Cvičení z Úvodu do teorie grup

5. ledna 2021

29.9.

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

(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

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

□

1.2 Konečné abelovské grupy

1.4. 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. $\square$

Další úlohy:

1. Popište všechny podgrupy a množiny automorfismů a endomorfismů grupy (a) $\mathbb{Z}_{50}$ (b) $\mathbb{Z}_{23}^*$.
2. Popište všechny podgrupy grupy $\mathbb{Z}_3^3$.

6.10.

2 Permutační grupy

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

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

2.1. 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. $\square$

2.2. 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 $(i\ i+1)$:

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

□

2.3. 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

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

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

2.4. 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 2.3.

(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

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

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). $\square$

2.5. Dokažte, že je grupa A_n pro všechna $n \neq 4$ 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 2.4, tedy jediné normální podgrupy A_n jsou $\{1\}$ a A_n. Grupa A_n je tudíž jednoduchá. $\square$

13.10.

Další úlohy:

1. Najděte všechny permutace $\sigma \in A_8$ $((123)(45)(67))^\sigma = (18)(237)(56)$.
2. Spočítejte velikost třídy konjugace $\{((13)(467))^\sigma \mid \sigma \in S_7\}$.

3 Normální a charakteristické podgrupy

3.1. Nechť $\mathcal{A} = (A, \cdot, ^{-1}, 1)$ je grupa a nechť $N \trianglelefteq A$ a $H \leq A$. Dokažte, že $H \cap N \trianglelefteq H$.

Víme, že průnik podgrup je opět podgrupa, tedy $H \cap N \leq A$. To znamená, že $H \cap N$ je uzavřená na všechny operace a je tedy podgrupou každé grupy, v níž je obsažena, speciálně $H \cap N \leq A$.

Zbývá ověřit uzavřenost podgrupy $H \cap N$ na všechny konjugace prvky z H. Zvolme libovolně $h \in H$ a $a \in H \cap N$. Protože $h, a \in H$ a H je podgrupa, platí, že

$$hah^{-1} \in H.$$

Protože $h \in A$ a $a \in N \trianglelefteq A$, platí, že

$$hah^{-1} \in N.$$

Tím jsme ověřili, že $hah^{-1} \in H \cap N$ pro každé $h \in H$ a $a \in H \cap N$, a proto $H \cap N \trianglelefteq H$. $\square$

3.2. Definujme podgrupu $A = \bigcup_n A_n$ grupy $S(\mathbb{N})$, kde A_n chápeme jako podgrupy $S(\mathbb{N})$. Dokažte, že je grupa A nekonečná jednoduchá.

Předpokládejme, že $N \neq \{1\}$ je normální podgrupa grupy A. Abychom ověřili, že je A jednoduchá, stačí dokázat, že $N = A$.

Zvolme $\sigma \in N \setminus \{1\}$. Protože $A_1 \leq A_2 \cdots \leq A_n \leq A_{n+1} \leq \ldots$ a $A = \bigcup_n A_n$, existuje takové n_0, že pro všechna $n \geq n_0$ leží $\sigma \in A_n$, a proto $A_n \neq \{1\}$. Využijeme-li tvrzení úlohy 3.1, pak dostáváme , že $\{1\} \neq A_n \cap N \trianglelefteq A_n$, a proto díky 2.5 $A_n \cap N = A_n$. Tudíž $A_n \subseteq N$ pro všechna $n \geq n_0$. čímž jsme dokázali, že

$$A = \bigcup_{n \geq n_0} A_n \subseteq N \subseteq A,$$

tedy $A = N$. Nekonečnost plyne z pozorování , že $|A| \geq |A_n| = \frac{n!}{2}$ pro všechna $n \geq 2$. $\square$

3.3. 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 $H \subseteq Z(G)$. $\square$

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

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

3.4. 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) spočítejte centrum grupy D_{2n} pro $n \geq 3$.

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

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

$= r^{-1}$. 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) Všimneme si, že pokud prvek $h \in H$ leží v centru, platí díky (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 3.4(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. □

20.10.

Další úlohy:

1. Popište všechny charakteristické a úplně charakteristické podgrupy grup $\mathbb{Z}$ a $\mathbb{Z}_n$ pro $n \in \mathbb{N}$.
2. Spočítejte pro grupu $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ řádu 121 centrum $Z(G)$.

4 Součiny

4.1 Direktní součiny

4.1. Nechť $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$ je pro každé $i \in I$ grupab a označme $\mathcal{G} = \coprod_{i\in I} \mathcal{G}_i$. Dokažte, že (a) $Z(\mathcal{G}) = \coprod_{i\in I} Z(\mathcal{G}_i)$, (b) $G' = \coprod_{i\in I} \mathcal{G}'_i$

Díky Větě 4.4 z přednášky můžeme bez újmy na obecnosti předpokládat, že $G_i \trianglelefteq G$ a platí, že $G_j \cap \langle\bigcup_{i\neq j} G_i\rangle = \{1\}$ pro všechna $j \in I$ a $\langle\bigcup_{i\in I} G_i\rangle = G$.

(a) Uvědomíme-li si, že pro $i \neq j$ a $g_i \in G_i, g_j \in G_j$ platí, že $g_i g_j = g_j g_i$, vidíme, že $\coprod_{i \in I} Z(\mathcal{G}_i) \subseteq Z(\mathcal{G})$.

Naopak, pro každý prvek $g \in Z(G)$ existují různé indexy $i_1, \dots, i_k$ a prvky $g_1 \in G_{i_1}, \dots, g_k \in G_{i_k}$ pro něž $g = g_1 \cdot \dots \cdot g_k$. zvolíme-li $a \in G_{i_1}$, pak s využitím původního pozorování dostáváme:

$$a \cdot g_1 \cdot g_2 \cdot \dots \cdot g_k = a \cdot g = g \cdot a = g_1 \cdot g_2 \cdot \dots \cdot g_k \cdot = g_1 \cdot a \cdot g_2 \cdot \dots \cdot g_k.$$

Vykrátíme-li nyní krajní výrazy zprava prvkem $g_2 \cdot \dots \cdot g_k$, dostáváme, že $a g_1 = g_1 a$ pro všechna $a \in G_{i_1}$, což znamená, že $g_1 \in Z(G_{i_1})$. Díky vzájemné komutativitě prvků $g_1, \dots, g_k$ vidíme, že $g_j \in\in Z(G_{i_j})$ pro všechna $j = 1, \dots, k$, a proto $g \in \coprod_{i \in I} Z(\mathcal{G}_i)$.

(b) Obdobnou úvahou jako v (a) snadno nahlédneme, že $\coprod_{i \in I} \mathcal{G}'_i \subseteq G'$. Naopak, vezmeme-li komutátor $[a, b]$ prvků a, b, pak opět jistě existují různé indexy $i_1, \dots, i_k$ a prvky $a_1, b_1 \in G_{i_1}, \dots, a_k, b_k \in G_{i_k}$ pro něž $a = a_1 \cdot \dots \cdot a_k$ a $b = b_1 \cdot \dots \cdot b_k$. Díky komutování prvků z různých podgrup G_i dostáváme:

$$[a, b] = [a_1 \cdot \dots \cdot a_k, b_1 \cdot \dots \cdot b_k] = [a_1, b_1] \cdot \dots \cdot [a_k, b_k] \in \coprod G'_i,$$

čímž jsme ověřili inkluzi $G' \subseteq \coprod_{i \in I} \mathcal{G}'_i$. □

4.2. 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. □

4.2 Semidirektní součiny

4.3. 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 3.4, 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 3.4 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 $D_{2n} \cong H \rtimes_\tau K \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$. $\square$

4.4. 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 $A_n \rtimes_\varphi \mathbb{Z}_2 \cong S_n$. $\square$

27.10.

Další úlohy:

1. Spočítejte všechny semidirektní součiny $\mathbb{Z}_2 \rtimes \mathbb{Z}_3$.
2. Spočítejte všechny semidirektní součiny $\mathbb{Z}_3 \rtimes \mathbb{Z}_2$.

5 Semidirektní součiny a řešitelnost

5.1 Grupy řádu $2p$ a p^2

5.1. Popište jak vypadají až na izomorfismus všechny grupy řádu 6.

Nechť $\mathcal{G}$ je grupa řádu 6. Potom podle Cauchyovy věty obsahuje podgrupu K (prvočíselného) řádu 2 a podgrupu H řádu 3, jejichž průnik je podle Lagrangeovy věty jednoprvkový, tedy $H \cap K = \{1\}$. Rovněž Lagrangeovy věty plyne, že $[G : H] = \frac{|G|}{|H|} = 2$, a proto $H \trianglelefteq \mathcal{G}$ a $HK = G$. To podle Věty 4.7 z přednášky znamená, že $\mathcal{G} \cong H \rtimes K \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$ a stačí tak jen prozkoumat všechny homomorfismy $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$. V úloze 1.3(b) jsme zjistili, že $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_3^* \cong \mathbb{Z}_2$, což znamená, že existují jen 2 homomorfismy $\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$. Pro triviální homomorfismus $\alpha : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ splňující $\alpha(\mathbb{Z}_2) = \{\mathrm{id}\}$ dostáváme

$$\mathcal{G} \cong \mathbb{Z}_3 \rtimes_\alpha \mathbb{Z}_2 \cong \mathbb{Z}_3 \times \mathbb{Z}_2 \cong \mathbb{Z}_6$$

Pro triviální izomorfismus $\beta : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_3)$ dostáváme

$$\mathcal{G} \cong \mathbb{Z}_3 \rtimes_\beta \cong S_3 \cong D_6,$$

neboť známe $S_3 \cong D_6$ je (jediná) šestiprvková nekomutativní grupa. □

5.2. Nechť H a K jsou grupy a $\varphi : K \to \mathrm{Aut}(H)$ homomorfismus. Dokažte, že $H \rtimes_\varphi K = H \times K$, právě když $\varphi_k = \mathrm{id}_H$ pro všechna $k \in K$.

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 implikace je triviální. □

5.3. Popište pro prvočíslo p až na izomorfismus všechny grupy řádu (a) $2p$ (b) p^2.

(a) Nechť $p > 2$. Použijeme stejnou úvahu jako v úloze 5.1.

Podle Cauchyovy a Lagrangeovy věty věty obsahuje grupa G řádu $2p$ podgrupy K a H splňující $|H| = p$, $|K| = 2$, $H \cap K = \{1\}$, $[G : H] = \frac{|G|}{|H|} = 2$, $H \trianglelefteq \mathcal{G}$ a $HK = G$, a proto

$$\mathcal{G} \cong H \rtimes K \cong \mathbb{Z}_p \rtimes \mathbb{Z}_2.$$

I tentokrát máme jen dva homomorfismy

$$\mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_p) \cong \mathbb{Z}_p^* \cong \mathbb{Z}_{p-1},$$

protože je p liché. Jim odpovídá abelovská grupa $\mathbb{Z}_{2p}$ a nekomutativní grupa D_{2p}, což jsou až na izomorfismus jediné dvě grupy řádu $2p$.

Jestliže $p = 2$, pak úlohu řeší bod (b).

(b) Z přednášky víme, že je grupa řádu p^2 nutně komutativní, tedy je buď izomorfní cyklické grupě $\mathbb{Z}_{p^2}$ nebo cyklická není, a pak je taková grupa vektorovým prostorem nad tělesem $\mathbb{Z}_p$. V druhém případě z lineární algebry víme, že je grupa izomorfní grupě $\mathbb{Z}_p^2$. $\square$

5.2 Řešitelnost a nilpotence grupy D_{2n}

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

Použijeme značení úlohy 3.4.

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 $D_{2n}^{(2)} = (D'_{2n})' = \{1\}$. Grupa D_{2n} je tedy řešitelná stupně nejvýše 2. Protože je D_{2n} nekomutativní, je stupně většího než 1, tudíž právě stupně 2. $\square$

3.11.

Další úlohy:

1. Popište jak vypadají až na izomorfismus všechny grupy řádu 34. Které z nich jsou řešitelné?
2. Ověřte, že je grupa A_4 řešitelná a určete stupeň její řešitelnosti.

6 Malé konečné grupy

6.1 Klasifikace

6.1. Klasifikujte (tj. najděte všechny až na izomorfismus) všechny grupy řádu:

$$2, 3, 4, 5, 6, 7, 9, 10, 11, 13, 14.$$

V klasifikaci využijeme toho, že víme, že grupa prvočíselného řádu p je cyklická, tedy izomorfní $\mathbb{Z}_p$ a že jsme pro $p > 2$ v 5.3 dokázali, že $\mathbb{Z}_{2p}$ a D_{2p} jsou až na izomorfismus jediné dvě grupy řádu $2p$ a $\mathbb{Z}_{p^2}$ nebo cyklická není, a že $\mathbb{Z}_{p^2}$ a $\mathbb{Z}_p^2$ jsou až na izomorfismus jediné dvě grupy řádu p^2:

- pro $|G| = 2$: $\mathcal{G} \cong \mathbb{Z}_2$,
- pro $|G| = 3$: $\mathcal{G} \cong \mathbb{Z}_3$,
- pro $|G| = 4$: $\mathcal{G} \cong \mathbb{Z}_4$ nebo $\mathcal{G} \cong \mathbb{Z}_2 \times \mathbb{Z}_2$,
- pro $|G| = 5$: $\mathcal{G} \cong \mathbb{Z}_5$,
- pro $|G| = 6$: $\mathcal{G} \cong \mathbb{Z}_6$, nebo $\mathcal{G} \cong S_3 \cong D_6$,
- pro $|G| = 7$: $\mathcal{G} \cong \mathbb{Z}_7$,
- pro $|G| = 9$: $\mathcal{G} \cong \mathbb{Z}_9$, nebo $\mathcal{G} \cong \mathbb{Z}_3 \times \mathbb{Z}_3$
- pro $|G| = 10$: $\mathcal{G} \cong \mathbb{Z}_{10}$, nebo $\mathcal{G} \cong D_{10}$
- pro $|G| = 11$: $\mathcal{G} \cong \mathbb{Z}_{11}$,
- pro $|G| = 13$: $\mathcal{G} \cong \mathbb{Z}_{13}$,
- pro $|G| = 14$: $\mathcal{G} \cong \mathbb{Z}_{14}$.

$\square$

6.2. Uveďte vždy aspoň čtyři neizomorfní příkladů grup řádu: $8, 12$

Osmiprvkové vzájemně neizomorfní grupy jsou například následující grupy

$$\mathbb{Z}_8, \mathbb{Z}_2 \times \mathbb{Z}_4, \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, D_8.$$

Dvanáctiprvkové vzájemně neizomorfní grupy jsou například následující

$$\mathbb{Z}_{12}, \mathbb{Z}_6 \times \mathbb{Z}_2, S_3 \times \mathbb{Z}_2, A_4.$$

$\square$

6.2 Sylowovy podgrupy

6.3. Najděte všechny Sylowovy podgrupy grupy (a) $\mathbb{Z}_{120}$ (b) S_3.

(a) $|\mathbb{Z}_{120}| = 120 = 2^3 \cdot 3 \cdot 5$. 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.

(b) $|S_3| = 2 \cdot 3$, 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 $\square$

Další úlohy:

1. Najděte všechny Sylowovy podgrupy grupy (a) S_4 (b) D_{10}.

7 Nilpotence a p-podgrupy

7.1 Sylowovy podgrupy

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

(a) $|S_6| = 2^4 \cdot 3^2 \cdot 5$. 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 pěticykly generují právě grupy řádu 5 a $Syl_p(S_6) = \{\{\mathrm{id}\}\}$ pro všechna ostaní prvočísla p.

(b) 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:

$$Syl_2(\mathbb{Z}_{200} \times \mathbb{Z}_{300}) = \{\langle 25\rangle \times \langle 75\rangle\} \cong \mathbb{Z}_{16} \times \mathbb{Z}_{16},$$

$$Syl_3(\mathbb{Z}_{200} \times \mathbb{Z}_{300}) = \{\{0\} \times \langle 100\rangle\} \cong \mathbb{Z}_3,$$

$$Syl_5(\mathbb{Z}_{200} \times \mathbb{Z}_{300}) = \{\langle 8\rangle \times \langle 12\rangle\} \cong \mathbb{Z}_{25} \times \mathbb{Z}_{25}.$$

(c) $|A_4| = 12 = 2^2 \cdot 3$. 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.

(d) $|A_6| = 2^4 \cdot 3^2 \cdot 5$. 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 Nilpotentní grupy

7.2. Rozhodněte, zda existuje konečná nilpotentní grupa $\mathcal{G}$, pro kterou $|Syl_5(\mathcal{G})| > 1$.

Sylowovy věty říkají, že konečná nilpotentní grupa má všechny Sylowovy podgrupy normální, tedy $|Syl_p(\mathcal{G})| = 1$ pro každé prvočíslo p. Proto konečná nilpotentní grupa $\mathcal{G}$, pro kterou $|Syl_5(\mathcal{G})| > 1$, neexistuje □

7.3. Popište (až na izomorfismus) všechny Sylowovy podgrupy nilpotentní grupy $\mathcal{G}$ jestliže (a) je řádu 105, (b) není cyklická a je řádu 99. Jaký je stupeň nilpotence těchto grup? $|Syl_5(\mathcal{G})| > 1$.

(a) Protože $105 = 3 \cdot 5 \cdot 7$ jsou všechny Sylovovy podgrupy $\mathcal{G}$ cyklické, tedy komutativní. Grupa je navíc nilpotentní, tedy jsou máme pro každé pro prvočísla $p = 3, 5, 7$ právě jednu (normální) Sylowovu p-grupu izomorfní $\mathbb{Z}_p$. Ostatní Sylowovy podgrupy jsou triviální.

(b) Protože $99 = 3^2 \cdot 11$ a grupa $\mathcal{G}$ je nilpotentní, obsahuje právě jednu právě jednu (normální) Sylowovu 3-grupu řádu 9 a právě jednu (normální) Sylowovu 11-grupu řádu 11. Obě tyto podrupy jsou nutně komutativní a grupa $\mathcal{G}$ je izomorfní součinu těchto dvou podgrup, proto je $\mathcal{G}$ nutně komutativní. Kdyby byla podgrupa řádu 9 cyklická, byla by podle Čínské věty o zbytcích cyklická i grupa $\mathcal{G}$, proto je Sylowovu 3-grupu izomorfní grupě $\mathbb{Z}_3 \times \mathbb{Z}_3$ a Sylowovu 11-grupu izomorfní grupě $\mathbb{Z}_{11}$. □

7.4. Nechť $n = 2m > 4$. 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 $b(a) = \{a, a+m\}$. Dokažte, že je zobrazení $\Psi : D_{2n} \to S_m$ zavedené vztahem $\Psi(\sigma) = b^{-1}\sigma b$ izomorfismus grup $D_{2n}/Z(D_{2n})$ a D_{2m}.

Nejprve je třeba ověřit, že jde o korektní 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 nahlédneme, 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

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

$\square$

24.11.

7.5. 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 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 7.4 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. □

7.6. Spočítejte velikosti iterovaných center grup (a) D_{32} a (b) D_{36}.

S využitím předchozí úlohy zjistíme, že $|\vartheta_1(D_{32})| = |Z(D_{32})| = 2$,
$|\vartheta_2(D_{32})| = |Z(D_{16})| \cdot |\vartheta_1(D_{32})| = 4$,
$|\vartheta_3(D_{32})| = |Z(D_8)| \cdot |\vartheta_2(D_{32})| = 8$,
$|\vartheta_4(D_{32})| = |Z(D_4)| \cdot |\vartheta_4(D_{32})| = 32$.
Proto $|\vartheta_i(D_{32})| = 32$ pro všechna $i \geq 4$.
Podobně

$$|\vartheta_1(D_{36})| = |Z(D_{36})| = 2, \quad |\vartheta_2(D_{36})| = |Z(D_{18})| \cdot |\vartheta_1(D_{32})| = 2,$$

proto $|\vartheta_i(D_{32})| = 2$ pro všechna $i \geq 2$. □

Další úlohy:

1. Popište (až na izomorfismus) všechny Sylowovy podgrupy nilpotentní grupy $\mathcal{G}$, jestliže je řádu 77.

8 Grupy řádu pq

8.1. Popište (až na izomorfismus) všechny grupy řádu
(a) 33, (b) 35, (c) 21, (d) 55.

Všechny uvedené řády jsou součiny dvou různých prvočísel, což nám umožňuje využít Poznámku 8.2 z přednášky.

(a) Protože $33 = 3 \cdot 11$ a 3 nedělí $10 = 11 - 1$, existuje pouze cyklická grupa řádu 33.

(b) Podobně pro $35 = 5 \cdot 7$, platí, že 5 nedělí $6 = 7 - 1$, tudíž opět existuje pouze cyklická grupa řádu 35.

(c) Tentokrát $21 = 3 \cdot 7$ a 3 dělí $6 = 7 - 1$, proto vedle (komuttaivní) cyklické grupy $\mathbb{Z}_{21}$ umíme zkonstruovat až na izomorfismus jedinou nekomutativní grupy řádu 21 jako semidirektní součin $\mathbb{Z}_7 \rtimes_\phi \mathbb{Z}_3$ pro prostý homomorfismus $\phi : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_7)$ daný vztahem $k \to \phi_k(s) = 2^k s$. Využili jsme při tom korespondence

$$\mathrm{Aut}(\mathbb{Z}_7) \cong \mathbb{Z}_7^* \cong \mathbb{Z}_6$$

a klíčové bylo najít prvek řádu v 3 v grupě $\mathbb{Z}_7^*$ (měli jsme na výběr právě 2 prvky: 2 a 5).

(d) Opět vidíme, že 5 dělí $10 = 11 - 1$ $21 = 3 \cdot 7$ a tudíž obdobným postupem jako v (c) najdeme až na izomorfismus jediné dvě grupy řádu 55:

$$\mathbb{Z}_{55}, \mathbb{Z}_{11} \rtimes_\phi \mathbb{Z}_5$$

pro prostý homomorfismus $\phi : \mathbb{Z}_5 \to \mathrm{Aut}(\mathbb{Z}_{11})$ daný vztahem $k \to \phi_k(s) = 3^k s$, kde $3 \in \mathbb{Z}_{11}^*$ je prvek řádu 5. □

8.2. Jak vypadají Sylowovy podgrupy grup z předchozí úlohy? Které z nich jsou řešitelné a které nilpotentní?

Protože jsou všechny uvedené grupy semidirektní součiny jedná se řešitelné grupy. Pro cyklické grupy snadno určíme jediné Sylpowovy p-grupy:

$$Syl_3(\mathbb{Z}_{33}) = \{\langle 11 \rangle\}, Syl_{11}(\mathbb{Z}_{33}) = \{\langle 3 \rangle\},$$

$$Syl_5(\mathbb{Z}_{35}) = \{\langle 7 \rangle\}, Syl_7(\mathbb{Z}_{35}) = \{\langle 5 \rangle\},$$
$$Syl_3(\mathbb{Z}_{21}) = \{\langle 7 \rangle\}, Syl_7(\mathbb{Z}_{21}) = \{\langle 3 \rangle\},$$
$$Syl_5(\mathbb{Z}_{55}) = \{\langle 11 \rangle\}, Syl_{11}(\mathbb{Z}_{55}) = \{\langle 5 \rangle\},$$

Všechny cyklické grupy jsou samozřejmě nilpotentní.

Konečně nekomutativní grupy $\mathbb{Z}_7 \rtimes \mathbb{Z}_3$ a $\mathbb{Z}_{11} \rtimes \mathbb{Z}_5$ nemohou být nilpotentní, protože obsahují Sylowovy podgrupy, které nejsou normální a máme:

$$Syl_7(\mathbb{Z}_7 \rtimes \mathbb{Z}_3) = \{\mathbb{Z}_7 \times \{0\}\}, Syl_3(\mathbb{Z}_7 \rtimes \mathbb{Z}_3) = \{\psi_{(i,0)}(\{0\} \times \mathbb{Z}_3) \mid i \in \mathbb{Z}_7\}, |Syl_3(\mathbb{Z}_7 \rtimes \mathbb{Z}_3)| = 7,$$

$$Syl_{11}(\mathbb{Z}_{11} \rtimes \mathbb{Z}_5) = \{\mathbb{Z}_{11} \times \{0\}\}, Syl_5(\mathbb{Z}_{11} \rtimes \mathbb{Z}_5) = \{\psi_{(i,0)}(\{0\} \times \mathbb{Z}_5) \mid i \in \mathbb{Z}_{11}\}, |Syl_5(\mathbb{Z}_{11} \rtimes \mathbb{Z}_5)| = 11.$$

□

1.12.

Další úlohy:

1. Popište až na izomorfismus všechny grupy řádu (a) 51, (b) 39.
2. Kolik existuje homomorfismů nekomutativní grupy řádu 21 do D_{14}?

9 Grupy řádu 8 a 12

9.1 Komutativní grupy

9.1. Popište (až na izomorfismus) všechny abelovské grupy řádu (a) 8, (b) 12, (c) 96.

(a) S využitím charakterizační věty popisujeme všechny možné direktní součiny cyklických grupa řádu 8. Protože $8 = 2^3$, jde nám o všechny možné rozklady exponentu 3 na součet kladných čísel, pro rozklady $3 = 3 = 1+2 = 1+1+1$ dostáváme 3 neizomorfní abelovské grupy řádu 8:

$$\mathbb{Z}_8, \quad \mathbb{Z}_2 \times \mathbb{Z}_4, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 = \mathbb{Z}_2^3.$$

(b) Nyní víme, že je dvanáctiprvková grupa součinem (Sylowovy) 2-grupy a 3-grupy grupy, proto máme právě dvě možnosti

$$\mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}, \quad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_2 \times \mathbb{Z}_6.$$

(c) Protože $96 = 2^5 \cdot 3$, potřebujeme uvážit všechny možné rozklady exponentu dvojky 5 na součet kladných čísel:

$$5 = 5 = 4+1 = 3+2 = 3+1+1 = 2+2+1 = 2+1+1+1 = 1+1+1+1+1.$$

Dostáváme celkem 7 neizomorfních abelovských grup řádu 96:

$$\mathbb{Z}_{32}\times\mathbb{Z}_3 \cong \mathbb{Z}_{96}, \ \mathbb{Z}_{16}\times\mathbb{Z}_2\times\mathbb{Z}_3 \cong \mathbb{Z}_{16}\times\mathbb{Z}_6, \ \mathbb{Z}_8\times\mathbb{Z}_4\times\mathbb{Z}_3 \cong \mathbb{Z}_8\times\mathbb{Z}_{12}, \ \mathbb{Z}_8\times\mathbb{Z}_2^2\times\mathbb{Z}_3 \cong \mathbb{Z}_2^2\times\mathbb{Z}_{24},$$

$$\mathbb{Z}_4^2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_4^2 \times \mathbb{Z}_6, \quad \mathbb{Z}_4 \times \mathbb{Z}_2^3 \times \mathbb{Z}_3 \cong \mathbb{Z}_2^3 \times \mathbb{Z}_{12}, \quad \mathbb{Z}_2^5 \times \mathbb{Z}_3 \cong \mathbb{Z}_2^4 \times \mathbb{Z}_6$$

□

9.2. Popište (až na izomorfismus) všechny abelovské grupy $\mathcal{G}$ řádu 32, pro něž (a) $\sigma_1(\mathcal{G}) \cong \mathbb{Z}_2$ (b) (b) $\sigma_1(\mathcal{G}) \cong \mathbb{Z}_2^2$, (c) $\sigma_1(\mathcal{G}) \cong \mathbb{Z}_2^3$.

Všimněme si, že $\sigma_1(\coprod_j H_j) \cong \mathbb{Z}_2 = \coprod_j \sigma_1(H_j)$ faktu, že právě cyklická 2-grupa má spodní vrstvu izomorfní grupě $\mathbb{Z}_2$.

(a) Existuje jediná grupa řádu $\mathcal{G}$ řádu 32, která je direktním součinem jediné cyklické grupy: $\mathbb{Z}_{32}$

(b) Tentokrát hledáme direktní součin dvou cyklických grup, který je řádu 32. Podmínku splňují grupy $\mathbb{Z}_{16} \times \mathbb{Z}_2$ a $\mathbb{Z}_8 \times \mathbb{Z}_4$.

(c) Analogicky najdeme direktní součiny tří cyklických grup, který je řádu 32: $\mathbb{Z}_8 \times \mathbb{Z}_2^2$ a $\mathbb{Z}_4^2 \times \mathbb{Z}_2$.

□

9.2 Neabelovské grupy řádu 8

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 $\mathcal{Q} = (Q, \cdot, ^{-1}, 1)$ grupu kvaternionů.

9.3. Nechť $\mathcal{G}$ je neabelovská grupa řádu 8. Dokažte, že

(a) obsahuje prvek řádu 4,

(b) jestliže $g \in G$ řádu 4 a $h \in G \setminus \langle h \rangle$ je řádu 2, pak je $\mathcal{G}$ izomorfní grupě D_8,

(c) jestliže $g \in G$ řádu 4 a všechny prvky $h \in G \setminus \langle g \rangle$ jsou řádu 4, pak $hgh^{-1} = g^3$, $h^2 = g^2$, $G = \langle g, h \rangle$ a $\mathcal{G}$ je izomorfní grupě $\mathcal{Q}$,

(d) $\mathcal{G}$ je izomorfní buď grupě D_8 nebo grupě $\mathcal{Q}$.

(a) Všechny prvky $\mathcal{G}$ jsou řádu 1, 2 či 4, grupa obsahující prvek řádu 8 už je nutně cyklická, tedy komutativní. Pokud by byly všechny prvky $\mathcal{G}$ řádu 1 nebo 2, tedy exponentu 2, pak by pro každou dvojici prvků $a, b \in G$ platilo

$$[a, b] = aba^{-1}b^{-1} = abab = (ab) = 1,$$

$a = a^{-1}$ a $b = b^{-1}$. Tedy taková grupa by byla abelovská.

(b) Stačí uvážit, že $\langle g \rangle \cap \langle h \rangle = \{1\}$, $\langle g \rangle\langle h \rangle = G$ a $\langle g \rangle \trianglelefteq G$, proto je podle 4.3 a Věty 4.7 z přednášky

$$G = \langle g \rangle\langle h \rangle \cong \langle g \rangle \rtimes \langle h \rangle \cong \mathbb{Z}_4 \rtimes \mathbb{Z}_2 \cong D_8.$$

(c) Protože je $\langle g \rangle$ normální podgrupa nekomutativní grupy a $hgh^{-1} \in \langle g \rangle$ je prvek řádu 3, dostáváme, že $hgh^{-1} = g^3 = g^{-1}$, proto $hg = g^{-1}h$ a $hg^i = g^{-i}h$. Dále $h^2 \in \langle g \rangle$ je prvek řádu 2, proto $h^2 = g^2$. Konečně $G = \langle g \rangle \cup \langle g \rangle h = \langle g, h \rangle$ a pro součin platí

$$g^i \cdot g^j = g^{i+j}, \quad g^i \cdot g^j h = g^{i+j}h, \quad g^i h \cdot g^j = g^{i-j}h, \quad g^i h \cdot g^j h = g^{i-j}h^2 = g^{i-j+2},$$

pro každé $i, j \in \mathbb{Z}$, z čehož plyne, že dvě grupy s prvkem $g_i \in G_i$ řádu 4, pro které jsou všechny prvky $h_i \in G \setminus \langle g \rangle$ řádu 4 pro $i = 1, 2$ jsou izomorfní, kde je izomorfismus určen zobrazením $g_1 \to g_2$, $h_1 \to h_2$. Tedy zobrazení $g \to i$, $h \to j$ určuje izomorfismus $G \to Q$.

(d) Nekomutativní grupa řádu 8 je popsána buď v bodu (b) nebo (c). První z nich je izomorfní D_8 a druhá $\mathcal{Q}$ □

8.12.

Další úlohy:

1. Popište až na izomorfismus všechny abelovské grupy řádu (a) 81, (b) 200.
2. Proč je každá grupa řádu 8 izomorfní právě jedné z grup $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, $\mathbb{Z}_2^3$, D_8 nebo $\mathcal{Q}$?
3. Které z výše uvedených grup je izomorfní grupa horních trojúhelníkových matic 3×3 nad tělesem $\mathbb{F}_2$?

10 Malé grupy

10.1 Grupy řádu 12

10.1. Dokažte pomocí Sylowových vět, že pro grupu $\mathcal{G}$ řádu 12 leží v $Syl_2 \cup Syl_3$ leží aspoň jedna normální podgrupa $\mathcal{G}$.

Označme $P_2 \in Syl_2$ a $P_3 \in Syl_3$. Ze Sylowových vět plyne, že

$$[G : N_G(P_2)] = |Syl_2| \equiv 1 \mod 2 \ \text{a}[G : N_G(P_3)] = |Syl_3| \equiv 1 \mod 3$$

Protože $P_p \trianglelefteq N_G(P_p)$, dostáváme $[G : N_G(P_p)]/[G : P_p]$ pro $p = 2, 3$, a proto $|Syl_2| \in \{1, 3\}$ a $|Syl_3| \in \{1, 2, 4\}$. Protože $[G : N_G(P_3)] = |Syl_3| \equiv 1 \mod 3$, vidíme, že $|Syl_3| \in \{1, 4\}$. Pokud $|Syl_3| = 1$, pak je P_3 normální podgrupa $\mathcal{G}$ a jsme hotovi.

Nyní předpokládejme, že P_3 není normální, tedy $|Syl_2| = 4$, což znamená, že máme 4 různé podgrupy prvočíselného řádu 3. Podle Lagrangeovy věty jsou jejich průniky triviální a v každé máme dva prvky řádu 3. Proto grupa $\mathcal{G}$ obsahuje aspoň $8 = 4 \cdot 2$ prvků řádu 3 a jeden prvek řádu 1. Zbývající 3 prvky, potom musí všechny ležet spolu s jednotkou ve čtyřprvkové grupě P_2, tudíž jde o jedinou podgrupu řádu 4 v $\mathcal{G}$. Proto $|Syl_2| = 1$ a P_2 je normální podgrupa $\mathcal{G}$. $\square$

10.2. Dokažte, že je každá neabelovská grupa řádu 12 izomorfní některému ze semidirektních součinů

$$\mathbb{Z}_2^2 \rtimes \mathbb{Z}_3, \mathbb{Z}_3 \rtimes \mathbb{Z}_2^2, \mathbb{Z}_3 \rtimes \mathbb{Z}_4.$$

Stačí využít Věty 4.7 z přednášky. Z předchozí úlohy víme, že ze Sylowových podgrup $P_2 \in Syl_2$ a $P_3 \in Syl_3$ je aspoň jedna normální a Lagrangeova věta nám říká, že $P_2 \cap P_3 = \{1\}$. Tedy

$$|P_2 P_3| = |P_2| \cdot |P_3| = 4 \cdot 3 = 12,$$

tedy $P_2P_3 = G$. Předpoklady Věty 4.7 jsou splněny, proto

$$\text{buď } \; G \cong P_2 \rtimes P_3, \quad \text{nebo } \; G \cong P_3 \rtimes P_2.$$

Protože P_2 je izomorfní $\mathbb{Z}_4$ nebo $\mathbb{Z}_2^2$ a P_3 je izomorfní $\mathbb{Z}_3$ máme 4 možnosti

$$\mathbb{Z}_4 \rtimes \mathbb{Z}_3, \quad \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3, \quad \mathbb{Z}_3 \rtimes \mathbb{Z}_4, \quad \mathbb{Z}_3 \rtimes \mathbb{Z}_2^2.$$

Konečně si uvědomme, že neexistuje žádný netriviální homomorfismus

$$\mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_4) \cong \mathbb{Z}_4^* \cong \mathbb{Z}_2,$$

dostáváme, že $\mathbb{Z}_4 \rtimes \mathbb{Z}_3 \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \cong \mathbb{Z}_{12}$, a proto se jedná o abelovskou grupu. □

10.3. Dokažte, že

(a) existují právě 3 neizomorfní neabelovské grupy řádu 12,

(b) žádná dvojice grup A_4, D_{12} a $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ není izomorfní,

(c) grupa řádu 12 je izomorfní právě jedné z grup $\mathbb{Z}_{12}$, $\mathbb{Z}_2 \times \mathbb{Z}_6$, A_4, D_{12} nebo nekomutativní grupě $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$.

(a) V úloze 10.2 jsme ukázali, že neabelovská grupa řádu 12 je izomorfní jedné z grup z množiny $M = \{\mathbb{Z}_2^2 \rtimes_{\phi_1} \mathbb{Z}_3, \mathbb{Z}_3 \rtimes_{\phi_2} \mathbb{Z}_2^2, \mathbb{Z}_3 \rtimes_{\phi_3} \mathbb{Z}_4\}$ pro netriviální homomorfismy ϕ_i, $i = 1, 2, 3$. Protože pro každé $i = 1, 2, 3$ existuje netriviální homomorfismus, jsou jim odpovídající semidirektní součiny neizomorfní, neboť každá z podgrup obsahuje jedinou normální Sylowovu podgrupu (Sylowovy podgrupy pro druhé prvočíslo nejsou normální, tedy jich je více), která je v prvním případě izomorfní grupě $\mathbb{Z}_3$, v druhém případě izomorfní grupě $\mathbb{Z}_2^2$ a v posledním případě je izomorfní grupě $\mathbb{Z}_4$.

Zbývá nahlédnout, že grupy až na izomorfismus nezávisí na volbě netriviálního homomorfismu ϕ_i. K tomu využijeme pozorování z přednášky po Poznámce 8.1. K tomu stačí ukázat, že pro všechny dvojice netriviálních homomorfismů

$$\phi_1, \overline{\phi_1} : \mathbb{Z}_3 \to \mathrm{Aut}(\mathbb{Z}_2^2) \cong S_3, \;\; \phi_2, \overline{\phi_2} : \mathbb{Z}_2^2 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2, \;\; \phi_3, \overline{\phi_3} : \mathbb{Z}_4 \to \mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2,$$

existují automorfismy $\sigma_1 \in \mathrm{Aut}(\mathbb{Z}_3)$, $\sigma_2 \in \mathrm{Aut}(\mathbb{Z}_2^2)$, $\sigma_3 \in \mathrm{Aut}(\mathbb{Z}_4)$, pro něž $\phi_i \sigma_i = \overline{\phi_i}$, $i = 1, 2, 3$.

V prvním případě vidíme, že ϕ_1, $\overline{\phi_1}$ jsou prosté a tříprvkový obraz jejich tříprvková obraz je jednoznačně určen, proto buď $\phi_1 = \overline{\phi_1}$ nebo $\phi_1 = \overline{\phi_1}(2 \cdot -)$. V druhém případě jsou oba homorfismy ϕ_2, $\overline{\phi_2}$ na celé $\mathrm{Aut}(\mathbb{Z}_3) \cong \mathbb{Z}_2$ a lineárně-algebraickou úvahou najdeme lineární bijekci $\sigma_2 \in \mathrm{Aut}(\mathbb{Z}_2^2)$, pro níž $\phi_2\sigma_2 = \overline{\phi_2}$. Konečně v posledním případě si stačí všimnout, že existuje pouze jediný netriviální homomorfismus ϕ_3

(b) O A_4 víme, že obsahuje čtyřprvkovou normální podgrupu, což o D_{12} neplatí (například proto, že obsahuje tříprvkovou normální podgrupu a kdyby obě Sylowovy podgrupy byly normální, pak by se jednalo o abelovskou grupu), tedy $A_4 \ncong D_{12}$. Grupa $\mathbb{Z}_3 \rtimes \mathbb{Z}_4$ jistě obsahuje prvek řádu 4, což neplatí ani o A_4 ani o D_{12}, tudíž $A_4 \ncong \mathbb{Z}_3 \rtimes \mathbb{Z}_4 \ncong D_{12}$. Na závěr poznamenejme, že $A_4 \cong \mathbb{Z}_2^2 \rtimes \mathbb{Z}_3$ a $D_8 \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2^2 \cong \mathbb{Z}_6 \rtimes \mathbb{Z}_2$, kde uvažujeme nekomutativní semidirektní součiny.

(c) Tvrzení už je přímým důsledkem předchozích úvah a úlohy 13.6. $\square$

10.2 Kompoziční řady

10.4. Určete nějakou kompoziční řadu grupy (a) $\mathbb{Z}_{30}$, (b) $\mathbb{Z}_{25}$ (c) $\mathbb{Z}_5^2$. Kolik kompoziční řad těchto grup existuje?

(a) Víme, že pro každý dělitel k čísla 30 je $\langle \frac{30}{k} \rangle$ jedin8 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 cyklické grupy prvočíselného řádu 2, 3 nebo 5, neboť $30 = 2 \cdot 3 \cdot 5$. Odtud plyne, že kompoziční řadu tvoří například řada 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 $\mathbb{Z}_{30}$.

(b) Protože $25 = 5^2$, stejnou úvahou jako v předchozí úloze 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.

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

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

kde $(a,b) \in \mathbb{Z}_5^2 \setminus \{(0,0)\}$. Abychom zjistili počet kompoziční řad, stačí určit počet různých přímek $\mathbb{F}_5^2$, kterých je právě $\frac{5^2-1}{5-1} = 6$. $\square$

10.5. Spočítejte všechny kompoziční řady symetrických grup S_n pro všechna $n \geq 5$.

Protože $S_n/A_n \cong \mathbb{Z}_2$ a A_n je jediná netriviální normální podgrupu grupy S_n, která je navíc jednoduchá, představuje jedinou kompoziční řadu grupy S_n pro $n \geq 5$ posloupnost $\{\{\mathrm{id}\}, A_n, S_n\}$. $\square$

15.12.

Další úlohy:

1. Které ze známých grup je izomorfní grupa $\mathbb{Z}_2 \times S_3$?
2. Spočítejte všechny kompoziční řady grupy a) $\mathbb{Z}_{18}$, b) D_8
3. Je-li $\{H_i\}_{i=0}^n$ kompoziční řada p-grupy řádu p^k, čemu se rovná n a jak vypadají faktory H_{i+1}/H_i.

11 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.

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

11.1. Dokažte pro prezentaci (X, R, π) grupy $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ a prvky $u, v \in F(X)$, že $u \cdot v^{-1} \in \ker \pi$, právě když $v^{-1} \cdot u \in \ker \pi$, právě když $\pi(u) = \pi(v)$.

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. $\square$

11.2. Najděte takový homomorfismus π, aby $(\{x\}, \{x^{20}\}, \pi)$ byla prezentace grupy $\mathbb{Z}_{20}$.

Okamžitě vidíme, že $\langle [x]^{20} \rangle \trianglelefteq F(x) = \langle [x] \rangle \cong \mathbb{Z}$, neboť volná grupa s jedním generátorem je cyklická. Protože $\pi([x]^k) = (k) \mathrm{mod}\ 20$ určuje homomorismus na grupu $\mathbb{Z}_{20}$ s jádrem rovným $\langle [x]^{20} \rangle$, je π hledaným homomorfismem. $\square$

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

Pro volnou grupu $F(\{x, y\})$ existuje (jednoznačně určený) homomorfismus $\pi : F(\{x, y\}) \to \mathbb{Z}^2$ splňující $\pi(x) = (1, 0)$ a $\pi(y) = (0, 1)$. Protože $\langle (1, 0), (0, 1) \rangle = \mathbb{Z}^2$, jedná o homomorfismus na celé $\mathbb{Z}^2$. Označme N nejmenší normální podgrupu obsahující $[x, y] = xyx^{-1}y^{-1}$. Ukážem, že hledanou prezentací je například trojice $(F(\{x, y\}), [x, y], \pi)$.

Nejprve si všimněme, že $N \subseteq \ker \pi$, protože $\pi[x,y] = [\pi(x), \pi(y)] \in \mathbb{Z}^2$ a $\mathbb{Z}^2$ je abelovská grupa. Podle Věty o homomorfismu existuje homomorfismus $\tilde{\pi} : F(\{x,y\})/N \to \mathbb{Z}^2$, který je na $\mathbb{Z}^2$ a platí $\tilde{\pi}(xN) = (1,0)$ a $\tilde{\pi}(yN) = (0,1)$. Navíc $\tilde{\pi}$ je izomorfismus, právě když $\ker \pi = N$. Ukážeme proto, že $\tilde{\pi}$ je izomorfismus.

Poznamenejme, že je grupa $F(\{x,y\})/N = \langle xN, yN \rangle$ komutativní, protože

$$xyx^{-1}y^{-1} \in N, \text{ tedy } xNyN = yNxN.$$

Protože je $\mathbb{Z}^2$ volná abelovská grupa, existuje homomorfismus $\psi : \mathbb{Z}^2 \to F(\{x,y\})/N$ splňující $\psi((1,0)) = xN$ a $\psi((0,1)) = xN$. To znamená, že

$$\psi\tilde{\pi}(xN) = xN, \psi\tilde{\pi}(yN) = yN \text{ a } \tilde{\pi}\psi(1,0) = (1,0), \tilde{\pi}\psi(0,1) = (0,1).$$

Zjistili jsme, že se obě složená zobrazení $\psi\tilde{\pi}$ i $\tilde{\pi}\psi$ shodují na generátorech s identickým zobrazením, proto už se jedná o identity. Tím jsme ověřili, že je $\tilde{\pi}$ izomorfismus, proto $\ker \pi = N$ a dostáváme tak prezentaci $(F(\{x,y\}), [x,y], \pi)$ grupy $\mathbb{Z}^2$.

Na závěr poznamenejme, že bychom mohli dokázat, že $N = F(\{x,y\})'$ a že homomorfismus π lze explicitně popsat 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}). $\square$

{

22.12.

Další úlohy:

1. Najděte nějakou prezentaci grupy (a) $\mathbb{Z}_2$, (b) $\mathbb{Z}$, (c) $\mathbb{Z}_{15}$.

12 Volné grupy

12.1 Normální podgrupy volné grupy a prezentace

12.1. Najděte takový homomorfismus π, aby

(a) $(\{x,y\}, \{x^3 = 1, y^5 = 1, xy = yx\}, \pi)$ byla prezentace grupy $\mathbb{Z}_{15}$,

(b) $(\{x,y\}, \{x^n = 1, y^2 = 1, yxy = x^{-1}\}, \pi)$ byla prezentace grupy D_{2n}.

(a) Využijeme-li homorfismus $\pi : F(\{x,y\}) \to \mathbb{Z}^2$ z úlohy 13.8, 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 $\tau(a,b) = (a \text{ mod}3, b \text{ mod}5)$. 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 $\mathbb{Z}_{15}$.

(b) Využijeme značení a výsledků úlohy 3.4, 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 3.4 vidíme, že $\ker\pi$ obsahuje relace $R = \{x^n, y^2, yxyx\}$ a jedná se o homomorfismus na. S využitím **??** 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}. □

12.2. 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), $F(x,y)/\text{Ker } f \cong S_6$ 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 $F(x,y)/\text{Ker } f \cong S_n$.

(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

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

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

12.2 Schreierova transversála

12.3. 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

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

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 pomocí srovnání obrazů $\varphi(s) = \varphi(t)$, kde s spočtené (rerdukované) slovo a $t \in T$ 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

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

□

5.1.

13 The best of ...

13.1 (1.3(b)). Spočítejte množiny $\mathrm{End}(\mathbb{Z}_n)$, $\mathrm{Aut}(\mathbb{Z}_n)$, $\mathrm{Inn}(\mathbb{Z}_n)$.

13.2 (3.2). Definujme podgrupu $A = \bigcup_n A_n$ grupy $S(\mathbb{N})$, kde A_n chápeme jako podgrupy $S(\mathbb{N})$. Dokažte, že je grupa A nekonečná jednoduchá.

13.3 (4.3). 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 $D_{2n} \cong \mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$.

13.4 (7.1). Najděte všechny Sylowovy podgrupy grupy (a) $\mathbb{Z}_{120}$ (b) S_3.

13.5 (8.1). Popište (až na izomorfismus) všechny grupy řádu
(a) 33, (b) 35, (c) 21, (d) 55.

13.6 (9.1). Popište (až na izomorfismus) všechny abelovské grupy řádu (a) 8, (b) 12, (c) 96.

13.7 (10.5). Spočítejte všechny kompoziční řady symetrických grup S_n pro všechna $n \geq 5$.

13.8 (11.3). Najděte nějakou prezentaci grupy $\mathbb{Z}^2$.

13.9 (12.2(c)). Nechť $F(x, y)$ je volná grupa o dvou generátorech a n buď přirozené. Ověřte, že existuje $N \trianglelefteq F(x, y)$, pro kterou $F(x, y)/N \cong S_n$.

Obsah