8 Řád a neřád v teorii grup

Řešení
Cvičení 10. a 11. dubna, verze ze dne 10. dubna 2024.

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 8.1. 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 $\mathbf{A}_{2020}$?

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

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

(b) Protože $|\mathbb{Z}_{20}^*| = \varphi(20) = 8$, jsou možné řády 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 $\operatorname{ord}(7) = 4$ a že $\operatorname{ord}(9) = 2$.

(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 $c_i^m = \mathrm{id}$, právě když je m násobkem délky cyklu c_i, proto je řád permutace roven právě nejmenšímu společnému násobku délek všech nezávislých cyklů, tedy

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

což v platí v obou grupách $\mathbf{S}_9$ a $\mathbf{A}_{2020}$.

Úloha 8.2. 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 π, tedy podgrupa $\langle\pi\rangle = \{\pi^i \mid i \in \mathbb{Z}_5\} = \{\mathrm{id}, (1\,2\,3\,4\,5), (1\,3\,5\,2\,4), (1\,4\,2\,5\,3), (1\,5\,4\,3\,2)\}$. Z Lagrangeovy věty dostáváme, že index $[\mathbf{S}_5 : \langle\pi\rangle] = \frac{|\mathbf{S}_5|}{|\langle\pi\rangle|} = \frac{5!}{5} = 24$.

Úloha 8.3. 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 $H = \{\mathrm{id}, (12), (23)\}$,

(d) $G = \mathbf{S}_3$ a $H = \{\mathrm{id}, (12)\}$.

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 $\mathbf{S}_3$.

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

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

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

Úloha 8.4. Rozhodněte, která z následujících zobrazení jsou homomorfismy grup. U homomorfismů popište jejich jádra a obrazy.

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

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

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

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

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

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

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

(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 $f(k + l) = (k + l) \mod 5 = f(k) + f(l)$, je zobrazení f homomorfismus a z definice spočítáme, že $\mathrm{Im}\, f = \mathbb{Z}_3$ a $\ker f = 3\mathbb{Z}_{15} = \{0, 3, 6, 9, 12\}$.

(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 8.5. Rozhodněte,

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

(b) zda existují v grupě $\mathbf{S}_{17}$ 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 $72 = \mathrm{nsn}(8, 9)$, stačí nám najít permutaci sestávající s jednoho cyklu délky 8 a jednoho cyklu délky 9, jíž 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 $\mathrm{nsn}(n_i \mid i \leq k) = 80$ 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 8.6. 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 8.7. Jaký řád mají následující prvky v daných grupách?

(a) rotace o 144° v 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 $GL_3(\mathbb{C})$

(c) dvojice $\big((1\,2\,3)(4\,5), (1\,2\,3\,4)\big)$ v direktním součinu grup $\mathbf{S}_5 \times \mathbf{S}_4$.

Řešení. (a) Ptáme se, kolik nejméně složení rotací o 144° nám dá rotaci, která je násobkem úhlu 360°, a snadno spočítáme, že jich potřebujeme pět, tedy má tato rotace v 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° kolem osy x složená se středovou symetrií, pak vidíme, že

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

Dále máme $\begin{pmatrix}1&1&0\\0&1&1\\0&0&2\end{pmatrix}^k = \begin{pmatrix}1&1&0\\0&1&1\\0&0&2^k\end{pmatrix} \neq I_3$ pro všechna kladná k, což znamená, že se jedná o prvek nekonečného řádu a 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 $\big((1\,2\,3)(4\,5),(1\,2\,3\,4)\big)^k = \big((1\,2\,3)^k(4\,5)^k,(1\,2\,3\,4)^k\big)$, vidíme, že řád prvku $\big((1\,2\,3)(4\,5),(1\,2\,3\,4)\big)$ je roven právě nejmenšímu společnému násobku řádů prvků obou složek, tedy

$$\operatorname{ord}\big((1\,2\,3)(4\,5),(1\,2\,3\,4)\big) = \operatorname{nsn}(\operatorname{ord}(1\,2\,3)(4\,5)),\operatorname{ord}(1\,2\,3\,4)) = \operatorname{nsn}(6,4) = 12.$$

Úloha 8.8. 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 $(\mathbf{S}_n,\circ,^{-1},\mathrm{id})$,

(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 tavru $f_k(x) = x$ 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 $\mathbb{Z}_n \to \mathbb{Z}$ 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 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 $f_\sigma(0) = \mathrm{id}$ a $f_\sigma(1) = \sigma$ pro libovolnou permutaci složenou z nezávislých transpozic $\sigma \in \mathbf{S}_n$, $\ker f_\sigma = \{0\}, \operatorname{Im} f_\sigma = \langle\sigma\rangle = \{\mathrm{id},\sigma\}$ 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 $\mathbb{Z}_3 \to \mathbb{Z}_5$ 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 $a \mapsto 2^{ka}$ (mod 11) pro $k \in \{0, 5\}$, tedy máme zde jediný netriviální homomorfismus$a \mapsto 2^{5a} \pmod{11}$.

Úloha 8.9. 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 by bylo prvočíslo, které nedělí b, pak pak by $\frac{1}{p} \notin \langle \frac{a}{b} \rangle$, tedy $\frac{a}{b}$ nemůže být generátor celého $\mathbb{Q}$. Podobně, uvážíme-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 8.10. 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 je uzavřená na sčítaní, 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 8.11. Rozhodněte, zda (a) $\{\pi \in A_4 : \pi^2 = \mathrm{id}\}$, (b) $\{\pi \in A_4 : \pi^3 = \mathrm{id}\}$ tvoří podgrupu grupy $\mathbf{A}_4$. Vyřešte analogickou úlohu pro grupu $\mathbf{S}_4$.

Řešení. (a) Snadno nahlédneme, že je množina

$$\{\pi \in A_4 : \pi^2 = \mathrm{id}\} = \{\mathrm{id}, (12)(34), (13)(24), (14)(24)\}$$

uzavřená na skládání, protože je zde každý prvek sám k sobě inverzní a leží zde neutrální prvek, proto se jedná o podgrupu A_4. Naopak množina

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

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

(b) Tentokrát okamžitě vidíme, že množina

$$\{\pi \in A_4 : \pi^3 = \mathrm{id}\} = \{\pi \in \mathbf{S}_4 : \pi^3 = \mathrm{id}\} = \{\mathrm{id}, (123), (132), (124), (142), (134), (143), (234), (243)\}$$

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

Úloha 8.12. 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) $\langle a, b \rangle_{\mathbb{Z}} = \langle \mathrm{NSD}(a,b) \rangle = \mathrm{NSD}(a,b)\mathbb{Z}$

(d) $\mathbf{S}_n = \langle (1\ 2), (1\ 3), \ldots, (1\ n) \rangle$

(e) $\mathbf{A}_n = \langle (1\ 2\ 3), (1\ 2\ 4), \ldots, (1\ 2\ n) \rangle$.

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) Nejprve si vzpomeneme, že každou permutaci dostaneme složením transpozic, což dokážeme například z rozepsání permutace na cyklický zápis a vyjádření cyklu pomocí transpozic. Poté si rozmyslíme, že libovolnou transpozici (ab) pro $a > b > 1$ dostaneme konjugací $(ab) = (1a)(1b)(1a)^{-1}$.

(e) Dokážeme podobnou úvahou jako u (d).

Úloha 8.13. Dokažte, že $D_{2n} = \langle \rho, \sigma \rangle$, kde ρ je rotace o úhel $2\pi/n$ a σ je libovolná reflexe.

Řešení. Jistě platí, že podgrupa $\langle \rho, \sigma \rangle$ obsahuje podgrupu všech rotaci $R = \{\rho^j \mid j \in \mathbb{Z}_n\}$. 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 $D_{2n} = \langle \rho, \sigma \rangle$.