CVIČENÍ Z ÚVODU DO TEORIE GRUP

7.10.

1. Příklady grup

1.1. Cyklické grupy.

1.1. Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je cyklická grupa řádu 20 s generátorem g.

(a) Popište všechny podgrupy grupy $\mathcal{G}$,
(b) určete řády všech prvků grupy $\mathcal{G}$.

(a) Grupa $\mathcal{G}$ je izomorfní aditivní grupě $(\mathbb{Z}_{20}, +, -, 0)$. Pro každý dělitel k jejího řádu existuje právě jedna podgrupa řádu k, všechny podgrupy jsou přitom cyklické. Proto $\mathcal{G}$ obsahuje právě 6 podgrup: $\{1\}$ je řádu 1, $\langle g^{10}\rangle$ je řádu 2, $\langle g^5\rangle$ je řádu 4, $\langle g^4\rangle$ je řádu 5, $\langle g^2\rangle$ je řádu 10 a G je řádu 20.

(b) Pro každý dělitel k řádu $\mathcal{G}$ existuje právě $\varphi(k)$ generátorů podgrupy řádu k, tedy prvků řádu k, kde φ označuje Eulerovu funkci. Proto je množina

$$\{g^r \mid \mathrm{NSD}(r, 20) = \frac{20}{k}\}$$

tvořena právě všemi prvky řádu k a $\mathcal{G}$, tedy máme právě 1 prvek řádu 1, 1 prvek řádu 2, 2 prvky řádu 4, 4 prvky řádu 5, 4 prvky řádu 10 a 8 prvků řádu 20. □

1.2. Najděte generátory cyklických podgrup $\langle 60\rangle \cap \langle 18\rangle$ a $\langle 60, 18\rangle$

(a) grupy $(\mathbb{Z}, +, -, 0)$,
(b) grupy $(\mathbb{Z}_{90}, +, -, 0)$.

(a) Stačí určit největší společný dělitel a nejmenší společný násobek čísel 60 a 18:

$$\langle 60\rangle \cap \langle 18\rangle = \langle \mathrm{nsn}(60, 18)\rangle = \langle 180\rangle, \quad \langle 60, 18\rangle = \langle \mathrm{NSD}(60, 18)\rangle = \langle 6\rangle$$

(b) V grupě $(\mathbb{Z}_{90}, +, -, 0)$ snadno spočítáme generátor podgrupy dělící řád grupy:

$$\langle 60\rangle = \langle \mathrm{NSD}(60, 90)\rangle = \langle 30\rangle \text{ a } \langle 18\rangle = \langle \mathrm{NSD}(18, 90)\rangle = \langle 9\rangle,$$

proto podobně jako v úloze (a) dostáváme

$$\langle 60\rangle \cap \langle 18\rangle = \langle 30\rangle \cap \langle 9\rangle = \langle \mathrm{nsn}(30, 9)\rangle = \langle 0\rangle,\ \langle 60, 18\rangle = \langle 30, 9\rangle = \langle \mathrm{NSD}(30, 9)\rangle = \langle 3\rangle.$$

□

1.3. Spočítejte množiny

(a) $\mathrm{End}(\mathbb{Z})$, $\mathrm{Aut}(\mathbb{Z})$, $\mathrm{Inn}(\mathbb{Z})$,
(b) $\mathrm{End}(\mathbb{Z}_n)$, $\mathrm{Aut}(\mathbb{Z}_n)$, $\mathrm{Inn}(\mathbb{Z}_n)$.

Date: 9. ledna 2020.

(a) Označme pro každé $k \in \mathbb{Z}$ zobrazení $\rho_k : \mathbb{Z} \to \mathbb{Z}$ dané předpisem $\rho_k(z) = kz$. Protože pro každou dvojici celých čísel z a u platí, že

$$\rho_k(z+u) = k(z+u) = kz + ku = \rho_k(z) + \rho_k(u),$$

je ρ_k endomorfismus. Zvolíme-li $\rho \in \mathrm{End}(\mathbb{Z})$ a položíme-li $k := \rho(1)$, pak vidíme, že $\rho = \rho_k$, neboť 1 generuje cyklickou grupu $\mathbb{Z}$. Tím jsme dokázali, že $\mathrm{End}(\mathbb{Z}) = \{\rho_k \mid k \in \mathbb{Z}\}$. Protože ρ_k je bijekce právě když $k = \pm 1$, máme $\mathrm{Aut}(\mathbb{Z}) = \{\mathrm{id}, -\mathrm{id}\}$. Konečně $\mathrm{Inn}(\mathbb{Z}) = \{\mathrm{id}\}$, protože grupa $\mathbb{Z}$ je komutativní.

(b) Podobně jako v (a) označíme zobrazení $\rho_k : \mathbb{Z}_n \to \mathbb{Z}_n$ splňující $\rho_k(z) = (kz) \mathrm{mod} n$ pro každé $k \in \mathbb{Z}_n$. Stejným způsobem nyní nahlédneme, že

$$\mathrm{End}(\mathbb{Z}_n) = \{\rho_k \mid k \in \mathbb{Z}_n\} \quad \text{a} \quad \mathrm{Inn}(\mathbb{Z}_n) = \{\mathrm{id}\}.$$

Protože je $\mathbb{Z}_n$ konečná grupa, ρ_k je izomorfismus, právě když je to zobrazení na a to nastává, právě když je k nesoudělné s n. Tudíž

$$\mathrm{Aut}(\mathbb{Z}_n) = \{\rho_k \mid k \in \mathbb{Z}_n, \mathrm{NSD}(k,n) = 1\} \cong \mathbb{Z}_n^*.$$

□

1.4. Popište všechny charakteristické a úplně charakteristické podgrupy grup $\mathbb{Z}$ a $\mathbb{Z}_n$ pro $n \in \mathbb{N}$.

Protože každý endomorfní obraz lze v $\mathbb{Z}$ i $\mathbb{Z}_n$ realizovat jako iterované sčítání prvku, je každá podgrupa $\mathbb{Z}$ i $\mathbb{Z}_n$ úplně charakteristickou a tudíž i charakteristickou podgrupou. □

1.2. **Konečné abelovské grupy.**

1.5. Popište všechny podgrupy a všechny řády prvků grupy

(a) $\mathbb{Z}_5 \times \mathbb{Z}_5$,
(b) $\mathbb{Z}_5 \times \mathbb{Z}_6$.

(a) Grupa $\mathbb{Z}_5 \times \mathbb{Z}_5$ má strukturu vektorového prostoru nad tělesem $\mathbb{Z}_5$. Protože lze násobení skalárem realizovat pomocí opakovaného sčítání, je i každá její podgrupa podprostorem. Tedy $\mathbb{Z}_5 \times \mathbb{Z}_5$ obsahuje právě 6 cyklických podgrup řádu 5 (tedy přímek chápeme-li grupu jako vektorový prostor) a triviální grupy $\{(0,0)\}$ a $\mathbb{Z}_5 \times \mathbb{Z}_5$.

(b) Podle Čínské věty o zbytcích je $\mathbb{Z}_5 \times \mathbb{Z}_6 \cong \mathbb{Z}_{30}$ cyklická grupa s generátorem $(1,1)$ a tudíž $\mathbb{Z}_5 \times \mathbb{Z}_6$ obsahuje 8 podgrup: $\langle(0,0)\rangle$ řádu 1, $\langle(0,3)\rangle$ řádu 2, $\langle(0,2)\rangle$ řádu 3, $\langle(1,0)\rangle$ řádu 5, $\langle(0,1)\rangle$ řádu 6, $\langle(1,3)\rangle$ řádu 10, $\langle(1,2)\rangle$ řádu 15 a $\langle(1,1)\rangle$ řádu 30. Pro každý dělitel k čísla 30 máme v $\mathbb{Z}_5 \times \mathbb{Z}_6$ právě $\varphi(k)$ prvků řádu k. □

1.6. Popište $\mathrm{End}(\mathbb{Z}_5^2)$, $\mathrm{Aut}(\mathbb{Z}_5^2)$, $\mathrm{Inn}(\mathbb{Z}_5^2)$ a najděte všechny charakteristické a úplně charakteristické podgrupy grupy $\mathbb{Z}_5^2$.

Protože lze násobení skalárem realizovat pomocí opakovaného sčítání, je každý prvek $\mathrm{End}(\mathbb{Z}_5^2)$ právě endomorfismus vektorového prostoru $\mathbb{Z}_5^2$ nad tělesem $\mathbb{Z}_5$. Označíme-li pro každou matici $M \in M_2(\mathbb{Z}_5)$ lineární operátor F_M daný násobením $F_M(v) = vM$, pak z lineární algebry víme, že

$$\mathrm{End}(\mathbb{Z}_5^2) = \{F_M \mid M \in M_2(\mathbb{Z}_5)\}, \quad \mathrm{Aut}(\mathbb{Z}_5^2) = \{F_M \mid M \in GL_2(\mathbb{Z}_5)\},$$

kde $GL_2(\mathbb{Z}_5)$ značí množinu všech regulárních matic 2×2 nad tělesem $\mathbb{Z}_5$. Protože je grupa $\mathbb{Z}_5^2$ komutativní je $\mathrm{Inn}(\mathbb{Z}_5^2) = \{\mathrm{id}\}$.

Triviální podgrupy $\{(0,0)\}$ a $\mathbb{Z}_5^2$ jsou jistě charakteristické a úplně charakteristické podgrupy. Uvážíme-li nenulový vektor u nějaké charakteristické podgrupy A

a vektor v, který je na něm lineárně nezávislý, pak určitě existuje lineární operátor F, který tyto vektory zamění. Protože (u, v) tvoří bázi $\mathbb{Z}_5^2$, jde o automorfismus, tedy A obsahuje bázi (u, v), proto $A = \mathbb{Z}_5^2$. Dokázali jsme, že $\mathbb{Z}_5^2$ jiné než triviální charakteristické a tudíž i úplně charakteristické podgrupy neobsahuje. □

14.10.

1.7. Popište $\mathrm{End}(\mathbb{Z}^2)$, $\mathrm{Aut}(\mathbb{Z}^2)$ a najděte všechny charakteristické a úplně charakteristické podgrupy grupy $\mathbb{Z}^2$.

Obdobně jako v úloze 1.6 s využitím lineární algebry nahlédneme, že endomorfismy grupy $\mathbb{Z}^2$ lze chápat jako restrikci $\mathbb{Q}$-lineárních operátorů vektorového prostoru $\mathbb{Q}^2$ zobrazujících kanonickou bázi do podmnožiny $\mathbb{Z}^2$, neboť každý endomorfismus $\mathbb{Z}^2$ je určen obrazy generující množiny (jíž je například kanonická báze). Takové lineární operátory mají právě celočíselnou matici vzhledem ke kanonické bázi. Označíme-li tedy opět pro matici $M \in M_2(\mathbb{Z})$ lineární operátor F_M daný násobením $F_M(v) = vM$, pak $\mathrm{End}(\mathbb{Z}^2) = \{F_M \mid M \in M_2(\mathbb{Z})\}$. Endomorfismus F_M je bijektivní, právě když je exsituje inverzní matice k matici M, která je celočíselná, což nastává právě tehdy když $\det M = \pm 1$, neboť z lineární algebry víme, že $M^{-1} = \frac{1}{\det M}\mathrm{adj}M$. To znamená, že $\mathrm{Aut}(\mathbb{Z}^2) = \{F_M \mid M \in M_2(\mathbb{Z}), \det M = \pm 1\}$.

Nejprve označme $c\mathbb{Z}^2 = \{cv \mid v \in \mathbb{Z}^2\}$ pro každé nezáporné celé c. Zřejmě se jedná o podgrupu generovanou prvky $(c, 0)$ a $(0, c)$, navíc $F_M(cv) = c(vM) \in c\mathbb{Z}^2$ pro každé $v \in \mathbb{Z}^2$ a $M \in M_2(\mathbb{Z})$, tedy je tato podgrupa úplně charakteristická (a tedy i charakteristická). Ukážeme, že jiné úplně charakteristické ani charakteristické podgrupy grupy $\mathbb{Z}^2$ neexistují.

Předpokládejme, že A je nenulová charakteristická podgrupy grupy $\mathbb{Z}^2$. Nechť $(a, b) \in A$. Potom

$$(b, a) = (a, b)\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \in A, \quad (a + b, b) = (a, b)\begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \in A,$$

a proto $(b, 0) = (a+b, b)-(a, b) \in A$. Stejný argument pro (b, a) nám dává $(a, 0) \in A$.

Položme nyní $c := \min(\{a > 0 \mid (a, 0) \in A\})$. Protože A obsahuje nenulový prvek, obsahuje podle předchozí úvahy i nějaký nenulvý prvek tvaru $(a, 0)$ a sním i prvek $(-a, 0)$. Tudíž c je dobře definované přirozené číslo. Protože $(c, 0), (0, c) \in \mathbb{Z}^2$, vidíme, že $c\mathbb{Z}^2 \subseteq A$. Protože s každým prvkem (a, b) obsahuje grupa i prvky $(a, 0)$ a $(b, 0)$, stačí nám ověřit pro prvek tvaru $(a, 0) \in A$, že $(a, 0) \in c\mathbb{Z}^2$, tedy že je prvek a celočíselným násobkem prvku c. K tomu můžeme využít obdobný argument jako v důkazu tvrzení, že jsou podrupy grupy celých čísel cyklické, tedy a vydělit se zbytkem číslem c. Je-li $q \in \mathbb{Z}$ a $r \in \mathbb{Z}_c$ čísla splňující rovnost $a = qc + r$, pak $(r, 0) = a - q(c, 0) \in A$ a z minimality volby c plyne, že $r = 0$. To znamená, že $A = c\mathbb{Z}^2$.

Dokázali jsme, že jiné charakteristická podgrupy grupy $\mathbb{Z}^2$ než tvaru $c\mathbb{Z}^2$ neexistují, tedy neexistují ani jiné úplně charakteristické podgrupy. □

1.3. **Permutační grupy.**

1.8. Určete centrum grupy S_3, dokažte, že $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3) \cong S_3$ a popište množinu $\mathrm{End}(S_3)$. Jak vypadají charakteristické a úplně charakteristické podgrupy grupy S_3?

Protože pro každou transpozici $(ab) \in S_3$ a trojcyklus $(abc) \in S_3$ platí, že $(abc)(ab) = (ab)(acb) \neq (ab)(abc)$, nemůže centrum obsahovat žádnou transpozici ani trojcyklus, a proto $Z(S_3) = \{\mathrm{id}\}$.

Využijeme-li homomorfismus $\tau : S_3 \to \mathrm{Inn}(S_3)$ na celé $\mathrm{Inn}(S_3)$ daný vztahem $\tau(g) = \psi_g$, kde ψ_g je vnitřní automorfismus příslušný prvku g, pak nám první věta o izomorfismu říká, že

$$S_3 \cong S_3/Z(S_3) \cong \mathrm{Inn}(S_3).$$

Je-li $\alpha \in \mathrm{Aut}(S_3)$ automorfismus, pak je jednoznačně určen obrazy generátorů, tedy například obrazy transpozic (12) a (23). Navíc obrazy $\alpha((12))$ a $\alpha((23))$ musí být rovněž řádu dva, tedy se jedná o dvě různé transpozice. Protože v S_3 existuje jen 6 uspořádaných dvojic různých transpozic, $\mathrm{Inn}(S_3) \leq \mathrm{Aut}(S_3)$ a $\mathrm{Inn}(S_3)$ je rovněž řádu 6, dostáváme rovnost $\mathrm{Aut}(S_3) = \mathrm{Inn}(S_3)$.

Nechť $\alpha \in \mathrm{End}(S_3) \setminus \mathrm{Aut}(S_3)$. Protože jádro homomorfismu je normální podgrupa, je $\mathrm{Ker}\alpha$ rovno S_3 nebo A_3. V prvním případě jde o triviální endomorfismus $\omega : S_3 \to \{\mathrm{id}\}$, který všechny prvky zobrazí na neutrální prvek. Pokud $\mathrm{Ker}\alpha = A_3$, pak je obraz $\alpha(S_3)$ dvouprvkový. Pro každou transpozici t, proto připadá v úvahu jediný homomorfismus α_t daný vztahy $\alpha_t(A_3) = \mathrm{id}$ a $\alpha_t((12)A_3) = t$.

Zjistili jsme, že $\mathrm{End}(S_3) = \mathrm{Aut}(S_3) \cup \{\omega, \alpha_{(12)}, \alpha_{(23)}, \alpha_{(13)}\}$. □

1.9. Spočítejte centrum grupy $A_4 \times \mathbb{Z}_2$ a dokažte, že centrum není úplně invariantní podgrupa.

Grupa A_4 obsahuje právě tři normální podgrupy: dvě triviální $\{\mathrm{id}\}$, A_4 a Kleinovu $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. Centrum je jistě normální podgrupa a protože například $(123) \circ (12)(34) \neq (12)(34) \circ (123)$ dostáváme, že $K \neq Z(A_4) \neq A_4$. Tedy $Z(A_4) = \{\mathrm{id}\}$, a proto

$$Z(A_4 \times \mathbb{Z}_2) = \mathrm{id} \times \mathbb{Z}_2 = \{(\mathrm{id}, 0), (\mathrm{id}, 1)\}.$$

Uvážíme-li endomorfismus $\epsilon \in \mathrm{End}(A_4 \times \mathbb{Z}_2)$ daný vztahy $\epsilon(A_4 \times 0) = \{(\mathrm{id}, 0)\}$ a $\epsilon(A_4 \times 1) = \{((12)(34), 0)\}$, potom vidíme, že $\epsilon((\mathrm{id}, 1)) = ((12)(34), 0) \notin Z(A_4 \times \mathbb{Z}_2)$, tedy centrum není úplně invariantní podgrupa. □

21.10.

1.10. Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je konečná grupa řádu n. Dokažte, že

(a) zobrazení $\psi : G \to S(G)$ dané vztahem $\psi(g) = L_g$, kde $L_g(h) = gh$, je prostý grupový homomorfismus;
(b) grupy $S(G)$ a S_n jsou izomorfní;
(c) grupa $\mathcal{G}$ je izomorfní nějaké podgrupě S_n.

(a) Stačí pro každé $g, h, a \in G$ spočítat

$$\psi(gh)(a) = L_{gh}(a) = (gh)a = g(ha) = L_g L_h(a) = \psi(g)\psi(h)(a)$$

a všimnout si, že $L_g = \mathrm{id}$, právě když $g = 1$.

(b) Označme $\alpha : \{1, 2, \ldots, n\} \to G$ libovolnou bijekci, která existuje, protože jsou množiny stejně velké. Definujme zobrazení $\tau : S_n \to S(G)$ vztahem $\tau(\sigma) = \alpha \circ \sigma \circ \alpha^{-1}$. Snadno ověříme, že jde o grupový homomorfismus:

$$\tau(\sigma) \circ \tau(\rho) = \alpha \circ \sigma \circ \alpha^{-1} \circ \alpha \circ \rho \circ \alpha^{-1} = \alpha \circ \sigma \circ \rho \circ \alpha^{-1} = \tau(\sigma \circ \rho).$$

Homomorfismus τ je izomorfismus, protože je zobrazení $\tau\alpha^{-1}(b = \alpha^{-1} \circ b \circ \alpha$ inverzní homomorfismus k τ.

(c) Složený prostý homomorfismus $\tau\psi$ je zobrazením na $\tau\psi(G)$, tudíž se jedná o izomorfismus grup G a $\tau\psi(G)$, kde $\tau\psi(G)$ tvoří podgrupu S_n. □

Jsou-li $\pi, \sigma \in S_n$ dvě permutace budeme konjugaci permutace π permutací σ značit $\pi^\sigma = \sigma\pi\sigma^{-1}$. Připomeňme, že pokud $\pi(a) = b$, pak $\pi^\sigma(\sigma(a)) = \sigma(b)$, tedy například

$$(123)(4567)(89)^\sigma = (\sigma(1)\sigma(2)\sigma(3))(\sigma(4)\sigma(5)\sigma(6)\sigma(7))(\sigma(8)\sigma(9))$$

1.11. Nechť $\pi, \sigma \in S_n$.

(a) Dokažte, že $\pi\sigma = \sigma\pi$, právě když $\pi^\sigma = \pi$,
(b) spočítejte π^σ pro $\pi = (134)(58)(279)$ a $\sigma = (17)(24)(39)(58)$ a rozhodněte, zda $\pi\sigma = \sigma\pi$.

(a) $\pi\sigma = \sigma\pi$, právě když $\pi\sigma\sigma^{-1} = \sigma\pi\sigma^{-1}$, právě když $\pi = \pi^\sigma$.
(b) $\pi^\sigma = (134)(58)(279)^{(17)(24)(39)(58)} = (792)(85)(413) = (134)(58)(279)$, proto prvky π a σ komutují. □

1.12. Dokažte, že

(a) $S_n = \langle\{(ij) \mid i < j, i, j \in \{1, \dots, n\}\}\rangle$,
(b) $S_n = \langle(12), (23), \dots (n-1\ n)\rangle$,
(c) $S_n = \langle(12), (12\dots n)\rangle$,

(a) Každou permutaci dostaneme jakou součin nezávislých cyklů, proto stačí vyjádřit jeden cyklus:

$$(a_1 a_2 \dots a_k) = (a_1 a_2)(a_2 a_3) \dots (a_{k-1} a_k),$$

tudíž $S_n = \langle\{(ij) \mid i < j, i, j \in \{1, \dots, n\}\}\rangle$.
(b) Díky (a) stačí vyjádřit každou transpozici (ij), $i < j$, pomocí transpozic tvaru $(aa+1)$, k tomu využijeme konjugování:

$$(ij) = (i+1\ i+2 \dots j)(i\ i+1)(i+1\ i+2 \dots j)^{-1} =$$

$$= (i+1\ i+2) \dots (j-1\ j)(i\ i+1)(j-1\ j) \dots (i+1\ i+2).$$

(c) Díky (b) stačí pomocí (12) a $(12\dots n)$ vyjádřit všehny transpozice tvaru $(i\ i+1)$:

$$(i\ i+1) = (12\dots n)^{i-1}(12)(12\dots n)^{-i+1} =$$

□

1.13. Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa a $X \subseteq G$ množina jejích generátorů, tj. $G = \langle X\rangle$ Dokažte, že $Z(G) = \{g \in G \mid gx = xg\ \forall g \in X\}$.

Označme $H := \{g \in G \mid gx = xg\ \forall g \in X\}$. Snadno nahlédneme, že $Z(G) \subseteq H$. Uvědomme si, že H je podgrupa $\mathcal{G}$: zřejmě $1 \in H$ a je-li $a, b \in H$, pak

$$abx = axb = xab, \quad xa^{-1} = a^{-1}axa^{-1} = a^{-1}xaa^{-1} = a^{-1}x.$$

Podobně i $K := \{g \in G \mid gh = hg\ \forall h \in H\}$ je podgrupa $\mathcal{G}$. Navíc $X \subseteq K$, a proto $K = G$. To ovšem znamená, že všechny prvky H komutují se všemi prvky G, tudíž $H \subseteq Z(G)$. □

Označme D_{2n} grupu všech symetrií pravidelného n-úhleníku.

1.14. Dokažte, že je grupa D_8 izomorfní podgrupě S_4 generované rotací (1234) a osovou symetrií (13), spočítejte $Z(D_8)$ a $\mathrm{Inn}(D_8)$.

Označme vrcholy čtverce po směru hodinových ručiček $1, 2, 3, 4$. Každá symetrie čtverce vytváří permutaci jeho vrcholů, což nám určuje prostý homomorfismus $F : D_8 \to S_4$. D_8 a tedy i $F(D_8)$ má osm prvků, a $\langle(1234)\rangle$ je čtyřprvková podgrupa $F(D_8)$. Protože $(13) \in F(D_8) \setminus \langle(1234)\rangle$, musí být podle Lagrangeovy věty $\langle(1234),(13)\rangle$ aspoň osmiprvková, proto $\langle(1234),(13)\rangle = F(D_8)$.

Nadále ztotožníme $F(D_8)$ a $\langle(1234),(13)\rangle$ a budeme psát $D_8 = \langle(1234),(13)\rangle$. Díky 1.13 stačí najít prvky D_8 komutující s generátory $(1234), (13)$, rychle spočítáme, že $Z(D_8) = \{\mathrm{id}, (13)(24)\}$.

Díky 1. Větě o izomorfismu a tvrzení z přednášky víme, že $\mathrm{Inn}(D_8) \cong D_8/Z(D_8)$, tedy $\mathrm{Inn}(D_8)$ je grupa řádu 4. Protože (1234) a $(4321) = (1234)^{-1}$ jsou jediné dva prvky řádu většího než 2 v D_8 stačí spočítat

$$((1234)Z(D_8))^2 = (1234)^2 Z(D_8) = (13)(24)Z(D_8) = \mathrm{id}Z(D_8), tedy$$

prvky $(1234)Z(D_8)$ a $(4321)Z(D_8)$ jsou v $D_8/Z(D_8)$ řádu 2 a tato grupa neobsahuje prvek řádu 4, tedy není cyklická. Proto $\mathrm{Inn}(D_8) \cong D_8/Z(D_8) \cong \mathbb{Z}_2 \times Z_2$. □

4.11.

2. Kompoziční řady

2.1. **Kompoziční řady komutativních grup.**

2.1. Popište všechny jednoduché komutativní grupy.

Protože je každá podgrupa komutativní grupy G normální, platí pro každý prvek $g \in G \setminus \{1\}$, že $\langle g\rangle = G$. Tedy jednoduché komutativní grupy jsou právě cyklické grupy prvočíselného řádu. □

2.2. Určete nějakou kompoziční a nějakou hlavní řadu grupy $\mathbb{Z}_{30}$. Kolik kompoziční řad této grupy existuje?

$\mathbb{Z}_{30}$ je cyklická, tedy komutativní grupa, proto jsou všechny její podgrupy normální a kompoziční a hlavní řady tak splývají. Víme, že pro každý dělitel k čísla 30 je $\langle\frac{30}{k}\rangle$ podgrupa řádu k a pokud $A \leq B \leq \mathbb{Z}_{30}$, pak z Lagrangeovy věty plyne, že $|B/A| = [B : A] = \frac{|B|}{|A|}$. Jednotlivé faktory jsou podle 2.1 cyklické grupy prvočíselného řádu 2, 3 nebo 5, neboť $30 = 2 \cdot 3 \cdot 5$. Odtud plyne, že kompoziční řadu tvoří například posloupnost podgrup

$$\{0\} \trianglelefteq \langle 15\rangle \trianglelefteq \langle 5\rangle \trianglelefteq \mathbb{Z}_{30}.$$

Protože jsme prvočíselné velikosti faktorů mohli libovolně permutovat existuje právě $3! = 6$ různých kompoziční řad grupy $\mathbb{Z}_{30}$. □

2.3. Popište všechny hlavní řady cyklické grupy řádu 72.

Je-li $G = \langle g\rangle$ cyklická grupa řádu $72 = 2^3 \cdot 3^2$, víme, že zobrazení $k \to g^k$ určuje izomorfismus grup G a $\mathbb{Z}_{72}$, můžeme proto postupovat stejně jako v předchozí úloze. Hlavní řadu tvoří například posloupnost podgrup

$$\{1\} \trianglelefteq \langle g^{36}\rangle \trianglelefteq \langle g^{18}\rangle \trianglelefteq \langle g^9\rangle \trianglelefteq \langle g^3\rangle \trianglelefteq G,$$

kde $\langle g^{36}\rangle/\{1\} \cong \langle g^{18}\rangle/\langle g^{36}\rangle \cong \langle g^9\rangle/\langle g^{18}\rangle \cong \mathbb{Z}_2$ a $\langle g^3\rangle/\langle g^9\rangle \cong G/\langle g^3\rangle \cong \mathbb{Z}_3$. I tentokrát můžeme prvočíselné velikosti faktorů libovolně permutovat, tedy pro cyklickou grupy řádu 72 existuje právě $\binom{5}{2} = 10$ různých hlavních řad. □

2.4. Popište všechny kompoziční řady grupy $\mathbb{Z}_5^2$ a ukažte, že jsou kompoziční řady grup $\mathbb{Z}_{25}$ a $\mathbb{Z}_5^2$ izomorfní.

Protože netriviální (normální) podgrupy grupy $\mathbb{Z}_5^2$ jsou právě přímky vektorového prostoru nad tělesem $\mathbb{Z}_5$ (viz 1.6) jsou všechny kompoziční řady $\mathbb{Z}_5^2$ tvaru

$$\{(0,0)\} \trianglelefteq \langle (a,b)\rangle \trianglelefteq \mathbb{Z}_5^2,$$

kde $(a,b) \in \mathbb{Z}_5^2 \setminus \{(0,0)\}$. Protože $25 = 5^2$, stejná úvahou jako v předchozích dvou úlohách zjistíme, že je kompoziční řada grupy $\mathbb{Z}_{25}$ jediná:

$$\{0\} \trianglelefteq \langle 5\rangle \trianglelefteq \mathbb{Z}_{25}.$$

Protože $\langle (a,b)\rangle/\{(0,0)\}\rangle \cong \mathbb{Z}_5^2/\langle (a,b)\rangle \cong \langle 5\rangle/\{0\} \cong \mathbb{Z}_{25}/\langle 5\rangle \cong \mathbb{Z}_5$, jsou kompoziční řady grup $\mathbb{Z}_{25}$ a $\mathbb{Z}_5^2$ izomorfní. □

2.5. Spočítejte $\mathrm{Aut}(\mathbb{Z}_5^2)$-kompoziční řadu grupy $\mathbb{Z}_5^2$ a $\mathrm{Aut}(\mathbb{Z}_{25})$-kompoziční řadu grupy $\mathbb{Z}_{25}$ (t.j. hlavní charakteristické řady).

Protože je podle úvahy úlohy 1.4 každá podgrupa grupy už nutně charakteristická, je $\mathrm{Aut}(\mathbb{Z}_{25})$-kompoziční řada grupy $\mathbb{Z}_{25}$ stejná jako její kompoziční řada. V úloze 1.6 jsme naopak dokázali, že je grupa $\mathbb{Z}_5^2$ $\mathrm{Aut}(\mathbb{Z}_5^2)$-jednoduchá, proto je její $\mathrm{Aut}(\mathbb{Z}_5^2)$-kompoziční řada triviální, tedy tvaru $\{(0,0)\} \trianglelefteq_{\mathrm{Aut}(\mathbb{Z}_5^2)} \mathbb{Z}_5^2$. □

2.6. Dokažte pomocí Jordan-Hölderovy věty základní větu aritmetiky.

Nechť $N = \prod_{i=1}^n p_i = \prod_{i=1}^m q_i$ jsou dva prvočíselné rozklady přirozeného čísla N. Definujme podgrupy $H_j := \langle \prod_{i=j+1}^n p_i\rangle$ a $K_j := \langle \prod_{i=j+1}^m q_i\rangle$ aditivní grupy $\mathbb{Z}_N$. Potom $H_0 = K_0 = \{0\}$, $H_n = K_m = \mathbb{Z}_N$ a $H_j/H_{j-1} \cong \mathbb{Z}_{p_j}$ pro $j = 1 \dots n$ a $K_j/K_{j-1} \cong \mathbb{Z}_{q_j}$ pro $j = 1 \dots m$. To znamená, že $\{H_i\}_{i=0}^n$ a $\{K_i\}_{i=0}^m$ jsou dvě kompoziční řady grupy $\mathbb{Z}_N$. Podle Jordan-Hölderovy věty jsou obě řady izomorfní, tedy $n = m$ a existuje permutace $\sigma \in S_n$ splňující pro každé $j = 1, \dots, n$

$$\mathbb{Z}_{p_j} \cong H_j/H_{j-1} \cong K_{\sigma(j)}/K_{\sigma(j)-1} \cong \mathbb{Z}_{q_{\sigma(j)}},$$

tudíž $p_j = q_\sigma(j)$. □

2.2. **Kompoziční řady permutačních grup.**

2.7. Dokažte, že je alternující grupa A_n pro všechna $n \geq 3$ generovaná trojcykly.

Víme, že každý prvek $\pi \in A_n$ dostaneme složením sudého počtu transpozic

$$\pi = t_1 \circ t_2 \circ \cdots \circ t_{2k-1} \circ t_{2k} = (t_1 \circ t_2) \circ \cdots \circ (t_{2i-1} \circ t_{2i}) \circ \cdots \circ t_{2k-1} \circ t_{2k}.$$

Stačí si tedy uvědomit, že každé složení dvou transpozic $t_{2i-1} \circ t_{2i}$ dostaneme složením trojcyklů. Jsou-li t_{2i-1} a t_{2i} nezávislé tedy $t_{2i-1} \circ t_{2i}$ je tvaru $(12) \circ (34)$, pak

$$(12) \circ (34) = (143) \circ (123).$$

Pokud jsou t_{2i-1} a t_{2i} různé závislé, tedy $t_1 \circ t_2$ je tvaru $(12) \circ (23)$, pak

$$(12) \circ (23) = (123).$$

Konečně pro $t_{2i-1} = t_{2i}$ máme $t_{2i-1} \circ t_{2i} = \mathrm{id}$. □

2.8. Nechť $n \geq 5$ a N je normální podgrupa alternující grupy A_n. Dokažte, že $N = A_n$, pokud

(a) N obsahuje nějaký trojcyklus,
(b) N obsahuje permutaci, která má v cyklickém zápisu cyklus délky aspoň 4,
(c) N obsahuje permutaci, která má v cyklickém zápisu právě jeden trojcyklus,

(d) N obsahuje permutaci, která má v cyklickém zápisu aspoň dva trojcykly,
(e) N obsahuje permutaci, která má v cyklickém zápisu nějaký dvojcyklus.

Bez újmy na obecnosti můžeme označovat permutované prvky postupně přirozenými čísly $1, 2, 3 \dots$

(a) Nechť $(123) \in N$ a zvolme libovolně trojcyklus $(a\ b\ c)$ (tj. $a \neq b \neq c \neq a$). Potom snadno najdeme permutaci $\sigma \in S_n$, pro niž

$$(123)^\sigma = (\sigma(1)\ \sigma(2)\ \sigma(3)) = (a\ b\ c).$$

Kdyby σ byla lichá stačí ji nahradit permutací $\sigma \circ (45) \in A_n$, jež splňuje stejný vztah a je sudá. Protože je N normální v A_n, tedy uzavřená na konjugace, leží $(a\ b\ c)$ v N. To znamená, že N obsahuje všechny trojcykly, tedy $N = A_n$ díky 2.7.

(b) Je-li $\pi := (1234\dots)(\dots)\dots(\dots) \in N$, a $\sigma := \pi^{(123)}$, pak

$$\sigma = (2314\dots)(\dots)\dots(\dots) \in N \quad \text{a} \quad \sigma \circ \pi^{-1} = (124) \in N.$$

Protože N obsahuje trojcyklus, plyne rovnost $N = A_n$ z (a).

(c) Díky (b) stačí uvažovat permutace, která mají cyklický zápis tvaru $\pi = (123)t_1 \dots t_k$, kde t_i jsou nezávislé dvojcykly. Potom $\pi^2 = (132) \in N$, tedy $N = A_n$ opět díky (a).

(d) Nechť $\pi := (123)(456)(\dots)(\dots)\dots(\dots) \in N$, a $\sigma := \pi^{(124)}$, pak

$$\sigma = (243)(156)(\dots)(\dots)\dots(\dots) \in N \text{ a } \sigma \circ \pi = (1463\dots)\cdots \in N.$$

Tedy N obsahuje permutaci, která má v cyklickém zápisu cyklus délky aspoň 4 a rovnost $N = A_n$ plyne z (b).

(e) Nechť $\pi \in N$ má v cyklickém zápisu dvojcyklus. Díky (b), (c) a (d) můžeme předpokládat, že obsahuje pouze dvojcykly, a protože jde o sudou permutaci obsahuje jich sudý počet. Jestliže π je tvaru $(12)(34)$, pak

$$\sigma = \pi^{(125)} = (25)(34) \in N \quad \text{a} \quad \sigma \circ \pi = (152) \in N,$$

což znamená, že $N = A_n$ podle (a). Jestliže π obsahuje alespoň čtyři dvojcykly, tedy je tvaru $(12)(34)(56)(78)\dots$, potom

$$\sigma = \pi^{(23)(45)} = (13)(25)(46)(78)\dots(\dots) \in N \quad \text{a} \quad \sigma \circ \pi = (154)(236) \in N$$

a tudíž $N = A_n$ plyne z (d). □

2.9. Dokažte, že je grupa A_n pro všechna $n \neq 1, 2, 4$ jednoduchá.

Zřejmě A_3 je řádu 3, tedy jde o cyklickou jednoduchou grupu.

Je-li $n \geq 5$ a N je alespoň dvouprvková normální podgrupa grupy A_n, potom $N = A_n$ podle 2.8, tedy jediné normální podgrupy A_n jsou $\{1\}$ a A_n. Grupa A_n je tudíž jednoduchá. □

2.10. Spočítejte kompoziční řadu symetrické grupy S_n pro všechna $n \geq 2$.

Protože $S_2 \cong \mathbb{Z}_2$ je kompoziční řada tvaru $\{\mathrm{id}\} \trianglelefteq S_2$.

Kompoziční řadu S_n pro $n \neq 1, 2, 4$ tvoří $\{\mathrm{id}\} \trianglelefteq A_n \trianglelefteq S_n$ podle předchozí úlohy a protože $S_n/A_n \cong \mathbb{Z}_2$.

Například posloupnost $\{\mathrm{id}\} \trianglelefteq \langle(12)(34)\rangle \trianglelefteq K \trianglelefteq A_4 \trianglelefteq S_4$ tvoří, kompoziční řadu S_4, kde $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$. □

11.11.

Připomeňme, že D_{2n} je grupa všech symetrií pravidelného n-úhleníku a že pro rotaci r u úhel $\frac{2\pi}{n}$ a osovou symetrii o platí

$$D_{2n} = \langle r, o\rangle \cong \langle (1\ 2\ 3\ \dots\ n-1\ n), (2\ n)(3n-1)\dots\rangle \leq S_n.$$

2.11. Nechť r je rotace u úhel $\frac{2\pi}{n}$ a o osovou symetrii . Označme $H := \langle r\rangle \leq D_{2n}$. Dokažte, že

(a) $[D_{2n} : H] = 2$ a $H \trianglelefteq D_{2n}$,
(b) $oho^{-1} = oho = h^{-1}$ pro každé $h \in H$,
(c) jestliže $K \leq H$, pak $K \trianglelefteq D_{2n}$,
(d) je-li $n = \prod_{i=1}^{k} p_i$, kde p_i jsou prvočísla, najděte kompoziční a hlavní řadu D_{2n}.

(a) Zřejmě $o^2 = \mathrm{id}$, proto $o^{-1} = o$. Předpokládejme, že $D_{2n} = \langle r, o\rangle \leq S_n$, kde $r = (1\ 2\ 3\ \dots\ n\ n-1)$ a $o = (2\ n)(3n-1)\dots$, pak $oro^{-1} =$

$= (\dots n{-}1\ n\ 1\ 2\ 3\dots) = (\dots o(n{-}1)\ o(n)\ o(1)\ o(2)\ o(3)\dots) = (\dots 3\ 2\ 1\ n\ n{-}1\dots) =$

$= r^{-1}$. Protože je $H := \langle r\rangle$ cyklická grupa, existuje pro každé $h \in H$ číslo $k \in \mathbb{N}$, pro které $h = r^k$, a proto

$$oho^{-1} = or^k o^{-1} = (oro^{-1})^k = r^{-k} = h^{-1}.$$

Protože $ghg^{-1} = h$ pro každé $h \in H$ je H normální podgrupa D_{2n} a $D_{2n} = \langle o\rangle H = H \cup oH \neq H$, proto $[D_{2n} : H] = 2$.

(b) Je-li σ libovolná rotace, potom $\sigma \in oH = D_{2n} \setminus H$, tedy existuje $g \in H$, pro něž $\sigma = og$. Potom pro každé $h \in H$

$$\sigma h\sigma^{-1} = ogh(og)^{-1} = oghg^{-1}o^{-1} = oho^{-1} = h^{-1}.$$

(c) Jestliže $K \leq N$, pak jistě $hKh^{-1} = K$ a podle předchozí úvahy i $\sigma K\sigma^{-1} = K$ pro každé $\sigma \in oH = D_{2n} \setminus H$, tedy $K \trianglelefteq D_{2n}$.

(d) Podobně jako v 2.6 definujme podgrupy $H_j := \langle r^{\prod_{i=j+1}^{n} p_i}\rangle$ grupy H. Potom $H_0 = \{\mathrm{id}\}$, $H_k = H$ a $H_j/H_{j-1} \cong \mathbb{Z}_{p_j}$ pro $j = 1\dots k$. Položíme-li $H_{k+1} := D_{2n}$, pak $H_{k+1}/H_k = D_{2n}/H \cong \mathbb{Z}_2$. To znamená, že faktory H_j/H_{j-1} jsou pro všechna $j = 1\dots k+1$ jednoduché grupy a H_j jsou normální podgrupy D_{2n}. Tím jsme ověřili, že $\{H_j\}_{j=0}^{k+1}$ představuje kompoziční i hlavní řadu grupy D_{2n} □

3. Řešitelné a nilpotentní grupy

3.1. Dihedrální grupy D_{2n}.

3.1. Dokažte, že je grupa G komutativní, právě když $G' = \{1\}$.

G je komutativní, právě když $ab = ba$ pro všechna $a, b \in G$, což platí, právě když $[a, b] = 1$ pro všechna $a, b \in G$, a to nastává, právě když $G' = \{1\}$. □

3.2. Ověřte, že je grupa D_{2n} pro $n \geq 3$ řešitelná grupa a určete stupeň její řešitelnosti.

Použijeme značení úlohy 2.11.

Protože $D_{2n}/H \cong \mathbb{Z}_2$ je komutativní grupa, máme podle tvrzení z přednášky $D'_{2n} \leq H$. To znamená, že D'_{2n} je komutativní, tedy podle tvrzení předchozí úlohy $D^{(2)}_{2n} = (D'_{2n})' = \{1\}$. Grupa D_{2n} je tedy řešitelná stupně nejvýše 2. Protože je D_{2n} nekomutativní, je stupně většího než 1, tudíž právě stupně 2. □

3.3. Spočítejte centrum grupy D_{2n} pro $n \geq 3$.

Opět využijeme značení předchozích úloh a všimneme si, že pokud prvek $h \in H$ leží v centru, platí díky 2.11(b), že

$$h^{-1} = oho^{-1} = h,$$

tedy $h^2 = \mathrm{id}$. To podmínka je kromě identity splněna pouze pro středovou symetrii s, která leží v $h \in H$ právě tehdy, když je n sudé. Žádná osová symetrie $o \in D_{2n} \setminus H$ neleží v centru, protože $oro^{-1} = r^{-1} \neq r$ opět díky 2.11(b). To znamená, že $Z(D_{2n}) = \langle s \rangle = \{\mathrm{id}, s\}$ pokud je n sudé a $Z(D_{2n}) = \{\mathrm{id}\}$ pro n liché. □

3.4. Jestliže $n = 2m > 4$, dokažte, že $D_{2n}/Z(D_{2n}) \cong D_{2m}$. Na množině $\{1, \ldots, n\}$ zavedeme ekvivalenci $\sim$ pravidlem $a \sim b$, právě když $a \equiv b \pmod m$, a definujme bijekci $b : \{1, \ldots, m\} \to \{1, \ldots, n\}/\sim$ předpisem $b(a) = \{a, a+m\}$. Nyní zavedeme zobrazení $\Psi : D_{2n} \to S_m$ vztahem $\Psi(\sigma) = b^{-1}\sigma b$.

Nejprve je třeba ověřit, že jde o koretktní definici. Musíme pro každé $\sigma \in D_{2n}$ dokázat, že $\sigma b(i) \in \{1, \ldots, n\}/\sim$, tedy že existuje j, pro které $\sigma\{i, i+m\} = \{j, j+m\}$. Snadno nahlédneme, že to platí jak pro rotace, tak pro osové symetrie, tedy že rotace i osová symetrie zobrazí pár středově symetrických bodů opět na pár středově symetrických bodů. Dále přímočaře mahlédneme, že je Ψ homomorfismus:

$$\Psi(\sigma \circ \rho) = b^{-1}\sigma\rho b = b^{-1}\sigma b b^{-1}\rho b = \Psi(\sigma) \circ \Psi(\rho).$$

Protože $\Psi(r) = (1\ 2 \ldots m-1\ m)$ a $\Psi(o) = (2\ m)(2\ m-1)\ldots$ je $\Psi(D_{2n}) = D_{2m}$ a $\mathrm{Ker}\Psi = \{\mathrm{id}, s\}$, platí díky První větě o izomorfismu a předchozí úloze, že

$$D_{2m} \cong D_{2n}/\mathrm{Ker}\Psi = D_{2n}/\langle s \rangle = D_{2n}/Z(D_{2n}).$$

□

3.5. Spočítejte iterovaná centra grupy D_{2n} pro $n \geq 3$, rozhodněte, pro která n je grupa D_{2n} nilpotentní, a případně určete stupeň nilpotence.

Stačí nám využít výsledků předchozích dvou úloh. Nechť $n = 2^a b$ pro b liché. Ukážeme indukcí, že $\theta_i(D_{2n}) = \langle r^{2^{a-i}b} \rangle$ je podgrupa řádu 2^i cyklické grupy $\langle r \rangle$ a $D_{2n}/\theta_i(D_{2n}) \cong D_{2^{1+a-i}b}$ pro $i = 0, \ldots, a$ a dále, že $\theta_i(D_{2n}) = \langle r^b \rangle$ pro všechna $i \geq a$.

Zřejmě $\theta_0(D_{2n}) = \{\mathrm{id}\} = \langle r^{2^a b} \rangle$ a $D_{2n}/\theta_0(D_{2n}) \cong D_{2n} = D_{2^{a+1}b}$. Nechť tvrzení platí pro $i < a$. Pak

$$\theta_{i+1}(D_{2n})/\theta_i(D_{2n}) = Z(D_{2n}/\langle r^{2^{a-i}b} \rangle) \cong Z(D_{2^{1+a-i}b}) = \langle s_i \rangle,$$

kde s_i je středová symetrie grupy $D_{2^{a-i+1}b}$. Z konstrukce izomorfismu nyní snadno spočítáme, že $\theta_{i+1}(D_{2n})$ je podgrupa cyklické grupy $\langle r \rangle$ generovaná prvkem řádu 2^{i+1}, tedy $\theta_{i+1}(D_{2n}) = \langle r^{2^{a-(i+1)}b} \rangle$. Konečně s využitím Druhé věty o izomorfismu a předchozích úvah spočteme

$$D_{2n}/\theta_{i+1}(D_{2n}) \cong \frac{D_{2n}/\theta_i(D_{2n})}{\theta_{i+1}(D_{2n})/\theta_i(D_{2n})} \cong \frac{D_{2^{1+a-i}b}}{Z(D_{2^{1+a-i}b})} \cong D_{2^{a-i}b}$$

Protože je podle 3.4 centrum grupy $D_{2n}/\theta_a(D_{2n}) \cong D_{2b}$ triviální, jsou už i-tá iterovaná centra pro všechna $i \geq a$ stejná jako $\theta_a(D_{2n}) = \langle r^b \rangle$.

Z uvedeného popisu iterovaných center okamžitě plyne, že D_{2n} je nilpotentní, právě když je n tvaru $n = 2^a$ a protože je $D_8/Z(D_8)$ čtyřprvková komutativní grupa, je stupeň nilpotence grupy $D_{2^{1+a}}$ roven a. □

3.6. Je-li $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupa a $M \subseteq G$, dokažte, že $C_G(M) \trianglelefteq N_G(M) \leq G$

Označme $\psi_g : G \to G$ vnitřní automorfismus $\psi_g(x) = gxg^{-1}$ pro $g \in G$ a $\overline{\psi_g}$ restrikci ψ_g na množinu M. Všimněme si, že $g \in C_G(M)$, právě když $\overline{\psi_g}$ je identita na M a $g \in N_G(M)$, právě když $\overline{\psi_g}$ je bijekce $M \to M$. Okamžitě tedy vidíme, že $1 \in C_G(M) \subseteq N_G(M)$. Nechť $a, b \in C_G(M)$. Pak

$$\overline{\psi_{ab}} = \overline{\psi_a} \circ \overline{\psi_b} = \mathrm{id}_M \mathrm{id}_M = \mathrm{id}_M, \quad \text{a} \quad \overline{\psi_{a^{-1}}} = \overline{\psi_a}^{-1} = \mathrm{id}_M^{-1} = \mathrm{id}_M,$$

a proto $a \cdot b, a^{-1} \in C_G(M)$, tedy $C_G(M) \leq G$. Podobně jestliže $a, b \in N_G(M)$, pak $\overline{\psi_{ab}} = \overline{\psi_a} \circ \overline{\psi_b}$ stejně jako $\overline{\psi_{a^{-1}}} = \overline{\psi_a}^{-1}$ tvoří bijekci na M, tudíž $a \cdot b, a^{-1} \in N_G(M)$ a rovněž $N_G(M) \leq G$. Konečně pro $c \in C_G(M)$ a $n \in N_G(M)$ dostáváme

$$\overline{\psi_{ncn^{-1}}} = \overline{\psi_n} \circ \overline{\psi_c} \circ \overline{\psi_n}^{-1} = \overline{\psi_n} \circ \overline{\psi_n}^{-1} = \mathrm{id}_M,$$

což znamená, že $C_G(M) \trianglelefteq N_G(M)$. □

18.11.

3.2. **Grupy řádu p^n.**

3.7. Je-li p prvočíslo, dokažte, že je grupa řádu p^2 komutativní.

Označme $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupu řádu p^2. Z věty dokázané na přednášce víme, že $Z(G) \neq \{1\}$ a podle Lagrangeovy věty je tedy

$$|G/Z(G)| = [G : Z(G)] = \frac{|G|}{|Z(G)|} = p^i$$

pro $i < 2$, tedy $G/Z(G)$ je nutně cyklická grupa. Potřebujeme dokázat, že $i = 0$, tedy že $G = Z(G)$. Protože je $G/Z(G)$ nutně cyklická, existuje $g \in G$, pro které $G/Z(G) = \langle gZ(G) \rangle$. Dále je $Z(G)$ charakteristická a tudíž normální podgrupa G, a proto

$$G = \langle g \rangle Z(G) = \{g^i z \mid i \in \mathbb{N}, z \in Z(G)\}.$$

Proto pro každé $z_1, z_2 \in Z(G)$ a $i, j \in \mathbb{N}$

$$g^i z_1 \cdot g^j z_2 = g^{i+j} z_2 z_1 = g^j z_2 \cdot g^i z_1,$$

tedy každé dva prvky G komutují a grupa G je komutativní. □

3.8. Spočítejte pro grupu $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ řádu 121 centrum $Z(G)$ a komutant G'.

Z předchozí úlohy víme, že je grupa $\mathcal{G}$ komutativní, proto $Z(G) = G$ a $G' = \{1\}$. □

Připomeňme, že definujme-li na množině $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ operaci násobení vztahy

$$i^2 = j^2 = k^2 = -1, ij = k, jk = i, ki = j$$

a dále pravidly $(-1)x = x(-1) = -x$, $xy = -(yx)$, $(-x)y = x(-y) = -(yx)$ pro všechna $x, y \in \{\pm i, \pm j, \pm k\}$, kde $-$ mění znaménko, tvoří Q grupu (kvaternionů).

3.9. Uvažujme grupu kvaternionů Q.

(a) Ukažte, že je Q nilpotentní a určete stupeň nilpotence,
(b) ukažte, že je Q řešitelná a určete stupeň řešitelnosti,
(c) spočítejte centrum $Z(Q)$ a komutant Q',
(d) spočítejte centralizátor $C_Q(g)$ pro všechny prvky $g \in Q$.

(a) Q je grupa řádu 2^3, tedy jde podle věty z přednášky o nilpotentní grupu stupně nejvýše 2. Protože není komutativní, je stupně větší než 1, tedy právě 2.

(b) Každá nilpotentní grupa stupně 2 je podle věty z přednášky řešitelná stupně nejvýše 2, protože Q není komutativní, je stupně řešitelnosti opět právě 2.

(c) Snadno zjistíme, že $Z(Q) = \{1, -1\}$. Protože je $Q/Z(Q)$ čtyřprvková, je to komutativní grupa, tedy $Q' \leq Z(Q)$. Protože $Q' \neq \{1\}$, dostáváme, že $Q' = Z(Q)$.

(d) Pokud $g \in Z(Q)$, pak z definice plyne, že $C_Q(g) = Q$. Pokud $g \notin Z(Q)$, pak $\langle g \rangle \subseteq C_Q(g) \neq Q$, a protože je prvek g řádu 4, nutně $C_Q(g) = \langle g \rangle$. □

4. Akce grupy na množině

4.1. Existuje věrná akce dihedrální grupy D_8 na
(a) tříprvkové množině?
(b) čtyřprvkové množině?

(a) Ptáme se, zda existuje prostý homomorfismus D_8 do grupy (izomorfní) S_3. Protože je D_8 řádu 8 a S_3 řádu 6, žádné prosté zobrazení D_8 do S_3 neexsituje.

(b) Uvážíme-li zobrazení, které symetrii dihedrální grupy D_8 přiřadí permutaci vrcholů příslušného čtverce (s tímto zobrazením, které určuje reprezentaci D_8 jako podgrupy symetrické grupy S_4 jsme pracovali), dostáváme zřejmě prostý homomorfismus D_8 do S_4. □

4.2. Existuje věrná akce grupy kvaternionů Q na čtyřprvkové množině?

Přdpokládejme, že existuje prostý homomorfismus $\varphi : Q \to S_4$. Potom pro všechny prvky $g \notin Z(Q)$ platí, že je g i $\varphi(g)$ řádu 4, tedy by osmiprvková podgrupa $\varphi(Q)$ obsahovala všech šest prvků S_4 řádu 4 (tedy všechny čtyřcykly). Tedy by například

$$(143) = (1234) \circ (2134) \in \varphi(Q),$$

což je ve sporu s tím, že $Q \cong \varphi(Q)$ žádný prvek řádu 3 neobsahuje. □

25.11.

Připomeňme, že centralizátor prvku (či obecně množiny) je právě stabilizátor prvku (množiny) akce konjugace na grupě.

4.3. Spočítejte v symetrické grupě centralizátory:
(a) $C_{S_5}((45))$,
(b) $C_{S_5}((13)(24))$,
(c) $C_{S_9}((12)(345)(6789))$.

(a) Hledáme všechny permutace $\sigma \in S_5$, pro něž $\sigma \circ (45) \circ \sigma^{-1} = (\sigma(4)\sigma(5)) = (45)$, tedy

$$C_{S_5}((45)) = \{\sigma \in S_5 \mid \sigma(\{4,5\}) = \{4,5\}\} = \{\tau \circ (45)^i \mid \tau \in S_3, i \in \mathbb{Z}_2\} = \langle (45) \rangle S_3,$$

vidíme, že $C_{S_5}((45))$ má právě 12 prvků.

(b) Tentokrát hledáme všechny permutace $\sigma \in S_5$, pro něž

$$\sigma \circ (13)(24)(5) \circ \sigma^{-1} = (\sigma(1)\sigma(3))(\sigma(2)\sigma(4))(\sigma(5)) = (13)(24)(5).$$

To znamená, že

$$C_{S_5}((13)(24)) = \{\sigma \in S_5 \mid \sigma(5) = 5 \wedge (\sigma(\{1,3\}) = \{1,3\} \vee \sigma(\{1,3\}) = \{2,4\}\}.$$

Snadno nahlédneme, že $C_{S_5}((13)(24))$ má právě 8 prvků (máme dvě možnosti kam zobrazit množinu $\{1,3\}$ a každé možnosti odpovídají 4 různé permutace). V úloze 1.14 jsme zjistili, že $Z(D_8) = \langle(13)(24)\rangle$, z čehož plyne, že $D_8 \subseteq C_{S_5}((13)(24))$. Protože jsou podgrupy $Z(D_8)$ a $C_{S_5}((13)(24))$ osmiprvkové, vidíme, že $C_{S_5}((13)(24)) = D_8$.

(c) Podobně jako u bodu (a) splňuje $\sigma \in C_{S_9}((12)(345)(6789))$ podmínky

$$\sigma(\{1,2\}) = \{1,2\}, \quad \sigma(\{3,4,5\}) = \{3,4,5\}, \quad \sigma(\{6,7,8,9\}) = \{6,7,8,9\}.$$

To znamená, že

$$\sigma|_{\{1,2\}} \in S(\{1,2\}), \quad \sigma|_{\{3,4,5\}} \in S(\{3,4,5\}), \quad \sigma|_{\{6,7,8,9\}} \in S(\{6,7,8,9\}).$$

Protože $C_{S(\{3,4,5\})}((345)) = \langle(345)\rangle$ a $C_{S(\{6,7,8,9\})}((6789)) = \langle(6789)\rangle$, dostáváme

$$C_{S_9}((12)(345)(6789)) = \{(12)^i \circ (345)^j \circ (6789)^k \mid i \in \mathbb{Z}_2, j \in \mathbb{Z}_3, k \in \mathbb{Z}_4\},$$

tudíž $C_{S_9}((12)(345)(6789)) = \langle(12)\rangle\langle(345)\rangle\langle(6789)\rangle$. □

5. Součiny

5.1. **Semidirektní součiny.**

5.1. Nechť H a K jsou grupy a $\varphi : K \to \mathrm{Aut}(H)$ homomorfismus. Dokažte, že

(a) $H \rtimes_\varphi K = H \times K$, právě když $\varphi_k = \mathrm{id}_H$ pro všechna $k \in K$,

(b) $\widetilde{H} = \{(h,1) \mid h \in H\} \trianglelefteq H \rtimes_\varphi K$ a $(H \rtimes_\varphi K)/\widetilde{H} \cong K$.

(a) Předpokládejme, že $H \rtimes_\varphi K = H \times K$. Potom pro každé $h_1, h_2 \in H$ a $k_1, k_2 \in K$ platí, že $(h_1h_2, k_1k_2) = (h_1\varphi_{k_1}(h_2), k_1k_2)$, a proto $\varphi_{k_1}(h_2) = h_2$ pro všechna $h_2 \in H$ a $k_1 \in K$. Tudíž $\varphi_{k_1} = \mathrm{id}_H$ pro všechna $k_1 \in K$.

Obrácená inkluze je triviální.

(b) Snadno nahlédneme, že je $\widetilde{H}$ podgrupa grupy $H \rtimes_\varphi K$. Nechť $g, h \in H$ a $k \in K$, potom konjugujeme v $H \rtimes_\varphi K$:

$$(h,k) \cdot (g,1) \cdot (h,k)^{-1} = (h\varphi_k(g), k) \cdot (\varphi_k^{-1}(h^{-1}), k^{-1}) =$$

$$= (h\varphi_k(g)\varphi_k(\varphi_k^{-1}(h^{-1})), kk^{-1}) = (h\varphi_k(g)h^{-1}, 1) \in \widetilde{H},$$

tedy H je normální podgrupa $H \rtimes_\varphi K$.

Označme $\widetilde{K} = \{(1,k) \mid k \in K\} \leq H \rtimes_\varphi K$. Okamžitě vidíme, že je zobrazení $k \to (1,k)$ izomorfismus grup K a $\widetilde{K}$ a dále že $H \rtimes_\varphi K = \widetilde{H}\widetilde{K}$ a $\widetilde{H} \cap \widetilde{K} = \{1\}$. Využijeme-li Třetí větu o izomorfismu, dostaneme

$$(H \rtimes_\varphi K)/\widetilde{H} = (\widetilde{H}\widetilde{K})/\widetilde{H} \cong \widetilde{K}/(\widetilde{H} \cap \widetilde{K}) = \widetilde{K}/\{1\} \cong \widetilde{K} \cong K.$$

□

5.2. Je-li $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$ zobrazení dané předpisem $\varphi_k(a) = \varphi(k)(a) = (-1)^k a$, dokažte, že $D_{2n} \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$.

Využijeme značení úlohy 2.11, tedy r je rotace u úhel $\frac{2\pi}{n}$, o osová symetrie a $H = \langle r\rangle$. Dále označme $K = \langle o\rangle$. Nejprve ukážeme, že $D_{2n} \cong H \rtimes_\tau K$ pro homomorfismus $\tau : K \to \mathrm{Aut}(H)$ daný předpisem $\tau_{o^i}(h) = (h)^{(-1)^i}$, tedy $\tau_{\mathrm{id}} = \mathrm{id}_H$ a $\tau_o(h) = h^{-1}$. V úloze 2.11 jsme dokázali, že $H \trianglelefteq D_{2n}$, $H \cap K = \{1\}$ a e $\psi_o = oho^{-1} = h^{-1}$, proto $\psi_o|_H = \tau_0$. Podle věty z přednášky je $D_{2n} \cong H \rtimes_\tau K$.

Nyní stačí uvážit kanonické izomorfismy $\sigma : \mathbb{Z}_n \to H$ dan $\sigma(i) = r^i$ a $\rho : \mathbb{Z}_n \to H$ dan $\rho(i) = o^i$, které indukují izomorfismus $\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2 \to H \rtimes_\tau K$ daný vztahem $(i,j) \to (\sigma(i), \rho(j)) = (r^i, o^j)$. Zřejmě se jedná o bijekci a homomorfismus je to proto, že $\tau_{\rho(j)}(\sigma(i)) = \sigma(\varphi_j(i))$ pro každé $i \in \mathbb{Z}_2$ a $j \in \mathbb{Z}_n$, tedy pro každou dvojici $(i,j),(k,l) \in \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$ je $(i,j)\cdot(k,l) = (i+\varphi_j(k), j+l)$ a pro součin obrazů těchto prvků dostáváme, že

$$(\sigma(i),\rho(j))\cdot(\sigma(k),\rho(l)) = (\sigma(i)\tau_{\rho(j)}(\sigma(k)), \rho(j)\rho(l)) =$$
$$= (\sigma(i)\sigma(\varphi_j(k)), \rho(j+l)) = (\sigma(i+\varphi_j(k)), \rho(j+l))$$

Dokázali jsme, že $D_{2n} \cong H \rtimes_\tau K \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$. □

5.3. Jsou-li H a K jsou grupy a $\varphi : K \to \mathrm{Aut}(H)$ homomorfismus, dokažte, že je operace na $H \rtimes_\varphi K$ asociativní.

Zvolme $(h_1,k_1),(h_2,k_2),(h_3,k_3) \in H \rtimes_\varphi K$. Stačí použít definici a spočítat:

$$[(h_1,k_1)\cdot(h_2,k_2)]\cdot(h_3,k_3) = (h_1\varphi_{k_1}(h_2), k_1k_2)\cdot(h_3,k_3) =$$
$$= (h_1\varphi_{k_1}(h_2)\varphi_{k_1k_2}(h_3), k_1k_2k_3) = (h_1\varphi_{k_1}(h_2\varphi_{k_2}(h_3)), k_1k_2k_3)$$

a

$$(h_1,k_1)\cdot[(h_2,k_2)\cdot(h_3,k_3)] = (h_1,k_1)\cdot(h_2\varphi_{k_2}(h_3), k_2k_3) =$$
$$= (h_1\varphi_{k_1}(h_2\varphi_{k_2}(h_3)), k_1k_2k_3) = [(h_1,k_1)\cdot(h_2,k_2)]\cdot(h_3,k_3).$$

□

2.12.

5.4. Nechť $\mathcal{H} := (H,+,-,0)$ je abelovská grupa a $\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(H)$ homomorfismus daný vztahem $\varphi_k(a) = \varphi(k)(a) = (-1)^k a$. Označme $D_H := H \rtimes_\varphi \mathbb{Z}_2$, $\widetilde{H} = \{(h,1) \mid h \in H\}$ a $\widetilde{H}_n := \{(h,0) \in \widetilde{H} \mid nh = 0\}$. Dokažte:

(a) $[D_H : \widetilde{H}] = 2$,
(b) pro $h \in H$ platí, že $(h,0) \in \widetilde{H}_2$, právě když $h = -h$
(c) $Z(D_H) = \widetilde{H}_2$, pokud $\widetilde{H}_2 \neq H$ a $Z(D_H) = D_H$, pokud $\widetilde{H}_2 = H$,
(d) D_H je řešitelná,
(e) D_H je nilpotentní, právě když existuje k, pro nějž $2^k H = 0$.

(a) Okamžitě z 5.1(b) dostáváme, že

$$[D_H : \widetilde{H}] = |D_H/\widetilde{H}| = |\mathbb{Z}_2| = 2.$$

(b) Podle definice $(h,0) \in \widetilde{H}_2$, právě když $2h = h + h = 0$, což nastává, právě když $h = -h$.

(c) Jestliže $(h,0) \in \widetilde{H}_2$ a $(g,i) \in D_H$, pak díky (b)

$$(g,i)\cdot(h,0) = (g+(-1)^i h, i) = (g+h,i) = (h+g,i) = (h,0)\cdot(g,i),$$

proto $\widetilde{H}_2 \subseteq Z(D_H)$. Jestliže $(h,0) \in \widetilde{H} \setminus \widetilde{H}_2$, pak

$$(g,1)\cdot(h,0) = (g-h,1) \neq (h+g,1) = (h,0)\cdot(g,1),$$

tedy ani $(h,0)$ ani $(g,1)$ pro žádné $g \in H$ neleží v $Z(D_H)$. To znamená, že $Z(D_H) = \widetilde{H}_2$, pokud $\widetilde{H}_2 \neq \widetilde{H}$.

Jestliže $\widetilde{H}_2 = H$, pak opět díky (a) vidíme, že

$$(g,i)\cdot(h,j) = (g+(-1)^i h, i) = (g+h, i+j) = (h+g(-1)^j, i+j) = (h,j)\cdot(g,i),$$

pro každé $(g,i),(h,j) \in D_H$, tedy D_H je komutativní a $Z(D_H) = D_H$.

(d) V (a) jsme si uvědomili, že $D_H/\widetilde{H} \cong \mathbb{Z}_2$, tedy jde o komutativní grupu. Věta z přednášky potom říká, že $D'_H \leq \widetilde{H}$ a protože je $\widetilde{H} \cong H$ komutativní, je D_H řešitelná stupně nejvýše 2.

(e) Spočítáme i-té iterované centrum $\theta_i(D_H)$. Indukcí ukážeme, že $\theta_i(D_H) = H_{2^i}$ pokud $\widetilde{H}_{2^i} \neq \widetilde{H}$ a $\theta_i(D_H) = D_H$ pokud $\widetilde{H}_{2^i} = \widetilde{H}$.

Platnost tvrzení jsme dokázali v (c) pro $i = 1$. Dokažme ho pro $i+1$ za předpokladu, že platí pro i.

Nechť nejprve $\widetilde{H}_{2^{i+1}} \neq \widetilde{H}$. Potom $\widetilde{H}_{2^i} \neq \widetilde{H}$ a

$$\theta_{i+1}(D_H)/\theta_i(D_H) = Z(D_H/\theta_i(D_H)) = Z(D_H/H_{2^i}).$$

Ovšem $D_H/\widetilde{H}_{2^i} \cong D_{H/H_{2^i}} = (H/H_{2^i}) \rtimes_\varphi \mathbb{Z}_2$ a z úlohy (c) okamžitě dostáváme, že $Z(D_{H/H_{2^i}}) = \widetilde{(H/H_{2^i})}_2 \cong \widetilde{H}_{2^{i+1}}/\widetilde{H}_{2^i}$.

Nechť $\widetilde{H}_{2^{i+1}} = \widetilde{H}$. Pokud rovněž $\widetilde{H}_{2^i} = \widetilde{H}$, tak $\theta_i(D_H) = D_H$ podle indukčního předpokladu a tedy i $\theta_{i+1}(D_H) = D_H$. a Pokud konečně $\widetilde{H}_{2^i} \neq \widetilde{H}$, dostáváme, že $\widetilde{(H/H_{2^i})}_2 = \widetilde{H/H_{2^i}}$ a proto je podle (c) $Z(D_{H/H_{2^i}}) = D_{H/H_{2^i}}$ a tudíž $\theta_{i+1}(D_H) = D_H$.

Dokázali jsme, že D_H je nilpotentní, právě když existuje k, pro které $H_{2^k} = H$, což nastává, právě když existuje k, pro které $2^k H = 0$. □

5.5. Dokažte, že S_n je pro každé $n > 1$ semidirektním součinem grupy $\mathbb{Z}_2$ a A_n

Stačí si všimnout, že $A_n \trianglelefteq S_n$, $\langle(12)\rangle \cong Z_2$ a $\langle(12)\rangle \cap A_n = \{\mathrm{id}\}$. Definujeme-li homomorfismy

$$\varphi : \mathbb{Z}_2 \to \mathrm{Aut}(A_n), \qquad \tau : \langle(12)\rangle \to \mathrm{Aut}(A_n),$$

$$\varphi_i(\alpha) = (12)^i \alpha (12)^{-i}, \quad \tau_{(12)^i}(\alpha) = \varphi_i(\alpha),$$

pak je podle tvrzení z přednášky $A_n \rtimes_\tau \langle(12)\rangle \cong A_n\langle(12)\rangle = S_n$ a protože

$$A_n \rtimes_\tau \langle(12)\rangle \cong A_n \rtimes_\varphi \mathbb{Z}_2,$$

dostáváme, že $A_n \rtimes_\varphi \mathbb{Z}_2 \cong S_n$. □

5.6. Dokažte, že je A_4 izomorfní semidirektnímu součinu netriviálních (tedy aspoň dvouprvkových) grup. Platí obdobné tvrzení pro A_n, jestliže $n > 4$?

Stačí si uvědomit, že množina $K_4 = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$ je normální podgrupa A_4 a že platí $\langle(123)\rangle K_4 = A_4$ a $\langle(123)\rangle \cap K_4 = \{\mathrm{id}\}$. Definujme-li homomorfismus $\varphi : \langle(123)\rangle \to \mathrm{Aut}(A_n)$ vztahem $\varphi_\sigma(\alpha) = \sigma\alpha\sigma^{-1} = \psi|_{K_4}$, pak nám stejné tvrzení jako v předchozí úloze dá izomorfismus $A_4 \cong K_4 \rtimes_\varphi \langle(123)\rangle$.

Existoval-li by semidirektní rozklad grupy $A_n \cong H \rtimes K$, pak by podle 5.1 obsahoval normální podrupu izomorfní podgrupě $H \cong \widetilde{H} = \{(h,1) \mid h \in H\}$ indexu $|K| = [H \rtimes K : \widetilde{H}]$. Protože je podle 2.9 grupa A_n pro $n > 4$ jednoduchá, musí být buď řád H nebo K roven jedné. □

5.2. **Kartézské součiny.**

5.7. Nechť $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$ je pro každé $i \in I$ grupa. Označme $\prod_{i\in I} \mathcal{G}_i = (\prod_{i\in I} G_i, \cdot, ^{-1}, 1)$ jejich součin a $\pi_j : \prod_{i\in I} G_i \to G_j$ projekci na j-tou složku $\pi_j(f) = f(j)$ pro každé $j \in I$. Dokažte, že

(a) π_j je pro každé $j \in I$ homomorfismus na,
(b) pro každou grupu $\mathcal{H} = (H, \cdot, ^{-1}, 1)$ a systém homomorfismů $\rho_j : H \to G_j$, $j \in I$ existuje právě jeden homomorfismus $\rho : H \to \prod_{i\in I} G_i$ splňující $\pi_j\rho = \rho_j$ pro každé $j \in I$.

(a) Zvolme $f, g \in \prod_{i\in I} G_i$ a $j \in I$. Protože jsou operace na $\prod_{i\in I} \mathcal{G}_i$ definovány po složkách dostáváme, že

$$\pi_j(f \cdot g) = (f \cdot g)(j) = f(j) \cdot g(j) = \pi_j(f) \cdot \pi_j(g).$$

(b) Nejprve definujme ρ pro každé $h \in H$ a $j \in I$ $[\rho(h)](j) = \rho_j(h)$. Přímo z definice vidíme, že toto zobrazení splňuje podmínku $\pi_j\rho = \rho_j$, navíc jde o homomorfismus, protože pro každé $h, k \in H$ a $j \in I$ platí

$$[\rho(h \cdot k)](j) = \rho_j(h \cdot k) = \rho_j(h) \cdot \rho_j(k) = [\rho(h) \cdot \rho(h)k)](j).$$

Je-li $\widetilde{\rho}$ zobrazení, které rovněž splňuje podmínku $\pi_j\widetilde{\rho} = \rho_j$, potom pro každé $h \in H$ a $j \in I$

$$[\widetilde{\rho}(h)](j) = [\pi_j\widetilde{\rho}(h)](j) = \rho_j(h) = [\pi_j\rho(h)](j) = [\rho(h)](j),$$

tedy $\widetilde{\rho} = \rho$ a homomorfismus ρ je určen jednoznačně □

9.12.

6. Prezentace grup

Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa, $\mathcal{F}(X) = (F(X), \cdot, ^{-1}, 1)$ je volná grupa s volnou bází X, $\pi : F(X) \to G$ homomorfismus na celé G a $R \subset F(X)$. Řekneme, že (X, R, π) je *prezentace grupy* $\mathcal{G}$, jestliže $\ker\pi$ je nejmenší normální podgrupa grupy $\mathcal{F}(X)$ obsahující množinu R.

6.1. Dokažte pro prezentaci (X, R, π) grupy $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ a prvky $u, v \in F(X)$:

(a) $\ker\pi = \langle\bigcup_{f\in F(X)} fRf^{-1}\rangle$,
(b) $u \cdot v^{-1} \in \ker\pi$, právě když $v^{-1} \cdot u \in \ker\pi$, právě když $\pi(u) = \pi(v)$.

(a) Protože je $\ker\pi$ normální podgrupa a $R \subseteq \ker\pi$, dostáváme okamžitě inkluzi $\langle\bigcup_{f\in F(X)} fRf^{-1}\rangle \subseteq \ker\pi$.

Protože je $\langle\bigcup_{f\in F(X)} fRf^{-1}\rangle$ podgrupa, která obsahuje frf^{-1} pro každý její generátor g a pro každé $f \in F(X)$, jedná se o normální podgrupu obsahující R. Ovšem $\ker\pi$ je nejmenší normální podgrupa obsahující R, proto $\ker\pi \subseteq \langle\bigcup_{f\in F(X)} fRf^{-1}\rangle$

(b) Stačí uvážit, že $u \cdot v^{-1} \in \ker\pi$, právě když $\pi(u) \cdot \pi(v)^{-1} = \pi(u \cdot v^{-1}) = 1$, což nastává právě tehdy, když $\pi(u) = \pi(v)$. Ekvivalence pro $v^{-1} \cdot u \in \ker\pi$ se nahlédne symetricky. □

Množina R se nazývá množinou *relací* prezentace a její prvky budeme zapisovat ve tvaru $u = v$ nebo $u \cdot v^{-1} = 1$ pokud $u \cdot v^{-1} \in R$.

6.2. Najděte nějakou prezentaci grupy $\mathbb{Z}^2$.

Pro volnou grupu $F(\{x,y\})$ definujeme homomorfismus $\pi : F(\{x,y\}) \to \mathbb{Z}^2$ vztahem $\pi([u]) = (l_x(u) - l_{x^{-1}}(u), l_y(u) - l_{y^{-1}}(u))$, kde l_x ($l_{x^{-1}}$, l_y, $l_{y^{-1}}$) značí počet výskytů symbolu x (x^{-1}, y, y^{-1}) ve slově u (x^i chápeme pro $i > 0$ jako výskyt i kopií symbolu x, obdobně pro x^{-1}, y, y^{-1}). Pokud $(u,v) \in \rho$, pak zřejmě

$$l_x(u) - l_{x^{-1}}(u) = l_x(v) - l_{x^{-1}}(v),$$

$$l_y(u) - l_{y^{-1}}(u) = l_y(v) - l_{y^{-1}}(v).$$

Indukčním rozšířením dostáváme tytéž vztahy pro každá dvě ekvivalentní slova $u \sim v$, a proto je definice π korektní. Snadno zjistíme, že pro každé dva prvky $[u],[v] \in F(\{x,y\})$ platí, že $\pi([u]) + \pi([v]) =$

$$= (l_x(u) + l_x(v) - (l_{x^{-1}}(u) + l_{x^{-1}}(v)), l_y(u) + l_y(v) - (l_{y^{-1}}(u) + l_{y^{-1}}(v))) =$$

$= \pi([u \cdot v]) = \pi([u] \cdot [v])$, tedy π je homomorfismus. Zobrazení je zřejmě na. Označme N nejmenší normální podgrupu obsahující $x^{-1}y^{-1}xy$. Potom jistě $N \subseteq \ker \pi$. Protože je podle 6.1(a) podgrupa N generována právě všemi komutátory, platí, že $N = [F(\{x,y\}), F(\{x,y\})] = F(\{x,y\})^{(1)}$. Navíc snadno nahlédneme, že každý prvek jádra π leží v komutantu $F(\{x,y\})^{(1)}$. To znamená, že

$$N \subseteq \ker \pi \subseteq F(\{x,y\})^{(1)} = N,$$

což jsme potřebovali dokázat. Tedy $(\{x,y\}, \{xy = yx\}, \pi)$ je hledaná prezentace grupy $\mathbb{Z}^2$. □

6.3. Nechť $\mathcal{F}(X) = (F(X), \cdot, ^{-1}, 1)$ je volná grupa s volnou bází X, $\pi : F(X) \to G$ homomorfismus na grupu $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ a n přirozené číslo. Pokud $|G| \geq n$, $R \subset \ker \pi$ a pro každé $N \trianglelefteq F(X)$ obsahující R platí, že $|F(X)/N| \leq n$, pak dokažte, že (X, R, π) je prezentace grupy $\mathcal{G}$.

Díky První větě o izomorfismu platí, že $G \cong F(X)/\ker \pi$. Jestliže N je nejmenší normální podgrupa obsahující R, pak $N \leq \ker \pi$ a podle předpokladů a Lagrangeovy věty je

$$n \leq |G| = [F(X) : \ker \pi] \leq [F(X) : \ker \pi][\ker \pi : N] = [F(X) : N] \leq n.$$

Proto $[\ker \pi : N] = 1$ a (X, R, π) je tudíž prezentace grupy $\mathcal{G}$. □

6.4. Najděte takový homomorfismus π, aby

(a) $(\{x\}, \{x^{15} = 1\}, \pi)$ byla prezentace grupy $\mathbb{Z}_{15}$,
(b) $(\{x,y\}, \{x^3 = 1, y^5 = 1, xy = yx\}, \pi)$ byla prezentace grupy $\mathbb{Z}_{15}$,
(c) $(\{x,y\}, \{x^n = 1, y^2 = 1, yxy = x{-}1\}, \pi)$ byla prezentace grupy D_{2n}.

(a) Okamžitě vidíme, že $\langle [x]^{15} \rangle \trianglelefteq F(x) = \langle [x] \rangle \cong \mathbb{Z}$, neboť volná grupa s jedním generátorem je cyklická. Protože $\pi([x]^k) = (k) \bmod 15$ určuje homomorismus na grupu $\mathbb{Z}_{15}$ s jádrem rovným $\langle [x]^{15} \rangle$, je π hledaným homomorfismem.

(b) Využijeme-li homorfismus $\pi : F(\{x,y\}) \to \mathbb{Z}^2$ z úlohy 6.2, vidíme, že nejmenší (normální) podgrupa grupy $\mathbb{Z}^2$ obsahující prvky

$$\pi(x^3) = 3 \cdot \pi(x) = 3 \cdot (1,0) = (3,0), \quad \pi(y^5) = 5 \cdot \pi(y) = 3 \cdot (0,1) = (0,5)$$

je právě jádro surjektivního homomorfismu $\tau : \mathbb{Z}^2 \to \mathbb{Z}_3 \times \mathbb{Z}_5$ určeného vztahem $\tau(a,b) = (a \bmod 3, b \bmod 5)$. Proto je $\pi^{-1}(\ker \tau) = \ker(\tau\pi)$ nejmenší normální podgrupou grupy $F(\{x,y\})$ obsahující relace $x^3, y^5, x^{-1}y^{-1}xy$, což znamená, že

$$(x, y \mid x^3 = 1, y^5 = 1, xy = yx, \tau\pi)$$

je prezentace grupy $\mathbb{Z}_3 \times \mathbb{Z}_5$. Ovšem Čínská věta o zbytcích nám zaručuje existenci izomorfismu $h : \mathbb{Z}_3 \times \mathbb{Z}_5 \to \mathbb{Z}_{15}$, tudíž $(x, y \mid x^3 = 1, y^5 = 1, xy = yx, h\tau\pi)$ představuje prezentaci grupy $\mathbb{Z}_{15}$.

(c) Využijeme značení a výsledků úlohy 2.11, tedy $D_{2n} = \langle o, r\rangle$, kde r představuje rotaci o úhel $\frac{2\pi}{n}$ a o osovou symetrii, tj. $r^n = 1$, $o^2 = 1$ a platí, že $oho^{-1} = oho = h^{-1}$ pro každé $h \in \langle r\rangle$. Uvážíme homomorfismus $\pi : F(\{x, y\}) \to D_{2n}$ určený podmínkami $\pi(x) = r$ a $\pi(y) = o$. Potom z 2.11 vidíme, že $\ker\pi$ obsahuje relace $R = \{x^n, y^2, yxyx\}$ a jedná se o homomorfismus na. S využitím 6.3 stačí pro každou normální pogrupu N obsahující R dokázat, že $|F(\{x, y\})/N| \leq 2n$.

K tomu si stačí uvědomit, že

$$F(\{x, y\})/N = \{x^i y^j N \mid i \in \mathbb{Z}_n, j \in \mathbb{Z}_2\}.$$

Protože $x^n, y^2 \in N$ platí, že

$$F(\{x, y\})/N = \{x^{i_1} y x^{i_2} y \dots x^{i_{m-1}} y x^{i_{m-2}} y^\epsilon H \mid i_j \in \mathbb{Z}_n, \epsilon \in \mathbb{Z}_2\}.$$

Protože $yx^iyx^i \in N$, a tudíž $yx^iyN = x^{-i}N$ a $yx^iN = x^{-i}yN$, dostáváme

$$F(\{x, y\})/N = \{x^i y^j N \mid i \in \mathbb{Z}_n, j \in \mathbb{Z}_2\},$$

a proto $|F(\{x, y\})/N| \leq 2n$. Dokázali jsme, že $(x, y \mid x^n = 1, y^2 = 1, yxy = x{-}1, \pi)$ je prezentací grupy D_{2n}. □

7. Sylowovy podgrupy

7.1. Najděte všechny Sylowovy podgrupy grupy
(a) S_3, (b) S_6, (c) $\mathbb{Z}_{120}$, (d) $\mathbb{Z}_{200} \times \mathbb{Z}_{300}$, (e) A_4, (f) A_6.

(a) $|S_3| = 2 \cdot 3$, tedy snadno nahlédneme , že

$$Syl_2(S_3) = \{\langle(12)\rangle, \langle(23)\rangle, \langle(13)\rangle\}, Syl_3(S_3) = \{A_3\} = \{\langle(123)\rangle\}$$

a $Syl_p(S_3) = \{\{\mathrm{id}\}\}$ pro ostaní prvočísla p
(b) $|S_6| = 2^4 \cdot 3^2 \cdot 5$. Protože grupa

$$D_8 \times \mathbb{Z}_2 \cong D_8\langle(56)\rangle = \langle(1234), (13), (56)\rangle \leq S_6$$

je řádu 2^4, dostáváme

$$Syl_2(S_6) = \{\langle(\sigma(1)\sigma(2)\sigma(3)\sigma(4)), (\sigma(1)\sigma(3)), (\sigma(5)\sigma(6))\rangle \mid \sigma \in S_6\}.$$

Dále

$$\mathbb{Z}_3 \times \mathbb{Z}_3 \cong \langle(123)\rangle\langle(456)\rangle = \langle(123), (456)\rangle \leq S_6$$

je grupa řádu 3^2, tudíž je

$$Syl_3(S_6) = \{\langle(\sigma(1)\sigma(2)\sigma(3)), (\sigma(4)\sigma(5)\sigma(6))\rangle \mid \sigma \in S_6\}.$$

Konečně $Syl_5(S_6) = \{\langle(\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))\rangle \mid \sigma \in S_6\}$, protože pětickly generují právě grupy řádu 5 a $Syl_p(S_6) = \{\{\mathrm{id}\}\}$ pro všechna ostaní prvočísla p.

16.12.

(c) $|\mathbb{Z}_{120}| = 120 = 2^3 \cdot 3 \cdot 5$. Protože je $\mathbb{Z}_{120}$ komutativní jsou všechny její podgrupy normální a třídy Sylowových podgrup jsou jednoprvkové:

$$Syl_2(\mathbb{Z}_{120}) = \{\langle 15\rangle\}, \quad Syl_3(\mathbb{Z}_{120}) = \{\langle 40\rangle\}, \quad Syl_5(\mathbb{Z}_{120}) = \{\langle 24\rangle\}$$

a $Syl_p(\mathbb{Z}_{120}) = \{\{0\}\}$ pro ostaní prvočísla p.

(d) Protože je grupa $\mathbb{Z}_{200} \times \mathbb{Z}_{300}$ komutativní jsou stejně jako v (c) všechny její třídy Sylowových podgrup jednoprvkové. Grupa $\mathbb{Z}_{200} \times \mathbb{Z}_{300}$ je řádu $120 = 2^5 \cdot 3 \cdot 5^4$, tedy netriviální jsou pouze Sylowovy 2-podgrupy, 3-podgrupy a 5-podgrupy:

$$Syl_2(\mathbb{Z}_{200} \times \mathbb{Z}_{300}) = \{\langle 25\rangle \times \langle 75\rangle\} \cong \mathbb{Z}_{16} \times \mathbb{Z}_{16},$$
$$Syl_3(\mathbb{Z}_{200} \times \mathbb{Z}_{300}) = \{\{0\} \times \langle 100\rangle\} \cong \mathbb{Z}_3,$$
$$Syl_5(\mathbb{Z}_{200} \times \mathbb{Z}_{300}) = \{\langle 8\rangle \times \langle 12\rangle\} \cong \mathbb{Z}_{25} \times \mathbb{Z}_{25}.$$

(e) $|A_4| = 12 = 2^2 \cdot 3$. Protože $K_4 = \{\langle (12)(34), (13)(24)\rangle\} \cong \mathbb{Z}_2^2$ je podgrupa řádu 4 a podgrupa řádu 3 je cyklická, tedy izomorfní $\mathbb{Z}_3$ dostáváme, že

$$Syl_2(A_4) = \{K_4\} = \{\langle (12)(34), (13)(24)\rangle\},\ \ Syl_3(A_4) = \{\langle (123)\rangle, \langle (124)\rangle, \langle (134)\rangle, \langle (234)\rangle\}$$

a $Syl_p(A_4) = \{\{\mathrm{id}\}\}$ pro ostaní prvočísla p.

(f) $|A_6| = 2^4 \cdot 3^2 \cdot 5$. Nejprve si všimněme, že $\langle (1234)(56), (13)(56)\rangle$ je podgrupa Sylowovy 2-podgrupy grupy S_6, je to tudíž 2-grupa řádu alespoň 8. Navíc

$$D_8 \cong \langle (1234)(56), (13)(56)\rangle \leq A_6,$$

tedy jde o grupu právě řádu 2^3, tedy Sylowovu 2-podgrupu grupy A_6. Proto

$$Syl_2(A_6) = \{\langle (\sigma(1)\sigma(2)\sigma(3)\sigma(4))(\sigma(5)\sigma(6)), (\sigma(1)\sigma(3))(\sigma(5)\sigma(6))\rangle \mid \sigma \in A_6\}.$$

Snadno z (c) dostáváme, že

$$Syl_3(A_6) = \{\langle (\sigma(1)\sigma(2)\sigma(3)), (\sigma(4)\sigma(5)\sigma(6))\rangle \mid \sigma \in A_6\},$$
$$Syl_5(A_6) = \{\langle (\sigma(1)\sigma(2)\sigma(3)\sigma(4)\sigma(5))\rangle \mid \sigma \in A_6\}.$$

□

7.2. Jsou-li $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$ pro $i = 1, \ldots, k$ grupy, dokažte, že pro libovolné n a n-té iterované centrum platí $\theta_n(\coprod_{i=1}^k G_i) = \coprod_{i=1}^k \theta_n(G_i)$.

Tvrzení dokážeme indukcí za využití charakterizace iterovaných center z přednášky, která říká, že $a \in \theta_{n+1}(G)$, právě když $[a, g] \in \theta_n(G)$ pro každé $g \in G$.

Pro $n = 0$ máme $\theta_0(\coprod_{i=1}^k G_i) = \{(1, \ldots, 1)\} = \coprod_{i=1}^k \theta_0(G_i)$.

Nechť platí, že $\theta_n(\coprod_{i=1}^k G_i) = \coprod_{i=1}^k \theta_n(G_i)$. Potom

$$a = (a_1, \ldots, a_n) \in \theta_{n+1}(\coprod_{i=1}^k G_i) \Leftrightarrow [a, g] \in \theta_n(\coprod_{i=1}^k G_i) \forall g = (g_1, \ldots, g_n) \in \coprod_{i=1}^k G_i \Leftrightarrow$$
$$\Leftrightarrow [a_i, g_i] \in \theta_n(G_i) \forall i = 1, \ldots, k, \forall g_i \in G_i \Leftrightarrow$$
$$\Leftrightarrow a_i \in \theta_{n+1}(G_i) \forall i = 1, \ldots, k \Leftrightarrow a \in \coprod_{i=1}^k \theta_{n+1}(G_i).$$

□

7.3. Nechť $p \geq q$ jsou prvočísla, $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa řádu $p \cdot q$ a $P \in Syl_p(G)$. Dokažte:

(a) Pokud $p = q$, potom $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ nebo $G \cong \mathbb{Z}_{p^2}$,
(b) jestliže $p > q$, pak $|Syl_p(G)| = 1$, proto $P \trianglelefteq G$, existuje prvek $g \in G$ řádu q a $G = P\langle g\rangle$.
(c) jestliže $p > q$, pak existuje takový homomorfismus $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$, že $G \cong \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$
(d) jestliže $p > q$ a q nedělí $p - 1$, pak $G \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq}$,

(e) jestliže q dělí $p-1$ pak existuje prostý homomorfismus $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ a buď $G \cong \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q$ je nekomutivní grupa nebo $G \cong \mathbb{Z}_{pq}$,
(f) grupa G je řešitelná.

(a) Jestliže $p = q$, víme, že $\mathcal{G}$ je komutativní. Je-li $\mathcal{G}$ cyklická, pak $G \cong Z_{p^2}$, v opačném případě G tvoří vektorový prostor nad tělesem $\mathbb{Z}_p$, proto $G \cong \mathbb{Z}_p \times \mathbb{Z}_p$ (jako vektorové prostory u tudíž i jako grupy).

(b) Podle Cauchyho věty existuje prvek $g \in G$ řádu q a podle Sylowových vět $|Syl_p(G)| \equiv 1 \pmod p$, proto existuje $k \geq 0$, pro které $|Syl_p(G)| = kp+1$. Protože $Syl_p(G)$ tvoří orbitu akce konjugace grupy $\mathcal{G}$, víme, že $|Syl_p(G)| = [G : N_G(P)]$, tudíž $|Syl_p(G)| = kp+1$ dělí pq, proto $kp+1$ dělí q. Protože $p > q$, nutně $k = 0$, Tudíž $|Syl_p(G)| = 1$ a $P \trianglelefteq G$. Z toho už plyne, že $P\langle g\rangle$ je podgrupa $\mathcal{G}$, jejíž řád dělí dle Lagrangeovy věty pq a která obsahuje podgrupy P i Q. Tedy $P\langle g\rangle = G$.

(c) Plyne okamžitě z věty o semidirektním rozkladu z přednášky, kterou použijeme na $P \cong \mathbb{Z}_p$ a $\langle g\rangle \cong \mathbb{Z}_q$ z tvrzení (b), kde podle Lagrangeovy věty $P \cap \langle g\rangle = \{1\}$.

(d) Protože $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$, znamená podle Lagrangeovy věty a První věty o izomorfismu předpoklad q nedělí $p-1$, že neexistuje žádný netriviální homomorfismus $\mathbb{Z}_q \to \mathbb{Z}_p^*$, a proto ani netriviální homomorfismus $\mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$. Tedy homomorfismus φ z (c) zobrazí vše na neutrální prvek, proto

$$G \cong \mathbb{Z}_p \rtimes_\varphi \mathbb{Z}_q \cong \mathbb{Z}_p \times \mathbb{Z}_q \cong \mathbb{Z}_{pq},$$

kde poslední izomorfismus plyne z Čínské věty o zbytcích.

(e) Opět uvážíme, že $\mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$, z čehož plyne, že $\mathrm{Aut}(\mathbb{Z}_p) = \langle\delta\rangle$ pro nějaký automorfismus δ a tudíž $\mathrm{Aut}(\mathbb{Z}_p)$ obsahuje jednoznačně určenou cyklickou podgrupu $\langle\sigma\rangle$ řádu q s generátorem $\sigma = \delta^{\frac{p-1}{q}}$. To znamená, že existuje $q-1$ netriviálních homorfismů $\varphi : \mathbb{Z}_q \to \mathrm{Aut}(\mathbb{Z}_p)$ a všechny jsou prosté a na podgrupu $\langle\sigma\rangle$. Závěr potom plyne z (c) a (d).

(f) Jestliže $p = q$, pak je G komutativní a tedy zřejmě řešitelná. Jestliže $p > q$, pak $\mathbb{Z}_p \cong P \trianglelefteq G$ a $\mathbb{Z}_q \cong G/P$, a proto i v tomto případě je G řešitelná. □

7.4. Nechť $\varphi : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_3^2)$ je prostý homomorfismus daný zobrazením $i \to \varphi_i$, kde matice φ_i vzhledem ke kanonické bázi je $\begin{pmatrix} 1 & i \\ 0 & 1 \end{pmatrix}$. Dokažte, že je grupa $\mathbb{Z}_3^2 \rtimes_\varphi \mathbb{Z}_3$ nilpotentní stupně 2 a grupa $D_{16} \times (\mathbb{Z}_3^2 \rtimes_\varphi \mathbb{Z}_3)$ nilpotentní stupně 3.

Podle 7.3(d) je $G = \mathbb{Z}_3^2 \rtimes_\varphi \mathbb{Z}_3$ nekomutativní 3-grupa, tedy jde o nekomutativní nilpotentní grupu. Protože $G/Z(G)$ je řádu 3 nebo 9, jedná se komutativní grupu, tedy G je nilpotentní stupně 2.

V 3.5 jsme dokázali, že grupa D_{16} je nilpotentní stupně 3 a z 7.2 okamžitě plyne, že $D_{16} \times (\mathbb{Z}_3^2 \rtimes_\varphi \mathbb{Z}_3)$ je rovněž nilpotentní stupně $\max(3, 2) = 3$. □

7.5. Dokažte, že $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je řešitelná grupa, pokud platí:
(a) $|G| = 77$,
(b) $|G| = 255$,
(c) $G \cong H \rtimes_\varphi K$, kde $\varphi : K \to \mathrm{Aut}(H)$ je homomorfismus, $|K| = 256$, $|H| = 255$.

(a) Protože $77 = 7 \cdot 11$, stačí využít výsledku 7.3(f).

(b) Všimněme si, že $255 = 3 \cdot 5 \cdot 17$. Podle Sylowových vět existuje k nezáporné celé, pro něž $|Syl_{17}(G)| = 1 + 17k$. Protože $Syl_{17}(G)$ tvoří orbitu akce konjugace grupy $\mathcal{G}$, víme, že $|Syl_{17}(G)| = [G : N_G(P)]$ pro $P \in Syl_{17}(G)$. Proto $|Syl_{17}(G)| =$

$1 + 17k$ dělí $|G| = 3 \cdot 5 \cdot 17$, tudíž $1 + 17k$ dělí $3 \cdot 5 = 15$. To nutně znamená, že $k = 0$, tedy existuje jediná Sylowova grupa P řádu 17, která je normální $\mathcal{G}$. Tedy $|G/P| = 3 \cdot 5$, proto je G/P řešitelná grupa a $P \cong \mathbb{Z}_{17}$ je cyklická, tedy rovněž řešitelná grupa. Z tvrzení z přednášky potom okamžitě plyne, že i grupa $\mathcal{G}$ je řešitelná.

(c) Stačí si uvědomit, že K je konečná 2-grupa, proto nilpotentní a tudíž i řešitelná grupa, H je řešitelná podle (b) a (izomorfní kopie) H je normální podgrupa $\mathcal{G}$. Potom zmíněné tvrzení z přednášky implikuje, že grupa $\mathcal{G}$ je řešitelná. □

7.6. Dokažte, že jsou grupy řádu 77 a 255 nutně cyklické. Najděte (nutně řešitelnou) grupu řádu $7 \cdot 29$, která není komutativní.

Protože 7 nedělí $10 = 11 - 1$, je podle 7.3(d) grupa řádu 77 nutně cyklická.

Je-li G grupa řádu 255, obsahuje podle 7.5(b) normální podgrupu $P \in Syl_{17}(G)$ řádu 17 a faktorová grupa G/P je řádu $3 \cdot 5$. Proto Protože 3 nedělí $4 = 5 - 1$, je podle 7.3(d) G/P cyklická, proto existuje prvek $g \in G$ jehož řád je dělitelný číslem 15. Proto cyklická grupa $\langle g \rangle$ obsahuje podgrupu $\langle h \rangle$ řádu 15 a platí, že $P\langle h \rangle = \langle h \rangle P \leq G$ a $P \cap \langle h \rangle = \{1\}$. Snadno si opět díky Lagrangeově větě rozmyslíme, že existuje pouze triviální homomorfismus $\varphi : \langle h \rangle \to \mathrm{Aut}(P)$, tudíž podle Věty z přednášky a Čínské věty o zbytcích

$$G \cong P \rtimes \langle h \rangle = P \times \langle h \rangle \cong \mathbb{Z}_{17} \times \mathbb{Z}_{15} \cong \mathbb{Z}_{255}$$

Protože $2^4 \not\equiv 1 \pmod{29}$ ani $2^7 \not\equiv \pm 1 \pmod{29}$ snadno pomocí Lagrangeovy věty odvodíme, že prvek 2 generuje multiplikativní grupu $\mathbb{Z}_{29}^*$, tj. $\langle 2 \rangle = \mathbb{Z}_{29}^*$. Označíme-li $\varphi_j \in \mathrm{Aut}(\mathbb{Z}_{29})$ pro $j \in \mathbb{Z}_7$ automorfismus určený vztahem $\varphi_j(k) = 2^{4j} \cdot k$, potom je zobrazení $j \to \varphi_j$ netriviální homomorfismus $\varphi : \mathbb{Z}_7 \to \mathrm{Aut}(\mathbb{Z}_{29})$, tudíž je podle 7.3(d) $\mathbb{Z}_{29} \rtimes_\varphi \mathbb{Z}_7$ nekomutativní grupa. □

6.1.

8. Volné grupy

8.1. Nechť $F(x, y)$ je volná grupa o dvou generátorech a n buď přirozené.

(a) Najděte homomorfismus $F(x, y)$ na grupu S_6,
(b) ověřte, že $F(x, y)$ není nilpotentní ani řešitelná,
(c) ověřte, že existuje $N \trianglelefteq F(x, y)$, pro kterou $F(x, y)/N \cong S_n$,
(d) dokažte, že $F(x, y)$ obsahuje normální podgrupu indexu n.

(a) Víme, že $S_6 = \langle (12), (123456) \rangle$ je dvougenerovaná, tedy stačí vzít homomorfismus $f : F(x, y) \to S_3$ určený vztahem $f(x) = (12)$ a $f(y) = (123456)$.

(b) Protože S_6 není řešitelná (tedy ani nilpotentní), $F(x, y)/\mathrm{Ker}\ f \cong S_6$ a řešitelné (i nilpotentní) grupy jsou uzavřené na faktorizaci, nemůže být řešitelná ani nilpotentní grupa $F(x, y)$.

(c) Každá symetrická grupa $S_n = \langle (12), (12 \dots n) \rangle$ je dvougenerovaná, proto existuje homomorfismus $f : F(x, y) \to S_n$ určený vztahem $f(x) = (12)$ a $f(y) = (12 \dots n)$, který je homomorfismem na celou grupu S_n. Podle První věty o izomorfismu je potom $F(x, y)/\mathrm{Ker}\ f \cong S_n$.

(d) Stačí, abychom uvážili například homomorfismus $g : F(x, y) \to \mathbb{Z}_n$ určený vztahem $f(x) = 1$ a $f(y) = 0$, pak podle První věty o izomorfismu dostáváme, že

$$|F(x, y)/\mathrm{Ker}\ g| = [F(x, y) : \mathrm{Ker}\ g] = |\mathbb{Z}_n| = n.$$

tedy $N = \mathrm{Ker}\ g$ je hledaná normální podgrupa indexu n. □

8.2. Uvažujme homomorfismus $\varphi : F(\{x,y\}) \to S_3$ na S_3 určený podmínkou $\varphi(x) = (12)$, $\varphi(y) = (123)$ a položme $H = Ker\ \varphi$.

(a) Najděte Schreierovu transversálu podgrupy H,
(b) najděte transversálu H, která není Schreierova,
(c) najděte volnou bázi grupy H.

(a) Víme, že $[F(\{x,y\}) : H] = |F(\{x,y\})/H| = |S_3| = 6$ je počet levých rozkladových tříd, tedy počet prvků jakékoli transversály. Navíc pro rozkladové třídy $t_1H \neq t_2H$ platí, že

$$\varphi(t_1) = \varphi(t_1H) \neq \varphi(t_2H) = \varphi(t_2)$$

Hledáme tedy postupně reprezentanty $t \in T$ v redukovaném zápisu, jejichž všechny sufixy (tj. pravé koce slov) tvoří prvky transversály a obrazy $\varphi(t)$ jsou různé. Jistě $1 \in T$. Dále jistě $\{1, y, y^2\}$ tvoří částečnou Schreierovu transversálu, protože

$$\varphi(1) = \mathrm{id} \quad \varphi(y) = (123), \quad \varphi(y^2) = (132).$$

Konečně vidíme, že můžeme přidat všechny prvky částečné Schreirovy transversály T zleva přenásobené prvkem součiny x, protože

$$\varphi(x) = (12) \quad \varphi(xy) = (12) \circ (123) = (23), \quad \varphi(xy^2) = (12) \circ (132) = (13)$$

a slova $1, y, y^2$ leží v T. Našli jsme Schreierovu transversálu $T = \{1, y, y^2, x, xy, xy^2\}$.

(b) Například $T = \{1, yx^2, y^2, x, xy, xy^2\}$ je transversála, ale není Schreierova, protože neobsahuje prvek x^2 tvořící sufix slova yx^2.

(c) Víme, že volnou bázi grupy H tvoří množina

$${}_TY_H = \{t_{z\omega}^{-1} z t_\omega \mid z \in \{x,y\}, \omega \in \Omega, zt_\omega \notin T\},$$

kde $\Omega = \{tH \mid t \in T\}$ a $t_{tH} = t$ pro $t \in T$. Nejprve spočítáme, pro která t platí, že $xt \notin T$. Zjevně $x1, xy, xy^2 \in T$, zatímco $x^2, x^2y, x^2y^2 \notin T$, proto vyhovují prvky transversály

$$t_{xH} = x, \quad t_{xyH} = xy, \quad t_{xy^2H} = xy^2$$

a snadno dopočítáme hodnoty t_{xtH}:

$$t_{xxH} = 1, \quad t_{xxyH} = y, t_{xxy^2H} = y^2.$$

Podobně zjistíme, pro která $t \in T$ platí, že $yt \notin T$: $y1, yy \in T$, zatímco $y^3, yx, yxy, yxy^2 \notin T$, a proto vyhovují prvky

$$t_{y^2H} = y^2, \quad t_{xH} = x, \quad t_{xyH} = xy, \quad t_{xy^2H} = xy^2$$

a dopočítáme hodnoty t_{ytH}:

$$t_{y^3H} = 1, \quad t_{yxH} = xy^2, \quad t_{yxyH} = x, \quad t_{yxy^2H} = xy$$

Nyní už podle definice množiny ${}_TY_H$ vyjádříme volnou bázi

$${}_TY_H = \{x^2, \ y^{-1}x^2y, \ y^{-2}x^2y^2, \ y^3, \ y^{-2}x^{-1}yx, \ x^{-1}yxy, \ y^{-1}x^{-1}yxy^2\}.$$

□

Obsah