

29 Homomorfismy a izomorfismy

29.1 Motivační příklad

Různé grupy – stejná struktura (1 z 6)

\mathbb{Z}_5^\times	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

řád: 4

podgrupy: $\{1\}$, $\{1, 4\}$, $\{1, 2, 3, 4\}$

neutrální prvek: 1

inverze: $1^{-1} = 1$, $2^{-1} = 3$, $3^{-1} = 2$, $4^{-1} = 4$

\mathbb{Z}_4^+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

řád: 4

podgrupy: $\{0\}$, $\{0, 2\}$, $\{0, 1, 2, 3\}$

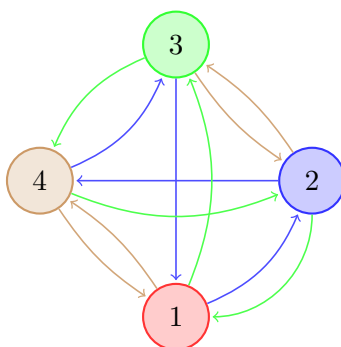
neutrální prvek: 0

inverze: $0^{-1} = 0$, $1^{-1} = 3$, $2^{-1} = 2$, $3^{-1} = 1$

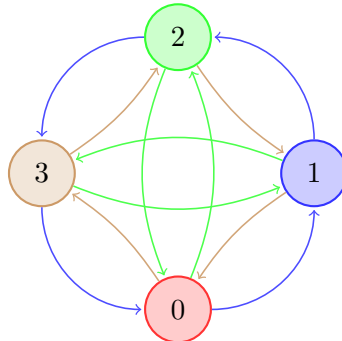
Nejsou \mathbb{Z}_4^+ a \mathbb{Z}_5^\times vlastně stejné grupy lišící se pouze ve „jménech“ svých prvků a označení operace?

Různé grupy – stejná struktura (2 z 6)

\mathbb{Z}_5^\times	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1



\mathbb{Z}_4^+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2



Různé grupy – stejná struktura (3 z 6)

\mathbb{Z}_5^\times	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

\mathbb{Z}_4^+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Zkusme přejmenovat prvky grupy \mathbb{Z}_5^\times tak, abychom dostali \mathbb{Z}_4^+ :

- neutrální prvek má velmi speciální a jedinečné vlastnosti, proto přejmenujme 1 na 0,
- pokud se má zachovat kompletně struktura, musí jediné dvouprvkové podgrupě $\{1, 4\}$ (v \mathbb{Z}_5^\times) odpovídat podgrupa $\{0, 2\}$ (v \mathbb{Z}_4^+), proto $4 \leftrightarrow 2$,
- nyní už stačí přejmenovat 2 a 3: zjistíme, že obě zbývající možnosti fungují, zvolme tedy např. $3 \leftrightarrow 1$ a $2 \leftrightarrow 3$,
- a nyní už stačí přeházet řádky ...a máme Cayleyho tabulku \mathbb{Z}_4^+ .

Různé grupy – stejná struktura (4 z 6)

- Našli jsme způsob, jak přeznačit prvky v jedné tabulce, abychom dostali přesně tabulku druhou (po přeházení řádků a sloupců).
- Toto přejmenování je vlastně **prosté** zobrazení množiny $\{1, 2, 3, 4\}$ na množinu $\{0, 1, 2, 3\}$, označme jej h_1 :

$$h_1(1) = 0, \quad h_1(2) = 3, \quad h_1(3) = 1, \quad h_1(4) = 2.$$

- Jak jsme naznačili, fungovalo by i h_2 (jen bychom museli na závěr jinak zpřeházet řádky a sloupce):

$$h_2(1) = 0, \quad h_2(2) = 1, \quad h_2(3) = 3, \quad h_2(4) = 2.$$

Nefungovaly by tedy všechny bijekce? A jestli ne, tak čím jsou tyto dvě výjimečné?

Různé grupy – stejná struktura (5 z 6)

Přejmenujme prvky grupy \mathbb{Z}_5^\times podle bijekce h_3 :

$$h_3(1) = 0, \quad h_3(2) = 3, \quad h_3(3) = 2, \quad h_3(4) = 1.$$

\mathbb{Z}_5^\times	1	2	3	4
1	1	2	3	4
2	2	4	1	3
3	3	1	4	2
4	4	3	2	1

\mathbb{Z}_4^+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

- Výsledná tabulka ale neodpovídá grupě \mathbb{Z}_4^+ s operací sčítání modulo 4, neboť například $3+3 \pmod{4} \neq 1$.
- Bijekce h_3 tedy nevytvoří stejnou strukturu jakou má grupa \mathbb{Z}_4^+ , takovou vlastnost mají pouze h_1 a h_2 .

Různé grupy – stejná struktura (6 z 6)

Hledaná vlastnost bijekce h , kterou mají pouze bijekce h_1 a h_2 , je tato:

$$\text{pro všechna } n, m \in \{1, 2, 3, 4\} \text{ platí } h(n \times_5 m) = h(n) +_4 h(m),$$

kde \times_5 značí operaci v grupě \mathbb{Z}_5^\times a $+_4$ v grupě \mathbb{Z}_4^+ .

Slovy: Jestliže na libovolné prvky v grupě \mathbb{Z}_5^\times aplikujeme operaci \times_5 a pak je zobrazíme do \mathbb{Z}_4^+ pomocí h , dostaneme vždy stejný výsledek, jako kdybychom je nejdříve pomocí h zobrazili do \mathbb{Z}_4^+ a **potom** aplikovali operaci $+_4$.

$$\begin{array}{ccc}
 n, m \in \mathbb{Z}_5^\times & \xrightarrow{\times_5} & n \times_5 m \in \mathbb{Z}_5^\times \\
 \downarrow h & & \downarrow h \\
 h(n), h(m) \in \mathbb{Z}_4^+ & \xrightarrow{+_4} & h(n) +_4 h(m) = h(n \times_5 m)
 \end{array}$$

Bijekce navíc musí tzv. **zachovávat operaci**. Vzpomeňte na lineární zobrazení...

29.2 Definice a vlastnosti

Homomorfismus a izomorfismus

Definice 29.1 Buďte $G = (M, \circ_G)$ a $H = (N, \circ_H)$ dva grupoidy. Zobrazení $h : M \rightarrow N$ nazveme **homomorfismem G do H** jestliže

$$\text{pro všechna } x, y \in M \text{ platí } h(x \circ_G y) = h(x) \circ_H h(y).$$

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

- Homomorfismus tedy zachovává strukturu danou binární operací: je jedno jestli nejdříve aplikují operaci a pak homomorfismus, nebo naopak.
- Jediné, co potřebujeme pro definování této vlastnosti, je uzavřenost množiny vůči binární operaci, proto jsme homomorfismus definovali pro nejobecnější grupoidy.
- Definice se přímo přenáší na grupy, a používá se termín **(homo|mono|epi|izo)morfismus grup**.

Řecké jazykové okénko

- morfismus: z řecké slova *morfé*, znamenajícího forma, tvar
- homo: *homós*, stejný,
- izo: *isos*, sobě rovný,
- epi: *epí*, na,
- mono: *monós*, samotný, jediný.

Izomorfní grupy

Definice 29.2 Grupy G a H nazýváme **izomorfní**, právě když existuje izomorfismus $G \rightarrow H$. O grupě G také říkáme, že je **izomorfní s** grupou H .

- Vlastnost dvou grup „být izomorfní“ je relace ekvivalence na třídě všech grup.
- Příkladem izomorfních grup jsou \mathbb{Z}_5^\times a \mathbb{Z}_4^+ : našli jsme dokonce dva různé izomorfismy h_1 a h_2 .
- Je jasné, že izomorfní grupy musí mít stejný řád!

Základní vlastnosti homomorfismu (1 ze 2)

Věta 29.3 Buď h homomorfismus grupy $G = (M, \circ_G)$ do grupoidu $H = (N, \circ_H)$. Potom $h(G) := (h(M), \circ_H)$ je grupa. !

Důkaz. Ukážeme postupně že v $h(G)$ platí asoc. zákon, existuje neutrální prvek a každý prvek má inverzi.

- Každý prvek $h(G)$ lze napsat jako $h(x)$ pro nějaké vhodné x .
- Pro všechna $x, y, z \in M$ platí

$$\begin{aligned} (h(x) \circ_H h(y)) \circ_H h(z) &= h(x \circ_G y) \circ_H h(z) = h((x \circ_G y) \circ_G z) = \\ &= h(x \circ_G (y \circ_G z)) = h(x) \circ_H (h(y) \circ_H h(z)) \end{aligned}$$

- Označme e_G neutr. prvek v G , potom $h(e_G)$ je neutrální prvek v $h(G)$, neboť pro všechna x platí $h(e_G) \circ_H h(x) = h(e_G \circ_G x) = h(x)$.
- Podobně se ukáže, že inverzí k $h(x)$ je $h(x^{-1})$. ■

Základní vlastnosti homomorfismu (2 ze 2)

Je-li H grupa, tak předchozí věta a její důkaz mají následující důsledky:

- Neutrální prvek jedné grupy se homomorfismem zobrazí vždy na neutrální prvek té druhé grupy.
- Také inverze se zachovávají v následujícím smyslu: $h(x^{-1}) = h(x)^{-1}$.
- Je-li h homomorfismus grupy G do H , pak $h(G)$ je podgrupa v H .
- Např. $h(n) = 2n$ je homomorfismus grupy \mathbb{Z}_4^+ do \mathbb{Z}_8^+ a $h(\mathbb{Z}_4^+)$ je podgrupa $\{0, 2, 4, 6\}$.

...až na izomorfismus (1 ze 4)

Izomorfní grupy jsou vlastně totožné, liší se pouze pojmenováním prvků, jak jsme viděli v případě grup \mathbb{Z}_4^+ a \mathbb{Z}_5^\times . Řekneme-li, že existuje pouze jedna grupa s jistou vlastností **až na izomorfismus**, znamená to, že všechny grupy s touto jistou vlastností jsou navzájem izomorfní. Ukážeme si tři známá tvrzení tohoto typu.

Věta 29.4 Libovolné dvě cyklické grupy mající stejný řád jsou izomorfní. !

Důkaz: náznak – doladit za domácí úkol. Buď $G = \langle a \rangle$ cyklická grupa s generátorem a . Ukážeme, že libovolná nekonečná cyklická grupa je izomorfní s grupou $(\mathbb{Z}, +)$ a že libovolná cyklická grupa řádu n je izomorfní s \mathbb{Z}_n^+ . Zbytek už plyne z tranzitivity relace „být izomorfní“. Hledaný izomorfismus je bijekce (ze \mathbb{Z} či \mathbb{Z}_n^+ na G) definovaná pro všechna k jako $h(k) = a^k$. ■

$(\mathbb{Z}, +)$ a \mathbb{Z}_n^+ jsou tedy jedinými cyklickými grupami **až na izomorfismus**.

...až na izomorfismus (2 ze 4)

■ **Příklad 29.5 — Kleinova grupa.** Kleinova grupa je grupa $(\mathbb{Z}_2 \times \mathbb{Z}_2, \circ)$, kde 

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


a \circ je sčítání modulo 2 po složkách: např. $(1, 0) \circ (1, 1) = (0, 1)$. ■

Kleinova grupa není cyklická a tedy nemůže být izomorfní se \mathbb{Z}_4^+ ! Kleinova grupa je izomorfní \mathbb{Z}_8^\times . Lze dokonce ukázat toto (zkuste si to, je to jednoduché):

Věta 29.6 Existují pouze dvě neizomorfní grupy řádu 4. !

\mathbb{Z}_4^+ a Kleinova grupa jsou tedy až na izomorfismus jediné grupy řádu 4.

...až na izomorfismus (3 ze 4)

■ **Příklad 29.7 — Symetrická grupa.** Symetrickou grupou množiny $\{1, 2, 3, \dots, n\}$ nazveme množinu všech permutací této množiny s operací skládání zobrazení a značíme ji S_n . 

- Permutace je bijekce z množiny do stejné množiny, tedy v našem případě z $\{1, 2, 3, \dots, n\}$ do $\{1, 2, 3, \dots, n\}$.

- Každou permutaci $\pi \in S_n$ můžeme zadat výčtem hodnot:

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \pi(1) & \pi(2) & \pi(3) & \dots & \pi(n) \end{pmatrix},$$

první řádek navíc můžeme vynechat, takže např. $(1\ 2\ 4\ 3\ 5) \in S_5$ je permutace prohazující 3. a 4. prvek.

- Složením permutací $(1\ 2\ 4\ 3\ 5) \circ (2\ 1\ 3\ 5\ 4)$ je $(2\ 1\ 4\ 5\ 3)$.
- Skládání zobrazení je asociativní, permutace $(1\ 2\ 3\ \dots\ n)$ je neutrální prvek a inverzním prvkem je inverzní zobrazení – jedná se tedy skutečně o grupu. Řád S_n je $n!$.

...až na izomorfismus (4 ze 4)

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

- Například permutace $(1\ 2\ 4\ 3\ 5) \in S_5$ prohazující 3. a 4. prvek generuje podgrupu grupy S_5 obsahující dva prvky

$$(1\ 2\ 4\ 3\ 5) \quad \text{a} \quad (1\ 2\ 3\ 4\ 5).$$

- Struktura podgrup S_n je velice (v jistém slova smyslu maximálně) bohatá, o čemž svědčí následující věta.

Věta 29.8 — Cayleyova. Libovolná konečná grupa je izomorfní s nějakou grupou permutací. !

Důkaz: náznak pro zájemce. Buď a prvek grupy G řádu n s binární operací \circ . Definujeme $\pi_a(x) = a \circ x$. Jelikož lze v grupě jednoznačně dělit, je π_a bijekce a tedy permutace! Hledaný monomorfismus (tj. izomorfismus s podgrupou S_n) je zobrazení definované pro každý prvek a takto: $h(a) = \pi_a \dots$ ■

30 Aplikace teorie grup v kryptografii

30.1 Problém diskretního logaritmu

Diskretní logaritmus obecně

Problém diskretního logaritmu můžeme definovat v libovolné cyklické grupě:

Definice 30.1 — problém diskretního logaritmu v grupě $G = (M, \cdot)$. Buď $G = (M, \cdot)$ cyklická grupa řádu n , α nějaký její generátor a β její prvek. Řešit **problém diskretního logaritmu** znamená najít celé číslo $1 \leq k \leq n$ takové, že

$$\alpha^k = \beta.$$

Použijeme-li aditivní značení:

Definice 30.2 — problém diskretního logaritmu v grupě $G = (M, +)$. Buď $G = (M, +)$ cyklická grupa řádu n , α nějaký její generátor a β její prvek. Řešit **problém diskretního logaritmu** znamená najít celé číslo $1 \leq k \leq n$ takové, že

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

Poznámka: Zahodíme-li požadavek na cykličnost grupy G , pak má úloha diskretního logaritmu řešení pouze pokud β patří do $\langle \alpha \rangle$, cyklické podgrupy generované α .

Ne ve všech grupách je to těžké

Uvažujme grupu \mathbb{Z}_p^+ . To je cyklická grupa prvočíselného řádu p , a každé kladné $\alpha \leq p-1$ je její generátor. Problém diskretního logaritmu v této grupě má formu rovnice

$$k\alpha \equiv \beta \pmod{p}.$$

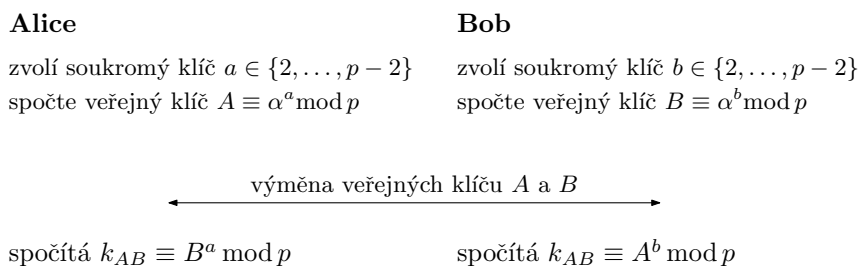
Tu umíme snadno vyřešit. Najdeme inverzi α^{-1} k α v grupě \mathbb{Z}_p^\times (pomocí polynomiálního EEA (v délce vstupu), viz další přednášky a dřívější studium) a řešením je

$$k = \beta\alpha^{-1} \pmod{p}.$$

■ **Příklad 30.3** Uvažujme $p = 11, \alpha = 3, \beta = 5$. Hledáme k tak, aby

$$k \cdot 3 \equiv 5 \pmod{11}.$$

Snadno ověříme, že v \mathbb{Z}_{11}^\times je $3^{-1} = 4$ a tedy $k = (5 \cdot 4) \pmod{11} = 9$. ■



Výpočet diskretního logaritmu obecně?

Obecně není známý žádný rozumně rychlý algoritmus řešící problém diskretního logaritmu.

V případě grupy \mathbb{Z}_p^\times je počet kroků známých algoritmů úměrný \sqrt{p} , což pro p délky 1024 bitů dává cca 2^{512} operací. (Obecně se je počet kroků úměrný \sqrt{n} , kde n je řád základu logaritmu.)

Inverzní operaci k logaritmu, tedy mocnění, umíme v \mathbb{Z}_p^\times rychle.

Získáváme tedy **jednosměrnou** (*one-way*) funkci, kterou lze použít pro **asymetrickou šifru**: najít $\beta \equiv \alpha^x \pmod p$ je lehké, známe-li x , α a p , najít x , známe-li β , α a p je **obecně** velmi obtížné

Poznámka: Pro konstrukci RSA byla použita jednosměrná funkce „násobení prvočísel“: násobit prvočísla je lehké a rychlé, hledat prvočíselný rozklad výsledku je **obecně** složité.

30.2 Diffie-Hellman Key Exchange

Diffie-Hellman Key Exchange

Inicializace: Alice si najde velké prvočíslo p a nějaký generátor α grupy \mathbb{Z}_p^\times . **Zveřejní p a α .** (najít velké prvočíslo a generátor nejsou lehké úkoly!)

Princip

Diffie-Hellman Key Exchange stojí na následujících faktech:

- Mocnění v \mathbb{Z}_p^\times je komutativní a tedy vypočtené k_{AB} je pro Alici i Boba stejné:

$$\begin{aligned} k_{AB} &\equiv (\alpha^b)^a \equiv \alpha^{ab} \pmod p \\ k_{AB} &\equiv (\alpha^a)^b \equiv \alpha^{ab} \pmod p, \end{aligned}$$

- mocnění není výpočetně náročné (square & multiply),
- inverzní operace k mocnění, tedy diskretní logaritmus, je výpočetně velmi náročná.

?

Kontrolní otázka 30.1. Víme, že grupy \mathbb{Z}_p^\times a \mathbb{Z}_{p-1}^+ jsou izomorfní a tedy vlastně totožné. Není to problém pro Diffie-Hellmana, nedělá to z řešení diskretního logaritmu v \mathbb{Z}_p^\times lehký problém?

ChangeLog

Verze	Datum	Autor	Log
1.12	6.10.2020	SS	Oprava pauzování.
1.11	1.6.2020	SS	Oprava formulace u definice hom/izo. grup.
1.1	23.9.2019	SS	Opravy v sekci o DLP.
1.0	23.9.2019	SS	Výchozí verze.