

Polia

7. októbra 2025

Definícia poľa

Definícia

Nech F je množina, $+$ a $\cdot$ sú binárne operácie na F . Hovoríme, že trojica $(F, +, \cdot)$ je *pole*, ak

- (i) $(F, +)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 0;
- (ii) $(F \setminus \{0\}, \cdot)$ je komutatívna grupa, jej neutrálny prvok budeme označovať 1;
- (iii) pre ľubovoľné $a, b, c \in F$ platí

$$a(b + c) = ab + ac,$$

$$(a + b)c = ac + bc.$$

(Túto vlastnosť nazývame *distributívnosť*.)

Definícia poľa

Označenie:

- ▶ Inverzný prvok v grupe $(F, +)$ označujeme $-a$;
- ▶ Inverzný prvok v grupe $(F \setminus \{0\}, \cdot)$ označujeme a^{-1} .
- ▶ Namiesto $b + (-c)$ píšeme $b - c$.

Príklady polí

- ▶ racionálne čísla $(\mathbb{Q}, +, \cdot)$
- ▶ reálne čísla $(\mathbb{R}, +, \cdot)$
- ▶ komplexné čísla $(\mathbb{C}, +, \cdot)$

Definícia poľa

- (i) pre všetky $a, b, c \in F$ platí $a + (b + c) = (a + b) + c$,
- (ii) pre všetky $a, b \in F$ platí $a + b = b + a$,
- (iii) existuje prvok $0 \in F$ taký, že pre každé $a \in F$ sa $a + 0 = a$,
- (iv) ku každému $a \in F$ existuje $b \in F$ tak, že $a + b = 0$,
- (v) pre všetky $a, b, c \in F$ platí $a \cdot (b \cdot c) = (a \cdot b) \cdot c$,
- (vi) pre všetky $a, b \in F$ platí $a \cdot b = b \cdot a$,
- (vii) existuje prvok $1 \in F$ taký, že $1 \neq 0$ a pre každé $a \in F$ sa $a \cdot 1 = a$,
- (viii) ku každému $a \in F$, $a \neq 0$ existuje $b \in F$ tak, že $a \cdot b = 1$,
- (ix) pre všetky $a, b, c \in F$ sa $a \cdot (b + c) = a \cdot b + a \cdot c$.

Vlastnosti polí

Tvrdenie

Nech $(F, +, \cdot)$ je pole. Potom pre $a, b, c \in F$ platí

(i) $a \cdot 0 = 0, 0 \cdot a = 0,$

(ii) $a \cdot b = b \cdot a,$

(iii) $1 \cdot a = a \cdot 1 = a,$

(iv) $(-a) \cdot b = -a \cdot b,$

(v) $(-a) \cdot (-b) = a \cdot b,$

(vi) $a \cdot b = 0 \Rightarrow a = 0 \vee b = 0,$

(vii) $a \cdot b = a \cdot c \wedge a \neq 0 \Rightarrow b = c,$

(viii) $a \cdot a = a \Rightarrow a = 0 \vee a = 1.$

Počítanie v $\mathbb{Z}_n$

Definícia

Nech $n \in \mathbb{N}$, $n \geq 2$. Množinu $\mathbb{Z}_n$ definujeme ako $\mathbb{Z}_n := \{0, 1, \dots, n-1\}$. (Teda množina $\mathbb{Z}_n$ obsahuje všetky možné zvyšky po delení číslom n .)

Na množine $\mathbb{Z}_n$ zavedieme operácie $\oplus$ a $\odot$ predpisom

$$a \oplus b = (a + b) \bmod n,$$

$$a \odot b = (ab) \bmod n,$$

kde operácia $\bmod$ označuje zvyšok po delení číslom n .

Počítanie v $\mathbb{Z}_7$

$$2 \oplus 4 = 6$$

$$3 \oplus 6 = 2$$

$$2 \odot 3 = 6$$

$$2 \odot 4 = 1$$

$$2^{-1} = 4$$

$$3 \odot (4 \oplus 2) \oplus 5 \odot (3 \oplus 6) = 3 \odot 6 \oplus 5 \odot 2 = 4 \oplus 3 = 0$$

$$3 \cdot (4 + 2) + 5 \cdot (3 + 6) = 3 \cdot 6 + 5 \cdot 9 = 18 + 45 = 63 = 9 \cdot 7 + 0$$

Vlastnosti prvočísel

Definícia

Číslo $n \in \mathbb{N}$, $n > 1$, nazývame *zloženým číslom*, ak $n = m \cdot k$ pre nejaké $m, k \in \mathbb{N}$ také, že $1 < m, k < n$.

Ak $n \in \mathbb{N}$, $n > 1$, nie je zložené, tak ho nazývame *prvočíslo*.

Číslo 1 nepovažujeme ani za prvočíslo ani za zložené číslo.

$$p \mid mn \Rightarrow p \mid m \vee p \mid n$$

$\mathbb{Z}_p$ je pole

Veta

Ak p je prvočíslo, tak $(\mathbb{Z}_p, \oplus, \odot)$ je pole.

Pre zložené čísla nedostaneme pole. (Prečo?)

Tu nepotrebujeme využívať, že p je prvočíslo:

- ▶ $(\mathbb{Z}_p, \oplus)$ je komutatívna grupa
- ▶ asociatívnosť a komutatívnosť násobenia;
- ▶ neutrálny prvok pre násobenie;
- ▶ distributívnosť;

Distributívnosť, asociatívnosť, komutatívnosť

Distributívnosť, obe asociatívnosti, obe komutatívnosti – základná idea je rovnaká:

$$a \cdot (b + c) = ab + ac$$

$$(a \cdot (b + c)) \bmod p = (ab + ac) \bmod p$$

$$a \odot (b \oplus c) = (a \odot b) \oplus (a \odot c)$$

Prečo platí $a \odot (b \oplus c) = (a \cdot (b + c)) \bmod p$ a
 $(a \odot b) \oplus (a \odot c) = (ab + ac) \bmod p$?

Distributívnosť, asociatívnosť, komutatívnosť

$$a + (b + c) = (a + b) + c$$

$$(a + (b + c)) \bmod p = ((a + b) + c) \bmod p$$

$$a \oplus (b \oplus c) = (a \oplus b) \oplus c$$

$$a \cdot b = b \cdot a$$

$$(a \cdot b) \bmod p = (b \cdot a) \bmod p$$

$$a \odot b = b \odot a$$

$\mathbb{Z}_p$ je pole

Ešte chýba:

- ▶ $\odot$ je binárna operácia na $\mathbb{Z}_p \setminus \{0\}$;
- ▶ existuje multiplikatívny inverz;

Binárna operácia na $\mathbb{Z}_p \setminus \{0\}$

$$a \neq 0 \wedge b \neq 0 \Rightarrow a \odot b \neq 0$$

$$a \odot b = 0 \Rightarrow a = 0 \vee b = 0$$

$$p \mid ab \Rightarrow p \mid a \vee p \mid b$$

Krátenie v $\mathbb{Z}_p$

Pre $a, k, l \in \mathbb{Z}_p$ také, že $a \neq 0$ platí

$$a \odot k = a \odot l \quad \Rightarrow \quad k = l.$$

$$p \mid a \cdot (k - l) \Rightarrow p \mid a \vee p \mid k - l$$

Inverzný prvok v $\mathbb{Z}_p$

$$a \odot 1 = \dots$$

$$a \odot 2 = \dots$$

$$\vdots$$

$$a \odot (p-1) = \dots$$

Vpravo sa vyskytnú všetky prvky zo $\mathbb{Z}_p$, teda aj jednotka.

Bézoutova identita a Euklidov algoritmus

Iný dôkaz – najprv dokázať, že pre $\gcd(a, b) = 1$ existujú $u, v \in \mathbb{Z}$ také, že

$$ax + by = 1.$$

(Špeciálny prípad Bézoutovej identity.)

Potom pre $a \in \{1, 2, \dots, p-1\}$ máme $\gcd(a, p) = 1$, a teda

$$ax + yp = 1$$

$$a \odot (x \bmod p) = 1$$

Bézoutova identita a Euklidov algoritmus

Například: $\gcd(2, 11) = \gcd(3, 11) = \gcd(4, 11) = \gcd(5, 11) = 1$

$$6 \cdot 2 - 1 \cdot 11 = 1$$

$$(-5) \cdot 2 + 1 \cdot 11 = 1$$

$$4 \cdot 3 - 1 \cdot 11 = 1$$

$$3 \cdot 4 - 1 \cdot 11 = 1$$

$$(-2) \cdot 5 + 1 \cdot 11 = 1$$

$$9 \cdot 5 - 4 \cdot 11 = 1$$

Malá Fermatova veta

Ak p je prvočíslo, tak v $\mathbb{Z}_p$ platí:

$$a \neq 0 \Rightarrow a^{p-1} = 1$$

$$a \neq 0 \Rightarrow a^{-1} = a^{p-2}$$

Obvyklá formulácia: Ak $a \in \mathbb{Z}$ a $p \nmid a$, tak

$$a^{p-1} \equiv 1 \pmod{p}$$

$$a^p \equiv a \pmod{p}$$

(V druhej formulácii už môžeme vynechať podmienku $p \nmid a$.)

Malá Fermatova veta

Například pro $p = 11$, $a = 2$ dostaneme (v $\mathbb{Z}_{11}$)

$$2^3 = 8$$

$$2^4 = 5$$

$$2^5 = -1$$

$$2^{10} = (2^5)^2 = 1$$

Malá Fermatova veta

Pre $p = 11$, $a = 3$ dostaneme (v $\mathbb{Z}_{11}$)

$$3^2 = -2$$

$$3^4 = 4$$

$$3^5 = 4 \odot 3 = 1$$

$$3^{10} = 1$$

Hľadanie inverzného prvku v $\mathbb{Z}_p$

- ▶ Vyskúšaním všetkých možností.
- ▶ Efektívnejší postup je rozšírený Euklidov algoritmus.
- ▶ Ak $d = \gcd(a, b)$, tak Euklidovým algoritmom vieme nájsť celé čísla $x, y \in \mathbb{Z}$ také, že

$$ax + by = d.$$

- ▶ Aj malá Fermatova veta nám dáva možnosť, ako počítať multiplikatívny inverz v $\mathbb{Z}_p$.