ÚVOD DO TEORIE GRUP

Obsah

1. Začínáme pěstovat grupy

T&N. $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je *grupa*, jestliže $\cdot$ je asociativní binární operace na G, $^{-1}$ unární operace a $1 \in G$ a pro každé $a, b \in G$ platí, že

$$a \cdot 1 = 1 \cdot a = a, \quad a \cdot a^{-1} = a^{-1} \cdot a = 1.$$

Je-li $\cdot$ komutativní mluvíme o abelovské grupě.

$|G|$ je *řád* grupy a řádem prvku $g \in G$ rozumíme nejmenší kladné n, pro něž $g^n = 1$, nebo ∞.

Příklad 1.1. Známé (a důležité) příklady grup:

(1) $(\mathbb{Z}, +, -, 0)$, $(\mathbb{Z}_n, +, -, 0)$ (cyklické grupy),
(2) $(S(X), \circ, ^{-1}, \mathrm{id})$, $(S_n, \circ, ^{-1}, \mathrm{id})$ (permutační grupy),
(3) $(GL_n(T), \cdot, ^{-1}, I_n)$ pro těleso T (grupy regulárních matic).

T&N. Nechť $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$ jsou pro $i = 1, 2$ grupy, pak řekneme, že je zobrazení $\varphi : G_1 \to G_2$

- *homomorfismus*, jestliže $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$ pro všechna $a, b \in G$,
- *izomorfismus*, je-li φ bijektivní homomorfismus,
- *endomorfismus*, je-li φ homomorfismus a $G_1 = G_2$,
- *automorfismus*, je-li φ bijektivní endomorfismus.

Date: 5. ledna 2021.

$\mathrm{Ker}\varphi = \{g \in G|\ \varphi(g) = 1\}$ se nazývá *jádro homomorfismu*. Existuje-li mezi grupami $\mathcal{G}_1$ a $\mathcal{G}_2$ izomorfismus, říkáme, že jsou *izomorfní* a píšeme $\mathcal{G}_1 \cong \mathcal{G}_2$.

Pozorování. Nechť $\varphi : G_1 \to G_2$ je homomorfismus grup $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$, $i = 1, 2$.

(1) $\varphi(1) = 1$ a $\varphi(a^{-1}) = (\varphi(a))^{-1}$ pro každé $a \in G_1$
(2) je-li φ izomorfismus, pak φ^{-1} je izomorfismus,
(3) zobrazení id_{G_1} a 1 dané vztahem $1(a) = 1$ jsou homomorfismy,
(4) zobrazení $\psi_g : G_1 \to G_1$ dané vztahem $\psi_g(h) = g \cdot h \cdot g^{-1}$ je izomorfismus, pro který $\psi_g^{-1} = \psi_{g^{-1}}$ a $\psi_1 = \mathrm{id}$.

T&N. Zobrazení ψ_g z pozorování (4) se nazývá *vnitřní automorfismus*.

Pro grupu $\mathcal{G}$ definujme množiny:
$\mathrm{End}(\mathcal{G}) := \{f : G \to G \mid f \text{ je endomorfismus}\}$,
$\mathrm{Aut}(\mathcal{G}) := \{f : G \to G \mid f \text{ je automorfismus}\}$
$\mathrm{Inn}(\mathcal{G}) := \{f : G \to G \mid f \text{ je vnitřní automorfismus}\}$.

Poznámka 1.2 (Cayley)**.** Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa a L_g značí pro každé $g \in G$ zobrazení určené předpisem $L_g(h) = gh\ \forall h \in G$. Pak je zobrazení $L : G \to S(G)$ dané vztahem $L(g) = L_g$ prostý homomorfismus.

T&N. Buď $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupa a $H \subseteq G$. Řekneme, že H je *podgrupa* $\mathcal{G}$ (píšeme $H \leq \mathcal{G}$), pokud pro každé $h, k \in H$ platí

$$h \cdot k \in H, \quad h^{-1} \in H, \quad 1 \in H.$$

Jestliže navíc $\psi_g(H) \subseteq H$ pro každé $hg \in G$, pak mluvíme o *normální podgrupě* (píšeme $H \trianglelefteq \mathcal{G}$).

Pozorování. Každá podgrupa tvoří s operací omezenou na svou nosnou množinu opět grupu.

Pozorování. Je-li $\varphi : G_1 \to G_2$ homomorfismus grup $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$, $i = 1, 2$, pak $\varphi(G_1) \leq \mathcal{G}_2$ a $\mathrm{Ker}\varphi \trianglelefteq \mathcal{G}_1$.

Důsledek 1.3. Každá konečná podgrupa je izomorfní podgrupě nějaké konečné symetrické grupy.

T&N. Je-li $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupa a $H, K \subseteq G$ a $a \in G$, definujme množiny

$$HK = \{h \cdot k|\ h \in H,\ k \in K\}, gH = \{g\}H, Hg = H\{g\}$$

a relace rmod H a lmod H na G :

$$(a, b) \in \text{rmod } H \Leftrightarrow a \cdot b^{-1} \in H$$

$$(a, b) \in \text{lmod } H \Leftrightarrow a^{-1} \cdot b \in H$$

Pozorování. Je-li $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupa a $H \leq \mathcal{G}$ pak

(1) rmod H i lmod H jsou ekvivalence na G,
(2) $(a, b) \in \text{rmod } H \Leftrightarrow (a^{-1}, b^{-1}) \in \text{lmod } H$ pro každé $a, b \in G$,
(3) $[a]_{\text{rmod } H} = Ha$ a $[a]_{\text{lmod } H} = aH$ pro každé $a \in G$,
(4) $\text{rmod } H = \text{lmod } H \Leftrightarrow H \trianglelefteq \mathcal{G} \Leftrightarrow aH = Ha\ \forall a \in G$.

Věta 1.4 (Lagrange)**.** Jestliže je H podgrupa grupy $\mathcal{G}$, pak
$$|G| = |H| \cdot [G : H],$$
kde $[G : H] = |G/\mathrm{rmod}\ H| = |G/\mathrm{lmod}\ H|$.

Poznámka 1.5 (Zobecněná Cayleyho věta)**.** Nechť $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa, $H \leq \mathcal{G}$ a $\tilde{L}_g$ značí pro každé $g \in G$ zobrazení určené předpisem $\tilde{L}_g(aH) = gaH\ \forall aH \in G/\mathrm{lmod}\ H$. Pak je zobrazení $\tilde{L} : G \to S(G/\mathrm{lmod}\ H)$ dané vztahem $\tilde{L}(g) = \tilde{L}_g$ homomorfismus a platí, že $\mathrm{Ker}\tilde{L} \leq H$.

2. Faktorizovat či nefaktorizovat?

Celou přednášku předpokládáme, že $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa.

Připomeňme, kdy pro $H \leq \mathcal{G}$ splývají dvě ekvivalence lmod H a rmod H:

Pozorování. $H \trianglelefteq \mathcal{G} \Leftrightarrow \mathrm{rmod}\ H = \mathrm{lmod}\ H \Leftrightarrow aH = Ha\ \forall a \in G$.

T&N. Nechť $H \trianglelefteq \mathcal{G}$.

Označme $\mathrm{mod}\ H := \mathrm{rmod}\ H = \mathrm{lmod}\ H$ a $G/H := G/\mathrm{mod}\ H$.

Na G/H definujme (faktorové) operace $aH \cdot bH = abH$ a $(aH)^{-1} = a^{-1}H$ pro $a, b \in G$.

Zobrazení $\pi_H : G \to G/H$ dané předpisem $\pi_H(a) = aH$ je *přirozená projekce.*

Pozorování. Jestliže $H \trianglelefteq \mathcal{G}$, pak $\mathcal{G}/H := (G/H, \cdot, ^{-1}, H)$ je grupa s výše zavedenými operacemi a $\pi_H : G \to G/H$ je homomorfismus.

Poznámka 2.1. Nechť $\sim$ je ekvivalence na G, $H := [1]_\sim$ a $\pi : G \to G/\sim$ je dané $\pi(a) = [a]_\sim$ pro všechna $a \in G$. Je-li $(G/\sim, \cdot, ^{-1}, H)$ grupa, pro níž je π homomorfismus, pak $H \trianglelefteq \mathcal{G}$ a ekvivalence $\sim$ a mod H splývají.

T&N. Grupa $\mathcal{G}$ se nazývá *jednoduchá*, má-li pouze triviální normální podgrupy $\{1\}$ a G.

Příklad 2.2. Příklady jednoduchých grup:

(1) $(\mathbb{Z}_p, +, -, 0)$ pro p prvočíslo,
(2) $(A_n, \circ, ^{-1}, \mathrm{id})$ pro přirozená $n \neq 4$ *(cvičení)*,
(3) (nekonečná) podgrupa $A = \bigcup_n A_n$ grupy $S(\mathbb{N})$, kde A_n chápeme jako podgrupu $S(\mathbb{N})$ *(cvičení)*.

Pozorování. Nechť $\mathcal{S} = (S, \cdot, ^{-1}, 1)$ je jednoduchá aspoň dvouprvková grupa a $\varphi : S \to G$ je homomorfismus. Pak $\varphi(S) \neq 1 \Leftrightarrow \mathrm{Ker}\varphi \neq S \Leftrightarrow \mathrm{Ker}\varphi = \{1\} \Leftrightarrow \varphi$ je prostý.

Poznámka 2.3. Buď $\mathcal{G}$ jednoduchá grupa a H její vlastní podgrupa.

(1) Jestiže $n = [G : H] < \infty$, pak existuje prostý homomorfismus $\mathcal{G}$ do grupy S_n.
(2) Je-li $\mathcal{G}$ nekonečná, pak $[G : H]$ je nekonečný.

Věta 2.4. Nechť $\varphi : G_1 \to G_2$ je homomorfismus grup $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$, $i = 1, 2$.

(1)(Věta o homomorfismu) Je-li $H \trianglelefteq \mathcal{G}_1$, pak existuje homomorfismus $\psi : G_1/H \to G_2$ splňující podmínku $\psi\pi_H = \varphi$ právě tehdy, když $H \subseteq \mathrm{Ker}\varphi$. Navíc, jestliže ψ existuje, je ψ izomorfismus, právě když φ je na a $\mathrm{Ker}\varphi = H$.

(2)(1. věta o izomorfismu) $\varphi(G_1)$ je podgrupa $\mathcal{G}_2$ a zobrazení $a\mathrm{Ker}\varphi \to \varphi(a)$ je izomorfismus grup $G_1/\mathrm{Ker}\varphi$ a $\varphi(G_1)$.

Věta 2.5. Nechť $H \leq \mathcal{G}$ a $N \trianglelefteq \mathcal{G}$.

(1)(2. věta o izomorfismu) Je-li $N \leq H \trianglelefteq \mathcal{G}$, pak $H/N \trianglelefteq \mathcal{G}/N$ a $\mathcal{G}/H \cong (\mathcal{G}/N)/(H/N)$.

(2)(3. věta o izomorfismu) $HN \leq G$ a zobrazení $a(H \cap N) \to aN$ je izomorfismus grup $H/(H \cap N)$ a HN/N.

Pozorování. $(\mathrm{Aut}(\mathcal{G}), \circ, ^{-1}, \mathrm{id})$ je grupa a $\mathrm{Inn}(\mathcal{G}) \trianglelefteq \mathrm{Aut}(\mathcal{G}) \leq S(G)$.

T&N. Uvažme grupy indukované grupou $\mathcal{G}$:
- $(\mathrm{Aut}(\mathcal{G}), \circ, ^{-1}, \mathrm{id})$ je *grupa automorfismů*,
- $(\mathrm{Inn}(\mathcal{G}), \circ, ^{-1}, \mathrm{id})$ je *grupa vnitřních automorfismů*,
- $\mathrm{Out}(\mathcal{G}) := \mathrm{Aut}(\mathcal{G})/\mathrm{Inn}(\mathcal{G})$ je *grupa vnějších automorfismů*,
- $Z(\mathcal{G}) := \{a \in G \mid ag = ga \forall g \in G\} = \{a \in G \mid \psi_a(g) = g \forall g \in G\}$ je *centrum* grupy $\mathcal{G}$.

Věta 2.6. $Z(\mathcal{G}) \trianglelefteq \mathcal{G}$ a $\mathcal{G}/Z(\mathcal{G}) \cong \mathrm{Inn}(\mathcal{G})$.

Příklad 2.7. Příklady center a grup vnitřních automorfismů:

(1) Je-li $\mathcal{G}$ abelovská, pak $Z(\mathcal{G}) = G$ a $\mathrm{Inn}(\mathcal{G}) = \{\mathrm{id}\}$,
(2) Je-li $\mathcal{G}$ jednoduchá neabelovská, pak $Z(\mathcal{G}) = \{1\}$ a $\mathrm{Inn}(\mathcal{G}) \cong G$, tedy $\mathrm{Inn}(A_n) \cong A_n$ pro $n > 4$
(3) $Z(S_n) = \{\mathrm{id}\}$ a $\mathrm{Inn}(S_n) \cong S_n$ pro $n > 2$,
(4) $Z(GL_n(T)) = \{tI_n \mid t \in T^*\}$ a $\mathrm{Inn}(S_n) \cong GL_n(T)/Z(GL_n(T))$ pro těleso T.

3. Cesta do středu grupy

Celou přednášku opět předpokládáme, že $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa, dále, že n je přirozené číslo a p prvočíslo.

Příklad 3.1 (Geometrické grupy)**.** (1) Připomeňme, že afinní bijektivní zobrazení $T_{a,A}$ afinního prostoru $\mathbb{R}^n$ do sebe je jednoznačně určeno obrazem a (například) počátku $\mathbf{0}$ a regulární maticí $A \in GL_n(\mathbb{R})$:
$$T_{a,A}(b) = a + Ab.$$
Množina všech afinních bijekcí $A(n, \mathbb{R}) = \{T_{a,A} \mid a \in \mathbb{R}^n, A \in GL_n(\mathbb{R})\}$ tvoří spolu se skládáním, inverzním zobrazením a identitou grupu.

(2) Označíme-li $O_n(\mathbb{R})$ podgrupu všech ortogonálních matic grupy $GL_n(\mathbb{R})$ a $SO_n(\mathbb{R}) = \{U \in O_n(\mathbb{R}) \mid \det U = 1\}$, pak
$$E(n, \mathbb{R}) = \{T_{a,U} \mid a \in \mathbb{R}^n, U \in O_n(\mathbb{R})\},$$
$$O(n, \mathbb{R}) = \{T_{0,U} \mid U \in O_n(\mathbb{R})\}, SO(n, \mathbb{R}) = \{T_{0,U} \mid U \in SO_n(\mathbb{R})\}$$
jsou postupně množiny všech izometrií (eukleidovských transformací), izometrií zachovávajících počátek a izometrií zachovávajících počátek a orientaci a platí
$$SO(n, \mathbb{R}) \trianglelefteq O(n, \mathbb{R}) \leq E(n, \mathbb{R}) \leq A(n, \mathbb{R}),$$
$$O(n, \mathbb{R}) \cong O_n(\mathbb{R}), SO(n, \mathbb{R}) \cong SO_n(\mathbb{R}) \text{ a } [O(n, \mathbb{R}) : SO(n, \mathbb{R})] = 2$$

T&N. Je-li Δ_n je pravidelný n-úhelník v eukleidovské rovině $\mathbb{R}^2$ se středem v počátku $\mathbf{0}$, definujme *dihedrální grupu*

$$D_{2n} = \{\sigma \in O(2,\mathbb{R}) \mid \sigma(\Delta_n) = \Delta_n\} \leq O(2,\mathbb{R})$$

Pozorování. Nechť $s \in D_{2n}$ je rotace o úhel $\frac{2\pi}{n}$ a $t \in D_{2n}$ osová symetrie Δ_n a V je množina vrcholů pravidelného n-úhelníku Δ_n, pak

(1) $D_{2n} = \langle s, t\rangle = \langle s\rangle \cup t\langle s\rangle = \{t^i s^j \mid i = 0, 1, j = 0, \dots, n-1\}$,
(2) $|D_{2n}| = 2n$, $[D_{2n} : \langle s\rangle] = 2$ a $\langle s\rangle \trianglelefteq D_{2n}$,
(3) $s^n = \mathrm{id} = t^2$, $tst = s^{-1}$
(4) zobrazení $\sigma \to \sigma|_V$ je prostý homomorfismus $D_{2n} \to S(V)(\cong S_n)$,
(5) $D_{2n} \cong \langle (12\dots n), (2\ n)(3\ n-1)\dots\rangle \leq S_n$.

D_{2n} budeme díky (4) a (5) často ztotožňovat s příslušnou podgrupou S_n.
Víme, že relace $\leq$ je tranzitivní, což obecně neplatí pro $\trianglelefteq$:

Příklad 3.2. Uvažujme $D_8 = \langle (1234), (24)\rangle \leq S_4$. Pak

$$\langle (24)\rangle \trianglelefteq \langle (13), (24)\rangle \trianglelefteq D_8, \quad \text{zatímco} \quad \langle (24)\rangle \ntrianglelefteq D_8.$$

Strukturu faktorové grupy nějaké normální podgrupy $N \trianglelefteq \mathcal{G}$ tedy nemusí být vždy možné rozšířit na strukturu faktorové grupy grupy $\mathcal{G}$.

T&N. Nechť $H \leq \mathcal{G}$, řekneme, že
- H je *charakteristická podgrupa* grupy $\mathcal{G}$ ($H \leq_{\mathrm{char}} \mathcal{G}$), jestliže $\varphi(H) \subseteq H$ $\forall \varphi \in \mathrm{Aut}(\mathcal{G})$,
- H je *úplně charakteristická podgrupa* grupy $\mathcal{G}$ ($H \leq_{\mathrm{fi}} \mathcal{G}$), jestliže $\varphi(H) \subseteq H$ $\forall \varphi \in \mathrm{End}(\mathcal{G})$.

Pozorování. Úplně charakteristická podgrupa je nutně charakteristická a charakteristická podgrupa je nutně normální.

Poznámka 3.3. Nechť $H \leq K \leq \mathcal{G}$ a H je charakteristická podgrupa grupy K.

(1) Jestliže $K \trianglelefteq \mathcal{G}$, pak $H \trianglelefteq \mathcal{G}$,
(2) jestliže je K charakteristická podgrupa $\mathcal{G}$, pak H je charakteristická podgrupa $\mathcal{G}$,
(3) jestliže je K úplně charakteristická podgrupa $\mathcal{G}$ a H je úplně charakteristická podgrupa grupy K, pak je i H úplně charakteristická podgrupa $\mathcal{G}$.

Poznámka 3.4. $Z(G)$ je charakteristická podgrupa grupy $\mathcal{G}$.

T&N. Je-li X množina, říkáme *akce* (působení) grupy $\mathcal{G}$ na množině X každému homomorfismu $\varphi : G \to S(X)$, je-li Je-li φ prosté mluvíme o *věrné* akci. Pro pevné φ a $g \in G$, $x \in X$ píšeme $g(x)$ místo $\varphi(g)(x)$. Akce určuje ekvivalenci $\sim$ na X danou podmínkou $x \sim y$, jestliže existuje $g \in G$, pro něž $g(x) = y$. Pro $x \in X$ je $[x] = [x]_\sim$ *orbita* prvku x a $G_x = \{g \in G \mid g(x) = x\}$ *stabilizátor* prvku x.

Pozorování. Mějme akci grupy $\mathcal{G}$ na množině X a nechť $x \in X$, $H \leq G$ a $g \in G$.

(1) $\psi_g(G_x) = G_{g(x)}$,
(2) $\psi_g(H) = G_x \Leftrightarrow H = G_{g^{-1}(x)} \Leftrightarrow \exists y \in [x] : H = G_y$,
(3) $G_x \leq \mathcal{G}$ a $[G : G_x] = |[x]|$.

S využitím akce grupy $\mathbb{Z}_p$ cyklickým posunutí složek na množině

$$\{(g_0, \dots, g_{p-1} \in G^p \mid \prod g_i = 1)\}$$

byla v Algebře 2 dokázána důležitá věta:

Věta 3.5 (Cauchy)**.** Jestliže p dělí řád konečné grupy G, pak $\mathcal{G}$ obsahuje prvek řádu p.

T&N. $\mathcal{G}$ se nazývá *p-grupa*, je-li každý její prvek řádu p^k pro nějaké nezáporné celé k.

Důsledek 3.6. Konečná p-grupa je řádu p^n pro nějaké nezáporné celé n.

Příklad 3.7. Homomorfismus $\psi : G \to \mathrm{Inn}(G) \leq S(G)$, $\psi(g) = \psi_g$ z 2.6 lze chápat jako akci grupy $\mathcal{G}$ na množině G, která je věrná právě když $Z(\mathcal{G}) = \mathrm{Ker}\psi = \{1\}$.

T&N. Akce z předchozího příkladu se nazývá *akce konjugace* a stabilizátor $C_g(\mathcal{G}) = G_g$ nazývá *centralizátor* prvku $g \in G$.

Pozorování. Pro akci konjugace grupy $\mathcal{G}$ a $g \in G$ platí, že

(1) $[g]$ obsahuje všechny prvky konjugované s g,
(2) $|[g]| = [G : C_g(\mathcal{G})]$,
(3) $g \in Z(G) \Leftrightarrow |[g]| = 1$.

Věta 3.8. Je-li $\mathcal{G}$ konečná p-grupa a $|G| > 1$, pak $Z(\mathcal{G}) \neq \{1\}$.

Důsledek 3.9. Jestliže $|G| = p^2$, pak je $\mathcal{G}$ abelovská.

Důsledek 3.10. Konečná netriviální p-grupa je jednoduchá, právě když je řádu p.

4. Skládáme grupu: direktní a semidirektní součin

Celou přednášku předpokládáme, že I je neprázdná (indexová) množina, a že pro $i \in I$ $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$ a $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ jsou grupy.

T&N. Na kartézském součinu $\prod_{i\in I} G_i = \{f : I \to \bigcup_{i\in I} G_i \mid f(i) \in G_i\}$ definujeme operace „po složkách", tj. pro $f, g \in \prod_{i\in I} G_i$:

$$(f \cdot g)(i) = f(i) \cdot g(i), \quad (f^{-1})(i) = f(i)^{-1}, \quad \mathbf{1}(i) = 1 \in G_i \quad \forall i \in I$$

Množinu

$$\coprod_{i\in I} G_i = \{f \in \prod_{i\in I} G_i \mid |\{i \in I \mid f(i) \neq 1\}| < \infty\}$$

budeme nazývat *direktní součin* systému grup $(\mathcal{G}_i \mid i \in I)$. Pro každé $j \in I$ označme $\mu_j : G_j \to \coprod_{i\in I} G_i$ zobrazení dané podmínkou $[\mu_j(g)](i) \begin{cases} = g, & \text{pokud } i = j \\ = 1, & \text{pokud } i \neq j \end{cases} \forall g \in G$. Dále $\langle X \rangle = \bigcap\{H \leq \mathcal{G} \mid X \subseteq H\}$ značí podgrupu generovaná množinou $X \subseteq G$.

Pozorování. Pro každé $j \in I$ platí:

(1) $(\prod_{i\in I} G_i, \cdot, ^{-1}, \mathbf{1})$ je grupa a $\coprod_{i\in I} G_i$ její normální podgrupa,
(2) $\prod_{i\in I} G_i = \coprod_{i\in I} G_i \Leftrightarrow \{i \in I \mid G_i \neq \{1\}\}$ je konečná,
(3) $\prod_{i\in I} G_i$ je abelovská $\Leftrightarrow \coprod_{i\in I} G_i$ je abelovská $\Leftrightarrow G_i$ jsou abelovské $\forall i \in I$,

(4) μ_j je prostý homomorfismus a $G_j \cong \mu_j(G_j) \trianglelefteq \coprod_{i\in I} G_i$,
(5) $\mu_j(G_j) \cap \langle \bigcup_{i\neq j} \mu_i(G_i)\rangle = \{1\}$ a $\langle \bigcup_{i\in I} \mu_i(G_i)\rangle = \coprod_{i\in I} G_i$.

T&N. Grupy z předchozího pozorování značíme

$$\prod_{i\in I} \mathcal{G}_i = (\prod_{i\in I} G_i, \cdot, ^{-1}, \mathbf{1}), \quad \coprod_{i\in I} \mathcal{G}_i = (\coprod_{i\in I} G_i, \cdot, ^{-1}, \mathbf{1}).$$

Příklad 4.1. Nechť $I = \mathbb{N}$ a $G_i = \mathbb{Z}_2 \forall i \in \mathbb{N}$.

Označme $\mathcal{P}(\mathbb{N})$ množinu všech podmnožin $\mathbb{N}$, $\mathcal{P}_{<\infty}(\mathbb{N})$ množinu všech konečných podmnožin $\mathbb{N}$ a $\div$ symetrickou diferenci, tj. $A \div B := (A \cup B) \setminus (A \cap B)$. Potom
$\prod_{i\in\mathbb{N}} \mathcal{G}_i = \prod_{i\in\mathbb{N}} \mathbb{Z}_2 \cong$ nekonečné posloupnosti prvků $\mathbb{Z}_2 \cong (\mathcal{P}(\mathbb{N}), \div, \mathrm{id}, \emptyset)$,
$\coprod_{i\in\mathbb{N}} \mathcal{G}_i = \coprod_{i\in\mathbb{N}} \mathbb{Z}_2 \cong$ skoro všude nulové posloupnosti prvků $\mathbb{Z}_2 \cong (\mathcal{P}_{<\infty}(\mathbb{N}), \div, \mathrm{id}, \emptyset)$,
kde na posloupnostech uvažujeme grupovou operaci definovanou po složkách.

T&N. Pro $a, b \in G$ a $A, B \leq \mathcal{G}$ značme

$$[a, b] = aba^{-1}b^{-1}, \quad [A, B] = \langle\{[a, b] \mid a \in A\, b \in B\}\rangle, G' = [G, G].$$

Prvek $[a, b]$ nazýváme *komutátor* prvků a, b a podgrupu $G' = [G, G]$ *komutant.*

Pozorování. Pro $a, b \in G$, $A, B \leq \mathcal{G}$, $\varphi \in \mathrm{End}(\mathcal{G})$ a $N \trianglelefteq \mathcal{G}$ platí:
(1) $[a, b] = 1 \Leftrightarrow ab = ba$,
(2) $\varphi([a, b]) = [\varphi(a), \varphi(b)]$, $\varphi([A, B]) \subseteq [\varphi(A), \varphi(B)]$ a $\varphi(G') \subseteq G'$,
(3) $A' \leq G'$ a $(G/N)' = (G'N)/N$.

Poznámka 4.2. Nechť $a \in G$ a $N \trianglelefteq \mathcal{G}$.
(1) G' je úplně charakteristická podgrupa $\mathcal{G}$,
(2) $[a, g] \in N$ pro všechna $g \in G \Leftrightarrow aN \in Z(G/N)$,
(3) $\mathcal{G}/N$ je abelovská $\Leftrightarrow G' \leq N$,
(4) $\mathcal{G}/G'$ je abelovská.

Poznámka 4.3. Jsou-li $H, K \trianglelefteq \mathcal{G}$, pro něž $H \cap K = \{1\}$, pak $hk = kh$ pro všechna $h \in H, k \in K$.

Věta 4.4 (Vnitřní součin). Nechť $G_i \trianglelefteq \mathcal{G}$ všechna $i \in I$. Jestliže $G_j \cap \langle \bigcup_{i\neq j} G_i\rangle = \{1\}$ pro všechna $j \in I$ a $\langle \bigcup_{i\in I} G_i\rangle = G$, pak je zobrazení $\alpha : \coprod_{i\in I} G_i \to G$ dané předpisem $\alpha(f) = \prod_{i:f(i)\neq 1} f(i)$ je izomorfismus.

T&N. Systém podgrup z předchozí věty se nazývá (vnitřní) *direktní rozklad.* Pokud neexistuje žádný direktní rozklad s aspoň jednou netriviální podgrupou G_i (tj. takovou, že $\{1\} \neq G_i \neq G$) je grupa *direktně nerozložitelná.*

Pozorování. $\langle \bigcup_{i=1}^n G_i\rangle = G_1 \dots G_n = \{g_1 \dots g_n \mid g_i \in G_i \forall i\}$, jestliže $G_i \trianglelefteq \mathcal{G}$ pro $i = 1, \dots, n$

Příklad 4.5. $\mathbb{Z}_{30} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times Z_5$ podle Čínské věty o zbytcích a zároveň je tedy $\mathbb{Z}_{30}$ vnitřním direktním součinem svých podgrup $\langle 15\rangle$, $\langle 10\rangle$ $\langle 5\rangle$:

$$\langle 15\rangle + \langle 10\rangle + \langle 6\rangle = \mathbb{Z}_{30} \cong \coprod_{i=15,10,6} \langle i\rangle.$$

Poznámka 4.6. Nechť $\mathcal{H} = (H, \cdot, ^{-1}, 1)$ a $\mathcal{K} = (K, \cdot, ^{-1}, 1)$ jsou grupy a $\varphi : K \to \mathrm{Aut}(H)$ je homomorfismus. Označme $\hat{H} = H \times \{1\}$, $\hat{K} = \{1\} \times K$, $\varphi_k = \varphi(k)$ pro všechna $k \in K$ a na $H \times K$ definujme operace:

$$(h_1, k_1) \cdot (h_2, k_2) = ((h_1 \varphi_{k_1}(h_2), k_1 k_2)), \quad (h_1, k_1)^{-1} = (\varphi_{k_1^{-1}}(h_1^{-1}), k_1^{-1}).$$

Potom $(H \times K, \cdot, ^{-1}, (1,1))$ je grupa, $\hat{H}$ její normální podgrupa, $\hat{K}$ její podgrupa a $G/\hat{H} \cong \hat{K} \cong K$.

T&N. Grupa $\mathcal{H} \rtimes_\varphi \mathcal{K} := (H \times K, \cdot, ^{-1}, (1,1))$ z 4.6 se nazývá *semidirektní součin* grup.

Věta 4.7. Nechť $H \trianglelefteq \mathcal{G}$, $K \leq \mathcal{G}$, $H \cap K = \{1\}$ a $HK = G$. Potom je zobrazení $\varphi : K \to \mathrm{Aut}(H)$ dané pro $k \in K$ vztahem $\varphi(k) = \psi_k|_H \in \mathrm{Aut}(H)$ homomorfismus a zobrazení $\alpha : H \rtimes_\varphi K \to G$ určené předpisem $\alpha((h,k)) = hk$ je izomorfismus.

T&N. Podgrupy H a K z předchozí věty se nazývají (vnitřní) *semidirektní rozklad.* Pokud neexistuje semidirektní rozklad s netriviální podgrupou K (tj. takovou, že $\{1\} \neq K \neq G$) je grupa *semidirektně nerozložitelná.*

Příklad 4.8. Buď $n > 2$ přirozené číslo.

(1) $A_n \trianglelefteq S_n$, $\langle(12)\rangle \leq S_n$, $A_n \cap \langle(12)\rangle = \{\mathrm{id}\}$ a $A_n\langle(12)\rangle = S_n$, proto podle právě dokázané věty $S_n \cong A_n \rtimes_\varphi \langle(12)\rangle$, pro $\varphi((12)^i) = \psi_{(12)^i}|_{A_n}$.

(2) Uvážíme-li prostý homomorfismus $\psi : \mathbb{Z}_2 \to \mathrm{Aut}(\mathbb{Z}_n)$, kde

$$[\psi(i)](j) = ((-1)^i j) \bmod n,$$

pak je $\mathbb{Z}_n \rtimes_\varphi \mathbb{Z}_2$ je grupa izomorfní dihedrální grupě D_{2n}.

(3) Označíme-li $P(n,\mathbb{R}) = \{T_{a,I_n} \in E(n,\mathbb{R}) \mid a \in \mathbb{R}^n\}$, pak

$$E(n,\mathbb{R}) = P(n,\mathbb{R})O(n,R) \cong P(n,\mathbb{R}) \rtimes O(n,R) \cong \mathbb{R}^n \rtimes_\tau O(n,R),$$

kde $\tau : O(n,R) \to \mathbb{R}^n$ je určeno $\tau(T_{0,U})(\mathbf{v}) = U\mathbf{v}$.

5. Do řady! Po podgrupách nahoru a zase dolů.

Celou přednášku opět předpokládáme, že $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ je grupa a n nezáporné celé číslo.

T&N. Induktivně konstruujme posloupnost *iterovaných komutantů* (derivovaných podgrup) $\{G^{(i)}\}_{i \geq 0}$ grupy $\mathcal{G}$:

$$G^{(0)} = G, \quad G^{(i)} = (G^{(i-1)})' \quad \forall i > 0.$$

Jestliže existuje n, pro které $G^{(n)} = \{1\}$ a n je nejmenší možné, pak je grupa $\mathcal{G}$ *řešitelná* stupně (řešitelnosti) n a $\{G^{(i)}\}_{i=0}^n$ se nazývá *derivovaná řada* grupy.

Příklad 5.1. (1) Každá abelovská i metabelovská grupa je řešitelná.

(2) Grupa S_4 je řešitelná stupně 3 s derivovanou řadou $\{S_4, A_4, K, \{\mathrm{id}\}\}$, kde $K = \{\mathrm{id}, (12)(34), (13)(24), (14)(23)\}$, zatímco žádná z grup S_n pro $n > 4$ řešitelná není.

Pozorování. Pro $H \leq G$, $N \trianglelefteq \mathcal{G}$, $i, j \geq 1$ a $\varphi \in \mathrm{End}(\mathcal{G})$ platí:

(1) $\varphi(G^{(i)}) = \varphi(G)^{(i)} \subseteq G^{(i)}$,

(2) $G^{(i)} \leq_{\text{fi}} \mathcal{G}$ a $G^{(i-1)}/G^{(i)}$ je abelovská,
(3) $H^{(i)} \leq G^{(i)}$ a $(G/N)^{(i)} = (G^{(i)}N)/N$,
(4) $(G^{(i)})^{(j)} = G^{(i+j)}$.

Poznámka 5.2. Nechť $H \leq \mathcal{G}$ a $N \trianglelefteq \mathcal{G}$.

(1) Jestliže je $\mathcal{G}$ je řešitelná stupně n, pak H i $\mathcal{G}/N$ jsou řešitelné stupně nejvýše n.
(2) $\mathcal{G}$ je řešitelná, právě když N i $\mathcal{G}/N$ jsou řešitelné.

Důsledek 5.3. Semidirektní součin řešitelných grup je řešitelná grupa.

T&N. Posloupnost podgrup $\{H_i\}_{i=0}^n$ se nazývá *subnormální řada* grupy $\mathcal{G}$, jestliže

$$H_0 = \{1\},\ H_n = G \text{ a } H_{i-1} \trianglelefteq H_i \quad \forall i = 1, \dots, n.$$

Věta 5.4. $\mathcal{G}$ je řešitelná stupně nejvýše n, právě když existuje její subnormální řada $\{H_i\}_{i=0}^n$, pro níž jsou všechny faktory H_i/H_{i-1}, $i = 1, \dots, n$, abelovské.

Poznámka 5.5. Nechť $N \leq K$ jsou podgrupy grupy $\mathcal{G}$. Je-li $N \leq_{\text{char}} \mathcal{G}$ a $K/N \leq_{\text{char}} \mathcal{G}/N$, pak i $K \leq_{\text{char}} \mathcal{G}$.

T&N. Induktivně konstruujme posloupnost *iterovaných center* $\{\vartheta_i(G)\}_{i \geq 0}$ grupy $\mathcal{G}$:

$$\vartheta_0(G) = \{1\} \text{ a } \vartheta_i(G) = \pi_{i-1}^{-1}(Z(\mathcal{G}/\vartheta_{i-1}(\mathcal{G}))) \quad \forall i > 0,$$

kde $\pi_{i-1} : G \to \mathcal{G}/\vartheta_{i-1}(\mathcal{G})$ je přirozená projekce.

Jestliže existuje n, pro které $\vartheta_n(G) = G$ a n je nejmenší možné, pak je grupa $\mathcal{G}$ *nilpotentní* stupně (nilpotence) n a $\{\vartheta_i(G)\}_{i=0}^n$ se nazývá *horní centrální řada* grupy.

Pozorování. Pro $i \geq 1$ platí, že

(1) $\vartheta_i(G) \leq_{\text{char}} \mathcal{G}$,
(2) $\vartheta_i(G)/\vartheta_{i-1}(\mathcal{G})) = Z(\mathcal{G}/\vartheta_{i-1}(\mathcal{G}))$ proto $\vartheta_i(G)/\vartheta_{i-1}(\mathcal{G}))$ je abelovská.

Příklad 5.6. (1) Každá abelovská grupa je nilpotentní.

(2) Grupa S_n není nilpotentní pro žádné $n > 2$, neboť $Z(S_n) = \{\mathrm{id}\}$.

(3) Nechť $\mathcal{G}$ je konečná aspoň dvouprvková p-grupa. Pak $Z(\mathcal{G}) \neq \{1\}$ podle 3.8 a $G/Z(G)$ je opět p-grupa podle 1.4, menšího řádu než $\mathcal{G}$. Indukcí dostaneme, že konečné p-grupy jsou nilpotentní.

(4) D_{2n} je nilpotentní, právě když je n mocnina dvojky.

Věta 5.7. Každá nilpotentní grupa stupně n je řešitelná stupně nejvýše n.

Uvědomme si, že charakterizace nilpotence pomocí subnormálních řad, tedy obdoba tvrzení 5.2(2) a 5.3 neplatí:

Příklad 5.8. Grupa $S_3 \cong D_6$ je semidirektním součinem komutativních (tedy nilpotentních) grup $\mathbb{Z}_3$ a $\mathbb{Z}_2$, který není nilpotentní.

6. Sylowovy podgrupy - kladivo na konečné grupy

Celou přednášku značí $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ tentokrát **konečnou** grupu a p prvočíslo.

T&N. Pro $M \subset G$ definujme *normalizátor* množiny M v grupě $\mathcal{G}$:
$$N_{\mathcal{G}}(M) = \{g \in G \mid gMg^{-1} = M\}.$$

Pozorování. Nechť $M \subset G$, $g \in G$ a $H \leq \mathcal{G}$.

(1) $g \in N_{\mathcal{G}}(M) \Leftrightarrow \psi_g(M) = M \Leftrightarrow \psi_g|_M \in S(M)$,
(2) $Z(G) \leq N_{\mathcal{G}}(M) \leq \mathcal{G}$ a $H \trianglelefteq N_{\mathcal{G}}(H) \leq \mathcal{G}$,
(3) jestliže $H \trianglelefteq K \leq \mathcal{G}$, pak $K \leq N_{\mathcal{G}}(H)$.

Příklad 6.1. (1) $N_{S_4}(K) = S_4$, protože $K \trianglelefteq S_4$ (definice K viz 5.1).
(2) $N_{S_4}(\langle(1234)\rangle) = D_8$, protože $[S_4 : D_8] = 3$, $\langle(1234)\rangle \trianglelefteq D_8$ a $\langle(1234)\rangle \ntrianglelefteq S_4$, tedy $N_{S_4}(\langle(1234)\rangle) \neq S_4$.

Poznámka 6.2. Nechť $H \leq \mathcal{G}$ a $H \neq G$.

(1) Jestliže p dělí $[N_G(H) : H]$, pak existuje taková podgrupa $K \leq N_G(H)$, že $|K| = p|H|$ a $H \trianglelefteq K$.
(2) Je-li $\mathcal{G}$ nilpotentní, pak je H vlastní normální podgrupa $N_{\mathcal{G}}(H)$.

T&N. Pro $H, K \leq \mathcal{G}$ označme $\mathrm{Conj}_H = \{gHg^{-1} \mid g \in G\}$ a dále ${}_K\tau_H : K \to S(\mathrm{Conj}_H)$ značme zobrazení dané podmínkou
$$[{}_K\tau_H(k)](P) = kPk^{-1} = \psi_k(P).$$
Připomeňme, že je akce *tranzitivní*, má-li jedinou orbitu.

Pozorování. Jestliže $H, K \leq \mathcal{G}$ a $a, b \in G$, pak

(1) ${}_K\tau_H$ je akce grupy K na množině Conj_H,
(2) ${}_G\tau_H$ je tranzitivní, neboť $[{}_G\tau_H(ba^{-1})](aHa^{-1}) = bHb^{-1}$,
(3) pro stabilizátor akce ${}_G\tau_H$ platí, že
$$G_{aHa^{-1}} = \{\xi \mid \xi aHa^{-1}\xi^{-1} = aHa^{-1}\} = aN_{\mathcal{G}}(H)a^{-1},$$
(4) $\ker_G \tau_H = \bigcap_{g\in G} G_{gHg^{-1}} = \bigcap_{g\in G} gN_{\mathcal{G}}(H)g^{-1}$ (tj. největší normální podgrupa $\mathcal{G}$ obsažená v $N_{\mathcal{G}}(H)$).

Poznámka 6.3. Jestliže $H \leq \mathcal{G}$, pak $|\mathrm{Conj}_H| = [G : N_{\mathcal{G}}(H)]$.

T&N. Označme $\mathcal{M}_p(\mathcal{G}) = \{H \leq \mathcal{G} \mid \exists k \geq 0 : |H| = p^k\}$ a
$$Syl_p(\mathcal{G}) = \{P \in \mathcal{M}_p \mid \forall H \in \mathcal{M}_p : P \leq H \to P = H\}.$$
Prvky $Syl_p(\mathcal{G})$ se nazývají *Sylowovy* (p-)podgrupy

Pozorování. Nechť $\varphi \in Aut(\mathcal{G})$, pak

(1) $\varphi(\mathcal{M}_p(\mathcal{G})) = \mathcal{M}_p(\mathcal{G})$,
(2) $\varphi(Syl_p(\mathcal{G})) = Syl_p(\mathcal{G})$,
(3) $Syl_p(\mathcal{G}) = \{\{1\}\} \Leftrightarrow p$ nedělí $|G|$ díky 3.5.

Věta 6.4 (Sylowovy věty)**.** Nechť $P \in Syl_p(\mathcal{G})$, $r, m \in \mathbb{N}$, prvočíslo p je nesoudělné s m a $|G| = p^r \cdot m$. Potom

(1) $|Syl_p(\mathcal{G})| \equiv 1 \mod p$ a $Syl_p(\mathcal{G}) = \mathrm{Conj}_P$ (tedy všechny Sylowovy p-podgrupy jsou konjugované),
(2) $|P| = p^r$,

(3) jestliže $H \leq \mathcal{G}$ splňuje $|H| = p^k$ pro $k < r$, pak existuje podgrupa $K \leq \mathcal{G}$ řádu p^{k+1}, pro niž $H \trianglelefteq K$.

Důsledek 6.5. Jestliže $P \in Syl_p(\mathcal{G})$, pak $P \trianglelefteq \mathcal{G} \Leftrightarrow |Syl_p(\mathcal{G})| = 1$.

7. Nilpotentní grupy - příběh lásky mezi p-grupami

Celou přednášku značí $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupu a p prvočíslo.

Příklad 7.1. $|S_4| = 3 \cdot 2^3$, proto její netriviální Sylowovy podgrupy jsou:
$Syl_3(S_4) = \{\langle (a, b, c) \rangle \mid a, b, c, \in \{1, 2, 3, 4\}, a \neq b \neq c \neq a\}$ a
$Syl_2(S_4) = \{\psi_\sigma(D_8) \mid \sigma \in S_4\}$.

Poznámka 7.2. Nechť $\mathcal{H} = (H, \cdot, ^{-1}, 1)$ a $\mathcal{G}_j = (G_j, \cdot, ^{-1}, 1)$, $j \in J$ jsou grupy, $\pi : G \to H$ je homomorfismus na H, $K \leq G$ a . Pak pro každé $i \geq 0$

(1) $\pi(\vartheta_i(G)) \leq \vartheta_i(H)$,
(2) $\vartheta_i(G) \cap K \leq \vartheta_i(K)$,
(2) $\vartheta_i(\coprod_{j \in J} G_j) = \coprod_{j \in J} \vartheta_i(G_j)$.

Důsledek 7.3. Podgrupa, faktorová grupa i konečný direktní součin nilpotentních grup jsou rovněž nilpotentní.

Poznámka 7.4. Je-li $\mathcal{G}$ konečná, $P \in Syl_p(\mathcal{G})$, $H \leq \mathcal{G}$ a $N_{\mathcal{G}}(P) \leq H$, potom $H = N_{\mathcal{G}}(H)$.

T&N. Podgrupa $H \leq \mathcal{G}$ je *maximální*, jestliže $H \neq G$ a pro každou podgrupu P splňující $H \leq P \leq G$ platí, že buď $P = H$ nebo $P = G$.

Věta 7.5. Následující tvrzení jsou pro konečnou grupu $\mathcal{G}$ ekvivalentní:

(1) $\mathcal{G}$ je nilpotentní,
(2) pro každou $H \leq \mathcal{G}$, $H \neq G$ platí, že $H \neq N_G(H)$,
(3) pro každou maximální $H \leq \mathcal{G}$ platí, že $H \trianglelefteq \mathcal{G}$,
(4) každá Sylowova podgrupa je normální v $\mathcal{G}$,
(5) $\mathcal{G}$ je izomorfní direktnímu součinu svých Sylowových podgrup.

Důsledek 7.6. Konečná grupa $\mathcal{G}$ je nilpotentní, právě když je izomorfní konečnému direktnímu součinu konečných p-grup.

Příklad 7.7. (1) Najdeme-li v grupě řádu $720 = 2^4 \cdot 3^2 \cdot 5$ dvě různé podgrupy řádu 16, pak podle předchozí věty nejde o nilpotentní grupu.

(2) Existuje jediná nilpotentní grupa řádu $42 = 2 \cdot 3 \cdot 7$ a ta je izomorfní cyklické grupě $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_7 \cong Z_{42}$.

(3) Všechny nilpotentní grupy řádu 100 jsou komutativní, protože jejich netriviální Sylowovy podgrupy jsou řádu 2^2, 5^2, tedy komutativní grupy.

8. Hledá se p-grupa

Celou přednášku značí $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupu a p prvočíslo.

Poznámka 8.1. Je-li p nejmenší prvočíselný dělitel řádu konečné grupy $\mathcal{G}$ a pro $H \leq \mathcal{G}$ platí, že $[G : H] = p$, pak $H \trianglelefteq \mathcal{G}$.

Pozorování. Jestliže $\mathcal{H} = (H, \cdot, ^{-1}, 1)$ a $\mathcal{K} = (K, \cdot, ^{-1}, 1)$ jsou grupy, $\varphi : K \to \mathrm{Aut}(H)$ je homomorfismus a $\sigma \in \mathrm{Aut}(K)$, pak je $\varphi\sigma$ homomorfismus $\varphi : K \to \mathrm{Aut}(H)$ a zobrazení $(h, k) \to (h, \sigma(k))$ je izomorfismus semidirektních součinů $H \rtimes_{\varphi\sigma} K \to H \rtimes_{\varphi} K$.

Poznámka 8.2. Nechť $p > q$ jsou dvě prvočísla a $|G| = pq$. Pak buď

(a) $\mathcal{G}$ je cyklická izomorfní $\mathbb{Z}_{pq}$ nebo

(b) $\mathcal{G}$ je nekomutativní, q dělí $p - 1$ a existují prvky $a, b \in G$ a $m \in \mathbb{Z}_p^* \setminus \{1\}$ pro něž:

  (1) a je řádu q, b je řádu p, $aba^{-1} = b^m$ a $m^q \equiv 1 \mod p$,

  (2) $\langle b \rangle \trianglelefteq \mathcal{G}$, $G = \langle b \rangle \langle a \rangle \cong \langle b \rangle \rtimes \langle a \rangle \cong \mathbb{Z}_p \rtimes \mathbb{Z}_q$,

  Každé dvě takové nekomutativní grupy jsou izomorfní.

Příklad 8.3. (1) Protože 3 nedělí $4 = 5 - 1$, existuje podle předchozí poznámky až na izomorfismus jediná grupa řád 15, jíž je cyklická grupa.

(2) Grupy řádu 21 existují až na izomorfismus právě dvě: cyklická $\mathbb{Z}_{21}$ a nekomutativní $\mathbb{Z}_7 \rtimes_{\psi} \mathbb{Z}_3$ pro $\psi_k(s) = 2^k s$.

T&N. Je-li $\mathcal{G}$ abelovská grupa, pak řekneme, že jsou prvky $g_1, \dots, g_k \in G$ *nezávislé*, platí-li pro všechna $r_1 \dots, r_k \in \mathbb{Z}$ implikace

$$g_1^{r_1} \cdot \dots \cdot g_k^{r_k} = 1 \Rightarrow g_1^{r_1} = \dots = g_k^{r_k} = 1.$$

Poznámka 8.4. Buď $\mathcal{G}$ abelovská grupa, $g_1, \dots, g_k \in G$ a označme $\alpha : \coprod_{i=1}^{k} \langle g_1 \rangle \to G$ zobrazení dané předpisem $\alpha((g_1^{r_1}, \dots, g_k^{r_k})) = g_1^{r_1} \cdot \dots \cdot g_k^{r_k}$. Pokud $G = \langle g_1, \dots, g_k \rangle$, pak α je izomorfismus, právě když jsou prvky $g_1, \dots, g_k$ nezávislé.

T&N. Je-li $\mathcal{G}$ p-grupa, označme pro $i \geq 0$

$$\sigma_i(G) = \{g \in G \mid g^{p^i} = 1\}$$

a připomeňme, že $\mathrm{ord}(g)$ značí řád prvku g.

Pozorování. Nechť $\mathcal{G}$ je abelovská p-grupa, $i, j, r \in \mathbb{Z}$, $i, j \geq 0$ a $g \in G$.

(1) $\sigma_i(G) \trianglelefteq \sigma_{i+1}(G) \trianglelefteq \mathcal{G}$ a $\sigma_j(G/\sigma_i(G)) = \sigma_{i+j}(G)/\sigma_i(G)$,

(2) $\sigma_0(G) = \{1\}$ a $\sigma_{i+1}(G) \setminus \sigma_i(G)$ obsahuje právě prvky řádu p^{i+1},

(3) $\sigma_{i+1}(G)/\sigma_i(G)$ tvoří vektorový prostor nad tělesem $\mathbb{F}_p$,

(4) jestliže $k = \dim_{\mathbb{F}_p}(\sigma_{i+1}(G)/\sigma_i(G)) < \infty$, pak $\sigma_{i+1}(G)/\sigma_i(G) \cong \mathbb{Z}_p^k$,

(5) $\mathrm{ord}(g^r) = \mathrm{ord}(g) \Leftrightarrow \langle g^r \rangle = \langle g \rangle \Leftrightarrow \gcd(p, r) = 1 \Leftrightarrow p$ nedělí r.

Věta 8.5. Konečná abelovská p-grupa je izomorfní direktnímu součinu cyklických p-grup.

9. Cyklické grupy celého světa, spojte se!

Celou přednášku značí $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ tentokrát **abelovskou** grupu a p je prvočíslo.

Věta 9.1 (Věta o bázi)**.** Konečná abelovská grupa je izomorfní direktnímu součinu cyklických grup.

T&N. Množině všech prvků konečného řádu $\tau(G) = \{g \in G \mid \exists n > 0 : g^n = 1\}$ budeme říkat *torzní část* abelovské grupy $\mathcal{G}$. Grupa $\mathcal{G}$ se nazývá
- *torzní*, pokud $\tau(G) = G$,
- *beztorzní*, pokud $\tau(G) = \{1\}$.

Označme $\mathcal{G}^{(I)} := \coprod_{i \in I} G$ a $\mathcal{G}^{(n)} := \coprod_{i=1}^{n} G$ pro libovolnou množinu I a přirozené n.

Pozorování. Nechť $g_1, \ldots, g_k \in \tau(G)$.

(1) $\tau(G) \leq \mathcal{G}$ a $\tau(G)$ je torzní,
(2) podgrupy i faktory $\tau(G)$ jsou torzní,
(3) grupa $G/\tau(G)$ i její podgrupy jsou beztorzní,
(4) $|\langle g_1, \ldots, g_k \rangle| \leq \prod_{i=1}^{k} |\langle g_i \rangle| = \prod_{i=1}^{k} \mathrm{ord}(g_i) < \infty$.

Příklad 9.2. (1) Konečná grupy i p-grupy jsou torzní,
(2) $\mathbb{Z}^{(I)}$ je pro každé I beztorzní abelovská grupa.
(3) Nekonečně generovaná aditivní grupa racionálních čísel $\mathbb{Q}$ je beztorzní a platí

$$\langle \frac{c_1}{j_1}, \ldots, \frac{c_k}{j_k} \rangle \leq \langle \frac{1}{\prod_i j_i} \rangle \text{ pro každé } \frac{c_i}{j_i} \in \mathbb{Q}^*, i = 1, \ldots, k,$$

proto $\langle \frac{c_1}{j_1}, \ldots, \frac{c_k}{j_k} \rangle$ je cyklická grupa, $\bigcap_i \langle \frac{c_i}{j_i} \rangle \neq \{0\}$ a podle 4.4 je $\mathbb{Q}$ direktně nerozložitelná.

T&N. Množina $B \subset G$ je *volná báze* abelovské grupy $\mathcal{G}$, jestliže $\langle B \rangle = G$ a pro každou abelovskou grupu $\mathcal{H} = (H, \cdot, ^{-1}, 1)$ a každé zobrazení $\phi : B \to H$ existuje homomorfismus $\tilde{\phi} : G \to H$, pro který $\tilde{\phi}|_B = \phi$. Obsahuje-li abelovská grupa volnou bázi, mluvíme o *volné abelovské grupě.*

Řekneme, že B je *nezávislá*, jsou-li prvky $g_1, \ldots, g_k$ nezávislé $\forall \{g_1, \ldots, g_k\} \subseteq B$.

Poznámka 9.3. Uvažujme pro $B \subset G$ zobrazení $\rho : \mathbb{Z}^{(B)} \to G$ dané vztahem

$$\rho(f) = \prod_{b \in B : f(b) \neq 0} b^{f(b)}.$$

Pak jsou následující podmínky ekvivalentní:

(1) $\mathcal{G}$ je volná abelovská s volnou bází B,
(2) ρ je izomorfismus,
(3) $\langle B \rangle = G$, B je nezávislá a $\mathrm{ord}(b) = \infty$ pro všechna $b \in B$.

Poznámka 9.4. Jestliže $H \leq \mathcal{G}$ a G/H je volná, pak $\mathcal{G} \cong H \coprod G/H$.

Poznámka 9.5. Konečně generovaná beztorzní abelovská grupa je volná.

Věta 9.6. Konečně generovaná abelovská grupa je izomorfní direktnímu součinu cyklických grup.

10. Kompoziční řady - jedinečnost až na pořadí

Celou přednášku značí $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupu a A, B, C, D její podgrupy.

Poznámka 10.1 (modularita)**.** Jestliže $A \leq C$, pak $A(B \cap C) = (AB) \cap C$.

Pozorování. Jsou li A, B, C normální (charakteristické, úplně charakteristické) podgrupy, pak AB, $A(B \cap C)$, $(AB) \cap C$ jsou normální (charakteristické, úplně charakteristické) podgrupy.

Všechna následující tvrzení přednášky, která vyslovíme pro normální podgrupy, bychom mohli zformulovat a dokázat i pro charakteristické a úplně charakteristické podgrupy

Pozorování. Jestliže $B \trianglelefteq A$ a $D \trianglelefteq C$, pak

(1) $B \cap C \trianglelefteq A \cap C$ a $A \cap D \trianglelefteq A \cap C$,
(2) $(B \cap C)D \trianglelefteq (A \cap C)D$ a $(A \cap D)B \trianglelefteq (A \cap C)B$.

Poznámka 10.2 (Zassenhausovo lemma)**.** Jestliže $B \trianglelefteq A$ a $D \trianglelefteq C$, pak

$$(A \cap C)B/(A \cap D)B \cong (A \cap C)D/(B \cap C)D.$$

T&N. Nechť $\mathfrak{H} = \{H_i\}_{i=0}^n$ a $\mathfrak{K} = \{K_i\}_{i=0}^m$ jsou subnormální řady grupy $\mathcal{G}$. Řekneme, že

- $\mathfrak{K}$ je *zjemnění* $\mathfrak{H}$, pokud existuj $j_1 < \cdots < j_{n-1} : K_{j_i} = H_i$ pro všechna $i = 1, \dots, n-1$,
- $\mathfrak{H}$ je *kompoziční* řada, pokud H_{i+1}/H_i je jednoduchá pro všechna $i = 0, \dots, n-1$,
- $\mathfrak{K}$ a $\mathfrak{H}$ jsou *izomorfní* ($\mathfrak{K} \cong \mathfrak{H}$), pokud $n = m$ a existuje taková permutace $\sigma \in S_n$, že $H_{i+1}/H_i \cong K_{\sigma(i)+1}/K_{\sigma(i)}$ pro všechna $i = 0, \dots, n-1$.

Příklad 10.3. (1) $\{\{\mathrm{id}\}, A_n, S_n\}$ je kompoziční řada grupy S_n pro všechna $n > 4$.
(2) $\{\{\mathrm{id}\}, \langle(13)(24)\rangle, \langle(1234)\rangle, D_8\}$ je kompoziční řada grupy D_8.
(3) $\{\langle 0\rangle, \langle 10\rangle, \langle 5\rangle, \langle 1\rangle\}$, $\{\langle 0\rangle, \langle 10\rangle, \langle 2\rangle, \langle 1\rangle\}$, $\{\langle 0\rangle, \langle 4\rangle, \langle 2\rangle, \langle 1\rangle\}$ jsou všechny kompoziční řady grupy $\mathbb{Z}_{20}$.

Poznámka 10.4. Nechť $\mathfrak{H} = \{H_i\}_{i=0}^n$ a $\mathfrak{K} = \{K_i\}_{i=0}^m$ jsou subnormální řady grupy $\mathcal{G}$. Pak existují zjemnění $\tilde{\mathfrak{H}} = \{\tilde{H}_i\}_{i=0}^{nm}$ řady $\mathfrak{H}$ a zjemnění $\tilde{\mathfrak{K}} = \{\tilde{K}_i\}_{i=0}^{nm}$ řady $\mathfrak{K}$, která jsou izomorfní.

Pozorování. Je-li $\{K_i\}_{i=0}^m$ zjemnění kompoziční řady $\{H_i\}_{i=0}^n$, pak $K_i = K_{i+1}$ právě pro $m - n$ indexů i.

Věta 10.5 (Jordan-Hölder)**.** Každé dvě kompoziční řady grupy $\mathcal{G}$ jsou izomorfní.

Všimněme si, že Jordanova-Hölderova věta zobecňuje Základní větu aritmetiky.

Důsledek 10.6. Nechť n je přirozené číslo.

(1) Všechny kompoziční řady abelovských grupy řádu n jsou izomorfní.
(2) Prvočíselný rozklad čísla n je určen jednoznačně až na pořadí.

11. Volnost součinů, rovnost homomorfismů, bratrství prezentací

Celou přednášku předpokládáme, že I je neprázdná množina, $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ a $\mathcal{G}_i = (G_i, \cdot, ^{-1}, 1)$, $i \in I$, jsou grupy se společnou jedničkou, tedy $G_i \cap G_j = \{1\}$ pro $i \neq j$.

T&N. Označme $G_i^* = G_i \setminus \{1\}$, $V = \bigcup_{i \in I} G_i^*$ a

$$W = \{v_1 \bullet \cdots \bullet v_k \mid v_i \in V \ \forall i = 1, \ldots, k\} \cup \{1\},$$

kde 1 značí prázdné slovo. Na W zavedeme binární operaci $\bullet$

$$(v_1 \bullet \cdots \bullet v_k) \bullet (u_1 \bullet \cdots \bullet u_l) = (v_1 \bullet \cdots \bullet v_k \bullet u_1 \bullet \cdots \bullet u_l)$$

$$(v_1 \bullet \cdots \bullet v_k) \bullet 1 = 1 \bullet (v_1 \bullet \cdots \bullet v_k) = (v_1 \bullet \cdots \bullet v_k)$$

a unární operaci $\overline{()}$

$$\overline{(v_1 \bullet \cdots \bullet v_k)} = (v_k^{-1} \bullet \cdots \bullet v_1^{-1}), \quad \overline{(1)} = 1$$

pro $v_1, \ldots, v_k, u_1, \ldots, u_l \in V$. Definujme délku slova $w = v_1 \bullet \cdots \bullet v_k$ jako $l(w) = k$ a $l(1) = 0$. Relace ρ a $\sim$ na W zavedeme podmínkami:

$$(u, v) \in \rho \Leftrightarrow \exists u_1, u_2 \in W, \exists i \in I, \exists w_1, w_2 \in G_i^* : u = u_1 \bullet w_1 \bullet w_2 \bullet u_2, v = u_1 \bullet w_1 w_2 \bullet u_2$$

a $\sim$ je nejmenší ekvivalence obsahující ρ.

Pro slovo $u \in W$ řekneme, že je *redukované*, pokud neexistuje žádné $v \in W$, pro něž $(u, v) \in \rho$ a značme $[u] = [u]_\sim$ ekvivalenční třídu obsahující u.

Pozorování. Nechť $u, v, y, z \in W$, $I \neq \emptyset$, $G_i \neq \{1\}$.

(1) $(u, v) \in \rho \Leftrightarrow \exists u_0, u_1, \ldots, u_k \in W : u = u_0, v = u_k$ a buď $(u_i, u_{i-1}) \in \rho$ nebo $(u_{i-1}, u_i) \in \rho \ \forall i = 1, \ldots, k$,
(2) jestliže $(u, v) \in \rho$, pak $l(u) > l(v)$,
(3) $[u]$ obsahuje redukované slovo,
(4) pokud $u \sim v$ a $y \sim z$, pak $u \bullet y \sim v \bullet y \sim v \bullet z$, a $\overline{u} \sim \overline{v}$,
(5) $(W/\sim, \cdot, ^{-1}, [1])$ je grupa s operacemi $[u] \cdot [v] = [u \bullet v]$, $[u]^{-1} = [\overline{u}]$.

T&N. Grupu $(\overline{W}, \cdot, ^{-1}, [1])$ pro $\overline{W} := W/\sim$ z pozorování budeme nazývat *volný součin grup* $(\mathcal{G}_i, i \in I)$ a budeme ji značit $\mathcal{W}(\mathcal{G}_i, i \in I)$.

Poznámka 11.1. Pro každé $u \in W$ leží v třídě $[u]$ právě jedno redukované slovo.

Věta 11.2 (Univerzální vlastnost volné grupy)**.** Nechť $\mathcal{W}(\mathcal{G}_i, i \in I) = (\overline{W}, \cdot, ^{-1}, [1])$ je volný součin grup $\mathcal{G}_i$, $i \in I$. Pak je zobrazení $\mu_i : G_i \to \overline{W}$ dané vztahem $\mu_i(g) = [g]$ pro každé $i \in I$ prostý homomorfismus, $\overline{W} = \langle \bigcup_{i \in I} \mu_i(G_i) \rangle$ a pro každou grupu $\mathcal{G}$ a systém homomorfismů $\nu_i : G_i \to G$, $i \in I$, existuje právě jeden homomorfismus $\nu : \overline{W} \to G$ splňující $\nu \mu_i = \nu_i$ pro všechna $i \in I$.

T&N. Množina $X \subset G$ je *volná báze* grupy $\mathcal{G}$, jestliže $\langle X \rangle = G$ a pro každou grupu $\mathcal{H} = (H, \cdot, ^{-1}, 1)$ a každé zobrazení $\phi : X \to H$ existuje homomorfismus $\tilde{\phi} : G \to H$, pro který $\tilde{\phi}|_X = \phi$. Obsahuje-li grupa volnou bázi, mluvíme o *volné grupě*.

Příklad 11.3. $\{1\}$ je volná báze volné grupy $\mathbb{Z}$. Volné abelovské grupy $\mathbb{Z}^n$ nejsou pro žádné $n > 1$ volné grupy.

Věta 11.4. Nechť $X \neq \emptyset$ a $C_x = \langle x \rangle$ jsou nekonečné cyklické grupy s generátory $x \in X$. Pak volný součin $\mathcal{W}(C_x, x \in X)$ je volná grupa s volnou bází $\{[x] \mid x \in X\}$.

T&N. Označujme $\mathcal{F}(X) = (F(X), \cdot, ^{-1}, 1)$ volnou grupu s volnou bází X.

Jestliže $R \subset F(X)$ a $\pi : F(X) \to G$ je takový homomorfismus na grupu $\mathcal{G}$, že $\ker \pi$ je nejmenší normální podgrupa obsahující množinu R, pak trojici (X, R, π) (respektive $(X, \{r = 1 \mid r \in R\}, \pi)$) říkáme *prezentace* grupy $\mathcal{G}$.

Příklad 11.5. (1) Grupa $\mathbb{Z}^2$ má prezentaci například tvaru

$$(\{x, y\}, \{xyx^{-1}y^{-1}\}, \pi) \text{ respektive } (\{x, y\}, \{xyx^{-1}y^{-1} = 1\}, \pi)$$

pro homomorfismus $\pi(x) = (1, 0), \pi(y) = (0, 1)$.

(2) Grupa $\mathbb{Z}_{20}$ má prezentaci například tvaru $(\{x\}, \{x^{20}\}, \pi)$ pro $\pi(x) = 1$ nebo

$$(\{x, y\}, \{x^4, y^5, xyx^{-1}y^{-1}\}, \pi)$$

pro homomorfismus $\pi(x) = 5, \pi(y) = 4$.

12. Schreierova transversála - matka volných podgrup

Celou přednášku značí $\mathcal{G} = (G, \cdot, ^{-1}, 1)$ grupu a $\mathcal{F}(X) = (F(X), \cdot, ^{-1}, 1)$ volnou grupu s volnou bází X.

T&N. Je-li $Y \subseteq G$, pak značme $Y^{-1} := \{y^{-1} \mid y \in Y\}$ a $Y^{\pm 1} := Y \cup Y^{-1}$

Pozorování. Nechť $X \subseteq G$. $G = \langle X \rangle \Leftrightarrow \forall g \in G\ \exists n,\ \exists y_1, \ldots, y_n \in X^{\pm 1}$, pro něž $g = y_1 \cdot \cdots \cdot y_n$.

Poznámka 12.1. Nechť $G = \langle X \rangle$ a uvažujme akci $\mathcal{G}$ na množině Ω. Je-li $\gamma \in \Omega$ a $\Gamma = [\gamma]$ orbita prvku γ, definujme $g_\gamma = 1$ a pro každé $\omega \in \Gamma \setminus \{\gamma\}$ volme $g_\omega \in G$ tak, aby $g_\omega(\gamma) = \omega$. Dále označme $s_{y,\omega} = g_{y(\omega)}^{-1} y g_\omega \in G$ pro každé $y \in X^{\pm 1}$ a $\omega \in \Gamma$.

Pak pro každé $y \in X^{\pm 1}$ a $\omega \in \Gamma$ platí:

(1) $s_{y,\omega} = 1 \Leftrightarrow y g_\omega \in \{g_\eta \mid \eta \in \Gamma\}$,
(2) $s_{y,\omega} \in G_\gamma$,
(3) $s_{y,\omega}^{-1} = s_{y^{-1}, y(\omega)}$,
(4) $G_\gamma = \langle \{s_{x,\omega} \mid x \in X, \omega \in \Gamma\} \rangle$.

T&N. Je-li $H \leq G$, pak $T \subseteq G$ nazveme
- *levou částečnou transversálou* podgrupy H, pokud $|gH \cap T| \leq 1$ pro všechna $g \in G$,
- *levou transversálou* podgrupy H, jedná-li se o množinu reprezentantů všech ekvivalenčních tříd ekvivalence lmod, tedy pokud $|gH \cap T| = 1$ pro všechna $g \in G$.

Nadále bude T označovat levou transversálu podgrupy $H \leq G$, grupa $\mathcal{G}$ bude působit na množině $\Omega = \{tH \mid t \in T\}$ a pro každé $\omega \in \Omega$ označme $t_\omega \in T$ jediný prvek průniku $\omega \cap T$. Uvažujme akci $\tau : G \to S(\Omega)$ danou vztahem $\tau(a)(gH) = agH$ a označme ${}_TY_H = \{t_{x\omega}^{-1} x t_\omega \mid x \in X, \omega \in \Omega, x t_\omega \notin T\}$.

Poznámka 12.2. Nechť $1 \in T$ (tedy $t_H = 1$) a $y \in X^{\pm 1}$, pak

(1) $y t_\omega \notin T \Leftrightarrow y^{-1} t_{y\omega} \notin T$,

(2) ${}_TY_H^{-1} = \{t_{y\omega}^{-1} y t_\omega \mid y \in X^{-1}, \omega \in \Omega, yt_\omega \notin T\}$,
(3) $H = \langle {}_TY_H \rangle$.

Důsledek 12.3. Je-li $\mathcal{G}$ konečně generovaná a $[G : H] < \infty$, pak i H je konečně generovaná.

Pozorování. Pro $G = \langle X \rangle$ je ekvivalentní

(1) X je volná báze $\mathcal{G}$,
(2) $\forall n > 0$, $\forall y_1, \dots, y_n \in X^{\pm 1}$ takové, že $y_i \neq y_{i-1}^{-1}$, platí, že $y_1 \cdot \dots \cdot y_n \neq 1$,
(3) $\forall g \in G \setminus \{1\}$ $\exists!$ $n, y_1, \dots, y_n \in X^{\pm 1}$ takové, že $y_i \neq y_{i-1}^{-1}$ a $g = y_1 \cdot \dots \cdot y_n$.

Pro $g = y_1 \cdot \dots \cdot y_n$ z (3) existují jednoznačně určené hodnoty $k \in \mathbb{N}$, $n_1, \dots, n_k \in \mathbb{Z}$ a $x_1, \dots, x_k \in X$, pro něž $g = x_1^{n_1} \cdot \dots \cdot x_k^{n_k}$ je redukované slovo (ve smyslu 11.1 a 11.4), $\sum_{i=1}^{k} |n_i| = n$ a $x_i \in \{y^{\pm 1}_{1+\sum_{j=1}^{i-1} n_j}\}$.

T&N. Zápisu prvku g volné grupy z Pozorování (3) říkáme *redukovaný zápis* a součin prvků $u_1 \cdot \dots \cdot u_n$ se nazývá *redukovaný součin*, pokud pro redukované zápisy $u_i = y_{i,1} \cdot \dots \cdot y_{i,n_i}$, $y_{i,j} \in X^{\pm 1}$ platí, že $y_{i,1} \neq y^{-1}_{i-1,n_{i-1}}$ $\forall i = 2, \dots, n$. Prvek 1 chápeme jako redukovaný (tj. prázdný součin), proto $u \cdot 1$ je redukovaný součin $\forall u \in G$

Levá (částečná) transversála T podgrupy volné grupy $\mathcal{F}(X)$ se nazývá *Schreierova*, jestliže $\forall u, v \in F(X)$ takové, že $u \cdot v$ je redukovaný a $u \cdot v \in T$, platí, že $v \in T$.

Pozorování. Každá Schreierova transversála obsahuje prvek 1. Uvážíme-li pro podgrupu $H \leq \mathcal{F}(X)$ množinu

$$\mathcal{T} = \{T \subset F(X) \mid \ T \text{ je částečná Schreierova transversála}\},$$

pak $\{1\} \in \mathcal{T}$ a její maximální prvek vzhledem k inkluzi, který existuje díky Zornovu lemmatu, je Schreierova transversála.

Příklad 12.4. (1) Mějme volnou cyklickou grupu $F(\{x\}) = \{x^i \mid i \in \mathbb{Z}\}$ a zvolme její podgrupu $H = \langle x^n \rangle \leq F(\{x\})$. Pak $\{x^i \mid i \in \mathbb{Z}_n\}$ a $\{x^{-i} \mid i \in \mathbb{Z}_n\}$ jsou Schreierovy transversály podgrupy H.

(2) Uvažujme dvougenerovanou volnou grupu $F(\{x, y\})$ a nechť $u = xy^{-1}$, $v = yx$. Pak uv není redukovaný součin, zatímco vu redukovaný součin je. Protože je $F(\{x, y\})$ volná, existuje (jednoznačně určený) homomorfismus $\varphi : F(\{x, y\}) \to S_3$ splňující $\varphi(x) = (12)$ a $\varphi(y) = (123)$, který je na S_3. Položíme-li $H = \mathrm{Ker}\varphi$, pak $[F(\{x, y\}) : H] = |S_3| = 6$ a $\{1, y, y^2, x, xy, xy^2\}$ tvoří Schreierovu transversálu podgrupy H.

Pozorování. Nechť T je Schreierova transversála podgrupy H v grupě $F(X)$, $x, \tilde{x} \in X^{\pm 1}$, $\omega, \tilde{\omega} \in \Omega$, $u \in F(X)$ a položme $y = t_{x\omega}^{-1} x t_\omega$, $\tilde{y} = t_{\tilde{x}\tilde{\omega}}^{-1} \tilde{x} t_{\tilde{\omega}}$, pak

(1) díky 12.2 platí:
- jestliže $t_\omega = x^{-1}u$ a $x^{-1}u$ je redukovaný, pak $u = xt_\omega \in T$, a proto $y \notin {}_TY_H$,
- jestliže $t_{x\omega} = xu$ a xu je redukovaný, pak $u = x^{-1}t_{x\omega} \in T$, a proto $y^{-1} \notin {}_TY_H$,

(2) jestliže $y \in {}_TY_H{}^{\pm 1}$, pak $y = t_{x\omega}^{-1} x t_\omega$ je redukovaný součin podle (1)
(3) nechť $y, \tilde{y} \in {}_TY_H{}^{\pm 1}$, pak $\tilde{y} = y^{-1} \Leftrightarrow \tilde{y} = y^{-1}$ a $y = \tilde{y}^{-1} \Leftrightarrow$
$\Leftrightarrow t_{\tilde{x}\tilde{\omega}}^{-1} \tilde{x} t_{\tilde{\omega}} = t_\omega^{-1} x^{-1} t_{x\omega}$ a $t_{x\omega}^{-1} x t_\omega = t_{\tilde{\omega}}^{-1} \tilde{x}^{-1} t_{\tilde{x}\tilde{\omega}} \Leftrightarrow t_\omega = t_{\tilde{x}\tilde{\omega}}$, $\tilde{x} = x^{-1}$ a $t_{\tilde{\omega}} = t_{x\omega}$,
protože žádný ze součinů $\tilde{x}t_{\tilde{\omega}}$, $x^{-1}t_{x\omega}$, xt_ω, $\tilde{x}^{-1}t_{\tilde{x}\tilde{\omega}}$ neleží „na konci”prvku T.

(4) jestliže $y, \tilde{y} \in {}_TY_H{}^{\pm 1}$ a $\tilde{y} \neq y^{-1}$, pak pro $u := t_\omega t_{\tilde{x}\tilde{\omega}}^{-1}$, platí, že $y\tilde{y} = t_{x\omega}^{-1} x u \tilde{x} t_{\tilde{\omega}}$, kde $t_{x\omega}^{-1} x u \tilde{x} t_{\tilde{\omega}}$ je redukovaný součin.

Věta 12.5. Je-li T Schreierova transversála $H \leq F(X)$, pak je ${}_TY_H$ volná báze H.

Příklad 12.6. (1) Volná báze podgrupy $\langle x^n \rangle$ volné cyklické grupy $F(\{x\}) = \{x^i \mid i \in \mathbb{Z}\}$ je $\{x^n\}$.

(2) Pro $H = \mathrm{Ker}\varphi$ z 12.4(2) tvoří pro $T = \{1, y, y^2, x, xy, xy^2\}$ množina

$$\begin{aligned} {}_TY_H &= \{t_{x\omega}^{-1} x t_\omega \mid x \in X, \omega \in \Omega, xt_\omega \notin T\} = \\ &= \{x^2, y^{-1}x^2y, y^{-2}x^2y^2, y^3, y^{-1}x^{-1}yxy^2, y^{-2}x^{-1}yx, x^{-1}yxy\} \end{aligned}$$

volnou bázi H.

13. A o čem to celé vlastně bylo?

Výsledky můžeme rozdělit do tří (různě rozsáhlých) oblastí:

- popis konečných grup,
- popis volných grup,
- popis abelovských grup.

Konečné grupy:

- Předpoklady:
  - Lagrangeova (1.4) a Cachyho (3.5) věta,
  - Věty o izomorfismu (2.4, 2.5).
- Rozklady a poklady (dekompozice a zaručené podgrupy):
  - abelovské vrstvy řad: řešitelnost (5.4), nilpotence silnější než řešitelnost (5.7), charakterizace nilpotence (7.5, 7.6),
  - jednoduché vrstvy: kompoziční řady (jednoznačnost 10.5),
  - p-podgrupy: Sylowovy věty (6.4).
- Sklady (konstrukce):
  - direktní součin a jeho vnitřní popis (4.4),
  - semidirektní součin a jeho vnitřní popis (4.7).

Volné grupy:

- Volný součin: univerzální vlastnost (11.2),
- Volná grupa: volný součin cyklických grup (11.4),
- Podgrupy volných grup jsou volné (12.5).

Abelovské grupy:

- Konečně generované abelovské grupy: součin cyklických grup (9.6),
- Konečné abelovské grupy: součin cyklických p-grup (8.5, 9.1).