Algebra

Jaroslav Langer *

Říjen 2020

Contents

*z přednášek NI-MPI/FIT/ČVUT

Abstract

Definice, věty a poznámky z předmětu NI-MPI.

1 Algebra 1.

1.1 Úvod

Věta 1.1

Pro všechna $b, c \in R \setminus \emptyset$ pro rovnici $b \cdot x = c$ existuje právě jedno řešení $x = \frac{c}{b}$

Poznámka

Dvojici $(M, \circ)$, kde $\circ : M \times M \to M$, $\circ$ je asociativní na M, neutrální prvek náleží M a pro každý prvek M inverzní prvek náleží M, říkáme grupa.

1.2 Hierarchie

Definice 2.1

Grupoid (magma) je uspořádaná dvojice $(M, \circ)$, kde M je neprázdná množina a $\circ$ je binární operace na M.

- **Pologrupa** (semigrupa) je grupoid $(M, \circ)$, kde operace $\circ$ je asociativní pro všechny prvky M.
- **Monoid** je pologrupa $(M, \circ)$, kde $\exists e, \forall a, \quad e, a \in M$,
$$a \circ e = e \circ a = a.$$
- **Grupa** je monoid $(M, \circ)$ a $e \in M$ je neutrální prvek, kde $\forall a \exists a^{-1}, \quad e, a \in M$,
$$a \circ a^{-1} = a^{-1} \circ a = e.$$
- **Komutativní (abelovská) grupa** je grupa $(M, \circ)$, kde operace $\circ$ je komutativní na M.

Poznámka

O množině M mluvíme také jako o *nosiči* grupy $(M, \circ)$

Poznámka

Binární operace je *na* M což znamená, že $\circ : M \times M \to M$, také můžeme říci, že množina M ja uzavřená vůči operaci $\circ$.

1.3 Neutrální a inverzní prvky

Věta 4.1

V monoidu existuje právě jeden neutrální prvek.

Věta 4.2

V grupě má každý prvek právě jeden inverzní prvek.

1.4 Znázornění grup

Poznámka

Pokud má množina M konečný počet prvků, pak strukturu dvojic $(M, \circ)$, lze kompletně zachytit Cayleyho tabulkou. Cayleyho tabulka pro $(M, \circ), |M| = n$ je tabulka $n \times n$, kde záhlaví sloupců i řádků jsou stejně seřazené prvky M, políčko $p_{a,b}$ pro a-tý řádek a b-tý sloupec má hodnotu $a \circ b$.

Poznámka

Latinský čtverec pro n prvkovou množinu M je tabulka $n \times n$, kde v každém řádku a sloupci, je každý prvek M právě jednou.

Věta 5.2

Cayleyho tabulka každé grupy tvoří latinský čtverec.

Věta 5.3

V každé grupě $(M, \circ)$ jde jednoznačně dělit. Tzn. $\forall a, b \in M$ mají rovnice

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

jediné řešení.

Poznámka

Grupu $(M, \circ)$ s konečným počtem prvků M lze vizualizovat pomocí *Cayleyho orientovaného grafu*. Cayleyho orientovaný graf

$$(V, E), \quad V = M, \quad E = \{(a, b) : b = a \circ c, \quad \forall a \in M, \forall c \in N \subset V\}$$

2 Algebra 2.

2.1 Podgrupy

Poznámka

Hledáme-li podgrupu $(N, \circ)$ grupy $(M, \circ)$ tak aby obsahovala prvek m, těleso musí zůstat grupou, proto musí také obsahovat všechny prvky tak, aby množina N byla uzavřená na operaci $\circ$, dále musí obsahovat neutrální prvek e, a inverzní prvek pro všechny prvky N. Takovou podgrupu nazýváme **podgrupa generovaná množinou** $\{m\}$.

Definice 6.2 Podgrupa (subgroup) $(N, \circ)$

Buď grupa $G = (M, \circ)$, podgrupa $H = (N, \circ)$ je libovolná dvojice, kde

- $N \subset M$
- $(N, \circ)$ je grupa.

Poznámka

Každá grupa $(M, \circ)$, kde $|M| \geq 2$ má vždy podrgrupy

- $(\{e\}, \circ), e \in M$

- $(N, \circ), N = M$

těmto dvěma podgrupám říkáme **triviální podgrupy**. Ostatní podgrupy nazýváme **valstní (proper)**.

Věta 6.3

Buď grupa $G = (M, \circ)$, pro každé i z indexové množiny I buď H_i podgrupa G, pak

$$H' = \bigcap_{i \in I} H_i$$

je také podgrupa G.

Věta 6.4

Buď grupa $G = (M, \circ), N \subset M \wedge N \neq \emptyset$, pak libovolná dvojice $(N, \circ)$ je podgrupa právě tehdy když

$$\forall a, b \in N, a \circ b^{-1} \in N$$

2.2 Lagrangeova věta

Definice 7.1 Řád (order)

Řádem grupy $G = (M, \circ)$ nazýváme počet prvků M, jeli počet prvků nekonečný, i řád je nekonečný, podle řádů rozdělujeme grupy na **konečné** a **nekonečné.** Řád grupy G značíme $\#G$ (nebo také $|G| = ord(G)$).

Věta 7.3 Lagrangeova

Buď $H = (N, \circ)$ podgrupa konečné grupy $G = (M, \circ)$, potom řád H dělí řád G.

Věta 7.4 Sylowova

Buď grupa konečná G řádu n a p prvočíselný dělitel n. Pokud p^k dělí n (pro k přírozená), potom existuje podgrupa G řádu p^k. (Pro $k = 1$ též Cauchyho věta).

2.3 Generující množiny a generátor grup

Věta 8.1

Buď grupa $G = (M, \circ)$ a $N \subset M \wedge N \neq \emptyset$, pak množina

$$\langle N \rangle = \bigcap \{H : H \text{ je podgrupa grupy } G \text{ obsahující } N\}$$

spolu s operací $\circ$ tvoří podgrupu grupy G obsahující prvek N.

Věta 8.2

Podgrupu $\langle N \rangle$ grupy $G = (M, \circ), N \subset M \wedge N \neq \emptyset$ nazýváme **podgrupou generovanou množinou** N. O množinu N pak nazýváme jako **generující množinu** grupy $\langle N \rangle$. V případě jednoprvkové generující množiny zavádíme značení $\langle a \rangle = \langle \{a\} \rangle$ nazýváme jednoprvkovou množinu **generátor** grupy $\langle a \rangle$.

Poznámka

Pro grupu $G = (M, \circ)$ s neutrálním prvkem $e \in M$ pro každý prvek $g \in M$ a $n \in \mathbb{N}$ zavádíme n-tou a $-n$-tou mocninu takto.

$$\begin{aligned}
g^0 &= e \\
g^1 &= g \\
g^2 &= g \circ g \\
g^n &= g \circ g \circ g ... \circ g \quad (n\text{-krát}) \\
g^{-2} &= g^{-1} \circ g^{-1} \\
g^{-n} &= (g^{-1})^n
\end{aligned}$$

Věta 8.5

Buď grupa $G = (M, \circ)$ a podmnožina $N \subset M \wedge N \neq \emptyset$, potom všechny prvky grupy $\langle N \rangle$ lze získat pomocí grupového obalu

$$\langle N \rangle = \{a_1^{k_1} \circ a_2^{k_2} \circ ... a_n^{k_n} \circ : n \in \mathbb{N}, k_i \in \mathbb{Z}, a_i \in N\}$$

Důsledek

$\langle N \rangle = \{a^k : k \in \mathbb{Z}\}$

2.4 Cyklické grupy

Věta 9.1

Grupa $\mathbb{Z}_n^+$ je rovna $\langle k \rangle, k \in \mathbb{Z}_n^+$ tehdy a jen tehdy, když k a n jsou nesoudělná čísla.

Definice 9.4 Cyklická grupa (cyclic group)

Grupa $G = (M, \circ)$ se nazývá **cyklická**, pokud existuje $a \in M, \langle a \rangle = G$. Prvek a se nazývá **generátor** cyklické grupy G.

Definice 9.5

Buď g prvek grupy $G = (M, \circ)$, existuje-li $m \in \mathbb{N}$ takové, že $g^m = e$, pak nejmenší takové m nazýváme **řádem prvku g**. Neexistuje-li takové m, pak prvek g má řád nekonečno. Řád prvku g značíme $ord(g)$.

Poznámka

Řád prvku g se rovná řádu množiny generované g, platí tedy rovnost

$$ord(g) = \#\langle g \rangle$$

Dále platí, že $g^k = e \Leftrightarrow k = l \cdot ord(g), l \in \mathbb{Z}$

Věta 9.6

Grupa $\mathbb{Z}_n^\times$ je cyklická právě tehdy když $n \in \{2, 4, p^k, 2p^k\}, k \in \mathbb{N}$ a p je liché prvočíslo.

Poznámka

Obecně najít generátor grupy není jednoduché, (třeba pro grupy $\mathbb{Z}_n^\times$). Pokud však jeden známe, je jednoduché najít všechny ostatní.

Věta 9.7

Je-li $G = (M, \circ)$ cyklická grupa řádu n a a nějaký její generátor. Potom a^k je také její tehdy a jen tehdy, když n a k jsou nesoudělné, tedy $gcd(n, k) = 1$

Důkaz

!!! brutus !!!

Poznámka

$\varphi(n)$ je **Eulerova funkce**, každému $n \in \mathbb{N}$ přiřazuje počet přirozených čísel z rozmezí $\langle 1; n)$, která jsou s ním nesoudělná.

Věta 9.8

V cyklické grupě řádu n je počet generátorů roven $\varphi(n)$.

Věta 9.9

Libovolná podgrupa cyklické grupy je opět cyklická grupa.

2.5 (Malá) Fermatova věta

Věta 10.1

V grupě $G = (M, \circ)$ řádu n pro libovolný prvek $a \in M$ platí $a^n = e$, kde e je neutrální prvek.

Poznámka

Grupa $\mathbb{Z}_p^\times$ je cyklická a řádu $p - 1$.

Věta 10.2

Pro libovolné p a libovolné $1 < a < p$

$$a^{p-1} \equiv 1 (mod \quad p). \quad (a^n \equiv a (mod \quad p))$$

3 Algebra 3.

3.1 Homomorfismy a izomorfismy

Definice 11.1

Buď $G = (M, \circ_G), H = (N, \circ_H)$ dva grupoidy, zobrazení $h : M \to N$, nazveme **homomorfismem G do H**, jestliže

$$\forall a, b \in M, h(a \circ_G b) = h(a) \circ_H h(b)$$

Je-li navíc h injektivní, resp. surjektivní, resp. bijektivní, říkáme, že jde o **monomorfismus**, resp. **epimorfismus**, resp. **izomorfismus**.

Definice 11.2

Grupy $G = (M, \circ_G), H = (N, \circ_H)$ nazýváme **izomorfní**, právě tehdy když existuje izomorfismus $h : M \to N$, také říkáme, že G je izomorfní s H.

Poznámka

Vlastnost dvou grup být izomorfní je relace ekvivalence na množině všech grup.

Věta 11.3

Buď homomorfismus grupy $G = (M, \circ_G)$ do grupoidu $H = (N, \circ_H)$ $h : M \to N$, potom $h(G) = (h(M), \circ_H)$ je grupa.

Důsledky: Je-li H grupa, potom

- neutrální prvek G se zobrazí na neutrální prvek H
- inverzní prvek se zobrazí na inverzní prvek H $h(x^{-1}) = h(x)^{-1}$
- je-li h homomorfismus z $G \to H$, $h(G)$ je podgrupa H

Věta 11.4

Libovolné dvě nekonečné cyklické grupy jsou izomorfní. Pro každé $n \in \mathbb{N}$ jsou libovolné dvě cyklické grupy řádu n izomorfní.

Poznámka

$(\mathbb{Z}, +), (\mathbb{Z}, +_n)$ jsou jediné cyklické grupy až na izomorfismus.

Poznámka Kleinova grupa

$(\mathbb{Z}_2 \times \mathbb{Z}_2, \circ)$, kde

$$\mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0,0), (0,1), (1,0), (1,1)\}$$

$\circ$ je modulo 2 po složkách $(1,0) \circ (1,1) = (0,1)$ Kleinova grupa není cyklická, nemůže být tedy izomorfní s $\mathbb{Z}_4^+$

Věta 11.6

Existují pouze dvě neizomorfní grupy řádu 4.

Poznámka (Symetrická grupa)

Symetrickou grupou množiny $\{1, 2, ..., n\}$ nazveme množinu všech permutací s operací skládání zobrazení a značíme ji S_n.

Poznámka

Permutace můžeme zadat výčtem hodnot

$$\begin{pmatrix} 1 & 2 & ... & n \\ \pi(1) & \pi(2) & ... & \pi(n) \end{pmatrix}$$

první řádek můžeme navíc vynechat. **Skládání permutací**

$$\begin{pmatrix} 1 & 2 & 4 & 3 & 5 \end{pmatrix} \circ \begin{pmatrix} 2 & 1 & 3 & 5 & 4 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 4 & 5 & 3 \end{pmatrix}$$

Skládání zobrazení je asociativní, matice

$$\begin{pmatrix} 1 & 2 & ... & n \end{pmatrix}$$

je neutrální prvek a inverzní prvek je inverzní zobrazení, S_n je tedy opravdu grupa a má řád $n!$

Poznámka

Podgrupy symetrické grupy S_n nazýváme **grupami permutací**.

Věta 11.8 (Cayleyova)

Každá konečná grupa G je izomorfní s nějakou grupou permutací.

3.2 Aplikace teorie grup v kryptografii

Definice 12.1 (Problém diskrétního logaritmu na grupě $G = (M, \cdot)$)

Buď $G = (M, \cdot)$ cyklická grupa řádu n, α její generátor a β její prvek. Řešit problém diskrétního logaritmu znamená najít číslo $1 \leq k \leq n$, takové, že

$$\alpha^k = \beta$$

.

Definice 12.2 (Problém diskrétního logaritmu na grupě $G = (M, +)$)

Buď $G = (M, +)$ cyklická grupa řádu n, α nějaký její generátor a β její prvek. Řešit problém diskrétního logaritmu znamená najít číslo $1 \leq k \leq n$, takové, že

$$k \times \alpha = \beta$$

.

Poznámka

Zahodíme li požadavek na cykličnost grupy G, problém má řešení pouze pokud, prvek β patří do cyklické podgrupy $\langle\alpha\rangle$ generované α.

Příklad, kde to lze snadno

Mějme grupu $\mathbb{Z}_p^+$, generátor α, prvek β, řešíme

$$k \times \alpha = \beta \mod p$$

Pomůžeme si grupou $\mathbb{Z}_p^\times$, kde řešením bude,

$$k = \beta \cdot \alpha^{-1} \mod p$$

Obecně

Není znám rozumně rychlý algoritmus řešící problém diskrétního logaritmu.

V případě grupy $\mathbb{Z}_p^\times$ znám algoritmus úměrný $\sqrt{p}$. Inverzní operaci, tedy mocnění umíme naopak velmi rychle (metoda opakovaných čtverců).

Dostáváme tedy **jednosměrnou (one-way) funkci**, kterou lze použít pro kryptografii. Spočítat $\beta = \alpha^x \mod p$ je snadné, známe-li x, α, p, naopak spočítat x známe-li α, β, p je velmi obtížné.

Poznámka: Pro konstrukci RSA šifry bylo použita jednosměrná funkce násobení prvočísel. Vynásobit dvě velká prvočísla je snadný úkol. Rozložit velké číslo na dvě prvočísla je velmi obtížné.

Diffie-Hellman Key Exchange

1. Inicializace:

   Alice zveřejní generátor α a prvočíslo p.

   Alice si zvolí x a spočítá svůj veřejný klíč $A = \alpha^x \mod p$.

   Bob si zvolí tajný klíč y a spočítá svůj veřejný klíč $B = \alpha^y \mod p$.

   Výměna klíčů.

2. Komunikace:

   Alice počítá zprávu jako $k_{AB} = B^x \mod p$.

   Bob počítá zprávu jako $k_{AB} = A^y \mod p$.

Fakta

- Operace mocnění je v $\mathbb{Z}_p^\times$ komutativní a tedy vypočtené k_{AB} je pro oba stejné, protože $k_{AB} \equiv (\alpha^y)^x \equiv (\alpha^x)^y \mod p$
- Mocnění není výpočetně náročné (square nad multiply).
- Řešení diskrétního logaritmu je velmi náročné.

4 Algebra 4.

4.1 Množiny se dvěma binárními operacemi

Definice 13.1 Okruh (Ring)

Buď M neprázdná množina a $+$ a $\cdot$ binární operace na M. Trojice $R = (M, +, \cdot)$ je **okruh**, pokud

- $(M, +)$ je **abelovská grupa**,
- $(M, \cdot)$ je **monoid**,
- platí (levý a pravý) **distributivní zákon**

$$(\forall a, b, c \in M)\,(a(b + c) = ab + ac \wedge (b + c)a = ba + ca)$$

Názvosloví

Buď $R = (M, +, \cdot)$ okruh

- je-li $\cdot$ komutativní, nazýváme R **komutativní okruh**
- $(M, +)$ se nazývá **aditivní grupa** okruhu R,
- $(M, \cdot)$ se nazývá **multiplikativní monoid** okruhu R,
- neutrální prvek M se nazývá **nulový prvek** a značí se 0, inverzní prvek a^{-1} vůči operaci $+, a \in M$, značíme $-a$,
- v okruhu můžeme definovat operaci odečítání $-$ předpisem

$$a - b = a + (-b)$$

- neutrálnímu prvku multiplikativního monoidu budeme zpravidla říkat **jednička** a značit jej 1.

Základní vlastnost okruhů

- Násobení nulovým prvkem dává opět nulový prvek
- Levý i pravý distributivní zákon pro odečítání

Definice 13.2 Obor integrity (Integral domain)

Nenulové prvky $a, b \in M$ z okruhu $(M, +, \cdot)$ nazýváme **dělitelé nuly** právě tehdy když, $a \cdot b = b \cdot a = 0$. **Obor integrity** je komutativní okruh ve kterém neexistují dělitelé nuly.

Definice 13.3 Těleso (Field)

Okruh $T = (M, +, \cdot)$ se nazývá těleso, pokud $(M \setminus \{0\}, \cdot)$ je abelovská grupa. Tuto grupu nazýváme multiplikativní grupou tělesa T.

Poznámka

- Z množiny M multiplikativní grupy tělesa T musíme odebrat prvek 0, protože $a \cdot 0 = 0 \cdot a = 0$ a tedy k nule neexistuje inverzní prvek, tj. nelze dělit nulou.
- všemi ostatními prvky dělit umíme.

  dělení = násobení inverzním prvkem

$$\frac{a}{b} = a \cdot b^{-1}, \quad \forall a, b \in M \setminus \{0\}$$

Příklady těles

- $(\mathbb{Z}, +, \cdot)$ není těleso,
- $(\mathbb{Q}, +, \cdot)$ je nejmenší těleso s běžnými operacemi + a $\cdot$,
- nejmenší těleso je tzv. **triviální těleso**

$$(\{0, 1\}, +_2, \cdot_2)$$

Některé vlastnosti těles

Každé těleso má definované aritmetické operace sčítání, odčítání, násobení, dělení a všechny operace z nich odvozené jako například mocnění, odmocňování, logaritmování.

Triviální těleso má tyto operace definované nad jedním bitem. Lze je rozšířit na libovolný počet bitů.

Věta 13.4

Mějme těleso T, pokud $ab = 0, a, b \in T$ pak $a = 0 \vee b = 0$.

Každé těleso je tedy oborem integrity.

Definice 13.5

Zobrazení h z okruhu (resp. tělesa) R do okruhu (resp. tělesa) S, je **homomorfismem** z R na S, pokud je h homomorfismem příslušných aditivních a multiplikativních grupoidů (resp. grup) a platí $h(1_R) = 1_S$.

Je-li navíc zobrazneí h bijekcí (prosté a na), jedná se o **izomorfismus** z R na S.

Definice 13.6

Tělesa T a K nazýváme **izomorfní**, právě tehdy když existuje izomorfismus z R na S. V tom případě říkáme, že těleso T **je izomorfní s** tělesem K.

Poznámka

Relace "být izomorfní" na množině všech těles je relace ekvivalence. Podmínka $h(1_R) = 1_S$ u homomorfismů okruhů je nutná abychom měli korektně homomorfismus monoidů. U těles ji můžeme vypustit.

4.2 Okruhy polynomů

Definice 13.6

Mějme okruh R a prvky $a_i \in R, i \in \{0, 1, 2, \ldots, n\}$. Formální výraz tvaru

$$P(x) = \sum_{i=1}^{n} a_i x^i$$

nazýváme **polynomem nad okruhem** R.

- Prvky $a_i \in R, i \in \{0, 1, 2, \ldots, n\}$ nazýváme **koeficienty** polynomu $P(x)$.
- x nazýváme **formální proměnnou** polynomu $P(x)$.

- Pokud pro polynom $P(x)$ existuje $k \in \{0, 1, 2, \ldots, n\}, a_k \neq 0$, pak nejvyšší z těchto k nazýváme **stupněm polynomu**.
- Polynom $P(x) = 0$ nazýváme **nulovým polynomem** a jeho stupeň nedefinujeme.

Věta 14.2 Okruh polynomů (polynomial ring)

... tvoří **okruh polynomů nad okruhem** R.
Tento okruh zančíme $R[x]$.

Lemma 14.3 (o dělení polynomů)

Věta 14.4 (Bézoutova věta pro polynomy)

Lemma 14.5 (o násobení polynomů)

Definice 14.6

... Řekneme, že $P(x)$ je **ireducibilní nad okruhem K**, jestliže

Věta 14.7

...
kde μ je Möbiova funkce
a **monický** polynom je takový, který má u koeficient u nejvyšší mocniny jedničku.

4.3 Konečná tělesa

Definice 15.1 Konečné těleso (finite field)

Těleso, které má konečný počet prvků se nazývá **konečné**.

Řádem tělesa se podobně jako u řádu grup nazývá počet prvků tělesa. Konečná tělesa mají i konečný řad.

O tělese $(\mathbb{Z}, +, \cdot)$

Věta 15.3

Řádem konečného tělesa musí být mocnina prvočísla, neboli číslo zapsatelné jako p^n, kde p je prvočíslo a n je kladné celé číslo. Navíc platí, že všechna

tělesa řádu p^n jsou **navzájem izomorfní**.

Definice 15.4

Těleso s řádem p^n nazýváme **Galois field** a značíme ho $GF(p^n)$ prvočíslo p se nazývá **charakteristikou** tělesa $GF(p^n)$.

$GF(p^n)$**: aditivní grupa**

$GF(p^n)$**: multiplikativní grupa**

4.4 Aplikace konečných těles v kryptografii

Bloková šifra AES

Eliptická křivka

Definice 16.1

Pro dva body

Definice 16.2

Eliptickou křivkou rozumíme množinu bodů splňující rovnici

5 Algebra 5.

5.1 Aritmetické operace v konečném tělese $GF(p^n)$

EEA: ukázka v $GF(3^3)$

5.2 Hledání izomorfismů mezi dvěma konečnými tělesy

5.3 Soustavy lineárních rovnic v $\mathbb{Z}_n^+$