

## 9 Řád a neřád v teorii grup

Řešení

verze ze dne 14. dubna 2025.

**Cíle cvičení:** Tentokrát si důkladně rozmyslíme, jak nám pomáhá Lagrangeova věta při zjišťování řádů prvků či indexů podgrup dané grupy. Tam, kam už její dlouhá a lačná chapadla nedosáhnou, nám nezbude než zapojit své počtářské svaly. Nakonec si za odměnu trochu pohrajeme s grupovými homomorfismy.

**Úlohy, které bychom určitě měli umět řešit:**

**Úloha 9.1.** Jaký řád mají následující prvky v grupách? (a) 4 a 15 v  $\mathbb{Z}_{75}$ , (b) 7 a 9 v  $\mathbb{Z}_{20}^*$ , (c) 4 a 15 v  $\mathbb{Z}$ , (d)  $(1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)$ ,  $(1\ 2)(5\ 6\ 8\ 9)$  v  $\mathbf{S}_9$  a  $\mathbf{A}_{2025}$ .

**Řešení.** (a) Hledáme nejmenší přirozené  $n$ , pro něž  $4n \equiv 0 \pmod{75}$ . Protože jsou čísla 4 a 75 nesoudělná, dostáváme  $\text{ord}(4) = n = 75$ .

V druhém případě hledáme nejmenší přirozené  $m$ , pro které  $15m \equiv 0 \pmod{75}$ , což je ekvivalentní kongruenci  $m \equiv 0 \pmod{5}$ , proto  $\text{ord}(15) = m = 5$ .

(b) Protože  $|\mathbb{Z}_{20}^*| = \varphi(20) = 8$ , jsou možné řady prvků této grupy podle Lagrangeovy věty pouze  $2^i$  pro  $i = 0, \dots, 4$ . Protože  $7^2 = 49 \equiv 9 \not\equiv 1 \pmod{20}$  a  $7^4 \equiv 9^2 \equiv 1 \pmod{20}$ , vidíme tentokrát, že  $\text{ord}(7) = 4$  a že  $\text{ord}(9) = 2$ .

(c) V grupě celých čísel opakovaným přičítáním nenulového prvku nikdy nedostaneme 0, proto mají oba prvky nekonečný řád.

(d) Z úvah o zápisu permutace v nezávislých cyklech  $\sigma = c_1 \dots c_k$  víme, že  $\sigma^m = c_1^m \dots c_k^m$  a  $c_i^m = \text{id}$ , právě když je  $m$  násobkem délky cyklu  $c_i$ , proto je řád permutace roven právě nejmenšímu společnému násobku délek všech nezávislých cyklů, tedy

$$\text{ord}((1\ 2\ 3\ 4)(5\ 6\ 7)(8\ 9)) = \text{nsn}(4, 3, 2) = 12, \quad \text{ord}((1\ 2)(5\ 6\ 8\ 9)) = \text{nsn}(2, 4) = 4,$$

což platí v obou grupách  $\mathbf{S}_9$  a  $\mathbf{A}_{2025}$ .

**Úloha 9.2.** Najděte nejmenší podgrupu grupy  $\mathbf{S}_5$ , která obsahuje prvek  $\pi = (1\ 2\ 3\ 4\ 5)$ , tj.  $\langle \pi \rangle_{\mathbf{S}_5}$ . Jakého je řádu a jakého indexu?

**Řešení.** Hledaná podgrupa  $H$  je právě cyklická grupa řádu 5 sestávající z mocnin prvku  $\pi$ , tedy podgrupa  $\langle \pi \rangle = \{\pi^i \mid i \in \mathbb{Z}_5\} = \{\text{id}, (1\ 2\ 3\ 4\ 5), (1\ 3\ 5\ 2\ 4), (1\ 4\ 2\ 5\ 3), (1\ 5\ 4\ 3\ 2)\}$ . Z Lagrangeovy věty dostáváme, že  $\text{index}[\mathbf{S}_5 : \langle \pi \rangle] = \frac{|\mathbf{S}_5|}{|\langle \pi \rangle|} = \frac{5!}{5} = 24$ .

**Úloha 9.3.** Rozhodněte, zda je  $H$  podgrupa  $G$  a pokud je, určete index  $[G : H]$  a všechny levé rozkladové třídy  $G$  podle  $H$ , jestliže

(a)  $G = \mathbb{Z}_{12}$  a  $H = \{0, 3, 6, 9\}$ ,

(b)  $G = \mathbb{Z}_{10}$  a  $H = \{0, 3, 6, 9\}$ ,

(c)  $G = \mathbf{S}_3$  a  $H = \{\text{id}, (1\ 2), (2\ 3)\}$ ,

(d)  $G = \mathbf{S}_3$  a  $H = \{\text{id}, (1\ 2)\}$ .

**Řešení.** (a) Vidíme, že  $H = \langle 3 \rangle$ , tedy se jedná o cyklickou podgrupu  $\mathbb{Z}_{12}$ . Její index můžeme spočítat pomocí Lagrangeovy věty  $[G : H] = \frac{|G|}{|H|} = \frac{12}{4} = 3$ . Rozkladové třídy jsou právě podmnožiny tvaru  $g + H$  pro  $g \in G$  a existují tři různé třídy:

$$H = 0 + H = \{0, 3, 6, 9\}, \quad 1 + H = \{1, 4, 7, 10\}, \quad 2 + H = \{2, 5, 8, 11\}.$$

(b) Tentokrát například  $6 + 6 = 2 \notin H$ , což znamená, že  $H$  není podgrupa  $G$ . Že se nejedná o podgrupu jsme mohli rovněž usoudit na základě Lagrangeovy věty, protože řád podgrupy musí dělit řád grupy.

(c) Protože  $(12), (23) \in H$ , ale  $(12) \circ (23) = (123) \notin H$ , nejde o podgrupu grupy  $S_3$ .

(d) Protože jsou oba prvky  $H$  samy k sobě inverzní, uzavřenost na součin s neutrálním prvkem triviálně platí pro každou podmnožinu grupy a  $(12) \circ (12) = \text{id}$  (což plyne z pozorování o inverzních prvcích), vidíme, že  $H$  je uzavřená na obě operace a obsahuje neutrální prvek, tedy jde o podgrupu. Levé rozkladové třídy jsou právě

$$H = \text{id}H = \{\text{id}, (12)\}, \quad (123)H = \{(123), (13)\}, \quad (132)H = \{(132), (23)\},$$

a proto  $[G : H] = 3$ .

**Úloha 9.4.** Rozhodněte, která z následujících zobrazení jsou homomorfismy grup. U homomorfismů popište jejich jádra a obrazy.

(a)  $f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_{15}$  je dáno předpisem  $f(k) = 5k$  pro každé  $k \in \mathbb{Z}_3$ ,

(b)  $f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_{16}$  je dáno předpisem  $f(k) = 5k$  pro každé  $k \in \mathbb{Z}_3$ ,

(c)  $f: \mathbb{Z}_3 \rightarrow \mathbb{Z}_{15}$  je dáno předpisem  $f(k) = 4k$  pro každé  $k \in \mathbb{Z}_3$ ,

(d)  $f: \mathbb{Z}_{15} \rightarrow \mathbb{Z}_3$  je dáno předpisem  $f(k) = k \bmod 3$  pro každé  $k \in \mathbb{Z}_{15}$ ,

(e)  $f: \mathbb{Z}_{16} \rightarrow \mathbb{Z}_3$  je dáno předpisem  $f(k) = k \bmod 3$  pro každé  $k \in \mathbb{Z}_{16}$ .

**Řešení.** (a) Protože  $f(k+l) = 5 \cdot ((k+l) \bmod 3) = (5(k+l) \bmod 15) = f(k) + f(l)$ , vidíme, že je  $f$  grupový homomorfismus. Přitom

$$\text{Im } f = \{5k \mid k \in \mathbb{Z}_3\} = \{0, 5, 10\} \quad \text{a} \quad \text{Ker } f = \{k \in \mathbb{Z}_3 \mid 5k = 0\} = \{0\}.$$

(b) Tentokrát se o homomorfismus nejedná, protože

$$f(1+2) = f(0) = 0 \neq 15 = 5 + 10 = f(1) + f(2).$$

(c) Ani nyní nemáme co do činění s homomorfismem, neboť

$$f(1+2) = f(0) = 0 \neq 12 = 4 + 8 = f(1) + f(2).$$

(d) Protože  $f(k+l) = (k+l) \bmod 3 = f(k) + f(l)$ , je zobrazení  $f$  homomorfismus a z definice spočítáme, že  $\text{Im } f = \mathbb{Z}_3$  a  $\text{Ker } f = 3\mathbb{Z}_{15} = \{0, 3, 6, 9, 12\}$ .

(e) Protože  $f(15+1) = f(0) = 0 \neq 1 = 0 + 1 = f(15) + f(1)$ , není zobrazení  $f$  homomorfismus.

**A teď něco pro potěšení ducha i obveselení těla (asi bude spokojenější duch):**

**Úloha 9.5.** Rozhodněte,

(a) zda existují v grupě  $\mathbb{Z}_{30}$  podgrupy řádu 4, 5, 6,

(b) zda existují v grupě  $S_{17}$  prvky řádu 71, 72, 80.

**Řešení.** (a) Protože má grupa  $\mathbb{Z}_{30}$  právě 30 prvků a  $4 \nmid 30$ , plyne okamžitě z Lagrangeovy věty, že podgrupu řádu 4 v  $\mathbb{Z}_{30}$  nenajdeme. Pro čísla 5 a 6 naopak snadno ověříme, že

$$\langle 6 \rangle = \left\langle \frac{30}{5} \right\rangle = \{0, 6, 12, 18, 24\}, \quad \langle 5 \rangle = \left\langle \frac{30}{6} \right\rangle = \{0, 5, 10, 15, 20, 25\}$$

jsou podgrupy řádů 5 a 6.

(b) Protože má grupa  $\mathbf{S}_{17}$  právě  $17!$  prvků a  $71 \nmid 17!$ , nemůže podle Lagrangeovy věty grupa žádnou podgrupu ani prvek řádu 71 obsahovat.

Připomeňme, že řád permutace můžeme spočítat jako nejmenší společný násobek délek všech jejích nezávislých cyklů. Protože  $72 = \text{nsn}(8, 9)$ , stačí nám najít permutaci sestávající z jednoho cyklu délky 8 a jednoho cyklu délky 9, již je například permutace  $\sigma = (1 \dots 8)(9 \dots 17)$ , pro niž  $o(\sigma) = 72$ .

Prvek řádu 80 v  $\mathbf{S}_{17}$  nenajdeme, neboť pro disjunktní cykly délek  $n_i$  s  $\text{nsn}(n_i \mid i \leq k) = 80$  by musely v permutaci existovat nezávislé cykly délky  $n_i = 16$  a  $n_j = 5$ , což by znamenalo, že  $\sum n_i \geq 16 + 5 > 17$ , což v permutační grupě  $\mathbf{S}_{17}$  není možné a prvek řádu 80 v  $\mathbf{S}_{17}$  není, ačkoli  $80 \mid 17!$ .

**Úloha 9.6.** Buď  $G$  grupa řádu 60,  $H \leq G$  řádu 5 a  $K \leq G$  buď v  $G$  indexu 5. Je  $H \cap K$  komutativní?

**Řešení.** Kupodivu se nám opět bude hodit Lagrangeova věta. Protože je  $H \cap K$  podgrupou jak grupy  $H$ , tak grupy  $K$ , musí řád  $H \cap K$  dělit oba řády. Víme, že grupa  $H$  je řádu 5 a  $K$  je v  $G$  indexu 5, což podle Lagrangeovy věty znamená, že je řádu  $\frac{|G|}{[G:K]} = \frac{30}{5} = 6$ . Čísla 5 a 6 jsou ovšem nesoudělná, proto je grupa  $H \cap K$  jednoprvková a z triviálních důvodů komutativní.

**Úloha 9.7.** Jaký řád mají následující prvky v daných grupách?

(a) rotace o  $144^\circ$  v  $\mathbf{D}_{10}$ ,

(b) matice  $\begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix}$ ,  $\begin{pmatrix} -1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix}$ ,  $\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}$  a  $\begin{pmatrix} 0 & 0 & i \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}$  v  $\mathbf{GL}_3(\mathbb{C})$ ,

(c) dvojice  $((123)(45), (1234))$  v direktním součinu grup  $\mathbf{S}_5 \times \mathbf{S}_4$ .

**Řešení.** (a) Ptáme se, kolik nejméně složení rotací o  $144^\circ$  nám dá rotaci, která je násobkem úhlu  $360^\circ$ , a snadno spočítáme, že jich potřebujeme pět, tedy má tato rotace v  $\mathbf{D}_{10}$  řád 5.

(b) Opět nás zajímá pro každou z matic  $A$  nejmenší kladné  $n$ , pro něž je  $A^n = I_3$ . Uvědomíme-li si, že je první matice permutační maticí odpovídající trojcyklu a že druhá matice je matice rotace o  $60^\circ$  kolem osy  $x$  složená se středovou symetrií, pak vidíme, že

$$\text{ord} \left( \begin{pmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & 0 \end{pmatrix} \right) = 3, \quad \text{ord} \left( \begin{pmatrix} -1 & 0 & 0 \\ 0 & -\frac{1}{2} & -\frac{\sqrt{3}}{2} \\ 0 & \frac{\sqrt{3}}{2} & -\frac{1}{2} \end{pmatrix} \right) = 6$$

Dále má matice

$$\begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 2 \end{pmatrix}^k$$

na pozici  $(3, 3)$  číslo  $2^k$  pro všechna  $k \in \mathbb{N}$ , tedy nejde o jednotkovou matici a pro zadanou matici to znamená, že se jedná o prvek nekonečného řádu. Konečně z výpočtu

$$\begin{pmatrix} 0 & 0 & i \\ 0 & -1 & 0 \\ 1 & 0 & 0 \end{pmatrix}^8 = \begin{pmatrix} i & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & i \end{pmatrix}^4 = \begin{pmatrix} -1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{pmatrix}^2 = I_3$$

vidíme, že řád poslední matice je 8.

(c) Protože  $((123)(45), (1234))^k = ((123)^k(45)^k, (1234)^k)$ , vidíme, že řád prvku  $((123)(45), (1234))$  je roven právě nejmenšímu společnému násobku řádů prvků obou složek, tedy

$$\text{ord}((123)(45), (1234)) = \text{nsn}(\text{ord}(123)(45), \text{ord}(1234)) = \text{nsn}(6, 4) = 12.$$

**Úloha 9.8.** Najděte všechny homomorfismy

- (a) ze  $(\mathbb{Z}, +, -, 0)$  do  $(\mathbb{Z}, +, -, 0)$ ,
- (b) ze  $(\mathbb{Z}, +, -, 0)$  do  $(\mathbb{Z}_n, +, -, 0)$ ,
- (c) ze  $(\mathbb{Z}_n, +, -, 0)$  do  $(\mathbb{Z}, +, -, 0)$ ,
- (d) ze  $(\mathbb{Z}_2, +, -, 0)$  do  $(\mathbf{S}_n, \circ, {}^{-1}, \text{id})$ ,
- (e) ze  $(\mathbb{Z}_3, +, -, 0)$  do  $(\mathbb{Z}_5, +, -, 0)$ ,
- (f) ze  $(\mathbb{Z}_6, +, -, 0)$  do  $(\mathbb{Z}_{15}, +, -, 0)$ ,
- (g) ze  $(\mathbb{Z}_{15}, +, -, 0)$  do  $(\mathbb{Z}_6, +, -, 0)$ ,
- (h) ze  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, -, (0, 0))$  do  $(\mathbb{Z}_4, +, -, 0)$ ,
- (i) ze  $(\mathbb{Z}_4, +, -, 0)$  do  $(\mathbb{Z}_2 \times \mathbb{Z}_2, +, -, (0, 0))$ ,
- (j) ze  $(\mathbb{Z}_{11}^*, \cdot, {}^{-1}, 1)$  do  $(\mathbb{Z}_6, +, -, 0)$ ,
- (k) ze  $(\mathbb{Z}_6, +, -, 0)$  do  $(\mathbb{Z}_{11}^*, \cdot, {}^{-1}, 1)$ .

**Řešení.** Ve všech případech existuje příslušný triviální homomorfismus  $f$  zobrazující všechny prvky na neutrální prvek (tedy s jádrem rovným výchozí grupě). Dále popíšeme netriviální homomorfismy.

(a) Každý homomorfismus je jednoznačně určen obrazem prvku 1 a všechny obrazy prvku jedna nám homomorfismus určí. To znamená, že netriviální homomorfismy jsou právě tvaru  $f_k(x) = x$  pro nenulová  $k \in \mathbb{Z}$ .

(b) Opět je každý určen obrazem prvku 1, pro nenulová  $k \in \mathbb{Z}_n$  platí  $f_k(x) = k \cdot x \pmod{n}$ ,

(c) Žádný netriviální homomorfismus  $\mathbb{Z}_n \rightarrow \mathbb{Z}$  neexistuje, neboť homomorfní obraz prvky konečného řádu musí být opět konečného řádu (který navíc díky Lagrangeově větě dělí řád vzoru), ovšem v grupě  $\mathbb{Z}$  je konečného řádu pouze prvek 0, zatímco v  $\mathbb{Z}_n$  jsou konečného řádu všechny prvky.

(d) Homomorfní obraz prvku 1, který je řádu 2, musí být díky Lagrangeově větě řádu 2 nebo 1. Snadnou diskusí nahlédneme, že  $f_\sigma(0) = \text{id}$  a  $f_\sigma(1) = \sigma$  pro libovolnou permutaci složenou z nezávislých transpozic  $\sigma \in \mathbf{S}_n$ ,  $\text{Ker } f_\sigma = \{0\}$ ,  $\text{Im } f_\sigma = \langle \sigma \rangle = \{\text{id}, \sigma\}$  jsou právě všechny netriviální homomorfismy.

(e) Protože řád homomorfního obrazu prvku dělí díky Lagrangeově větě řád prvku, nenulové prvky grupy  $\mathbb{Z}_3$  jsou řádu 3 a nenulové prvky grupy  $\mathbb{Z}_5$  jsou řádu 5, mají homomorfní obrazy všech prvků grupy  $\mathbb{Z}_3$  v grupě  $\mathbb{Z}_5$  řád 1, tedy jsou nulové. Tudíž žádný netriviální homomorfismus  $\mathbb{Z}_3 \rightarrow \mathbb{Z}_5$  neexistuje.

(f) Každý homomorfismus je opět určen obrazem generátoru 1. To znamená, že možné řády homomorfního obrazu prvku 1 jsou buď 1, což má pouze prvek 0, nebo 3, kterého jsou prvky 5 a 10. Nyní podobně jako v předchozích úlohách vidíme, že netriviální homomorfismy jsou právě zobrazení  $f_k(x) = k \cdot x \pmod{15}$  pro  $k \in \{5, 10\}$ .

(g) Obdobnou diskusí jako v (f) dostaneme netriviální homomorfismy  $f_k(x) = k \cdot x \pmod{6}$  pro  $k \in \{2, 4\}$ .

(h) Diskusí zjistíme, že jediné netriviální homomorfismy jsou:

$$f_1: (1, 0), (0, 1) \mapsto 2, \quad f_2: (1, 0), (1, 1) \mapsto 2, \quad f_3: (1, 1), (0, 1) \mapsto 2,$$

kde obrazy zbylých dvou prvků jsou vždy 0.

(i) Opět uvážíme, že je každý homomorfismus určen obrazem prvku 1, a dále si rozmyslíme, že všechny možnosti nám homomorfismus určují, tedy  $f_1(1) = (1, 0)$ ,  $f_2(1) = (1, 1)$ ,  $f_3(1) = (0, 1)$  a dále  $f_i(2) = 0$  a  $f_i(3) = f_i(1)$  pro  $i = 1, 2, 3$  jsou právě všechny netriviální homomorfismy.

(j) Protože  $\mathbb{Z}_{11}^*$  je generována např. prvkem 2, který je řádu 10, jsou všechny možné homomorfismy dány předpisem  $2^a \mapsto ka \pmod{6}$  pro  $k \in \{0, 3\}$ .

(k) Z podobného důvodu jako v (j) jsou všechny možné homomorfismy dány předpisem  $a \mapsto 2^{ka} \pmod{11}$  pro  $k \in \{0, 5\}$ , tedy máme zde jediný netriviální homomorfismus  $a \mapsto 2^{5a} \pmod{11}$ .

**Úloha 9.9.** Uvažujme grupu  $(\mathbb{Q}, +, -, 0)$ . Ukažte, že

(a) v ní mají každé dvě netriviální podgrupy netriviální průnik,

(b) ji nelze generovat jedním prvkem (dokonce ani žádnou konečnou podmnožinou).

**Řešení.** (a) Pokud  $0 \neq \frac{a}{b} \in A$  a  $0 \neq \frac{c}{d} \in B$ , kde  $A, B \leq \mathbb{Q}$ , pak  $ac = cb \cdot \frac{a}{b} \in A$  a  $ac = ad \cdot \frac{c}{d} \in B$ , tedy  $ac \in A \cap B$ .

(b) Kdyby  $\frac{a}{b} \in \mathbb{Q}$  a  $p$  bylo prvočíslo, které nedělí  $b$ , pak by  $\frac{1}{p} \notin \langle \frac{a}{b} \rangle$ , tedy  $\frac{a}{b}$  nemůže být generátor celého  $\mathbb{Q}$ . Podobně, uvažíme-li pro libovolnou konečnou množinu  $\{\frac{a_1}{b_1}, \dots, \frac{a_n}{b_n}\}$  a prvočíslo  $p$ , které nedělí žádný ze jmenovatelů  $b_i$ , pak opět  $\frac{1}{p} \notin \langle \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \rangle$ , tedy  $\mathbb{Q} \neq \langle \frac{a_1}{b_1}, \dots, \frac{a_n}{b_n} \rangle$ .

**Úloha 9.10.** Určete, v kterých z následujících grup tvoří sudá čísla podgrupu:  $\mathbb{Z}, \mathbb{Z}_{15}, \mathbb{Z}_{16}, \mathbb{Z}_{15}^*, \mathbb{Z}_{16}^*$ .

**Řešení.** Množina všech sudých čísel představuje celočíselné násobky dvojky a je tudíž uzavřená na sčítání, odčítání a obsahuje 0, tedy v  $\mathbb{Z}$  se jedná o podgrupu.

Sudá čísla v  $\mathbb{Z}_{15}$  nejsou uzavřená na sčítání, protože například  $8 + 8 = 1$ , tedy tentokrát se o podgrupu nejedná.

V případě  $\mathbb{Z}_{16}$  nahlédneme, že stejně jako u  $\mathbb{Z}$  tvoří sudé hodnoty podgrupu.

Sudá čísla v  $\mathbb{Z}_{15}^*$  ani  $\mathbb{Z}_{16}^*$  nezahrnují neutrální prvek 1, tedy se o podgrupu nemůže jednat.

**Úloha 9.11.** Rozhodněte, zda (a)  $\{\pi \in \mathbf{A}_4 \mid \pi^2 = \text{id}\}$ , (b)  $\{\pi \in \mathbf{A}_4 \mid \pi^3 = \text{id}\}$  tvoří podgrupu grupy  $\mathbf{A}_4$ . Vyřešte analogickou úlohu pro grupu  $\mathbf{S}_4$ .

**Řešení.** (a) Snadno ověříme, že je množina

$$\{\pi \in \mathbf{A}_4 \mid \pi^2 = \text{id}\} = \{\text{id}, (12)(34), (13)(24), (14)(23)\}$$

uzavřená na skládání, každý prvek je zde sám k sobě inverzní a leží zde neutrální prvek, proto se jedná o podgrupu  $\mathbf{A}_4$ . Naopak množina

$$\{\pi \in \mathbf{S}_4 \mid \pi^2 = \text{id}\} = \{\text{id}, (12), (13), (14), (23), (24), (34), (12)(34), (13)(24), (14)(23)\}$$

zjevně není uzavřena na skládání, proto se nejedná o podgrupu.

(b) Tentokrát okamžitě vidíme, že množina

$$\{\pi \in \mathbf{A}_4 \mid \pi^3 = \text{id}\} = \{\pi \in \mathbf{S}_4 \mid \pi^3 = \text{id}\} = \{\text{id}, (123), (132), (124), (142), (134), (143), (234), (243)\}$$

není uzavřena na skládání (například  $(123) \circ (124) = (13)(24)$ ), tedy se nejedná o podgrupu v žádné z grup.

**Úloha 9.12.** Ukažte, že platí:

(a)  $\langle 1 \rangle_{\mathbb{Z}} = \mathbb{Z} = \langle 1 \rangle_{\mathbb{Q}}$

(b)  $\langle (1, 0), (0, 1) \rangle_{\mathbb{Z} \times \mathbb{Z}} = \mathbb{Z} \times \mathbb{Z}$

(c)  $\langle a, b \rangle_{\mathbb{Z}} = \langle \text{NSD}(a, b) \rangle = \text{NSD}(a, b)\mathbb{Z}$

(d)  $\mathbf{A}_n = \langle (1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n) \rangle$ . (Nápověda: Nejprve dokažte, že  $\mathbf{A}_n$  je generována všemi trojcykly.)

**Řešení.** (a), (b) dostaneme přímo z definice podgrupy generované množinou prvků.

(c) Stačí si uvědomit, že podgrupy grupy  $\mathbb{Z}$  jsou právě ideály oboru  $\mathbb{Z}$ , o nichž už jsme odpovídající tvrzení dokázali.

(d) Každý prvek alternující grupy  $A_n$  je sudou permutací, tedy jej lze zapsat jako součin sudého počtu transpozic. Proto stačí dokázat, že každý součin dvou transpozic lze vyjádřit jako součin trojcyklů. Uvažujme libovolný součin dvou transpozic  $(ab)(cd)$ . Máme následující možnosti:

- Pokud jsou množiny  $\{a, b\}$  a  $\{c, d\}$  totožné, pak  $(ab)(ab) = \text{id}$ , což nevyžaduje další rozklad.
- Pokud množiny mají právě jeden společný prvek, např.  $b = c$ , pak máme  $(ab)(bd) = (abd)$ . Tato permutace je již trojcyklem.
- Pokud jsou množiny disjunktní, platí  $(ab)(cd) = (ab)(bc) \circ (bc)(cd) = (abc) \circ (bcd)$ .

Tím je dokázáno, že každá sudá permutace se rozkládá na trojcykly, a proto jsou trojcykly generátory  $A_n$ .

Nyní ukážeme, že alternující grupa  $A_n$  je generována konkrétně trojcykly tvaru

$$(1\ 2\ 3), (1\ 2\ 4), \dots, (1\ 2\ n).$$

Z předchozího již víme, že  $A_n$  generují všechny trojcykly. Proto postačí ukázat, že libovolný trojcyklus lze vyjádřit pomocí trojcyklů tvaru  $(1\ 2\ k)$ . Konjugováním obdržíme

$$(1\ 2\ \ell) \circ (1\ 2\ k) \circ (1\ 2\ \ell)^{-1} = (2\ k\ \ell)$$

a obdobně získáme i trojcyklus obsahující jedničku a kterékoliv dva další prvky. Uvažme konečně trojcyklus  $(abc)$ , kde ani jeden z prvků není 1 ani 2; ten obdržíme následovně:

$$(abc) = (1\ 2\ a) \circ (2\ b\ c) \circ (1\ 2\ a)^{-1}.$$

Tím je dokázáno, že alternující grupa  $A_n$  je generována právě trojcykly tvaru  $(1\ 2\ 3), \dots, (1\ 2\ n)$ .

**Úloha 9.13.** Dokažte, že  $D_{2n} = \langle \rho, \sigma \rangle$ , kde  $\rho$  je rotace o úhel  $2\pi/n$  a  $\sigma$  je libovolná reflexe.

**Řešení.** Jistě platí, že podgrupa  $\langle \rho, \sigma \rangle$  obsahuje podgrupu všech rotací  $R = \{\rho^j \mid j \in \mathbb{Z}_n\}$ . Ta už je indexu  $[D_{2n} : R] = \frac{2n}{n} = 2$ , a protože  $\sigma \in D_{2n} \setminus R$ , plyne z Lagrangeovy věty, že  $2 > [D_{2n} : \langle \rho, \sigma \rangle] = 1$ , tedy  $D_{2n} = \langle \rho, \sigma \rangle$ .

★ **Úloha 9.14.** Jaký největší řád prvku nalezneme v grupě všech symetrií krychle, pokud uvažujeme (a) jen přímé symetrie (rotace), (b) všechny symetrie?

**Řešení.** (a) Není těžké nahlédnout, že nejvyšší řád má rotace o  $90^\circ$  podle osy procházející protějšími stěnami, kterýžto prvek má řád 4.

(b) Úloha je snadná ve chvíli, kdy víme, že grupa všech symetrií krychle je isomorfní součinu  $S_4 \times \mathbb{Z}_2$ ; jelikož v  $S_4$  jsou prvky řádů 1, 2, 3 a 4, největšího řádu v součinu dostaneme volbou prvku řádu 3 v  $S_4$  a (jediného) prvku řádu 2 v  $\mathbb{Z}_2$ , jde tedy např. o dvojici  $((1\ 2\ 3), 1)$ . Geometricky jde o rotaci o  $60^\circ$  podle tělesové úhlopříčky následovanou středovou symetrií.