Линеарна алгебра 1

другo предавање

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

Прстен полинома

Нека је $(\mathbb{F}, +, \cdot, 0, 1)$ поље и $a_0, a_1, \ldots, a_n \in \mathbb{F}$. Нека је операција степеновања уведена на уобичајени начин помоћу
$x^0 = 1, \qquad x^k = xx^{k-1}, \quad k \in \mathbb{N}.$

Прстен полинома

Нека је $(\mathbb{F}, +, \cdot, 0, 1)$ поље и $a_0, a_1, \ldots, a_n \in \mathbb{F}$. Нека је операција степеновања уведена на уобичајени начин помоћу
$x^0 = 1, \qquad x^k = xx^{k-1}, \quad k \in \mathbb{N}.$

Дефиниција

Ако $x \in \mathbb{F}$ и $n \in \mathbb{N} \cup \{0\}$, $a_0, a_1, \ldots, a_n \in \mathbb{F}$, формални израз

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

назива се алгебарски полином по x над пољем $\mathbb{F}$.

Прстен полинома

Нека је $(\mathbb{F}, +, \cdot, 0, 1)$ поље и $a_0, a_1, \dots, a_n \in \mathbb{F}$. Нека је операција степеновања уведена на уобичајени начин помоћу
$x^0 = 1, \qquad x^k = xx^{k-1}, \quad k \in \mathbb{N}.$

Дефиниција

Ако $x \in \mathbb{F}$ и $n \in \mathbb{N} \cup \{0\}$, $a_0, a_1, \dots, a_n \in \mathbb{F}$, формални израз

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

назива се алгебарски полином по x над пољем $\mathbb{F}$. За елементе a_k кажемо да су коефицијенти полинома $p(x)$.

Прстен полинома

Нека је $(\mathbb{F}, +, \cdot, 0, 1)$ поље и $a_0, a_1, \ldots, a_n \in \mathbb{F}$. Нека је операција степеновања уведена на уобичајени начин помоћу
$x^0 = 1, \qquad x^k = xx^{k-1}, \quad k \in \mathbb{N}$.

Дефиниција

Ако $x \in \mathbb{F}$ и $n \in \mathbb{N} \cup \{0\}$, $a_0, a_1, \ldots, a_n \in \mathbb{F}$, формални израз

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

назива се алгебарски полином по x над пољем $\mathbb{F}$. За елементе a_k кажемо да су коефицијенти полинома $p(x)$. Ако је коефицијент $a_n \neq 0$, за полином $p(x)$ кажемо да је степена n и то означавамо са $\deg p(x) = n$.

Прстен полинома

Нека је $(\mathbb{F}, +, \cdot, 0, 1)$ поље и $a_0, a_1, \ldots, a_n \in \mathbb{F}$. Нека је операција степеновања уведена на уобичајени начин помоћу
$x^0 = 1, \qquad x^k = xx^{k-1}, \quad k \in \mathbb{N}.$

Дефиниција

Ако $x \in \mathbb{F}$ и $n \in \mathbb{N} \cup \{0\}$, $a_0, a_1, \ldots, a_n \in \mathbb{F}$, формални израз

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n,$$

назива се алгебарски полином по x над пољем $\mathbb{F}$. За елементе a_k кажемо да су коефицијенти полинома $p(x)$. Ако је коефицијент $a_n \neq 0$, за полином $p(x)$ кажемо да је степена n и то означавамо са $\deg p(x) = n$. За коефицијент $a_n \neq 0$ кажемо да је водећи или најстарији коефицијент полинома $p(x)$.

Дефиниција

За полином $O(x) = 0 + 0x + \cdots + 0x^{n-1} + 0x^n$ *кажемо да је нула полином и означавамо га просто са* 0.

Дефиниција

За полином $O(x) = 0 + 0x + \cdots + 0x^{n-1} + 0x^n$ кажемо да је нула полином и означавамо га просто са 0.

Степен нула полинома $O(x)$ се не дефинише.

Дефиниција

За полином $O(x) = 0 + 0x + \cdots + 0x^{n-1} + 0x^n$ *кажемо да је нула полином и означавамо га просто са* 0.

Степен нула полинома $O(x)$ се не дефинише.
Полиноми степена нула се називају константе и то су елементи поља $\mathbb{F}$.

Дефиниција

За полином $O(x) = 0 + 0x + \cdots + 0x^{n-1} + 0x^n$ *кажемо да је нула полином и означавамо га просто са* 0.

Степен нула полинома $O(x)$ се не дефинише.
Полиноми степена нула се називају константе и то су елементи поља $\mathbb{F}$.

Дефиниција

За полином чији је водећи коефицијент једнак јединици кажемо да је нормиран (моничан).

Дефиниција

За полином $O(x) = 0 + 0x + \cdots + 0x^{n-1} + 0x^n$ *кажемо да је нула полином и означавамо га просто са* 0.

Степен нула полинома $O(x)$ се не дефинише.
Полиноми степена нула се називају константе и то су елементи поља $\mathbb{F}$.

Дефиниција

За полином чији је водећи коефицијент једнак јединици кажемо да је нормиран (моничан).

Дакле, нормирани полином има облик

$$p(x) = a_0 + a_1 x + \cdots + a_{(n-1)} x^{n-1} + x^n.$$

Скуп свих полинома над пољем $\mathbb{F}$ означавамо са $\mathbb{F}[x]$.

Скуп свих полинома над пољем $\mathbb{F}$ означавамо са $\mathbb{F}[x]$.
Од интереса је често уочити скуп свих оних полинома чији степен није већи од n. Тај подскуп ћемо означавати са $\mathbb{F}_n[x]$.

Скуп свих полинома над пољем $\mathbb{F}$ означавамо са $\mathbb{F}[x]$.

Од интереса је често уочити скуп свих оних полинома чији степен није већи од n. Тај подскуп ћемо означавати са $\mathbb{F}_n[x]$. Произвољни полином из $\mathbb{F}_n[x]$ има облик $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, при чему ако је $\deg p(x) = m < n$ имамо да је $a_{m+1} = \cdots = a_n = 0$.

Скуп свих полинома над пољем $\mathbb{F}$ означавамо са $\mathbb{F}[x]$.
Од интереса је често уочити скуп свих оних полинома чији степен није већи од n. Тај подскуп ћемо означавати са $\mathbb{F}_n[x]$. Произвољни полином из $\mathbb{F}_n[x]$ има облик $p(x) = a_0 + a_1 x + \cdots + a_n x^n$, при чему ако је $\deg p(x) = m < n$ имамо да је $a_{m+1} = \cdots = a_n = 0$.
У скуп $\mathbb{F}[x]$ можемо увести релацију једнакост као и операције: сабирање и множење полинома на следећи начин:

Скуп свих полинома над пољем $\mathbb{F}$ означавамо са $\mathbb{F}[x]$.
Од интереса је често уочити скуп свих оних полинома чији степен није већи од n. Тај подскуп ћемо означавати са $\mathbb{F}_n[x]$. Произвољни полином из $\mathbb{F}_n[x]$ има облик $p(x) = a_0 + a_1x + \cdots + a_nx^n$, при чему ако је $\deg p(x) = m < n$ имамо да је $a_{m+1} = \cdots = a_n = 0$.
У скуп $\mathbb{F}[x]$ можемо увести релацију једнакост као и операције: сабирање и множење полинома на следећи начин:

Дефиниција

Полиноми

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \quad \text{и} \quad q(x) = b_0 + b_1x + \cdots + b_mx^m$$

су једнаки ако и само ако је $a_k = b_k$ за свако $k \geqslant 0$, тј. када су њихови коефицијенти једнаки.

Дефиниција

За два полинома

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \ \text{ и } \ q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

збир и производ су редом

$$(p+q)(x) = p(x) + q(x) = c_0 + c_1 x + \cdots + c_r x^r$$

Дефиниција

За два полинома

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \text{ и } q(x) = b_0 + b_1x + \cdots + b_mx^m$$

збир и производ су редом

$$(p+q)(x) = p(x) + q(x) = c_0 + c_1x + \cdots + c_rx^r$$

и $(pq)(x) = p(x)q(x) = d_0 + d_1x + \cdots + d_sx^s$

Дефиниција

За два полинома

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ и } q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

збир и производ су редом

$$(p+q)(x) = p(x) + q(x) = c_0 + c_1 x + \cdots + c_r x^r$$

и $(pq)(x) = p(x)q(x) = d_0 + d_1 x + \cdots + d_s x^s$ где су

$$c_k = a_k + b_k, \quad 0 \leqslant k \leqslant r = \max\{n, m\},$$

Дефиниција

За два полинома

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ и } q(x) = b_0 + b_1 x + \cdots + b_m x^m$$

збир и производ су редом

$$(p+q)(x) = p(x) + q(x) = c_0 + c_1 x + \cdots + c_r x^r$$

и $(pq)(x) = p(x)q(x) = d_0 + d_1 x + \cdots + d_s x^s$ *где су*

$$c_k = a_k + b_k, \quad 0 \leqslant k \leqslant r = \max\{n, m\},$$

и

$$d_k = \sum_{i=0}^{k} a_i b_{k-i}, \quad 0 \leqslant k \leqslant s = n + m.$$

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$.

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$.
Напоменимо да за ненула полиноме $p(x)$ и $q(x)$ важи

$$\deg(pq)(x) = \deg p(x) + \deg q(x).$$

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$.
Напоменимо да за ненула полиноме $p(x)$ и $q(x)$ важи

$$\deg(pq)(x) = \deg p(x) + \deg q(x).$$

Такође, ако $p(x), q(x) \in \mathbb{F}[x]$ и $p(x) + q(x) \neq 0$, тада је

$$\deg(p+q)(x) \leqslant \max\{\deg p(x), \deg q(x)\}.$$

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$.

Напоменимо да за ненула полиноме $p(x)$ и $q(x)$ важи

$$\deg(pq)(x) = \deg p(x) + \deg q(x).$$

Такође, ако $p(x), q(x) \in \mathbb{F}[x]$ и $p(x) + q(x) \neq 0$, тада је

$$\deg(p+q)(x) \leqslant \max\{\deg p(x), \deg q(x)\}.$$

Као специјалан случај производа полинома имамо производ полинома $p(x)$ скаларом $\alpha \in \mathbb{F}$, који се може третирати као полином нултог степена.

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$.
Напоменимо да за ненула полиноме $p(x)$ и $q(x)$ важи

$$\deg(pq)(x) = \deg p(x) + \deg q(x).$$

Такође, ако $p(x), q(x) \in \mathbb{F}[x]$ и $p(x) + q(x) \neq 0$, тада је

$$\deg(p+q)(x) \leqslant \max\{\deg p(x), \deg q(x)\}.$$

Као специјалан случај производа полинома имамо производ полинома $p(x)$ скаларом $\alpha \in \mathbb{F}$, који се може третирати као полином нултог степена. Дакле,

$$\alpha p(x) = \alpha(a_0 + a_1 x + \cdots + a_n x^n) = (\alpha a_0) + (\alpha a_1)x + \cdots + (\alpha a_n)x^n.$$

Дакле, ако $p(x) \in \mathbb{F}_n[x]$ и $q(x) \in \mathbb{F}_m[x]$, тада $(p+q)(x) \in \mathbb{F}_r[x]$ и $(pq)(x) \in \mathbb{F}_s[x]$, где су $r = \max\{n, m\}$ и $s = n + m$.
Напоменимо да за ненула полиноме $p(x)$ и $q(x)$ важи

$$\deg(pq)(x) = \deg p(x) + \deg q(x).$$

Такође, ако $p(x), q(x) \in \mathbb{F}[x]$ и $p(x) + q(x) \neq 0$, тада је

$$\deg(p+q)(x) \leqslant \max\{\deg p(x), \deg q(x)\}.$$

Као специјалан случај производа полинома имамо производ полинома $p(x)$ скаларом $\alpha \in \mathbb{F}$, који се може третирати као полином нултог степена. Дакле,

$$\alpha p(x) = \alpha(a_0 + a_1 x + \cdots + a_n x^n) = (\alpha a_0) + (\alpha a_1)x + \cdots + (\alpha a_n)x^n.$$

Теорема

$(\mathbb{F}[x], +, \cdot)$ *је интегрални домен (комутативан прстен са јединицом без делилаца нуле).*

Доказ.

(P_1) $(F[x], +)$ је Абелова група.

Доказ.

(P_1) $(F[x], +)$ је Абелова група.

Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$.

Доказ.
(P_1) $(F[x], +)$ је Абелова група.
Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$.
Неутрални за сабирање је нула полином,

Доказ.
(P_1) $(F[x], +)$ је Абелова група.
Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$.
Неутрални за сабирање је нула полином, а супротни (инверзни) полином за полином $p(x) = a_0 + a_1x + \cdots + a_nx^n$ је полином $-p(x) = -a_0 + (-a_1)x + \cdots + (-a_n)x^n$.

Доказ.

(P_1) $(F[x], +)$ је Абелова група.

Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$. Неутрални за сабирање је нула полином, а супротни (инверзни) полином за полином $p(x) = a_0 + a_1x + \cdots + a_nx^n$ је полином $-p(x) = -a_0 + (-a_1)x + \cdots + (-a_n)x^n$.

(P_2) Асоцијативност множења полинома следи из дефиниције операције $\cdot$, асоцијативности множења у $\mathbb{F}$ и дистрибутивности $\cdot$ према $+$ у $\mathbb{F}$.

Доказ.
(P_1) $(F[x], +)$ је Абелова група.
Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$.
Неутрални за сабирање је нула полином, а супротни (инверзни) полином за полином $p(x) = a_0 + a_1x + \cdots + a_nx^n$ је полином $-p(x) = -a_0 + (-a_1)x + \cdots + (-a_n)x^n$.

(P_2) Асоцијативност множења полинома следи из дефиниције операције $\cdot$, асоцијативности множења у $\mathbb{F}$ и дистрибутивности $\cdot$ према $+$ у $\mathbb{F}$.

(P_3) Дистрибутивност $\cdot$ према $+$ следи из дистрибутивности $+$ и $\cdot$ у пољу $\mathbb{F}$.

Доказ.
(P_1) $(F[x], +)$ је Абелова група.
Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$.
Неутрални за сабирање је нула полином, а супротни (инверзни) полином за полином $p(x) = a_0 + a_1x + \cdots + a_nx^n$ је полином $-p(x) = -a_0 + (-a_1)x + \cdots + (-a_n)x^n$.

(P_2) Асоцијативност множења полинома следи из дефиниције операције $\cdot$, асоцијативности множења у $\mathbb{F}$ и дистрибутивности $\cdot$ према $+$ у $\mathbb{F}$.

(P_3) Дистрибутивност $\cdot$ према $+$ следи из дистрибутивности $+$ и $\cdot$ у пољу $\mathbb{F}$. Неутрални за множење је константни полином 1.

Доказ.
(P_1) $(F[x], +)$ је Абелова група.
Комутативност и асоцијативност сабирања полинома следе из дефиниције сабирања полинома и особина сабирања у пољу $\mathbb{F}$.
Неутрални за сабирање је нула полином, а супротни (инверзни) полином за полином $p(x) = a_0 + a_1 x + \cdots + a_n x^n$ је полином $-p(x) = -a_0 + (-a_1)x + \cdots + (-a_n)x^n$.

(P_2) Асоцијативност множења полинома следи из дефиниције операције $\cdot$, асоцијативности множења у $\mathbb{F}$ и дистрибутивности $\cdot$ према $+$ у $\mathbb{F}$.

(P_3) Дистрибутивност $\cdot$ према $+$ следи из дистрибутивности $+$ и $\cdot$ у пољу $\mathbb{F}$. Неутрални за множење је константни полином 1.

Дакле, $F[x]$ је комутативан прстен са јединицом.

Доказ.

Докажимо да $F[x]$ нема делиоце нуле, тј. да производ два ненула полинома не може бити нула полином.

Доказ.
Докажимо да $F[x]$ нема делиоце нуле, тј. да производ два ненула полинома не може бити нула полином.

Нека су $p(x), q(x) \in F[x], p(x) \neq 0,\ q(x) \neq 0.$

Доказ.

Докажимо да $F[x]$ нема делиоце нуле, тј. да производ два ненула полинома не може бити нула полином.

Нека су $p(x), q(x) \in F[x], p(x) \neq 0,\ q(x) \neq 0.$

Тада постоји $\mathrm{deg} p(x) = m, \mathrm{deg} q(x) = n, m, n \in \mathbb{N} \cup \{0\}$, па следи да је $\deg(p(x)q(x)) = \mathrm{deg} p(x) + \mathrm{deg} q(x) = n + m$.

Доказ.
Докажимо да $F[x]$ нема делиоце нуле, тј. да производ два ненула полинома не може бити нула полином.

Нека су $p(x), q(x) \in F[x], p(x) \neq 0,\ q(x) \neq 0$.
Тада постоји $\deg p(x) = m, \deg q(x) = n, m, n \in \mathbb{N} \cup \{0\}$, па следи да је $\deg(p(x)q(x)) = \deg p(x) + \deg q(x) = n + m$.
Дакле, полином $p(x)q(x)$ има степен, па је $p(x)q(x) \neq 0$.

Доказ.

Докажимо да $F[x]$ нема делиоце нуле, тј. да производ два ненула полинома не може бити нула полином.

Нека су $p(x), q(x) \in F[x]$, $p(x) \neq 0,\ q(x) \neq 0.$
Тада постоји $\mathrm{deg} p(x) = m$, $\mathrm{deg} q(x) = n$, $m, n \in \mathbb{N} \cup \{0\}$, па следи да је $\deg(p(x)q(x)) = \mathrm{deg} p(x) + \mathrm{deg} q(x) = n + m$.
Дакле, полином $p(x)q(x)$ има степен, па је $p(x)q(x) \neq 0$.

Закључујемо да је $F[x]$ комутативан прстен са јединицом без делилаца нуле, тј. $F[x]$ је интегрални домен. $\square$

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Теорема

Елемент $p(x) \in F[x]$, $p(x) \neq 0$, *има инверзни акко је* $\deg p(x) = 0$, *тј.* $p(x)$ *је ненула константни полином.*

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Теорема

Елемент $p(x) \in F[x]$, $p(x) \neq 0$, *има инверзни акко је* $\mathrm{deg} p(x) = 0$, *тј.* $p(x)$ *је ненула константни полином.*

Доказ. Нека $p(x)$ има инверзни и нека је то $q(x) \in \mathbb{F}[x]$.

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Теорема

Елемент $p(x) \in F[x],\ p(x) \neq 0$, *има инверзни акко је* $\mathrm{deg} p(x) = 0$, *тј.* $p(x)$ *је ненула константни полином.*

Доказ. Нека $p(x)$ има инверзни и нека је то $q(x) \in \mathbb{F}[x]$.
Тада је $p(x)q(x) = q(x)p(x) = 1$.

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Теорема

Елемент $p(x) \in F[x]$, $p(x) \neq 0$, *има инверзни акко је* $\deg p(x) = 0$, *тј.* $p(x)$ *је ненула константни полином.*

Доказ. Нека $p(x)$ има инверзни и нека је то $q(x) \in \mathbb{F}[x]$.
Тада је $p(x)q(x) = q(x)p(x) = 1$.
Претпоставимо да је $\deg p(x) \geqslant 1$.

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Теорема

Елемент $p(x) \in F[x]$, $p(x) \neq 0$, *има инверзни акко је* $\deg p(x) = 0$, *тј.* $p(x)$ *је ненула константни полином.*

Доказ. Нека $p(x)$ има инверзни и нека је то $q(x) \in \mathbb{F}[x]$.
Тада је $p(x)q(x) = q(x)p(x) = 1$.
Претпоставимо да је $\deg p(x) \geqslant 1$. Тада је
$0 = \deg(1) = \deg(p(x)q(x)) = \deg p(x) + \deg q(x) \geqslant 1$, што је контрадикција.

Пример

Имамо да је $(\mathbb{R}[x], +, \cdot)$ *прстен реалних полинома, а* $(\mathbb{C}[x], +, \cdot)$ *прстен комплексних полинома. За такве скупове полинома важи* $\mathbb{R}[x] \subset \mathbb{C}[x]$.

Теорема

Елемент $p(x) \in F[x]$, $p(x) \neq 0$, *има инверзни акко је* $\deg p(x) = 0$, *тј.* $p(x)$ *је ненула константни полином.*

Доказ. Нека $p(x)$ има инверзни и нека је то $q(x) \in \mathbb{F}[x]$.
Тада је $p(x)q(x) = q(x)p(x) = 1$.
Претпоставимо да је $\deg p(x) \geqslant 1$. Тада је
$0 = \deg(1) = \deg(p(x)q(x)) = \deg p(x) + \deg q(x) \geqslant 1$, што је контрадикција.
Дакле, следи да је $\deg p(x) = 0$.

Доказ. Обратно, нека је $p(x)$ ненула константни полином.

Доказ. Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x) = a_0,\ a_0 \in \mathbb{F},\ a_0 \neq 0.$

Доказ. Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x) = a_0,\ a_0 \in \mathbb{F},\ a_0 \neq 0$. Тада постоји $a_0^{-1} \in \mathbb{F}$ (инверзни од a_0 у односу на операцију $\cdot$ у пољу $\mathbb{F}$).

Доказ. Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x) = a_0,\ a_0 \in \mathbb{F},\ a_0 \neq 0$. Тада постоји $a_0^{-1} \in \mathbb{F}$ (инверзни од a_0 у односу на операцију $\cdot$ у пољу $\mathbb{F}$). За $q(x) = a_0^{-1} \in \mathbb{F} \subseteq \mathbb{F}[x]$ важи $p(x)q(x) = a_0 \cdot a_0^{-1} = 1$.

Доказ. Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x) = a_0,\ a_0 \in \mathbb{F},\ a_0 \neq 0$. Тада постоји $a_0^{-1} \in \mathbb{F}$ (инверзни од a_0 у односу на операцију $\cdot$ у пољу $\mathbb{F}$). За $q(x) = a_0^{-1} \in \mathbb{F} \subseteq \mathbb{F}[x]$ важи $p(x)q(x) = a_0 \cdot a_0^{-1} = 1$. Следи да је $q(x)$ инверзни од $p(x)$ у $\mathbb{F}[x]$. $\square$

На крају овог одељка укажимо на важну чињеницу да се полином може третирати и као функција.

Доказ. Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x) = a_0,\ a_0 \in \mathbb{F},\ a_0 \neq 0$. Тада постоји $a_0^{-1} \in \mathbb{F}$ (инверзни од a_0 у односу на операцију $\cdot$ у пољу $\mathbb{F}$). За $q(x) = a_0^{-1} \in \mathbb{F} \subseteq \mathbb{F}[x]$ важи $p(x)q(x) = a_0 \cdot a_0^{-1} = 1$. Следи да је $q(x)$ инверзни од $p(x)$ у $\mathbb{F}[x]$. $\square$

На крају овог одељка укажимо на важну чињеницу да се полином може третирати и као функција. Наиме, на основу дефиниције полинома може се дефинисати пресликавање $f : \mathbb{F} \to \mathbb{F}$, помоћу

$$f(c) = a_0 + a_1 c + \cdots + a_n c^n \in \mathbb{F}.$$

Доказ. Обратно, нека је $p(x)$ ненула константни полином. То значи $p(x) = a_0,\ a_0 \in \mathbb{F},\ a_0 \neq 0$. Тада постоји $a_0^{-1} \in \mathbb{F}$ (инверзни од a_0 у односу на операцију $\cdot$ у пољу $\mathbb{F}$). За $q(x) = a_0^{-1} \in \mathbb{F} \subseteq \mathbb{F}[x]$ важи $p(x)q(x) = a_0 \cdot a_0^{-1} = 1$. Следи да је $q(x)$ инверзни од $p(x)$ у $\mathbb{F}[x]$. $\square$

На крају овог одељка укажимо на важну чињеницу да се полином може третирати и као функција. Наиме, на основу дефиниције полинома може се дефинисати пресликавање $f : \mathbb{F} \to \mathbb{F}$, помоћу

$$f(c) = a_0 + a_1 c + \cdots + a_n c^n \in \mathbb{F}.$$

Пресликавање f називамо полиномска (полиномна) функција.

Дељивост полинома

Дефиниција

Ако важи $p(c) = 0$ *онда се* c *назива нула или корен полинома* $p(x)$.

Дељивост полинома

Дефиниција

Ако важи $p(c) = 0$ онда се c назива нула или корен полинома $p(x)$.

Једначина $a_0 + a_1 x + \cdots + a_n x^n = 0$ ($a_n \neq 0$) се назива алгебарска једначина n-тог степена.

Дељивост полинома

Дефиниција

Ако важи $p(c) = 0$ *онда се* c *назива нула или корен полинома* $p(x)$.

Једначина $a_0 + a_1x + \cdots + a_nx^n = 0$ ($a_n \neq 0$) се назива алгебарска једначина n-тог степена.

$n = 1: \quad a_0 + a_1x = 0$ ($a_1 \neq 0$) - линеарна једначина;

Дељивост полинома

Дефиниција

Ако важи $p(c) = 0$ онда се c назива нула или корен полинома $p(x)$.

Једначина $a_0 + a_1x + \cdots + a_nx^n = 0$ ($a_n \neq 0$) се назива алгебарска једначина n-тог степена.

$n = 1 : \quad a_0 + a_1x = 0$ ($a_1 \neq 0$) - линеарна једначина;

$n = 2 : \quad a_0 + a_1x + a_2x^2 = 0$ ($a_2 \neq 0$) - квадратна једначина.

Пример

(a) *Нула полинома* $p(x) = 2 - 3x + x^3$, $p(x) \in \mathbb{R}[x]$ *је број* -2, *јер* $p(-2) = 2 - 3(-2) + (-2)^3 = 0.$

Пример

(а) *Нула полинома* $p(x) = 2 - 3x + x^3$, $p(x) \in \mathbb{R}[x]$ *је број* -2, *јер* $p(-2) = 2 - 3(-2) + (-2)^3 = 0$.

(б) *Полином* $q(x) = x^2 + 1$, $q(x) \in \mathbb{R}[x]$, *нема нуле (у* $\mathbb{R}$*)*.

Пример

(а) *Нула полинома* $p(x) = 2 - 3x + x^3$, $p(x) \in \mathbb{R}[x]$ *је број* -2, *јер* $p(-2) = 2 - 3(-2) + (-2)^3 = 0$.

(б) *Полином* $q(x) = x^2 + 1$, $q(x) \in \mathbb{R}[x]$, *нема нуле (у* $\mathbb{R}$*).*

(в) *Полином* $q(x) = x^2 + 1$, $f \in \mathbb{C}[x]$, *има нуле* i *и* $-i$.

Пример

(а) *Нула полинома* $p(x) = 2 - 3x + x^3$, $p(x) \in \mathbb{R}[x]$ *је број* -2, *јер* $p(-2) = 2 - 3(-2) + (-2)^3 = 0$.

(б) *Полином* $q(x) = x^2 + 1$, $q(x) \in \mathbb{R}[x]$, *нема нуле (у* $\mathbb{R}$*).*

(в) *Полином* $q(x) = x^2 + 1$, $f \in \mathbb{C}[x]$, *има нуле* i *и* $-i$.

Теорема

За сваки полином $p(x)$ *и сваки ненула полином* $q(x)$, *постоје јединствени полиноми* $s(x)$ *и* $r(x)$ *такви да важи једнакост*

$$p(x) = s(x)q(x) + r(x),$$

при чему је $r(x)$ *нула полином или* $\deg r(x) < \deg q(x)$.

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно,

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно, и да су

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \text{ и } q(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно, и да су

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{и} \quad q(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

Ако је $n < m$ или $p(x) = 0$, тада једнакост важи са $s(x) = 0$ и $r(x) = p(x)$.

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно, и да су

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \quad \text{и} \quad q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Ако је $n < m$ или $p(x) = 0$, тада једнакост важи са $s(x) = 0$ и $r(x) = p(x)$.
Претпоставимо зато да је $n \geqslant m$.

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно, и да су

$$p(x) = a_0 + a_1x + \cdots + a_nx^n \text{ и } q(x) = b_0 + b_1x + \cdots + b_mx^m.$$

Ако је $n < m$ или $p(x) = 0$, тада једнакост важи са $s(x) = 0$ и $r(x) = p(x)$.
Претпоставимо зато да је $n \geqslant m$. Посматрајмо полином

$$p_1(x) = p(x) - \frac{a_n}{b_m}x^{n-m}q(x),$$

чији је степен, очигледно, мањи од n.

Доказ. Претпоставимо да $p(x)$ и $q(x)$ имају степене n и m, респективно, и да су

$$p(x) = a_0 + a_1 x + \cdots + a_n x^n \quad \text{и} \quad q(x) = b_0 + b_1 x + \cdots + b_m x^m.$$

Ако је $n < m$ или $p(x) = 0$, тада једнакост важи са $s(x) = 0$ и $r(x) = p(x)$.
Претпоставимо зато да је $n \geqslant m$. Посматрајмо полином

$$p_1(x) = p(x) - \frac{a_n}{b_m} x^{n-m} q(x),$$

чији је степен, очигледно, мањи од n. Са n_1 означимо тај степен, а са $a_{n_1}^{(1)}$ најстарији коефицијент полинома $p_1(x)$.

Доказ. Ако је $n_1 \geqslant m$ ставимо даље

$$p_2(x) = p_1(x) - \frac{a_{n_1}^{(1)}}{b_m} x^{n_1 - m} q(x),$$

и са n_2 и $a_{n_2}^{(2)}$ означимо степен и најстарији коефицијент овог полинома, респективно.

Доказ. Ако је $n_1 \geqslant m$ ставимо даље

$$p_2(x) = p_1(x) - \frac{a_{n_1}^{(1)}}{b_m} x^{n_1 - m} q(x),$$

и са n_2 и $a_{n_2}^{(2)}$ означимо степен и најстарији коефицијент овог полинома, респективно. Процес настављамо ако је $n_2 \geqslant m$.

Доказ. Ако је $n_1 \geqslant m$ ставимо даље

$$p_2(x) = p_1(x) - \frac{a_{n_1}^{(1)}}{b_m} x^{n_1 - m} q(x),$$

и са n_2 и $a_{n_2}^{(2)}$ означимо степен и најстарији коефицијент овог полинома, респективно. Процес настављамо ако је $n_2 \geqslant m$. Јасно је да степени полинома $p_1(x), p_2(x), \ldots$ опадају и да после коначног броја корака добијамо једнакост

$$p_k(x) = p_{k-1}(x) - \frac{a_{n_{k-1}}^{(k-1)}}{b_m} x^{n_{k-1} - m} q(x),$$

Доказ. Ако је $n_1 \geqslant m$ ставимо даље

$$p_2(x) = p_1(x) - \frac{a_{n_1}^{(1)}}{b_m} x^{n_1 - m} q(x),$$

и са n_2 и $a_{n_2}^{(2)}$ означимо степен и најстарији коефицијент овог полинома, респективно. Процес настављамо ако је $n_2 \geqslant m$. Јасно је да степени полинома $p_1(x), p_2(x), \ldots$ опадају и да после коначног броја корака добијамо једнакост

$$p_k(x) = p_{k-1}(x) - \frac{a_{n_{k-1}}^{(k-1)}}{b_m} x^{n_{k-1} - m} q(x),$$

у којој је $p_k(x)$ нула полином или такав да му је степен n_k мањи од m.

Доказ. У том случају процес прекидамо, а $p_k(x)$ се, коришћењем претходних једнакости, може представити у облику $p_k(x) = p(x) - s(x)q(x)$, где смо ставили

$$s(x) = \frac{a_n}{b_m}x^{n-m} + \frac{a_{n_1}^{(1)}}{b_m}x^{n_1-m} + \cdots + \frac{a_{n_{k-1}}^{(k-1)}}{b_m}x^{n_{k-1}-m}.$$

Доказ. У том случају процес прекидамо, а $p_k(x)$ се, коришћењем претходних једнакости, може представити у облику $p_k(x) = p(x) - s(x)q(x)$, где смо ставили

$$s(x) = \frac{a_n}{b_m}x^{n-m} + \frac{a_{n_1}^{(1)}}{b_m}x^{n_1-m} + \cdots + \frac{a_{n_{k-1}}^{(k-1)}}{b_m}x^{n_{k-1}-m}.$$

Дакле, овај полином $s(x)$ и $r(x) = p_k(x)$ задовољавају једнакост, при чему је $r(x)$ нула полином или је његов степен мањи од степена полинома $q(x)$.

Доказ. У том случају процес прекидамо, а $p_k(x)$ се, коришћењем претходних једнакости, може представити у облику $p_k(x) = p(x) - s(x)q(x)$, где смо ставили

$$s(x) = \frac{a_n}{b_m}x^{n-m} + \frac{a_{n_1}^{(1)}}{b_m}x^{n_1-m} + \cdots + \frac{a_{n_{k-1}}^{(k-1)}}{b_m}x^{n_{k-1}-m}.$$

Дакле, овај полином $s(x)$ и $r(x) = p_k(x)$ задовољавају једнакост, при чему је $r(x)$ нула полином или је његов степен мањи од степена полинома $q(x)$.
За доказ јединствености полинома $s(x)$ и $r(x)$, претпоставимо да постоје и полиноми $\widehat{s}(x)$ и $\widehat{r}(x)$, који задовољавају једнакост

$$p(x) = \widehat{s}(x)q(x) + \widehat{r}(x),$$

при чему је $\widehat{r}(x) = 0$ или $\deg\widehat{r}(x) < \deg q(x)$.

Доказ. Тада је

$$(s(x)-\widehat{s}(x))q(x)=\widehat{r}(x)-r(x),$$

при чему је полином на десној страни ове једнакости нула полином или је, пак његов степен мањи од степена полинома $q(x)$.

Доказ. Тада је

$$(s(x) - \widehat{s}(x))q(x) = \widehat{r}(x) - r(x),$$

при чему је полином на десној страни ове једнакости нула полином или је, пак његов степен мањи од степена полинома $q(x)$. С друге стране, ако је $s(x) - \widehat{s}(x) \neq 0$, тада полином на левој страни у једнакости је не мањег степена од степена полинома $q(x)$.

Доказ. Тада је

$$(s(x) - \widehat{s}(x))q(x) = \widehat{r}(x) - r(x),$$

при чему је полином на десној страни ове једнакости нула полином или је, пак његов степен мањи од степена полинома $q(x)$. С друге стране, ако је $s(x) - \widehat{s}(x) \neq 0$, тада полином на левој страни у једнакости је не мањег степена од степена полинома $q(x)$. Према томе, једнакост је могућа само ако је

$$\widehat{s}(x) = s(x), \qquad \widehat{r}(x) = r(x),$$

па је тиме доказ завршен. □

За полиноме у скупу $\mathbb{F}[x]$ не постоји операција дељење, инверзна операцији множења.

За полиноме у скупу $\mathbb{F}[x]$ не постоји операција дељење, инверзна операцији множења. Може се, међутим, сагласно особини из претходне теореме, дефинисати дељење полинома полиномом са остатком.

За полиноме у скупу $\mathbb{F}[x]$ не постоји операција дељење, инверзна операцији множења. Може се, међутим, сагласно особини из претходне теореме, дефинисати дељење полинома полиномом са остатком.

Дефиниција

За полином $s(x)$ који задовољава једнакост кажемо да је количник при дељењу полинома $p(x)$ полиномом $q(x)$, а за одговарајући полином $r(x)$ да је остатак при том дељењу.

За полиноме у скупу $\mathbb{F}[x]$ не постоји операција дељење, инверзна операцији множења. Може се, међутим, сагласно особини из претходне теореме, дефинисати дељење полинома полиномом са остатком.

Дефиниција

За полином $s(x)$ који задовољава једнакост кажемо да је количник при дељењу полинома $p(x)$ полиномом $q(x)$, а за одговарајући полином $r(x)$ да је остатак при том дељењу.
Ако је остатак нула полином, кажемо да је $p(x)$ дељиво са $q(x)$ и полином $q(x)$ зовемо делилац полинома $p(x)$.

За полиноме у скупу $\mathbb{F}[x]$ не постоји операција дељење, инверзна операцији множења. Може се, међутим, сагласно особини из претходне теореме, дефинисати дељење полинома полиномом са остатком.

Дефиниција

За полином $s(x)$ који задовољава једнакост кажемо да је количник при дељењу полинома $p(x)$ полиномом $q(x)$, а за одговарајући полином $r(x)$ да је остатак при том дељењу.
Ако је остатак нула полином, кажемо да је $p(x)$ дељиво са $q(x)$ и полином $q(x)$ зовемо делилац полинома $p(x)$.

Чињеницу да је $q(x)$ делилац полинома $p(x)$ симболизујемо са $q(x) \mid p(x)$.

Највећи заједнички делилац

Дефиниција

Полином $d(x)$ *је заједнички делилац за полиноме* $p(x)$ *и* $q(x)$ *ако* $d(x) \mid p(x)$ *и* $d(x) \mid q(x)$.

Највећи заједнички делилац

Дефиниција

Полином $d(x)$ *је заједнички делилац за полиноме* $p(x)$ *и* $q(x)$ *ако* $d(x) \mid p(x)$ *и* $d(x) \mid q(x)$.

Дефиниција

Полином $d(x)$ *је највећи заједнички делилац за полиноме* $p(x)$ *и* $q(x)$*, тј.* $d(x) = \mathrm{NZD}(p(x), q(x))$*, ако је заједнички делилац за ове полиноме и ако је дељив са свим осталим заједничким делиоцима ових полинома.*

Највећи заједнички делилац

Дефиниција

Полином $d(x)$ *је заједнички делилац за полиноме* $p(x)$ *и* $q(x)$ *ако* $d(x) \mid p(x)$ *и* $d(x) \mid q(x)$.

Дефиниција

Полином $d(x)$ *је највећи заједнички делилац за полиноме* $p(x)$ *и* $q(x)$*, тј.* $d(x) = \mathrm{NZD}(p(x), q(x))$*, ако је заједнички делилац за ове полиноме и ако је дељив са свим осталим заједничким делиоцима ових полинома.*

Приметимо да ако је $d(x) = \mathrm{NZD}(p(x), q(x))$, тада је и полином $\alpha d(x)$, ($\alpha \neq 0$, $\alpha \in \mathbb{F}$) такође највећи заједнички делилац полинома $p(x)$ и $q(x)$.

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Теорема

За свака два полинома $p(x)$ *и* $q(x)$ *постоји највећи заједнички делилац* $d(x)$ *и он је јединствен до на мултипликативну константу.*

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$.

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$.

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$. Ако је $r_1(x) = 0$ тада је $q(x)$ највећи заједнички делилац полинома $p(x)$ и $q(x)$.

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$. Ако је $r_1(x) = 0$ тада је $q(x)$ највећи заједнички делилац полинома $p(x)$ и $q(x)$. Међутим, ако $r_1(x)$ није нула полином, тада делимо полином $q(x)$ са $r_1(x)$, и одговарајући количник и остатак при дељењу означавамо са $s_2(x)$ и $r_2(x)$, респективно.

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$. Ако је $r_1(x) = 0$ тада је $q(x)$ највећи заједнички делилац полинома $p(x)$ и $q(x)$. Међутим, ако $r_1(x)$ није нула полином, тада делимо полином $q(x)$ са $r_1(x)$, и одговарајући количник и остатак при дељењу означавамо са $s_2(x)$ и $r_2(x)$, респективно. Ако је $r_2(x) = 0$ тада је $r_1(x)$ највећи заједнички делилац за полиноме $p(x)$ и $q(x)$.

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$. Ако је $r_1(x) = 0$ тада је $q(x)$ највећи заједнички делилац полинома $p(x)$ и $q(x)$. Међутим, ако $r_1(x)$ није нула полином, тада делимо полином $q(x)$ са $r_1(x)$, и одговарајући количник и остатак при дељењу означавамо са $s_2(x)$ и $r_2(x)$, респективно. Ако је $r_2(x) = 0$ тада је $r_1(x)$ највећи заједнички делилац за полиноме $p(x)$ и $q(x)$. Заиста, из $p(x) = s_1(x)q(x) + r_1(x)$,
$q(x) = s_2(x)r_1(x) + r_2(x)$, следује $p(x) = (s_1(x)s_2(x) + 1)r_1(x)$ и
$q(x) = s_2(x)r_1(x)$,

Теорема

За свака два полинома $p(x)$ и $q(x)$ постоји највећи заједнички делилац $d(x)$ и он је јединствен до на мултипликативну константу.

Доказ. Претпоставимо да је $\deg p(x) \geqslant \deg q(x)$. Са $s_1(x)$ и $r_1(x)$ означимо редом количник и остатак при дељењу полинома $p(x)$ са $q(x)$. Ако је $r_1(x) = 0$ тада је $q(x)$ највећи заједнички делилац полинома $p(x)$ и $q(x)$. Међутим, ако $r_1(x)$ није нула полином, тада делимо полином $q(x)$ са $r_1(x)$, и одговарајући количник и остатак при дељењу означавамо са $s_2(x)$ и $r_2(x)$, респективно. Ако је $r_2(x) = 0$ тада је $r_1(x)$ највећи заједнички делилац за полиноме $p(x)$ и $q(x)$. Заиста, из $p(x) = s_1(x)q(x) + r_1(x)$, $q(x) = s_2(x)r_1(x) + r_2(x)$, следује $p(x) = (s_1(x)s_2(x) + 1)r_1(x)$ и $q(x) = s_2(x)r_1(x)$, тј. $r_1(x) \mid p(x)$ и $r_1(x) \mid q(x)$.

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$.

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

$$\vdots$$

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

$$\vdots$$

$$r_{k-1}(x) = s_{k+1}(x)r_k(x) + r_{k+1}(x),$$

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

$$\vdots$$

$$r_{k-1}(x) = s_{k+1}(x)r_k(x) + r_{k+1}(x),$$

све до испуњења услова $r_{k+1}(x) = 0$.

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

$$\vdots$$

$$r_{k-1}(x) = s_{k+1}(x)r_k(x) + r_{k+1}(x),$$

све до испуњења услова $r_{k+1}(x) = 0$. Тада је $r_k(x) = \mathrm{NZD}(p(x), q(x))$.

Доказ. Да бисмо доказали да је $r_1(x)$ највећи заједнички делилац за $p(x)$ и $q(x)$ довољно је претпоставити да ови полиноми имају заједнички делилац $d(x)$ и приметити да следује $d(x) \mid r_1(x)$. Међутим, уколико $r_2(x)$ није нула полином, претходни поступак се наставља, сагласно следећим једнакостима,

$$r_1(x) = s_3(x)r_2(x) + r_3(x),$$

$$r_2(x) = s_4(x)r_3(x) + r_4(x),$$

$$\vdots$$

$$r_{k-1}(x) = s_{k+1}(x)r_k(x) + r_{k+1}(x),$$

све до испуњења услова $r_{k+1}(x) = 0$. Тада је $r_k(x) = \mathrm{NZD}(p(x), q(x))$. Ово закључујемо сличним резоновањем као у случају $k = 1$. $\square$

У доказу ове теореме коришћен је Еуклидов алгоритам, при чему су за одређивање највећег заједничког делиоца (NZD) два полинома битни само остаци $r_\nu(x)$, а не и количници $s_\nu(x)$, $\nu = 1, 2, \ldots$.

У доказу ове теореме коришћен је Еуклидов алгоритам, при чему су за одређивање највећег заједничког делиоца (NZD) два полинома битни само остаци $r_\nu(x)$, а не и количници $s_\nu(x)$, $\nu = 1, 2, \ldots$.

Имајући на уму јединственост NZD до на мултипликативну константу могуће је у сваком кораку Еуклидовог алгоритма множити остатке $r_\nu(x)$ погодним константама различитим од нуле у циљу добијања једноставнијих израза при дељењу.

У доказу ове теореме коришћен је Еуклидов алгоритам, при чему су за одређивање највећег заједничког делиоца (NZD) два полинома битни само остаци $r_\nu(x)$, а не и количници $s_\nu(x)$, $\nu = 1, 2, \ldots$.

Имајући на уму јединственост NZD до на мултипликативну константу могуће је у сваком кораку Еуклидовог алгоритма множити остатке $r_\nu(x)$ погодним константама различитим од нуле у циљу добијања једноставнијих израза при дељењу.

Дефиниција

Ако је највћи заједнички делилац за полиноме $p(x)$ и $q(x)$ константа, за те полиноме кажемо да су узајамно прости.

Пример

За полиноме у $\mathbb{R}[x]$,

$$p(x) = 2x^4 + 4x^3 + x^2 - 2x - 8, \quad q(x) = x^3 + x^2 + 4,$$

одредићемо NZD.

Пример

За полиноме у $\mathbb{R}[x]$,

$$p(x) = 2x^4 + 4x^3 + x^2 - 2x - 8, \quad q(x) = x^3 + x^2 + 4,$$

одредићемо NZD.

Добијамо да је

$$d(x) = \mathrm{NZD}(p(x), q(x)) = x + 2.$$

Теорема

Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ *тада постоје полиноми* $u(x)$ *и* $v(x)$ *такви да је*

$$d(x) = u(x)p(x) + v(x)q(x).$$

Теорема

Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ *тада постоје полиноми* $u(x)$ *и* $v(x)$ *такви да је*

$$d(x) = u(x)p(x) + v(x)q(x).$$

Доказ. На основу претходне теореме имамо редом
$r_1(x) = p(x) - s_1(x)q(x),$

Теорема

Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ *тада постоје полиноми* $u(x)$ *и* $v(x)$ *такви да је*

$$d(x) = u(x)p(x) + v(x)q(x).$$

Доказ. На основу претходне теореме имамо редом

$r_1(x) = p(x) - s_1(x)q(x),$

$r_2(x) = -s_2(x)p(x) + (1 + s_1(x)s_2(x))q(x),$

Теорема

Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ *тада постоје полиноми* $u(x)$ *и* $v(x)$ *такви да је*

$$d(x) = u(x)p(x) + v(x)q(x).$$

Доказ. На основу претходне теореме имамо редом

$r_1(x) = p(x) - s_1(x)q(x),$

$r_2(x) = -s_2(x)p(x) + (1 + s_1(x)s_2(x))q(x),$

$r_3(x) =$
$(1 + s_2(x)s_3(x))p(x) - (s_1(x) + s_3(x) + s_1(x)s_2(x)s_3(x))q(x),$

Теорема

Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ *тада постоје полиноми* $u(x)$ *и* $v(x)$ *такви да је*

$$d(x) = u(x)p(x) + v(x)q(x).$$

Доказ. На основу претходне теореме имамо редом

$r_1(x) = p(x) - s_1(x)q(x),$

$r_2(x) = -s_2(x)p(x) + (1 + s_1(x)s_2(x))q(x),$

$r_3(x) =$
$(1 + s_2(x)s_3(x))p(x) - (s_1(x) + s_3(x) + s_1(x)s_2(x)s_3(x))q(x),$
итд.

Теорема

Ако је $d(x) = \mathrm{NZD}(p(x), q(x))$ *тада постоје полиноми* $u(x)$ *и* $v(x)$ *такви да је*

$$d(x) = u(x)p(x) + v(x)q(x).$$

Доказ. На основу претходне теореме имамо редом
$r_1(x) = p(x) - s_1(x)q(x),$

$r_2(x) = -s_2(x)p(x) + (1 + s_1(x)s_2(x))q(x),$

$r_3(x) =$
$(1 + s_2(x)s_3(x))p(x) - (s_1(x) + s_3(x) + s_1(x)s_2(x)s_3(x))q(x),$
итд.

Најзад, $d(x) = r_k(x)$ има облик који се тражи. $\square$