

Grupy, tělesa

- grupa: množina s jednou „rozumnou“ operací
- příklady grup, vlastnosti
- těleso: množina se dvěma „rozumnými“ operacemi
- příklady těles, vlastnosti, charakteristika tělesa
- lineární prostor nad tělesem
- polynomy nad tělesem
- polynomy modulo polynom

Reálná čísla, inspirace

Na množině \mathbf{R} reálných čísel máme operaci $+$. Přitom platí:

- $x + (y + z) = (x + y) + z \dots$ (asociativní zákon),
- existuje prvek $0 \in \mathbf{R}$ takový, že $0 + x = x + 0 = x \quad \forall x \in \mathbf{R}$
... (existence neutrálního prvku),
- $\forall x \in \mathbf{R}$ existuje opačný prvek $y \in \mathbf{R}$ tak, že $x + y = y + x = 0$
... (existence opačného prvku, značíme $y = -x$),
- $x + y = y + x \dots$ (komutativní zákon).

Na množině \mathbf{R} máme také operaci \cdot , která splňuje:

- $x \cdot (y \cdot z) = (x \cdot y) \cdot z \dots$ (asociativní zákon),
- existuje prvek $1 \in \mathbf{R}$ takový, že $1 \cdot x = x \cdot 1 = x \quad \forall x \in \mathbf{R}$
... (existence jednotkového prvku),
- $\forall x \in \mathbf{R}, x \neq 0$ existuje prvek $y \in \mathbf{R}$ tak, že $x \cdot y = y \cdot x = 1$
... (existence inverzního prvku, značíme $y = x^{-1}$),
- $x \cdot y = y \cdot x \dots$ (komutativní zákon).

Množina s jednou operací: grupoid, grupa

Definice: Předpokládejme množinu G a na ní operaci \circ .

Dále uvažujme vlastnosti:

(1) $x \circ (y \circ z) = (x \circ y) \circ z \quad \forall x, y, z \in G \dots$ (asociativní zákon),

(2) existuje prvek $e \in G$ takový, že $e \circ x = x \circ e = x \quad \forall x \in G$
 \dots (existence neutrálního/jednotkového prvku),

(3) $\forall x \in G$ existuje prvek $y \in G$ tak, že $x \circ y = y \circ x = e$
 \dots (existence opačného/inverzního prvku),

(4) $x \circ y = y \circ x \quad \forall x, y \in G \dots$ (komutativní zákon).

- Množina G s operací \circ se nazývá *grupoid*.
- Grupoid, kde platí asociativní zákon (1), se nazývá *pologrupa*.
- Pologrupa s vlastnostmi (2) a (3) se nazývá *grupa*.
- Grupa, kde platí komutativní zákon (4), je *komutativní grupa*.

Příklady

- \mathbf{R} s operací $+$ je komutativní grupa.
- \mathbf{R} s operací \cdot je pologrupa, $\mathbf{R} \setminus \{0\}$ je komutativní grupa.
- \mathbf{Q} , \mathbf{Z} s operací $+$ jsou komutativní grupy (podgrupy grupy \mathbf{R} s $+$).
- $\mathbf{Z} \setminus \{0\}$ s operací \cdot není grupa (je to pologrupa).
- Množina $\{e\}$ s operací \circ , pro kterou $e \circ e = e$, je grupa.
- Množina regulárních matic s maticovým násobením je grupa.
- Množina ctvercových matic s násobením je pologrupa.
- Množina funkcí $\mathbf{R} \rightarrow \mathbf{R}$ prostých a na s operací skládání je grupa.
- Množina bijektivních zobrazení $M \rightarrow M$ s op. skládání je grupa.
- Množina permutací s operací skládání je grupa
- Množina $\{0, 1, \dots, m-1\}$ s operací „+ modulo m “ je grupa.

Terminologie: jednotkový/neutrální prvek

Operace komutativní grupy bývá někdy označena symbolem $+$. V takovém případě prvek e z vlastnosti (2) grupy se nazývá *neutrální prvek* a prvek y z vlastnosti (3) se nazývá *opačný prvek*.

Neutrální prvek se v tomto případě značí symbolem 0 a opačný prvek k prvku x se značí $-x$. Operaci $a + (-b)$ značíme stručněji $a - b$ a říkáme ji *odečítání*.

Je-li operace grupy označena symbolem \cdot (krát), pak prvku e z vlastnosti (2) grupy říkáme *jednotkový prvek* a prvku y z vlastnosti (3) říkáme *inverzní prvek*.

Jednotkový prvek v takovém případě značíme symbolem 1 a inverzní prvek k prvku x značíme x^{-1} . Je-li grupa komutativní, pak operaci $a \cdot b^{-1}$ značíme stručněji a/b a říkáme ji *dělení*.

Základní vlastnosti grupy

- Neutrální/jednotkový prvek je v grupě jediný.
Kdyby byly dva e, f , pak $e = e \circ f = f$, takže nemohou být různé.
- Opačný/inverzní prvek existuje ke každému prvku $x \in G$ jediný.
Kdyby existovaly y_1, y_2 tak, že $y_1 \circ x = e, x \circ y_2 = e$, pak

$$y_1 = y_1 \circ e = y_1 \circ (x \circ y_2) = (y_1 \circ x) \circ y_2 = e \circ y_2 = y_2.$$

- Pologrupa G je grupou právě když pro každé $a, b \in G$ existují řešení rovnic

$$a \circ x = b, \quad y \circ a = b.$$

Náznak důkazu: Je-li G grupa, pak $x = a^{-1} \circ b$ a $y = b \circ a^{-1}$ jsou řešení uvedených rovnic. Umíme-li řešit tyto rovnice, pak jednotkový prvek e je řešení rovnice $a \circ e = a$ (je třeba ukázat, že to nezávisí na volbě a). Dále inverzní prvek k a je řešení $a \circ x = e$ (je třeba ukázat, že je to totéž, jako řešení rovnice $y \circ a = e$).

Vlastnosti inverzních prvků grupy

- Jednotkový prvek e má inverzní prvek e (je inverzní sám sobě).
Skutečně: $e = e \circ e$.
- Je-li a^{-1} inverzní prvek k a , je-li dále b^{-1} inverzní prvek k b , pak inverzní prvek k $a \circ b$ je tvaru $b^{-1} \circ a^{-1}$.
Skutečně:

$$(b^{-1} \circ a^{-1}) \circ (a \circ b) = b^{-1} \circ (a^{-1} \circ a) \circ b = b^{-1} \circ e \circ b = b^{-1} \circ b = e,$$

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e.$$

- Je-li a^{-1} inverzní k a , pak a je inverzní k a^{-1} .
Skutečně: $a^{-1} \circ a = a \circ a^{-1} = e$.

Mocnina

Je-li $a \in G$, pak symbolem a^k označme prvek $a \circ a \circ \dots \circ a$ (k -krát).

Tvrzení: Je-li G konečná komutativní grupa s n prvky, pak pro každé $a \in G$ je

$$a^n = e.$$

Důkaz: Označme $G = \{g_1, g_2, \dots, g_n\}$ a zvolme $a \in G$. Ukážeme, že

$$\{g_1, g_2, \dots, g_n\} = \{a \circ g_1, a \circ g_2, \dots, a \circ g_n\}.$$

Zobrazení, které přiřadí prvku g_i prvek $a \circ g_i$ je prosté, protože, pokud $a \circ g_i = a \circ g_j$, pak po aplikaci a^{-1} zleva máme $g_i = g_j$. Uvedené množiny jsou tedy stejně početné a tedy stejné a mají tedy stejný součin všech prvků:

$$a \circ g_1 \circ a \circ g_2 \circ \dots \circ a \circ g_n = g_1 \circ g_2 \circ \dots \circ g_n = u$$

Díky komutativnímu zákonu se rovnost dá přepsat na $a^n \circ u = u$ a dokazovaná rovnost plyne aplikací u^{-1} na obě strany rovnosti.

Podgrupy

Podgrupa P je podmnožina grupy G se stejnou operací, která je sama grupou. Tj. P musí mít (stejný) jednotkový prvek a každý prvek z P musí mít inverzi v P .

Příklady:

- \mathbf{Q} a \mathbf{Z} je podgrupa grupy \mathbf{R} s operací $+$,
- $\mathbf{Q} \setminus \{0\}$ je podgrupa grupy $\mathbf{R} \setminus \{0\}$ s operací \cdot ,
- symetrické matice tvoří podgrupu čtvercových matic s operací $+$,
- matice s $\det = 1$ tvoří podgrupu regulárních matic s operací \cdot ,
- Sudá čísla tvoří podgrupu \mathbf{Z} s operací $+$,
- Kladná čísla tvoří podgrupu grupy \mathbf{R} s operací \cdot .

Vlastnosti pologrupy „krát modulo m “

Předpokládejme množinu $\{0, 1, 2, \dots, m-1\}$ s operací „krát modulo m “, tj. $a \circ b = a \cdot b$ pro $a \cdot b < m$, jinak $a \circ b$ je zbytek po dělení čísla $a \cdot b$ číslem m . Je to pologrupa. Tato pologrupa má jednotkový prvek: 1.

Tvrzení: je-li m složené, tj. $m = n_1 \cdot n_2$, ($n_1 \neq 1$, $n_2 \neq 1$) pak číslo n_1 nemá inverzní prvek.

Důkaz: $v \circ n_1 = z$, tj. $vn_1 = kn_1n_2 + z$, tj. $z = n_1(v - kn_2)$, takže z musí být násobek n_1 a nemůže tedy být roven jedné.

Tvrzení: je-li m prvočíslo, pak množina $\{1, 2, \dots, m-1\}$ s operací \circ je grupa.

Dokážeme*, že každý nenulový prvek a má inverzi. Platí totiž, že $\{a, 2 \circ a, \dots, (m-1) \circ a\} = \{1, \dots, m-1\}$. Důvod: pro $k_1 \neq k_2$ je $a \circ k_1 \neq a \circ k_2$, protože z $a(k_1 - k_2) = km$ plyne $k_1 - k_2 = k'm$ (je a nesoudělné s m). Protože $0 \leq k_1 - k_2 < m$, musí $k' = 0$, takže $k_1 = k_2$.

Malá Fermatova věta

Nechť p je prvočíslo, nechť a je přirozené číslo, $a < p$. Pak

$$a^{p-1} = 1 \pmod{p}.$$

Důkaz: stačí si uvědomit, že grupa $\{1, 2, \dots, p-1\}$ s operací „krát modulo p “ má $p-1$ prvků a použít větu ze stránky [8].

Množina se dvěma operacemi: okruh, těleso

Definice: *Okruh* je množina T s operacemi $+$ a \cdot , pro které platí:

- (1) T s operací $+$ je komutativní grupa (neutrální prvek značíme 0),
- (2) T s operací \cdot je pologrupa,
- (3) $\forall x, y, z \in T$ platí $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.
... (distributivní zákon).

Definice: *Těleso* je množina T s operacemi $+$ a \cdot , pro které platí:

- (1) T s operací $+$ je komutativní grupa (neutrální prvek značíme 0),
- (2) $T \setminus \{0\}$ s operací \cdot je grupa (jednotkový prvek značíme 1),
- (3) $\forall x, y, z \in T$ platí $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$, $(y + z) \cdot x = (y \cdot x) + (z \cdot x)$.
... (distributivní zákon).

Pozorování: Každé těleso musí mít aspoň dva prvky: 0 a 1 .

Varianty okruhů a těles

Předpokládejme množinu T s vlastnostmi (1) a (3).

- Je-li T s operací \cdot komutativní pologrupa, pak T se nazývá *komutativní okruh*.
- Je-li T s operací \cdot pologrupa a má-li jednotkový prvek, pak T se nazývá *okruh s jednotkou*.
- Je-li T s operací \cdot komutativní pologrupa a má-li jednotkový prvek, pak T se nazývá *komutativní okruh s jednotkou*.
- Je-li $T \setminus \{0\}$ s operací \cdot komutativní grupa, pak T se nazývá *komutativní těleso*.

Poznámčička: příklad nekomutativního tělesa (kvaterniony) pro nedostatek místa vynecháme. Všechna ostatní tělesa, o kterých budeme mluvit, jsou komutativní tělesa. Takže slovo „komutativní“ nebudeme v případě těles nadále zdůrazňovat.

Příklady

- Množina reálných čísel s operacemi $+$ a \cdot tvoří těleso.
- Množiny \mathbf{Q} a \mathbf{C} s operacemi $+$ a \cdot jsou také tělesa.
- Množina \mathbf{Z} s operacemi $+$ a \cdot je to komutativní okruh s jednotkou.
- Množina sudých celých čísel s $+$ a \cdot je komutativní okruh.
- Množina regulárních matic s operacemi $+$ a \cdot není těleso ani okruh, protože součet dvou reg. matic nemusí být regulární.
- Množina čtvercových matic (stejného typu) s operacemi $+$ a \cdot je nekomutativní okruh s jednotkou. Není to těleso.
- Množina $\{0, 1\}$ s operacemi $0 + 0 = 0$, $0 + 1 = 1 + 0 = 1$, $1 + 1 = 0$, $0 \cdot a = a \cdot 0 = 0$, $1 \cdot a = a \cdot 1 = a$, tvoří těleso.
- Množina $\{0, 1, \dots, p - 1\}$ s operacemi „+ modulo p “ a „krát modulo p “ tvoří těleso, právě když je p prvočíslo. Jinak je to okruh.

Konečná (Galoisova) tělesa

Dá se ukázat, že pokud je těleso T konečné, pak nastává jen jedna z následujících možností:

- $T = \{0, 1, 2, \dots, p - 1\}$ s operací „+ modulo p “ a „krát modulo p “, kde p je prvočíslo. Toto těleso se značí \mathbf{Z}_p a má p prvků.
- T je množina všech polynomů nad \mathbf{Z}_p stupně menšího než n s operacemi „plus a krát modulo ireducibilní polynom stupně n “. Toto těleso má p^n prvků, podrobněji se k němu vrátíme za chvíli.

Jiné konečné těleso (až na izomorfismus) neexistuje. Konečná tělesa se někdy značí $\text{GF}(p^n)$, kde argument informuje o počtu prvků tělesa a GF je zkratka pro „Galois field“.

Příklady: neexistuje těleso, které má 6 prvků. Existuje ale těleso, které má 8 prvků: $\text{GF}(2^3)$ nebo 9 prvků: $\text{GF}(3^2)$.

\mathbf{Z}_5 je těleso, ale \mathbf{Z}_8 není těleso (je to jen okruh).

Základní vlastnosti tělesa

- Pro libovolné $a, b \in T$ je: $a \cdot b = 0$, právě když $a = 0$ nebo $b = 0$.
Důkaz: Nechť $a \neq 0$ a $b \neq 0$. Pak $a \cdot b \neq 0$ z vlastnosti (2) definice tělesa. Obráceně: BÚNO $a = 0$, ukážeme, že $0 \cdot b = 0$. Platí:

$$0 \cdot b = (0 + 0) \cdot b = 0 \cdot b + 0 \cdot b.$$

Přičtením $-(0 \cdot b)$ k oběma stranám rovnosti máme $0 = 0 \cdot b$.

- Jestliže existuje konečný počet jedniček, které v součtu dají nulu, je nejmenší takový počet prvočíslo.

Důkaz: Nejmenší počet jedniček, které dají v součtu nulu, označím λ . Pro spor budiž $\lambda = m \cdot n$, $m < \lambda$, $n < \lambda$. Pak

$$\left(\sum_1^m 1 \right) \cdot \left(\sum_1^n 1 \right) = \sum_1^{m n} 1 = \sum_1^{\lambda} 1 = 0$$

takže (dle předchozí vlastnosti) musí být aspoň jedna závorka nulová. Tj. existuje menší počet jedniček, které mají součet nula.

Charakteristika tělesa

Definice: Charakteristika tělesa λ je nejmenší počet jedniček, které dají v součtu nulu. Pokud konečný počet jedniček s touto vlastností neexistuje, klademe $\lambda = 0$.

Příklady:

- Tělesa \mathbf{Q} , \mathbf{R} , \mathbf{C} mají charakteristiku $\lambda = 0$.
- Těleso \mathbf{Z}_p (p prvočíslo) má charakteristku $\lambda = p$.

Pozorování: z předchozí stránky víme, že charakteristika tělesa je rovna prvočíslu (je-li konečná).

Tvrzení:

- Je-li p charakteristika tělesa, pak $(a + b)^p = a^p + b^p$.
- V tělese \mathbf{Z}_p dokonce platí: $a^p = a$ (díky malé Fermatově větě).
- V obecném tělese s charakteristikou p ovšem neplatí $a^p = a$.

Znovu definice lineárního prostoru

Definice: *Lineární prostor nad tělesem T* je neprázdňá množina L s operacemi $+$: $L \times L \rightarrow L$ a \cdot : $T \times L \rightarrow L$, které splňují vlastnosti:

(+) L s operací $+$ je komutativní grupa, nulový prvek značíme $\vec{0}$,

(A) $\alpha \cdot (\beta \cdot \vec{x}) = (\alpha \cdot \beta) \cdot \vec{x}$ pro všechna $\vec{x} \in L$, $\alpha, \beta \in T$,

(B) $\alpha \cdot (\vec{x} + \vec{y}) = \alpha \cdot \vec{x} + \alpha \cdot \vec{y}$ pro všechna $\vec{x}, \vec{y} \in L$, $\alpha \in T$,

(C) $(\alpha + \beta) \cdot \vec{x} = \alpha \cdot \vec{x} + \beta \cdot \vec{x}$ pro všechna $\vec{x} \in L$, $\alpha, \beta \in T$,

(D) $1 \cdot \vec{x} = \vec{x}$ pro všechna $\vec{x} \in L$.

Pozorování: Pro $T = \mathbf{R}$ se definice shoduje s původní definicí lin. prostoru. Stačí ověřit, že platí (7): $0 \cdot \vec{x} = \vec{0}$ pro všechny $\vec{x} \in L$:

$$0 \cdot \vec{x} = (0 + 0) \cdot \vec{x} = 0 \cdot \vec{x} + 0 \cdot \vec{x},$$

k této rovnosti přičteme $-(0 \cdot \vec{x})$ a dostáváme $\vec{0} = 0 \cdot \vec{x}$.

Aritmetický lineární prostor T^n

je analogií lineárního prostoru \mathbf{R}^n . Množina T^n je množinou všech uspořádaných n -tic prvků z tělesa T s operacemi sčítání n -tic a násobení n -tice skalárem z T , které jsou definovány takto:

$$(1) (a_1, a_2, \dots, a_n) + (b_1, b_2, \dots, b_n) = (a_1 + b_1, a_2 + b_2, \dots, a_n + b_n),$$

$$(2) \alpha \cdot (a_1, a_2, \dots, a_n) = (\alpha \cdot a_1, \alpha \cdot a_2, \dots, \alpha \cdot a_n).$$

Pozorování: Tento lineární prostor má bázi

$$(1, 0, \dots, 0), (0, 1, \dots, 0), \dots, (0, 0, \dots, 1),$$

takže má dimenzi n .

Je-li T konečné těleso, které má m prvků, pak celkový počet vektorů v T^n je m^n .

Každý podprostor prostoru T^n dimenze k má m^k prvků, protože existuje m^k různých lineárních kombinací báze.

Příklad: lineární prostor \mathbf{Z}_2^n

je lineární prostor uspořádaných n -tic jedniček a nul nad tělesem \mathbf{Z}_2 . Prvky tělesa $\mathbf{Z}_2 = \{0, 1\}$ sčítáme podle pravidla

$$0 + 0 = 0, \quad 0 + 1 = 1 + 0 = 1, \quad 1 + 1 = 0$$

a vektory (uspořádané n -tice) sčítáme a násobíme po složkách, jako na předchozí stránce. Jmenovitě pro libovolný $\vec{u} \in \mathbf{Z}_2^n$ je $1 \cdot \vec{u} = \vec{u}$ a $0 \cdot \vec{u} = \vec{o}$. S jinými skaláry nepracujeme.

Příklad: soustava lineárních rovnic v \mathbf{Z}_5

Vyřešíme soustavu lineárních rovnic v \mathbf{Z}_5 s následující rozšířenou maticí. V první eliminační úpravě jsem sečetl první řádek s druhým a dále od třetího odečetl dvojnásobek prvního.

$$\left(\begin{array}{cccc|c} 2 & 3 & 1 & 1 & 4 \\ 3 & 1 & 2 & 2 & 2 \\ 4 & 3 & 3 & 1 & 1 \end{array} \right) \sim \left(\begin{array}{cccc|c} 2 & 3 & 1 & 1 & 4 \\ 0 & 4 & 3 & 3 & 1 \\ 0 & 2 & 1 & 4 & 3 \end{array} \right) \sim \left(\begin{array}{cccc|c} 2 & 3 & 1 & 1 & 4 \\ 0 & 2 & 1 & 4 & 3 \\ 0 & 0 & 1 & 0 & 0 \end{array} \right)$$

Množina řešení přidružené homogenní soustavy $M_0 = \langle (0, 3, 0, 1) \rangle$ a partikulární řešení je např. $(1, 4, 0, 0)$. Všechny principy lineární algebry (o dimenzích, lineárních obalech, bázích) zůstávají v platnosti. Rozdíl proti lin. prostoru nad \mathbf{R} je jen ten, že zde jsou (pod)prostory konečné. Např. M_0 zde má pět prvků (vektor je možné násobit jen čísly 0, 1, 2, 3, 4), takže množinu řešení můžeme zapsat výčtem prvků:

$$M = \{(1, 4, 0, 0), (1, 2, 0, 1), (1, 0, 0, 2), (1, 3, 0, 3), (1, 1, 0, 4)\}$$

Polynom nad komutativním tělesem T

je vzorec

$$a_n x^n + a_{n-1} x^{n-1} + \cdots + a_1 x + a_0$$

kde $a_i \in T$. Tento vzorec vymezuje předpis pro hodnoty zobrazení z T do T (za x dosazujeme prvky z tělesa T a dostáváme hodnoty polynomu: prvky z tělesa T).

Rovnost polynomů: dva polynomy se rovnají, když se rovnají jejich odpovídající koeficienty (až na případné přebytečné nulové koeficienty s nejvyššími indexy).

Pozor: rovnost není zaručena rovností zobrazení $T \rightarrow T$.

Příklad: Polynom $x^2 + 1$ nad \mathbf{Z}_2 odpovídá zobrazení $0 \rightarrow 1, 1 \rightarrow 0$. Polynom $x^3 + 1$ odpovídá stejnému zobrazení, ale není to stejný polynom.

Operace s polynomy nad tělesem

Součet, rozdíl nebo součin polynomů nad T provedeme jako součet, rozdíl nebo součin příslušných vzorců. Přitom provádíme výpočty s jednotlivými koeficienty polynomů za použití operací v tělese T .

Příklad: Sečteme polynomy nad \mathbf{Z}_5 :

$$(2x^3 + 4x^2 + 2x + 1) + (3x^2 + 2x) = 2x^3 + (4+3)x^2 + (2+2)x + 1 = 2x^3 + 2x^2 + 4x + 1.$$

Příklad: Vynásobíme polynomy nad \mathbf{Z}_5 :

$$\begin{aligned} & (2x^3 + 4x^2 + 2x + 1) \cdot (3x^2 + 2x) = \\ & = (2 \cdot 3)x^5 + (4 \cdot 3)x^4 + (2 \cdot 3)x^3 + 3x^2 + (2 \cdot 2)x^4 + (4 \cdot 2)x^3 + (2 \cdot 2)x^2 + 2x = \\ & = x^5 + 2x^4 + x^3 + 3x^2 + 4x^4 + 3x^3 + 4x^2 + 2x = \\ & = x^5 + (2 + 4)x^4 + (1 + 3)x^3 + (3 + 4)x^2 + 2x = \\ & = x^5 + x^4 + 4x^3 + 2x^2 + 2x \end{aligned}$$

Částečný podíl polynomů

Věta: pro každé dva polynomy p, q (q nenulový) existují jednoznačně polynomy r, z tak, že

1) $p = r \cdot q + z,$

2) stupeň z je menší než stupeň q .

Algoritmus částečného dělení polynomu polynomem lze použít stejně nad libovolným tělesem. Naučili jsme se ho používat pro polynomy nad \mathbf{R} a nyní jej budeme používat pro polynomy nad libovolným tělesem. Zaskočit nás může jen úkon dělení koeficientu a koeficientem b , což je ale v každém komutativním tělese proveditelné jako $a \cdot b^{-1}$.

Příklad: algoritmus částečného podílu

Vydělíme polynomy nad \mathbf{Z}_5 . V tomto případě si uvědomíme, že $3^{-1} = 2$, protože $3 \cdot 2 = 1$ modulo 5. Takže například první krok algoritmu obsahuje výpočet $2x^3 : 3x^2 = (2 \cdot 3^{-1})x = (2 \cdot 2)x = 4x$

$$\begin{array}{r}
 (2x^3 + 4x^2 + 2x + 1) : (3x^2 + 2x) = 4x + 2 \\
 - (2x^3 + 3x^2) \\
 \hline
 x^2 + 2x + 1 \\
 - (x^2 + 4x) \\
 \hline
 -2x + 1
 \end{array}$$

Podíl daných polynomů roven $4x + 2$ a zbytek je $-2x + 1 = 3x + 1$.

Operace modulo polynom

Srovnajme dvě tvrzení:

- Pro každé dvě celá čísla a, b (b nenulové) existují celá čísla r, z tak, že $a = rb + z$, přitom $0 \leq z < b$. Číslo z je zbytek po dělení a číslem b .
- Pro každé dva polynomy p, q (q nenulový) existují polynomy r, z tak, že $p = r \cdot q + z$, přitom $\text{st}z < \text{st}q$. Polynom z je zbytek po dělení p polynomem q .

Tak jako můžeme pro dvě čísla najít zbytek po dělení, můžeme pro dva polynomy najít zbytek po dělení. Je-li dán nenulový polynom, modul q , pak každý polynom p můžeme ztotožnit se zbytkem po dělení p polynomem q . Označíme-li z tento zbytek, pak říkáme:

$$p = z \quad \text{modulo } q.$$

Okruh polynomů modulo polynom

Zvolme nenulový polynom q stupně n jako modul a prvočíslo p . Symbolem $\mathbf{Z}_p[x]/q$ označíme množinu všech polynomů nad tělesem \mathbf{Z}_p , která má stupeň menší než n . Zavedeme tyto operace:

- **Sčítání** prvků z $\mathbf{Z}_p[x]/q$: provedeme jako obvyklé sčítání polynomů nad \mathbf{Z}_p . Stupeň součtu je jistě menší než n , takže leží v $\mathbf{Z}_p[x]/q$. Množina $\mathbf{Z}_p[x]/q$ s tímto sčítáním zjevně tvoří komutativní grupu.
- **Násobení** prvků a $\mathbf{Z}_p[x]/q$: provedeme obvyklé násobení polynomů nad \mathbf{Z}_p . Pokud stupeň výsledku je větší nebo roven n , provedeme navíc na výsledek operaci „modulo polynom q “. Množina $\mathbf{Z}_p[x]/q$ s tímto násobením je pologrupa.

Platí distributivní zákony: tj. množina $\mathbf{Z}_p[x]/q$ s uvedenými operacemi je okruh.

Ireducibilní polynom

Polynom q je *ireducibilní*, právě když jej nelze rozložit na součin dvou polynomů nižších stupňů.

Příklad: Polynom $x^2 + x + 1$ nad \mathbf{Z}_2 je ireducibilní, protože kdyby šel rozložit na součin polynomů nižších stupňů, pak je to součin kořenových činitelů, ale tento polynom v \mathbf{Z}_2 nemá kořeny (vyzkoušejte postupným dosazením čísel 0 a 1).

Příklad: Polynom $x^3 + x + 1$ nad \mathbf{Z}_2 je ireducibilní (ze stejných důvodů).

Příklad: Polynom $x^5 + x^4 + 1$ nad \mathbf{Z}_2 je reducibilní, protože

$$x^5 + x^4 + 1 = (x^3 + x + 1) \cdot (x^2 + x + 1).$$

V případě polynomu stupně 4. a více nám test existence kořenů k rozhodnutí o ireducibilitě nepomůže.

Polynomy modulo ireducibilní polynom

Dá se ukázat, že pokud je polynom q ireducibilní, pak okruh $\mathbf{Z}_p[x]/q$ je těleso, tj. každý polynom z množiny $\mathbf{Z}_p[x]/q$ má při operaci násobení inverzní polynom.

Důkaz* se dá provést anologicky, jako s čísly. Povšimneme si této podobnosti:

- p je prvočíslo, tj. nelze rozložit na součin menších čísel.
- q je ireducibilní, tj. nelze rozložit na součin polynomů menších stupňů.

Je možné přečíst důkaz tvrzení ze stránky [10] znovu, jen slovo číslo nahradíme slovem polynom, slovo prvočíslo slovem ireducibilní polynom a výrok „číslo a je menší než b “ výrokem „stupeň polynomu p je menší než stupeň q “.

Příklad: těleso $\mathbf{Z}_2[x]/(x^3 + x + 1)$

Modul $(x^3 + x + 1)$ je ireducibilní. Toto těleso obsahuje:

$$\mathbf{Z}_2[x]/x^3 + x + 1 = \{0, 1, x, x + 1, x^2, x^2 + 1, x^2 + x, x^2 + x + 1\}$$

Sčítání prvků provádíme jako sčítání polynomů nad \mathbf{Z}_2 , například:

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

Násobení prvků provádíme jako násobení polynomů nad \mathbf{Z}_2 s případnou dodatečnou operací „modulo $x^3 + x + 1$ “. Například:

$$(x + 1) \cdot (x^2 + x) = x^3 + x = 1 \quad \text{modulo } (x^3 + x + 1)$$

Vidíme, že prvky $x + 1$ a $x^2 + x$ jsou si vzájemně inverzní.

Toto je příklad tělesa, který obsahuje 8 prvků, je to tedy $\text{GF}(2^3)$.

- Má-li ireducibilní modul q stupeň n , je $\mathbf{Z}_p[x]/q = \text{GF}(p^n)$.

Příklad: komplexní čísla

Polynom $x^2 + 1$ je nad \mathbf{R} ireducibilní. Označme symbolem $\mathbf{R}[x]$ všechny polynomy nad \mathbf{R} a dále $\mathbf{R}[x]/(x^2 + 1)$ bude značit množinu všech polynomů nejvýše prvního stupně s obvyklou operací $+$ a s operací „krát modulo polynom $x^2 + 1$ “. Takže

$$\mathbf{R}[x]/(x^2 + 1) = \{a + bx; a, b \in \mathbf{R}\}$$

Dva polynomy v $\mathbf{R}[x]/(x^2 + 1)$ sčítáme podle pravidla:

$$(a + bx) + (c + dx) = (a + c) + (b + d)x.$$

Dva polynomy v $\mathbf{R}[x]/(x^2 + 1)$ násobíme podle pravidla:

$$\begin{aligned} (a + bx) \cdot (c + dx) &= bdx^2 + (ad + bc)x + ac = \\ &= (ac - bd) + (ad + bc)x \quad \text{modulo } x^2 + 1 \end{aligned}$$

Nahrazením symbolu x symbolem i shledáváme, že těleso $\mathbf{R}[x]/(x^2 + 1)$ je izomorfní s tělesem komplexních čísel.