Algebra — cvičení 9, řešení

1. Určete počet všech permutací v $\mathbf{S}_5$, které jsou konjugované se $\sigma = \left(\begin{smallmatrix}1&2&3&4&5\\2&3&1&5&4\end{smallmatrix}\right)$. Tvoří množina těchto permutací podgrupu v $\mathbf{S}_5$?

Nejprve si zadanou permutaci rozložíme na nezávislé cykly. Dostaneme $\sigma = (1\ 2\ 3)(4\ 5)$. Z přednášky či skript bychom měli vědět, že dvě permutace jsou v $\mathbf{S}_n$ konjugované právě tehdy, když mají stejný typ, tj. stejnou neuspořádanou posloupnost udávající kolik cyklů jaké délky se nalézá v rozkladu zadané permutace na nezávislé cykly. Naše permutace σ má typ $[3,2]$ nebo také $[2,3]$.

Máme tedy zjistit, kolik permutací typu $[3,2]$ se nalézá v $\mathbf{S}_5$. To je kombinatorická úloha, kdy vybereme libovolně transpozici (tj. neuspořádanou dvojici z pěti prvků) a k ní máme vždy k dispozici dvě možnosti — trojcyklus a trojcyklus k němu inverzní. Dohromady tedy dostáváme $2 \cdot \binom{5}{2} = 5 \cdot 4 = 20$ prvků konjugovaných v $\mathbf{S}_n$ se zadanou permutací σ.

Množina všech konjugovaných prvků s neidentickou permutací nikdy nemůže tvořit podgrupu, jelikož tato množina neobsahuje neutrální prvek. (Vlastně všchny její prvky jsou v našem případě řádu 6.)

3. Ukažte, že platí:

(c) $\langle a, b\rangle_{\mathbb{Z}} = \mathrm{NSD}(a,b)\mathbb{Z}$;
(f) $\langle\{(1\,2), (1\,\ldots\,n)\}\rangle_{\mathbf{S}_n} = \mathbf{S}_n$.

Případ (c) byl, jak jsem se dozvěděl, na přednášce. Inkluze $\supseteq$ plyne z vyjádření $\mathrm{NSD}(a,b)$ pomocí Bézoutovy rovnosti (a z uzavřenosti $\langle a, b\rangle_{\mathbb{Z}}$ na konečné součty a rozdíly, což vyjde nastejno jako uzavřenost na násobení celými čísly). Inkluze $\subseteq$ pak plyne z toho, že $\mathrm{NSD}(a,b)$ je společný dělitel $a, b \in \mathbb{Z}$ (a že $\mathrm{NSD}(a,b)\mathbb{Z}$ je podgrupa v $\mathbb{Z}$); existují tedy $m, n \in \mathbb{Z}$ taková, že $a = m\mathrm{NSD}(a,b)$ a $b = n\mathrm{NSD}(a,b)$.

Pro (f) stačí, ve světle (e), ukázat, že grupa $G = \langle\{(1\,2), (1\,\ldots\,n)\}\rangle_{\mathbf{S}_n}$ obsahuje všechny transpozice $(i\ i+1)$, kde $i \in \{1, \ldots, n-1\}$. To lze například indukcí. Z definice vidíme, že $(1\ 2) \in G$. Předpokládáme-li, že $(i-1\ i) \in G$ pro nějaké $i \in \{2, \ldots, n-1\}$, stačí si všimnout, že $(i\ i+1) = (1\ \ldots\ n)(i-1\ i)(1\ \ldots\ n)^{-1}$.

4. Rozhodněte, zda existuje v grupě $\mathbf{S}_{17}$ prvek řádu (a) 71, (b) 72, (c) 80.

Pouze (b) má kladnou odpověď. Konkrétně kupř. $(1\ 2\ 3\ 4\ 5\ 6\ 7\ 8)(9\ 10\ 11\ 12\ 13\ 14\ 15\ 16\ 17)$ má řád 72. Dále 71 je prvočíslo, a tak nemůže být nejmenším společným násobkem menších čísel. Nakonec $80 = 5 \cdot 16$. Aby tedy bylo 80 nejmenším společným násobkem nějakých menších čísel, musí být jedno z těchto menších čísel dělitelné pěti a nějaké další dělitelné 16. Permutaci řádu 80 proto najdeme až v $\mathbf{S}_{21}$.

5. Buď G grupa řádu 60, $H \leq G$ řádu 5 a $K \leq G$ buď v G indexu 5. Je $H \cap K$ komutativní?

Ano, je. To, že K má v G index 5, znamená, že K má 12 prvků: z Lagrangeovy věty totiž máme $|G| = |K| \cdot [G : K]$. Užívajíce Lagrangeovu větu podruhé, vidíme, že musí mít každý prvek grupy $H \cap K$ řád dělitelný jak pěti, tak dvanácti. Jelikož čísla 5 a 12 jsou nesoudělná, je nutně $H \cap K$ triviální (tj. jednoprvková) grupa.

6. Najděte všechny homomorfismy a popište příslušná jádra a obrazy:

(b) ze $(\mathbb{Z}, +, -, 0)$ do $(\mathbb{Z}_n, +, -, 0)$;
(d) ze $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, -, (0,0))$ do $(\mathbb{Z}_4, +, -, 0)$;
(e) ze $(\mathbb{Z}_4, +, -, 0)$ do $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, -, (0,0))$;
(g) ze $(\mathbb{Z}_m, +, -, 0)$ do $(\mathbb{Z}_n, +, -, 0)$.

Při řešení se nám bude hodit následující pozorování (pro obecné grupy užíváme multiplikativní notaci): Je-li $f : G \to H$ homomorfismus grup, pak pro každé $a \in G$ konečného řádu platí $\mathrm{ord}(f(a)) \mid \mathrm{ord}(a)$. To plyne snadno z implikace $a^n = 1 \implies f(a)^n = f(a^n) = 1$. Dále se hodí mít na paměti, že každý homomorfismus je jednoznačně určen svými hodnotami na libovolné generující množině. Pozor: z toho samozřejmě neplyne, že určíme-li hodnoty zobrazení na nějaké generující množině, jde toto zobrazení rozšířit do homomorfismu grup!

V případu (b) ovšem tvrdíme, že pro každé $k \in \mathbb{Z}_n$ je $g_k : \mathbb{Z} \to \mathbb{Z}_n$ definované vztahem $g_k(z) = kz \mod n$ homomorfismem zadaných grup. Inu jedná se o složení homomorfismu $f_k : \mathbb{Z} \to \mathbb{Z}$, kde $f_k(z) = kz$, který jsme uvažovali on-line na cvičení, a homomorfismu $h_n : \mathbb{Z} \to \mathbb{Z}_n$, kde $h_n(z) = z \mod n$, který znáte například z důkazu Čínské zbytkové věty (jde dokonce o okruhový homomorfimsus, což zde ale nepotřebujeme).

Máme $\operatorname{Ker} g_k = \{z \in \mathbb{Z};\, kz \mod n = 0\} = \frac{\mathrm{NSN}(n,k)}{k}\mathbb{Z} = \frac{n}{\mathrm{NSD}(n,k)}\mathbb{Z}$ a $\operatorname{Im} g_k = \langle k\rangle_{\mathbb{Z}_n} = \langle \mathrm{NSD}(n,k)\rangle_{\mathbb{Z}_n}$, kde ovšem, formálně vzato, platí poslední rovnost jen pokud $k \neq 0$. Nakonec: žádné další homomorfismy kromě $g_k, k \in \mathbb{Z}_n$, neexistují; je-li totiž $g : \mathbb{Z} \to \mathbb{Z}_n$ jakýkoliv homomorfismus, je již určen svou hodnotou v 1, a tedy $g = g_k$ pro $k = g(1)$.

Pro součiny grup je užitečné vědět (a měli byste si snadno zvládnout dokázat), že $f : A \to B \times C$ je homomorfismus grup $\iff$ existují homomorfismy $f_1 : A \to B$ a $f_2 : A \to C$ takové, že $(\forall a \in A)\, f(a) = (f_1(a), f_2(a))$. Jsou-li grupy A, B, C komutativní, pak platí i druhý směr, tj. $g : B \times C \to A$ je homomorfismus právě tehdy, když existují homomorfismy $g_1 : B \to A$ a $g_2 : C \to A$ takové, že $g(b,c) = g_1(b) \cdot g_2(c)$ pro každé $(b,c) \in B \times C$.

Nyní k dalším příkladům. (d) Grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ obsahuje pouze prvky řádů 1 a 2, pročež prvky $1, 3 \in \mathbb{Z}_4$ řádu 4 nemohou být v obrazu žádného homomorfismu. Jelikož homomorfismy $\mathbb{Z}_2 \to \mathbb{Z}_4$ jsou právě dva — identicky nulový a násobení dvěma (tj. izomorfismus $\mathbb{Z}_2$ a podgrupy $\{0,2\} \leq \mathbb{Z}_4$) —, jsou dle předchozího odstavce homomorfismy ze $\mathbb{Z}_2 \times \mathbb{Z}_2$ do $\mathbb{Z}_4$ právě čtyři: prvek $(1,0)$ může jít na 0 či na 2, stejně jako prvek $(0,1)$; hodnota na prvku $(1,1)$ je pak již jednoznačně určena. Obrazem nenulového homomorfismu je vždy podgrupa $\{0,2\}$ grupy $\mathbb{Z}_4$, zatímco jeho jádro může být kterákoliv ze tří dvouprvkových podgrup grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$.

(e) Opět se vzhledem k odstavci o součinech stačí zaměřit na homomorfismy ze $\mathbb{Z}_4$ do $\mathbb{Z}_2$. Každý takový je jednoznačně určen hodnotou v generátoru 1 grupy $\mathbb{Z}_4$. Máme dvě možnosti: poslat 1 na 0, což dává nulový homomorfismus, nebo poslat 1 na 1, což dá homomorfismus „modulo 2“. Dohromady opět máme čtyři různé homomorfismy ze $\mathbb{Z}_4$ do $\mathbb{Z}_2 \times \mathbb{Z}_2$. Obrazem nenulového homomorfismu může být kterákoliv ze tří dvouprvkových podgrup grupy $\mathbb{Z}_2 \times \mathbb{Z}_2$. Jeho jádrem bude vždy podgrupa $\{0,2\}$ grupy $\mathbb{Z}_4$.

(g). Tato část je celkem netriviální a užívá znalost podgrup grupy $\mathbb{Z}_n$, které jste si podrobně probrali na přednášce. Víme, že každý homomorfismus $f : \mathbb{Z}_m \to \mathbb{Z}_n$ je určen obrazem prvku 1, který má v $\mathbb{Z}_m$ řád m. Co se týče možné hodnoty $f(1)$ jsme omezeni jednak tím, že $\mathrm{ord}(f(1)) \mid \mathrm{ord}(1) = m$, a jednak Lagrangeovou větou v $\mathbb{Z}_n$, která má za důsledek, že $\mathrm{ord}(f(1)) \mid n$. Dostáváme, že $\mathrm{ord}(f(1)) \mid \mathrm{NSD}(m,n) =: d$. Je-li $d = 1$, máme jen jednu možnost, a sice homomorfismus identicky nulový. V opačném případě je $\langle n/d\rangle_{\mathbb{Z}_n}$ podgrupa grupy $\mathbb{Z}_n$ řádu d. Rozmyslete si, že je to jediná podgrupa řádu d v $\mathbb{Z}_n$ a že každý prvek grupy $\mathbb{Z}_n$ řádu dělícího d se nachází v této podgrupě. Vidíme, že pro homomorfismus $f : \mathbb{Z}_m \to \mathbb{Z}_n$ musí být $f(1) \in \langle n/d\rangle_{\mathbb{Z}_n}$. Na druhou stranu se snadno ověří, že pro libovolné $c \in \langle n/d\rangle_{\mathbb{Z}_n}$ je $f_c(x) = c \cdot x \mod n$ definice homomorfismu ze $\mathbb{Z}_m$ do $\mathbb{Z}_n$, pro nějž $f(1) = c$.

7. Dokažte, že zadané grupy nejsou izomorfní: (1) $\mathbb{Z}$ a $\mathbb{Z} \times \mathbb{Z}$; (2)* $\mathbb{Q}$ a $\mathbb{Q} \times \mathbb{Q}$.

Ukážeme nejprve, jak vyřešit (a) pomocí invariantu. Uvědomme si totiž, že v grupě $\mathbb{Z}$ platí formule $(\forall x, y)(\exists z)\, x = z + z \vee y = z + z \vee x + y = z + z$, která říká, že pro libovolná dvě celá čísla je buď jedno z nich sudé, nebo je sudý jejich součet. Tato formule ale neplatí v $\mathbb{Z} \times \mathbb{Z}$: stačí vzít prvky $(1,0)$ a $(0,1)$.

Důkaz sporem je pak již nasnadě. Ať $\psi : \mathbb{Z} \to \mathbb{Z} \times \mathbb{Z}$ je nějaký grupový izomorfismus. Zvolme $c, d \in \mathbb{Z}$ tak, aby $\psi(c) = (1,0)$, $\psi(d) = (0,1)$. Je-li jedno z těchto celých čísel, BÚNO c, sudé,

pak existuje $k \in \mathbb{Z}$ takové, že $k + k = c$, a proto také $(1, 0) = \psi(c) = \psi(k + k) = \psi(k) + \psi(k)$, což je spor s tím, že je 1 liché číslo. Podobně, pokud je $c + d$ sudé, opět máme nějaké $j \in \mathbb{Z}$, že $j + j = c + d$, v důsledku čehož pak $(1, 1) = \psi(c) + \psi(d) = \psi(c + d) = \psi(j + j) = \psi(j) + \psi(j)$, což je opět spor. Rozmyslete si, že lze tento argument zobecnit a dokázat tak, že $\mathbb{Z}^m \ncong \mathbb{Z}^n$ pro libovolná $m, n \in \mathbb{N}$, kde $m \neq n$.

Nyní ukážeme část (b). První půle důkazu ale funguje stejně tak dobře i jako důkaz části (a). Mějme libovolný grupový homomorfismus $f : \mathbb{Q} \to \mathbb{Q} \times \mathbb{Q}$. Položme $(r, s) = f(1)$. Tvrdíme, že $(\forall q \in \mathbb{Q})\, f(q) = (qr, qs)$. Pokud se nám to podaří ukázat, zjistíme tím mimo jiné, že f není surjektivní (třeba proto, že je f dokonce homomorfismem vektorových prostorů nad $\mathbb{Q}$), a tedy se nemůže jednak o izomorfismus.

Předně pro $n \in \mathbb{N}$ jest $f(n) = f(\underbrace{1 + \cdots + 1}_{n\times}) = \underbrace{f(1) + \cdots + f(1)}_{n\times} = (nr, ns)$. Také ovšem $f(-n) = -f(n) = (-nr, -ns)$. Pokud nyní budeme mít libovolné $q = m/n \in \mathbb{Q}$, kde $m \in \mathbb{Z}$ a $n \in \mathbb{N}$, pak

$$(mr, ms) = f(m) = f(\underbrace{q + \cdots + q}_{n\times}) = \underbrace{f(q) + \cdots + f(q)}_{n\times},$$

a tedy $f(q) = (mr/n, ms/n) = (qr, qs)$. Tím je důkaz dokončen. Je netriviálním faktem, že část (b) nelze dokázat prostřednictvím invariantu jako tomu bylo u části (a): $\mathbb{Q}$ a $\mathbb{Q} \times \mathbb{Q}$ jsou totiž obě nekonečné beztorzní divizibilní abelovské grupy (definice těchto pojmů na naší přednášce nehledejte); prostředky matematické logiky lze ukázat, že musí obě splňovat tytéž formule jazyka teorie (abelovských) grup.

8. Uvažujme grupu $(\mathbb{Q}, +, -, 0)$. Ukažte, že:

(a) zde mají každé dvě netriviální podgrupy netriviální průnik;

(b) ji nelze nagenerovat žádnou konečnou podmnožinou.

(a). Buďte G, H dvě netriviální podrgupy v $\mathbb{Q}$. Pak existují $q_1 = m_1/n_1 \in G$, $q_2 = m_2/n_2 \in H$ taková, že $m_1, m_2 \in \mathbb{Z} \setminus \{0\}$ a $n_1, n_2 \in \mathbb{N}$. Pak ovšem také $n_1 q_1 = m_1 \in G$ a $n_2 q_2 = m_2 \in H$. V důsledku potom ale $\mathrm{NSN}(m_1, m_2) \in G \cap H$.

(b). Nechť $M = \{m_1/n_1, \ldots, m_k/n_k\} \subseteq \mathbb{Q}$, kde $k \in \mathbb{N}$, $m_i \in \mathbb{Z}$ a $n_i \in \mathbb{N}$ pro každé $i \in \{1, \ldots, k\}$. Převedením na společného jmenovatele lze BÚNO předpokládat, že $n_1 = n_2 = \cdots = n_k$. Pak je ovšem $\langle M \rangle_{\mathbb{Q}} \subseteq \langle 1/n_1 \rangle_{\mathbb{Q}} = \frac{1}{n_1}\mathbb{Z} \subsetneq \mathbb{Q}$. Coby dobrovolné rozšíření tohoto cvičení se můžete pokusit dokázat, že $\mathbb{Q}$ nemá maximální podgrupu, tj. takovou podgrupu $G \leq \mathbb{Q}$, že $G \neq \mathbb{Q}$ a zároveň platí: kdykoliv $G \subsetneq H \leq \mathbb{Q}$, pak $H = \mathbb{Q}$.

9. Buď $n \geq 4$.

(a) Ukažte, že permutaci $\pi = (a\, b)(c\, d)$ sestávající ze dvou disjunktních cyklů lze napsat jako součin trojcyklů.

(b) S využitím předchozího bodu si rozmyslete, že každou sudou permutaci lze napsat jako součin trojcyklů.

(c) Uvědomte si, že jste právě ukázali, že $\mathbf{A}_n$ je pro $n \geq 3$ generována trojcykly.

Pro (a) stačí ověřit, že $\pi = (b\ d\ c)(a\ c\ b)$. Co se (b) týče, každou sudou permutaci lze napsat jako složení sudého počtu (ne nutně nezávislých) transpozic. Vzhledem k (a) si stačí uvědomit, že závislé (tj. nedisjunktní) transpozice jsou buď tvaru $(a\ b)(a\ b)$, což je ovšem identická permutace, nebo tvaru $(a\ b)(b\ c)$, kde $a \neq b \neq c \neq a$. V druhém případě ale máme $(a\ b)(b\ c) = (a\ b\ c)$. Zjistili jsme, že každou dvojici transpozic lze nahradit jedním, popřípadě dvěma trojcykly, a tedy každou sudou permutaci můžeme napsat jako složení trojcyklů. Pro část (c) si pak už jen zbývá uvědomit, že všechny trojcykly jsou v $\mathbf{A}_n$ (pokud $n \geq 3$).

10. Buď $G = \{\left(\begin{smallmatrix} a & b \\ 0 & 1 \end{smallmatrix}\right);\ a, b \in \mathbb{R}, a > 0\}$ grupa s operací maticového násobení.

(a) Ukažte, že $H = \{\left(\begin{smallmatrix} a & 0 \\ 0 & 1 \end{smallmatrix}\right);\ a \in \mathbb{R}, a > 0\}$ je podgrupa v G.

(b) Popište levé a pravé rozkladové třídy podgrupy H.
(c) Najděte nějakou levou/pravou transverzálu rozkladu.

Označme $\mathbb{R}^+$ množinu všech kladných reálných čísel. Spolu s násobením tvoří zřejmě grupu. K tomu, abychom nahlédli (a), si stačí jednak uvědomit, že $1 \in H$ (tj. identická matice náleží do H), a jednak, že H je uzavřená na násobení a inverzní prvky, což plyne ihned z odpovídající vlastnosti pro $\mathbb{R}^+$. Mimochodem, podgrupu H je zvykem kompaktně značit jako $\left(\begin{smallmatrix}\mathbb{R}^+ & 0\\ 0 & 1\end{smallmatrix}\right)$.

Podívejme se na (b) a (c). Každá levá rozkladová třída je tvaru $\left(\begin{smallmatrix}a & b\\ 0 & 1\end{smallmatrix}\right) H$ pro nějaká $a, b \in \mathbb{R}, a > 0$, což je právě množina $\{\left(\begin{smallmatrix}c & b\\ 0 & 1\end{smallmatrix}\right);\, c \in \mathbb{R}^+\} = \left(\begin{smallmatrix}\mathbb{R}^+ & b\\ 0 & 1\end{smallmatrix}\right)$. Levou transverzálou je proto například $\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right);\, b \in \mathbb{R}\}$.

Každá pravá rozkladová třída je tvaru $H\left(\begin{smallmatrix}a & b\\ 0 & 1\end{smallmatrix}\right)$ pro nějaká $a, b \in \mathbb{R}, a > 0$, což je právě množina $\{\left(\begin{smallmatrix}ac & bc\\ 0 & 1\end{smallmatrix}\right);\, c \in \mathbb{R}^+\} = \left\{\left(\begin{smallmatrix}c & bc/a\\ 0 & 1\end{smallmatrix}\right);\, c \in \mathbb{R}^+\right\}$. Jako pravou transverzálu proto můžeme opět zvolit $\{\left(\begin{smallmatrix}1 & b\\ 0 & 1\end{smallmatrix}\right);\, b \in \mathbb{R}\}$.

11. Dokažte, že jsou navzájem izomorfní grupy $K = \{id, (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\} \leq \mathbf{S}_4$, $\mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_8^*$.

Všechny zadané grupy jsou 4prvkové. Nejjednodušší je asi uvědomit si, jaké čtyřprvkové grupy, až na izomorfismus, existují. Úvaha je následující: buď má čtyřprvková grupa $\mathbf{G} = (G, \cdot, ^{-1}, 1)$ prvek řádu 4, a pak je cyklická, tj. izomorfní grupě $\mathbb{Z}_4$ (se sčítáním); nebo jsou všechny prvky $a \in G$, $a \neq 1$, řádu 2 (dle Lagrangeovy věty). V tomto druhém případu pak platí $a^2 = 1$ pro každé $a \in G$. Na druhou stranu, jsou-li $a, b \in G$ takové, že $a \neq b \neq 1 \neq a$, pak $a \cdot b$ musí být rovno zbývajícímu čtvrtému prvku, a tedy také rovno $b \cdot a$. Tím je (komutativní) operace $\cdot$ již určena jednoznačně. Až na izomorfismus tedy existují jen dvě různé 4prvkové grupy.

Nyní si stačí již jen všimnout, že v žádné ze zadaných grup se nevyskytuje prvek řádu 4. To je netriviální snad pouze v případě multiplikativní grupy $\mathbb{Z}_8^* = \{1, 3, 5, 7\}$, kde ale snadno ověříme, že $3^2 = 5^2 = 7^2 = 1$ (vlastně to již víme někdy z druhého či třetího cvičení).

12. Dokažte, že grupy $\mathbf{S}_3 \times \mathbb{Z}_2$, $\mathbf{A}_4$ a $\mathbb{Z}_{12}$ jsou po dvou neizomorfní.

Jedná se o grupy řádu 12. S vědomím, že každý izomorfismus musí zachovávat řády prvků, stačí poukázat na rozdíly v tomto ukazateli. Grupa $\mathbb{Z}_{12}$ je jediná cyklická (a také jediná komutativní), tj. obsahuje prvek řádu 12, zatímco zbylé dvě nikoliv. Grupa $\mathbf{A}_4$ sestává z osmi trojcyklů a prvků grupy K z předchozího cvičení. Neobsahuje tedy prvek řádu 6, zatímco $((1\ 2\ 3), 1) \in \mathbf{S}_3 \times \mathbb{Z}_2$ je prvek řádu 6.

13. Dokažte, že všechny (aditivní) grupy $\mathbb{R}$, $\mathbb{C}$, $\mathbb{R}^n$, kde $n \in \mathbb{N}$ je libovolné, jsou navzájem izomorfní.

Jedná se ve všech případech o vektorové prostory nad tělesem $\mathbb{Q}$ dimenze kontinuum. Každý izomorfismus vektorových prostorů je (z definice) i grupovým izomorfismem (vzhledem k binární operaci $+$).