Algebra — cvičení 11, řešení

2. Rozhodněte, zda množina $\{\pi \in \mathbf{S}_4;\ \pi^3 = \mathrm{id}\}$ tvoří normální podgrupu grupy $\mathbf{S}_4$. Netvoří, jelikož se v zadané množině nalézají například trojcykly (1 2 3) a (1 2 4), ale nikoliv jejich složení (1 2 3) $\circ$ (1 2 4) = (1 3)(2 4), které je řádu 2. Nejedná se proto ani o podgrupu.

3. V grupě $\mathbb{R}/\mathbb{Z}$ popište prvky konečného řádu a ukažte, že $\mathbb{R}/\mathbb{Z}$ je izomorfní podgrupě grupy $\mathbb{C}^*$ sestávající z prvků normy 1.

Předně, $r+\mathbb{Z}$ je prvek konečného řádu v $\mathbb{R}/\mathbb{Z}$ právě tehdy, když pro nějaké $n \in \mathbb{N}$ je $n(r+\mathbb{Z}) = nr+\mathbb{Z} = \mathbb{Z}$, což je ekvivalentní tomu, že $nr \in \mathbb{Z}$. To zřejmě platí právě pro $r \in \mathbb{Q}$. Zbývá najít izomorfismus grupy $\mathbb{R}/\mathbb{Z}$ a grupy $\mathbf{S}^1 = \{c \in \mathbb{C}^*;\ \|c\| = 1\}$.

Pro každé $r \in \mathbb{R}$ definujeme $f(r) = e^{2\pi i r}$. To je jistě homomorfismus z $\mathbb{R}$ na $\mathbf{S}^1$: platí totiž $(\forall r, s \in \mathbb{R})\ f(r+s) = e^{2\pi i(r+s)} = e^{2\pi i r} \cdot e^{2\pi i s} = f(r) \cdot f(s)$. Dále bezprostředně vidíme, že $\mathrm{Ker}(f) = \{r \in \mathbb{R};\ f(r) = 1\} = \mathbb{Z}$. První věta o izomorfismu nám pak ihned dá $\mathbb{R}/\mathbb{Z} \cong \mathbf{S}^1$. I bez ní ale můžeme zadefinovat $g : \mathbb{R}/\mathbb{Z} \to \mathbf{S}^1$ předpisem $g(r+\mathbb{Z}) = f(r)$. To je korektně definované zobrazení, jelikož pokud $r+\mathbb{Z} = s+\mathbb{Z}$, znamená to, že existuje $z \in \mathbb{Z}$ takové, že $r+z = s$, a tedy $g(r+\mathbb{Z}) = f(r) = f(r+z) = f(s) = g(s+\mathbb{Z})$. Dále je toto g opět homomorfismus na $\mathbf{S}^1$. Nakonec $\mathrm{Ker}(g) = \{\mathbb{Z}\}$, jelikož $\mathrm{Ker}(f) = \mathbb{Z}$. Homomorfismus g je proto i prostý.

5. Jaké známé grupě je izomorfní grupa a) $\mathbf{D}_{12}/\,\mathrm{Z}(\mathbf{D}_{12})$; b) $\mathbf{S}_4/K$, kde K je Kleinova 4prvková podgrupa?

a) Označme $F = \mathbf{D}_{12}/\mathrm{Z}(\mathbf{D}_{12})$. Všimněte si, že v $\mathbf{D}_{12}$ platí pro libovolnou rotaci r a zrcadlení z, že $zrz = r^{-1}$. Z toho dostáváme, že z a r komutují jen tehdy, pokud $r = r^{-1}$, což je právě v případě, že r je buď identické zobrazení, nebo středová symetrie (tj. rotace o 180°). Mimo jiné tedy rotace o 60° nekomutuje s žádným zrcadlením, což implikuje, že $\mathrm{Z}(\mathbf{D}_{12})$ sestává právě z identického zobrazení a středové symetrie (víme, že všechny rotace spolu navzájem komutují).

Grupa F je proto 6prvková. Neobsahuje ale žádný prvek řádu 6, jelikož jediné dva prvky tohoto řádu v grupě $\mathbf{D}_{12}$ se při přirozené projekci na F zobrazí na prvky řádu 3: složením tří totožných rotací o 60° je středová symetrie, která v F reprezentuje neutrální prvek $\mathrm{Z}(\mathbf{D}_{12}) \in F$.

Grupa F tedy není cyklická, čímž víme, že není izomorfní grupě $\mathbb{Z}_6$. Jediná další 6prvková grupa, až na izomorfismus, je ale $\mathbf{S}_3$, proto $F \cong \mathbf{S}_3$.

Proč existují právě dvě 6prvkové grupy až na izomorfismus? Inu, je-li $(G, \cdot, {}^{-1}, 1)$ grupa o šesti prvcích, pak dle Cauchyovy věty obsahuje prvek a řádu 3 a prvek b řádu 2. Podgrupa $A = \langle a\rangle$ musí být normální, jelikož je indexu 2: levé i pravé rozkladové třídy jsou právě A a $G\setminus A$. Označme $B = \langle b\rangle$. Z Lagrangeovy věty nyní plyne, že $\langle a, b\rangle = G$ a $A \cap B = \{1\}$. Je-li normální i podgrupa B, pak lze užít **14**. úlohu níže a dostat $G \cong G/A \times G/B \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$. V opačném případě b a a nekomutují, a tedy $a = abb \neq bab = a^2$. Poslední rovnost zde platí, jelikož $bab = bab^{-1}$ musí být opět prvek řádu 3 a A je normální podgrupa, která obsahuje právě dva různé prvky řádu 3, a to a a $a^2 = a^{-1}$. V důsledku je potom $aba = b$, $abab = baba = 1$ a platí $G = \{1, a, b, a^2, ab, ba\}$.

Nyní stačí jen zadefinovat izomorfismus $f : G \to \mathbf{S}_3$ vztahem $f(a) = (1\ 2\ 3)$, $f(b) = (2\ 3)$ (lze zvolit libovolný trojcyklus a libovolnou transpozici). Potom lze již f jednoznačně rozšířit: $f(a^2) = (1\ 3\ 2) = (2\ 3)(1\ 2\ 3)(2\ 3) = f(b)f(a)f(b)$, $f(ab) = (1\ 2\ 3)(2\ 3) = (1\ 2)$, $f(ba) = (2\ 3)(1\ 2\ 3) = (1\ 3)$ a samozřejmě $f(1) = \mathrm{id}$. (Abychom skutečně viděli, že jde o izomorfismus, můžeme si napsat obě tabulky pro binární operace $\cdot$, resp. $\circ$.)

b) Nejprve si uvědomíme, že skutečně $K \trianglelefteq \mathbf{S}_4$, jelikož K je podgrupa v $\mathbf{S}_4$ a obsahuje s každou permutací všechny permutace stejného typu: obsahuje totiž právě identickou permutaci a všechna nezávislá složení dvou transpozic. Jelikož $|\mathbf{S}_4| = 24$, máme stejně jako v příkladu výše $|\mathbf{S}_4/K| = 6$.

Zbývá rozhodnout, zda $\mathbf{S}_4/K \cong \mathbb{Z}_6$, či $\mathbf{S}_4/K \cong \mathbf{S}_3$. První možnost je ovšem vyloučena, neboť již v $\mathbf{S}_4$ není žádný prvek řádu 6 (dokonce žádný prvek řádu většího než 4) a přechodem k faktorgrupě se řády prvků nemohou zvětšit. (To už jsme dříve používali, že při homomorfismu $f : G \to H$ řád prvku $f(g)$ dělí řád prvku g, je-li tento konečný. Zde stačí uvážit přirozenou projekci.)

6. Uvažujme působení grupy $\mathbf{A}_5$ na množinu $X = \{1,2,3,4,5\}^3$, kteréžto působení je definováno vztahem

$$\pi(k,l,m) = (\pi(k), \pi(l), \pi(m)) \text{ pro každé } \pi \in \mathbf{A}_5.$$

Určete počet orbit tohoto působení a nějakou množinu reprezentantů těchto orbit.

Označme $Y = \{1,2,3,4,5\}$. Máme definovanou akci $\psi : \mathbf{A}_5 \to \mathbf{S}_X$, kde $X = Y^3$ a $\psi(\pi)(k,l,m) = (\pi(k), \pi(l), \pi(m))$. Jelikož (1 2 3 4 5) $\in \mathbf{A}_5$, dostáváme orbitu $[(1,1,1)]_\sim = \{(a,a,a);\, a \in Y\}$ a jejího reprezentanta $(1,1,1)$.

Podobně bychom chtěli ukázat, že $[(1,1,2)]_\sim = \{(a,a,b);\, a,b \in Y, a \neq b\}$. Inkluze $\subseteq$ je zřejmá, neb každé $\pi \in \mathbf{A}_5$ je prosté zobrazení. Druhou inkluzi ukážeme nejprve pracněji z definice orbity a posléze elegantněji.

Ať je dáno $a,b \in Y$, $a \neq b$, $(a,a,b) \neq (1,1,2)$. Chceme najít $\pi \in \mathbf{A}_5$ takovou, že $\pi(1) = a, \pi(2) = b$. To uděláme rozborem případů. Pokud $a = 1$, vezmeme $\pi = (2\ b\ c)$, kde c je různé od prvků $1,2,b$. Tím zajistíme, že $(1,1,y) \sim (1,1,2)$ pro každé $y \in Y \setminus \{1\}$. V obecném případě pak uvažujeme rozdíl $d = b - a \mod 5 \in \{1,2,3,4\}$. Případnou opakovanou aplikací pěticyklu (1 2 3 4 5) na $(1,1,1+d)$ dostaneme $(a,a,b) \sim (1,1,1+d) \sim (1,1,2)$.

Elegantnější řešení spočívá v užití vztahu, který říká, že velikost naší orbity je rovna indexu stabilizátoru prvku $(1,1,2)$. K ověření druhé inkluze nám stačí nahlédnout, že tento index je roven $5 \cdot 4 = 20$. Prvek $(1,1,2) \in X$ je stabilizován všemi permutacemi z $\mathbf{A}_5$, které nehýbou ani prvkem 1, ani prvkem 2. Stabilizátorem prvku $(1,1,2)$ je proto podgrupa v $\mathbf{A}_5$ generovaná trojcyklem (3 4 5). Ta má 3 prvky, pročež její index v 60prvkové grupě $\mathbf{A}_5$ je kýžených 20.

Analogicky řešíme orbity $[(1,2,1)]_\sim$ a $[(2,1,1)]_\sim$.

Zbývá ukázat, že $[(1,2,3)]_\sim = \{(a,b,c) \in X;\, a \neq b \neq c \neq a\}$, přičemž inkluze $\subseteq$ je opět zřejmá z prostoty permutací. Pro druhou inkluzi nám stačí, jako v elegantním řešení výše, ukázat, že $|[(1,2,3)]_\sim| = 5 \cdot 4 \cdot 3 = 60$. To je ale jasné, neboť prvek $(1,2,3) \in X$ je stabilizován pouze identickou permutací z $\mathbf{A}_5$.

Nalezli jsme 5 orbit, jejichž reprezentanti jsou po řadě $(1,1,1), (1,1,2), (1,2,1), (2,1,1), (1,2,3)$.

7.

(a) Určete grupu rotací pravidelného čtyřstěnu (tip: označte si stěny čísly 1–4 a přemýšlejte, které permutace z $\mathbf{S}_4$ můžete realizovat otáčením čtyřstěnu).

(b) Pro každé $n \in \mathbb{N}$ určete, kolika způsoby lze obarvit stěny pravidelného čtyřstěnu n barvami (až na orotování čtyřstěnu). Předpokládáme, že α) každou stěnu barvíme celistvě právě jednou barvou (tedy žádné puntíky či proužky), β) různé stěny mohou mít totožné barvy a γ) není nutné použít barvy všecky.

Každá rotace pravidelného čtyřstěnu je jednoznačně určena permutací jeho stěn. Označíme-li tyto stěny $1,2,3,4$, pak lze jistě realizovat libovolný trojcyklus tak, že čtyřstěn položíme na vodorovnou plochu jednou stěnou, kterou tím fixujeme, a otáčíme ho. Na druhou stranu nelze realizovat žádnou transpozici, jak se snadno přesvědčíme. Jelikož trojcykly generují alternující grupu, dostáváme, že $G = \mathbf{A}_4$ je grupou rotací pravidelného čtyřstěnu.

Buď $n \in \mathbb{N}$ libovolné a označme B množinu sestávající z n barev. Množina úplně všech obarvení stěn je potom $X = \{c : \{1,2,3,4\} \to B;\, c \text{ je zobrazení}\}$. Grupa G na X působí akcí ψ, kde $\psi(g)(c) = c \circ g^{-1}$. Ověřme, že jde o akci: předně $\psi(g) \in \mathbf{S}_X$, jelikož $\psi(g) \circ \psi(g^{-1}) = \psi(g^{-1}) \circ \psi(g) = \mathrm{id}_X$ pro každé $g \in G$; dále pro libovolné $c \in X$ máme $\psi(g \circ h)(c) = c \circ (g \circ h)^{-1} = c \circ h^{-1} \circ g^{-1} = \psi(g)(\psi(h)(c)) = (\psi(g) \circ \psi(h))(c)$.

Hledaný počet obarvení dostaneme z Burnsideovy věty jako $\frac{1}{12} \sum_{g \in G} |X_g|$, kde $X_g = \{c \in X;\, c \circ g^{-1} = c\}$ je množina pevných bodů sestávající z takových obarvení c stěn čtyřstěnu n barvami z B, kterážto obarvení se nezmění při rotaci g. Pro každou z 12 permutací z $\mathbf{A}_4$ nyní musíme spočítat hodnotu $|X_g|$.

Nejprve zřejmě $|X_{\mathrm{id}}| = n^4$. Je-li g trojcyklus, pak aby c bylo v X_g, musí barvit stejnou barvou všechny stěny, jimiž g hýbe, a zbylou stěnu libovolně. To dává n^2 možností.

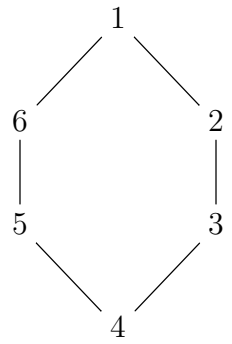
Pokud je g složení dvou nezávislých transpozic, řekněme $(1\ 4)(2\ 3)$, pak musí být stěny $1, 4$ obarveny toutéž barvou a zároveň musí být stěny $2, 3$ obarveny touž barvou. Dohromady opět n^2 možností. (A propos, u analogických obarvovacích úloh vychází vždy n^k možností, kde n je počet barev a k počet různých cyklů v rozkladu g na nezávislé cykly, počítaje v to i jednocykly.)

Celkově dostáváme $\frac{n^4+11n^2}{12}$ obarvení čtyřstěnu n barvami až na otočení. Coby vedlejší produkt našeho snažení jsme ukázali, že $12 \mid n^4 + 11n^2$ pro libovolné $n \in \mathbb{N}$.

8. Uvažujte grupu $\mathbf{D}_{12}$ jakožto podgrupu grupy $\mathbf{S}_6$ generovanou „rotací“ $(1\ 2\ 3\ 4\ 5\ 6)$ a „zrcadlením“ $(2\ 6)(3\ 5)$.

(a) Popište přirozené působení grupy $\mathbf{D}_{12}$ na množině $X = \{\{1,4\},\{2,5\},\{3,6\}\}$ a také na množině $Y = \{\{1,3,5\},\{2,4,6\}\}$.
(b) Užijte (a) k důkazu, že $\mathbf{D}_{12} \cong \mathbf{S}_3 \times \mathbf{S}_2$.

Využijeme toho, že v našem pojetí není grupa $\mathbf{D}_{12}$ nic jiného než grupa automorfismů neorientovaného grafu níže.



Každý grafový izomorfismus musí zachovávat vzdálenosti mezi vrcholy. Grupa $\mathbf{D}_{12}$ proto přirozeně působí na množině sestávající z dvojic protilehlých vrcholů, tj. na $X = \{\{1,4\},\{2,5\},\{3,6\}\}$. Tím myslíme, že $f : \mathbf{D}_{12} \to \mathbf{S}_X$, kde pro každé $\pi \in \mathbf{D}_{12}$ klademe $f(\pi)(\{a,b\}) = \{\pi(a), \pi(b)\}$, je korektně definovaná akce grupy $\mathbf{D}_{12}$ na X.

Nahlédneme, že f je surjektivní. K tomu stačí, aby v obraze homomorfismu f byla nějaká množina generátorů grupy $\mathbf{S}_X$. Například všechny transpozice. Ovšem ty tam jistě jsou, neboť každé ze tří zrcadlení s osou procházející protilehlými vrcholy šestiúhelníka poskytuje jinou transpozici v grupě $\mathbf{S}_X$.

Nyní celou úvahu zopakujeme pro dvouprvkovou množinu $Y = \{\{1,3,5\},\{2,4,6\}\}$. Její prvky jsou (všechny) trojice vrcholů splňující, že každé dva různé vrcholy v trojici mají v grafu vzdálenost 2. Grafový automorfismus zachovává vzdálenosti, a tedy $g : \mathbf{D}_{12} \to \mathbf{S}_Y$, kde klademe $g(\pi)(\{a,b,c\}) = \{\pi(a), \pi(b), \pi(c)\}$, je korektně definovaná akce grupy $\mathbf{D}_{12}$ na množině Y. Zřejmě je g surjektivní, jelikož $g(\pi)$, kde π je středová symetrie, je transpozice v dvouprvkové grupě $\mathbf{S}_Y$.

Závěr. Zobrazení $F : \mathbf{D}_{12} \to \mathbf{S}_X \times \mathbf{S}_Y$ definované vztahem $F(\pi) = (f(\pi), g(\pi))$ je, jak víme z jednoho z minulých cvičení, homomorfismus grup. Konkrétně dvou dvanáctiprvkových grup. Jeho jádro je ovšem triviální, jelikož v $\mathrm{Ker}(f)$ leží kromě identického grafového automorfismu pouze středová symetrie, která ovšem zase není v $\mathrm{Ker}(g)$, jak jsme se přesvědčili na konci předchozího odstavce. Zobrazení F je proto prosté. Jedná se o hledaný izomorfismus grup $\mathbf{D}_{12}$ a $\mathbf{S}_X \times \mathbf{S}_Y$; triviálně je totiž $\mathbf{S}_X \cong \mathbf{S}_3$ a $\mathbf{S}_Y \cong \mathbf{S}_2$.

9. Buď $n \in \mathbb{N}$, $n > 1$. Rozhodněte, zda je grupa všech regulárních horních trojúhelníkových matic $n \times n$ nad tělesem $\mathbb{Q}$ *s jedničkami na diagonále* normální podgrupou a) grupy $\mathbf{GL}_n(\mathbb{Q})$, b) grupy všech regulárních horních trojúhelníkových matic nad $\mathbb{Q}$.

Odpověď je NE v případě a). Pro $n = 2$ stačí uvažovat součin $P \cdot A \cdot P^{-1}$, kde $A = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ a $P = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Pak $P \cdot A \cdot P^{-1} = \begin{pmatrix} 2 & -1 \\ 1 & 0 \end{pmatrix}$, což není horní trojúhelníhová matice. Pro $n > 2$ uvažujeme místo A, resp. P, blokové matice $\begin{pmatrix} W & X \\ Y & Z \end{pmatrix}$, kde $W = A$, resp. $W = P$, dále X a Y jsou nulové a Z je jednotková matice $n - 2 \times n - 2$, tj. $Z = E_{n-2}$.

V případě b) je odpověď ANO. Zde totiž musí konjugující matice P být všude na hlavní diagonále nenulová (aby byla regulární). Má-li P na $i$tém místě (kde $i = 1, \ldots, n$) hlavní diagonály nenulový prvek $a \in \mathbb{Q}$, pak je na témže místě v matici P^{-1} prvek a^{-1}. V součinu $P \cdot A \cdot P^{-1}$, který je zřejmě horní trojúhelníkovou maticí, tedy na $i$tém místě hlavní diagonály máme $a \cdot 1 \cdot a^{-1} = 1$.

10.

(a) Buď $(G, \cdot, ^{-1}, 1)$ grupa a $\varphi : G \to \mathrm{Aut}(G)$ zobrazení definované vztahem $\varphi(g)(x) = g \cdot x \cdot g^{-1}$. Ověřte, že se jedná o korektně definovaný homomorfismus grup $(G, \cdot, ^{-1}, 1)$ a $(\mathrm{Aut}(G), \circ, ^{-1}, \mathrm{id}_G)$. Popište jeho jádro a zjistěte, zda $\mathrm{Inn}(G) := \mathrm{Im}(\varphi)$ tvoří normální podgrupu v $(\mathrm{Aut}(G), \circ, ^{-1}, \mathrm{id}_G)$.

(b) Předpokládejme, že zadaná grupa G je konečná. Ukažte, že $\mathrm{Inn}(G) \cong G$ právě tehdy, když $\mathrm{Z}(G)$ je triviální podgrupa.

(a). Korektnost: je třeba ukázat, že $\varphi(g) \in \mathrm{Aut}(G)$ pro každé $g \in G$. Předně

$$\varphi(g)(x \cdot y) = g \cdot x \cdot y \cdot g^{-1} = g \cdot x \cdot g^{-1} \cdot g \cdot y \cdot g^{-1} = (\varphi(g)(x)) \cdot (\varphi(g)(y)),$$

jedná se tedy o homomorfismus z G do G (také říkáme *endomorfismus* grupy G). Ihned z definice také vidíme, že $\varphi(g) \circ \varphi(g^{-1}) = \mathrm{id}_G = \varphi(g^{-1}) \circ \varphi(g)$, což znamená, že $\varphi(g)$ musí být bijekce; a $\varphi(g^{-1})$ je bijekce k ní inverzní.

Homomorfismus: dokazujeme, že φ je homomorfismus grup. Pro libovolné $g, h, x \in G$ máme

$$\varphi(g \cdot h)(x) = g \cdot h \cdot x \cdot h^{-1} \cdot g^{-1} = g \cdot \varphi(h)(x) \cdot g^{-1} = \varphi(g)(\varphi(h)(x)) = (\varphi(g) \circ \varphi(h))(x).$$

Zobrazení $\varphi(g \cdot h)$ a $\varphi(g) \circ \varphi(h)$ jsou proto totožná.

Jádro: Dle definice jest $\mathrm{Ker}(\varphi) = \{g \in G;\ \varphi(g) = \mathrm{id}_G\}$. V jádru jsou tedy právě takové prvky $g \in G$, že $(\forall x \in G)\, g \cdot x \cdot g^{-1} = x$. Jinými slovy $(\forall x \in G)\, g \cdot x = x \cdot g$, což znamená, že $\mathrm{Ker}(\varphi) = \mathrm{Z}(G)$.

Normalita $\mathrm{Inn}(G)$ v $\mathrm{Aut}(G)$: Pro libovolný $\psi \in \mathrm{Aut}(G)$ a $g, x \in G$ platí:

$$(\psi \circ \varphi(g) \circ \psi^{-1})(x) = \psi(g \cdot \psi^{-1}(x) \cdot g^{-1}) = \psi(g) \cdot x \cdot \psi(g^{-1}) = \psi(g) \cdot x \cdot (\psi(g))^{-1} = \varphi(\psi(g)).$$

Vidíme, že $\mathrm{Inn}(G)$ je uzavřena na konjugace podle $\mathrm{Aut}(G)$, a proto je $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. (To, že obraz homomorfismu, v našem případě $\mathrm{Im}(\varphi)$, je vždy podgrupa, víte z přednášky.)

(b). Z části (a) a 1. věty o izomorfismu plyne $G/\mathrm{Z}(G) \cong \mathrm{Inn}(G)$. Pokud je $\mathrm{Z}(G)$ triviální, pak samozřejmě ihned dostáváme $G \cong G/\{1\} \cong \mathrm{Inn}(G)$. V opačném případě má $G/\mathrm{Z}(G)$ méně prvků, a tedy $\mathrm{Inn}(G)$ má méně prvků než G, a nemůže s ním být proto izomorfní. Tady využíváme konečnosti grupy G. Nekonečné grupě G nic a priori nebrání splňovat $G \cong G/\mathrm{Z}(G)$, byť by její centrum bylo netriviální.

11. Ukažte, že je-li G grupa a $G/\mathrm{Z}(G)$ je cyklická, pak je G komutativní.

Je-li $G/\mathrm{Z}(G)$ cyklická, můžeme si pevně zvolit nějaký její generátor $g\mathrm{Z}(G)$. Jelikož dle definice násobení ve faktorgrupě máme $(g\mathrm{Z}(G))^n = g^n\mathrm{Z}(G)$ pro každé $n \in \mathbb{Z}$, dostáváme $G/\mathrm{Z}(G) = \{g^n\mathrm{Z}(G);\ n \in \mathbb{Z}\}$; při vědomí možnosti, že ve výčtu napravo se prvky opakují, je-li $G/\mathrm{Z}(G)$ konečná. (Zde užíváme standardní značení, kdy $g^0 = 1$ a $g^{-m} = (g^{-1})^m$ pro $m \in \mathbb{N}$.)

Ukazujeme, že G je komutativní. Vezměme libovolné prvky $a, b \in G$. Jelikož je $G/\mathrm{Z}(G)$ rozklad grupy G, musí existovat $m, n \in \mathbb{Z}$ a $y, z \in \mathrm{Z}(G)$ takové, že $a = g^m y$ a $b = g^n z$. Pak $ab = g^m y g^n z = yzg^{m+n} = zyg^n g^m = zg^n yg^m = g^n zg^m y = ba$. Grupa G je proto komutativní, jinak řečeno $G = \mathrm{Z}(G)$.

12. Dokažte, že kdykoliv má (libovolná) grupa G lineárně uspořádané podgrupy, pak $G \cong \mathbb{Z}_{p^k}$ pro nějaké $k \in \mathbb{N}_0 \cup \{\infty\}$ a prvočíslo p.

Nechť je nejprve G konečná. Kdykoliv $a \in G$ a existuje $b \in G \setminus \langle a \rangle$, pak z předpokladu lineární uspořádanosti podgrup musí být $\langle a \rangle \lneq \langle b \rangle$. Indukcí pak snadno ukážeme, že G musí být cyklická. Je proto izomorfní nějaké $\mathbb{Z}_n$, kde $n \in \mathbb{N}$. Pokud by ale n nebyla (nezáporná) mocnina prvočísla, pak by bylo lze napsat $n = l \cdot m$, kde $l, m > 1$ jsou nesoudělná. Dostali bychom $G \cong \mathbb{Z}_n \cong \mathbb{Z}_l \times \mathbb{Z}_m$, což by ale znamenalo, že G obsahuje $l$prvkovou a $m$prvkovou podgrupu, které mají triviální průnik, ve sporu s předpokladem o lineárně uspořádaných podgrupách. Zbývá si uvědomit, že $\mathbb{Z}_{p^k}$ má lineárně uspořádané podgrupy, kdykoliv je p prvočíslo a $k \in \mathbb{N}_0$.

Uvažujme nyní případ, kdy by G byla nekonečná. Nemůže pak obsahovat prvek nekonečného řádu, jelikož ten by generoval podgrupu izomorfní s $\mathbb{Z}$, která zřejmě nemá lineárně uspořádané podgrupy. Stejnou úvahou jako v předchozím odstavci můžeme zkonstruovat posloupnost cyklických podgrup $\langle a_0 \rangle \lneq \langle a_1 \rangle \lneq \ldots$. Rozdíl je v tom, že tentokrát v konečně mnoha krocích nedosáhneme celé grupy G. Položíme-li ale $H = \bigcup_{i \in \mathbb{N}_0} \langle a_i \rangle$, jedná se o nekonečnou podgrupu grupy H. Kdyby nyní existoval nějaký $b \in G \setminus H$, pak by muselo z linearity platit $H \lneq \langle b \rangle$, což není možné vzhledem k tomu, že b musí mít konečný řád. Je tedy $G = H$ a — dle předchozího odstavce a Lagrangeovy věty — musí existovat nějaké prvočíslo p takové, že každá podgrupa $\langle a_i \rangle$ má řád mocniny prvočísla p.

Zbývá ukázat, že $G \cong \mathbb{Z}_{p^\infty}$ a že $\mathbb{Z}_{p^\infty}$ má lineárně uspořádané podgrupy. Tuto část pro nedostatek času vynecháme.

13. Na rozdíl od grupy $\mathbb{R}/\mathbb{Z}$, kterou si lze představit třeba tak, že stočíte reálnou přímku do kružnice o obvodu 1 a počítáte tam s reálnými čísly modulo 1, je to s grupou $\mathbb{R}/\mathbb{Q}$ o poznání méně názorné. Uvědomte si například, že na $\mathbb{R}$ lze pohlížet jako na vektorový prostor nad $\mathbb{Q}$. Lze tak psát $\mathbb{R} = \mathbb{Q} \oplus D$ pro nějaký vektorový podprostor D prostoru $\mathbb{R}$.

(a) Dokažte, že (aditivní) grupy D a $\mathbb{R}/\mathbb{Q}$ jsou izomorfní.

(b) Ukažte, že existuje bijekce (nikoliv izomorfismus) $\beta : \mathbb{R}/\mathbb{Q} \to \mathbb{R}$ a pevně nějakou zvolte. Uvažujte reálnou funkci $f = \beta \circ \pi$, kde $\pi : \mathbb{R} \to \mathbb{R}/\mathbb{Q}$ je přirozená projekce na faktorgrupu, tj. $\pi(r) = r + \mathbb{Q}$. Zvolte si dvě oblíbená reálná čísla a, b, kde $a < b$, a ukažte čemu se rovná $\{f(x);\, a < x < b\}$.

V (a) stačí uvažovat projekci z $\mathbb{R}$ na podprostor D. To je mimo jiné surjektivní homomorfismus grup, jehož jádro je právě $\mathbb{Q}$. Zbývá tedy užít 1. větu o izomorfismu.

Klíčem v (b) je si uvědomit, že $\mathbb{R}/\mathbb{Q} = \{r + \mathbb{Q};\, r \in \mathbb{R}\}$ je rozklad množiny $\mathbb{R}$, jehož bloky jsou spočetné (a v $\mathbb{R}$ husté) množiny $r + \mathbb{Q}$, kde r probíhá $\mathbb{R}$. Reálná přímka se (v důsledku axiomu výběru) nedá napsat jako sjednocení méně než kontinua spočetných množin. Musí proto existovat nějaká bijekce $\beta : \mathbb{R}/\mathbb{Q} \to \mathbb{R}$. Zvolme reálná čísla $a < b$ libovolně a k tomu ještě libovolné $r \in \mathbb{R}$. Položme $s + \mathbb{Q} = \beta^{-1}(r)$. To je v $\mathbb{R}$ hustá podmnožina, a proto musí existovat $c \in \mathbb{R}$ takové, že $a < c < b$ a $c \in s + \mathbb{Q}$. Jinak řečeno $c + \mathbb{Q} = s + \mathbb{Q}$, pročež $f(c) = \beta(\pi(c)) = \beta(c + \mathbb{Q}) = \beta(s + \mathbb{Q}) = r$. Můžeme uzavřít, že obraz libovolného neprázdného otevřeného intervalu zobrazením f je celé $\mathbb{R}$. (Tahle funkce se opravdu špatně kreslí jedním tahem.)

Mimochodem, zobrazení β se dá volit dokonce jako izomorfismus vektorových prostorů nad $\mathbb{Q}$ dimenze kontinua. Zobrazení f je potom nespojitý endomorfismus aditivní grupy $\mathbb{R}$ (dokonce vektorového prostoru $\mathbb{R}$ nad $\mathbb{Q}$).

14. Dokažte, že má-li grupa G normální podgrupy A, B takové, že $AB = G$ a $A \cap B = \{1\}$, pak je $G \cong G/A \times G/B$.

Označme $\pi : G \to G/A$ a $\rho : G \to G/B$ přirozené projekce. Již víme, že tyto určují homomorfismus $\psi : G \to G/A \times G/B$ definovaný vztahem $\psi(g) = (\pi(g), \rho(g)) = (gA, gB)$. Ukážeme, že je ψ dokonce izomorfismus.

Uvažujme $g \in \mathrm{Ker}(\psi)$. To jest $\psi(g) = (A, B)$, což je ekvivalentní tomu, že $g \in A \cap B$. Vzhledem k našemu předpokladu dostáváme $g = 1$ a vidíme, že ψ je prosté.

Mějme nyní libovolné $(g_1A, g_2B) \in G/A \times G/B$. Hledáme $g \in G$ takové, že $(gA, gB) = (g_1A, g_2B)$. Z předpokladu (a přednášky) víme, že $G = AB = BA$. Můžeme si proto vyjádřit $g_1 = b_1a_1$ a $g_2 = a_2b_2$, kde $a_i \in A$, $b_i \in B$ pro $i = 1, 2$. Vidíme, že $g_1A = b_1a_1A = b_1A$ a $g_2B = a_2b_2B = a_2B$. Položíme $g = a_2b_1$. Pak $gA = Ag = Aa_2b_1 = Ab_1 = b_1A = g_1A$ a $gB = a_2b_1B = a_2B = g_2B$, kde jsme v prvním případě využili normality podgrupy A.

Mimochodem, můžeme si uvědomit, že také platí $B \cong G/A$ (a symetricky $A \cong G/B$). Stačí uvažovat $\pi \restriction B : B \to G/A$. Jelikož $\mathrm{Ker}(\pi) = A$ a $A \cap B = \{1\}$, je $\pi \restriction B$ prosté. Na druhou stranu jsme v předchozím odstavci viděli, že pro každé $g_1 \in G$ najdeme $b_1 \in B$ takové, že $g_1A = b_1A$, tj. zobrazení $\pi \restriction B$ je také surjektivní. Dostáváme proto rovněž $G \cong B \times A$.

15. Uvažujte krychli jakožto neorientovaný graf s 8 vrcholy a 12 hranami. Nechť G značí grupu všech automorfismů tohoto grafu. Dokažte, že $G \cong \mathbf{S}_4 \times \mathbf{S}_2$.

Uvažujme akci φ grupy G na čtyřprvkové množině X sestávající z neuspořádaných dvojic vrcholů krychle, které leží na tělesové úhlopříčce. Z hlediska grafu se jedná právě o takové dvojice vrcholů, které od sebe mají v grafu vzdálenost 3 (tj. největší možnou). Každý automorfismus grafu zachovává vzdálenosti, a proto se jedná o dobře definovanou akci.

Jaké je jádro $\mathrm{Ker}(\varphi)$? Jedná se o takové prvky grupy G, které ponechají na místě všechny tělesové úhlopříčky. Snadno se nahlédne, že kromě identického zobrazení má tuto vlastnost již pouze středová symetrie krychle. Je tedy $\mathrm{Ker}(\varphi) \cong \mathbb{Z}_2$.

Označme R 24prvkovou podgrupu grupy G sestávající ze všech rotací krychle (na konkrétní rotace se můžete podívat např. do skript: řešení úlohy nahoře na straně 86). Ta neobsahuje středovou symetrii krychle, a proto je $\varphi \restriction R$ prosté. Z toho ihned plyne, že φ je zobrazení na grupu $\mathbf{S}_X$, která má ovšem právě 24 prvků.

Z Lagrangeovy věty a 1. věty o izomorfismu pak plyne, že G musí mít 48 prvků, neboť $|G| = |\mathrm{Ker}(\varphi)| \cdot [G : \mathrm{Ker}(\varphi)] = 2 \cdot |G/\mathrm{Ker}(\varphi)| = 2 \cdot |\mathrm{Im}(\varphi)| = 2 \cdot |\mathbf{S}_X|$.

Víme, že $R \trianglelefteq G$, jelikož $[G : R] = 2$; navíc je jistě $R \cap \mathrm{Ker}(\varphi)$ triviální a $R\,\mathrm{Ker}(\varphi) = G$, jelikož $R\,\mathrm{Ker}(\varphi)$ má alespoň 25 prvků. Užitím předchozího příkladu a 1. věty o izomorfismu proto můžeme uzavřít, že $G \cong G/\mathrm{Ker}(\varphi) \times G/R \cong \mathbf{S}_X \times \mathbb{Z}_2 \cong \mathbf{S}_4 \times \mathbf{S}_2$.

16. Kolik různých náhrdelníků lze sestavit ze šesti černých a tří žlutých korálků, použijeme-li vždy všech devět? (Předpokládáme, že máme k dispozici potřebné propriety jako šňůrku apod.)

Odkazujeme na řešení ekvivalentní úlohy ve skriptech na straně 85. Výsledek je 7.