10 Izomorfismus – dobrý sluha, ale zlý pán

Řešení
verze ze dne 21. dubna 2025.

Cíle cvičení: Cílem dnešního cvičení je to, abychom po jeho skončení chápali, jak dobře a útulno je na světě s izomorfismy. Ochočené izomorfismy nám pomohou s odhalováním všech generátorů cyklických grup. Naopak, invarianty izomorfismů, tedy vlastnosti grupy, které musí izomorfismus zachovat, nám odhalí i situaci, kde s láskyplnou pomocí izomorfismu počítat nemůžeme. Nakonec s úspěchem využijeme dvojici ochočených izomorfismů, které nám poskytuje čínská věta o zbytcích.

Úlohy, které bychom určitě měli umět řešit:

Úloha 10.1. Dokažte, že jsou izomorfní grupy:

(a) $(\mathbb{R}, +, -, 0)$ a $(\mathbb{R}^+, \cdot, ^{-1}, 1)$, kde $\mathbb{R}^+$ množina kladných reálných čísel,

(b) aditivní grupa $\mathbb{Z}_6$ a multiplikativní grupa $\mathbb{Z}_7^*$ (najděte konkrétní izomorfismus),

(c) součin aditivních grup $\mathbb{Z}_2 \times \mathbb{Z}_2$ a multiplikativní grupa $\mathbb{Z}_8^*$.

Řešení. (a) Z připomeňme si, že exponenciála $r \mapsto e^r$ představuje rostoucí spojité zobrazení $\mathbb{R} \to \mathbb{R}^+$, tedy jde o bijekci, která pro každé $r, s \in \mathbb{R}$ splňuje podmínku $e^{r+s} = e^r \cdot e^s$, což znamená, že jde o izomorfismus grupy $(\mathbb{R}, +, -, 0)$ na grupu $(\mathbb{R}^+, \cdot, ^{-1}, 1)$.

(b) Tentokrát nejprve najdeme generátory obou cyklických grup $\mathbb{Z}_6$ a $\mathbb{Z}_7^*$, v prvním příkladě si vezmeme například generátor 1. V druhém případě stačí díky Lagrangeově větě otestovat, zda druhá a třetí mocnina zvoleného prvku není rovna jedné, najdeme například generátor 3, neboť $3^2 = 2 \neq 1$, $3^3 = 6 \neq 1$). Nyní definujeme zobrazení podobně jako v (a) předpisem $f(j) = 3^j$. Vidíme, že

$$f(j+k) = 3^{(j+k) \bmod 6} = 3^{j+k} = 3^j \cdot 3^k = f(j) \cdot f(k) \in \mathbb{Z}_7^*,$$

a protože jde o prostý homomorfismus mezi dvěma grupami řádu 6, je f izomorfismus.

(c) Vidíme, že $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, neboť prvky okruhu $\mathbb{Z}_8$ jsou invertibilní, právě když jsou nesoudělné s číslem 8. Dále snadno spočítáme, že

$$3^2 = 5^2 = 7^2 = 1, \quad 3 \cdot 5 = 7, \quad 3 \cdot 7 = 5, \quad 5 \cdot 7 = 3.$$

Definujeme-li bijekci $f \colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_8^*$ například podmínkami

$$f((0,0)) = 1, \quad f((0,1)) = 3, \quad f((1,0)) = 5, \quad f((1,1)) = 7,$$

snadnou diskusí ověříme, že $f(\alpha + \beta) = f(\alpha) + f(\beta)$ pro všechny hodnoty $\alpha, \beta \in \mathbb{Z}_2 \times \mathbb{Z}_2$, tedy f je izomorfismus a grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ a $\mathbb{Z}_8^*$ jsou tudíž izomorfní.

Úloha 10.2. Ukažte, že nejsou izomorfní dvojice grup (a) $\mathbb{Z}_6$ a $\mathbf{S}_3$, (b) $\mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}$, (c) $\mathbb{Q}$ a $\mathbb{Q} \times \mathbb{Q}$.

Řešení. Tentokrát budeme hledat nějaký invariant, tedy vlastnost, kterou by izomorfismus musel zachovat, ovšem splňuje ji jen jedna z grup a druhá nikoli.

(a) Grupy nemohou být izomorfní, protože grupa $\mathbb{Z}_6$ je komutativní, zatímco grupa permutací $\mathbf{S}_3$ komutativní není.

(b) Tentokrát si všimneme, že je grupa $\mathbb{Z}$ na rozdíl od $\mathbb{Z} \times \mathbb{Z}$ cyklická.

(c) Můžeme uvážit vlastnost, že pro každé dva nenulové prvky $\frac{a}{b}, \frac{c}{d}$ grupy $\mathbb{Q}$ existují nenulová celá $u, v \in \mathbb{Z}$, pro něž $u \cdot \frac{a}{b} = v \cdot \frac{c}{d}$ (stačí položit $u = cb$ a $v = ad$), což v grupě $\mathbb{Q} \times \mathbb{Q}$ například pro prvky $(1,0)$ a $(0,1)$ určitě neplatí.

Výše uvedené se dá ekvivalentně říct i tak, že každé dvě netriviální podgrupy $\mathbb{Q}$ mají netriviální průnik, což v $\mathbb{Q} \times \mathbb{Q}$ není pravda.

Komu se nelíbí důkaz pomocí invariantu, může alternativně nahlédnout, že každý homomorfismus $\varphi\colon \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q}$ je určen svou hodnotou $\varphi(1) = (r, s)$ a že toto zobrazení nemůže být na.

Úloha 10.3. Rozhodněte, zda jsou cyklické grupy (a) $\mathbf{S}_3$ (b) $\mathbf{A}_3$ (c) $\mathbb{Z}_{12}^*$ (d) $\mathbb{Z}_{14}^*$.

Řešení. (a) Grupa $\mathbf{S}_3$ není ani komutativní (například $(12)(23) \neq (23)(12)$), proto nemůže být cyklická, neboť všechny cyklické grupy jsou abelovské.

(b) Grupa $\mathbf{A}_3$ je řádu 3, proto je jako každá grupa prvočíselného řádu díky Lagrangeově větě cyklická, každý nejednotkový prvek totiž generuje cyklickou podgrupu řádu většího než jedna, který musí být už roven řádu celé grupy.

(c) Využijeme algebraickou verzi čínské věty o zbytcích (věta 15.6), která nám říká, že $\mathbb{Z}_{12}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_4^*$. Snadno zjistíme, že grupy Z_3^*, Z_4^* jsou dvouprvkové, tedy cyklické, máme

$$\mathbb{Z}_{12}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_4^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Protože jsou všechny prvky grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$ řádu nejvýše 2, grupa není cyklická, a proto cyklická není ani jí izomorfní grupa $\mathbb{Z}_{12}^*$.

(d) Opět využijeme větu 15.6 spolu s větou 16.7, která říká, že konečná multiplikativní grupa tělesa je cyklická, v našem případě tedy, že $\mathbb{Z}_7^* \cong \mathbb{Z}_6$ a dostáváme

$$\mathbb{Z}_{14}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_7^* \cong \mathbb{Z}_1 \times \mathbb{Z}_6 \cong \mathbb{Z}_6$$

tedy grupa $\mathbb{Z}_{14}^*$ je cyklická grupa řádu 6.

Úloha 10.4. Najděte všechny generátory zadané grupy (a) $\mathbb{Z}_{12}$, (b) $\mathbb{Z}_7^*$.

Řešení. (a) Hledáme prvky nosné množiny $\mathbb{Z}_{12}$, které jsou nesoudělné s dvanáctkou. Víme, že je jich právě $\varphi(12) = 4$, a snadno zjistíme, že se jedná o prvky 1, 5, 7, 11.

(b) Grupa $\mathbb{Z}_7^*$ je multiplikativní grupa konečného tělesa, tedy cyklická grupa řádu 6. Opět tedy předem známe počet generátorů, jichž je právě $\varphi(6) = 2$, a protože podle Lagrangeovy věty jsou jediné možné řády prvků $\mathbb{Z}_7^*$ jen 1, 2, 3, 6 a

$$3^2 = 2 \neq 1, 3^3 = 6 \neq 1 \quad \text{a} \quad 5^2 = 4 \neq 1, 5^3 = 6 \neq 1$$

(u druhého prvku stačilo uvážit $5 = 3^{-1}$) a vidíme, že máme dva generátory 3, 5 grupy $\mathbb{Z}_7^*$.

Úloha 10.5. Jaké jsou maximální možné řády prvků v grupách (a) $\mathbb{Z}_{18}$, (b) $\mathbb{Z}_{29}^*$, (c) $\mathbb{Z}_{21}^*$, (d) $\mathbb{Z}_{30}^*$? Zkuste nějaké takové prvky najít.

Řešení. (a) $\mathbb{Z}_{18}$ je cyklická grupa řádu 18, tedy obsahuje $\varphi(18) = 6$ generátorů, tedy prvků maximálního možného řádu 18. Víme, že je představují právě čísla nesoudělná s 18, tedy prvky 1, 5, 7, 11, 13, 17.

(b) Protože je $\mathbb{Z}_{29}^*$ multiplikativní grupa konečného tělesa, je opět cyklická, tedy prvkem maximálního možného řádu 28 je jakýkoli generátor, například prvek 2.

(c) Protože díky větě 15.6 máme $\mathbb{Z}_{21}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_7^* \cong \mathbb{Z}_2 \times \mathbb{Z}_6$, vidíme, že $6(a, b) = (6a, 6b) = 0$ pro všechna $(a, b) \in \mathbb{Z}_2 \times \mathbb{Z}_6$, tedy mají všechny prvky grup $\mathbb{Z}_2 \times \mathbb{Z}_6$ i $\mathbb{Z}_{21}^*$ jako řád dělitel 6, přímo řádu 6 jsou potom, jak můžeme zkusmo zjistit, prvky 5, 17, 2, 19, 10, 11.

(d) Stejnou úvahou jako v (c) zjistíme, že všechny prvky grupy $\mathbb{Z}_{30}^* \cong \mathbb{Z}_2^* \times \mathbb{Z}_3^* \times \mathbb{Z}_5^* \times \cong \mathbb{Z}_2 \times \mathbb{Z}_4$ mají za řád dělitel 4, a z nich právě prvky $7, 13, 23, 17 \in \mathbb{Z}_{30}^*$ jsou řádu 4.

A na závěr si dáme ještě jeden divoký slalom mezi izomorfismy:

Úloha 10.6. Pro devítiprvkové těleso $T = \mathbb{Z}_3[\alpha]/(\alpha^2+1)$ najděte generátor grupy T^*. Kolik má tato grupa generátorů celkem?

Řešení. Víme, že těleso T má 9 prvků, tedy podle věty 16.7 je jeho multiplikativní grupa T^* cyklická řádu 8 a ta má podle tvrzení 16.4 právě $\varphi(8) = 4$ generátorů. Zkusmo zjistíme, že $(\alpha+1)^4 = (2\alpha)^2 = 2 \neq 1$, tedy $\alpha+1$ je prvek řádu 8, tedy jeden z generátorů.

Úloha 10.7. Rozhodněte, zda jsou izomorfní grupy:

(a) $\mathbb{Z}_8^*$ a $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\} \leq \mathbf{S}_4$,

(b) $\mathbf{GL}_2(\mathbb{Z}_2)$ a $\mathbf{S}_3$,

(c) $\mathbb{Z}_{24}^*$ a $\mathbb{Z}_{15}^*$,

⋆ (d) $\mathbb{R}$ a $\mathbb{R}^2$.

Řešení. V úloze 10.1(c) jsme si všimli, že $\mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Podobně ukážeme o bijekci $g\colon \mathbb{Z}_2 \times \mathbb{Z}_2 \to K$ definované

$$g((0,0)) = \mathrm{id}, \quad g((0,1)) = (12)(34), \quad g((1,0)) = (13)(24), \quad g((1,1)) = (14)(23),$$

že jde o homomorfismus. Protože jsou obě grupy komutativní a pro každé α platí, že

$$g((0,0)+\alpha) = \mathrm{id} \circ g(\alpha), \qquad g(\alpha+\alpha) = g((0,0)) = \mathrm{id} = g(\alpha) \circ g(\alpha),$$

stačí uvážit, že

$$g((0,1)+(1,0)) = g((1,1)) = (14)(23) = (12)(34) \circ (13)(24) = g((0,1)) + g((1,0)),$$

$$g((0,1)+(1,1)) = g((1,0)) = (13)(24) = (12)(34) \circ (14)(23) = g((0,1)) + g((1,1)),$$

$$g((1,0)+(1,1)) = g((0,1)) = (12)(34) = (13)(24) \circ (14)(23) = g((1,0)) + g((1,1)),$$

abychom zjistili, že je g izomorfismus. Relace „být izomorfní“ je tranzitivní, proto $\mathbb{Z}_8^* \cong K$.

(b) Protože $\mathbf{GL}_2(\mathbb{Z}_2)$ permutuje množinu nenulových vektorů vektorového prostoru $\mathbb{Z}_2^2$, které jsou právě 3, jsou grupy izomorfní – pokud bychom označili bijekci $b\colon \{1,2,3\} \to \mathbb{Z}_2^2 \setminus \{(0,0)\}$, pak je zobrazení $\psi\colon \mathbf{GL}_2(\mathbb{Z}_2) \to \mathbf{S}_3$ dané vztahem $\psi(f) = b^{-1}fb$ dosvědčujícím izomorfismem.

(c) Díky tvrzení 15.6 a 10.1(c) máme

$$\mathbb{Z}_{24}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_8^* \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2,$$

což je grupa, jejíž všechny nejednotkové prvky jsou řádu 2. Opět pomocí tvrzení 15.6 a věty 16.7 dostáváme izomorfismy

$$\mathbb{Z}_{15}^* \cong \mathbb{Z}_3^* \times \mathbb{Z}_5^* \cong \mathbb{Z}_2 \times \mathbb{Z}_4,$$

což je grupa, která obsahuje prvek řádu 4, a proto grupy $\mathbb{Z}_{24}^*$ a $\mathbb{Z}_{15}^*$ nejsou izomorfní.

(d) Podíváme-li se na $\mathbb{R}$ a $\mathbb{R}^2$ jako na vektorové prostory nad tělesem $\mathbb{Q}$, pak jejich báze mají stejnou mohutnost (kontinua), tudíž jde o izomorfní vektorové prostory. Onen izomorfismus prostorů je nutně také izomorfismem komutativních grup.

Úloha 10.8. Napište všechny podgrupy grupy (a) $\mathbb{Z}$, (b) $\mathbb{Z}_{18}$, (c) $\mathbb{Z}_{23}^*$, (d) $\mathbb{Z}_{17}^*$. Jak jsou podgrupy uspořádány inkluzí?

Řešení. (a) Podgrupy grupy $\mathbb{Z}$ jsou právě ideály okruhu celých čísel, o němž jsme dokázali, že jde o obor hlavních ideálů, tedy to jsou množiny násobků $\langle k\rangle = k\mathbb{Z}$ pro $k \in \mathbb{N}\cup\{0\}$. Uspořádány jsou pomocí inverzní relace dělitelnosti, tj. $\langle a\rangle \subseteq \langle b\rangle$ právě když $b \mid a$, přičemž $a \mid 0$ pro všechna a.

(b) I tentokrát stačí uvážit cyklické podgrupy $k\mathbb{Z}_{18} = \langle k\rangle$ pro k, která dělí 18 (a nulu), a uspořádání je analogické tomu pro $\mathbb{Z}$.

(c) Protože je 23 prvočíslo, je okruh $\mathbb{Z}_{23}$ tělesem a jeho multiplikativní grupa $\mathbb{Z}_{23}^*$ je cyklická řádu 22, a proto izomorfní aditivní cyklické grupě $\mathbb{Z}_{22}$. To znamená, že má grupa $\mathbb{Z}_{23}^*$ kromě triviálních podgrup právě jednu cyklickou podgrupu řádu 2 a jednu cyklickou podgrupu řádu 11. Okamžitě vidíme, že $\langle 22\rangle = \langle -1\rangle$ je podgrupa řádu 2, a protože například 2 je v $\mathbb{Z}_{23}^*$ prvek řádu 11, vidíme, že

$$\{1\} \subsetneq \langle 2\rangle, \langle 22\rangle \subsetneq \mathbb{Z}_{23}^*$$

jsou všechny podgrupy grupy $\mathbb{Z}_{23}^*$.

(d) Stejně jako v (c) nahlédneme, že je grupa $\mathbb{Z}_{17}^*$ cyklická řádu 16. Snadno spočítáme, že $3^8 = 9^4 = 13^2 = (-4)^2 = -1 = 16$ tedy 3 je generátor grupy $\mathbb{Z}_{17}^*$, tudíž

$$\{1\} \subsetneq \langle 16\rangle \subsetneq \langle 13\rangle \subsetneq \langle 9\rangle \subsetneq \langle 3\rangle = \mathbb{Z}_{17}^*$$

jsou všechny podgrupy grupy $\mathbb{Z}_{17}^*$

Úloha 10.9. Rozložte grupy (a) $\mathbb{Z}_{18}$, (b) $\mathbb{Z}_{29}^*$, (c) $\mathbb{Z}_{21}^*$, (d) $\mathbb{Z}_{30}^*$ z úlohy 10.5 na direktní součin co nejvíce netriviálních cyklických grup

Řešení. Využijeme algebraickou verzi čínské věty o zbytcích (věta 15.6) pro multiplikativní grupy okruhu $\mathbb{Z}_n$ a větu 16.7, která říká, že multiplikativní grupa tělesa $\mathbb{Z}_p$ pro prvočíslo p je cyklická, tedy izomorfní aditivní grupě $\mathbb{Z}_{p-1}$.

(a) např. $\langle 2\rangle \times \langle 9\rangle \simeq \mathbb{Z}_9 \times \mathbb{Z}_2$

(b) např. $\langle 12\rangle \times \langle 16\rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_7$

(c) např. $\langle 8\rangle \times \langle 13\rangle \times \langle 16\rangle \simeq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3$

(d) např. $\langle 21\rangle \times \langle 25\rangle \simeq \mathbb{Z}_4 \times \mathbb{Z}_2$

⋆ **Úloha 10.10.** Ukažte, že $\mathbf{D}_{12} \simeq \mathbf{S}_3 \times \mathbb{Z}_2$.

⋆ **Úloha 10.11.** Ukažte obecněji, že pro lichá n platí $\mathbf{D}_{4n} \simeq \mathbf{D}_{2n} \times \mathbb{Z}_2$, ale pro sudá ne.

Řešení. Nejprve nahlédneme, že je každá symetrie šestiúhelníka jednoznačně určena permutací jeho tří úhlopříček a znaménkem permutace jeho vrcholů, tedy zobrazením

$$\varphi(s) = (\text{permutace os}, \operatorname{sgn}(\text{permutace vrcholů})).$$

Rozmyslíme si po složkách, že jde o homomorfismus. Pokud je symetrie s výsledkem složení dvou symetrií s_1, s_2, tj. $s = s_2 \circ s_1$, z nichž každá permutuje úhlopříčky odpovídající permutací π_i $(i = 1, 2)$, pak jejich složení permutuje úhlopříčky permutací $\pi_2 \circ \pi_1$. Podobně i pro permutace vrcholů a jelikož sgn je grupový homomorfismus, získáváme slučitelnost zobrazení φ i v druhé složce. Celkem máme $\varphi(s_2 \circ s_1) = \varphi(s_2)\varphi(s_1)$. Navíc je φ na a tedy i prosté, jelikož jde o konečné množiny stejné velikosti. Tedy jádrem φ je pouze identita (toto si lze rozmyslet i naopak, neboť pro zadanou permutaci os jsou dvě různé symetrie: v případě trojcyklů buď rotací o $k\pi/3$, nebo o $(k+3)\pi/3$, v případě dvojcyklů reflexe kolem os úhlů mezi permutovanými úhlopříčkami.

Úloha 10.12. Následující zčásti vyplněné tabulky zadávají binární grupovou operaci $\bullet$, tj. v buňce příslušící řádku x a sloupci y se nachází $x \bullet y$. Doplňte zbytek tabulky.

(a)

$\bullet$	a	b
a		b
b		

(b)

$\bullet$	a	b	c	d
a				b
b	d	c		
c				
d				

Řešení. (a) Z informace, že $a \bullet b = b$, plyne, že a musí být neutrální prvek operace, tedy nejprve dostáváme hodnoty prvního řádku a sloupce a protože prvek b musí mít v grupě inverzní prvek, doplníme tabulku jediným možným způsobem:

$\bullet$	a	b
a		b
b		

$\rightarrow$

$\bullet$	a	b
a	a	b
b	b	

$\rightarrow$

$\bullet$	a	b
a	a	b
b	b	a

(b) I v druhém případě nejprve odhalíme neutrální prvek – protože $a \bullet d = b$ a $b \bullet a = d$, nemůže jím být žádný z prvků a, b, d, a zbývá tak jediný kandidát c. Dále snadno uvážíme, že $b \bullet d$ musí mít poslední nepoužitou hodnotu na řádku, tedy hodnotu a. Rovněž víme, že $b \bullet d$ musí mít poslední nepoužitou hodnotu v sloupci, tedy $b \bullet d = a$ a $d \bullet d = c$. Protože $b^{-1} = b \neq a$, máme $a^{-1} \neq b$, tedy $a \bullet b \neq c$, kde víme, že c je neutrální prvek, tudíž zbývá jen $a \bullet b = d$. Nakonec už jen doplníme hodnoty tak, abychom v každém řádku i sloupci s výsledky operace měli každou hodnotu právě jednou:

$\bullet$	a	b	c	d
a				b
b	d	c		
c				
d				

$\rightarrow$

$\bullet$	a	b	c	d
a			a	b
b	d	c	b	
c	a	b	c	d
d			d	

$\rightarrow$

$\bullet$	a	b	c	d
a		d	a	b
b	d	c	b	a
c	a	b	c	d
d			d	c

$\rightarrow$

$\bullet$	a	b	c	d
a	c	d	a	b
b	d	c	b	a
c	a	b	c	d
d	b	a	d	c

(Jedná se o grupu izomorfní grupě $\mathbb{Z}_2 \times \mathbb{Z}_2$.)

Úloha 10.13. Rozhodněte, zda existuje unární operace $'$ a prvek e takové, aby následující čtveřice byly grupami:

(a) $(\mathbb{Q}^+, \cdot, ', e)$,

(b) $(\mathbb{Z}, -, ', e)$,

(c) $(\mathbb{Q} \setminus \{0\}, *, ', e)$, kde $a * b = |a \cdot b|$.

Řešení. (a) Ano, neutrální prvek vzhledem k násobení je $e = 1$ a operace inverzního prvku je zobrazení $a' = \frac{1}{a}$.

(b) Protože operace minus není asociativní (například $(0 - 1) - 1 \neq 0 - (1 - 1)$), nemůže jít o grupovou binární operaci, proto vhodná operace $'$ a prvek e neexistují.

(c) Ne, protože pokud by existoval neutrální prvek a, dostali bychom pro libovolné záporné a, že $0 > a = a * e = |a \cdot e| \geq 0$. tedy spor.