Линеарна алгебра 1

четврто предавање

Институт за математику и информатику
Природно-математички факултет
Универзитет у Крагујевцу

Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће.

Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће. Из тог разлога, уводимо појмове сводљив и несводљив полином.

Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће. Из тог разлога, уводимо појмове сводљив и несводљив полином. Нека је $p(x) \in \mathbb{F}[x]$ и нека је $\mathrm{deg} p(x) = n \geqslant 1$. Тривијални делиоци полинома $p(x)$ су полиноми нултог степена, тј. полиноми c, где је $c \in \mathbb{F} \setminus \{0\}$ и полиноми $cp(x)$.

Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће. Из тог разлога, уводимо појмове сводљив и несводљив полином. Нека је $p(x) \in \mathbb{F}[x]$ и нека је $\mathrm{deg} p(x) = n \geqslant 1$. Тривијални делиоци полинома $p(x)$ су полиноми нултог степена, тј. полиноми c, где је $c \in \mathbb{F} \setminus \{0\}$ и полиноми $cp(x)$. Поставља се питање да ли полином $p(x)$ има и нетривијалних делилаца, тј. делилаца степена k, где је $0 < k < n$?

Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће. Из тог разлога, уводимо појмове сводљив и несводљив полином. Нека је $p(x) \in \mathbb{F}[x]$ и нека је $\deg p(x) = n \geqslant 1$. Тривијални делиоци полинома $p(x)$ су полиноми нултог степена, тј. полиноми c, где је $c \in \mathbb{F} \setminus \{0\}$ и полиноми $cp(x)$. Поставља се питање да ли полином $p(x)$ има и нетривијалних делилаца, тј. делилаца степена k, где је $0 < k < n$?

Дефиниција

Полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ је сводљив над пољем $\mathbb{F}$ ако постоје полиноми $g(x), h(x) \in \mathbb{F}[x]$, такви да је $p(x) = g(x) \cdot h(x)$, $\deg g(x) < n, \deg h(x) < n$.

Сводљивост полинома

Један од битних задатака јесте растављање полинома на чиниоце, наравно, уколико је то могуће. Из тог разлога, уводимо појмове сводљив и несводљив полином. Нека је $p(x) \in \mathbb{F}[x]$ и нека је $\deg p(x) = n \geqslant 1$. Тривијални делиоци полинома $p(x)$ су полиноми нултог степена, тј. полиноми c, где је $c \in \mathbb{F} \setminus \{0\}$ и полиноми $cp(x)$. Поставља се питање да ли полином $p(x)$ има и нетривијалних делилаца, тј. делилаца степена k, где је $0 < k < n$?

Дефиниција

Полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ је сводљив над пољем $\mathbb{F}$ ако постоје полиноми $g(x), h(x) \in \mathbb{F}[x]$, такви да је $p(x) = g(x) \cdot h(x)$, $\deg g(x) < n, \deg h(x) < n$. У супротном, $p(x)$ је несводљив над пољем $\mathbb{F}$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.

Из дефиниције непосредно следи:

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n. Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = 2$ или $\mathrm{deg} p(x) = 3$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = 2$ или $\mathrm{deg} p(x) = 3$.
Претпоставимо да је полином $p(x)$ сводљив.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = 2$ или $\deg p(x) = 3$.
Претпоставимо да је полином $p(x)$ сводљив. Тада је $p(x) = g(x) \cdot h(x)$, где је $\deg g(x) = 1$ или $\deg h(x) = 1$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = 2$ или $\deg p(x) = 3$.
Претпоставимо да је полином $p(x)$ сводљив. Тада је $p(x) = g(x) \cdot h(x)$, где је $\deg g(x) = 1$ или $\deg h(x) = 1$. Нека је на пример $g(x) = ax + b, a \neq 0$,

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = 2$ или $\deg p(x) = 3$.
Претпоставимо да је полином $p(x)$ сводљив. Тада је $p(x) = g(x) \cdot h(x)$, где је $\deg g(x) = 1$ или $\deg h(x) = 1$. Нека је на пример $g(x) = ax + b, a \neq 0$, па је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $g(x)$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = 2$ или $\deg p(x) = 3$.
Претпоставимо да је полином $p(x)$ сводљив. Тада је $p(x) = g(x) \cdot h(x)$, где је $\deg g(x) = 1$ или $\deg h(x) = 1$. Нека је на пример $g(x) = ax + b, a \neq 0$, па је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $g(x)$. Дакле, имамо да је $p(c) = g(c) \cdot h(c) = 0$.

Другим речима, полином $p(x)$ степена $n \geqslant 1$ је несводљив ако има само тривијалне делиоце, тј. само делиоце степена 0 и степена n.
Из дефиниције непосредно следи:

- Сви полиноми степена 1 су несводљиви.
- Полиноми степена 0 нису ни сводљиви, ни несводљиви.

Теорема

Полином $p(x) \in \mathbb{F}[x]$ степена 2 или 3 је сводљив над $\mathbb{F}$ ако и само ако $p(x)$ има корен у $\mathbb{F}$.

Доказ. Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = 2$ или $\deg p(x) = 3$.
Претпоставимо да је полином $p(x)$ сводљив. Тада је $p(x) = g(x) \cdot h(x)$, где је $\deg g(x) = 1$ или $\deg h(x) = 1$. Нека је на пример $g(x) = ax + b, a \neq 0$, па је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $g(x)$. Дакле, имамо да је $p(c) = g(c) \cdot h(c) = 0$.

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$.

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$.
Имамо да $(x - c) \mid p(x)$,

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$.

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Пример

Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Пример

Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$ несводљив, док полином $x^2 - 2 \in \mathbb{R}[x]$

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Пример

Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$ несводљив, док полином $x^2 - 2 \in \mathbb{R}[x]$ јесте сводљив, јер је $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$.

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Пример

Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$ несводљив, док полином $x^2 - 2 \in \mathbb{R}[x]$ јесте сводљив, јер је $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Полином $x^2 + 1 \in \mathbb{R}[x]$

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Пример

Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$ несводљив, док полином $x^2 - 2 \in \mathbb{R}[x]$ јесте сводљив, јер је $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Полином $x^2 + 1 \in \mathbb{R}[x]$ је несводљив, а $x^2 + 1 \in \mathbb{C}[x]$ је сводљив полином, јер је $x^2 + 1 = (x - i)(x + i)$.

Обратно, претпоставимо да постоји $c \in \mathbb{F}$ тако да је $p(c) = 0$. Имамо да $(x - c) \mid p(x)$, па је $p(x) = q(c) \cdot (x - c)$, где је $\deg(x - c) < \deg p(x)$ и $\deg q(x) < \deg p(x)$. Дакле, полином $p(x)$ је сводљив. $\square$

Пример

Приметимо да је полином $x^2 - 2 \in \mathbb{Q}[x]$ несводљив, док полином $x^2 - 2 \in \mathbb{R}[x]$ јесте сводљив, јер је $x^2 - 2 = (x - \sqrt{2})(x + \sqrt{2})$. Полином $x^2 + 1 \in \mathbb{R}[x]$ је несводљив, а $x^2 + 1 \in \mathbb{C}[x]$ је сводљив полином, јер је $x^2 + 1 = (x - i)(x + i)$.

Претходно тврђење (смер $\rightarrow$) не важи за полиноме степена већег од 3, тј. полином степена већег од 3 може бити сводљив над $\mathbb{F}$ иако нема корен у $\mathbb{F}$, што показује следећи пример.

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$, *али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$, *али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$, *али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 1. Ако је $p(x) \in \mathbb{F}[x]$ несводљив полином и $q(x) \in \mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$.

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$*, али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 1. Ако је $p(x) \in \mathbb{F}[x]$ несводљив полином и $q(x) \in \mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$.

Доказ. Нека је $d(x) = \mathrm{NZD}(p(x), q(x))$ и нека је $p(x)$ несводљив полином.

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$*, али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 1. Ако је $p(x) \in \mathbb{F}[x]$ несводљив полином и $q(x) \in \mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$.

Доказ. Нека је $d(x) = \mathrm{NZD}(p(x), q(x))$ и нека је $p(x)$ несводљив полином. Како $d(x) \mid p(x)$, то је $d(x)$ тривијални делилац.

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$*, али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 1. Ако је $p(x) \in \mathbb{F}[x]$ несводљив полином и $q(x) \in \mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$.

Доказ. Нека је $d(x) = \mathrm{NZD}(p(x), q(x))$ и нека је $p(x)$ несводљив полином. Како $d(x) \mid p(x)$, то је $d(x)$ тривијални делилац. Дакле, имамо да је $d(x)$ константан полином или $d(x) = cp(x)$ за неко $c \in \mathbb{F} \setminus \{0\}$.

Пример

Посматрајмо пример $x^4 + x^2 + 1 = (x^2 + 1)^2 - x^2 = (x^2 - x + 1)(x^2 + x + 1)$ *који је сводљив над* $\mathbb{R}$*, али* $x^4 + x^2 + 1$ *нема корен у* $\mathbb{R}$ *(јер* $x^2 - x + 1$ *и* $x^2 + x + 1$ *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 1. Ако је $p(x) \in \mathbb{F}[x]$ несводљив полином и $q(x) \in \mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x), q(x)) = 1$ или $p(x) \mid q(x)$.

Доказ. Нека је $d(x) = \mathrm{NZD}(p(x), q(x))$ и нека је $p(x)$ несводљив полином. Како $d(x) \mid p(x)$, то је $d(x)$ тривијални делилац. Дакле, имамо да је $d(x)$ константан полином или $d(x) = cp(x)$ за неко $c \in \mathbb{F} \setminus \{0\}$. Тада је $d(x) = 1$ због нормираности или $(cp(x)) \mid q(x)$,

Пример

Посматрајмо пример $x^4+x^2+1=(x^2+1)^2-x^2=(x^2-x+1)(x^2+x+1)$ *који је сводљив над* $\mathbb{R}$*, али* x^4+x^2+1 *нема корен у* $\mathbb{R}$ *(јер* x^2-x+1 *и* x^2+x+1 *немају корен у* $\mathbb{R}$*).*

Доказујема два помоћна тврђења (леме), која су аналогна одговарајућим тврђењима за просте бројеве:

Лема 1. Ако је $p(x)\in\mathbb{F}[x]$ несводљив полином и $q(x)\in\mathbb{F}[x]$ произвољан, тада је или $\mathrm{NZD}(p(x),q(x))=1$ или $p(x)\mid q(x)$.

Доказ. Нека је $d(x)=\mathrm{NZD}(p(x),q(x))$ и нека је $p(x)$ несводљив полином. Како $d(x)\mid p(x)$, то је $d(x)$ тривијални делилац. Дакле, имамо да је $d(x)$ константан полином или $d(x)=cp(x)$ за неко $c\in\mathbb{F}\setminus\{0\}$. Тада је $d(x)=1$ због нормираности или $(cp(x))\mid q(x)$, односно $\mathrm{NZD}(p(x),q(x))=1$ или $p(x)\mid q(x)$. $\square$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$.

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$,

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1.

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$.

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је $h(x) = h(x) \cdot 1$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је

$h(x) = h(x) \cdot 1$

$= h(x) \cdot (s_0(x) \cdot p(x) + t_0(x) \cdot g(x))$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је

$$\begin{aligned} h(x) &= h(x) \cdot 1 \\ &= h(x) \cdot (s_0(x) \cdot p(x) + t_0(x) \cdot g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(h(x)g(x)) \end{aligned}$$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је

$$\begin{aligned} h(x) &= h(x) \cdot 1 \\ &= h(x) \cdot (s_0(x) \cdot p(x) + t_0(x) \cdot g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(h(x)g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(q(x)p(x)) \end{aligned}$$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је

$$\begin{aligned} h(x) &= h(x) \cdot 1 \\ &= h(x) \cdot (s_0(x) \cdot p(x) + t_0(x) \cdot g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(h(x)g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(q(x)p(x)) \\ &= (s_0(x)h(x) + t_0(x)q(x))p(x). \end{aligned}$$

Лема 2. Ако је $p(x) \in \mathbb{F}[x]$ несводљив, а $g(x), h(x) \in \mathbb{F}[x]$ произвољни, тада

$$p(x) \mid (g(x) \cdot h(x)) \Rightarrow p(x) \mid g(x) \vee p(x) \mid h(x).$$

Доказ. Нека је $p(x)$ несводљив и $p(x) \mid (g(x) \cdot h(x))$. Претпоставимо да $p(x) \nmid g(x)$, па закључујемо да је $\mathrm{NZD}(p(x), g(x)) = 1$ на основу леме 1. Из теореме о највећем заједничком делиоцу имамо да је $1 = s_0(x) \cdot p(x) + t_0(x) \cdot g(x)$ за неко $s_0(x), t_0(x) \in \mathbb{F}[x]$. Дакле, имамо да је

$$\begin{aligned} h(x) &= h(x) \cdot 1 \\ &= h(x) \cdot (s_0(x) \cdot p(x) + t_0(x) \cdot g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(h(x)g(x)) \\ &= s_0(x)p(x)h(x) + t_0(x)(q(x)p(x)) \\ &= (s_0(x)h(x) + t_0(x)q(x))p(x). \end{aligned}$$

Дакле, $p(x) \mid h(x)$. $\square$

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$.

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

- Нека је полином $p(x)$ степена $n = 1$,

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

- Нека је полином $p(x)$ степена $n = 1$, односно нека је $p(x) = ax + b = a\underbrace{(x + a^{-1}b)}_{=p_1}$, где је $p_1 = x + a^{-1}b$ је нормиран и несводљив полином.

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

- Нека је полином $p(x)$ степена $n = 1$, односно нека је $p(x) = ax + b = a\underbrace{(x + a^{-1}b)}_{=p_1}$, где је $p_1 = x + a^{-1}b$ је нормиран и несводљив полином. Дакле, база индукције важи.

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

- Нека је полином $p(x)$ степена $n = 1$, односно нека је $p(x) = ax + b = a\underbrace{(x + a^{-1}b)}_{=p_1}$, где је $p_1 = x + a^{-1}b$ је нормиран и несводљив полином. Дакле, база индукције важи.
- Претпоставимо да тврђење важи за све полиноме степена мањег од n.

Следећа теореме је позната као теорема дуална основном ставу аритметике.

Теорема

Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ се може јединствено, до редоследа фактора, представити у облику $p(x) = ap_1(x)p_2(x)\dots p_r(x)$, где $a \in \mathbb{F} \setminus \{0\}$ и $p_1(x), \dots, p_r(x)$ су несводљиви нормирани полиноми у $\mathbb{F}[x]$ (не обавезно различити).

Доказ. Прво, докажимо егзистенцију таквог представљања полинома $p(x)$. Доказ изводимо трансфинитном индукцијом по степену n полинома $p(x)$.

- Нека је полином $p(x)$ степена $n = 1$, односно нека је $p(x) = ax + b = a\underbrace{(x + a^{-1}b)}_{=p_1}$, где је $p_1 = x + a^{-1}b$ је нормиран и несводљив полином. Дакле, база индукције важи.
- Претпоставимо да тврђење важи за све полиноме степена мањег од n.

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив,

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.
  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.
  (2) Ако је $p(x)$ сводљив,

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

  (2) Ако је $p(x)$ сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

  (2) Ако је $p(x)$ сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи $g(x) = b p_1(x) \ldots p_k(x)$,

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

  (2) Ако је $p(x)$ сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи $g(x) = bp_1(x) \dots p_k(x)$, $h(x) = cp_{k+1}(x) \dots p_r(x)$,

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

  (2) Ако је $p(x)$ сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи $g(x) = bp_1(x) \ldots p_k(x)$, $h(x) = cp_{k+1}(x) \ldots p_r(x)$, где су $b \neq 0$ и $c \neq 0$ и сви $p_i(x)$ су нормирани и несводљиви полиноми,

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

  (2) Ако је $p(x)$ сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи $g(x) = bp_1(x) \ldots p_k(x)$, $h(x) = cp_{k+1}(x) \ldots p_r(x)$, где су $b \neq 0$ и $c \neq 0$ и сви $p_i(x)$ су нормирани и несводљиви полиноми, па је

$$p(x) = g(x) \cdot h(x) = \underbrace{(b \cdot c)}_{=a} p_1(x) \ldots p_k(x) p_{k+1}(x) \ldots p_r(x),$$

  где је $a = bc \neq 0$, што је и требало показати.

- Докажимо да тврђење важи и за полином $p(x)$ степена $n > 1$. Разликујемо два случаја.

  (1) Ако је $p(x)$ несводљив, $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, $a_n \neq 0$, тада је $p(x) = a_n p_1$, где је $p_1 = a_n^{-1} a_0 + a_n^{-1} a_1 x + \cdots + x^n$ несводљив и нормиран полином.

  (2) Ако је $p(x)$ сводљив, тј. $p(x) = g(x)h(x)$, где је $\deg g(x) < n, \deg h(x) < n$. Тада, по индуктивној хипотези имамо да важи $g(x) = bp_1(x) \ldots p_k(x)$, $h(x) = cp_{k+1}(x) \ldots p_r(x)$, где су $b \neq 0$ и $c \neq 0$ и сви $p_i(x)$ су нормирани и несводљиви полиноми, па је

$$p(x) = g(x) \cdot h(x) = \underbrace{(b \cdot c)}_{=a} p_1(x) \ldots p_k(x) p_{k+1}(x) \ldots p_r(x),$$

  где је $a = bc \neq 0$, што је и требало показати.

Докажимо јединственост таквог представљања полинома $p(x)$.

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина,

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј.
$p(x) = ap_1(x) \dots p_r(x)$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$,

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$.

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$p(x) = ap_1(x) \quad \Rightarrow$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$p(x) = ap_1(x) \quad \Rightarrow \quad p_1(x) = a^{-1}p(x)$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \dots q_s(x) \end{aligned}$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x) \dots p_r(x)$ и $p(x) = bq_1(x) \dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \end{aligned}$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x)\dots p_r(x)$ и $p(x) = bq_1(x)\dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x)\dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \end{aligned}$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x)\dots p_r(x)$ и $p(x) = bq_1(x)\dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x)\dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \\ &\Rightarrow \quad a^{-1}b = 1 \quad (\text{јер су } p_1(x), q_1(x) \text{ нормирани}) \end{aligned}$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x)\dots p_r(x)$ и $p(x) = bq_1(x)\dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x)\dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \\ &\Rightarrow \quad a^{-1}b = 1 \quad (\text{јер су } p_1(x), q_1(x) \text{ нормирани}) \\ &\Rightarrow \quad a = b, \quad p_1(x) = q_1(x). \end{aligned}$$

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x)\dots p_r(x)$ и $p(x) = bq_1(x)\dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x)\dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \\ &\Rightarrow \quad a^{-1}b = 1 \quad (\text{јер су } p_1(x), q_1(x) \text{ нормирани}) \\ &\Rightarrow \quad a = b, \quad p_1(x) = q_1(x). \end{aligned}$$

- Нека тврђење важи за $r - 1$.

Докажимо јединственост таквог представљања полинома $p(x)$. Нека се полином $p(x)$ може представити бар на два начина, тј. $p(x) = ap_1(x)\dots p_r(x)$ и $p(x) = bq_1(x)\dots q_s(x)$, где је $a \neq 0,\ b \neq 0$ и $p_1(x), \dots, p_r(x), q_1(x), \dots, q_s(x)$ су нормирани и несводљиви полиноми.

Индукцијом по r докажимо да је $a = b, r = s$ и $\{p_1(x), \dots, p_r(x)\} = \{q_1(x), \dots, q_s(x)\}$.

- Нека је $r = 1$. Тада пратећи следеће импликације налазимо да

$$\begin{aligned} p(x) = ap_1(x) \quad &\Rightarrow \quad p_1(x) = a^{-1}p(x) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x)\dots q_s(x) \\ &\Rightarrow \quad s = 1 \quad (\text{јер је } p_1(x) \text{ несводљив}) \\ &\Rightarrow \quad p_1(x) = (a^{-1}b)q_1(x) \\ &\Rightarrow \quad a^{-1}b = 1 \quad (\text{јер су } p_1(x), q_1(x) \text{ нормирани}) \\ &\Rightarrow \quad a = b, \quad p_1(x) = q_1(x). \end{aligned}$$

- Нека тврђење важи за $r - 1$.

- Докажимо да тврђење важи и за r,

- Докажимо да тврђење важи и за r, па имамо да из

$$ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x)$$

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \end{aligned}$$

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \end{aligned}$$ (из Леме 2)

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2)} \end{aligned}$$

Нека важи да $p_1(x) \mid q_1(x)$.

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \end{aligned}$$ (из Леме 2)

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$,

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2)} \end{aligned}$$

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$, па из

$$ap_1(x)p_2(x)\dots p_r(x) \quad = \quad bp_1(x)q_2(x)\dots q_s(x)$$

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2)} \end{aligned}$$

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$, па из

$$\begin{aligned} ap_1(x)p_2(x)\dots p_r(x) &= bp_1(x)q_2(x)\dots q_s(x) \\ \Rightarrow\ a(\underbrace{p_2(x)\dots p_r(x)}_{r-1}) &= b(q_2(x)\dots q_s(x)) \end{aligned}$$

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2)} \end{aligned}$$

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$, па из

$$\begin{aligned} ap_1(x)p_2(x)\dots p_r(x) &= bp_1(x)q_2(x)\dots q_s(x) \\ \Rightarrow\ a(\underbrace{p_2(x)\dots p_r(x)}_{r-1}) &= b(q_2(x)\dots q_s(x)) \\ \Rightarrow\ a = b,\ r = s,\ \{p_2(x),\dots,p_r(x)\} &= \{q_2(x),\dots,q_s(x)\}\ \text{(и.п.)} \end{aligned}$$

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2)} \end{aligned}$$

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$, па из

$$\begin{aligned} ap_1(x)p_2(x)\dots p_r(x) &= bp_1(x)q_2(x)\dots q_s(x) \\ \Rightarrow\ a(\underbrace{p_2(x)\dots p_r(x)}_{r-1}) &= b(q_2(x)\dots q_s(x)) \\ \Rightarrow\ a = b,\ r = s,\ \{p_2(x),\dots,p_r(x)\} &= \{q_2(x),\dots,q_s(x)\} \text{ (и.п.)} \\ \Rightarrow \{p_1(x),\dots,p_r(x)\} &= \{q_1(x),\dots,q_s(x)\}, \end{aligned}$$

што је и требало показати.

- Докажимо да тврђење важи и за r, па имамо да из

$$\begin{aligned} & ap_1(x)\dots p_r(x) = bq_1(x)\dots q_s(x) \\ \Rightarrow \quad & p_1(x) \mid (bq_1(x)\dots q_s(x)) \\ \Rightarrow \quad & p_1(x) \mid q_1(x) \vee p_1(x) \mid q_2(x) \vee \dots \vee p_1(x) \mid q_s(x) \quad \text{(из Леме 2)} \end{aligned}$$

Нека важи да $p_1(x) \mid q_1(x)$. Тада из несводљивости и нормираности полинома $p_1(x)$ и $q_1(x)$ следи $p_1(x) = q_1(x)$, па из

$$\begin{aligned} ap_1(x)p_2(x)\dots p_r(x) &= bp_1(x)q_2(x)\dots q_s(x) \\ \Rightarrow\ a(\underbrace{p_2(x)\dots p_r(x)}_{r-1}) &= b(q_2(x)\dots q_s(x)) \\ \Rightarrow\ a = b,\ r = s,\ \{p_2(x),\dots,p_r(x)\} &= \{q_2(x),\dots,q_s(x)\}\ \text{(и.п.)} \\ \Rightarrow \{p_1(x),\dots,p_r(x)\} &= \{q_1(x),\dots,q_s(x)\}, \end{aligned}$$

што је и требало показати. □

Алгебарски затворена поља

Полиноми карактеришу и поља на известан начин. Из тог разлога имамо класификацију поља на основу следеће дефиниције.

Алгебарски затворена поља

Полиноми карактеришу и поља на известан начин. Из тог разлога имамо класификацију поља на основу следеће дефиниције.

Дефиниција

Поље $\mathbb{F}$ је алгебарски затворено ако сваки полином $p(x) \in \mathbb{F}[x]$, степена $n \geqslant 1$ има бар један корен у $\mathbb{F}$.

Алгебарски затворена поља

Полиноми карактеришу и поља на известан начин. Из тог разлога имамо класификацију поља на основу следеће дефиниције.

Дефиниција

Поље $\mathbb{F}$ је алгебарски затворено ако сваки полином $p(x) \in \mathbb{F}[x]$, степена $n \geqslant 1$ има бар један корен у $\mathbb{F}$.

Пример

Поље $\mathbb{R}$ није алгебарски затворено, нпр. полином $p(x) = x^2 + 1 \in \mathbb{R}[x]$ нема корен у $\mathbb{R}$.

Алгебарски затворена поља

Полиноми карактеришу и поља на известан начин. Из тог разлога имамо класификацију поља на основу следеће дефиниције.

Дефиниција

Поље $\mathbb{F}$ је алгебарски затворено ако сваки полином $p(x) \in \mathbb{F}[x]$, степена $n \geqslant 1$ има бар један корен у $\mathbb{F}$.

Пример

Поље $\mathbb{R}$ није алгебарски затворено, нпр. полином $p(x) = x^2 + 1 \in \mathbb{R}[x]$ нема корен у $\mathbb{R}$.

За разлику од поља реалних бројева које није алгебарски затворено, поље комплексних бројева јесте о чему сведочи следеће тврђење.

Основни став линеарне алгебре. Поље комплексних бројева је алгебарски затворено.

Основни став линеарне алгебре. Поље комплексних бројева је алгебарски затворено.

Сада, можемо описати несводљиве полиноме над алгебарски затвореним пољем.

Основни став линеарне алгебре. Поље комплексних бројева је алгебарски затворено.

Сада, можемо описати несводљиве полиноме над алгебарски затвореним пољем.

Теорема

Следећа тврђења су еквивалентна:

1. *Поље $\mathbb{F}$ је алгебарски затворено.*
2. *Једини несводљиви полиноми у $\mathbb{F}[x]$ су линеарни полиноми.*
3. *Сваки полином $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$ може се факторисати у производ n линеарних полинома (чинилаца).*

Доказ. (1. $\rightarrow$ 2.)

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$,

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.
(2. $\rightarrow$ 3.)

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.
(2. $\rightarrow$ 3.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.
(2. $\rightarrow$ 3.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$. Тада на основу теореме која је дуална Основном ставу аритметике налазимо да је $p(x) = a \cdot p_1(x) \cdot \ldots \cdot p_r(x)$, где су сви $p_i(x)$ нормирани и несводљиви полиноми.

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.
(2. $\rightarrow$ 3.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$. Тада на основу теореме која је дуална Основном ставу аритметике налазимо да је $p(x) = a \cdot p_1(x) \cdot \ldots \cdot p_r(x)$, где су сви $p_i(x)$ нормирани и несводљиви полиноми. Из услова теореме закључујемо да су сви $p_i(x)$ линеарни.

Доказ. (1. $\to$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.
(2. $\to$ 3.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$. Тада на основу теореме која је дуална Основном ставу аритметике налазимо да је $p(x) = a \cdot p_1(x) \cdot \ldots \cdot p_r(x)$, где су сви $p_i(x)$ нормирани и несводљиви полиноми. Из услова теореме закључујемо да су сви $p_i(x)$ линеарни. Како је $\deg p(x) = \deg p_1(x) + \cdots + \deg p_r(x) =$
$= \underbrace{1 + \cdots + 1}_{r}$, следи да је $n = r$,

Доказ. (1. $\rightarrow$ 2.) Претпоставимо да је поље $\mathbb{F}$ алгебарски затворено. Како су линеарни полиноми несводљиви, покажимо да над алгебарски затвореним пољем $\mathbb{F}$ нема других несводљивих полинома. Нека је $p(x) \in \mathbb{F}[x]$, произвољан полином степена већег од један. Искористимо чињеницу да је поље $\mathbb{F}$ алгебарски затворено и закључити да постоји $c \in \mathbb{F}$ такав да је $p(c) = 0$, односно да важи $(x - c) \mid p(x)$. Дакле, имамо да је $p(x) = (x - c)q(x)$, где је $x - c, q(x) \in \mathbb{F}[x]$ и важи $\deg(x - c) = 1 < \deg p(x)$, одакле можемо закључити да је полином $p(x)$ сводљив.
(2. $\rightarrow$ 3.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\deg p(x) = n \geqslant 1$. Тада на основу теореме која је дуална Основном ставу аритметике налазимо да је $p(x) = a \cdot p_1(x) \cdot \ldots \cdot p_r(x)$, где су сви $p_i(x)$ нормирани и несводљиви полиноми. Из услова теореме закључујемо да су сви $p_i(x)$ линеарни. Како је $\deg p(x) = \deg p_1(x) + \cdots + \deg p_r(x) =$
$= \underbrace{1 + \cdots + 1}_{r}$, следи да је $n = r$, па је $p(x)$ производ n линеарних полинома (чинилаца).

(3. $\rightarrow$ 1.)

(3. $\rightarrow$ 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = n \geqslant 1$.

(3. $\rightarrow$ 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = n \geqslant 1$. На основу претпоставке теореме имамо да је $p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ и сви $p_i(x)$ су линеарни.

(3. $\rightarrow$ 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = n \geqslant 1$. На основу претпоставке теореме имамо да је $p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ и сви $p_i(x)$ су линеарни. Претпоставимо да је $p_1(x) = ax + b$, $a \neq 0$.

(3. $\rightarrow$ 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = n \geqslant 1$. На основу претпоставке теореме имамо да је $p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ и сви $p_i(x)$ су линеарни. Претпоставимо да је $p_1(x) = ax + b$, $a \neq 0$. Лако налазимо да је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $p_1(x)$, а тиме и полинома $p(x)$, што је и требало показати. $\square$

(3. $\to$ 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = n \geqslant 1$. На основу претпоставке теореме имамо да је $p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ и сви $p_i(x)$ су линеарни. Претпоставимо да је $p_1(x) = ax + b$, $a \neq 0$. Лако налазимо да је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $p_1(x)$, а тиме и полинома $p(x)$, што је и требало показати. $\square$

Последица 1. Полином $p(c) \in \mathbb{C}[x]$ степена $n \geqslant 1$, са водећим коефицијентом a_n, може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x - c_1)(x - c_2) \cdot \ldots \cdot (x - c_n),$$

где су $c_1, \ldots, c_n$ корени (не морају бити различити) полинома $p(x)$.

(3. $\to$ 1.) Нека је $p(x) \in \mathbb{F}[x]$, такав да је $\mathrm{deg} p(x) = n \geqslant 1$. На основу претпоставке теореме имамо да је $p(x) = p_1(x) \cdot \ldots \cdot p_n(x)$ и сви $p_i(x)$ су линеарни. Претпоставимо да је $p_1(x) = ax + b$, $a \neq 0$. Лако налазимо да је $c = -a^{-1}b \in \mathbb{F}$ корен полинома $p_1(x)$, а тиме и полинома $p(x)$, што је и требало показати. $\square$

Последица 1. Полином $p(c) \in \mathbb{C}[x]$ степена $n \geqslant 1$, са водећим коефицијентом a_n, може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x - c_1)(x - c_2) \cdot \ldots \cdot (x - c_n),$$

где су $c_1, \ldots, c_n$ корени (не морају бити различити) полинома $p(x)$.

Пример

Испитати сводљивост полинома $p(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ *над пољима* $\mathbb{Q}$, $\mathbb{R}$ *и* $\mathbb{C}$, *а затим га представити као производ несводљивих полинома редом, над свим тим пољима.*

Пример

Испитати сводљивост полинома $p(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ *над пољима* $\mathbb{Q}$, $\mathbb{R}$ *и* $\mathbb{C}$, *а затим га представити као производ несводљивих полинома редом, над свим тим пољима. Имамо да је*

$$p(x) = x^6(x-1)+x^4(x-1)+x^2(x-1)+(x-1) = (x-1)(x^6+x^4+x^2+1),$$

Пример

Испитати сводљивост полинома $p(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ *над пољима* $\mathbb{Q}$, $\mathbb{R}$ *и* $\mathbb{C}$, *а затим га представити као производ несводљивих полинома редом, над свим тим пољима. Имамо да је*

$$p(x) = x^6(x-1)+x^4(x-1)+x^2(x-1)+(x-1) = (x-1)(x^6+x^4+x^2+1),$$

где су $x - 1$, $x^6 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$ *полиноми нижег степена од* $p(x)$, *па је* $p(x)$ *сводљив над пољем* $\mathbb{Q}$, *а тиме и над пољима* $\mathbb{R}$ *и* $\mathbb{C}$.

Пример

Испитати сводљивост полинома $p(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ *над пољима* $\mathbb{Q}$, $\mathbb{R}$ *и* $\mathbb{C}$, *а затим га представити као производ несводљивих полинома редом, над свим тим пољима. Имамо да је*

$$p(x) = x^6(x-1)+x^4(x-1)+x^2(x-1)+(x-1) = (x-1)(x^6+x^4+x^2+1),$$

где су $x - 1$, $x^6 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$ *полиноми нижег степена од* $p(x)$, *па је* $p(x)$ *сводљив над пољем* $\mathbb{Q}$, *а тиме и над пољима* $\mathbb{R}$ *и* $\mathbb{C}$.

Даље, покушајмо да дати полином раставимо на седам линеарних фактора у датим пољима.

Пример

Испитати сводљивост полинома $p(x) = x^7 - x^6 + x^5 - x^4 + x^3 - x^2 + x - 1$ *над пољима* $\mathbb{Q}$, $\mathbb{R}$ *и* $\mathbb{C}$, *а затим га представити као производ несводљивих полинома редом, над свим тим пољима. Имамо да је*

$$p(x) = x^6(x-1)+x^4(x-1)+x^2(x-1)+(x-1) = (x-1)(x^6+x^4+x^2+1),$$

где су $x - 1$, $x^6 + x^4 + x^2 + 1 \in \mathbb{Q}[x]$ *полиноми нижег степена од* $p(x)$, *па је* $p(x)$ *сводљив над пољем* $\mathbb{Q}$, *а тиме и над пољима* $\mathbb{R}$ *и* $\mathbb{C}$.

Даље, покушајмо да дати полином раставимо на седам линеарних фактора у датим пољима.

Пример

- *У пољу $\mathbb{Q}$ то није могуће, јер је*

$$p(x) = (x-1)(x^4(x^2+1)+(x^2+1)) = (x-1)(x^2+1)(x^4+1)$$

Пример

- *У пољу $\mathbb{Q}$ то није могуће, јер је*

$$p(x) = (x-1)(x^4(x^2+1)+(x^2+1)) = (x-1)(x^2+1)(x^4+1)$$

факторизација над $\mathbb{Q}$, док полиноми x^2+1 и x^4+1 су несводљиви над $\mathbb{Q}$.

Пример

- *У пољу $\mathbb{Q}$ то није могуће, јер је*

$$p(x) = (x-1)(x^4(x^2+1)+(x^2+1)) = (x-1)(x^2+1)(x^4+1)$$

факторизација над $\mathbb{Q}$, док полиноми x^2+1 и x^4+1 су несводљиви над $\mathbb{Q}$.

- *Ни у пољу реалних бројева то није могуће,*

Пример

- *У пољу $\mathbb{Q}$ то није могуће, јер је*

$$p(x) = (x-1)(x^4(x^2+1)+(x^2+1)) = (x-1)(x^2+1)(x^4+1)$$

факторизација над $\mathbb{Q}$, док полиноми x^2+1 и x^4+1 су несводљиви над $\mathbb{Q}$.

- *Ни у пољу реалних бројева то није могуће, јер је*

$$p(x) = (x-1)(x^2+1)((x^2+1)^2-2x^2)$$

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

факторизација над $\mathbb{R}$, а три квадратана полинома су несводљива.

Пример

- *У пољу $\mathbb{Q}$ то није могуће, јер је*

$$p(x) = (x-1)(x^4(x^2+1)+(x^2+1)) = (x-1)(x^2+1)(x^4+1)$$

факторизација над $\mathbb{Q}$, док полиноми x^2+1 и x^4+1 су несводљиви над $\mathbb{Q}$.

- *Ни у пољу реалних бројева то није могуће, јер је*

$$p(x) = (x-1)(x^2+1)((x^2+1)^2-2x^2)$$

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

факторизација над $\mathbb{R}$, а три квадратана полинома су несводљива.

Пример

- *У пољу комплексних бројева то јесте могуће*

Пример

- *У пољу комплексних бројева то јесте могуће и добијамо да је*

$$p(x) = (x-1)(x+i)(x-i)(x+\frac{\sqrt{2}}{2}(1+i))(x+\frac{\sqrt{2}}{2}(1-i))$$

$$(x-\frac{\sqrt{2}}{2}(1+i))(x-\frac{\sqrt{2}}{2}(1-i))$$

факторизација над $\mathbb{C}$.

Пример

- *У пољу комплексних бројева то јесте могуће и добијамо да је*

$$p(x) = (x-1)(x+i)(x-i)(x+\frac{\sqrt{2}}{2}(1+i))(x+\frac{\sqrt{2}}{2}(1-i))$$

$$(x-\frac{\sqrt{2}}{2}(1+i))(x-\frac{\sqrt{2}}{2}(1-i))$$

факторизација над $\mathbb{C}$.

Вишеструки корени полинома

Ако се у разлагању $p(x) = a_n(x - c_1)(x - c_2)\dots(x - c_n)$ полинома $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$, елемент $c \in \mathbb{F}$ јавља у низу $c_1, \dots, c_n$ тачно k пута, где је $1 \leqslant k \leqslant n$, кажемо да је $c \in \mathbb{F}$ корен реда k полинома $p(x)$.

Вишеструки корени полинома

Ако се у разлагању $p(x) = a_n(x - c_1)(x - c_2)\dots(x - c_n)$ полинома $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$, елемент $c \in \mathbb{F}$ јавља у низу $c_1, \dots, c_n$ тачно k пута, где је $1 \leqslant k \leqslant n$, кажемо да је $c \in \mathbb{F}$ корен реда k полинома $p(x)$.

Дефиниција

Елемент $c \in \mathbb{F}$ је корен реда k полинома $p(x) \in \mathbb{F}[x]$ ако $(x - c)^k \mid p(x)$ и $(x - c)^{k+1} \nmid p(x)$, тј.

$$p(x) = (x - c)^k q(x), \qquad q(x) \in \mathbb{F}[x], \qquad q(c) \neq 0.$$

Вишеструки корени полинома

Ако се у разлагању $p(x) = a_n(x - c_1)(x - c_2)\dots(x - c_n)$ полинома $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$, елемент $c \in \mathbb{F}$ јавља у низу $c_1, \dots, c_n$ тачно k пута, где је $1 \leqslant k \leqslant n$, кажемо да је $c \in \mathbb{F}$ корен реда k полинома $p(x)$.

Дефиниција

Елемент $c \in \mathbb{F}$ је корен реда k полинома $p(x) \in \mathbb{F}[x]$ ако $(x - c)^k \mid p(x)$ и $(x - c)^{k+1} \nmid p(x)$, тј.

$$p(x) = (x - c)^k q(x), \qquad q(x) \in \mathbb{F}[x], \qquad q(c) \neq 0.$$

- Ако је $k > 1$, тада је c вишеструк корен,

Вишеструки корени полинома

Ако се у разлагању $p(x) = a_n(x - c_1)(x - c_2)\dots(x - c_n)$ полинома $p(x) \in \mathbb{F}[x]$ степена $n \geqslant 1$, елемент $c \in \mathbb{F}$ јавља у низу $c_1, \dots, c_n$ тачно k пута, где је $1 \leqslant k \leqslant n$, кажемо да је $c \in \mathbb{F}$ корен реда k полинома $p(x)$.

Дефиниција

Елемент $c \in \mathbb{F}$ је корен реда k полинома $p(x) \in \mathbb{F}[x]$ ако $(x - c)^k \mid p(x)$ и $(x - c)^{k+1} \nmid p(x)$, тј.

$$p(x) = (x - c)^k q(x), \qquad q(x) \in \mathbb{F}[x], \qquad q(c) \neq 0.$$

- Ако је $k > 1$, тада је c вишеструк корен,
- ако је $k = 1$, тада је c прост корен.

Полином $p(x) \in \mathbb{C}[x]$ степена $n \geqslant 1$ са водећим коефицијентом a_n може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x - c_1)^{k_1}(x - c_2)^{k_2} \dots (x - c_r)^{k_r}, \quad a_n \neq 0,$$

где су $c_1, \dots, c_r$ различити корени полинома $p(x)$ реда $k_1, \dots, k_r$, респективно, и важи да је $k_1 + k_2 + \cdots + k_r = n$.

Полином $p(x) \in \mathbb{C}[x]$ степена $n \geqslant 1$ са водећим коефицијентом a_n може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x - c_1)^{k_1}(x - c_2)^{k_2} \dots (x - c_r)^{k_r}, \quad a_n \neq 0,$$

где су $c_1, \dots, c_r$ различити корени полинома $p(x)$ реда $k_1, \dots, k_r$, респективно, и важи да је $k_1 + k_2 + \cdots + k_r = n$.

Теорема

Нека је $\mathbb{F}$ поље, $\mathrm{char}\mathbb{F} = 0$ и $c \in \mathbb{F}$ корен реда k полинома $p(x) \in \mathbb{F}[x]$.

- *Ако је $k > 1$, тада је c корен реда $k - 1$ првог изводног полинома $p'(x)$,*
- *ако је $k = 1$ тада c није корен полинома $p'(x)$.*

Полином $p(x) \in \mathbb{C}[x]$ степена $n \geqslant 1$ са водећим коефицијентом a_n може се на јединствен начин (до редоследа фактора) факторисати у облику

$$p(x) = a_n(x - c_1)^{k_1}(x - c_2)^{k_2} \dots (x - c_r)^{k_r}, \quad a_n \neq 0,$$

где су $c_1, \dots, c_r$ различити корени полинома $p(x)$ реда $k_1, \dots, k_r$, респективно, и важи да је $k_1 + k_2 + \cdots + k_r = n$.

Теорема

Нека је $\mathbb{F}$ поље, $\mathrm{char}\mathbb{F} = 0$ и $c \in \mathbb{F}$ корен реда k полинома $p(x) \in \mathbb{F}[x]$.

- *Ако је $k > 1$, тада је c корен реда $k - 1$ првог изводног полинома $p'(x)$,*
- *ако је $k = 1$ тада c није корен полинома $p'(x)$.*

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$.

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) =$$

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Сада, размотримо следеће случајеве.

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Сада, размотримо следеће случајеве.

- Нека је $k > 1$.

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Сада, размотримо следеће случајеве.

- Нека је $k > 1$. Како је $p'(x) = (x-c)^{k-1}q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да је $c \in \mathbb{F}$ корен реда $k-1$ полинома $p'(x)$.

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Сада, размотримо следеће случајеве.

- Нека је $k > 1$. Како је $p'(x) = (x-c)^{k-1}q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да је $c \in \mathbb{F}$ корен реда $k-1$ полинома $p'(x)$.
- Нека је $k = 1$.

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Сада, размотримо следеће случајеве.

- Нека је $k > 1$. Како је $p'(x) = (x-c)^{k-1}q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да је $c \in \mathbb{F}$ корен реда $k-1$ полинома $p'(x)$.
- Нека је $k = 1$. Из чињенице да је $p'(x) = q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да $c \in \mathbb{F}$ није корен полинома $p'(x)$.

□

Доказ. Нека је $p(x) = (x-c)^k q(x)$, $q(x) \in \mathbb{F}[x]$ и $q(c) \neq 0$. Тада имамо да је

$$p'(x) = k(x-c)^{k-1}q(x) + (x-c)^k q'(x) = (x-c)^{k-1} \underbrace{(kq(x) + (x-c)q'(x))}_{q_1(x)}$$

Сада, размотримо следеће случајеве.

- Нека је $k > 1$. Како је $p'(x) = (x-c)^{k-1}q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да је $c \in \mathbb{F}$ корен реда $k-1$ полинома $p'(x)$.
- Нека је $k = 1$. Из чињенице да је $p'(x) = q_1(x)$ и $q_1(c) = kq(c) \neq 0$ следи да $c \in \mathbb{F}$ није корен полинома $p'(x)$.

□

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$c \in \mathbb{F}$ је вишеструки корен полинома $p(x)$

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$c \in \mathbb{F}$ је вишеструки корен полинома $p(x)$
$\Leftrightarrow$ c је корен полинома $p(x)$ и $p'(x)$ (на основу претходне теореме)

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$$
\begin{aligned}
& c \in \mathbb{F} \text{ је вишеструки корен полинома } p(x) \\
\Leftrightarrow\ & c \text{ је корен полинома } p(x) \text{ и } p'(x) \quad (\text{на основу претходне теореме}) \\
\Leftrightarrow\ & (x-c) \mid p(x), \quad (x-c) \mid p'(x)
\end{aligned}
$$

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$$
\begin{aligned}
& c \in \mathbb{F} \text{ је вишеструки корен полинома } p(x) \\
\Leftrightarrow\ & c \text{ је корен полинома } p(x) \text{ и } p'(x) \quad (\text{на основу претходне теореме}) \\
\Leftrightarrow\ & (x-c) \mid p(x), \quad (x-c) \mid p'(x) \\
\Leftrightarrow\ & (x-c) \mid \mathrm{NZD}(p(x), p'(x))
\end{aligned}
$$

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$$
\begin{aligned}
& c \in \mathbb{F} \text{ је вишеструки корен полинома } p(x) \\
\Leftrightarrow\ & c \text{ је корен полинома } p(x) \text{ и } p'(x) \quad (\text{на основу претходне теореме}) \\
\Leftrightarrow\ & (x-c) \mid p(x), \quad (x-c) \mid p'(x) \\
\Leftrightarrow\ & (x-c) \mid \mathrm{NZD}(p(x), p'(x)) \\
\Leftrightarrow\ & c \text{ је корен полинома } \mathrm{NZD}(p(x), p'(x)).
\end{aligned}
$$

Дакле, важи тврђење последице. □

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$$
\begin{aligned}
& c \in \mathbb{F} \text{ је вишеструки корен полинома } p(x) \\
\Leftrightarrow\ & c \text{ је корен полинома } p(x) \text{ и } p'(x) \quad (\text{на основу претходне теореме}) \\
\Leftrightarrow\ & (x-c) \mid p(x), \quad (x-c) \mid p'(x) \\
\Leftrightarrow\ & (x-c) \mid \mathrm{NZD}(p(x), p'(x)) \\
\Leftrightarrow\ & c \text{ је корен полинома } \mathrm{NZD}(p(x), p'(x)).
\end{aligned}
$$

Дакле, важи тврђење последице. □

Последица 2. Полином $\dfrac{p(x)}{\mathrm{NZD}(p(x), p'(x))}$ има само просте корене и ти корени су различити корени полинома $p(x)$.

Последица 1. Све вишеструке нуле полинома $p(x)$ су све нуле полинома $\mathrm{NZD}(p(x), p'(x))$.

Доказ. Посматрајмо следећи еквиваленцијски ланац.

$$
\begin{aligned}
& c \in \mathbb{F} \text{ је вишеструки корен полинома } p(x) \\
\Leftrightarrow\ & c \text{ је корен полинома } p(x) \text{ и } p'(x) \quad (\text{на основу претходне теореме}) \\
\Leftrightarrow\ & (x-c) \mid p(x), \quad (x-c) \mid p'(x) \\
\Leftrightarrow\ & (x-c) \mid \mathrm{NZD}(p(x), p'(x)) \\
\Leftrightarrow\ & c \text{ је корен полинома } \mathrm{NZD}(p(x), p'(x)).
\end{aligned}
$$

Дакле, важи тврђење последице. □

Последица 2. Полином $\dfrac{p(x)}{\mathrm{NZD}(p(x), p'(x))}$ има само просте корене и ти корени су различити корени полинома $p(x)$.

Пример

Одредити вишеструке корене полинома
$p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1.$

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$.

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$. *Најпре, одредимо* $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$.

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$. *Најпре, одредимо* $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$. *Познатим поступком налазимо да је*

$$\mathrm{NZD}(p(x), p'(x)) = x^3 - x^2 - x + 1 = (x-1)^2(x+1),$$

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$. *Најпре, одредимо* $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$. *Познатим поступком налазимо да је*

$$\mathrm{NZD}(p(x), p'(x)) = x^3 - x^2 - x + 1 = (x-1)^2(x+1),$$

- 1 *и* -1 *су заједнички корени полинома* $p(x)$ *и* $p'(x)$,

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$. *Најпре, одредимо* $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$. *Познатим поступком налазимо да је*

$$\mathrm{NZD}(p(x), p'(x)) = x^3 - x^2 - x + 1 = (x-1)^2(x+1),$$

- 1 *и* -1 *су заједнички корени полинома* $p(x)$ *и* $p'(x)$,
- -1 *је прост корен полинома* $p'(x)$ *и корен реда 2 полинома* $p(x)$,

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$. *Најпре, одредимо* $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$. *Познатим поступком налазимо да је*

$$\mathrm{NZD}(p(x), p'(x)) = x^3 - x^2 - x + 1 = (x-1)^2(x+1),$$

- 1 *и* -1 *су заједнички корени полинома* $p(x)$ *и* $p'(x)$,
- -1 *је прост корен полинома* $p'(x)$ *и корен реда 2 полинома* $p(x)$,
- 1 *је корен реда 2 полинома* $p'(x)$ *и корен реда 3 полинома* $p(x)$,

Пример

Одредити вишеструке корене полинома $p(x) = x^7 - 2x^5 - x^4 + x^3 + 2x^2 - 1$. *Потребно је одредити* $\mathrm{NZD}(p(x), p'(x))$. *Најпре, одредимо* $p'(x) = 7x^6 - 10x^4 - 4x^3 + 3x^2 + 4x$. *Познатим поступком налазимо да је*

$$\mathrm{NZD}(p(x), p'(x)) = x^3 - x^2 - x + 1 = (x-1)^2(x+1),$$

- 1 *и* -1 *су заједнички корени полинома* $p(x)$ *и* $p'(x)$,
- -1 *је прост корен полинома* $p'(x)$ *и корен реда 2 полинома* $p(x)$,
- 1 *је корен реда 2 полинома* $p'(x)$ *и корен реда 3 полинома* $p(x)$,

па је $p(x) = (x-1)^3(x+1)^2 q(x), \qquad \deg q(x) = 2.$

Пример

Из Хорнерове шеме добијамо

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	
-1	1	3	4	3	1	0		

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	
-1	1	3	4	3	1	0		
	1	2	2	1	0			

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	
-1	1	3	4	3	1	0		
	1	2	2	1	0			
	1	1	1	0				

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	
-1	1	3	4	3	1	0		
	1	2	2	1	0			
	1	1	1	0				

па је $q(x) = x^2 + x + 1$, *односно*
$p(x) = (x-1)^3(x+1)^2(x^2+x+1)$.

Пример

Из Хорнерове шеме добијамо

1	1	0	-2	-1	1	2	0	-1
	1	1	-1	-2	-1	1	1	0
	1	2	1	-1	-2	-1	0	
-1	1	3	4	3	1	0		
	1	2	2	1	0			
	1	1	1	0				

па је $q(x) = x^2 + x + 1$, *односно*
$p(x) = (x-1)^3(x+1)^2(x^2+x+1)$.

Заиста, полином $\dfrac{p(x)}{\mathrm{NZD}(p(x), p'(x))} = (x-1)(x+1)(x^2+x+1)$

има само просте корене и то су корени полинома $p(x)$.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

и $\quad a_k = \dfrac{p^{(k)}(0)}{k!}\ (k = 0, 1, \ldots, n),$ *где* $p^{(0)} \overset{\text{def}}{=} p(x).$

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

и $\quad a_k = \dfrac{p^{(k)}(0)}{k!}\ (k = 0, 1, \ldots, n)$, *где* $p^{(0)} \overset{\text{def}}{=} p(x)$.

Доказ. Нека је $p(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n$.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

и $\quad a_k = \dfrac{p^{(k)}(0)}{k!}\ (k = 0, 1, \ldots, n)$, *где* $p^{(0)} \overset{\text{def}}{=} p(x)$.

Доказ. Нека је $p(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n$.
Одредимо коефицијенте $b_0, \ldots, b_n$.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

и $\quad a_k = \dfrac{p^{(k)}(0)}{k!}\ (k = 0, 1, \ldots, n)$, *где* $p^{(0)} \overset{\text{def}}{=} p(x)$.

Доказ. Нека је $p(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n$.
Одредимо коефицијенте $b_0, \ldots, b_n$.
Стављајући да је $x = c$ добијамо да је $b_0 = p(c)$,

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

и $\quad a_k = \dfrac{p^{(k)}(0)}{k!}\ (k = 0, 1, \ldots, n)$, *где* $p^{(0)} \overset{\text{def}}{=} p(x)$.

Доказ. Нека је $p(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n$.
Одредимо коефицијенте $b_0, \ldots, b_n$.
Стављајући да је $x = c$ добијамо да је $b_0 = p(c)$, а то можемо записати у облику $b_0 = \dfrac{p^{(0)}(c)}{0!}$.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0$, $p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ *и* $c \in \mathbb{F}$, *тада је*

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$$

и $\quad a_k = \dfrac{p^{(k)}(0)}{k!}\ (k = 0, 1, \ldots, n)$, *где* $p^{(0)} \overset{\text{def}}{=} p(x)$.

Доказ. Нека је $p(x) = b_0 + b_1(x-c) + b_2(x-c)^2 + \cdots + b_n(x-c)^n$.
Одредимо коефицијенте $b_0, \ldots, b_n$.
Стављајући да је $x = c$ добијамо да је $b_0 = p(c)$, а то можемо записати у облику $b_0 = \dfrac{p^{(0)}(c)}{0!}$.

Сада, одредимо први изводни полином,

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином,

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$,

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Настављајући поступак,

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Настављајући поступак, налазимо да је

$$p^{(k)} = k!b_k + (k+1)!b_{k+1}(x-c) + \cdots + n(n-1)\ldots(n-k+1)b_n(x-c)^{n-k},$$

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Настављајући поступак, налазимо да је

$$p^{(k)} = k!b_k + (k+1)!b_{k+1}(x-c) + \cdots + n(n-1)\ldots(n-k+1)b_n(x-c)^{n-k},$$

па стављајући да је $x = c$ добијамо $p^{(k)}(c) = k!b_k$,

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Настављајући поступак, налазимо да је

$$p^{(k)} = k!b_k + (k+1)!b_{k+1}(x-c) + \cdots + n(n-1)\ldots(n-k+1)b_n(x-c)^{n-k},$$

па стављајући да је $x = c$ добијамо $p^{(k)}(c) = k!b_k$, а то можемо записати у облику $b_k = \dfrac{p^{(k)}(c)}{k!}$, за $k = 0, 1, 2, \ldots, n$.

Сада, одредимо први изводни полином, тј. налазимо да је

$$p'(x) = b_1 + 2b_2(x-c) + 3b_3(x-c)^2 + \cdots + nb_n(x-c)^{n-1},$$

па стављајући да је $x = c$ добијамо $b_1 = p'(c)$, а то можемо записати у облику $b_1 = \dfrac{p'(c)}{1!}$.

Сада, одредимо други изводни полином, тј. налазимо да је

$$p''(x) = 2 \cdot 1 \cdot b_2 + 3 \cdot 2b_3(x-c) + \cdots + n(n-1)b_n(x-c)^{n-2},$$

па стављајући да је $x = c$ добијамо $p''(c) = 2!b_2$, а то можемо записати у облику $b_2 = \dfrac{p''(c)}{2!}$.

Настављајући поступак, налазимо да је

$$p^{(k)} = k!b_k + (k+1)!b_{k+1}(x-c) + \cdots + n(n-1)\ldots(n-k+1)b_n(x-c)^{n-k},$$

па стављајући да је $x = c$ добијамо $p^{(k)}(c) = k!b_k$, а то можемо записати у облику $b_k = \dfrac{p^{(k)}(c)}{k!}$, за $k = 0, 1, 2, \ldots, n$.

Дакле, важи да је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

Дакле, важи да је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

За $c = 0$ добијамо

$$p(x) = p(0) + \frac{p'(0)}{1!}x + \cdots + \frac{p^{(n)}(0)}{n!}x^n.$$

Дакле, важи да је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

За $c = 0$ добијамо

$$p(x) = p(0) + \frac{p'(0)}{1!}x + \cdots + \frac{p^{(n)}(0)}{n!}x^n.$$

Упоређивањем коефицијената са
$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ следи

Дакле, важи да је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

За $c = 0$ добијамо

$$p(x) = p(0) + \frac{p'(0)}{1!}x + \cdots + \frac{p^{(n)}(0)}{n!}x^n.$$

Упоређивањем коефицијената са
$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ следи

$$a_k = \frac{p^{(k)}(0)}{k!} \quad (k = 0, 1, \ldots, n),$$

што је и требало показати. □

Дакле, важи да је

$$p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \frac{p''(c)}{2!}(x-c)^2 + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

За $c = 0$ добијамо

$$p(x) = p(0) + \frac{p'(0)}{1!}x + \cdots + \frac{p^{(n)}(0)}{n!}x^n.$$

Упоређивањем коефицијената са
$p(x) = a_0 + a_1 x + \cdots + a_n x^n \in \mathbb{F}[x]$ следи

$$a_k = \frac{p^{(k)}(0)}{k!} \quad (k = 0, 1, \ldots, n),$$

што је и требало показати. □

Полином из претходне теореме се назива Тејлоров полином.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$, *тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$*, тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$, *тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$. Тада је c корен реда $k-1$ полинома $p'(x)$ итд.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$, *тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \textit{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$. Тада је c корен реда $k-1$ полинома $p'(x)$ итд. Односно, c је прост корен полинома $p^{(k-1)}(x)$ и c није корен полинома $p^{(k)}(x)$.

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$, *тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \textit{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$. Тада је c корен реда $k-1$ полинома $p'(x)$ итд. Односно, c је прост корен полинома $p^{(k-1)}(x)$ и c није корен полинома $p^{(k)}(x)$. Дакле, важи да је

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$, *тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$. Тада је c корен реда $k-1$ полинома $p'(x)$ итд. Односно, c је прост корен полинома $p^{(k-1)}(x)$ и c није корен полинома $p^{(k)}(x)$. Дакле, важи да је

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Обратно,

Теорема

Ако је $\mathbb{F}$ *поље,* $\mathrm{char}\mathbb{F} = 0, p(x) \in \mathbb{F}[x]$ *полином степена* $n \geqslant 1$ *и* $c \in \mathbb{F}$, *тада је* c *корен реда* k *полинома* $p(x)$ *акко је*

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Доказ. Нека је c корен реда k полинома $p(x)$. Тада је c корен реда $k-1$ полинома $p'(x)$ итд. Односно, c је прост корен полинома $p^{(k-1)}(x)$ и c није корен полинома $p^{(k)}(x)$. Дакле, важи да је

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Обратно, нека важи следеће

$$p(c) = p'(c) = \cdots = p^{(k-1)}(c) = 0 \quad \text{и} \quad p^{(k)}(c) \neq 0.$$

Из $p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$

Из $p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$ и $p(c) = \cdots = p^{(k-1)}(c) = 0$ следи да је

$$p(x) = \frac{p^{(k)}(c)}{k!}(x-c)^k + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c)^{k+1} + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

Из $p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$ и $p(c) = \cdots = p^{(k-1)}(c) = 0$ следи да је

$$p(x) = \frac{p^{(k)}(c)}{k!}(x-c)^k + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c)^{k+1} + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

Дакле, имамо облик

$$p(x) = (x-c)^k \left(\underbrace{\frac{p^{(k)}(c)}{k!} + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^{n-k}}_{q(x)} \right)$$

Из $p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$ и $p(c) = \cdots = p^{(k-1)}(c) = 0$ следи да је

$$p(x) = \frac{p^{(k)}(c)}{k!}(x-c)^k + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c)^{k+1} + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

Дакле, имамо облик

$$p(x) = (x-c)^k \left(\underbrace{\frac{p^{(k)}(c)}{k!} + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^{n-k}}_{q(x)} \right)$$

при чему је $q(c) = \frac{p^{(k)}(c)}{k!} \neq 0$, па је c корен реда k полинома $p(x)$.

□

Из $p(x) = p(c) + \frac{p'(c)}{1!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n$ и $p(c) = \cdots = p^{(k-1)}(c) = 0$ следи да је

$$p(x) = \frac{p^{(k)}(c)}{k!}(x-c)^k + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c)^{k+1} + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^n.$$

Дакле, имамо облик

$$p(x) = (x-c)^k \left(\underbrace{\frac{p^{(k)}(c)}{k!} + \frac{p^{(k+1)}(c)}{(k+1)!}(x-c) + \cdots + \frac{p^{(n)}(c)}{n!}(x-c)^{n-k}}_{q(x)} \right)$$

при чему је $q(c) = \frac{p^{(k)}(c)}{k!} \neq 0$, па је c корен реда k полинома $p(x)$.

□

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$p(1) = 0,$

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$p(1) = 0,$
$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$$p(1) = 0,$$
$$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$$
$$p''(x) = 60x^4 - 20x^3 - 156x^2 + 78x + 38, \quad p''(1) = 0,$$

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$$p(1) = 0,$$
$$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$$
$$p''(x) = 60x^4 - 20x^3 - 156x^2 + 78x + 38, \quad p''(1) = 0,$$
$$p'''(x) = 240x^3 - 60x^2 - 312x + 78, \quad p'''(1) = -54 \neq 0,$$

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$$p(1) = 0,$$
$$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$$
$$p''(x) = 60x^4 - 20x^3 - 156x^2 + 78x + 38, \quad p''(1) = 0,$$
$$p'''(x) = 240x^3 - 60x^2 - 312x + 78, \quad p'''(1) = -54 \neq 0,$$

па је $c = 1$ *корен реда* 3 *полинома* $p(x)$.

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$$p(1) = 0,$$
$$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$$
$$p''(x) = 60x^4 - 20x^3 - 156x^2 + 78x + 38, \quad p''(1) = 0,$$
$$p'''(x) = 240x^3 - 60x^2 - 312x + 78, \quad p'''(1) = -54 \neq 0,$$

па је $c = 1$ *корен реда* 3 *полинома* $p(x)$*. Дакле, важи да је* $p(x) = (x-1)^3 q(x)$.

Пример

За полином $p(x) = 2x^6 - x^5 - 13x^4 + 13x^3 + 19x^2 - 32x + 12$ *и* $c = 1$ *важи следеће*

$$p(1) = 0,$$
$$p'(x) = 12x^5 - 5x^4 - 52x^3 + 39x^2 + 38x - 32, \quad p'(1) = 0,$$
$$p''(x) = 60x^4 - 20x^3 - 156x^2 + 78x + 38, \quad p''(1) = 0,$$
$$p'''(x) = 240x^3 - 60x^2 - 312x + 78, \quad p'''(1) = -54 \neq 0,$$

па је $c = 1$ *корен реда* 3 *полинома* $p(x)$. *Дакле, важи да је* $p(x) = (x-1)^3 q(x)$.

Помоћу Хорнерове шеме налазимо $q(x) = 2x^3 + 5x^2 - 4x - 12$, *па је*

$$p(x) = (x-1)^3(2x^3 + 5x^2 - 4x - 12).$$