Algebra1, alapszint

ELTE Algebra és Számelmélet Tanszék

Előadó: Kiss Emil
ewkiss@cs.elte.hu

11. előadás

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom **osztója** $f \in R[x]$-nek $R[x]$-ben,
ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$.

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom osztója $f \in R[x]$-nek $R[x]$-ben, ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$. Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom **osztója** $f \in R[x]$-nek $R[x]$-ben, ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$. Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

(2) a $g \in R[x]$ polinom **egység** $R[x]$-ben, ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom osztója $f \in R[x]$-nek $R[x]$-ben,
ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$.
Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

(2) a $g \in R[x]$ polinom egység $R[x]$-ben,
ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Példák

$x + 1$ osztója $x^2 - 1$-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ mindegyikében.

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom osztója $f \in R[x]$-nek $R[x]$-ben,
ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$.
Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

(2) a $g \in R[x]$ polinom egység $R[x]$-ben,
ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Példák

$x + 1$ osztója $x^2 - 1$-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ mindegyikében.
2 osztója x-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$-ben,

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom osztója $f \in R[x]$-nek $R[x]$-ben, ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$. Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

(2) a $g \in R[x]$ polinom egység $R[x]$-ben, ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Példák

$x + 1$ osztója $x^2 - 1$-nek $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$ mindegyikében.
2 osztója x-nek $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x]$-ben, de $\mathbb{Z}[x]$-ben nem.

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom **osztója** $f \in R[x]$-nek $R[x]$-ben,
ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$.
Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

(2) a $g \in R[x]$ polinom **egység** $R[x]$-ben,
ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Példák

$x + 1$ osztója $x^2 - 1$-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ mindegyikében.
2 osztója x-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$-ben, de $\mathbb{Z}[x]$-ben nem.
$\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ egységei a nem nulla konstans polinomok.

Oszthatóság, egységek

Emlékeztető

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy

(1) a $g \in R[x]$ polinom **osztója** $f \in R[x]$-nek $R[x]$-ben, ha létezik olyan $h \in R[x]$ polinom, hogy $f(x) = g(x)h(x)$. Jelölés: $g \mid f$ (vagy néha $g \mid_{R[x]} f$).

(2) a $g \in R[x]$ polinom **egység** $R[x]$-ben, ha minden $R[x]$-beli polinomnak osztója $R[x]$-ben.

Példák

$x + 1$ osztója $x^2 - 1$-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$, $\mathbb{Z}[x]$ mindegyikében.
2 osztója x-nek $\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$-ben, de $\mathbb{Z}[x]$-ben nem.
$\mathbb{C}[x]$, $\mathbb{R}[x]$, $\mathbb{Q}[x]$ egységei a nem nulla konstans polinomok.
$\mathbb{Z}[x]$ egységei csak az 1 és a -1.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához:

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak),

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis?

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x$

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x)$

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x) = (1/2)(2x)$.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x) = (1/2)(2x)$.
Ugyanígy $2 = 1 \cdot 2$,

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x) = (1/2)(2x)$.
Ugyanígy $2 = 1 \cdot 2$, de a 2 mégis felbonthatatlan szám.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x) = (1/2)(2x)$.
Ugyanígy $2 = 1 \cdot 2$, de a 2 mégis felbonthatatlan szám.

(2) $x^2 + 1 = (x + i)(x - i)$ valós fölött nem bontható föl.

Polinomok szorzatra bontása

Cél

Polinomok szorzatra bontása, ameddig csak lehetséges.
Hasonlít a számok szorzatra bontásához: $12 = 2 \cdot 2 \cdot 3$.
Itt 2 és 3 felbonthatatlan, azaz irreducibilis számok.

Definíció-kísérlet

Egy polinomot nevezzünk irreducibilisnek (felbonthatatlannak), ha nem lehet szorzatra bontani.

Problémák

(1) Az x irreducibilis? $x = 1 \cdot x = (-1)(-x) = (1/2)(2x)$.
Ugyanígy $2 = 1 \cdot 2$, de a 2 mégis felbonthatatlan szám.

(2) $x^2 + 1 = (x + i)(x - i)$ valós fölött nem bontható föl.
Akkor most $x^2 + 1$ irreducibilis-e, vagy sem?

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.

Az n szám triviális felbontása $n = ab$,

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az **egységek**: 1 és -1.
Az n szám **triviális felbontása** $n = ab$, ha a vagy b egység.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n$

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.

Az n szám triviális felbontása $n = ab$, ha a vagy b egység.

Vagyis $n = 1 \cdot n = n \cdot 1$

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.

Az n szám triviális felbontása $n = ab$, ha a vagy b egység.

Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n)$

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás,

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak. Mivel 2 nem egység, ezért a 2 felbonthatatlan.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak. Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám felírható felbonthatatlanok szorzataként.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak.
Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám felírható felbonthatatlanok szorzataként.
Ez egyértelmű, ha eltekintünk.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak. Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám felírható felbonthatatlanok szorzataként. Ez egyértelmű, ha a sorrendtől eltekintünk.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak.
Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám felírható felbonthatatlanok szorzataként.
Ez egyértelmű, ha a sorrendtől és egységszerestől eltekintünk.

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak.
Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám felírható felbonthatatlanok szorzataként.
Ez egyértelmű, ha a sorrendtől és egységszerestől eltekintünk.
A bizonyítás fő eszköze:

Felbonthatatlan számok

Emlékeztető számelméletből

Az egész számok között az egységek: 1 és -1.
Az n szám triviális felbontása $n = ab$, ha a vagy b egység.
Vagyis $n = 1 \cdot n = n \cdot 1 = (-1)(-n) = (-n)(-1)$.
Az n szám felbonthatatlan, ha nincs nemtriviális felbontása.
A felbonthatatlanok közül kizárjuk az egységeket.

Példa: A $6 = 2 \cdot 3$ nemtriviális felbontás, mert 2 és 3 nem egység. Ezért a 6 nem felbonthatatlan.
Példa: A 2 számnak csak triviális felbontásai vannak. Mivel 2 nem egység, ezért a 2 felbonthatatlan.

A számelmélet alaptétele: minden nullától és egységtől különböző szám felírható felbonthatatlanok szorzataként.
Ez egyértelmű, ha a sorrendtől és egységszerestől eltekintünk.
A bizonyítás fő eszköze: a kitüntetett közös osztó.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, $\mathbb{Z}$ egyike.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$),

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.

Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött),

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása,

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása, és nem egység.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása, és nem egység.
Reducibilis azt jelenti: nem egység és nem irreducibilis.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása, és nem egység.
Reducibilis azt jelenti: nem egység és nem irreducibilis.

A számelmélet alaptétele polinomokra

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása, és nem egység.
Reducibilis azt jelenti: nem egység és nem irreducibilis.

A számelmélet alaptétele polinomokra

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike.
Minden nullától és egységtől különböző $R[x]$-beli polinom felírható $R[x]$-beli irreducibilisek szorzataként.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása, és nem egység.
Reducibilis azt jelenti: nem egység és nem irreducibilis.

A számelmélet alaptétele polinomokra

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike.
Minden nullától és egységtől különböző $R[x]$-beli polinom felírható $R[x]$-beli irreducibilisek szorzataként.
Ez egyértelmű, ha a sorrendtől és egységszerestől eltekintünk.

Irreducibilis polinomok

Definíció

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike. Azt mondjuk, hogy az $f \in R[x]$ polinom $f = gh$ felbontása triviális ($g, h \in R[x]$), ha g és h valamelyike egység $R[x]$-ben.
Az $f \in R[x]$ polinom irreducibilis $R[x]$-ben (R fölött), ha nincs nemtriviális felbontása, és nem egység.
Reducibilis azt jelenti: nem egység és nem irreducibilis.

A számelmélet alaptétele polinomokra

Legyen R a $\mathbb{C}, \mathbb{R}, \mathbb{Q}, \mathbb{Z}$ egyike.
Minden nullától és egységtől különböző $R[x]$-beli polinom felírható $R[x]$-beli irreducibilisek szorzataként.
Ez egyértelmű, ha a sorrendtől és egységszerestől eltekintünk.

Lásd Kiss-jegyzet, 3.2.10. Tétel, és 3.4.10. Tétel.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

Példák felbontásra

Példa

Az $f(x) = 6(x^2-2)(x^2+1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:
$\mathbb{C}[x]$-ben 4 tényező:

$$(6x-6\sqrt{2}) \cdot (x+\sqrt{2}) \cdot (x+i) \cdot (x-i)$$

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:
$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött,

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:
$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:
$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

$$(6x^2 - 12) \cdot (x^2 + 1)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

$$(6x^2 - 12) \cdot (x^2 + 1)$$

$\mathbb{Z}[x]$-ben 4 tényező:

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

$$(6x^2 - 12) \cdot (x^2 + 1)$$

$\mathbb{Z}[x]$-ben 4 tényező:

$$2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

$$(6x^2 - 12) \cdot (x^2 + 1)$$

$\mathbb{Z}[x]$-ben 4 tényező:

$$2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.
A $\mathbb{Z}[x]$-ben 6 nem egység,

Példák felbontásra

Példa

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontásai:

$\mathbb{C}[x]$-ben 4 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x + i) \cdot (x - i)$$

$\mathbb{R}[x]$-ben 3 tényező:

$$(6x - 6\sqrt{2}) \cdot (x + \sqrt{2}) \cdot (x^2 + 1)$$

$\mathbb{Q}[x]$-ben 2 tényező:

$$(6x^2 - 12) \cdot (x^2 + 1)$$

$\mathbb{Z}[x]$-ben 4 tényező:

$$2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$$

Tanulság

A 6 nem lehet külön tényező $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött, mert egység.
A $\mathbb{Z}[x]$-ben 6 nem egység, sőt 2, 3 itt irreducibilis polinomok.

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság:

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú:

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság:
$(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú:
ha $f \mid gh$,

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság:
$(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú:
ha $f \mid gh$, akkor $f \mid g$

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság:
$(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú:
ha $f \mid gh$, akkor $f \mid g$ vagy $f \mid h$.

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú: ha $f \mid gh$, akkor $f \mid g$ vagy $f \mid h$.

(4) Ebből következik az alaptétel egyértelműségi állítása (ugyanúgy, mint egész számokra).

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú: ha $f \mid gh$, akkor $f \mid g$ vagy $f \mid h$.

(4) Ebből következik az alaptétel egyértelműségi állítása (ugyanúgy, mint egész számokra).

(5) A felbontás létezése fokszám szerinti indukcióval.

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú: ha $f \mid gh$, akkor $f \mid g$ vagy $f \mid h$.

(4) Ebből következik az alaptétel egyértelműségi állítása (ugyanúgy, mint egész számokra).

(5) A felbontás létezése fokszám szerinti indukcióval.

A $\mathbb{Z}[x]$-beli alaptételt a $\mathbb{Q}[x]$-beli alaptételre vezetjük vissza

Az alaptétel bizonyítása

Az alaptétel bizonyítása

$\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ fölött ugyanúgy, mint egész számokra:

(1) Az euklideszi algoritmus miatt bármely két polinomnak van kitüntetett közös osztója.

(2) Erre teljesül a kiemelési tulajdonság: $(fg, fh) = f(g, h)$ (lásd Kiss-jegyzet, 3.1.22. Tétel).

(3) Emiatt minden irreducibilis f polinom prímtulajdonságú: ha $f \mid gh$, akkor $f \mid g$ vagy $f \mid h$.

(4) Ebből következik az alaptétel egyértelműségi állítása (ugyanúgy, mint egész számokra).

(5) A felbontás létezése fokszám szerinti indukcióval.

A $\mathbb{Z}[x]$-beli alaptételt a $\mathbb{Q}[x]$-beli alaptételre vezetjük vissza (Kiss-jegyzet, 2.4. Szakasz).

Gyökök és irreducibilitás

Tétel (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

Gyökök és irreducibilitás

Tétel (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

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

Gyökök és irreducibilitás

Tétel (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

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

Gyökök és irreducibilitás

Tétel (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}, \mathbb{R}, \mathbb{Q}$ egyike.

(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 (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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.

Gyökök és irreducibilitás

Tétel (Kiss-jegyzet, 3.3. Szakasz)

Legyen T a $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$ egyike.

(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.

Ezek közül csak (4) igaz $\mathbb{Z}[x]$-ben!

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $\quad \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú,

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.
Ez a felbontás triviális kell legyen,

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.
Ez a felbontás triviális kell legyen, és ezért h egység.

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.
Ez a felbontás triviális kell legyen, és ezért h egység.
Tehát f tényleg elsőfokú. $\square$

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.
Ez a felbontás triviális kell legyen, és ezért h egység.
Tehát f tényleg elsőfokú. $\square$

Egy komplex együtthatós polinom irreducibilisekre való felbontását úgy kapjuk,

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.
Ez a felbontás triviális kell legyen, és ezért h egység.
Tehát f tényleg elsőfokú. $\square$

Egy komplex együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk,

Irreducibilitás $\mathbb{C}[x]$-ben

Tétel

A $\mathbb{C}[x]$ irreducibilis polinomjai pontosan az elsőfokúak.

Bizonyítás

Ha f elsőfokú, és $f = gh$, akkor $1 = \mathrm{gr}(f) = \mathrm{gr}(g) + \mathrm{gr}(h)$.
Ezért g és h egyike nulladfokú, és így egység.
Megfordítva: Ha f irreducibilis, akkor legalább elsőfokú.
Az algebra alaptétele miatt van f-nek egy $c \in \mathbb{C}$ gyöke.
Ekkor $f(x) = (x - c)h(x)$ alkalmas $h \in \mathbb{C}[x]$-re.
Ez a felbontás triviális kell legyen, és ezért h egység.
Tehát f tényleg elsőfokú. $\square$

Egy komplex együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk, és a főegyütthatót valamelyik tényezőhöz hozzácsapjuk.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak,

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x - c)(x - \overline{c})$ valós együtthatós,

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x-c)(x-\overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető,

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x-c)(x-\overline{c})$ valós együtthatós, és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x-c)(x-\overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.
Ezért ha f irreducibilis $\mathbb{R}$ fölött,

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x - c)(x - \overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.
Ezért ha f irreducibilis $\mathbb{R}$ fölött, akkor legfeljebb másodfokú.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x - c)(x - \overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.
Ezért ha f irreducibilis $\mathbb{R}$ fölött, akkor legfeljebb másodfokú.

Egy valós együtthatós polinom irreducibilisekre való felbontását úgy kapjuk,

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x-c)(x-\overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.
Ezért ha f irreducibilis $\mathbb{R}$ fölött, akkor legfeljebb másodfokú.

Egy valós együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk $\mathbb{C}$ fölött,

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x-c)(x-\overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.
Ezért ha f irreducibilis $\mathbb{R}$ fölött, akkor legfeljebb másodfokú.

Egy valós együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk $\mathbb{C}$ fölött, és mindegyik nem valós gyököt párosítjuk a komplex konjugáltjával.

Irreducibilitás $\mathbb{R}[x]$-ben

Tétel

Az $\mathbb{R}[x]$ irreducibilis polinomjai pontosan az elsőfokúak, továbbá azok a másodfokúak, melyeknek nincs valós gyöke.

Bizonyítás (vázlat)

Legyen $f \in \mathbb{R}[x]$ legalább elsőfokú polinom.
Az algebra alaptétele miatt ennek van egy c komplex gyöke.
Láttuk korábban: $(x-c)(x-\overline{c})$ valós együtthatós,
és $f(x)$-ből kiemelhető, ami $\mathbb{R}$ fölötti felbontást ad.
Ezért ha f irreducibilis $\mathbb{R}$ fölött, akkor legfeljebb másodfokú.

Egy valós együtthatós polinom irreducibilisekre való felbontását úgy kapjuk, hogy gyöktényezőkre bontjuk $\mathbb{C}$ fölött, és mindegyik nem valós gyököt párosítjuk a komplex konjugáltjával.
Példa: $x^4+4=(x^2+2x+2)(x^2-2x+2)$ (2.5.10. Gyakorlat).

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött ($p = 2$ jó).

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött ($p = 2$ jó).
A $p = 3$ nem jó:

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött ($p = 2$ jó).
A $p = 3$ nem jó: $3 \mid 21$.

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött ($p = 2$ jó).
A $p = 3$ nem jó: $3 \mid 21$. A $p = 5$ nem jó:

Irreducibilitás $\mathbb{Q}[x]$-ben

A $\mathbb{Q}[x]$ legfeljebb harmadfokú polinomjainak irreducibilitását eldönthetjük a racionális gyökteszt segítségével.

Általános módszert nem tanulunk, az alábbi néha működik.

Schönemann–Eisenstein-kritérium (3.5.3. Gyakorlat)

Legyen f egész együtthatós, nem konstans polinom.
HA van olyan p prímszám, amelyre

(1) p nem osztja f főegyütthatóját;

(2) p osztja f összes többi együtthatóját;

(3) p^2 nem osztja f konstans tagját,

AKKOR f irreducibilis $\mathbb{Q}$ fölött.

Példa: $21x^4 + 60x - 150$ irreducibilis $\mathbb{Q}$ fölött ($p = 2$ jó).
A $p = 3$ nem jó: $3 \mid 21$. A $p = 5$ nem jó: $5^2 \mid 150$.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött,

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött,

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x+1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7+(2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x+18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re. Azaz létezik $\mathbb{Q}$ fölött akárhányadfokú irreducibilis polinom.

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re. Azaz létezik $\mathbb{Q}$ fölött akárhányadfokú irreducibilis polinom.

(5) Fordított Schönemann–Eisenstein-kritérium:

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re. Azaz létezik $\mathbb{Q}$ fölött akárhányadfokú irreducibilis polinom.

(5) Fordított Schönemann–Eisenstein-kritérium: Ha a p prím osztja a polinom minden együtthatóját a konstans tag kivételével,

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re. Azaz létezik $\mathbb{Q}$ fölött akárhányadfokú irreducibilis polinom.

(5) Fordított Schönemann–Eisenstein-kritérium:
Ha a p prím osztja a polinom minden együtthatóját a konstans tag kivételével, és p^2 nem osztja a főegyütthatót,

A Schönemann–Eisenstein-kritérium tanulságai

Tanulságok

(1) Nem igaz a megfordítása. Példa: $x + 1$ irreducibilis $\mathbb{Q}$ fölött, de nem alkalmazható rá a kritérium.

(2) A nevezőkkel felszorozva racionális együtthatós polinomokra is alkalmazható lehet. Példa: $x^7 + (2/3)$.

(3) Csak $\mathbb{Q}$ fölötti, és nem $\mathbb{Z}$ fölötti irreducibilitást biztosít. Példa: $9x + 18$ irreducibilis $\mathbb{Q}$ fölött, de $\mathbb{Z}$ fölött nem.

(4) A kritérium miatt $x^n - 2$ irreducibilis minden $n \geq 1$-re. Azaz létezik $\mathbb{Q}$ fölött akárhányadfokú irreducibilis polinom.

(5) Fordított Schönemann–Eisenstein-kritérium: Ha a p prím osztja a polinom minden együtthatóját a konstans tag kivételével, és p^2 nem osztja a főegyütthatót, a polinom akkor is irreducibilis $\mathbb{Q}$ fölött.

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja,

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

$x^4 + 1$-re nem alkalmazható a Schönemann–Eisenstein.

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

x^4+1-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$,

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

$x^4 + 1$-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, erre már igen, $p = 2$-vel.

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja,
vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

x^4+1-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$, erre már igen, $p=2$-vel.
Tehát x^4+1 is irreducibilis $\mathbb{Q}$ fölött.

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

x^4+1-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$, erre már igen, $p=2$-vel.
Tehát x^4+1 is irreducibilis $\mathbb{Q}$ fölött.

Tétel (nehéz)

Mindegyik körosztási polinom irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

x^4+1-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4+1 = x^4+4x^3+6x^2+4x+2$, erre már igen, $p=2$-vel.
Tehát x^4+1 is irreducibilis $\mathbb{Q}$ fölött.

Tétel (nehéz)

Mindegyik körosztási polinom irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Létezik algoritmus az irreducibilitás eldöntésére $\mathbb{Q}$ fölött,

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

$x^4 + 1$-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, erre már igen, $p = 2$-vel.
Tehát $x^4 + 1$ is irreducibilis $\mathbb{Q}$ fölött.

Tétel (nehéz)

Mindegyik körosztási polinom irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Létezik algoritmus az irreducibilitás eldöntésére $\mathbb{Q}$ fölött, például interpoláció segítségével.

További módszerek $\mathbb{Q}$ fölött

Állítás

$f \in \mathbb{Q}[x]$ irreducibilis $\mathbb{Q}$ fölött, ha alkalmas eltoltja, vagyis az $f(x+c)$ polinom irreducibilis $\mathbb{Q}$ fölött ($c \in \mathbb{Q}$).

Példa

$x^4 + 1$-re nem alkalmazható a Schönemann–Eisenstein.
$(x+1)^4 + 1 = x^4 + 4x^3 + 6x^2 + 4x + 2$, erre már igen, $p = 2$-vel.
Tehát $x^4 + 1$ is irreducibilis $\mathbb{Q}$ fölött.

Tétel (nehéz)

Mindegyik körosztási polinom irreducibilis $\mathbb{Q}$ és $\mathbb{Z}$ fölött.

Létezik algoritmus az irreducibilitás eldöntésére $\mathbb{Q}$ fölött, például interpoláció segítségével. Van hatékony algoritmus is.

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős:

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás

Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom,

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás

Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom, és egy egész szám szorzataként.

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás

Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom, és egy egész szám szorzataként.

Példa: $60x^6 + 36x^4 + 90 =$

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás

Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom, és egy egész szám szorzataként.

Példa: $60x^6 + 36x^4 + 90 = 6(10x^6 + 6x^4 + 15)$.

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás

Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom, és egy egész szám szorzataként.

Példa: $60x^6 + 36x^4 + 90 = 6(10x^6 + 6x^4 + 15)$.
Nyilván $(10, 6, 15) = 1$

Primitív polinomok

Emlékeztető

Az $f(x) = 6(x^2 - 2)(x^2 + 1) \in \mathbb{Z}[x]$ alaptétel szerinti felbontása $\mathbb{Z}[x]$-ben 4 tényezős: $2 \cdot 3 \cdot (x^2 - 2) \cdot (x^2 + 1)$.

Kiemeltük az együtthatók legnagyobb közös osztóját.

Definíció

Primitív polinom: együtthatóinak legnagyobb közös osztója 1.

Állítás

Minden egész együtthatós polinom egyértelműen fölírható egy primitív polinom, és egy egész szám szorzataként.

Példa: $60x^6 + 36x^4 + 90 = 6(10x^6 + 6x^4 + 15)$.
Nyilván $(10, 6, 15) = 1$ (de nem páronként relatív prímek).

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját:

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját: $f(x) = ng(x)$,

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját: $f(x) = ng(x)$, ahol g már primitív polinom;

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját: $f(x) = ng(x)$, ahol g már primitív polinom;

(2) Az n számot $\mathbb{Z}$-ben prímek szorzatára bontjuk;

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját: $f(x) = ng(x)$, ahol g már primitív polinom;

(2) Az n számot $\mathbb{Z}$-ben prímek szorzatára bontjuk;

(3) A g polinomot $\mathbb{Q}[x]$-ben bontjuk irreducibilisek szorzatára.

Irreducibilitás $\mathbb{Z}[x]$-ben

Tétel (Kiss-jegyzet, 3.4.8. Tétel)

Egy $f \in \mathbb{Z}[x]$ polinom pontosan akkor irreducibilis $\mathbb{Z}$ fölött, ha

(1) vagy egy $\mathbb{Z}$-beli prímszám (mint konstans polinom),

(2) vagy egy primitív polinom, amely $\mathbb{Q}$ fölött irreducibilis.

Az $f \in \mathbb{Z}[x]$ polinomot a következőképpen bonthatjuk $\mathbb{Z}$ fölött irreducibilisek szorzatára:

(1) Kiemeljük az együtthatóinak a legnagyobb közös osztóját: $f(x) = ng(x)$, ahol g már primitív polinom;

(2) Az n számot $\mathbb{Z}$-ben prímek szorzatára bontjuk;

(3) A g polinomot $\mathbb{Q}[x]$-ben bontjuk irreducibilisek szorzatára.

Meg lehet mutatni, hogy g felbontása is „lényegében” egész együtthatós polinomokra történik (II. Gauss-lemma, 3.4.7).