Klasszikus algebra előadás

Waldhauser Tamás
2013 április 11.

4. Test feletti egyhatározatlanú polinomok

Eddig a polinomokkal mint formális kifejezésekkel számoltunk, nem éltünk azzal a lehetőséggel, hogy x helyébe az alaptest (vagy -gyűrű) elemeit be lehet helyettesíteni. Mostantól viszont a polinomokat függvényeknek (is) tekintjük. Ebben a fejezetben T mindig tetszőleges testet jelöl.

4. Test feletti egyhatározatlanú polinomok

Eddig a polinomokkal mint formális kifejezésekkel számoltunk, nem éltünk azzal a lehetőséggel, hogy x helyébe az alaptest (vagy -gyűrű) elemeit be lehet helyettesíteni. Mostantól viszont a polinomokat függvényeknek (is) tekintjük. Ebben a fejezetben T mindig tetszőleges testet jelöl.

4.1. Definíció

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett **helyettesítési érték**én az $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in T$ elemet értjük.

4. Test feletti egyhatározatlanú polinomok

Eddig a polinomokkal mint formális kifejezésekkel számoltunk, nem éltünk azzal a lehetőséggel, hogy x helyébe az alaptest (vagy -gyűrű) elemeit be lehet helyettesíteni. Mostantól viszont a polinomokat függvényeknek (is) tekintjük. Ebben a fejezetben T mindig tetszőleges testet jelöl.

4.1. Definíció

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett **helyettesítési érték**én az $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in T$ elemet értjük.

Az $f \in T[x]$ polinomhoz tartozó **polinomfüggvény** pedig nem más, mint az

$$f\colon T \to T,\ c \mapsto f(c)$$

leképezés.

4. Test feletti egyhatározatlanú polinomok

Eddig a polinomokkal mint formális kifejezésekkel számoltunk, nem éltünk azzal a lehetőséggel, hogy x helyébe az alaptest (vagy -gyűrű) elemeit be lehet helyettesíteni. Mostantól viszont a polinomokat függvényeknek (is) tekintjük. Ebben a fejezetben T mindig tetszőleges testet jelöl.

4.1. Definíció

Az $f = a_n x^n + \cdots + a_1 x + a_0 \in T[x]$ polinom $c \in T$ helyen vett **helyettesítési érték**én az $f(c) = a_n c^n + \cdots + a_1 c + a_0 \in T$ elemet értjük.

Az $f \in T[x]$ polinomhoz tartozó **polinomfüggvény** pedig nem más, mint az

$$f \colon T \to T,\ c \mapsto f(c)$$

leképezés.

A polinomot és a hozzá tartozó polinomfüggvényt ugyanúgy jelöljük; a szövegkörnyezetből kiderül, hogy mikor melyikről van szó. Ha polinomfüggvényekről van szó, akkor x-et **változó**nak nevezzük (nem pedig határozatlannak).

Példa

Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

Példa

Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

Példa

Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

Példa

Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

Látjuk, hogy f-hez és g-hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha f és g két különböző polinom.

Példa

Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

Látjuk, hogy f-hez és g-hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha f és g két különböző polinom. Ezért nagyon fontos, hogy

Példa

Az $f = x^3 \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0}^3 = \overline{0},\ \overline{1} \mapsto \overline{1}^3 = \overline{1},\ \overline{2} \mapsto \overline{2}^3 = \overline{2}.$$

A $g = x \in \mathbb{Z}_3[x]$ polinomhoz tartozó polinomfüggvény:

$$\mathbb{Z}_3 \to \mathbb{Z}_3,\ \overline{0} \mapsto \overline{0},\ \overline{1} \mapsto \overline{1},\ \overline{2} \mapsto \overline{2}.$$

Látjuk, hogy f-hez és g-hez ugyanaz a polinomfüggvény tartozik (nevezetesen az identikus függvény), noha f és g két különböző polinom. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma 

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma  q^q,

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma  q^q, míg
- T feletti polinomból 

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma  q^q, míg
- T feletti polinomból  végtelen sok van,

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma  q^q, míg
- T feletti polinomból  végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény.

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma  q^q, míg
- T feletti polinomból  végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény. Ezért nagyon fontos, hogy

Általánosabban, ha T egy q-elemű test, akkor

- a $T \longrightarrow T$ leképezések száma  q^q, míg
- T feletti polinomból  végtelen sok van,

így végtelen sok különböző polinomhoz tartozik ugyanaz a polinomfüggvény. Ezért nagyon fontos, hogy

NE KEVERJÜK A POLINOMOT A POLINOMFÜGGVÉNNYEL!!!

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom.

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom. Értékeljük ki az $x = \alpha$ helyen a fenti egyenlőség mindkét oldalát:

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + r$$

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom. Értékeljük ki az $x = \alpha$ helyen a fenti egyenlőség mindkét oldalát:

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r.$$

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom. Értékeljük ki az $x = \alpha$ helyen a fenti egyenlőség mindkét oldalát:

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r.$$

Tehát

$$x - \alpha \mid f \iff r = 0$$

4.3. Definíció

Az $\alpha \in T$ elem **gyök**e (más szóval **zérushely**e) az $f \in T[x]$ polinomnak, ha $f(\alpha) = 0$.

4.4. Tétel (Bézout tétele)

Bármely $f \in T[x]$ és $\alpha \in T$ esetén $f(\alpha) = 0 \iff x - \alpha \mid f$.

Bizonyítás.

Osszuk el f-et $(x - \alpha)$-val maradékosan:

$$f = q(x - \alpha) + r, \text{ ahol } q, r \in T[x] \text{ és } \deg r < \deg(x - \alpha) = 1.$$

Vegyük észre, hogy itt r konstans polinom. Értékeljük ki az $x = \alpha$ helyen a fenti egyenlőség mindkét oldalát:

$$f(\alpha) = q(\alpha)(\alpha - \alpha) + r = r.$$

Tehát

$$x - \alpha \mid f \iff r = 0 \iff f(\alpha) = 0.$$

□

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\text{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \text{lnko}(f, g)$.

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} \iff f(\alpha) = 0 \text{ és } g(\alpha) = 0$$

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\begin{aligned} \alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\ &\iff x - \alpha \mid f \text{ és } x - \alpha \mid g \end{aligned}$$

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\begin{aligned} \alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\ &\iff x - \alpha \mid f \text{ és } x - \alpha \mid g \end{aligned}$$

 (Bézout)

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\begin{aligned} \alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\ &\iff x - \alpha \mid f \text{ és } x - \alpha \mid g \\ &\iff x - \alpha \mid d \end{aligned}$$

(Bézout)

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$\begin{aligned}
\alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\
&\iff x - \alpha \mid f \text{ és } x - \alpha \mid g \qquad \text{(Bézout)} \\
&\iff x - \alpha \mid d \qquad \text{(lnko def.)}
\end{aligned}$$

4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$
\begin{aligned}
\alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\
&\iff x - \alpha \mid f \text{ és } x - \alpha \mid g \qquad \text{(Bézout)} \\
&\iff x - \alpha \mid d \qquad \text{(lnko def.)} \\
&\iff d(\alpha) = 0.
\end{aligned}
$$



4.5. Következmény

Tetszőleges $f, g \in T[x]$ polinomok esetén f és g közös gyökei ugyanazok, mint $\operatorname{lnko}(f, g)$ gyökei.

Bizonyítás.

Legyen $d = \operatorname{lnko}(f, g)$. Tetszőleges $\alpha \in T$ esetén

$$
\begin{aligned}
\alpha \text{ közös gyöke } f\text{-nek és } g\text{-nek} &\iff f(\alpha) = 0 \text{ és } g(\alpha) = 0 \\
&\iff x - \alpha \mid f \text{ és } x - \alpha \mid g && \text{(Bézout)} \\
&\iff x - \alpha \mid d && \text{(Inko def.)} \\
&\iff d(\alpha) = 0. && \text{(tuozéB)}
\end{aligned}
$$

□

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f$ (Bézout)

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f \qquad \text{(Bézout)}$$

$$\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \qquad \text{(miért?)}$$

□

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f \qquad \text{(Bézout)}$$

$$\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \qquad \text{(miért?)}$$

□

4.7. Következmény

Ha az $f \in T[x]$ polinom fokszáma n, akkor legfeljebb n különböző gyöke van a T testben.

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f \qquad \text{(Bézout)}$$

$$\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \qquad \text{(miért?)}$$

□

4.7. Következmény

Ha az $f \in T[x]$ polinom fokszáma n, akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás.

Legyenek $\alpha_1, \ldots, \alpha_k \in T$ az f polinom összes különböző gyökei.

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f \qquad \text{(Bézout)}$$

$$\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \qquad \text{(miért?)}$$

□

4.7. Következmény

Ha az $f \in T[x]$ polinom fokszáma n, akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás.

Legyenek $\alpha_1, \ldots, \alpha_k \in T$ az f polinom összes különböző gyökei. Ekkor

$$(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f$$

4.6. Következmény

Ha $\alpha_1, \ldots, \alpha_k \in T$ páronként különböző elemek és $f \in T[x]$, akkor

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f.$$

Bizonyítás.

$$f(\alpha_1) = \ldots = f(\alpha_k) = 0 \iff x - \alpha_1, \ldots, x - \alpha_k \mid f \qquad \text{(Bézout)}$$

$$\iff (x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \qquad \text{(miért?)}$$

□

4.7. Következmény

Ha az $f \in T[x]$ polinom fokszáma n, akkor legfeljebb n különböző gyöke van a T testben.

Bizonyítás.

Legyenek $\alpha_1, \ldots, \alpha_k \in T$ az f polinom összes különböző gyökei. Ekkor

$$(x - \alpha_1) \cdot \ldots \cdot (x - \alpha_k) \mid f \implies k \leq \deg f = n.$$

□

Adósságrendezés

A Bevezetés a számelméletbe előadáson bizonyítás nélkül szerepelt az alábbi állítás.

4.9. Lemma

Ha p prímszám, akkor az $x^d \equiv 1 \pmod{p}$ kongruenciának legföljebb d megoldása lehet modulo p.

Adósságrendezés

A Bevezetés a számelméletbe előadáson bizonyítás nélkül szerepelt az alábbi állítás.

4.9. Lemma

Ha p prímszám, akkor az $x^d \equiv 1 \pmod{p}$ kongruenciának legföljebb d megoldása lehet modulo p.

Bizonyítás.

Ha p prímszám, akkor $\mathbb{Z}_p$ test, így az $x^d - \overline{1} \in \mathbb{Z}_p[x]$ polinomnak legföljebb d gyöke lehet. □

Adósságrendezés

A Bevezetés a számelméletbe előadáson bizonyítás nélkül szerepelt az alábbi állítás.

4.9. Lemma

Ha p prímszám, akkor az $x^d \equiv 1 \pmod{p}$ kongruenciának legföljebb d megoldása lehet modulo p.

Bizonyítás.

Ha p prímszám, akkor $\mathbb{Z}_p$ test, így az $x^d - \overline{1} \in \mathbb{Z}_p[x]$ polinomnak legföljebb d gyöke lehet. □

Példa

Az $x^2 - \overline{1} \in \mathbb{Z}_{12}[x]$ polinomnak négy gyöke is van! 

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem **k-szoros gyök**e, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem
k-szoros gyöke, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.9. Megjegyzés

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem
k-szoros gyöke, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.9. Megjegyzés

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

Példa

Hányszoros gyöke a 2 az $f = x^5 - 4x^4 - 3x^3 + 34x^2 - 52x + 24$ polinomnak?

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem
k-szoros gyöke, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.9. Megjegyzés

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

Példa

Hányszoros gyöke a 2 az $f = x^5 - 4x^4 - 3x^3 + 34x^2 - 52x + 24$ polinomnak?

$$f = (x-2)\left(x^4 - 2x^3 - 7x^2 + 20x - 12\right)$$

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem
k-szoros gyöke, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.9. Megjegyzés

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

Példa

Hányszoros gyöke a 2 az $f = x^5 - 4x^4 - 3x^3 + 34x^2 - 52x + 24$ polinomnak?

$$\begin{aligned} f &= (x-2)\left(x^4 - 2x^3 - 7x^2 + 20x - 12\right) = \\ &= (x-2)^2\left(x^3 - 7x + 6\right) \end{aligned}$$

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem
k-szoros gyöke, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.9. Megjegyzés

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

Példa

Hányszoros gyöke a 2 az $f = x^5 - 4x^4 - 3x^3 + 34x^2 - 52x + 24$ polinomnak?

$$\begin{aligned} f &= (x-2)\left(x^4 - 2x^3 - 7x^2 + 20x - 12\right) = \\ &= (x-2)^2\left(x^3 - 7x + 6\right) = \\ &= (x-2)^3 \underbrace{(x^2 + 2x - 3)}_{\text{nem gyöke a 2}} \end{aligned}$$

4.8. Definíció

Azt mondjuk, hogy az $f \in T[x]$ polinomnak az $\alpha \in T$ elem
k-szoros gyöke, ha

$$(x-\alpha)^k \mid f, \quad \text{de} \quad (x-\alpha)^{k+1} \nmid f.$$

A k számot az α gyök **multiplicitás**ának nevezzük.

4.9. Megjegyzés

Megengedjük a $k = 0$ esetet is: α pontosan akkor nullaszoros gyök, ha nem gyök.

Példa

Hányszoros gyöke a 2 az $f = x^5 - 4x^4 - 3x^3 + 34x^2 - 52x + 24$ polinomnak?

$$\begin{aligned} f &= (x-2)\left(x^4 - 2x^3 - 7x^2 + 20x - 12\right) = \\ &= (x-2)^2\left(x^3 - 7x + 6\right) = \\ &= (x-2)^3 \underbrace{\left(x^2 + 2x - 3\right)}_{\text{nem gyöke a 2}} \implies \text{háromszoros gyök} \end{aligned}$$

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$ 

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol 

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

4.10. Állítás

Az elsőfokú polinomok bármely test felett irreducibilisek.

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

4.10. Állítás

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f =$  $\cdot$  , akkor $\deg$  $+ \deg$  $= 1$

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

4.10. Állítás

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f =$  $\cdot$  , akkor $\deg$  $+ \deg$  $= 1$, és így

$$\deg \text{  } = 1, \deg \text{  } = 0 \text{ vagy } \deg \text{  } = 0, \deg \text{  } = 1.$$

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

4.10. Állítás

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f =$  $\cdot$  , akkor $\deg$  $+ \deg$  $= 1$, és így

$$\deg \text{  } = 1, \deg \text{  } = 0 \text{ vagy } \deg \text{  } = 0, \deg \text{  } = 1.$$

Mindkét esetben triviális a felbontás. □

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

4.10. Állítás

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f =$  $\cdot$  , akkor $\deg$  $+ \deg$  $= 1$, és így

$$\deg \text{  } = 1, \deg \text{  } = 0 \text{ vagy } \deg \text{  } = 0, \deg \text{  } = 1.$$

Mindkét esetben triviális a felbontás. □

4.11. Tétel

Ha $f \in T[x]$ irreducibilis és $\deg f \geq 2$, akkor f-nek nincs gyöke.

Mikor irreducibilis egy f polinom a T test felett?

- $f \nsim 0, 1 \iff$  $\deg f \geq 1$
- triviális felbontás: $f =$  $\cdot$  , ahol  $\deg$  $= 0, \deg$  $= \deg f$ (vagy fordítva)
- nemtriviális felbontás: $f =$  $\cdot$  , ahol $1 \leq \deg$  , $\deg$  $< \deg f$

4.10. Állítás

Az elsőfokú polinomok bármely test felett irreducibilisek.

Bizonyítás.

Ha $f =$  $\cdot$  , akkor $\deg$  $+ \deg$  $= 1$, és így

$$\deg \text{  } = 1, \deg \text{  } = 0 \text{ vagy } \deg \text{  } = 0, \deg \text{  } = 1.$$

Mindkét esetben triviális a felbontás. □

4.11. Tétel

Ha $f \in T[x]$ irreducibilis és $\deg f \geq 2$, akkor f-nek nincs gyöke.

Bizonyítás.

Ha α gyöke f-nek, akkor $f = (x - \alpha)(\cdots)$ nemtriviális felbontás. □

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = \text{  } \cdot \text{  }$, akkor $\deg \text{  } + \deg \text{  } = 2, 3$

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = \text{  } \cdot \text{  }$, akkor $\deg \text{} + \deg \text{} = 2, 3$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg$ 	$\deg$ 
2	1	1
3	2	1
3	1	2

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = \text{  } \cdot \text{  }$, akkor $\deg \text{  } + \deg \text{  } = 2, 3$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg$ 	$\deg$ 
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója.

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = \text{  } \cdot \text{  }$, akkor $\deg \text{  } + \deg \text{  } = 2, 3$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg$ 	$\deg$ 
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója. Egy elsőfokú polinom asszociáltság erejéig mindig $x - \alpha$ alakban írható*

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = \text{  } \cdot \text{  }$, akkor $\deg \text{} + \deg \text{} = 2, 3$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg$ 	$\deg$ 
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója. Egy elsőfokú polinom asszociáltság erejéig mindig $x - \alpha$ alakban írható*, ez pedig akkor és csak akkor osztja f-et, ha α gyöke f-nek.

4.12. Tétel

Ha $f \in T[x]$ és $2 \leq \deg f \leq 3$, akkor f pontosan akkor irreducibilis, ha nincs gyöke.

Bizonyítás.

Ha $f = \text{  } \cdot \text{  }$, akkor $\deg \text{} + \deg \text{} = 2, 3$, így a nemtriviális felbontásokra a következő lehetőségek vannak:

$\deg f$	$\deg$ 	$\deg$ 
2	1	1
3	2	1
3	1	2

Tehát f akkor és csak akkor nem irreducibilis, ha van elsőfokú osztója. Egy elsőfokú polinom asszociáltság erejéig mindig $x - \alpha$ alakban írható*, ez pedig akkor és csak akkor osztja f-et, ha α gyöke f-nek.

□

*$ax + b = a\left(x + \frac{b}{a}\right) \sim x + \frac{b}{a} = x - \left(-\frac{b}{a}\right) = x - \alpha$

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra.

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz:

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!
A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra,

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!
A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!
A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Példa

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!
A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Példa

Az $f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ polinomnak nincs valós gyöke, mégsem irreducibilis $\mathbb{R}$ felett:

Összefoglalva:
Az

$$\text{irreducibilis} \implies \text{nincs gyöke}$$

impikáció igaz a legalább másodfokú polinomokra. Elsőfokúakra nem igaz: azok mindig irreducibilisek és mindig van gyökük!
A

$$\text{nincs gyöke} \implies \text{irreducibilis}$$

implikáció igaz a másod- és harmadfokú polinomokra, de magasabbfokúakra nem!

Példa

Az $f = x^4 + 2x^2 + 1 \in \mathbb{R}[x]$ polinomnak nincs valós gyöke, mégsem irreducibilis $\mathbb{R}$ felett:

$$f = \left(x^2 + 1\right)\left(x^2 + 1\right).$$

Legalább negyedfokú polinomok esetén

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

Legalább negyedfokú polinomok esetén

A GYÖKNÉLKÜLISÉGBŐL

NEM

KÖVETKEZIK

AZ IRREDUCIBILITÁS!!!

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik: 

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik: 

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik:  $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik:  $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

(És persze $\mathbb{C}[x]$-ben is felbomlik.)

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik:  $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

(És persze $\mathbb{C}[x]$-ben is felbomlik.)

Általában, minél nagyobb az alaptest, annál „több esélye” van egy polinomnak felbomlani.

Ha T részteste K-nak és $f \in T[x]$, akkor

Példa

Az $f = x^2 + 1 \in \mathbb{R}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{C}[x]$-ben már felbomlik:  $x^2 + 1 = (x + i)(x - i)$.

Példa

Az $f = x^2 - 2 \in \mathbb{Q}[x]$ polinom irreducibilis, de ugyanez a polinom $\mathbb{R}[x]$-ben már felbomlik:  $x^2 - 2 = \left(x - \sqrt{2}\right)\left(x + \sqrt{2}\right)$.

(És persze $\mathbb{C}[x]$-ben is felbomlik.)

Általában, minél nagyobb az alaptest, annál „több esélye” van egy polinomnak felbomlani.

Ha T részteste K-nak és $f \in T[x]$, akkor

$$f \text{ irreducibilis } K \text{ felett } \begin{array}{c} \Rightarrow \\ \not\Leftarrow \end{array} \quad f \text{ irreducibilis } T \text{ felett.}$$

Irreducibilis polinomok a komplex számtest felett

4.13. Tétel* (az algebra alaptétele)

Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

Irreducibilis polinomok a komplex számtest felett

4.13. Tétel* (az algebra alaptétele)

Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

4.14. Következmény

A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

Irreducibilis polinomok a komplex számtest felett

4.13. Tétel* (az algebra alaptétele)

Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

4.14. Következmény

A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

Bizonyítás.

Tudjuk, hogy az elsőfokúak bármely test felett irreducibilisek.

Irreducibilis polinomok a komplex számtest felett

4.13. Tétel* (az algebra alaptétele)

Minden legalább elsőfokú komplex együtthatós polinomnak van gyöke a komplex számok testében.

4.14. Következmény

A komplex számok teste felett pontosan az elsőfokú polinomok irreducibilisek.

Bizonyítás.

Tudjuk, hogy az elsőfokúak bármely test felett irreducibilisek.
Ha $f \in \mathbb{C}[x]$ legalább másodfokú, akkor az algebra alaptétele szerint van valódi (pl. elsőfokú) osztója. $\square$

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY $\Longrightarrow$ FIGY

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY $\Longrightarrow$ FIGY $\Longrightarrow$ GAGY

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY $\Longrightarrow$ FIGY $\Longrightarrow$ GAGY $\Longrightarrow$ minden $\mathbb{C}$ feletti legalább elsőfokú polinom irreducibilisek, azaz elsőfokúak szorzatára bomlik.

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY $\Longrightarrow$ FIGY $\Longrightarrow$ GAGY $\Longrightarrow$ minden $\mathbb{C}$ feletti legalább elsőfokú polinom irreducibilisek, azaz elsőfokúak szorzatára bomlik. Ezek az elsőfokúak asszociáltság erejéig $x - \alpha$ alakúak.

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY $\Longrightarrow$ FIGY $\Longrightarrow$ GAGY $\Longrightarrow$ minden $\mathbb{C}$ feletti legalább elsőfokú polinom irreducibilisek, azaz elsőfokúak szorzatára bomlik. Ezek az elsőfokúak asszociáltság erejéig $x - \alpha$ alakúak. Tehát $f \in \mathbb{C}[x]$ irreducibilis faktorizációja így fest:

$$f \sim (x - \alpha_1) \cdots (x - \alpha_n).$$

4.15. Következmény

Minden legalább elsőfokú komplex együtthatós polinom elsőfokú polinomok szorzatára bomlik. Ha $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{C}[x]$ $(n \geq 1, a_n \neq 0)$, akkor f-nek multiplicitással számolva pontosan n gyöke van. Ha ezek a gyökök $\alpha_1, \ldots, \alpha_n$ (mindegyiket annyiszor feltüntetve, amennyi a multiplicitása), akkor $f = a_n (x - \alpha_1) \cdots (x - \alpha_n)$. Ezt nevezzük a polinom **gyöktényezős felbontás**ának.

Bizonyítás.

$\mathbb{C}[x]$ EUGY $\Longrightarrow$ FIGY $\Longrightarrow$ GAGY $\Longrightarrow$ minden $\mathbb{C}$ feletti legalább elsőfokú polinom irreducibilisek, azaz elsőfokúak szorzatára bomlik. Ezek az elsőfokúak asszociáltság erejéig $x - \alpha$ alakúak. Tehát $f \in \mathbb{C}[x]$ irreducibilis faktorizációja így fest:

$$f \sim (x - \alpha_1) \cdots (x - \alpha_n).$$

Világos, hogy ekkor f gyökei éppen az $\alpha_1, \ldots, \alpha_n$ komplex számok. □

4.16. Következmény

Bármely $f, g \in \mathbb{C}[x]$ esetén $f \mid g$ akkor és csak akkor teljesül, ha f minden gyöke egyúttal gyöke g-nek is, mégpedig legalább akkora multiplicitással, mint f-nek.

4.16. Következmény

Bármely $f, g \in \mathbb{C}[x]$ esetén $f \mid g$ akkor és csak akkor teljesül, ha f minden gyöke egyúttal gyöke g-nek is, mégpedig legalább akkora multiplicitással, mint f-nek.

Bizonyítás.

Használjuk a 3.51. Tételt (oszthatóság eldöntése az irreducibilis faktorizációban fellépő kitevők segítségével)!

4.16. Következmény

Bármely $f, g \in \mathbb{C}[x]$ esetén $f \mid g$ akkor és csak akkor teljesül, ha f minden gyöke egyúttal gyöke g-nek is, mégpedig legalább akkora multiplicitással, mint f-nek.

Bizonyítás.

Használjuk a 3.51. Tételt (oszthatóság eldöntése az irreducibilis faktorizációban fellépő kitevők segítségével)! Az f polinom gyökei „egy az egybe” megfelelnek f prímosztóinak,

4.16. Következmény

Bármely $f, g \in \mathbb{C}[x]$ esetén $f \mid g$ akkor és csak akkor teljesül, ha f minden gyöke egyúttal gyöke g-nek is, mégpedig legalább akkora multiplicitással, mint f-nek.

Bizonyítás.

Használjuk a 3.51. Tételt (oszthatóság eldöntése az irreducibilis faktorizációban fellépő kitevők segítségével)! Az f polinom gyökei „egy az egybe" megfelelnek f prímosztóinak, továbbá az α gyök multiplicitása éppen az $x - \alpha$ prímtényező kitevője f prímfelbontásában. □

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$f(\overline{z}) = a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0$$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} \end{aligned}$$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} \end{aligned}$$

$(a_i \in \mathbb{R})$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} \qquad (a_i \in \mathbb{R}) \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \end{aligned}$$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} \qquad (a_i \in \mathbb{R}) \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} \qquad (1.11/(4)) \end{aligned}$$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned} f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\ &= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} && (a_i \in \mathbb{R}) \\ &= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} && (1.11/(4)) \\ &= \overline{a_n z^n + \cdots + a_1 z + a_0} && (1.11/(2)) \end{aligned}$$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned}
f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\
&= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} && (a_i \in \mathbb{R}) \\
&= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} && (1.11/(4)) \\
&= \overline{a_n z^n + \cdots + a_1 z + a_0} && (1.11/(2)) \\
&= \overline{f(z)}
\end{aligned}$$

Irreducibilis polinomok a valós számtest felett

4.17. Tétel

A valós polinomok nemvalós gyökei komplex konjugált párokban lépnek fel:

$$\forall f \in \mathbb{R}[x] \ \forall z \in \mathbb{C} \setminus \mathbb{R} : f(z) = 0 \implies f(\overline{z}) = 0.$$

(Igaz $z \in \mathbb{R}$ esetén is, de akkor semmitmondó!)

Bizonyítás.

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$, ahol $a_n, \ldots, a_1, a_0 \in \mathbb{R}$.

$$\begin{aligned}
f(\overline{z}) &= a_n \cdot \overline{z}^n + \cdots + a_1 \cdot \overline{z} + a_0 \\
&= \overline{a_n} \cdot \overline{z}^n + \cdots + \overline{a_1} \cdot \overline{z} + \overline{a_0} && (a_i \in \mathbb{R}) \\
&= \overline{a_n z^n} + \cdots + \overline{a_1 z} + \overline{a_0} && (1.11/(4)) \\
&= \overline{a_n z^n + \cdots + a_1 z + a_0} && (1.11/(2)) \\
&= \overline{f(z)}
\end{aligned}$$

Tehát $f(z) = 0 \implies f(\overline{z}) = \overline{f(z)} = \overline{0} = 0.$ □

4.18. Következmény

Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

4.18. Következmény

Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

Bizonyítás.

4.18. Következmény

Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

Bizonyítás.

Levezethető az előző tételből, de függvényvizsgálattal még könnyebb. □

4.18. Következmény

Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

Bizonyítás.

Levezethető az előző tételből, de függvényvizsgálattal még könnyebb. □

4.19. Következmény

Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:

- $ax + b \ \ (a, b \in \mathbb{R}, a \neq 0)$;
- $ax^2 + bx + c \ \ \left(a, b, c \in \mathbb{R}, a \neq 0, b^2 - 4ac < 0\right)$.

4.18. Következmény

Minden páratlan fokszámú valós együtthatós polinomnak van valós gyöke.

Bizonyítás.

Levezethető az előző tételből, de függvényvizsgálattal még könnyebb. □

4.19. Következmény

Egy valós együtthatós polinom pontosan akkor irreducibilis a valós számok teste felett, ha elsőfokú, vagy olyan másodfokú polinom, melynek nincs valós gyöke. Tehát az $\mathbb{R}$ feletti irreducibilis polinomok a következők:

- $ax + b \ \ (a, b \in \mathbb{R}, a \neq 0)$;
- $ax^2 + bx + c \ \ \left(a, b, c \in \mathbb{R}, a \neq 0, b^2 - 4ac < 0\right)$.

Bizonyítás.

Tudjuk, hogy a legfeljebb másodfokú polinomok között pontosan a fentiek az irreducibilisek (lásd 4.12. Tétel).

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök.

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel),

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$.

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$. Ezért az $(x-\alpha)(x-\overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben (4.6. Következmény).

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$. Ezért az $(x-\alpha)(x-\overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben (4.6. Következmény). Node

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2$$

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$. Ezért az $(x-\alpha)(x-\overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben (4.6. Következmény). Node

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2 \in \mathbb{R}[x],$$

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$. Ezért az $(x-\alpha)(x-\overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben (4.6. Következmény). Node

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2 \in \mathbb{R}[x],$$

így f-nek $(x-\alpha)(x-\overline{\alpha})$ valódi osztója $\mathbb{R}[x]$-ben (miért?). 

Bizonyítás (folyt.)

Legyen most $f \in \mathbb{R}[x]$ legalább harmadfokú.

- Ha f-nek van valós gyöke, akkor nem irreducibilis $\mathbb{R}$ felett (4.11. Tétel).
- Ha f-nek nincs valós gyöke, akkor legyen $\alpha \in \mathbb{C} \setminus \mathbb{R}$ egy nemvalós komplex gyök. Ekkor $\overline{\alpha}$ is gyöke f-nek (4.17. Tétel), és $\overline{\alpha} \neq \alpha$ mert $\alpha \notin \mathbb{R}$. Ezért az $(x-\alpha)(x-\overline{\alpha}) \mid f$ oszthatóság teljesül $\mathbb{C}[x]$-ben (4.6. Következmény). Node

$$(x-\alpha)(x-\overline{\alpha}) = x^2 - 2\operatorname{Re}\alpha \cdot x + |\alpha|^2 \in \mathbb{R}[x],$$

  így f-nek $(x-\alpha)(x-\overline{\alpha})$ valódi osztója $\mathbb{R}[x]$-ben (miért?). 
  Tehát f nem irreducibilis.

□

Irreducibilis polinomok a racionális számtest felett

Primitív polinomok

4.20. Definíció

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot **primitív polinom**nak nevezzük, ha együtthatói relatív prímek, azaz lnko $(a_0, \ldots, a_n) = 1$.

Primitív polinomok

4.20. Definíció

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot **primitív polinom**nak nevezzük, ha együtthatói relatív prímek, azaz lnko $(a_0, \ldots, a_n) = 1$.

4.21. Állítás

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára:

$$\forall f \in \mathbb{Q}[x] \ \exists r \in \mathbb{Q} \ \exists f^* \in \mathbb{Z}[x] : \ f = r \cdot f^* \text{ és } f^* \text{ primitív polinom.}$$

Primitív polinomok

4.20. Definíció

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot **primitív polinom**nak nevezzük, ha együtthatói relatív prímek, azaz $\text{lnko}(a_0, \ldots, a_n) = 1$.

4.21. Állítás

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára:

$$\forall f \in \mathbb{Q}[x] \ \exists r \in \mathbb{Q} \ \exists f^* \in \mathbb{Z}[x] : \ f = r \cdot f^* \text{ és } f^* \text{ primitív polinom.}$$

Bizonyítás.

Legyen $f = \sum_{i=0}^{n} \frac{p_i}{q_i} \cdot x^i$, ahol $p_i, q_i \in \mathbb{Z}$, $\text{lnko}(p_i, q_i) = 1 \ \ (i = 0, \ldots, n)$.

Primitív polinomok

4.20. Definíció

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot **primitív polinom**nak nevezzük, ha együtthatói relatív prímek, azaz $\text{lnko}(a_0, \ldots, a_n) = 1$.

4.21. Állítás

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára:

$$\forall f \in \mathbb{Q}[x] \ \exists r \in \mathbb{Q} \ \exists f^* \in \mathbb{Z}[x] : \ f = r \cdot f^* \text{ és } f^* \text{ primitív polinom.}$$

Bizonyítás.

Legyen $f = \sum_{i=0}^{n} \frac{p_i}{q_i} \cdot x^i$, ahol $p_i, q_i \in \mathbb{Z}$, $\text{lnko}(p_i, q_i) = 1 \ \ (i = 0, \ldots, n)$.

$$f = \tfrac{1}{Q} \cdot \sum_{i=0}^{n} \underbrace{\frac{Q}{q_i} p_i}_{b_i \in \mathbb{Z}} \cdot x^i, \quad \text{ahol } Q = \text{lkkt}(q_0, \ldots, q_n)$$

Primitív polinomok

4.20. Definíció

Az $a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$ polinomot **primitív polinom**nak nevezzük, ha együtthatói relatív prímek, azaz $\text{lnko}(a_0, \ldots, a_n) = 1$.

4.21. Állítás

Minden racionális együtthatós polinom felbontható egy racionális szám és egy primitív polinom szorzatára:

$$\forall f \in \mathbb{Q}[x] \ \exists r \in \mathbb{Q} \ \exists f^* \in \mathbb{Z}[x] : \ f = r \cdot f^* \text{ és } f^* \text{ primitív polinom.}$$

Bizonyítás.

Legyen $f = \sum_{i=0}^{n} \frac{p_i}{q_i} \cdot x^i$, ahol $p_i, q_i \in \mathbb{Z}$, $\text{lnko}(p_i, q_i) = 1 \ \ (i = 0, \ldots, n)$.

$$f = \tfrac{1}{Q} \cdot \sum_{i=0}^{n} \underbrace{\frac{Q}{q_i} p_i}_{b_i \in \mathbb{Z}} \cdot x^i, \quad \text{ahol } Q = \text{lkkt}(q_0, \ldots, q_n)$$

$$f = \tfrac{d}{Q} \cdot \sum_{i=0}^{n} \tfrac{b_i}{d} \cdot x^i, \qquad \text{ahol } d = \text{lnko}(b_0, \ldots, b_n)$$

Primitív polinomok

Bizonyítás (folyt.)

Tehát $f = r \cdot f^*$, ahol

$$r = \frac{d}{Q} \in \mathbb{Q} \quad \text{és} \quad f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x] \text{ primitív polinom.}$$

□

Primitív polinomok

Bizonyítás (folyt.)

Tehát $f = r \cdot f^*$, ahol

$$r = \frac{d}{Q} \in \mathbb{Q} \quad \text{és} \quad f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x] \text{ primitív polinom.}$$  □

4.22. Megjegyzés

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Primitív polinomok

Bizonyítás (folyt.)

Tehát $f = r \cdot f^*$, ahol

$$r = \frac{d}{Q} \in \mathbb{Q} \quad \text{és} \quad f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x] \text{ primitív polinom.}$$

□

4.22. Megjegyzés

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Példa

Legyen $f = \frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} \in \mathbb{Q}[x]$.

$$f = \tfrac{15}{7}x^2 + \tfrac{45}{4}x + \tfrac{5}{2} =$$

Primitív polinomok

Bizonyítás (folyt.)

Tehát $f = r \cdot f^*$, ahol

$$r = \frac{d}{Q} \in \mathbb{Q} \quad \text{és} \quad f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x] \text{ primitív polinom.}$$  □

4.22. Megjegyzés

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Példa

Legyen $f = \frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} \in \mathbb{Q}[x]$.

$$f = \tfrac{15}{7}x^2 + \tfrac{45}{4}x + \tfrac{5}{2} \overset{\text{  }}{=} \tfrac{60}{28}x^2 + \tfrac{315}{28}x + \tfrac{70}{28}$$

Primitív polinomok

Bizonyítás (folyt.)

Tehát $f = r \cdot f^*$, ahol

$$r = \frac{d}{Q} \in \mathbb{Q} \quad \text{és} \quad f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x] \text{ primitív polinom.}$$  □

4.22. Megjegyzés

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Példa

Legyen $f = \frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} \in \mathbb{Q}[x]$.

$$f = \tfrac{15}{7}x^2 + \tfrac{45}{4}x + \tfrac{5}{2} \overset{\text{  }}{=} \tfrac{60}{28}x^2 + \tfrac{315}{28}x + \tfrac{70}{28}$$

$$= \tfrac{1}{28} \cdot \left(60x^2 + 315x + 70\right) \overset{\text{  }}{=}$$

Primitív polinomok

Bizonyítás (folyt.)

Tehát $f = r \cdot f^*$, ahol

$$r = \frac{d}{Q} \in \mathbb{Q} \quad \text{és} \quad f^* = \sum_{i=0}^{n} \frac{b_i}{d} \cdot x^i \in \mathbb{Z}[x] \text{ primitív polinom.}$$  □

4.22. Megjegyzés

Az előző állításban $f \sim f^*$ (ha $f \neq 0$), tehát $\mathbb{Q}[x]$-ben asszociáltság erejéig mindig lehet primitív polinomokkal számolni.

Példa

Legyen $f = \frac{15}{7}x^2 + \frac{45}{4}x + \frac{5}{2} \in \mathbb{Q}[x]$.

$$f = \tfrac{15}{7}x^2 + \tfrac{45}{4}x + \tfrac{5}{2} \overset{\text{  }}{=} \tfrac{60}{28}x^2 + \tfrac{315}{28}x + \tfrac{70}{28}$$

$$= \tfrac{1}{28} \cdot (60x^2 + 315x + 70) \overset{\text{  }}{=} \underbrace{\frac{5}{28}}_{r} \cdot (\underbrace{12x^2 + 63x + 14}_{f^*})$$

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$,

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \mid a_n$, akkor $\overline{a_n} = \overline{0}$, és így $\deg \overline{f} < \deg f = n$.

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x] : \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \mid a_n$, akkor $\overline{a_n} = \overline{0}$, és így $\deg \overline{f} < \deg f = n$.

Példa

Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$.

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \mid a_n$, akkor $\overline{a_n} = \overline{0}$, és így $\deg \overline{f} < \deg f = n$.

Példa

Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$. Ekkor

$$\overline{f} = \overline{10}x^3 + \overline{7}x^2 + \overline{25}x + \overline{-2}$$

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \mid a_n$, akkor $\overline{a_n} = \overline{0}$, és így $\deg \overline{f} < \deg f = n$.

Példa

Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$. Ekkor

$$\overline{f} = \overline{10}x^3 + \overline{7}x^2 + \overline{25}x + \overline{-2} = \overline{0}x^3 + \overline{2}x^2 + \overline{0}x + \overline{3}$$

Redukció modulo p

Rögzítsünk egy p prímszámot, és tekintsük az $f = \sum_{i=0}^{n} a_i \cdot x^i \in \mathbb{Z}[x]$ polinom együtthatóit modulo p:

$$\overline{f} := \sum_{i=0}^{n} \overline{a_i} \cdot x^i \in \mathbb{Z}_p[x].$$

A maradékosztályokkal való számolás definíciójából adódik, hogy

$$\forall f, g \in \mathbb{Z}[x]: \ \overline{f \cdot g} = \overline{f} \cdot \overline{g}.$$

Nyilván $\deg \overline{f} \leq \deg f$, továbbá ha $p \mid a_n$, akkor $\overline{a_n} = \overline{0}$, és így $\deg \overline{f} < \deg f = n$.

Példa

Legyen $p = 5$ és $f = 10x^3 + 7x^2 + 25x - 2$. Ekkor

$$\overline{f} = \overline{10}x^3 + \overline{7}x^2 + \overline{25}x + \overline{-2} = \overline{0}x^3 + \overline{2}x^2 + \overline{0}x + \overline{3} = \overline{2}x^2 + \overline{3} \in \mathbb{Z}_5[x].$$

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját 

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.
- g primitív $\Longrightarrow$ $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.
- g primitív $\Longrightarrow$ $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Tehát a $\mathbb{Z}_p[x]$ gyűrűben $\overline{f}$ és $\overline{g}$ 

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.
- g primitív $\Longrightarrow$ $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Tehát a $\mathbb{Z}_p[x]$ gyűrűben $\overline{f}$ és $\overline{g}$  zérusosztók

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.
- g primitív $\Longrightarrow$ $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Tehát a $\mathbb{Z}_p[x]$ gyűrűben $\overline{f}$ és $\overline{g}$  zérusosztók, ez pedig lehetetlen 

Gauss-lemma

4.23. Lemma

$f \in \mathbb{Z}[x]$ primitív $\iff$ minden p prímszámra $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Bizonyítás.

$\Longleftarrow$: Ha f nem primitív, akkor létezik olyan p prím, ami osztja f minden együtthatóját  , és így $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$.

$\Longrightarrow$: Ha létezik olyan p prím, amelyre $\overline{f} = \overline{0} \in \mathbb{Z}_p[x]$, akkor p osztja f minden együtthatóját, és így f nem primitív. □

4.24. Tétel (Gauss -lemma)

Primitív polinomok szorzata is primitív.

Bizonyítás.

Legyenek f és g primitív polinomok, és tegyük fel, hogy fg nem primitív.

- fg nem primitív $\Longrightarrow$ létezik olyan p prím, amelyre $\overline{fg} = \overline{0} \in \mathbb{Z}_p[x]$.
- f primitív $\Longrightarrow$ $\overline{f} \neq \overline{0} \in \mathbb{Z}_p[x]$.
- g primitív $\Longrightarrow$ $\overline{g} \neq \overline{0} \in \mathbb{Z}_p[x]$.

Tehát a $\mathbb{Z}_p[x]$ gyűrűben $\overline{f}$ és $\overline{g}$  zérusosztók, ez pedig lehetetlen  , mivel $\mathbb{Z}_p$ test. (Lásd a 2.21. Állítást és a 2.30. Tételt.) □

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

4.26. Megjegyzés

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

4.26. Megjegyzés

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont **nem** ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

4.26. Megjegyzés

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont **nem** ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett. Tehát a fenti tételt **nem** fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha irreducibilis $\mathbb{Q}$ felett.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

4.26. Megjegyzés

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont **nem** ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett. Tehát a fenti tételt **nem** fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha irreducibilis $\mathbb{Q}$ felett.

Például a $2x$ polinom nem irreducibilis $\mathbb{Z}$ felett de irreducibilis $\mathbb{Q}$ felett. 

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

Ha egy legalább elsőfokú egész együtthatós polinom nem bontható fel nála kisebb fokszámú egész együtthatós polinomok szorzatára, akkor $\mathbb{Q}$ felett sem bomlik így fel, és viszont. Formálisan: ha $f \in \mathbb{Z}[x]$ és $\deg f = n \geq 1$, akkor az alábbi két állítás ekvivalens:

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

4.26. Megjegyzés

A második feltétel azzal ekvivalens, hogy f reducibilis $\mathbb{Q}$ felett. Az első viszont **nem** ekvivalens azzal, hogy f reducibilis $\mathbb{Z}$ felett. Tehát a fenti tételt **nem** fogalmazhatjuk meg egyszerűen úgy, hogy egy egész együtthatós polinom akkor és csak akkor irreducibilis $\mathbb{Z}$ felett, ha irreducibilis $\mathbb{Q}$ felett.

Például a $2x$ polinom nem irreducibilis $\mathbb{Z}$ felett de irreducibilis $\mathbb{Q}$ felett. 
Meg lehet mutatni, hogy a $\mathbb{Z}$ feletti irreducibilis polinomok éppen a $\mathbb{Q}$ felett irreducibilis primitív polinomok, valamint a prímszámok (mint konstans polinomok).

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ esetén $(1) \iff (2)$

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Bizonyítás.

Az világos, hogy

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ esetén $(1) \iff (2)$

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Bizonyítás.

Az világos, hogy $(1) \implies (2)$.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ esetén $(1) \iff (2)$

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Bizonyítás.

Az világos, hogy $(1) \implies (2)$.
Tegyük fel, hogy (2) teljesül, és legyen

$$g = r \cdot g^*, \ h = s \cdot h^*, \text{ ahol } r, s \in \mathbb{Q} \text{ és } g^*, h^* \in \mathbb{Z}[x] \text{ primitív polinomok.}$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ esetén $(1) \iff (2)$

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Bizonyítás.

Az világos, hogy $(1) \implies (2)$.
Tegyük fel, hogy (2) teljesül, és legyen

$$g = r \cdot g^*, \ h = s \cdot h^*, \text{ ahol } r, s \in \mathbb{Q} \text{ és } g^*, h^* \in \mathbb{Z}[x] \text{ primitív polinomok.}$$

Legyen $rs = \frac{p}{q}$, ahol $\text{lnko}(p, q) = 1$ és $q > 0$.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ esetén $(1) \iff (2)$

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Bizonyítás.

Az világos, hogy $(1) \implies (2)$.
Tegyük fel, hogy (2) teljesül, és legyen

$$g = r \cdot g^*, \ h = s \cdot h^*, \text{ ahol } r, s \in \mathbb{Q} \text{ és } g^*, h^* \in \mathbb{Z}[x] \text{ primitív polinomok.}$$

Legyen $rs = \frac{p}{q}$, ahol $\operatorname{lnko}(p, q) = 1$ és $q > 0$. Ekkor

$$f = g \cdot h = rg^* \cdot sh^* = rs \cdot g^* h^* = \frac{p}{q} \cdot g^* h^*.$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

4.25. Tétel

$\forall f \in \mathbb{Z}[x], \deg f \geq 1$ esetén $(1) \iff (2)$

(1) $\exists g, h \in \mathbb{Z}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$;

(2) $\exists g, h \in \mathbb{Q}[x] : f = g \cdot h$ és $0 < \deg g, \deg h < n$.

Bizonyítás.

Az világos, hogy $(1) \implies (2)$.
Tegyük fel, hogy (2) teljesül, és legyen

$$g = r \cdot g^*, \ h = s \cdot h^*, \text{ ahol } r, s \in \mathbb{Q} \text{ és } g^*, h^* \in \mathbb{Z}[x] \text{ primitív polinomok.}$$

Legyen $rs = \frac{p}{q}$, ahol $\text{lnko}(p, q) = 1$ és $q > 0$. Ekkor

$$f = g \cdot h = rg^* \cdot sh^* = rs \cdot g^* h^* = \frac{p}{q} \cdot g^* h^*.$$

Meg fogjuk mutatni, hogy $q = 1$.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$.

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\forall i \in \{0, \ldots, n\} : \; q \mid p \cdot a_i$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\forall i \in \{0, \ldots, n\} : \; q \mid p \cdot a_i$$

$$\implies \forall i \in \{0, \ldots, n\} : \; q \mid a_i$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned} & \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\ \implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\ \implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \end{aligned}$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned}
& \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\
\implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\
\implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \\
\implies & q = 1
\end{aligned}$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned}
& \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\
\implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\
\implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \\
\implies & q = 1
\end{aligned}$$

Tehát

$$f = \frac{p}{q} \cdot g^* h^*$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned} & \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\ \implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\ \implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \\ \implies & q = 1 \end{aligned}$$

Tehát

$$f = \frac{p}{q} \cdot g^* h^* = \underbrace{pg^*}_{\in \mathbb{Z}[x]} \cdot \underbrace{h^*}_{\in \mathbb{Z}[x]}.$$

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned} & \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\ \implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\ \implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \\ \implies & q = 1 \end{aligned}$$

Tehát

$$f = \frac{p}{q} \cdot g^* h^* = \underbrace{pg^*}_{\in \mathbb{Z}[x]} \cdot \underbrace{h^*}_{\in \mathbb{Z}[x]}.$$

A fenti felbontásban a fokszámok ugyanazok, mint az eredeti $f = gh$ felbontásban,

Felbontás $\mathbb{Q}$, illetve $\mathbb{Z}$ felett

Bizonyítás (folyt.)

$$f = \frac{p}{q} \cdot g^* h^* \implies q \cdot f = p \cdot g^* h^*$$

Legyen $g^* h^* = \sum_{i=0}^{n} a_i \cdot x^i$. A fentiek szerint

$$\begin{aligned} & \forall i \in \{0, \ldots, n\} : \ q \mid p \cdot a_i \\ \implies & \forall i \in \{0, \ldots, n\} : \ q \mid a_i \\ \implies & q \mid \operatorname{lnko}(a_0, \ldots, a_n) \\ \implies & q = 1 \end{aligned}$$

Tehát

$$f = \frac{p}{q} \cdot g^* h^* = \underbrace{pg^*}_{\in \mathbb{Z}[x]} \cdot \underbrace{h^*}_{\in \mathbb{Z}[x]}.$$

A fenti felbontásban a fokszámok ugyanazok, mint az eredeti $f = gh$ felbontásban, hiszen $pg^* \sim g$ és $h^* \sim h$. □

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$,

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek.

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek. Így csak véges sok lehetőség van $g(c)$-re

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek. Így csak véges sok lehetőség van $g(c)$-re (kivéve, ha

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek. Így csak véges sok lehetőség van $g(c)$-re (kivéve, ha $f(c) = 0$).

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek. Így csak véges sok lehetőség van $g(c)$-re (kivéve, ha $f(c) = 0$).
- Ha elég sok helyen ismerjük g értékét, akkor g-t meg tudjuk határozni. 

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek. Így csak véges sok lehetőség van $g(c)$-re (kivéve, ha $f(c) = 0$).
- Ha elég sok helyen ismerjük g értékét, akkor g-t meg tudjuk határozni. 

$\longrightarrow$ Kronecker-algoritmus

Felbontás $\mathbb{Z}$ felett

Probléma

Adott n-edfokú $f \in \mathbb{Z}[x]$ polinom esetén hogyan dönthetjük el, hogy léteznek-e olyan $g, h \in \mathbb{Z}[x]$ polinomok, melyekre $f = g \cdot h$ és $0 < \deg g, \deg h < n$?

Ötlet

- Ha $f = g \cdot h$, akkor bármely c egész számra $f(c) = g(c) \cdot h(c)$, tehát $g(c)$ osztója $f(c)$-nek. Így csak véges sok lehetőség van $g(c)$-re (kivéve, ha $f(c) = 0$).
- Ha elég sok helyen ismerjük g értékét, akkor g-t meg tudjuk határozni. 

$\longrightarrow$ Kronecker-algoritmus

4.27. Definíció

Azt mondjuk, hogy a p prímszám **pontos osztó**ja az a egész számnak, ha a osztható p-vel, de p^2-tel már nem.
A pontos oszthatóságot $\|$ jelöli: $p \| a \iff p \mid a$ és $p^2 \nmid a$.

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ p \mid a_{n-1}, \ldots,\ p \mid a_1,\ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ p \mid a_{n-1}, \ldots,\ p \mid a_1,\ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett.

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ p \mid a_{n-1}, \ldots,\ p \mid a_1,\ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ p \mid a_{n-1}, \ldots,\ p \mid a_1,\ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$.

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Ha itt valamelyik egyenlőtlenség szigorú lenne, akkor

$$\deg \overline{f} = \deg \overline{g \cdot h} = \deg \overline{g} + \deg \overline{h}$$

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Ha itt valamelyik egyenlőtlenség szigorú lenne, akkor

$$\deg \overline{f} = \deg \overline{g \cdot h} = \deg \overline{g} + \deg \overline{h} < \deg g + \deg h = \deg f = n,$$

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Ha itt valamelyik egyenlőtlenség szigorú lenne, akkor

$$\deg \overline{f} = \deg \overline{g \cdot h} = \deg \overline{g} + \deg \overline{h} < \deg g + \deg h = \deg f = n,$$

ami

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Ha itt valamelyik egyenlőtlenség szigorú lenne, akkor

$$\deg \overline{f} = \deg \overline{g \cdot h} = \deg \overline{g} + \deg \overline{h} < \deg g + \deg h = \deg f = n,$$

ami 

Schönemann–Eisenstein

4.28. Tétel (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \parallel a_0 = f(0),$$

akkor f irreducibilis a racionális számok teste felett.

Bizonyítás.

Tfh. van ilyen prím, és f mégsem irreducibilis $\mathbb{Q}$ felett. A 4.25. Tétel szerint

$$\exists g, h \in \mathbb{Z}[x] : f = g \cdot h \text{ és } 0 < \deg g, \deg h < n.$$

Redukáljunk modulo p: $\overline{f} = \overline{g \cdot h} = \overline{g} \cdot \overline{h} \in \mathbb{Z}_p[x]$. Tudjuk, hogy

$$\deg \overline{g} \leq \deg g \text{ és } \deg \overline{h} \leq \deg h.$$

Ha itt valamelyik egyenlőtlenség szigorú lenne, akkor

$$\deg \overline{f} = \deg \overline{g \cdot h} = \deg \overline{g} + \deg \overline{h} < \deg g + \deg h = \deg f = n,$$

ami   , hiszen $p \nmid a_n$ miatt f fokszáma nem csökken a mod p redukciónál.

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} =$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} \overset{\text{!}}{=} \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\overline{g(0)} \overset{\text{!}}{=} \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0}$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} \overset{\text{!}}{=} \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\overline{g(0)} \overset{\text{!}}{=} \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} \implies p \mid g(0)$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\begin{aligned} \overline{g(0)} &= \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} \implies p \mid g(0) \\ \overline{h(0)} &= \overline{h}(\overline{0}) = \overline{c} \cdot \overline{0}^l = \overline{0} \implies p \mid h(0) \end{aligned}$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\left.\begin{array}{rcl} \overline{g(0)} = \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} & \Longrightarrow & p \mid g(0) \\ \overline{h(0)} = \overline{h}(\overline{0}) = \overline{c} \cdot \overline{0}^l = \overline{0} & \Longrightarrow & p \mid h(0) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow \ p^2 \mid g(0) \cdot h(0)$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\left.\begin{array}{rcl} \overline{g(0)} = \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} & \Longrightarrow & p \mid g(0) \\ \overline{h(0)} = \overline{h}(\overline{0}) = \overline{c} \cdot \overline{0}^l = \overline{0} & \Longrightarrow & p \mid h(0) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow \ p^2 \mid g(0) \cdot h(0) = f(0)$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\left.\begin{array}{rcl} \overline{g(0)} = \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} & \Longrightarrow & p \mid g(0) \\ \overline{h(0)} = \overline{h}(\overline{0}) = \overline{c} \cdot \overline{0}^l = \overline{0} & \Longrightarrow & p \mid h(0) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow \ p^2 \mid g(0) \cdot h(0) = f(0) = a_0.$$

Schönemann–Eisenstein

Bizonyítás (folyt.)

Tehát

$$0 < k := \deg \overline{g} = \deg g \quad \text{és} \quad 0 < l := \deg \overline{h} = \deg h.$$

Az f együtthatóira kirótt oszthatósági feltétel alapján

$$\overline{g} \cdot \overline{h} = \overline{f} = \overline{a_n} x^n \in \mathbb{Z}_p [x],$$

és így szükségképpen

$$\overline{g} = \overline{b} x^k, \ \overline{h} = \overline{c} x^l, \text{ ahol } k + l = n \text{ és } \overline{b} \cdot \overline{c} = \overline{a_n}.$$

Ebből következik, hogy

$$\left.\begin{array}{rcl} \overline{g(0)} = \overline{g}(\overline{0}) = \overline{b} \cdot \overline{0}^k = \overline{0} & \Longrightarrow & p \mid g(0) \\ \overline{h(0)} = \overline{h}(\overline{0}) = \overline{c} \cdot \overline{0}^l = \overline{0} & \Longrightarrow & p \mid h(0) \end{array}\right\} \Longrightarrow$$

$$\Longrightarrow p^2 \mid g(0) \cdot h(0) = f(0) = a_0. \qquad \square$$

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

$x^n + 2$ □

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

$x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

 $x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

 $x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak az elsőfokúak,

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

 $x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak az elsőfokúak,
- $\mathbb{R}$ felett csak

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

 $x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak az elsőfokúak,
- $\mathbb{R}$ felett csak az elsőfokúak és bizonyos másodfokúak

irreducibilisek.

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

 $x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak az elsőfokúak,
- $\mathbb{R}$ felett csak az elsőfokúak és bizonyos másodfokúak

irreducibilisek.

Még szerencse, hogy a racionális számok testének már nincs valódi részteste! 

Schönemann–Eisenstein

4.29. Következmény

Minden $n \geq 1$ egész számra létezik $\mathbb{Q}$ felett irreducibilis n-edfokú polinom.

Bizonyítás.

 $x^n + 2$ □

Érdemes ezt összehasonlítani a komplex és a valós számtest esetével:

- $\mathbb{C}$ felett csak az elsőfokúak,
- $\mathbb{R}$ felett csak az elsőfokúak és bizonyos másodfokúak

irreducibilisek.

Még szerencse, hogy a racionális számok testének már nincs valódi részteste! 

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

Schönemann–Eisenstein

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

Schönemann–Eisenstein

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

NEM IGAZ!!!

Schönemann–Eisenstein

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

NEM IGAZ!!!

Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, **nem következik**, hogy a polinom nem irreducibilis

Schönemann–Eisenstein

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

NEM IGAZ!!!

Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, **nem következik**, hogy a polinom nem irreducibilis (keressünk ellenpéldát! ).

Schönemann–Eisenstein

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

NEM IGAZ!!!

Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, **nem következik**, hogy a polinom nem irreducibilis (keressünk ellenpéldát! ).
A megfordítás helyett következzék inkább a tétel „tükörképe”.

Schönemann–Eisenstein

4.30. Megjegyzés

A Schönemann–Eisenstein-tétel megfordítása...

NEM IGAZ!!!

Vagyis abból, hogy nem létezik olyan p prímszám, ami teljesítené a megfelelő oszthatósági feltételeket, **nem következik**, hogy a polinom nem irreducibilis (keressünk ellenpéldát! ).
A megfordítás helyett következzék inkább a tétel „tükörképe”.

4.31. Tétel* (Schönemann–Eisenstein-féle irreducibilitási kritérium)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0 \in \mathbb{Z}[x]$. Ha létezik olyan p prímszám amelyre

$$p \nmid a_n,\ \ p \mid a_{n-1}, \ldots,\ \ p \mid a_1,\ \ p \nmid a_0,$$

akkor f irreducibilis a racionális számok teste felett.

Racionális gyökök

4.32. Tétel (Rolle tétele)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám

Racionális gyökök

4.32. Tétel (Rolle tétele)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és $\text{lnko}\,(p, q) = 1$)

Racionális gyökök

4.32. Tétel (Rolle tétele)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és lnko $(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Racionális gyökök

4.32. Tétel (Rolle tétele)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és lnko $(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Racionális gyökök

4.32. Tétel (Rolle tétele)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és lnko $(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Természetesen a fenti nyíl nem fordítható meg: $q \mid a_n$ és $p \mid a_0$ nem garantálja, hogy $\frac{p}{q}$ gyöke f-nek.

Racionális gyökök

4.32. Tétel (Rolle tétele)

Legyen $f = a_n x^n + \cdots + a_1 x + a_0$ egy tetszőleges egész együtthatós polinom. Ha $\frac{p}{q}$ egy egyszerűsíthetetlen tört alakjában felírt racionális szám (azaz $p, q \in \mathbb{Z}$, $q \neq 0$ és lnko $(p, q) = 1$), akkor

$$f\left(\frac{p}{q}\right) = 0 \implies q \mid a_n \text{ és } p \mid a_0.$$

Speciálisan: egész együtthatós főpolinom racionális gyökei mindig egész számok.

Természetesen a fenti nyíl nem fordítható meg: $q \mid a_n$ és $p \mid a_0$ nem garantálja, hogy $\frac{p}{q}$ gyöke f-nek.

A Rolle-tételben „az a jó”, hogy egy véges halmazt ad meg, amelyben az összes racionális gyököt megtalálhatjuk (ha van egyáltalán racionális gyök).

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1}}_{} \quad + \quad \underbrace{a_0 q^n}_{}$$

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1} \frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1} p^{n-1} q + \cdots + a_1 p q^{n-1}}_{p \mid} + \underbrace{a_0 q^n}$$

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (lnko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1}}_{p\,|} + \underbrace{a_0 q^n}_{\Longrightarrow}$$

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (lnko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1}}_{p\,|} + \underbrace{a_0 q^n}_{p\,|}$$


Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (Inko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1}}_{p\,|} + \underbrace{a_0 q^n}_{p\,|} \Longrightarrow p \mid a_0$$

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (lnko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1}}_{p\,|} + \underbrace{a_0 q^n}_{p\,|} \Longrightarrow p \mid a_0$$

Hasonlóan:

Racionális gyökök

Bizonyítás.

Tegyök fel, hogy $\frac{p}{q}$ gyöke f-nek (lnko $(p, q) = 1$).

$$0 = f\left(\frac{p}{q}\right) = a_n \frac{p^n}{q^n} + a_{n-1}\frac{p^{n-1}}{q^{n-1}} + \cdots + a_1 \frac{p}{q} + a_0.$$

Szorozzunk be q^n-nel:

$$0 = \underbrace{a_n p^n + a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1}}_{p \mid} + \underbrace{a_0 q^n}_{p \mid} \Longrightarrow p \mid a_0$$

Hasonlóan:

$$q \mid a_n \Longleftarrow \underbrace{a_n p^n}_{q \mid} + \underbrace{a_{n-1}p^{n-1}q + \cdots + a_1 pq^{n-1} + a_0 q^n}_{q \mid} = 0 \Longrightarrow q \mid a_0$$