ALGEBRA

Grupy, okruhy a Galoisove polia

doc. RNDr. Štefan Peško, CSc.

Katedra matematických metód, FRI ŽU

11. decembra 2015

Binárne operácie – opakovanie

Nech je X neprázdna množina. Potom zobrazenie $\circ : X \times X \to X$ nazývame binárnou operáciou na množine X.
Binárna operácia $\circ$ na množine X sa nazýva

- asociatívna, ak pre všetky $x, y, z \in X$ platí

$$x \circ (y \circ z) = (x \circ y) \circ z.$$

- komutatívna, ak pre všetky $x, y \in X$ platí

$$x \circ y = y \circ x.$$

Prvok $e \in X$ sa nazýva neutrálny prvok binárnej operácie $\circ$ na množine X, ak pre všetky $x \in X$ platí

$$x \circ e = e \circ x = x.$$

Ak má binárna operácia $\circ$ na množine X neutrálny prvok e a k danému prvku $x \in X$ existuje prvok $y \in Y$ tak, že

$$x \circ y = y \circ x = e,$$

hovoríme, že y je inverzný prvok k prvku x.

Algebraická štruktúra

Usporiadanú n-ticu $(M, \circ_1, \circ_2, \ldots, \circ_{n-1})$, kde M je neprázdna množina a $\circ_1, \circ_2, \ldots, \circ_{n-1}$ sú binárne operácie na množine M, nazývame algebraická štruktúra.

Príklad 7.1

a) Usporiadaná trojica $(\mathbb{Z}_p, +, \cdot)$ je algebraická štruktúra s dvoma binárnymi operáciami $+$ a $\cdot$ na množine $\mathbb{Z}_p$.

b) Usporiadaná dvojica $(\mathbb{R}^{n\times n}, \cdot)$ je algebraická štruktúra s jednou binárnou operáciou násobenia matíc na množine všetkých reálnych štvorcových matíc stupňa n.

c) Max-plus algebra (Vorobyev,1967) je algebraická štruktúra $(\mathbb{R}_{max}, \oplus, \odot)$ definovaná na množine $\mathbb{R}_{max} = \mathbb{R} \cup \{-\infty\}$ s binárnymi operáciami $x \oplus y = max\{x, y\}, x \odot y = x + y$.

Grupa

Grupoid je algebraická štruktúra s jednou binárnou operáciou $(M, \circ)$.

Pologrupa je taký grupoid, ktorého operácia $\circ$ je asociatívna.

Grupa je taká pologrupa $(M, \circ)$ s neutrálnym prvkom, v ktorej ku každému prvku $a \in M$ existuje inverzný prvok $a^{-1} \in M$.

Ak je operácia $\circ$ komutatívna, hovoríme o komutatívnom grupoide, pologrupe a grupe. Komutatívna grupa sa nazýva aj abelovská grupa.

Príklad 7.2

Je daná množina $A = \{a, b\}$. Množina jej všetkých podmožín $\mathcal{P}(A) = \big\{\emptyset, \{a\}, \{b\}, \{a, b\}\big\}$.

Potom $(\mathcal{P}(A), \cup)$ je komutatívny grupoid s neutrálnym prvkom $\emptyset$ a $(\mathcal{P}(A), \cap)$ je komutatívny grupoid s neutrálnym prvkom A.

Príklad 7.3

Binárna operácia skladania permutácií $\circ$ na množine všetkých permutácií množiny $\langle n \rangle$ je definovaná takto: Pre $\pi, \psi \in \Pi_n$ je $(\pi \circ \psi)(i) = \psi(\pi(i)), i \in \langle n \rangle$. Neutrálnym prvkom je identická permutácia $\varepsilon = (1, 2, \ldots, n)$. Ku každej $\pi \in \Pi_n$ existuje invezná permutácia $\pi^{-1} \in \Pi_n$. $S_n = (\Pi_n, \circ)$ je nekomutatívna grupa.

Cvičenie 7.1

a) Overte, že usporiadaná dvojice $(\mathbb{Z}_p, +)$ a $(\mathbb{Z}_p, \cdot)$ sú pologrupy, pričom obe operácie sú komutatívne a majú neutrálne prvky 0 a 1. Presvedčte sa, že v prípade, ak p nie je prvočíslo, potom k niektorým prvkom pologrupy $(\mathbb{Z}_p - \{0\}, \cdot)$ neexistuje inverzný prvok.

b) Usporiadaná dvojica $(\mathbb{R}^{n\times n}, \cdot)$ je pologrupa, v ktorej operácia násobenia matíc nie je komutatívna. Aká matica je jej neutrálnym (resp. inverzným) prvkom, ak existuje? Akú ďalšiu vlastnosť musí mať množina matíc, aby ku každej matici existoval inverzný prvok?

c) Nech je $q(x)$ normovaný polynóm stupňa $n \geq 0$ nad poľom $\mathbb{P}$,

- $\mathbb{P}/q(x)$ je množina všetkých polynómov nad poľom $\mathbb{P}$ stupňa nanajvýš $n-1$,
- $\forall a(x), b(x) \in \mathbb{P}/q(x)$ je $a(x) \oplus b(x) = a(x) + b(x)$
- $\forall a(x), b(x) \in \mathbb{P}/q(x)$ je $a(x) \odot b(x) = a(x) \cdot b(x) \bmod q(x)$.

Overte, že usporiadané dvojice $(\mathbb{P}/q(x), \oplus)$ a $(\mathbb{P}/q(x), \otimes)$ sú komutatívne pologrupy.

O krátení v grupe

Tvrdenie 7.1

Nech $(M, \circ)$ je grupa. Nech $a, b, q \in M$.

(i) Ak platí $q \circ a = q \circ b$, potom platí $a = b$,

(ii) Ak platí $a \circ q = b \circ q$, potom platí $a = b$.

Dôkaz:

(i) K prvku q existuje inverzný prvok q^{-1}. Vynásobme zľava prvkom q^{-1} rovnicu $q \circ a = q \circ b$.

$$\begin{aligned} q^{-1} \circ (q \circ a) &= q^{-1} \circ (q \circ b) \\ (q^{-1} \circ q) \circ a &= (q^{-1} \circ q) \circ b \\ e \circ a &= e \circ b \\ a &= b \end{aligned}$$

Analogicky sa dokáže (ii).

Príklad 7.3

$(Z_4, +)$ je abelovská grupa.

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

0 je neutrálny prvok, 1 inverzný prvok 3 a naopak, 0 aj 2 sú rovné svojim inverzným prvkom.

Dôsledkom tvrdeniu (i) je, že v každom v riadku Cayleyho tabuľky sú všetky prvky navzájom rôzne. Podobný je dôsledok tvrdenia (ii) o rôznych prvkoch v stĺpcoch tabuľky.

Tvrdenie 7.2

V grupe $(M, \circ)$ má rovnica

(i) $a \circ x = b$ jediné riešenie $x = a^{-1} \circ b$,

(ii) $y \circ a = b$ jediné riešenie $y = b \circ a^{-1}$.

Dôkaz: (i) Dosadením $x = a^{-1} \circ b$ do rovnice $a \circ x = b$ overíme $a \circ x = a \circ (a^{-1} \circ b) = (a \circ a^{-1}) \circ b = e \circ b = b$. Jednoznačnosť riešenia dokážeme sporom: Nech x_1, x_2 sú dve rôzne riešenia t.j. $a \circ x_1 = b$ a $a \circ x_2 = b$. Vynásobením $a \circ x_1 = a \circ x_2$ prvkom a^{-1} zľava dostaneme

$$\begin{aligned} a^{-1} \circ (a \circ x_1) &= a^{-1} \circ (a \circ x_2) \\ (a^{-1} \circ a) \circ x_1 &= (a^{-1} \circ a) \circ x_2 \\ e \circ x_1 &= e \circ x_2 \\ x_1 &= x_2 \end{aligned}$$

čo je spor s predpokladom dvoch rôznych riešení. Analogicky (ii). ■

Príklad 7.3 – pokračovanie

V abelovskej grupe $(Z_4, +)$ riešme rovnicu $1 + x = 0$.

$$x = 1^{-1} + 0 = 3 + 0 = 3.$$

Tvrdenie 7.3

Nech $(M, \circ)$ je grupa. Inverzný prvok k prvku $a \in M$ je určený jednoznačne.

Dôkaz sporom:
Pre dve rôzne inverzné prvky a_1^{-1}, a_2^{-1} k prvku a platí

$$a_1^{-1} \circ a = e, \quad a_2^{-1} \circ a = e.$$

Z rovnosti pravých strán máme

$$a_1^{-1} \circ a = a_2^{-1} \circ a.$$

Podľa tvrdenia *7.1 (ii)* je potom $a_1^{-1} = a_2^{-1}$, čo je spor.

Podgrupa grupy

Nech $\mathcal{G} = (G, \circ)$ a $\mathcal{H} = (H, \odot)$ sú dve grupy. Ak $H \subseteq G$ a pre každé dva prvky $x, y \in H$ platí

$$x \odot y = x \circ y$$

potom hovoríme, že grupa $\mathcal{H}$ je podgrupou grupy $\mathcal{G}$.
Ak naviac $H \neq G$, hovoríme, že $\mathcal{H}$ je vlastná podgrupa grupy $\mathcal{G}$.

Príklad 7.4

- $(\mathbb{Z}, +)$ je vlastná podgrupa grupy $(\mathbb{Q}, +)$,
- $(\mathbb{Q}, +)$ je vlastná podgrupa grupy $(\mathbb{R}, +)$,
- $(\mathbb{R}, +)$ je vlastná podgrupa grupy $(\mathbb{C}, +)$.

Neutrálne prvky podgrúp

Tvrdenie 7.4

Nech grupa $(B, \odot)$ je podgrupou grupy $(A, \circ)$. Nech e_A, e_B sú po rade neutrálne prvky grúp $(A, \circ), (B, \odot)$. Potom $e_A = e_B$.

Dôkaz:

Pre neutrálny prvok e_B grupy $(B, \odot)$ platí $e_B \in A$ a

$$e_B = e_B \odot e_B = e_B \circ e_B.$$

Pre neutrálny prvok e_A grupy $(A, \circ)$ je $e_B = e_B \circ e_A$. Máme $e_B \circ e_B = e_B \circ e_A$ a tak z tvrdenia *6.1 (i)* je $e_A = e_B$. ■

Príklad 7.4 – pokračovanie

Prvok 0 je spoločným neutrálnym prvkom abelovských grúp

$$(\mathbb{Z}, +), \quad (\mathbb{Q}, +), \quad (\mathbb{R}, +), \quad (\mathbb{C}, +).$$

Tvrdenie 7.5

Nech $(G, \circ)$ je grupa s neutrálnym prvkom e. Nech $H \subset G, H \neq \emptyset$. Potom $(H, \circ)$ je podgrupa grupy $(G, \circ)$ vtedy a len vtedy, ak

(i) pre každé dva prvky $x, y \in H$ je aj $x \circ y \in H$,

(ii) pre každý prvok $x \in H$ je aj inverzný prvok $x^{-1} \in H$.

Dôkaz:

Ak je $(G, \circ)$ grupa a $H \subset G, H \neq \emptyset$ a platí (i), potom je binárna operácia $\circ$ asociatívna aj na H.

Ak platí (ii), potom aj $x \circ x^{-1} = e \in H$. A tak je $(H, \circ)$ grupa. ■

Príklad 7.5

Grupa $\mathcal{H} = (\{0, 3\}, \oplus)$ s neutrálnym prvkom 0 je podgrupou grupy $\mathcal{G} = (\{0, 1, 2, 3\}, \oplus)$.

$\oplus$	0	3	1	2
0	0	3	1	2
3	3	0	2	1
1	1	2	0	3
2	2	1	3	0

Príklad 7.6

Označme $\mathbb{C}^* = \mathbb{C} - \{0\}$. Najskôr ukážeme, že $(\mathbb{C}^*, \cdot)$ tvorí abelovskú grupu.

Z vlastnosti operácie násobenia komplexných čísel vyplýva, že sa jedná o komutatívnu pologrupu s neutrálnym prvkom je 1. Inverzný prvok k prvku $a + ib \in \mathbb{C}^*$ je

$$(a + ib)^{-1} = \frac{a}{a^2 + b^2} - i\frac{b}{a^2 + b^2} \in \mathbb{C}^*.$$

Označme množinu $\mathbb{C}_1 = \{z \in \mathbb{C} : |z| = 1\}$. Aplikujme tvrdenie *7.5*. Zrejme $\emptyset \neq \mathbb{C}_1 \subset \mathbb{C}$. Nech $x, y \in \mathbb{C}_1$. Potom $|xy| = |x||y| = 1$ to znamená, že $xy \in \mathbb{C}_1$ a platí (i). Máme $1 \in \mathbb{C}_1$ a pre $z \in \mathbb{C}_1$ je aj $z^{-1} = \overline{z} \in \mathbb{C}_1$ a platí (ii). A tak je $(\mathbb{C}_1, \cdot)$ nekonečná vlastná podgrupa grupy $(\mathbb{C}^*, \cdot)$.

Bonusový príklad 7.1

1. (2b) Nech $M = \{(a, b) : a, b \in \mathbb{R}, a < 0 < b\}$ je množina otvorených intervalov reálnych čísel. O aké algebraické štruktúry $(M, \cup)$ a $(M, \cap)$ sa jedná?
2. (3b) Rozhodnite, či grupoid $(\mathbb{Z}^{3\times 3}, +)$ s operáciou sčítania matíc je grupa, prípadne či nie je abelovská.
3. (x3b) Je daná neúplná Cayleyho tabuľka pre binárnu operáciu $\circ$ na množine $M = \{a, b, c, d\}$

$\circ$	a	b	c	d
a	b	d	a	c
b	.	.	.	a
c	.	.	.	.
d	.	.	.	b

Doplňte tabuľku tak, aby grupoid $(M, \circ)$

a) bol pologrupou, ktorá nie je grupou,
b) mal neutrálny prvok a nebol pologrupou,
c) bol abelovskou grupou.

Bonusový príklad 7.2

1. (3b) V grupe $(M, \otimes)$ nájdite inverzný prvok k prvku $a \otimes b$, ak poznáme inverné prvky a^{-1} a b^{-1}.
2. (4b) Majme dané dve prvky a, b abelovskej grupy $(M, \circ)$. Nájdite riešenie systému dvoch rovníc o dvoch neznámych

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

3. (5b) Nech $\mathbf{A}, \mathbf{B} \in \mathbb{R}^{4\times 4}$ sú dané regulárne matice. Nájdite riešenie $\mathbf{X}, \mathbf{Y} \in \mathbb{R}^{4\times 4}$ takéhoto systému dvoch maticových rovníc

$$\mathbf{AX} = \mathbf{B}, \quad \mathbf{YB} = \mathbf{X}.$$

4. (6b) Zostavte Cayleyho tabuľku grupovej operácie skladania permutácií v grupe S_3 a nájdite všetky podgrupy grupy S_3; (viď. príklady *7.3* a *7.5*).

Bonusový príklad 7.3

Nech $n \geq 3$ je prirodzené číslo. Označme ε identickú permutáciu na množine $\langle n \rangle$ (viď. príklad 6.3) a ρ cyklickú permutáciu $1 \to 2 \to 3 \to \cdots \to (n-1) \to n \to 1$.

1. (3b) Ukážte, že permutácie $\varepsilon = \rho^0$, $\rho = \rho^1, \ldots, \rho^k, \ldots, \rho^{n-1}$ predstavujú otočenie (proti smeru hodinových ručičiek) pravidelného n-uholníka s vrcholmi $1, 2, \ldots, n$ o uhly $2k\pi/n$ pre $0 \leq k \leq n-1$.
2. (6b) Dokážte, že množina permutácií $\Phi = \{\varepsilon, \rho, \ldots, \rho^{n-1}\}$ s binárnou operáciou skladania permutácii $\circ$ vytvára podgrupu grupy S_n.
3. (8b) Dokážte, že množina všetkých párnych permutácii množiny $\langle n \rangle$ tvorí vlastnú podgrupu grupy S_n.

Okruh

Nech M je neprázdna množina a nech $\oplus$ a $\odot$ sú dve binárne operácie na množine M. Algebraickú štruktúru $\mathcal{O} = (M, \oplus, \odot)$ nazveme okruh ak

- $(M, \oplus)$ je abelovská grupa,
- $(M, \odot)$ je pologrupa,
- operácia $\odot$ je distributívna vzhľadom k operácii $\oplus$ t.j. platia distributívne zákony:

$$\begin{aligned} a \odot (b \oplus c) &= (a \odot b) \oplus (a \odot c), \\ (a \oplus b) \odot c &= (a \odot c) \oplus (b \odot c). \end{aligned}$$

Grupu $(M, \oplus)$ nazývame aditívna grupa okruhu $\mathcal{O}$, binárnu operáciu $\oplus$ aditívna operácia s nulou, neutrálnym prvkom 0; inverzný prvok k $a \in M$ značíme $\ominus a \in M$.

Pologrupu $(M, \odot)$ nazývame multiplikatívna pologrupa okruhu $\mathcal{O}$, jej binárnu operáciu $\odot$ multiplikatívna operácia.

Ak existuje neutrálny prvok multiplikatívnej operácie, tak ho nazveme jednotkou a označíme symbolom 1 a okruh $\mathcal{O}$ nazveme okruhom s jednotkou.

Ak existuje inverzný prvok k prvku $a \in M$, označíme ho $a^{-1} \in M$.

Okruh, v ktorom platí komutatívny zákon vzhľadom na operáciu $\odot$, nazveme komutatívny okruh.

Príklad 7.7

$(\mathbb{Z}, +, \cdot), (\mathbb{Q}, +, \cdot), (\mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sú komutatívne okruhy s jednotkou. Príslušné aditívne abelovské grupy majú nulu 0. Ich multiplikatívne pologrupy majú jednotku 1, no pre prvok 0 v nich neexistuje inverzný prvok.

Tvrdenie 7.6

Nech $(M, \oplus, \odot)$ je okruh. Potom pre všetky $a \in M$ platí $a \odot 0 = 0 \odot a = 0$.

Dôkaz:
Nech 0 je nula. Potom pre $b \in M$ je

$$b \oplus 0 = b.$$

Po roznásobení rovnosti sprava prvkom $a \in M$ a použití distributívneho zákona a krátenia

$$\begin{aligned} (b \oplus 0) \odot a &= b \odot a \\ (b \odot a) \oplus (0 \odot a) &= b \odot a \\ 0 \odot a &= 0. \end{aligned}$$

Analogicky sa dokáže $a \odot 0 = 0$. ■

Príklad 7.8

Na množine celých čísel $\mathbb{Z}$ s binárnymi operáciami $\oplus$ a $\odot$ definovanými vzťahmi

$$a \oplus b = a + b - 1 \qquad a \odot b = a + b - a \cdot b.$$

je $(\mathbb{Z}, \oplus, \odot)$ okruh.

Nulou abelovskej grupy $(\mathbb{Z}, \oplus)$ je 1, pretože $\forall a \in \mathbb{Z}$ je

$$a \oplus 1 = a + 1 - 1 = a,$$
$$1 \oplus a = 1 + a - 1 = a,$$

a tak v pologrupe $(\mathbb{Z}, \odot)$ platí tvrdenie *7.6*

$$a \odot 1 = a + 1 - a \cdot 1 = 1,$$
$$1 \odot a = 1 + a - 1 \cdot a = 1.$$

Neutrálny prvok $1 \in \mathbb{Z}$ okruhu $(\mathbb{Z}, \oplus, \odot)$ je tu nula, zatiaľ čo $1 \in \mathbb{R}$ v okruhu $(\mathbb{R}, +, \cdot)$ je jednotkou!

Teleso a pole

Nech $\mathcal{T} = (M, \oplus, \odot)$ je okruh. Hovoríme, že $\mathcal{T}$ je teleso, ak algebraická štruktúra $(M - \{0\}, \odot)$ je grupou.

Neutrálny prvok tejto grupy budeme nazývať jednotkový prvok telesa $\mathcal{T}$ a budeme značiť 1.

Ak je naviac operácia $\odot$ komutatívna na M hovoríme, že $\mathcal{T}$ je komutatívne teleso resp. pole.

Príklad 7.7 – pokračovanie

Okruhy $(\mathbb{Q}, +, \cdot), \mathbb{R}, +, \cdot), (\mathbb{C}, +, \cdot)$ sú polia.

Príklad 7.9

$(\mathbb{R}, \oplus, \odot)$, kde pre $a, b \in \mathbb{R}$ máme definované binárne operácie $a \oplus b = a + b - 1, a \odot b = a + b - a \cdot b$, je pole s nulovým prvkom 1 a jednotkovým prvkom 0. $(\mathbb{R} - \{1\}, \odot)$ je grupa, nakoľko pre $\forall a \in \mathbb{R} - \{1\}$ existuje inverzný prvok $a^{-1} = \frac{a}{a-1}$.

Cvičenie 7.2

Overte platnosť axiómov poľa $(\mathbb{P}, +, \cdot)$ s nulou 0 a jednotkou 1

(1) $(\forall a, b \in \mathbb{P})(a + b = b + a)$,

(2) $(\forall a, b, c \in \mathbb{P})(a + (b + c) = (a + b) + c)$,

(3) $(\forall a \in \mathbb{P})(a + 0 = a)$,

(4) $(\forall a \in \mathbb{P})(\exists b \in \mathbb{P})(a + b = 0)$,

(5) $(\forall a, b, c \in \mathbb{P})(a \cdot (b + c) = a \cdot b + a \cdot c)$,

(6) $(\forall a, b \in \mathbb{P})(a \cdot b = b \cdot a)$,

(7) $(\forall a, b, c \in \mathbb{P})(a \cdot (b \cdot c) = (a \cdot b) \cdot c)$,

(8) $(\forall a \in \mathbb{P})(1 \cdot a = a)$,

(9) $(\forall a \in \mathbb{P} - \{0\})(\exists b \in \mathbb{P})(a \cdot b = 1)$,

(10) $0 \neq 1$.

Okruh polynómov modulo

Okrem nekonečných polí $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +.\cdot)$ sme doteraz spoznali jediné konečné pole $(\mathbb{Z}_p, \oplus, \odot)$, kde p je prvočíslo, s aditívnou operáciou $\oplus$ a multiplikatívnou operáciou $\odot$

$$\begin{aligned} a \oplus b &= a + b \bmod p, \\ a \odot b &= a \cdot b \bmod p. \end{aligned}$$

Nech $(\mathbb{P}, +.\cdot)$ je pole, $q(x)$ normovaný polynóm stupňa $n \geq 0$ nad poľom $\mathbb{P}$. Okruhom polynómov modulo $q(x)$ rozumieme okruh $(\mathbb{P}/q(x), \oplus, \odot)$, kde

- $\mathbb{P}/q(x)$ je množina všetkých polynómov nad poľom $\mathbb{P}$ stupňa nanajvýš $n-1$,
- pre $a(x), b(x) \in \mathbb{P}/q(x)$ definujeme

$$a(x) \oplus b(x) = a(x) + b(x)$$

- pre $a(x), b(x) \in \mathbb{P}/q(x)$ definujeme

$$a(x) \odot b(x) = a(x) \cdot b(x) \bmod q(x).$$

Príklad 7.10

Nech $q(x) = x^3 + x + 1$ je zvolený normovaný polynóm tretieho stupňa nad poľom $\mathbb{Z}_2$. Množina všetkých polynómov stupňa nanajvýš 2 nad poľom $\mathbb{Z}_2$ je

$$\mathbb{Z}_2/q(x) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

Ak $a(x) = x^2 + 1, b(x) = x + 1$. Obvyklý súčet polynómov $a(x)$ a $b(x)$ nad poľom $\mathbb{Z}_2$ je polynóm

$$a(x) \oplus b(x) = a(x) + b(x) = x^2 + 1 + x + 1 = x^2 + x.$$

Súčin polynómov $a(x)$ a $b(x)$ je tu definovaný ako zvyšok po delení polynómu $a(x) \cdot b(x)$ polynómom $q(x)$

$$\begin{aligned} a(x) \odot b(x) &= a(x) \cdot b(x) \bmod q(x) = \\ &= (x^2+1) \cdot (x+1) \bmod x^3 + x + 1 = \\ &= x^3 + x^2 + x + 1 \bmod x^3 + x + 1 = \\ &= x^2. \end{aligned}$$

1. Polynóm $x^2 + x + 1$ je ireducibilný nad poľom $\mathbb{Z}_2$. Ak by bol reducibilný, potom

$$x^2 + x + 1 = (x + a) \cdot (x + b) = x^2 + (a + b) \cdot x + a \cdot b.$$

   Ale v poli $\mathbb{Z}_2$ neexistujú prvky $a, b \in \mathbb{Z}_2$, aby $a + b \bmod 2 = 1$ a $a \cdot b \bmod 2 = 1$.

2. Ostatné polynómy stupňa 2 sú reducibilné nad poľom $\mathbb{Z}_2$

$$\begin{aligned} x^2 &= x \cdot x, \\ x^2 + x &= x \cdot (x + 1), \\ x^2 + 1 &= (x + 1) \cdot (x + 1). \end{aligned}$$

Aj polynóm $q(x) = x^3 + x + 1$ je ireducibilný nad poľom $\mathbb{Z}_2$. Platí, že $q(0) = q(1) = 1$ a tak ani x ani $x + 1$ nedelí $q(x)$. Skúmať deliteľnosť polynómu $q(x)$ polynómami stupňa 2 už nie je potrebné ;-) prečo?

Tvrdenie 7.7

Pre každý ireducibilný polynóm $q(x)$ nad poľom $\mathbb{P}$ je okruh polynómov $\mathbb{P}/q(x)$ poľom.

Príklad 7.10 – pokračovanie

Overte, že $(\mathbb{Z}_2/q(x), \oplus, \odot)$ je pre $q(x) = x^3 + x + 1$ poľom.

$(\mathbb{Z}_2/q(x), \oplus)$ je abelovská grupa s nulou 0, inverzný prvkom k prvku $a(x) \in \mathbb{Z}_2/q(x)$ je $a(x)$ a binárna operácie $\oplus$ je komutatívna.

$(\mathbb{Z}_2/q(x), \odot)$ je pologrupa, pretože pre násobenie polynómov platí asociatívny zákon $a(x) \cdot (b(x) \cdot c(x)) = (a(x) \cdot b(x)) \cdot c(x)$ a tak aj $a(x) \odot (b(x) \odot c(x)) = (a(x) \odot b(x)) \odot c(x)$. Podobne sa overí, že platia distributívne zákony. A tak $(\mathbb{Z}_2/q(x), \oplus, \odot)$ je okruh.

$(\mathbb{Z}_2/q(x) - \{0\}, \odot)$ je abelovská grupa s jednotkou 1, pretože platí $a(x) \cdot 1 = 1 \cdot a(x) = a(x) \bmod q(x)$. Pomerne pracnými úpravami nájdeme pre $a(x) \in \mathbb{Z}_2/q(x) - \{0\}$ príslušné inverzné prvky:

$$\begin{aligned} 1^{-1} &= 1,\ x^{-1} = x^2 + 1,\ (x+1)^{-1} = x^2 + x,\ (x^2)^{-1} = x^2 + x + 1, \\ (x^2+1)^{-1} &= x,\ (x^2 + x)^{-1} = x + 1,\ (x^2 + x + 1)^{-1} = x^2. \end{aligned}$$

Príklad 7.11

Všetky normované ireducibilné polynómy stupňa 2 nad $\mathbb{Z}_3$ sú

$$\begin{aligned} q_1(x) &= x^2 + x + 2, \\ q_2(x) &= x^2 + 2x + 2, \\ q_3(x) &= x^2 + 1. \end{aligned}$$

Ostatné normované polynómy sú reducibilné:

$$\begin{aligned} x^2 &= x \cdot x, \\ x^2 + 2 &= (x+1) \cdot (x+2), \\ x^2 + x &= x \cdot (x+1), \\ x^2 + x + 1 &= (x+2) \cdot (x+2), \\ x^2 + 2x &= x \cdot (x+2), \\ x^2 + 2x + 1 &= (x+1) \cdot (x+1). \end{aligned}$$

Galoisovo pole (Évariste Galois, 1811–1831)

Pole $(\mathbb{Z}_p/q(x), \oplus, \odot)$, kde p je prvočíslo a $q(x)$ ireducibilný polynóm stupňa n nad poľom $\mathbb{Z}_p$, sa nazýva Galoisovo pole a označuje sa $\mathbb{GP}(p^n)$.

Pre informatiku sú dôležité Galoisove polia nad poľom $\mathbb{Z}_2$, pre konštrukciu ktorých sú potrebné normované ireducibilné polynómy. Ich počty sú:

n	2	3	4	5	6	7	...	14	15
#	1	2	3	6	9	18	...	1161	2182

Príklad 7.12

Všetky normované ireducibilné polynómy stupňa 4 nad $\mathbb{Z}_2$ sú

$$\begin{aligned} q_1(x) &= x^4 + x + 1, \\ q_2(x) &= x^4 + x^3 + 1, \\ q_3(x) &= x^4 + x^3 + x^2 + x + 1. \end{aligned}$$

Ireducibilným polynómom $q_i(x), i = 1, 2, 3$ zodpovedajú 3 typy Galoisových polí typu $\mathbb{GF}(2^4)$ s rovnakým počtom prvkov, ktoré sú izomorfné.

Hovoríme, že polia $(\mathbb{P}_1, +, \cdot)$ a $(\mathbb{P}_2, \oplus, \odot)$ sú izomorfné polia, ak existuje bijekcia $\psi : \mathbb{P}_1 \to \mathbb{P}_2$, ktorá zachováva binárne operácie t.j. pre každé $x, y \in \mathbb{P}_1$ platí

$$\begin{aligned} \psi(x + y) &= \psi(x) \oplus \psi(y), \\ \psi(x \cdot y) &= \psi(x) \odot \psi(y). \end{aligned}$$

Izomorfizmus konečných polí

Tvrdenie 7.8

Každé konečné pole je izomorfné s niektorým Galoisovým poľom. Dve konečné polia s rovnakým počtom prvkov sú izomorfné.

Počet prvkov konečného poľa musí byť buď prvočíslo p (pre $n = 1$ máme $\mathbb{GF}(p^1) = \mathbb{Z}_p$) alebo mocnina prvočísla p^n (pre $n > 1$ máme $\mathbb{GF}(p^n)$). Neexistuje žiadne konečné pole s počtom prvkov

$$6, 10, 12, 14, 15, 18, 20, 21, \ldots$$

Príklad 6.12 – pokračovanie

Galoisovo pole $\mathbb{GF}(2^4)$ je pole $\mathbb{Z}_4/q_1(x)$, pričom sme zvolili ireducibilný polynóm $q_1(x)$. Pri inej voľbe polynómov ($q_2(x)$ resp. $q_3(x)$) dostávame izomorfné polia polynómov.

Ide tu teda o pole, ktorého prvkami je 2^4 plynómov stupňa nanajvýš 3 s operáciou sčítania $\oplus$ a násobena $\odot$.

Reprezentácie Galoisovho poľa

Nenulové prvky $\mathbb{GF}(2^p)$ je vhodné interpretovať v niektorej reprezentácii

- exponenciálnej ako mocniny niektorého polynómu $\alpha(x)$, napr $\alpha(x) = x$,
- binárnej ako postupnosť koeficientov polynómu,
- hexadecimálnej ako obvyklú reprezentaciu p miestnych čísel v dvojkovej sústave symbolmi 0–9, A–F.

Príklad 6.11 – pokračovanie

V Galoisovom poli $\mathbb{GF}(2^3)$ zvolíme ireducibilný polynóm $q(x) = x^3 + x + 1$, má prvky z množiny

$$\mathbb{Z}_2/q(x) = \{0, 1, x, x+1, x^2, x^2+1, x^2+x, x^2+x+1\}.$$

V exponenciálnej reprezentácii zvolíme $\alpha(x) = x$. Potom pre nenulové prvky poľa dostaneme $\alpha^i = x^i \bmod q(x)$ t.j.
$\alpha^0 = 1, \alpha^1 = x, \alpha^2 = x^2,$
$\alpha^3 = x+1, \alpha^4 = x^2+x, \alpha^5 = x^2+x+1, \alpha^6 = x^2+1$ a $\alpha^7 = 1$.

Exponenciálna	*Polynomiálna*	*Binárna*	*Hexadecimálna*
0	*0*	*000*	*"0"*
α^0	1	*001*	*"1"*
α^1	x	*010*	*"2"*
α^2	x^2	*100*	*"4"*
α^3	$x+1$	*011*	*"3"*
α^4	x^2+x	*110*	*"6"*
α^5	x^2+x+1	*111*	*"7"*
α^6	x^2+1	*101*	*"5"*
$\alpha^7=\alpha^0$			

Sčítanie prvkov v $\mathbb{GF}(2^3)$ je jednoduché, príslušné trojbitové slová binárnej reprezentácie sčítame po bitoch v $\mathbb{Z}_2$, napr.

$$001 \oplus 011 = 010.$$

Pre násobenie je výhodná exponenciálna reprezentácia: "7"$\odot$"3"$= \alpha^5 \cdot \alpha^3 = \alpha^8 = \alpha^7 \cdot \alpha = 1 \cdot \alpha =$ "2". Inverzný prvok k prvku α^i je prvok α^{7-i}, platí

$$\alpha^i \cdot \alpha^{7-i} = \alpha^7 = 1 \quad \text{pre } i = 0, 2, \ldots, 6.$$