Elementarna matematika 1

Prsten polinoma u jednoj varijabli

2011/2012

Definicija grupe

Definicija. *Grupa* je uređen par $(G, \cdot)$ nepraznog skupa G i binarne operacije $\cdot : G \times G \to G$ takve da vrijedi

1. asocijativnost: $x \cdot (y \cdot z) = (x \cdot y) \cdot z, \ \forall x, y, z \in G$,
2. postoji *neutralni element* $e \in G$ takav da je $e \cdot x = x \cdot e = x, \ \forall x \in G$,
3. za svaki $x \in G$ postoji *inverzni element* $x^{-1} \in G$ takav da je $x \cdot x^{-1} = x^{-1} \cdot x = e$.

Ako uz to vrijedi komutativnost: $x \cdot y = y \cdot x, \ \forall x, y \in G$, kažemo da je grupa *Abelova* ili *komutativna*.

Primjeri grupa

- Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijom zbrajanja "$+$". Neutralni element je nula 0, a inverzni element od x je suprotni broj $-x$. Zbrajanje je komutativno.
- Skupovi $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ i $\mathbb{C} \setminus \{0\}$ s operacijom množenja "$\cdot$". Neutrajni element je jedinica 1, a inverzni element od x je recipročni broj $x^{-1} = \frac{1}{x}$. Množenje je komutativno.
- Za bilo koji skup X, skup $S(X)$ svih bijekcija s X u X uz operaciju kompozicije je nekomutativna grupa. Neutralni element je identiteta id_X, a inverzni element od f je inverzna funkcija f^{-1}.

Primjeri grupa

- Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijom zbrajanja "$+$". Neutralni element je nula 0, a inverzni element od x je suprotni broj $-x$. Zbrajanje je komutativno.
- Skupovi $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ i $\mathbb{C} \setminus \{0\}$ s operacijom množenja "$\cdot$". Neutrajni element je jedinica 1, a inverzni element od x je recipročni broj $x^{-1} = \frac{1}{x}$. Množenje je komutativno.
- Za bilo koji skup X, skup $S(X)$ svih bijekcija s X u X uz operaciju kompozicije je nekomutativna grupa. Neutralni element je identiteta id_X, a inverzni element od f je inverzna funkcija f^{-1}.

Primjeri grupa

- Skupovi $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijom zbrajanja "$+$". Neutralni element je nula 0, a inverzni element od x je suprotni broj $-x$. Zbrajanje je komutativno.
- Skupovi $\mathbb{Q} \setminus \{0\}$, $\mathbb{R} \setminus \{0\}$ i $\mathbb{C} \setminus \{0\}$ s operacijom množenja "$\cdot$". Neutrajni element je jedinica 1, a inverzni element od x je recipročni broj $x^{-1} = \frac{1}{x}$. Množenje je komutativno.
- Za bilo koji skup X, skup $S(X)$ svih bijekcija s X u X uz operaciju kompozicije je nekomutativna grupa. Neutralni element je identiteta id_X, a inverzni element od f je inverzna funkcija f^{-1}.

Definicija prstena

Definicija. *Prsten* (točnije, *komutativni prsten s jedinicom*) je uređena trojka $(P, +, \cdot)$ nepraznog skupa P i dvije binarne operacije $+, \cdot : P \times P \to P$ takva da vrijedi

1. $(P, +)$ je komutativna grupa s neutralnim elementom 0,
2. $(P, \cdot)$ je komutativni *monoid*, tj. operacija $\cdot$ je komutativna, asocijativna i ima neutralni element 1,
3. distributivnost: $x \cdot (y + z) = x \cdot y + x \cdot z$, $(x + y) \cdot z = x \cdot z + y \cdot z, \ \forall x, y, z \in P$.

Ako je $(P \setminus \{0\}, \cdot)$ grupa, tj. ako svaki element $x \neq 0$ ima inverz obzirom na operaciju $\cdot$, kažemo da je $(P, +, \cdot)$ *polje*.

Primjeri prstena

- Skupovi $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijama zbrajanja i množenja su polja.
- Skup $\mathbb{Z}$ s operacijom zbrajanja i množenja je prsten koji nije polje.
- Skup $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ s operacijom zbrajanja $+_n$ i množenja $\cdot_n$ modulo $n \in \mathbb{N}$ je prsten. Taj prsten je polje ako i samo ako je n prost broj.
- Za bilo koji skup S i prsten P, skup svih funkcija sa S u P uz operacije zbrajanja i množenja po točkama je prsten: $(f+g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$. Što su nula i jedinica u tom prstenu? Ako je kodomena polje, čine li funkcije polje?

Primjeri prstena

- Skupovi $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijama zbrajanja i množenja su polja.
- Skup $\mathbb{Z}$ s operacijom zbrajanja i množenja je prsten koji nije polje.
- Skup $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ s operacijom zbrajanja $+_n$ i množenja $\cdot_n$ modulo $n \in \mathbb{N}$ je prsten. Taj prsten je polje ako i samo ako je n prost broj.
- Za bilo koji skup S i prsten P, skup svih funkcija sa S u P uz operacije zbrajanja i množenja po točkama je prsten: $(f+g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$. Što su nula i jedinica u tom prstenu? Ako je kodomena polje, čine li funkcije polje?

Primjeri prstena

- Skupovi $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijama zbrajanja i množenja su polja.
- Skup $\mathbb{Z}$ s operacijom zbrajanja i množenja je prsten koji nije polje.
- Skup $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ s operacijom zbrajanja $+_n$ i množenja $\cdot_n$ modulo $n \in \mathbb{N}$ je prsten. Taj prsten je polje ako i samo ako je n prost broj.
- Za bilo koji skup S i prsten P, skup svih funkcija sa S u P uz operacije zbrajanja i množenja po točkama je prsten: $(f+g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$. Što su nula i jedinica u tom prstenu? Ako je kodomena polje, čine li funkcije polje?

Primjeri prstena

- Skupovi $\mathbb{Q}$, $\mathbb{R}$ i $\mathbb{C}$ s operacijama zbrajanja i množenja su polja.
- Skup $\mathbb{Z}$ s operacijom zbrajanja i množenja je prsten koji nije polje.
- Skup $\mathbb{Z}_n = \{0, 1, \ldots, n-1\}$ s operacijom zbrajanja $+_n$ i množenja $\cdot_n$ modulo $n \in \mathbb{N}$ je prsten. Taj prsten je polje ako i samo ako je n prost broj.
- Za bilo koji skup S i prsten P, skup svih funkcija sa S u P uz operacije zbrajanja i množenja po točkama je prsten: $(f+g)(x) = f(x) + g(x)$, $(f \cdot g)(x) = f(x) \cdot g(x)$. Što su nula i jedinica u tom prstenu? Ako je kodomena polje, čine li funkcije polje?

Prsten polinoma

Prsten polinoma $P[x]$ možemo definirati kao potprsten prstena svih funkcija s P u P. Polinomi su funkcije oblika

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.$$

Zbroj i produkt takvih funkcija također je funkcija tog oblika, pa polinomi čine potprsten. Ovaj pristup zvat ćemo **"funkcijskom definicijom polinoma"**.

Alternativno, polinome možemo definirati kao nizove koeficijenata $a : \mathbb{N}_0 \to P$ u kojima su svi članovi osim njih konačno mnogo jednaki nuli. Nizovi se zbrajaju po koordinatama:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

Prsten polinoma

Prsten polinoma $P[x]$ možemo definirati kao potprsten prstena svih funkcija s P u P. Polinomi su funkcije oblika

$$f(x) = a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n.$$

Zbroj i produkt takvih funkcija također je funkcija tog oblika, pa polinomi čine potprsten. Ovaj pristup zvat ćemo "**funkcijskom definicijom polinoma**".

Alternativno, polinome možemo definirati kao nizove koeficijenata $a : \mathbb{N}_0 \to P$ u kojima su svi članovi osim njih konačno mnogo jednaki nuli. Nizovi se zbrajaju po koordinatama:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (a_0 + b_0, a_1 + b_1, a_2 + b_2, \ldots)$$

Prsten polinoma

Definicija množenja nizova nešto je kompliciranija:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$$

Teorem. Skup svih nizova u kojima su skoro svi koeficijenti jednaki 0 s upravo definiranim operacijama zbrajanja i množenja čini prsten. Neutralni element za zbrajanje je niz $(0, 0, 0, \ldots)$, a neutralni element za množenje niz $(1, 0, 0, \ldots)$.

Ovaj prsten također zovemo *prsten polinoma nad P* i označavamo $P[x]$. To je takozvana **"algebarska definicija polinoma"**.

Prsten polinoma

Definicija množenja nizova nešto je kompliciranija:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$$

Teorem. Skup svih nizova u kojima su skoro svi koeficijenti jednaki 0 s upravo definiranim operacijama zbrajanja i množenja čini prsten. Neutralni element za zbrajanje je niz $(0, 0, 0, \ldots)$, a neutralni element za množenje niz $(1, 0, 0, \ldots)$.

Ovaj prsten također zovemo *prsten polinoma nad P* i označavamo $P[x]$. To je takozvana **"algebarska definicija polinoma"**.

Prsten polinoma

Definicija množenja nizova nešto je kompliciranija:

$$(a_0, a_1, a_2, \ldots) + (b_0, b_1, b_2, \ldots) = (c_0, c_1, c_2, \ldots)$$

$$c_n = \sum_{i=0}^{n} a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$$

Teorem. Skup svih nizova u kojima su skoro svi koeficijenti jednaki 0 s upravo definiranim operacijama zbrajanja i množenja čini prsten. Neutralni element za zbrajanje je niz $(0, 0, 0, \ldots)$, a neutralni element za množenje niz $(1, 0, 0, \ldots)$.

Ovaj prsten također zovemo *prsten polinoma nad P* i označavamo $P[x]$. To je takozvana **"algebarska definicija polinoma"**.

Veza između algebarske i funkcijske definicije polinoma

Oznake:

Za $a \in P$ identificiramo $a = (a, 0, 0, \ldots)$.

Varijabla je niz $x = (0, 1, 0, 0, \ldots)$.

Propozicija. $x^n = (0, \ldots, 0, 1, 0, \ldots)$, $\forall n \in \mathbb{N}$.

Tada niz $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ možemo pisati kao $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

Jesu li algebarska i funkcijska definicija polinoma ekvivalentne?

Veza između algebarske i funkcijske definicije polinoma

Oznake:

Za $a \in P$ identificiramo $a = (a, 0, 0, \ldots)$.

Varijabla je niz $x = (0, 1, 0, 0, \ldots)$.

Propozicija. $x^n = (0, \ldots, 0, 1, 0, \ldots), \forall n \in \mathbb{N}$.

Tada niz $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ možemo pisati kao $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

Jesu li algebarska i funkcijska definicija polinoma ekvivalentne?

Veza između algebarske i funkcijske definicije polinoma

Oznake:

Za $a \in P$ identificiramo $a = (a, 0, 0, \ldots)$.

Varijabla je niz $x = (0, 1, 0, 0, \ldots)$.

Propozicija. $x^n = (0, \ldots, 0, 1, 0, \ldots), \forall n \in \mathbb{N}$.

Tada niz $(a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$ možemo pisati kao $a_0 + a_1 x + a_2 x^2 + \ldots + a_n x^n$.

Jesu li algebarska i funkcijska definicija polinoma ekvivalentne?

Primjer: $P = \mathbb{Z}_2$

Najmanji prsten / polje je $\mathbb{Z}_2 = \{0, 1\}$ uz operacije

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Postoje samo četiri različite funkcije $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ koje se mogu zadati kao polinomi: $f_1(x) = 0$, $f_2(x) = 1$, $f_3(x) = x$, $f_4(x) = 1 + x$.

Međutim, postoji beskonačno mnogo nizova $a : \mathbb{N}_0 \to \mathbb{Z}_2$ kojima su skoro svi članovi 0. Npr. nizovi $0 = (0, 0, \dots)$ i $x + x^2 = (0, 1, 1, 0, 0, \dots)$ predstavljaju istu funkciju (*nulfunkciju*).

Primjer: $P = \mathbb{Z}_2$

Najmanji prsten / polje je $\mathbb{Z}_2 = \{0, 1\}$ uz operacije

$+$	0	1
0	0	1
1	1	0

$\cdot$	0	1
0	0	0
1	0	1

Postoje samo četiri različite funkcije $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ koje se mogu zadati kao polinomi: $f_1(x) = 0$, $f_2(x) = 1$, $f_3(x) = x$, $f_4(x) = 1 + x$.

Međutim, postoji beskonačno mnogo nizova $a : \mathbb{N}_0 \to \mathbb{Z}_2$ kojima su skoro svi članovi 0. Npr. nizovi $0 = (0, 0, \dots)$ i $x + x^2 = (0, 1, 1, 0, 0, \dots)$ predstavljaju istu funkciju (*nulfunkciju*).

Primjer: $P = \mathbb{Z}_2$

Najmanji prsten / polje je $\mathbb{Z}_2 = \{0, 1\}$ uz operacije

+	0	1
0	0	1
1	1	0

·	0	1
0	0	0
1	0	1

Postoje samo četiri različite funkcije $f : \mathbb{Z}_2 \to \mathbb{Z}_2$ koje se mogu zadati kao polinomi: $f_1(x) = 0$, $f_2(x) = 1$, $f_3(x) = x$, $f_4(x) = 1 + x$.

Međutim, postoji beskonačno mnogo nizova $a : \mathbb{N}_0 \to \mathbb{Z}_2$ kojima su skoro svi članovi 0. Npr. nizovi $0 = (0, 0, \ldots)$ i $x + x^2 = (0, 1, 1, 0, 0, \ldots)$ predstavljaju istu funkciju (*nulfunkciju*).

Primjer: $P = \mathbb{R}$

Za polinome s realnim koeficijentima algebarska i funkcijska definicija su ekvivalentne!

Teorem (o jednakosti polinoma). Polinomi

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = b_0 + b_1 x + b_2 x^2 + \dots$$

su jednaki (kao funkcije) ako i samo ako su istog stupnja i odgovarajući koeficijenti su im jednaki, tj. vrijedi $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2, \dots$

Teorem (o nulpolinomu). Polinom $f : \mathbb{R} \to \mathbb{R}$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$ je nulpolinom (tj. nulfunkcija) ako i samo ako je $a_0 = a_1 = \dots = a_n = 0$.

Primjer: $P = \mathbb{R}$

Za polinome s realnim koeficijentima algebarska i funkcijska definicija su ekvivalentne!

Teorem (o jednakosti polinoma). Polinomi

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = b_0 + b_1 x + b_2 x^2 + \dots$$

su jednaki (kao funkcije) ako i samo ako su istog stupnja i odgovarajući koeficijenti su im jednaki, tj. vrijedi $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2, \dots$

Teorem (o nulpolinomu). Polinom $f : \mathbb{R} \to \mathbb{R}$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$ je nulpolinom (tj. nulfunkcija) ako i samo ako je $a_0 = a_1 = \dots = a_n = 0$.

Primjer: $P = \mathbb{R}$

Za polinome s realnim koeficijentima algebarska i funkcijska definicija su ekvivalentne!

Teorem (o jednakosti polinoma). Polinomi

$$f : \mathbb{R} \to \mathbb{R}, \quad f(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

$$g : \mathbb{R} \to \mathbb{R}, \quad g(x) = b_0 + b_1 x + b_2 x^2 + \dots$$

su jednaki (kao funkcije) ako i samo ako su istog stupnja i odgovarajući koeficijenti su im jednaki, tj. vrijedi $a_0 = b_0$, $a_1 = b_1$, $a_2 = b_2, \dots$

Teorem (o nulpolinomu). Polinom $f : \mathbb{R} \to \mathbb{R}$, $f(x) = a_0 + a_1 x + \dots + a_n x^n$ je nulpolinom (tj. nulfunkcija) ako i samo ako je $a_0 = a_1 = \dots = a_n = 0$.