
Tehát  $s_2$  az elemi szimmetrikus polinomok **polinomja**.

## Tétel (K2.7.3)

Legyen  $R$  szokásos gyűrű. Ekkor minden  $f \in R[x_1, \dots, x_n]$  szimmetrikus polinom **egyértelműen** fölírható az elemi szimmetrikus polinomok polinomjaként.

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .  
Tehát  $s_2$  az elemi szimmetrikus polinomok **polinomja**.

## Tétel (K2.7.3)

Legyen  $R$  szokásos gyűrű. Ekkor minden  $f \in R[x_1, \dots, x_n]$  szimmetrikus polinom **egyértelműen** fölírható az elemi szimmetrikus polinomok polinomjaként.

Azaz létezik pontosan egy  $F \in R[y_1, \dots, y_n]$  polinom, melyre

$$f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n).$$

# A szimmetrikus polinomok alaptétele

## Példa

A négyzetösszeg:  $s_2 = x_1^2 + \dots + x_n^2 = \sigma_1^2 - 2\sigma_2$ . Vagyis ha  $F(y_1, y_2, \dots, y_n) = y_1^2 - 2y_2$ , akkor  $s_2 = F(\sigma_1, \sigma_2, \dots, \sigma_n)$ .  
Tehát  $s_2$  az elemi szimmetrikus polinomok **polinomja**.

## Tétel (K2.7.3)

Legyen  $R$  szokásos gyűrű. Ekkor minden  $f \in R[x_1, \dots, x_n]$  szimmetrikus polinom **egyértelműen** fölírható az elemi szimmetrikus polinomok polinomjaként.

Azaz létezik pontosan egy  $F \in R[y_1, \dots, y_n]$  polinom, melyre

$$f(x_1, \dots, x_n) = F(\sigma_1, \dots, \sigma_n).$$

A  $F$  együtthatói a  $f$  együtthatóiból összeadás és kivonás segítségével kaphatók.

# A többhatározatlanú polinomok számelmélete

Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes.

# A többhatározatlanú polinomok számelmélete

Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. Ugyanígy:

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.



# A többhatározatlanú polinomok számelmélete

## Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. **Ugyanígy:**

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

## Bizonyítás

Csak haladón és intenzíven, lásd K3.4. és K5.7. szakasz.

# A többhatározatlanú polinomok számelmélete

## Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. **Ugyanígy:**

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

## Bizonyítás

Csak haladón és intenzíven, lásd K3.4. és K5.7. szakasz.

## Következmény (vö. K3.4.12)

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x_1, x_2, \dots, x_n]$  is az.

# A többhatározatlanú polinomok számelmélete

## Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. **Ugyanígy:**  
Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

## Bizonyítás

Csak haladón és intenzíven, lásd K3.4. és K5.7. szakasz.

## Következmény (vö. K3.4.12)

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x_1, x_2, \dots, x_n]$  is az.  
**Speciálisan**  $\mathbb{Z}[x_1, x_2, \dots, x_n]$ ,

# A többhatározatlanú polinomok számelmélete

## Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. **Ugyanígy:**  
Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

## Bizonyítás

Csak haladón és intenzíven, lásd K3.4. és K5.7. szakasz.

## Következmény (vö. K3.4.12)

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x_1, x_2, \dots, x_n]$  is az.  
**Speciálisan  $\mathbb{Z}[x_1, x_2, \dots, x_n]$ ,  
alaptételes gyűrűk.**

# A többhatározatlanú polinomok számelmélete

## Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. **Ugyanígy:**  
Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

## Bizonyítás

Csak haladón és intenzíven, lásd K3.4. és K5.7. szakasz.

## Következmény (vö. K3.4.12)

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x_1, x_2, \dots, x_n]$  is az.  
**Speciálisan**  $\mathbb{Z}[x_1, x_2, \dots, x_n]$ , és ha  $T$  test,  
akkor  $T[x_1, x_2, \dots, x_n]$  is **alaptételes gyűrűk**.

# A többhatározatlanú polinomok számelmélete

## Tétel (K3.4.10, K3.4.11)

A  $\mathbb{Z}[x]$  polinomgyűrű alaptételes. **Ugyanígy:**  
Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x]$  is az.

## Bizonyítás

Csak haladón és intenzíven, lásd K3.4. és K5.7. szakasz.

## Következmény (vö. K3.4.12)

Ha  $R$  alaptételes, szokásos gyűrű, akkor  $R[x_1, x_2, \dots, x_n]$  is az.  
**Speciálisan**  $\mathbb{Z}[x_1, x_2, \dots, x_n]$ , és ha  $T$  test,  
akkor  $T[x_1, x_2, \dots, x_n]$  is **alaptételes gyűrűk**.

Általános gyűrűkben az alaptétel vizsgálata:  
K5.5. szakasz (az Algebra3 tárgy keretében).

# A 11. előadáshoz tartozó vizsgaanyag

## Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.

# A 11. előadáshoz tartozó vizsgaanyag

## Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok.



# A 11. előadáshoz tartozó vizsgaanyag

## Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.

# A 11. előadáshoz tartozó vizsgaanyag

## Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.

Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.

Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó általános gyűrűben.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.

Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.

Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó általános gyűrűben. Alaptételes gyűrű,

# A 11. előadáshoz tartozó vizsgaanyag

## Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.

Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.

Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.  
A polinom és a polinomfüggvény véges és végtelen gyűrű fölött.



## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.  
A polinom és a polinomfüggvény véges és végtelen gyűrű fölött.  
Ha van legnagyobb közös osztó, akkor minden irreducibilis prím.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.  
A polinom és a polinomfüggvény véges és végtelen gyűrű fölött.  
Ha van legnagyobb közös osztó, akkor minden irreducibilis prím.  
Maradékos osztás szokásos gyűrű fölött.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.  
A polinom és a polinomfüggvény véges és végtelen gyűrű fölött.  
Ha van legnagyobb közös osztó, akkor minden irreducibilis prím.  
Maradékos osztás szokásos gyűrű fölött. Gyökök és irreducibilitás  
kapcsolata test fölött.

## A 11. előadáshoz tartozó vizsgaanyag

### Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

### Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.  
A polinom és a polinomfüggvény véges és végtelen gyűrű fölött.  
Ha van legnagyobb közös osztó, akkor minden irreducibilis prím.  
Maradékos osztás szokásos gyűrű fölött. Gyökök és irreducibilitás  
kapcsolata test fölött. A szimmetrikus polinomok alaptétele.

# A 11. előadáshoz tartozó vizsgaanyag

## Fogalmak

Hatvány és többszörös általános gyűrűben, tulajdonságaik.  
Gyűrű fölötti polinomgyűrű, műveletek, fok. Polinomfüggvény.  
Oszthatóság, egység, felbonthatatlan, prím, kitüntetett közös osztó  
általános gyűrűben. Alaptételes gyűrű, kanonikus alak.

## Tételek

Ha  $(\forall r)(pr = 0)$ , akkor tagonként lehet  $p$ -edik hatványra emelni.  
A polinomgyűrű egységei. Gyöktényezők egyszerre kiemelhetősége.  
A polinom és a polinomfüggvény véges és végtelen gyűrű fölött.  
Ha van legnagyobb közös osztó, akkor minden irreducibilis prím.  
Maradékos osztás szokásos gyűrű fölött. Gyökök és irreducibilitás  
kapcsolata test fölött. A szimmetrikus polinomok alaptétele.  
 $\mathbb{Z}[x_1, x_2, \dots, x_n]$ ,  $T[x_1, x_2, \dots, x_n]$  alaptételes ( $T$  test).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzése (K1.5.13).



# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzése (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzései (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzése (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).
- 6 A Lagrange-interpoláció (K2.4.12).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzései (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).
- 6 A Lagrange-interpoláció (K2.4.12).
- 7  $f \in \mathbb{R}[x]$  gyöke konjugáltjának multiplicitása (K3.3.6).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzései (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).
- 6 A Lagrange-interpoláció (K2.4.12).
- 7  $f \in \mathbb{R}[x]$  gyöke konjugáltjának multiplicitása (K3.3.6).
- 8 A maradékos osztás tétele: létezés és egyértelműség (K3.2.1).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzései (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).
- 6 A Lagrange-interpoláció (K2.4.12).
- 7  $f \in \mathbb{R}[x]$  gyöke konjugáltjának multiplicitása (K3.3.6).
- 8 A maradékos osztás tétele: létezés és egyértelműség (K3.2.1).
- 9 A polinom és a polinomfüggvény kapcsolata véges és végtelen gyűrű fölött (K2.4.10, K2.4.11).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzései (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).
- 6 A Lagrange-interpoláció (K2.4.12).
- 7  $f \in \mathbb{R}[x]$  gyöke konjugáltjának multiplicitása (K3.3.6).
- 8 A maradékos osztás tétele: létezés és egyértelműség (K3.2.1).
- 9 A polinom és a polinomfüggvény kapcsolata véges és végtelen gyűrű fölött (K2.4.10, K2.4.11).
- 10 Minden test nullosztómentes (K2.2.29).

# Komplex számok, polinomok

- 1 A rend és a jó kitevők kapcsolata (K1.5.8).
- 2 Hatvány rendjének képlete (K1.5.9, K1.5.10).
- 3 A primitív egységgyökök jellemzései (K1.5.13).
- 4 Gyöktényezők kiemelése **egyszerre** (K2.4.7).
- 5 A racionális gyökteszt (K3.3.10).
- 6 A Lagrange-interpoláció (K2.4.12).
- 7  $f \in \mathbb{R}[x]$  gyöke konjugáltjának multiplicitása (K3.3.6).
- 8 A maradékos osztás tétele: létezés és egyértelműség (K3.2.1).
- 9 A polinom és a polinomfüggvény kapcsolata véges és végtelen gyűrű fölött (K2.4.10, K2.4.11).
- 10 Minden test nullosztómentes (K2.2.29).
- 11 Ha az  $R$  kommutatív gyűrűben  $pr$  azonosan nulla, akkor tagonként lehet  $p$ -edik hatványra emelni (K3.3.22).



# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).
- 14. A páros permutációk száma (K4.2.16).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).
- 14. A páros permutációk száma (K4.2.16).
- 15. Felső háromszögmátrix determinánsa (F1.2.3. Feladat).

# Lineáris algebra

- 12 Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13 Transzpozíció előjele (K4.2.12).
- 14 A páros permutációk száma (K4.2.16).
- 15 Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16 A transzponált determinánsa (F1.3.6. Tétel).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).
- 14. A páros permutációk száma (K4.2.16).
- 15. Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16. A transzponált determinánsa (F1.3.6. Tétel).
- 17. Ha a determináns két sora egyenlő, akkor nulla (F1.3.3. Tétel).

# Lineáris algebra

- 12 Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13 Transzpozíció előjele (K4.2.12).
- 14 A páros permutációk száma (K4.2.16).
- 15 Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16 A transzponált determinánsa (F1.3.6. Tétel).
- 17 Ha a determináns két sora egyenlő, akkor nulla (F1.3.3. Tétel).
- 18 A ferde kifejtési tétel (F1.4.3. Tétel).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).
- 14. A páros permutációk száma (K4.2.16).
- 15. Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16. A transzponált determinánsa (F1.3.6. Tétel).
- 17. Ha a determináns két sora egyenlő, akkor nulla (F1.3.3. Tétel).
- 18. A ferde kifejtési tétel (F1.4.3. Tétel).
- 19. Az inverz mátrix képlete (F2.2.2. Tétel, F2.2.3. Lemma).



# Lineáris algebra

- 12 Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13 Transzpozíció előjele (K4.2.12).
- 14 A páros permutációk száma (K4.2.16).
- 15 Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16 A transzponált determinánsa (F1.3.6. Tétel).
- 17 Ha a determináns két sora egyenlő, akkor nulla (F1.3.3. Tétel).
- 18 A ferde kifejtési tétel (F1.4.3. Tétel).
- 19 Az inverz mátrix képlete (F2.2.2. Tétel, F2.2.3. Lemma).
- 20 A Vandermonde-determináns (F1.5.2. Tétel).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).
- 14. A páros permutációk száma (K4.2.16).
- 15. Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16. A transzponált determinánsa (F1.3.6. Tétel).
- 17. Ha a determináns két sora egyenlő, akkor nulla (F1.3.3. Tétel).
- 18. A ferde kifejtési tétel (F1.4.3. Tétel).
- 19. Az inverz mátrix képlete (F2.2.2. Tétel, F2.2.3. Lemma).
- 20. A Vandermonde-determináns (F1.5.2. Tétel).
- 21. A Cramer-szabály (F3.2.1. Tétel).

# Lineáris algebra

- 12. Összefüggés lineáris, illetve homogén lineáris egyenletrendszer esetében a megoldások száma, az egyenletek száma és az ismeretlenek száma között (F3.1.2, F3.1.4. Tétel).
- 13. Transzpozíció előjele (K4.2.12).
- 14. A páros permutációk száma (K4.2.16).
- 15. Felső háromszögmátrix determinánsa (F1.2.3. Feladat).
- 16. A transzponált determinánsa (F1.3.6. Tétel).
- 17. Ha a determináns két sora egyenlő, akkor nulla (F1.3.3. Tétel).
- 18. A ferde kifejtési tétel (F1.4.3. Tétel).
- 19. Az inverz mátrix képlete (F2.2.2. Tétel, F2.2.3. Lemma).
- 20. A Vandermonde-determináns (F1.5.2. Tétel).
- 21. A Cramer-szabály (F3.2.1. Tétel).

A felsorolt 21 bizonyítás szerepelhet a vizsga **harmadik** részében.