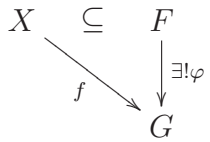
KOMBINATORICKÁ TEORIE GRUP

1. Volná grupa a volný součin grup

1.1. Existence volné grupy.

Definice. Podmnožina X grupy F je její *volnou bází* jestliže každé zobrazení $f\colon X \to G$ z množiny X do grupy G je možné rozšířit právě jedním způsobem na homomorfismus $\varphi\colon F \to G$ (viz obrázek).



Grupa F je *volná*, má-li nějakou volnou bázi.

Nyní, maje libovolnou množinu X, budeme směřovat ke konstrukci volné F_X grupy s bazí X. Ukážeme, že hledanou grupou je grupa všech redukovaných slov nad X spolu s operací redukovaného násobení. Označme $X^{-1} = \{x^{-1} \mid x \in X\}$.

Definice. *Slovem* nad množinou X budeme rozumět (případně i prázdnou) posloupnost $w = x_0, \ldots, x_{n-1}$, kde $x_i \in X \cup X^{-1}$. Prázdné slovo budeme značit $\emptyset$.

Fixujme množinu X. Nebude-li řečeno jinak, budeme slovem ve zbytku této kapitoly mínit slovo nad množinou X.

Definice. *Součinem* slov $v = x_0, \ldots, x_{n-1}$ a $w = y_0, \ldots, y_{m-1}$ budeme rozumět slovo $v^\wedge w = x_0, \ldots, x_{n-1}, y_0, \ldots, y_{n-1}$.

Slovo x je *úsekem* slova w existují-li slova u, v tak, že $w = u^\wedge x^\wedge v$.

Definice. Slovo w je *v redukovaném tvaru* neobsahuje-li úsek x, x^{-1} nebo x^{-1}, x pro nějaké $x \in X$. Označme F_X množinu všech slov v redukovaném tvaru.

Pro $x \in X$ definujme $(x^{-1})^{-1} = x$ a pro slovo $w = x_0, \ldots, x_{n-1}$ položme $w^{-1} = x_{n-1}^{-1}, \ldots, x_0^{-1}$.

Definice. Nechť v, w jsou slova a nechť u je nejdelší počáteční úsek slova w takový, že u^{-1} je koncový úsek slova v, tj. takový, že $v = p^\wedge u^{-1}$ a $w = u^\wedge q$ pro vhodné úseky p, resp. q slov v, resp. w. *Redukovaným součinem* slov v, w, který značíme vw, pak rozumíme slovo $p^\wedge q$.

Snadno nahlédneme, že redukovaný součin slov v redukovaném tvaru je opět slovo v redukovaném tvaru.

Věta 1.1. *Ztotožníme-li prvek $x \in X$ s posloupností x, tvoří množina F_X spolu s redukovaným násobením volnou grupu s bazí X.*

Důkaz. Označme S grupu všech permutací množiny F_X. Definujme zobrazení $\Phi\colon F_X \to S$ takto: Pro $x \in X$ a $x_0, \dots, x_{n-1} \in F_X$ nechť

$$\Phi(x)(x_0, \dots, x_{n-1}) = \begin{cases} x_1, \dots, x_{n-1} & \text{pokud } x_0 = x^{-1} \\ x, x_0, \dots, x_{n-1} & \text{jinak} \end{cases}$$

a

$$\Phi(x^{-1})(x_0, \dots, x_{n-1}) = \begin{cases} x_1, \dots, x_{n-1} & \text{pokud } x_0 = x. \\ x^{-1}, x_0, \dots, x_{n-1} & \text{jinak.} \end{cases}$$

Pro slovo $\Phi(x_0, \dots, x_{n-1})$ definujme

$$\Phi(x_0, \dots, x_{n-1}) = \Phi(x_0) \circ \cdots \circ \Phi(x_{n-1}).$$

Snadno ověříme, že $\Phi(x)$ a $\Phi(x^{-1})$ jsou vzájemně inverzní zobrazení a tedy to jsou permutace množiny F_X. Odtud plyne, že $\Phi(x_0, \dots, x_{n-1}) \in S$ pro každé slovo $x_0, \dots, x_{n-1}$ a že $\Phi\colon F_X \to S$ je homomorfismus grupoidu F_X s redukovaným násobením na podgrupu grupy S.

Je-li $x_0, \dots, x_{n-1}$ slovo v redukovaném tvaru, je

$$\Phi(x_0, \dots, x_{n-1})(1) = x_0, \dots, x_{n-1}.$$

Odtud je vidět, že jsou-li v, w různá slova v redukovaném tvaru, je $\Phi(v)(1) = v \neq w = \Phi(w)(1)$ a tedy $\Phi(v) \neq \Phi(w)$. Proto je zobrazení Φ prosté. Odtud plyne, že F_X je grupa.

Buď G grupa a φ zobrazení z množiny všech slov nad X do G. Pokud pro libovolná slova u, v platí, že

(i) $\varphi(u^{-1}) = \varphi(u)^{-1}$,
(ii) $\varphi(u^\wedge v) = \varphi(u)\varphi(v)$,

je restrikce $\varphi\colon F_X \to G$ grupový homomorfismus. Potom totiž pro slova $v = p^\wedge u^{-1}$ a $w = u^\wedge q$ v redukovaném tvaru, kde u je nejdelší počáteční úsek slova w, který jehož inverse je zároveň koncovým úsekem slova v, platí

$$\varphi(vw) = \varphi(p)\varphi(q) = \varphi(p)\varphi(u^{-1})\varphi(u)\varphi(q) = \varphi(v)\varphi(w).$$

Buď G grupa a $f\colon X \to G$ zobrazení. Každý homomorfismus $\varphi\colon F_X \to G$ rozčiřující zobrazení f nutně splňuje

$$\varphi(x_0^{\varepsilon_0}, \dots, x_{n-1}^{\varepsilon_{n-1}}) = f(x_0)^{\varepsilon_0} \cdots f(x_{n-1})^{\varepsilon_{n-1}}, \tag{1.1}$$

pro každé redukované slovo $w = x_0^{\varepsilon_0}, \dots, x_{n-1}^{\varepsilon_{n-1}}$, kde $x_i \in X$ a $\varepsilon_i \in \{-1, 1\}$. Tím je však tento homomorfismus určen jednoznačně. Naopak

zobrazení, které slovu w přiřadí hodnotu určenou rovností (1.1) splňuje podmínky (i) a (ii) a tedy $\varphi\colon F_X \to G$ je grupový homomorfismus. □

Důsledek 1.2. *Buď X podmnožina grupy G. Potom je X volnou bazí grupy $\langle X\rangle$ právě když v G platí, že*

$$x_0 \cdots x_{n-1} \neq 1. \tag{1.2}$$

pro každé neprázdné slovo v redukovaném tvaru $x_0, \ldots, x_{n-1}$ nad X.

Důkaz. Je-li podmínka (1.2) splněna, je homomorfismus $\varphi\colon F_X \to G$ rozšiřující identitu $f\colon X \to X$ vnoření, a tedy $\varphi(F_X) = \langle X\rangle$ je volná grupa s bazí X.

Naopak, je-li X volnou bazí grupu $\langle X\rangle$, je identita $f\colon X \to X$ rozšířena homomorfismem $\psi\colon \langle X\rangle \to F_X$. Pro neprázdné slovo v redukovaném tvaru $x_0, \ldots, x_{n-1}$ pak platí

$$\psi(x_0 \cdots x_{n-1}) = x_0, \ldots, x_{n-1} \neq 1,$$

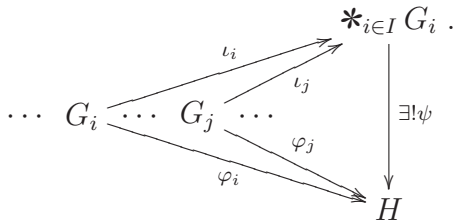
odkud plyne (1.2). □

Důsledek 1.3. *Každý prvek volné grupy s bazí X je součinem právě jednoho slova v redukovaném tvaru nad X.*

1.2. **Volný součin grup.** Po té co jsme definovali volnou grupu podívejme se ještě na volný součin grup, který pojem volné grupy přirozeně zobecňuje. Volná grupa totiž odpovídá volnému součinu cyklickýc grup nekonečného řádu.

Definice. *Volným součinem* grup $\{G_i \mid i \in I\}$, kde I je nějaká indexová množina, rozumíme grupu označenou $\ast_{i\in I} G_i$ spolu s vnořeními $\iota_i\colon G_i \to \ast_{i\in I} G_i$ takovou, že pro každou grupu H a každé homomorfismy $\{\varphi_i\colon G_i \to H \mid i \in I\}$ existuje právě jeden homomorfismus $\psi\colon \ast_{i\in I} G_i \to H$ takový, že $\varphi_i = \psi \circ \iota_i$ pro všechna $i \in I$.

Vlastnosti volného součinu znázorňuje následující diagram:



Buď $\mathcal{G} = \{G_i \mid i \in I\}$ soubor (pro jednoduchost předpokládejme po dvou disjunktních) grup. *Slovem* nad souborem $\mathcal{G}$ rozumějme posloupnost $g_0, \ldots, g_{n-1}$ takovou, že každý z prvků g_j je různý od jednotky a leží v některé z grup G_i. Řekneme, že slovo $g_0, \ldots, g_{n-1}$ nad souborem

$\mathcal{G}$ je v *$*$-redukovaném tvaru* (též *$*$-redukované*) pokud $g_j \in G_i$ implikuje $g_{j+1} \notin G_i$ pro každé $j \in \{0, \dots, n-2\}$, tj., leží-li jeho sousední znaky v různých grupách ze souboru $\mathcal{G}$. Podobně jako v případě volné grupy bychom ukázali, že volný součin $\ast_{i\in I} G_i$ můžeme ztotožnit s grupou všech $*$-redukovaných slov.

Věta 1.4. *Buď $\mathcal{G} = \{G_i \mid i \in I\}$ soubor disjunktních grup. Potom ve volném součinu $\ast_{i\in I} G_i$ platí tato dvě tvrzení:*

(i) *Součin neprázdného $*$-redukovaného slova je různý od jednotky.*
(ii) *Každý prvek $\ast_{i\in I} G_i$ je součinem právě jednoho $*$-redukovan0ho slova.*

2. Nielsenovsky redukovaná množina

Buď daná množina X. Slovem budeme opět rozumět slovo nad X. Délku prázdného slova definujme jako 0. Délka $|w|$ neprázdného slova $w = x_0, \dots, x_{n-1}$ buď číslo n. Pro podmnožinu $U \subseteq F_X$ položme $U^{\pm 1} = U \cup U^{-1}$.

Definice. Neprázdnou podmnožina U grupy F_X je *Nielsenovsky redukovaná* (krátce *N-redukovaná*), jestliže $U \cap U^{-1} = \emptyset$ a pro všechna $u, v, w \in U^{\pm 1}$ platí, že

(N) je-li $uv \neq 1 \neq vw$, potom $|uvw| > |u| + |w| - |v|$.

Věta 2.1. *Je-li $U \subseteq F$ N-redukovaná množina, potom je grupa $\langle U \rangle$ volná a U tvoří její bázi.*

Důkaz. Pro $u \in U^{\pm 1}$ označme $L(u)$ nejdelší počáteční úsek slova u, který se krátí v součinu xu pro některé $x \in U^{\pm 1} \setminus \{u^{-1}\}$. Podobně označme $R(u)$ nejdelší koncový úsek slova u, který se krátí v součinu uy pro některé $y \in U^{\pm 1} \setminus \{u^{-1}\}$ (tedy $R(u) = L(u^{-1})^{-1}$).

Z podmínky (N) plyne $|u| > |L(u)| + |R(u)|$. Jinak by se totiž slovo u v redukovaném součinu xuy zcela vykrátilo a platilo by tedy, že

$$|xuy| \leq |x| + |u| + |y| - 2|u| = |x| + |y| - |u|.$$

Odtud plyne, že existuje neprázdný úsek $M(u)$ slova u tak, že

$$u = L(u)^\wedge M(u)^\wedge R(u).$$

Indukcí snadno nahlédneme, že je-li $v_1, \dots, v_n$ posloupnost prvků z $U^{\pm 1}$ taková, že $v_i v_{i+1} \neq 1$ pro $1 \leq i < n$, podslova $M(v_i)$ zůstanou v redukovaném součinu $v_1 \cdots v_n$ nezkrácena. Speciálně $|v_1 \cdots v_n| \geq n$ a tedy $v_1 \cdots v_n \neq 1$. Protože $U \cap U^{-1} = \emptyset$, je součin neprázdné redukované posoupnosti nad U různý od jedné, odkud plyne dokazované. □

3. HNN-rozšíření a amalgámy grup

3.1. **HNN-rozšíření.** Budeme užívat následující značení: Je-li dána grupa G s prezentací $\langle X \mid \Delta \rangle$, označíme symbolem $\langle G;\, Y \mid \Gamma \rangle$ grupu s prezentací $\langle X \cup Y \mid \Delta \cup \Gamma \rangle$, přitom vždy předpokládáme, že množiny X a Y jsou disjunktní.

Definice. Buď G grupa s danou dvojicí izomorfních podgrup A, B a izomorfismem $\varphi\colon A \to B$. Grupu

$$G_\varphi = \left\langle G; t \mid t^{-1}at = \varphi(a),\ a \in A \right\rangle$$

nazveme *HNN-rozšířením* grupy G se *stabilizujícím znakem* t a *asociovanými podgrupami* A, B.

Fixujme HNN-rozšíření G_φ. Níže budeme pracovat s posloupnostmi tvaru $g_0,\ t^{\varepsilon_1}, \ldots,\ t^{\varepsilon_n},\ g_n$, kde $g_i \in G$ a $\varepsilon_i \in \{-1, 1\}$. Symbolem $\mathcal{V}$ označme množinu všech takových posloupností. Číslo n nazveme *délkou* posloupnosti $g_0,\ t^{\varepsilon_1}, \ldots,\ t^{\varepsilon_n},\ g_n$.

Definice. *Štěp* buď posloupnost tvaru $t^\varepsilon, g, t^{-\varepsilon}$ taková, že buďto $\varepsilon = -1$ a $g \in A$ nebo $\varepsilon = 1$ a $g \in B$. Řekneme, že posloupnost $g_0,\ t^{\varepsilon_1}, \ldots,\ t^{\varepsilon_n},\ g_n \in \mathcal{V}$ je v *HNN-redukovaném tvaru* (též *HNN-redukovaná*) pokud neobsahuje štěp.

Lemma 3.1. *Každý prvek $g \in G_\varphi$ je součinem posloupnosti v HNN-redukovaném tvaru.*

Důkaz. Zvolme $g \in G_\varphi$. Mezi všemi posloupnostmi z $\mathcal{V}$ jejichž součinem je prvek g vyberme nejkratší a ukažme, že je v HNN-redukovaném tvaru. Pro spor předpokládejme, že tomu tak není. Potom vybraná posloupnost $g_0,\ t^{\varepsilon_1}, \ldots,\ t^{\varepsilon_n},\ g_n$ obsahuje štěp $t^{\varepsilon_i},\ g_i,\ t^{\varepsilon_{i+1}}$, který lze nahradit prvkem $\varphi^{-\varepsilon_i}(g_i)$. Tím dostaneme posloupnost $g_0, t^{\varepsilon_1}, \ldots, t^{\varepsilon_{i-1}}$, $g_{i-1}\varphi^{-\varepsilon_i}(g_i)g_{i+1},\ t^{\varepsilon_{i+2}}, \ldots,\ t^{\varepsilon_n},\ g_n$ z $\mathcal{V}$ kratší délky, jejímž součinem je opět prvek g. To je spor. □

V grupě G zvolme systémy reprezentantů pravých rozkladových tříd podle podgrup A, resp. B v nichž jsou podgrupy A, resp. B reprezentovány jednotkou. Pro každé $g \in G$ označme symboly g^A, resp. g^B, zvolené reprezentanty podle A, resp. B takové, že $Ag = Ag^A$, resp. $Bg = Bg^B$.

Definice. Řekneme, že posloupnost $g_0, t^{\varepsilon_1}, \ldots, t^{\varepsilon_n}, g_n \in \mathcal{V}$ je *v normálním tvaru*, jestliže neobsahuje podposloupnost $t^\varepsilon, 1, t^{-\varepsilon}$ a

$$\text{je-li } \begin{cases} \varepsilon_i = -1, & \text{je } g_i \text{ zvolený reprezentant třídy } Ag_i, \\ \varepsilon_i = 1, & \text{je } g_i \text{ zvolený reprezentant třídy } Bg_i. \end{cases}$$

Lemma 3.2. *Buď $g \in G_\varphi$ součinem posloupnosti $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n$ v HNN-redukovaném tvaru. Potom je g součinem nějaké posloupnosti $h_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, h_n$ v normálním tvaru téže délky a se stejnou posloupností exponentů $\varepsilon_1, \dots, \varepsilon_n$.*

Důkaz. Ukážeme, že navíc platí, že $g_0^{-1}h_0 \in A$ pokud $\varepsilon_1 = 1$ a $g_0^{-1}h_0 \in B$ pokud $\varepsilon_1 = -1$. Důkaz provedem indukcí podle n. Pro $n = 0$ je $g = g_0$ a „jednočlená“ posloupnost g_0 je v normálním tvaru. Předpokládejme, že dokazované platí pro každý prvek $h \in G_\varphi$ jež je součinem kratší posloupností v HNN-redukovaném tvaru. Speciálně $h = g_1 t^{\varepsilon_2} \cdots t^{\varepsilon_n} g_n$ je součinem posloupnosti $h_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, h_n$ v normálním tvaru. Je-li $\varepsilon_1 = -1$, rozložme $h_1 = a{h_1}^A$, kde nutně $a \in A$. Z definujících relací grupy G_φ pak dostaneme, že $t^{-1}a = \varphi(a)t^{-1}$ a proto je g součinem prosloupnosti $g_0\varphi(a), t^{\varepsilon_1}, h_1^A, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, h_n$. Je-li $h_1^A \neq 1$ nebo $\varepsilon_2 = -1$, je výsledná posloupnost v normálním tvaru. Je-li $h_1^A = 1$ a $\varepsilon_2 = 1$ je $h_1 = a \in A$ a z indukčního předpokladu $g_1^{-1}h_1 \in A$ dostáváme, že $g_1 \in A$. To by ale znamenalo existenci štěpu $t^{\varepsilon_1}, g_1, t^{\varepsilon_2}$ v posloupnosti $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n$, která je HNN-redukovaném tvaru, což je spor. Všimněme si ještě, že $g_0^{-1}g_0\varphi(a) = \varphi(a) \in A$ a tedy v tomto případě je indukční krok hotov. Je-li $\varepsilon_1 = 1$ postupujeme obdobně. □

Věta 3.3 (O normálním tvaru)**.** *Každý prvek G_φ je součinem právě jedné posloupnosti v normálním tvaru.*

Důkaz. Vzhledem k Lemmatu 3.1 je každý prvek $g \in G_\varphi$ součinem posloupnosti v HNN-redukovaném tvaru a podle Lemmatu 3.2 je pak také součinem posloupnosti v normálním tvaru. Zbývá ukázat jednoznačnost této posloupnosti.

Uvažme množinu $\mathcal{W}$ všech posloupností v normálním tvaru a označme $S(\mathcal{W})$ grupu všech permutací této množiny. Pro $g \in G$ a $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n \in \mathcal{W}$ definujme

$$\Psi(g) = gg_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n.$$

Je ihned vidět, že $\Psi(gh) = \Psi(g) \circ \Psi(h)$ a že $\Psi(gg^{-1})$ je identickou permutací množiny $\mathcal{W}$. Proto je $\Psi\colon G \to S(\mathcal{W})$ grupový homomorfismus.

Fixujme posloupnost $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n \in \mathcal{W}$. Nejprve rozložme $g_0 = b_0 g_0^B$ (kde $b_0 \in B$) a definujme

$$\Psi(t)(g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n) = \begin{cases} \varphi^{-1}(b_0)g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n & : g_0^B = 1 \text{ a } \varepsilon_1 = -1, \\ \varphi^{-1}(b_0), t, g_0^B, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n & : \text{ jinak.} \end{cases}$$

Dále rozložme $g_0 = a_0 g_0^A$ (kde $a_0 \in A$) a definujme

$$\Psi(t^{-1})(g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n) = \begin{cases} \varphi(a_0)g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n & : g_0^A = 1 \text{ a } \varepsilon_1 = 1, \\ \varphi(a_0), t, g_0^A, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n & : \text{ jinak.} \end{cases}$$

Mějme libovolné $a \in A$. Nejprve předpokládejme, že $g_0^B = 1$ a $\varepsilon_1 = -1$. Potom $g_0 = b_0$ a podle předchozích definic platí, že

$$\begin{aligned}&(\Psi(t^{-1}) \circ \Psi(a) \circ \Psi(t))(g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n) = \\ &(\Psi(t^{-1}) \circ \Psi(a))(\varphi^{-1}(b_0)g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n) = \\ &(\Psi(t^{-1})(a\varphi^{-1}(b_0)g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n).\end{aligned}$$

Protože je posloupnost $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n$ v normálním tvaru, je g_1 zvolený reprezentant rozkladové třídy podle A a je-li $g_1 = 1$, nutně $\varepsilon_2 = -1$ (zvolená posloupnost neobsahuje podposloupnost t^{-1}, t). Odtud a z předpisů pro zobrazení Ψ dostáváme, že

$$\begin{aligned}&\Psi(t^{-1})(a\varphi^{-1}(b_0)g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n) = \\ &\varphi(a)b_0, t^{-1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n = \\ &\varphi(a)g_0, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n = \\ &\Psi(\varphi(a))(g_0, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n).\end{aligned}$$

Nyní předpokládejme, že $g_0^B \neq 1$ nebo $\varepsilon_1 = 1$. Potom

$$\begin{aligned}&(\Psi(t^{-1}) \circ \Psi(a) \circ \Psi(t))(g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n) = \\ &(\Psi(t^{-1}) \circ \Psi(a))(\varphi^{-1}(b_0), t, g_0^B, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n) = \\ &\Psi(t^{-1})(a\varphi^{-1}(b_0), t, g_0^B, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n) = \\ &\varphi(a)b_0 g_0^B, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n = \\ &\varphi(a)g_0, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n = \\ &\Psi(\varphi(a))(g_0, t^{\varepsilon_1}, g_1, t^{\varepsilon_2}, \dots, t^{\varepsilon_n}, g_n).\end{aligned}$$

Pro $a = 1$ vidíme, že $\Psi(t^{-1}) \circ \Psi(t)$ je identickým zobrazením na $\mathcal{W}$. Proto lze zobrazení $gY \colon G \cup \{t, t^{-1}\} \to S(\mathcal{W})$ rozšířit na homomorfismus $\Psi \colon \langle G; t\rangle \to S(\mathcal{W})$. Z uvedeného rozboru je navíc vidět, že

$$\Psi(\varphi(a)) = \Psi(t^{-1})\Psi(a)\Psi(t) = \Psi(t^{-1}at),$$

to jest, že definující relace grupy G_φ jsou v jádru zobrazení Ψ. Proto je toto zobrazení možné faktorizovat na homomorfismus $\Psi \colon G_\varphi \to S(\mathcal{W})$.

Snadno ověříme z předpisů definujících zobrazení Ψ, že pro posloupnost g_0, $t^{\varepsilon_1}, \dots, t^{\varepsilon_n}$, g_n v normálním tvaru platí

$$\Psi(g_0 t^{\varepsilon_1} \cdots t^{\varepsilon_n} g_n)(1) = g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n.$$

To znamená, že jsou-li g_0, t^{ε_1}, $\dots, t^{\varepsilon_n}$, g_n a h_0, t^{η_1}, $\dots, t^{\eta_m}$, h_m dvě různé posloupnosti v normálním tvaru, je

$$\Psi(g_0 t^{\varepsilon_1} \cdots t^{\varepsilon_n} g_n) \neq \Psi(h_0 t^{\eta_1} \cdots t^{\eta_m} h_m),$$

odkud plyne dokazovaná jednoznačnost. □

Věta 3.4 (Brittonovo lemma)**.** *Předpisem, který prvku $g \in G$ přiřadí součin HNN-redukované posloupnosti g délky nula je definováno vnoření $G \hookrightarrow G_\varphi$. Je-li $g_0, t^{\varepsilon_1}, \ldots, t^{\varepsilon_n}, g_n$ posloupnost v HNN-redukovaném tvaru kladné délky, potom $g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n \neq 1$.*

Důkaz. Pro $g \in G$ je posloupnost sestávající z g v normálním tvaru. Z jednoznačnosti normálního tvaru plune, že zobrazení, které prvku $g \in G$ přiřadí součin posloupnosti $g \in \mathcal{W}$ je vnoření. Z Lemmatu 3.2 plyne, že je-li $g \in G_\varphi$ součinem posloupnosti v HNN-redukovaném tvaru kladné délky je také součinem posloupnosti v normálním tvaru kladné délky. Z Věty 3.3 potom plyne, že tento součin je různý od jednotky. □

Definice. Slovo $g_0, t_1^{\varepsilon_1}, \ldots, g_{n-1}, t_n^{\varepsilon_n}$ je *cyklicky HNN-redukované*, je-li každá jeho cyklická permutace HNN-redukovaná.

Řekneme, že dvě slova jsou *konjugovaná*, jsou-li konjugované jejich součiny. Všimněme si, že všechny cyklické permutace slova w jsou konjugované. Uvažme nyní HNN-redukované tvary všech cyklických permutací daného slova w. Ten z nich, který je nejkratší délky je slovo cyklicky HNN-redukované. Proto je každé slovo konjugované s nějakým cyklicky HNN-redukovaným slovem.

Věta 3.5. *Obsahuje-li HNN-rozšíření G_φ prvek g konečného řádu n, potom grupa G obsahuje prvek téhož řádu, který je v grupě G_φ s prvkem g konjugován.*

Důkaz. Buď $g \in G_\varphi$ prvek konečného řádu n. Buď w slovo v HNN-redukovaném tvaru jehož součinem je g. Slovo w je konjugováno s cyklicky HNN-redukovaným slovem u. Z Brittonova lemmatu plyne, že řád cyklicky HNN-redukované slovo kladné délky má nekonečný řád ($w^\wedge \cdots {}^\wedge w$ je slovo v HNN-redukovaném tvaru). Řád součinu slova u má však být n. Proto u musí být slovo v HNN-redukovaném tvaru nulové délky a tedy odpovídá prvku z G. □

Lemma 3.6. *Nechť G je podgrupa grupy H a nechť $\varphi\colon A \to B$ je izomorfismus dvou podgrup grupy G. Potom je G_φ podgrupou grupy H_φ.*

Důkaz. Buď $g \in G_\varphi$ prvek různý od jednotky. Podle Lemmatu 3.1 je prvek g součinem posloupnosti $g_0, t^{\varepsilon_1}, \ldots, t^{\varepsilon_n}, g_n$ v HNN-redukovaném tvaru. Podle Brittonova lemmatu je součin této posloupnosti v grupě H_φ různý od jednotky, odkud plyne dokazované. □

HNN-rozšíření můžeme definivat i pro soubor dvojic izomorfních podgrup A_j, B_j, $j \in j$ spolu se zvolenými izomorfismy $\varphi_\alpha\colon A_j \to B_j$, $j \in J$, kde J je (ne nutně konečná) indexová množina.

Definice. Nechť jsou dány soubory $\{A_j \mid j \in J\}$ a $\{B_j \mid j \in J\}$ podgrup grupy G spolu se souborem $\boldsymbol{\varphi} = \{\varphi_j \colon A_j \to B_j \mid j \in J\}$ izomorfismů. Potom grupu

$$G_{\boldsymbol{\varphi}} = \langle G; t_j, j \in J \mid t_j^{-1} a t_j = \varphi_j(a), a \in A_j, j \in J \rangle$$

nazveme *HNN-rozšířením* s *bazí* G, *stabilizujícími znaky* $\{t_j \mid j \in J\}$ a *souborem asociovaných podgrup* $\{A_j, B_j \mid j \in J\}$.

Symbolem $\mathcal{V}_J$ označme množinu všech posloupností $g_0, t_{j_1}^{\varepsilon_1}, \ldots, t_{j_n}^{\varepsilon_n}, g_n$, kde $g_i \in G$, $\varepsilon_i \in \{-1, 1\}$ a $j_i \in J$. Číslo n nazveme *délkou* této posloupnosti.

Definice. *Štěpem* nazveme posloupnost tvaru $t_j^{\varepsilon}, g, t_j^{-\varepsilon}$ takovou, že buďto $\varepsilon = -1$ a $g \in A_j$ nebo $\varepsilon = 1$ a $g \in B_j$, kde $j \in J$. Řekneme, že posloupnost $g_0, t_{j_1}^{\varepsilon_1}, \ldots, t_{j_n}^{\varepsilon_n}, g_n \in \mathcal{V}_J$ je v *HNN-redukovaném tvaru* (nebo *HNN-redukovaná*) pokud neobsahuje štěp.

Je-li indexová množina $J = \{1, \ldots, n\}$ konečná, je zřejmě

$$G_{\boldsymbol{\varphi}} = (\ldots((G_{\varphi_1})_{\varphi_2})\ldots)_{\varphi_n}.$$

Je-li množina J nekonečná, snadno nahlédneme, že

$$G_{\boldsymbol{\varphi}} = \varinjlim G_{\boldsymbol{\varphi}_F},$$

kde F probíhá všechny konečné podmnožiny J. Odtud odvodíme příslušné zobecnění Brittonova lemmatu.

Věta 3.7. *Předpisem, který prvku $g \in G$ přiřadí součin HNN-redukované posloupnosti g délky nula je definováno vnoření grupy G do $G_{\boldsymbol{\varphi}}$. Součin posloupnosti v HNN-redukovaném tvaru kladné délky je různý od jedné.*

3.2. **Amalgámy grup.** S HNN-rozšířením úzce souvisí pojem amalgámu grup, který, jak je zřejmé z následujících definic přirozeně zobecňuje volný součin. Pro jednoduchost se omezme na amalgám dvojice grup G_0, G_1 o kterých budeme navíc vždy předpokládat, že jsou disjunktní.

Definice. Nechť A, a G_i, $i = 0, 1$ jsou grupy a $j_i \colon A \to G_i$ jsou vnoření. *Amalgámem grup* G_0, G_1 *podle* A nazveme grupu P s prezentací

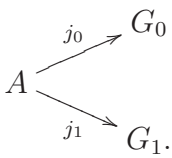
$$P = \langle G_0; G_1 \mid j_0(a) = j_1(a),\ a \in A \rangle .$$

Položme $A_i = j_i(A) \leq G_i$ a $\varphi = j_1 \circ j_0^{-1}$. Potom zřejmě

$$P = \langle G_0 * G_1 \mid \varphi(a) = a,\ a \in A_0 \rangle$$

a tedy $P = (G_0 * G_1)/N$, kde N je normální podgrupa grupy $G_0 * G_1$ generovaná množinou $\{\varphi(a)a^{-1} \mid a \in A_0\}$.

Z definice a následujících úvah snadno nahlédneme, že amalgám P spolu s vnořeními grup G_0, G_1 tvoří kolimitu diagramu



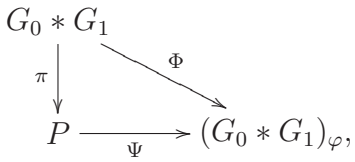
Lemma 3.8. *Buď*

$$(G_0 * G_1)_\varphi = \left\langle G_0 * G_1; t \mid \varphi(a) = t^{-1}at,\ a \in A_0 \right\rangle$$

HNN-rozšíření volného součinu $G_0 * G_1$ s asociovanými podgrupami A_0 a A_1. Potom je homomorfismus $\Phi\colon G_0 * G_1 \to (G_0 * G_1)_\varphi$ určený předpisy

$$\begin{cases} \Phi(g) = t^{-1}gt & \text{pokud } g \in G_0 \\ \Phi(g) = g & \text{pokud } g \in G_1 \end{cases} \tag{3.1}$$

možné faktorizovat přes homomorfismus $\Psi\colon P \to (G_0 * G_1)_\varphi$. To znamená, že diagram



ve kterém $\pi\colon (G_0 * G_1) \to P$ značí kanonickou projekci s jádrem N, komutuje.

Důkaz. Stačí ověřit, že obraz $\Phi(G_0 * G_1)$ splňuje definující relace grupy P. Podle definic ale pro každé $a \in A_0$ platí, že

$$\Phi(a) = t^{-1}at = \varphi(a) = \Phi(\varphi(a)).$$

□

Definice. Pro $i = 0, 1$ označme $G_i' = G_i \setminus A_i$. Řekneme, že $*$-redukované slovo $g_0, \ldots, g_{n-1}$ z volného součinu $G_0 * G_1$ je v *P-redukovaném tvaru* (též *P-redukované*), pokud každý z prvků g_i leží v některé z množin G_0', G_1'. *Délkou* posloupnosti v P-redukovaném tvaru rozumnějme číslo n.

Lemma 3.9. *Každý prvek $g \in P \setminus \pi(A_0)$ je součinem posloupnosti v P-redukovaném tvaru.*

Důkaz. Buď $g_0, \ldots, g_n$ nejkratší $*$-redukovaná posloupnost v $G_0 * G_1$ taková, že $g = \pi(g_0) \cdots \pi(g_n)$. Pokud $n = 0$, plyne z předpokladu $g \in P \setminus \pi(A_0)$, že $g_0 \notin G_0' \cap G_1'$ a tedy zvolená posloupnost je podle definice P-redukovaná. Předpokládejme, že $n > 0$. Pokud by $g_i \in A_0$

pro některé $0 \leq i \leq n$, mohli bychom zvolenou posloupnost nahradit kratší posloupností $g_0, \ldots, g_{i-2}, g_{i-1}\varphi(g_i)g_{i+1}, g_{i+2}, \ldots, g_n$, která by byla opět v $*$-redukovaném tvaru. Pokud by $g_i \in A_1$ pro některé $0 \leq i \leq n$, mohli bychom analogicky zvolenou posloupnost nahradit kratší posloupností $g_0, \ldots g_{i-2}, g_{i-1}\varphi^{-1}(g_i)g_{i+1}, g_{i+2}, \ldots, g_n$ v $*$-redukovaném tvaru. V obou případech dostáváme spor s minimalitou n (v zápise pokládáme $g_{-1} = 1 = g_{n+1}$). Proto je zvolená posloupnost v P-redukovaném. □

Následující věta je analogií Brittonova lemmatu pro amalgám grup.

Věta 3.10. *Platí následující:*

(a) *Grupy G_0 a G_1 jsou vnořeny do P.*
(b) *Součin P-redukované posloupnosti v P je různý od jedné.*

Důkaz. Z první části Brittonova lemmatu snadno nahlédneme, že předpisy (3.1) jsou definovány vnoření $\Phi\colon G_i \to (G_0 * G_1)_\varphi$. Pro $1 \neq g \in G_i$ je proto $1 \neq \Phi(g) = (\Psi \circ \pi)(g)$, odkud plyne, že $\pi(g) \neq 1$. To dokazuje část(a).

Z části (a) plyne, že součin P-redukované posloupnosti délky 0 je různý od jedné. Buď $g_0, \ldots, g_n$ P-redukovaná posloupnost kladné délky a g její součin. Z definice P-redukované posloupnosti je vidět, že obraz $\Psi(g) = \Psi(g_0) \cdots \Psi(g_n)$ je součinem HNN-redukované posloupnosti kladné délky v $(G_0 * G_1)_\varphi$ a proto, podle Brittonova lemmatu, různý od jedné. Odtud plyne, že $g \neq 1$. Tím je dokázána část (b). □

Z Věty 3.10 a z Lemmatu 3.9 okamžitě plyne, že:

Důsledek 3.11. *Zobrazení $\Psi\colon P \to (G_1 * G_2)_\varphi$ popsané v Lemmatu 3.8 je vnoření.*

Vidíme tedy, že amalgám dvojice grup je podgrupou HNN-rozšíření jejich volného součinu. Ukažme si nyní, že HNN-rozšíření je naopak vnořeno do jistého amalgámu grup.

Pro podmnožinu A grupy G značme symbolem $\mathrm{Gp}(X)$ podgrupu grupy G, kterou tato množina generuje. Jsou-li navíc dány prvky $a_1, a_2, \ldots$ grupy G, budeme značit $Gp(A; a_1, a_2, \ldots)$ podgrupu generovanou množinou A a danými prvky.

Budeme potřebovat následující pomocné tvrzení.

Lemma 3.12. *Nechť G je grupa a A její netriviální podgrupa. Buď $G * \langle u \rangle$ volný součit grupy G s cyklickou grupou nekonečného řádu. Potom platí, že*

$$\mathrm{Gp}(G, u^{-1}Au) \simeq G * A.$$

Důkaz. Uvažme vnoření grup G, resp. A do grupy $G * \langle u \rangle$ určené předpisy $g \mapsto g$, resp. $a \mapsto u^{-1}au$. Sjednocení těchto vnoření je možné jednoznačně rozšířit na homomorfismus $\varphi\colon G * A \to G * \langle u \rangle$. Je zřejmé, že obrazem $G * A$ je grupa $\mathrm{Gp}(G, u^{-1}Au)$. Nyní si stačí uvědomit, že obrazem součinu netriviálního $*$-redukovaného slova v $G * A$ je součin netriviálního $*$-redukovaného slova v grupě $G * \langle u \rangle$. Je-li totiž prvek $g \in G * A$ součinem $*$-redukovaného slova, například g_0, $a_0, \ldots, g_{n-1}$, a_n, je jeho obraz $\varphi(g)$ součinem slova g_0, u^{-1}, a_0, $u, \ldots, g_{n-1}$, u^{-1}, a_n, u, které je v $*$-redukovaném tvaru v grupě $G * \langle u \rangle$. Proto je homomorfismus φ je prostý, odkud plyne dokazované. □

Mějme grupu G s dvojicí izomorfních podgrup A, B a izomorfismem $\varphi\colon A \to B$. Uvažme volné součiny $G*\langle u \rangle$, resp. $G*\langle v \rangle$ a jejich podgrupy $U = \mathrm{Gp}(G, u^{-1}Au)$, resp. $V = \mathrm{Gp}(G, v^{-1}Bv)$. Podle Lemmatu 3.12 je homomorfismus $\varphi_u\colon G * A \to G * \langle u \rangle$ identický na G a splňující $a \mapsto u^{-1}au$, $a \in A$, vnořením na U. Podobně je homomorfismus $\varphi_v\colon G*A \to G*\langle v \rangle$ který je identický na G a splňuje $a \mapsto v^{-1}\varphi(a)v$, $a \in A$, vnořením na V. Buď P amalgám grup $G * \langle u \rangle$ a $G * \langle v \rangle$ podle $G * A$ a položme $t = uv^{-1}$. Potom pro každé $a \in A$ platí rovnost

$$t^{-1}at = v\varphi_u(a)v^{-1} = v\varphi_v(a)v^{-1} = \varphi(a). \tag{3.2}$$

Uvažme HNN-rozšíření

$$G_\varphi = \left\langle G; t \mid t^{-1}at = \varphi(a),\ a \in A \right\rangle.$$

Vzhledem k (3.2) je přiřazeními $g \mapsto g$, $g \in G$, a $t \mapsto t$ určen homomorfismus $\Phi\colon G_\varphi \to P$.

Věta 3.13. *Buď G grupa s dvojicí izomorfních podgrup A, B a izomorfismem $\varphi\colon A \to B$. Sestrojme grupy U, V a P jako výše. Ptom je homomorfismus $\Phi\colon G_\varphi \to P$ vnořením HNN-rozšíření G_φ do amalgámu P.*

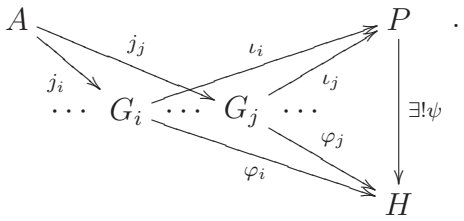
Důkaz. Zbývá ukázat, že homomorfismus Φ je prostý. Buď $h \in G_\varphi$ součinem HNN-redukovaného slova $w = g_0, t^{\varepsilon_1}, g_1, \ldots, t^{\varepsilon_n}, g_n$ kladné délky. Potom je $\Phi(h)$ součinem slova $\Phi(w)$ jehož znaky setávají z těchto prvků g_0u, g_0v, $u^{-1}gu$, $v^{-1}gv$, $u^{-1}g$, $v^{-1}g$, u a v přitom prvky z grup $G*\langle u \rangle$ a $G*\langle v \rangle$ se střídají. K tomu, aby slovo w bylo v $*$-redukovaném tvaru stačí ověřit, že z těchto znaků neleží v grupách U a V. To by nastalo pouze kdyby slovo $\Phi(w)$ obsahovalo znak $u^{-1}gu$ pro $g \in A$ nebo znak $v^{-1}gv$ pro $g \in B$. V prvním případě by pak slovo w obsahovalo štěp $t^{-1}gt$ pro $g \in A$, ve druhém štěp tgt^{-1} pro $g \in B$. To neplatí, neboť je HNN-redukované. □

Podobně jako v případě volného součinu můžeme definovat amalgám souboru grup.

Definice. Nechť A, a $\{G_i \mid i \in I\}$ jsou grupy a $j_i\colon A \to G_i$ jsou vnoření. *Amalgámem souboru grup* $\{G_i \mid i \in I\}$ *podle* A nazveme grupu P s prezentací

$$P = \langle G_i,\, i \in I \mid j_i(a) = j_j(a),\ a \in A,\, i, j \in I \rangle\,.$$

Pro $i \in I$ položme $A_i = j_i(A) \leq G_i$. Potom je $P = (*_{i\in I}\, G_i)/N$, kde N je normální podgrupa volného součinu $*_{i\in I}\, G_i$ generovaná množinou $\{j_i(a)j_j(a)^{-1} \mid a \in A,\, i, j \in I\}$. Vidíme, že amalgám souboru grup podle triviální grupy odpovídá jejich volnému součinu. Podobně jako volný součin, je amalgám souboru grup $\{G_i \mid i \in I\}$ podle vnořené grupy A charakterizován takto: Označme $\iota_i\colon G_i \to P$, $i \in I$ kanonická vnoření. Potom pro každou grupu H a každý soubor homomorfismů $\{\varphi_i\colon G_i \to H \mid i \in I\}$ takový, že $\varphi_i \circ j_i = \varphi_j \circ j_j$ pro všechny $i, j \in I$, existuje právě jeden homomorfismus $\psi\colon *_{i\in I}\, G_i \to H$ splňující $\varphi_i = \psi \circ \iota_i$ pro všechna $i \in I$. Tuto vlastnost znázorňuje následující diagram:



Pro $i \in I$ položíme $G_i' = G_i \setminus j_i(A)$ a definujeme *P-redukované* slovo jako $*$-redukované slovo jehož každý znak leží v některé z grup G_i'. Stejně jako v případě amalgámu dvojice grup, je každý prvek $P \setminus j_i(A)$ (pro libovolně zvolené $i \in I$) součinem P-redukovaného slova a součin netriviálního P-redukovaného slova je různý od jednotky.

4. O vnořeních spočetných grup

Věta 4.1 (G. Higman, H. Neumann, B. H. Neumann (1949))**.** *Každou spočetnou grupu G můžeme vnořit do grupy H_φ generované dvěma prvky nekonečného řádu. Navíc platí následující:*

(a) *Leží-li v grupě H_φ prvek konečného řádu n, pak je konjugován s nějakým prvkem z G. Proto i v grupě G leží prvek konečného řádu n.*

(b) *Má-li grupa G prezentaci s n-relacemi, existuje prezentace grupy H_φ se dvěma generátory a n-relacemi.*

Důkaz. Položme $H = G * \langle a, b\rangle$. Buď $\{g_1, g_2, \dots\}$ množina generátorů grupy G. Všimněmě si, že množina

$$A = \{a, b^{-1}ab, b^{-2}ab^2, \dots\}$$

je N-redukovaná, a tedy tvoří bázi volné podgrupy grup G. Uvažme množinu

$$B = \{b, g_1a^{-1}ba, g_2a^{-2}ba^2, \dots\}.$$

Přiřazeními $b \mapsto a$, $a \mapsto b$ a $g_i \mapsto 1$, pro pro všechna i, definujeme projekci grupy H na $\langle a, b\rangle$. Přitom obrazem množiny B je N-redukovaná množina A, odkud plyne, že B bazí volné podgrupy grupy H. Navíc restrikce této projekce určuje izomorfizmus $\varphi\colon \mathrm{Gp}(B) \to \mathrm{Gp}(A)$ a tedy přidáním stabilizujícího prvku t dostaneme HNN-rozšíření

$$H_\varphi = \left\langle H; t \mid t^{-1}bt = a, t^{-1}g_ia^{-i}ba^it = b^{-i}ab^i,\ i \in \mathbb{N}\right\rangle.$$

Podle Brittonova lemmatu je grupa H, a tedy i grupa G, vnořena do H_φ. Protože $b = tat^{-1}$ a

$$g_i = tb^{-i}ab^it^{-1}a^ib^{-1}a^{-i} = \underbrace{t^{i+1}a^{-1}t^{-i}at^iat^{-(i+1)}a^ita^{-1}t^{-i}a^{-i}}_{w_i}, \tag{4.1}$$

pro každé i, je grupa H_φ generovaná dvojicí prvků a, t. Z Brittonova lemmatu navíc plyne, že prvky a a t jsou nekonečného řádu.

Předpokládejme, že v grupě H_φ leží prvek konečného řádu n. Podle Věty 3.5 je pak konjugován s nějakým prvkem grupy H a tedy i grupy G. Odtud plyne (a).

Uvažme prezentaci

$$G = \langle X \mid \Delta\rangle,$$

kde $X = \{g_1, g_2, \dots\}$ a $\Delta = \{\delta_1, \delta_2, \dots\}$ jsou spočetné (ne nutně nekonečné) množiny. Navíc, označíme-li γ_j relaci, která vznikne nahrazením každého výskytu mocniny znaku g_i v relaci δ_i příslušnou mocninou výrazu w_i, tvořícího pravou stranu rovnosti (4.1), dostaneme prezentaci

$$H_\varphi = \langle a, t \mid \gamma_1, \gamma_2, \dots\rangle$$

grupy H_φ. Speciálně má-li grupa G prezentaci s n relacemi $\delta_1, \dots, \delta_n$, má grupa H_φ konečnou prezentaci s generátory a, t a n-ticí relací $\gamma_1, \dots, \gamma_n$. Tím jsme ukázali (b). □

Důsledek 4.2. *Existuje $2^{\aleph_0}$ vzájemně neizomorfních grup generovaných dvěma prvky nekonečného řádu.*

Důkaz. Označme $\mathbb{P}$ množinu všech prvočísel. Pro každou podmnožinu M množiny $\mathbb{P}$ uvažme Abelovu grupu

$$A_M = \bigoplus_{p\in\mathbb{P}} \mathbb{Z}_p.$$

Podle předchozí Věty 4.1 existuje grupa G_M generovaná dvěma prvky nekonečného řádu obsahující A_M. Navíc pro každé $n \in \mathbb{N}$ obsahuje grupa G_M prvek řádu n právě když grupa A_M obsahuje prvek řádu n. Přitom grupa A_M obsahuje prvek prvočíselmého řádu p právě když $p \in M$. Proto grupa G_M určuje množinu A. Porotože existuje $2^{\aleph_0}$ podmnožin množiny $\mathbb{P}$, existuje $2^{\aleph_0}$ vzájemně neizomorfních grup generovaných dvěma prvky nekonečného řádu. □

Připomeňme, že automorfismus φ grupy G je *vnitřní* pokud existuje $h \in G$ tak, že pro každé $g \in G$ platí $\varphi(g) = h^{-1}gh$.

Lemma 4.3. *Každou spočetnou grupu G můžeme vnořit do spočetné grupy H, ve které je každý izomorfismus mezi dvěma konečně generovanými podgrupami restrikcí vnitřního automorfimu.*

Důkaz. Pro danou konečně generovanou grupu A a spočetnou grupu B existuje nejvýše spočetně mnoho různých homomorfismů z grupy A do grupy B. Speciálně existuje nejvýše spočetně mnoho různých izomorfismů mezi dvěma konečně generovanými grupami. Protože existuje nejvýše spočetně mnoho konečně generovaných podgrup grupy G, je množina všech izomorfismů mezi dvěma konečně generovanými podgrupami grupy G nejvýše spočetná. Označme je $\varphi_1, \varphi_2, \ldots$, kde φ_i je izomorfismus konečně generované podgrupy A_i grupy G na konečně generovanou podgrupu B_i grupy G. Uvažme HNN-rozšíření

$$G^* = \left\langle G; t_1, t_2, \ldots \mid t_i^{-1} a t_i = \varphi_i a,\ a \in A_i,\ i = 1, 2, \ldots \right\rangle.$$

Grupa G je vnořena do G^* a každý z izomorfismů φ_i je restrikcí vnitřního automorfismu grupy G^* určeného konjugací prvkem t_i. Setrojme rostoucí spočetnou posloupnost grup

$$G = G_0 < G_1 < \ldots$$

takovou, že $G_{j+1} = G_j^*$ pro každé $j \in \mathbb{N}_0$ a položme $H = \bigcup_{j \in \mathbb{N}_0} G_j$. Izomorfní konečně generované podgrupy A, B grupy H jsou obsaženy v některé z grupě G_j (pro dosti velké j) a tedy každý izomorfismus grupy A na grupu B je restrikcí vnitřního automorfismu grupy G_{j+1} (a následně i grupy H) určeného konjugací vhodným stabilizujícím prvkem t. □

Omezíme-li se na cyklické podgrupy grupy G dostaneme tento okamžitý důsledek předcházejcího lemmatu:

Důsledek 4.4. *Každou spočetnou grupu G můžeme vnořit do spočetné grupy H, ve které jsou každé dva prvky téhož řádu konjugované.*

Tento důsledek využijeme v důkazu následující věty.

Věta 4.5. *Každou spočetnou grupu G můžeme vnořit do spočetné, jednoduché grupy H.*

Důkaz. Jako cvičení ponechme důkaz toho, že Abelova grupa $\mathbb{Q}/\mathbb{Z}$ obsahuje prvky všech konečných řádů. Uvažme posloupnost vnoření

$$G \to U \to V \to W \to H$$

definovanou takto:

- U je spočetná grupa ubsahující prvky všech konečných řádů, například $U = G \times (\mathbb{Q}/\mathbb{Z})$;
- $V = U * \langle x \rangle$, je volným součinem grupy U a volné cyklické grupy;
- W je grupa obsahující V, která je generovaná dvěma prvky nekonečného řádu (existuje podle Věty 4.1);
- H je spočetná grupa obsahující W v níž jsou každé dva prvky téhož řádu konjugovány (existuje podle Důsledku 4.4).

Ukážeme, že grupa H je jednoduchá. Buď N netriviální normální podgrupa grupy H. Zvolme prvek $a \neq 1$ grupy N. Protože x^{-1}, a^{-1}, x, a je slovo, které je ve volném součinu $U * \langle x \rangle$ cyklicky $*$-redukované, je jeho součin b prvek nekonečného řádu. Protože N je normální podgrupa grupy G, je $b \in N$. Navíc grupa N obsahuje všechny prvky konjugované s prvkem b a tedy, vhledem k vlastnostnem grupy H, všechny prvky nekonečného řádu. Proto N obsahuje oba generátory grupy W a tedy $W \leq N$. Speciálně $U \leq N$, odkud plyne, že W obsahuje prvky všech konečných řádů odkud již okamžitě plyne, že $N = H$. Ukázali jsme, že grupa H je jednoduchá. □

Na závěr této kapitoly ukážeme, že grupu H v předcházející větě je možné sestrojit tak, že je jednoduchá a konečně generovaná. To ukázal poprvé P. Hall v roce 1968, který sestrojil vnoření libovolné spočetné grupy do jednoduché grupy generované devítiprvkovou množinou. Postupně se mu podařilo zredukovat počet generátorů na tři. V polovině 70-tých let A. P. Gorjuškin a P. E. Shupp nezávisle ukázali, že každou spočetnou grupu je možné vnořit do jednoduché grupy generované dvěma prvky. My se omezíme na důkaz existence vnoření do jednoduché grupy s šesti generátory.

Symbolem $\mathbf{1}$ budeme značit triviální grupu.

Lemma 4.6. *Buď G grupa s izomorfními podgrupami A, B a daným izomorfismem $\varphi\colon A \to B$. Buď*

$$G_\varphi = \left\langle G; t \mid t^{-1}at = \varphi(a),\ a \in A \right\rangle$$

příslušné HNN-rozšíření. Je-li H podgrupa grupy G taková, že

$$H \cap \mathrm{Gp}(A, B) = \mathbf{1},$$

potom

$$\mathrm{Gp}(H; t) \simeq H * \langle t \rangle .$$

Důkaz. Mějme libovolné $*$-redukované slovo v $H * \langle t \rangle$. Nahraďme v něm každou mocninu t^n, resp. t^{-n} posloupností $t, \ldots, t$, resp. $t^{-1}, \ldots, t^{-1}$ délky n. Z předpokladu $H \cap \mathrm{Gp}(A, B) = \mathbf{1}$ snadno nahlédneme, že výsledné slovo je HNN-redukované. Odtud plyne dokazované. □

Věta 4.7. *Každou spočetnou grupu můžeme vnořit do jednoduché grupy generované šesti prvky.*

Důkaz. Buď G libovolná netriviální spočetná grupa. Podle Věty 4.5 ji můžeme vnořit do jednoduché spočetné grupy H. Podle Věty 4.1 je možné vnořit dále volný součin $H * \langle x \rangle$ do grupy U generované dvěma prvky u_0, u_1 nekonečného řádu. Dále uvažme posloupnost HNN-rozšíření $U \leq J \leq K$, kde

$$J = \left\langle U; y_0, y_1 \mid y_i^{-1} u_i y_i = u_i^2,\ i = 0, 1 \right\rangle ,$$

a

$$K = \left\langle J; z \mid z^{-1} y_i z = y_i^2,\ i = 0, 1 \right\rangle .$$

Zvolme $g \in G$ různé od jednotky a položme $h = [g, x] = g^{-1}x^{-1}gx$. Protože slovo g^{-1}, x^{-1}, g, x je cyklicky $*$-redukované v $G * \langle x \rangle$, je prvek h nekonečného řádu. Z Brittonovo lemmatu plyne, že $U \cap \mathrm{Gp}(y_0, y_1) = \mathbf{1}$. Vzhledem k Lemmatu 4.6 odtud dostaneme, že $\mathrm{Gp}(U; z) \simeq U * \langle z \rangle$, speciálně pak $\mathrm{Gp}(h, z) \simeq \langle h \rangle * \langle z \rangle \simeq \mathbb{Z} * \mathbb{Z}$.

Uvažme nyní grupu

$$Q = \left\langle r, s, t \mid s^{-1} r s = r^2,\ t^{-1} s t = s^2 \right\rangle .$$

Všiměme si, že grupu Q dostaneme jako posloupnost HNN-rozšíření $\langle r \rangle \leq P \leq Q$, kde

$$P = \left\langle r, s \mid s^{-1} r s = r^2 \right\rangle \text{ a } Q = \left\langle P; t \mid t^{-1} s t = t^2 \right\rangle .$$

Z Brittonova lemmatu, aplikovaného v grupě P, dostaneme, že $\langle r \rangle \cap \langle s \rangle = \mathbf{1}$. Z Lemmatu 4.6 pak plyne, že $\mathrm{Gp}(r, t) \simeq \langle r \rangle * \langle t \rangle \simeq \mathbb{Z} * \mathbb{Z}$.

Uvažme amalgám

$$D = \langle K; Q \mid h = t, z = r \rangle \tag{4.2}$$

grup K a Q podle izomorfních podgrup $\mathrm{Gp}(h, z)$ a $\mathrm{Gp}(r, t)$ (v prezentaci záměrně ztotožníme generátory h, t a z, r). Ukážeme, že je-li N vlastní normální podgrupa grupy D, potom $N \cap H = \mathbf{1}$. Pro spor předpokládejme, že je průnik $N \cap H$ netriviální. Protože je grupa H jednoduchá,

je nutně $H \leq N$, speciálně $g \in N$. Potom také $h = g^{-1}(x^{-1}gx) \in N$, odkud postupně dostaneme, že $t \in N$, $s \in N$ (neboť $s^2 \in NsN$, odkud $s \in s^{-1}NsN = N$), $r \in N$ (podobně jako pro s), $z \in N$ (neboť $z = r$), $y_0, y_1 \in N$ (opět stejný trik jako v případě prvku s) a konečně $u_0, u_1 \in N$ (ještě jednou týž trik). Vidíme, že $N = D$, což je spor s předpokladem, že N je vlastní podgrupa D.

Prezentace (4.2) dává $D = \mathrm{Gp}(K; s)$. Protože $K = \mathrm{Gp}(J; z) = \mathrm{Gp}(U; y_0, y_1, z) = \mathrm{Gp}(u_0, u_1, y_0, y_1, z)$, je $D = \mathrm{Gp}(u_0, u_1, y_0, y_1, z, s)$. Podle Zornova lemmatu pak existuje maximální vlastní normální podgrupa N grupy D. Již jsme ukázali, že $N \cap H = \mathbf{1}$, odkud plyne, že grupa G je vnořena do faktoru D/N. Ten je vzhledem k maximalitě N jednoduchý a je generován obrazy šestice u_0, u_1, y_0, y_1, z a s. □

5. Higmanova vnořovací věta

V 50-tých minulého století ukázali nezávisle Novikov a Boone, že existuje konečně prezentovaná grupa s neřešitelným problémem slov. V roce 1961 ukázal Higman, že konečně generovaná grupa je rekurzivně prezentovaná právě když je vnořitelná do konečně prezentované grupy. Odtud Novikov-Booneova věta snadno plyne. Cílem této kapitoly je důkaz obou tvrzení. Účinným nástrojem nám bude pojem benigní podgrupy, kterému věnujeme první sekci.

5.1. **Benigní podgrupy.** Pro podgrupu H grupy G položme

$$G_H = \{G; t \mid t^{-1}ht = h,\ h \in H\}.$$

Definice. Podgrupa H konečně generované grupy G je *benigní* v G, je-li grupu G_H možné vnořit do konečně prezentované grupy.

Lemma 5.1. *Nechť $H \leq G \leq E$ je řetízek grup. Je-li H benigní v E, potom je H benigní také v G.*

Důkaz. Podle Lemmatu 3.6 je G_H podgrupa grupy E_H. Proto je-li grupu E_H vnořit do konečně prezentované grupy P, platí totéž i pro grupu G_H. □

Lemma 5.2. *Buď G konečně generovaná podgrupa konečně prezentované grupy E. Potom je každá konečně generovaná podgrupa grupy G benigní.*

Důkaz. Nechť A je libovolná konečná podmnožina G. Položme $H = \mathrm{Gp}(A)$. Potom je

$$E_H = \left\langle E; t \mid t^{-1}ht = h,\ h \in H \right\rangle = \left\langle E; t \mid t^{-1}at = a,\ a \in A \right\rangle.$$

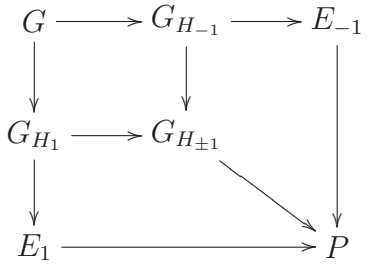
Vzhledem k tomu, že grupa E je konečně prezentovaná a množina A je konečná, je grupa E_H konečně prezentovaná. Proto je H benigní v E a podle předchozího lemmatu je pak benigní také v G. □

Lemma 5.3. *Průnik dvou benigních podgrup konečně generované grupy G je benigní podgrupa G.*

Důkaz. Nechť H_{-1} a H_1 jsou benigní podgrupy grupy G. Pro $i = -1, 1$ položme $G_{H_i} = \left\langle G, t_i \mid t_i^{-1} h t_i = h_i, h_i \in H_i \right\rangle$. Podle předpokladu můžeme grupu G_{H_i} vnořit do konečně prezentované grupy E_i. Buď P amalgám grup E_{-1}, E_1 podle G. Protože grupy E_{-1}, E_1 jsou konečně prezentované a grupa G je konečně generovaná, je amalgám P konečně prezentovaný. Snadno nahlédneme, že grupa

$$G_{H_{\pm 1}} = \left\langle G; t_{-1}, t_1 \mid t_i^{-1} h t_i = h_i,\ h_i \in H_i,\ i = -1, 1 \right\rangle$$

je izomorfní amalgámu grup $G_{H_{-1}}$ a G_{H_1} podle G a je vnořena do P. Popsanou situaci znázorněme graficky (všechny vyznačené homomorfimy jsou vnoření):



Položme $G_{H_{-1} \cap H_1} = \langle G; s \mid s^{-1} h s,\ h \in H_{-1} \cap H_1 \rangle$. Protože pro každé $h \in H_{-1} \cap H_1$ platí rovnost $(t_{-1} t_1)^{-1} h (t_{-1} t_1) = h$, určují předpisy $g \mapsto g$ pro $g \in G$ a $s \mapsto t_{-1} t_1$ homomorfismus $\varphi \colon G_{H_{-1} \cap H_1} \to G_{H_{\pm 1}}$. Ukážeme, že je to homomorfismus prostý. Restrikce φ na G je zřejmě prostá. Buď $\boldsymbol{g} = g_0, s^{\varepsilon_1}, \dots\ s^{\varepsilon_n}, g_n$ posloupnost v HNN-redukovaném tvaru kladné délky. Jejím obrazem je posloupnost $\varphi(\boldsymbol{g}) = g_0, t_{-\varepsilon_1}^{\varepsilon_1}, t_{\varepsilon_1}^{\varepsilon_1}, \dots\ t_{-\varepsilon_n}^{\varepsilon_n}, t_{\varepsilon_n}^{\varepsilon_n}, g_n$. Ta nemusí být v HNN-redukovaném tvaru, obsahuje-li však štěp, je to buďto úsek t_{-1}^{-1}, g_i, t_{-1} pro $g_i \in H_{-1}$ nebo úsek t_1, g_j, t_1^{-1} pro $g_j \in H_1$. Navíc jsou tyto štěpy součástmi úseků $t_1^{-1}, t_{-1}^{-1}, g_i, t_{-1}, t_1$, respektive t_{-1}, t_1, g_j, t_1^{-1}, nt_{-1}^{-1}. Protože původní posloupnost $\boldsymbol{g}$ je v HNN-redukovaném tvaru, a tedy neobsahuje štěp, je nutně $g_i \notin H_1$ a $g_j \notin H_{-1}$. Odtud plyne, že substitucemi $t_{-1}^{-1}, g_i, t_{-1} \mapsto g_i$ a $t_1, g_j, t_1^{-1} \mapsto g_j$, provedenými na všechny výskyty štěpů v posloupnosti $\varphi(\boldsymbol{g})$, dostaneme posloupnost v HNN-redukovaném tvaru délky alespoň n. Dle Brittonova lematu je součin této posloupnosti různý od jednotky. Odtud vidíme, že je zobrazení φ prosté. Proto je možné grupu $G_{H_{-1} \cap H_1}$ vnořit do konečně

prezentované grupy P což znamená, že $H_{-1} \cap H_1$ je benigní podgrupou grupy G. □

Lemma 5.4. *Buď G konečně generovaná grupa. Jsou-li H_0, H_1 benigní podgrupy grupy G, potom je také $\mathrm{Gp}(H_0 \cup H_1)$ benigní podgrupou grupy G.*

Důkaz. Pro $i = 0, 1$ položme $G_{H_i} = \left\langle G, t_i \mid t_i^{-1} h t_i = h,\ h \in H_i \right\rangle$ a zvolme konečně prezentovanou grupu E_i obsahující G_{H_i}. Podobně jako v důkazu předchozího lemmatu, uvažme amalgám P grup E_0, E_1 nad G. Ověříme, že platí

$$\mathrm{Gp}(H_0 \cup H_1) = \mathrm{Gp}(t_i^{-1} G t_i,\ i = 0, 1) \cap G. \tag{5.1}$$

Grupa $\mathrm{Gp}(H_0 \cup H_1)$ je zřejmě obsažena jak v $\mathrm{Gp}(t_i^{-1} G t_i,\ i = 0, 1)$ tak v grupě G a tedy i v průniku těchto grup. Ukážeme opačnou inkluzi. Prvek $g \in \mathrm{Gp}(t_i^{-1} G t_i,\ i = 0, 1)$ je součinem posloupnosti

$$\boldsymbol{g}_0 = t_0^{-1}, g_1, t_0, 1, t_1^{-1}, g_2, t_1, \ldots, t_0^{-1}, g_{2n-1}, t_0, 1, t_1^{-1}, g_{2n}, t_1.$$

Je-li navíc $g \in G$, existují posloupnosti $\boldsymbol{g}_1, \ldots, \boldsymbol{g}_m$ tak, že $\boldsymbol{g}_m = g$ a pro $0 \leq i < m$ dostaneme posloupnost $\boldsymbol{g}_{i+1}$ z posloupnosti $\boldsymbol{g}_i$ redukcí jednoho štěpu. Odtud indukcí snadno nahlédneme, že každá z posloupností $\boldsymbol{g}_i$ je tvaru $g_0, t_{\nu_1}^{\varepsilon_1}, g_1, \ldots, g_{k-1}, t_{\nu_k}^{\varepsilon_k}, g_k$, kde $g_0, g_k \in \mathrm{Gp}(H_0 \cup H_1)$. Proto $g \in \mathrm{Gp}(H_0 \cup H_1)$.

Podle předpokladu jsou grupy G a $\mathrm{Gp}(t_i^{-1} G t_i,\ i = 0, 1)$ konečně generované a tedy podle Lemmatu 5.2 benigní v P. Z rovnosti (5.1) a Lemmatu 5.3 pak plyne, že $\mathrm{Gp}(H_0 \cup H_1)$ je benigní v P a vzhledem k Lemmatu 5.2 je benigní v G. □

5.2. **Rekurzivní, rekurzivně spočetné a diofantické množiny.** Buď daná spočetná množina N (často množina celých nebo přirozených čísel). Řekneme, že podmnožina X množiny N je *rekurzivně spočetná*, pokud existuje algoritmus, který postupně vypíše všechny její prvky. Podmnožina X množiny N je *rekurzivní*, existuje-li algoritmus, který pro každé $n \in N$ rozhodne zda $n \in X$.

Lemma 5.5. *Buď daná spočetná množina N. Podmnožina X množiny N je rekurzivní, právě když jsou množiny X a $N \setminus X$ rekurzivně spočetné.*

Důkaz. Nejprve předpokládejme, že je X rekurzivní. Pak můžeme vypsat prvky množiny X tak, že postupně bereme prvky N a o každém rozhodneme, zda náleží do X. Tedy každá rekurzivní množina je rekurzivně spočetná. Je-li X rekurzivní, je zřejmě také $N \setminus X$ rekurzivní (použijeme stejný algoritmus, jen znegujeme výstup) a tedy i rekurzivně spočetná.

Nyní předpokládejme, že jsou obě množiny X a $N \setminus X$ rekurzivně spočetné. Potom existují algoritmy jejichž výstupy jsou posloupnosti $x_0, x_2, x_4, \ldots$ všech prvků množiny X a $x_1, x_3, x_5, \ldots$ všech prvků množiny $N \setminus X$. Kombinací těchto algoritmů získáme algoritmus jehož výstupem je posloupnost $x_0, x_1, x_2, \ldots$ všech prvků množiny N. Přitom $x_i \in X$ právě když $2 \mid i$. Odtud vidíme, že množina X je rekurzivní. □

Definice. Podmnožina $X \subseteq \mathbb{Z}^n$ je *diofantická*, existuje-li polynom

$$P \in \mathbb{Z}[x_0, \ldots, x_{n-1}, y_0, \ldots, y_{m-1}]$$

tak, že $(z_0, \ldots, z_{n-1}) \in X$ právě když má polynom

$$P(z_0, \ldots, z_{n-1}, y_0, \ldots, y_{m-1}) \in \mathbb{Z}[y_0, \ldots, y_{m-1}]$$

kořen. Řekneme, že polynom P *určuje* množinu X.

K úplnému pochopení pojmů rekurzivní a rekurzivně spočetná množina by bylo třeba exaktně popsat co je to algoritmus. Tomuto popisu se vyhneme odkazem na následující hlubokou Matijasevičovu větu.

Věta 5.6 (Matijasevič (1970))**.** *Podmnožina $X \subseteq \mathbb{Z}^n$ je diofantická právě když je rekurzivně spočetná.*

Tato věta má zajímavou hitorii. V roce 1900 sestavil David Hilbert seznam 23 problémů jejichž řešení považoval za zásadní pro další vývoj matematiky. Desátý Hilbertův problém je tento: „Existuje algortimus, který pro libovolný polynom $P \in \mathbb{Z}[x_0, \ldots, x_{n-1}]$ rozhodne, zda má kořen v $\mathbb{Z}^n$?“ Tento problém odolával snahám o vyřešení přes půl století. V roce 1970 jej zodpověděl negativně tehdy dvaadvacetiletý ruský student Yury Matijasevič, když navázal na předchozí výsledky především Julie Robinson, Martina Davise a Hilary Putmana. Extraktem Matijasevičova řešení je námi uvedená hluboká Věta 5.6.

Tvrzení 5.7. *Existuje rekurzivně spočetná podmnožina přirozených čísel S, která není rekurzivní.*

Důkaz. Buď $X = \{x_0, x_1, \ldots\}$ spočetná množina proměnných. Nejprve ukažme, jak efektivně přiřadit každému polynomu $P \in \mathbb{Z}[X]$ jednoznačně určené přirozené číslo $\gamma(P)$. Snadno ověříme, že předpisem

$$\alpha(z) = z^4 + 2z + 1$$

definujeme prosté zobrazení $\alpha\colon \mathbb{Z} \to \mathbb{N}$. Dále označme n-té liché prvočíslo symbolem p_{n-1}, tj. $p_0 = 3$, $p_1 = 5$, $p_2 = 7$, $p_3 = 11, \ldots$ atd. a posloupnosti $\boldsymbol{t} = t_0, \ldots, t_n \in \mathbb{N}_0^{n+1}$ přiřaďme jednoznačně určené přirozené číslo

$$\beta(\boldsymbol{t}) = p_0^{t_0} \cdots p_n^{t_n}$$

Pro $n \in \mathbb{N}_0$ a posloupnost $\boldsymbol{t} = t_0, \ldots, t_n \in \mathbb{N}_0^{n+1}$ značme $\boldsymbol{x}^{\boldsymbol{t}} = x_0^{t_0} \cdots x_n^{t_n}$. Nyní, pro libovolný polynom

$$P(x_0, \ldots, x_n) = a_0 \boldsymbol{x}^{\boldsymbol{t}_0} + \cdots + a_m \boldsymbol{x}^{\boldsymbol{t}_m}, \text{ kde } \beta(\boldsymbol{x}^{\boldsymbol{t}_0}) < \cdots < \beta(\boldsymbol{x}^{\boldsymbol{t}_m}),$$

položme $\alpha(\boldsymbol{a}) = \alpha(a_0), \ldots, \alpha(a_n)$ a definujme

$$\gamma(P) = 2^{\beta(\alpha(\boldsymbol{a}))} p_0^{\beta(\boldsymbol{t}_0)} \cdots p_m^{\beta(\boldsymbol{t}_m)}.$$

Položme

$$S = \{\gamma(P(x_0, \ldots, x_n)) \mid P(\gamma, x_1, \ldots, x_n) \text{ má kořen.}\}.$$

Postupně můžeme generovat všechny polynomy $P(x_0, \ldots, x_n) \in P[X]$, pro každý spočítat $\gamma(P)$ a dosadit výslednou hodnotu za x_0. Dále budeme do výsledného polynonu v proměnných $x_1, \ldots, x_n$ postupně dosazovat všechny n-tice celých čísel. Tak najdeme všechny prvky množiny S odkud je vidět, že množina S je rekurzivně spočetná.

Pro spor předpokládejme, že je množina S rekurzivní. Potom je množina $\mathbb{Z} \setminus S$ rekurzivně spočetná a existují $n \in \mathbb{N}_0$ a polynom $P \in \mathbb{Z}[x_0, \ldots, x_n]$ tak, že $z \in \mathbb{Z} \setminus S$ právě když má $P(z, x_1, \ldots, x_n)$ kořen v $\mathbb{Z}^n$. Odtud plyne, že $\gamma(P) \in \mathbb{Z} \setminus S$ právě když má polynom $P(\gamma(P), x_1, \ldots, x_n)$ kořen v $\mathbb{Z}^n$, což však nastane právě když $\gamma(P) \in S$. To je hledaný spor. □

Definice. *Elementární formulí* rozumějme formuli $\varphi(x_0, \ldots, x_m)$ jednoho z těchto tvarů:

$$\begin{aligned}
x_i &= c, \text{ pro nějaké } c \in \mathbb{Z}, \\
x_i &= x_j, \text{ kde } i \neq j, \\
x_k &= x_i + x_j, \text{ kde } i, j, k \text{ jsou po dvou různé}, \\
x_k &= x_i x_j, \text{ kde } 0 < k < i < j.
\end{aligned}$$

Připomeňme, že *konjunkcí* formulí $\varphi_0, \ldots, \varphi_t$ rozumíme formuli

$$\Phi = \bigwedge_{j=0}^{t} \varphi_j.$$

Lemma 5.8. *Pro každé $n \in \mathbb{N}_0$ a každý polynom $P \in \mathbb{Z}[x_0, \ldots, x_n]$ existují nezáporné celé číslo m a konjunkce elementárních formulí Φ_P tak, že $P(x_0, \ldots, x_n) = y_m$ právě když $\Phi_P(x_0, \ldots, x_n, y_0, \ldots, y_m)$ pro nějaké $(y_0, \ldots, y_{m-1}) \in \mathbb{Z}^m$.*

Důkaz. Tvrzení ukážeme indukcí podle počtu proměnných a stupně plynomu P v proměnné x_n. Nemá-li P žádnou proměnnou (tj., je-li stupně 0), je $P = c$ a buď $\Phi_P(y_0)$ elementární formule $y_0 = c$. Každý polynom $P \in \mathbb{Z}[x_0, \ldots, x_n]$ je tvaru

$$P(x_0, \ldots x_n) = P_1(x_0, \ldots, x_n) x_n + P_0(x_0, \ldots, x_{n-1}),$$

kde polynom P_1 má menší stupeň v proměnné x_n a P_0 má méně proměnných. Podle indukčního předpokladu existují $k, m \in \mathbb{N}_0$ a konjunkce elementárních formulí Φ_{P_1}, resp. Φ_{P_0} tak, že $P_1(x_0, \ldots, x_n) = y_k$ právě když $\Phi_{P_1}(x_0, \ldots, x_n, y_2, \ldots, y_k)$ pro nějaké $(y_2, \ldots, y_{k-1}) \in \mathbb{Z}^{k-2}$, resp. $P_0(x_0, \ldots, x_{n-1}) = y_{m-1}$ právě když $\Phi_{P_0}(x_0, \ldots, x_n, y_{k+1}, \ldots, y_{m-1})$ pro nějaké $(y_{k+1}, \ldots, y_{m-2}) \in \mathbb{Z}^{m-k-2}$. Formuli Φ_P najdeme jako konjunkci formulí Φ_{P_1}, Φ_{P_0} a elementárních formulí:

$$\Phi_P = \Phi_{P_1} \wedge \Phi_{P_0} \wedge (y_1 = x_n) \wedge (y_0 = y_1 y_k) \wedge (y_m = y_0 + y_{m-1}).$$

□

Důsledek 5.9. *Pro každé $n \in \mathbb{N}_0$ a každý polynom $P \in \mathbb{Z}[x_0, \ldots, x_n]$ existují nezáporné celé číslo m a konjunkce elementárních formulí Ψ_P tak, že $P(x_0, \ldots, x_n) = 0$ právě když $\Psi_P(x_0, \ldots, x_n, y_0, \ldots, y_m)$ pro nějaké $(y_0, \ldots, y_m) \in \mathbb{Z}^{m+1}$.*

Důkaz. Položme

$$\Psi_P = \Phi_P \wedge (y_m = 0).$$

□

Lemma 5.10. *Buď dána konjunkce elementárních formulí*

$$\Phi(x_0, \ldots, x_n) = \bigwedge_{j=0}^{t} \varphi_j.$$

Potom existuje polynom $P_\Phi(x_0, \ldots, x_n)$ tak, že pro každou $(x_0, \ldots, x_n) \in \mathbb{Z}^{n+1}$ platí, že $\Phi(x_0, \ldots, x_n)$ právě když $P_\Phi(x_0, \ldots, x_n) = 0$.

Důkaz. Elementární formuli φ přiřadíme polynom P_φ tak, že je-li φ formule

$$\begin{aligned}
x_0 = c, &\text{ je } P_\varphi = x_0 - c,\\
x_i = x_j, &\text{ je } P_\varphi = x_i - x_j,\\
x_k = x_i + x_j, &\text{ je } P_\varphi = x_i + x_j = x_k,\\
x_k = x_i x_j, &\text{ je } P_\varphi = x_i x_j - x_k
\end{aligned}$$

a položíme

$$P_\Phi = \sum_{i=0}^{t} P_{\varphi_j}^2.$$

□

Lemma 5.11. *Podmnožina $X \subseteq \mathbb{Z}^n$ je diofantická právě když existuje konjunkce elementárních formulí Φ s následující vlastností: $(z_0, \ldots, z_{n-1}) \in X$ právě když existují $(y_0, \ldots, y_{m-1}) \in \mathbb{Z}^m$ tak, že*

$$\Phi(z_0, \ldots, z_{n-1}, y_0, \ldots, y_{m-1}).$$

Důkaz. Předpokládejme, že je X diofantická. Potom existuje $k \in \mathbb{N}$ a polynom $P \in \mathbb{Z}[x_0, \ldots, x_{n-1}, y_0, \ldots, y_{k-1}]$, kde tak, že $(z_0, \ldots, z_{n-1}) \in X$ právě když má polynom

$$P(z_0, \ldots, z_{n-1}, y_0, \ldots, y_{k-1}) \in \mathbb{Z}[y_0, \ldots, y_{k-1}]$$

kořen. Podle Lemmatu 5.8 existuje $m \geq k$ tak, že $(z_0, \ldots, z_{n-1}) \in X$ právě když existují $(y_0, \ldots, y_{m-1}) \in \mathbb{Z}^m$ tak, že

$$\Phi_P(z_0, \ldots, z_{n-1}, y_0, \ldots, y_{m-1}).$$

Naopak, je-li množina X definována formulí Φ je podle Lemmatu 5.10 určena polynomem P_Φ a tedy je diofantická. □

5.3. **Novikov-Booneova věta.** V této podkapitole nejprve ukážeme, že rekurzivně spočetné množiny vymezují benigní podgrupy volné grupy. Tento fakt využijeme k důkazu Novikov-Booneovy věty, tedy ke konstrukci konečně prezentované grupy, která nemá řešitelný problém slov.

Lemma 5.12. *Buď G grupa, A_i, B_i, $i \in I$, dvojice izomorfních podgrup grupy G s izomorfismy $\varphi_i \colon A_i \to B_i$, $i \in I$, a*

$$G_{\boldsymbol{\varphi}} = \left\langle G; t_i,\ i \in I \mid t_i^{-1} a t_i = \varphi_i(a),\ a \in A_i,\ i \in I \right\rangle$$

příslušné HNN-rozšíření. Buď H podgrupa grupy G taková, že

$$t_i^{-1}(H \cap A_i)t_i = H \cap B_i \tag{5.2}$$

pro každé $i \in I$. Potom

$$H = \mathrm{Gp}(H; t_i,\ i \in I) \cap G.$$

Důkaz. Položme

$$H_{\boldsymbol{\varphi}} = \left\langle H, t_i,\ i \in I \mid t_i^{-1} a t_i = \varphi_i(a),\ a \in H \cap A_i,\ i \in I \right\rangle.$$

Jednoznačným rozšířením inkluze $H \cup \{t_i,\ i \in I\} \subseteq G_{\boldsymbol{\varphi}}$ dostaneme homomorfismus $\Psi \colon H_{\boldsymbol{\varphi}} \to G_{\boldsymbol{\varphi}}$. Tvrdíme, že tento homomorfismus je prostý. K tomu stačí ověřit, že obrazem HNN-redukované posloupnosti v $H_{\boldsymbol{\varphi}}$ je HNN-redukovaná posloupnost v $G_{\boldsymbol{\varphi}}$. Buď $h_0, t_{i_1}^{\varepsilon_1}, \ldots, h_{n-1}, t_{i_n}^{\varepsilon_n}, h_n$ Hn-redukovaná posloupnost v HNN-rozšíření $H_{\boldsymbol{\varphi}}$. Pokud by tato posloupnost nebyla HNN-redukovaná v $G_{\boldsymbol{\varphi}}$, obsahovala by štěp $t_i^{-\varepsilon}$, h, t_i^{ε}, kde buďto $\varepsilon = 1$ a $h \in H \cap A_i$ nebo $\varepsilon = -1$ a $h \in H \cap B_i$. Vzhledem k (5.2) však žádná z těchto možností nemůže nastat.

Odtud plyne, že homomorfismus Ψ je prostý a grupu $H_{\boldsymbol{\varphi}}$ můžeme ztotožnit s jejím obrazem, který odpovídá grupě $\mathrm{Gp}(H; t_i,\ i \in I)$. Proto stačí ověřit rovnost $H = H_{\boldsymbol{\varphi}} \cap G$. Ta však plyne okamžitě z toho, že HNN-redukované posloupnosti délky nula v HNN-rozšíření $H_{\boldsymbol{\varphi}}$ odpovídají prvkům H. □

Pro $m \in \mathbb{N}_0$ označme F_m volnou grupu s bazí

$$B_m = \{a_0, b_0, c_0, \ldots, a_m, b_m, c_m\}.$$

Každé posloupnosti $\boldsymbol{z} = (z_0, \ldots, z_m)$ celých čísel přiřaďme prvek $w_{\boldsymbol{z}} \in F_m$ definovaný předpisem

$$w_{\boldsymbol{z}} = c_m^{-z_m} b_m^{-1} a_m^{-z_m} \cdots c_1^{-z_1} b_1^{-1} a_1^{-z_1} a_0^{z_0} b_0 c_0^{z_0} \cdots a_m^{z_m} b_m c_m^{z_m}.$$

Formuli φ v proměnných $x_0, \ldots, x_m$ přiřaďme grupu

$$G^\varphi = \mathrm{Gp}(w_{(z_0,\ldots,z_m)} \mid \varphi(z_0, \ldots, z_m)).$$

Lemma 5.13. *Pro každou elementární formuli φ v proměnných $x_0, \ldots, x_m$ je G^φ benigní podgrupou grupy F_m.*

Důkaz. Nahradíme-li v množině B_m některé z prvků b_i součiny $a_i b_i c_i$ dostaneme opět množinu volných generátorů grupy F_m. Proto je adjunkcí stabilizujících prvků t_i takových, že $t_i^{-1} b_i t_i = a_i b_i c_i$ a t_i komutuje se zbylými prvky báze B_m a t_{ij} takových, že $t_{ij}^{-1} b_i t_{ij} = a_i b_i c_i$, $t_{ij}^{-1} b_j t_{ij} = a_j b_j c_j$ a t_{ij} komutuje se zbylými prvky B_m definováno HNN-rozšíření grupy F_m. Označme jej F_m^*. Označme $\boldsymbol{e}_i$ posloupnost $(z_0, \ldots, z_m)$ takovou, že $z_i = 1$ a $z_j = 0$ pro $j \neq i$. Snadno ověříme, že pro celé číslo d a posloupnost $\boldsymbol{z} = (z_0, \ldots, z_m) \in \mathbb{Z}^{m+1}$ platí vztahy

$$t_i^{-d} w_{\boldsymbol{z}} t_i^d = w_{\boldsymbol{z}+d\boldsymbol{e}_i}, \tag{5.3}$$

$$t_{ij}^{-d} w_{\boldsymbol{z}} t_{ij}^d = w_{\boldsymbol{z}+d\boldsymbol{e}_i+d\boldsymbol{e}_j}. \tag{5.4}$$

Buď φ elementrní formule tvaru $x_i = c$. Položme

$$H^\varphi = \mathrm{Gp}(w_{c\boldsymbol{e}_i}, t_j,\ i \neq j).$$

Z formule (5.3) plyne, že $G^\varphi \subseteq H^\varphi \cap F_m$. Navíc, z (5.3) snadno odvodíme, že $G^\varphi = t_j^{-1} G^\varphi t_j$ pro každé $j \neq i$- Proto vzhledem k Lemmatu 5.12 platí také opačná inkluze. Odtud dostáváme

$$G^\varphi = H^\varphi \cap F_m.$$

Protože jsou H^φ i F_m konečně generované podgrupy grupy F_m^*, která je konečně prezentovaná, jsou v ní podle Lemmatu 5.2 benigní. Z Lemmatu 5.3 plyne, že je také G^φ benigní v F_m^* a tedy je benigní v také v F_m.

Označme $\mathbf{0} = (0, \ldots, 0) \in \mathbb{Z}^{m+1}$. Pro elementární formule φ tvaru $x_i = x_j$ pro $i \neq j$ uvažme grupu

$$H^\varphi = \mathrm{Gp}(w_{\mathbf{0}}, t_{ij}, t_k\, k \neq i, j).$$

Ze vztahů (5.3) a (5.4) dostaneme podobně jako v předchozím případě použitím Lemmatu 5.12, že

$$G^\varphi = H^\varphi \cap F_m.$$

Odtud odvodíme, že G^φ je benigní podgrupou grupy F_m.

Nyní mějme elementární formuli φ tvaru $x_k = x_i + x_j$. V tomto případě buď

$$H^\varphi = \mathrm{Gp}(w_{\mathbf{0}}, , t_{ik}, t_{jk}, t_l,\ l \neq i, j, k).$$

Pomocí Lemmatu 5.12 a vztahů (5.3), (5.4) opět odvodíme, že

$$G^\varphi = H^\varphi \cap F_m,$$

odkud dostaneme, že G^φ je benigní podgrupou grupy F_m.

Nakonec, buď φ elementární formule tvaru $x_k = x_i x_j$, kde $k < i < j$. V tomto případě je situace složitější. Uvažme homomorfismus $\psi'_{j;ik}\colon F_m * \langle t_k\rangle \to \mathrm{Gp}(F_m, t_k)$ definovaný předpisy $\psi'_{j;ik}(b_j) = a_j b_j c_j$, $\psi'_{j;ik}(c_i) = t_k c_i$ a zbylé generátory grupy F_m a prvek t_k se zobrazí na sebe. Ověříme, že $\psi'_{j;ik}$ splňuje definující relace grupy $\mathrm{Gp}(F_m, t_k)$ a proto se faktorizuje přes endomorfismus $\psi_{j;ik}\colon \mathrm{Gp}(F_m, t_k) \to \mathrm{Gp}(F_m, t_k)$ jak je znázorněno na následujícím obrázku (π značí kanonickou projekci).

$$\begin{array}{ccc} F_m * \langle t_k\rangle & & \\ \downarrow{\scriptstyle \pi} & \searrow^{\psi'_{j;ik}} & \\ \mathrm{Gp}(F_m, t_k) & \xrightarrow{\psi_{j;ik}} & \mathrm{Gp}(F_m, t_k). \end{array}$$

Je zřejmé, že $\psi'_{j;ik}$ splňuje definující relace neobsahující prvky b_j a c_i. Pro zbylou dvojici relací ověříme, že platí

$$\begin{aligned} \psi'_{j;ik}(t_k^{-1} b_j t_k) &= t_k^{-1} a_j b_j c_j t_k = a_j b_j c_j = \psi'_{j;ik}(b_j),\\ \psi'_{j;ik}(t_k^{-1} c_i t_k) &= t_k^{-1} t_k c_i t_k = c_i t_k = t_k c_i = \psi'_{j;ik}(c_i). \end{aligned}$$

Podobně ověříme, že se homomorfismus ${\psi'_{j;ik}}^{-1}\colon F_m * \langle t_k\rangle \to \mathrm{Gp}(F_m, t_k)$ definovaný předpisy ${\psi'_{j;ik}}^{-1}(b_j) = a_j^{-1} b_j c_j^{-1}$, ${\psi'_{j;ik}}^{-1}(c_i) = t_k^{-1} c_i$ a zbylé generátory grupy F_m a prvek t_k se zobrazí na sebe faktorizuje přes endomorfismus $\psi^{-1}_{j;ik}$ grupy $\mathrm{Gp}(F_m, t_k)$. Z definujících předpisů obou zobrazení je vidět, že $\psi_{j;ik}$ a $\psi^{-1}_{j;ik}$ jsou vzájemně inverzní automorfimy grupy $\mathrm{Gp}(F_m, t_k)$, speciálně $\psi_{j;ik}$ je automorfismus. Podobně ukážeme, že je předpisy $\psi_{i;jk}(b_i) = a_i b_i c_i$, $\psi_{i;jk}(c_j) = t_k c_j$ a zbylé generátory grupy F_m a prvek t_k se zobrazí na sebe určen automorfismus grupy $\mathrm{Gp}(F_m, t_k)$. Odtud plyne, že přidáním stabilizujících prvků $s_{j;ik}$, resp. $s_{i;jk}$ splňujících $s^{-1}_{j;ik} b_j s^{-1}_{j;ik} = a_j b_j c_j$ a $s^{-1}_{j;ik} c_i s_{j;ik} = t_k c_i$, resp. $s^{-1}_{i;jk} b_i s^{-1}_{i;jk} = a_i b_i c_i$ a $s^{-1}_{i;jk} c_j s_{i;jk} = t_k c_j$ a komutujících se zbylými generátory grupy F_m a s prvkem t_k dostaneme HNN-rozšíření grupy F_m^*. Označme jej F_m^{**}. S využitím toho, že $k < i, j$ snadno spočteme, že pro $d \in \mathbb{Z}$ a $\boldsymbol{z} = (z_0, \dots, z_m) \in \mathbb{Z}^{m+1}$ platí

$$s^{-d}_{j;ik} w_{\boldsymbol{z}} s^d_{j;ik} = w_{\boldsymbol{z}+d\boldsymbol{e}_j+dz_i\boldsymbol{e}_k} \text{ a } s^{-d}_{i;jk} w_{\boldsymbol{z}} s^d_{i;jk} = w_{\boldsymbol{z}+d\boldsymbol{e}_i+dz_j\boldsymbol{e}_k}. \tag{5.5}$$

Položme

$$H^\varphi_* = \mathrm{Gp}(w_{\mathbf{0}}, s_{j;ik}, s_{i;jk}, t_l,\ l \neq i,j,k), \quad H^\varphi = \mathrm{Gp}(G^\varphi, t_l,\ l \neq i,j,k).$$

Z rovností (5.3) a (5.5) plyne, že $G^\varphi \leq H^\varphi_*$ a tedy $H^\varphi \leq H^\varphi_*$. Všimněme si, že $G^\varphi = H^\varphi \cap \mathrm{Gp}(G^\varphi, t_k)$. Z rovností (5.5) plyne, že $s^{-1}_{j;ik} G^\varphi s_{j;ik} = G^\varphi$ a $s^{-1}_{i;jk} G^\varphi s_{i;jk} = G^\varphi$. Podle Lemmatu 5.12 je potom

$$H^\varphi = H^\varphi_* \cap F^*_m. \tag{5.6}$$

Z rovností (5.3) je vidět, že $t_l^{-1} G^\varphi t_l^{-1} = G^\varphi$ pro každé $l \neq i,j,k$, odkud vhledem k Lemmatu 5.12 plyne, že

$$G^\varphi = H^\varphi \cap F_m. \tag{5.7}$$

Protože, H^φ_* a F_m a F^*_m jsou konečně generované podgrupy konečně prezentované grupy F^{**}_m, dotaneme z rovnosti (5.6), že H^φ je benigní v F^*_m a následně z rovnosti (5.7), že G^φ je benigní v F_m. □

Lemma 5.14. *Buď S rekurzivně spočetná množina celých čísel. Potom je grupa*

$$G^S = \mathrm{Gp}(a_0^{z_0} b_0 c_0^{z_0} \mid z_0 \in S)$$

benigní podgrupou grupy F_0.

Důkaz. Protože je množina S rekurzivně spočetná, existuje podle Lemmatu 5.11 konjunkce elementárních formulí (v proměnných $x_0, \ldots, x_n$ pro vhodné $n \in \mathbb{N}_0$)

$$\Phi = \bigwedge_{i=0}^{t} \varphi_t$$

tak, že celé číslo $z_0 \in S$ právě když existují $z_1, \ldots, z_m \in \mathbb{Z}$ pro které platí $\Phi(z_0, \ldots, z_m)$. Nejprve ověřme, že platí

$$G^\Phi = \bigcap_{i=0}^{t} G^{\varphi_t}. \tag{5.8}$$

Snadno nahlédneme že je množina B_m N-redukovaná a proto tvoří volnou bázi grupy F_m. Speciálně pro každou formuli φ tvoří množina $B^\varphi = \{w_{\boldsymbol{z}} \mid \varphi(\boldsymbol{z})\}$ volnou bázi grupy G^φ. Proto $g = w^{\varepsilon_0}_{\boldsymbol{z}_0} \ldots w^{\varepsilon_k}_{\boldsymbol{z}_k} \in G^\varphi$ právě když $\varphi(w_j)$ pro všechna $j \in \{0, \ldots, k\}$. Odtud vidíme, že $g = w^{\varepsilon_0}_{\boldsymbol{z}_0} \ldots w^{\varepsilon_k}_{\boldsymbol{z}_k} \in G^\Phi$ právě když $\Phi(\boldsymbol{z}_j)$ pro všechna j. To nastane právě když $\varphi_i(\boldsymbol{z}_j)$ pro každé j a každé i, což je ekvivalentní $g \in \bigcap_{i=0}^t G^{\varphi_i}$. Tím je rovnost (5.8) ověřena. Z této rovnosti a z Lemmatu 5.3 plyne, že G^Φ je benigní v F_m.

Nyní ověřme rovnost

$$G^S = \mathrm{Gp}(G^\Phi, a_i, b_i, c_i,\ 1 \leq i \leq m) \cap F_0. \tag{5.9}$$

Buď $\rho\colon F_0 \to F_m$ přirozené vnoření, tj. $a_0 \mapsto a_0, b_0 \mapsto b_0$ a $c_0 \mapsto c_0$ s retraktem $\pi\colon F_m \to F_0$ (definovaným předpisy $a_0 \mapsto a_0, b_0 \mapsto b_0, c_0 \mapsto c_0$ a $a_i \mapsto 0, b_i \mapsto 0, c_i \mapsto 0$ pro $1 \leq i \leq m$). Buď $w_{\boldsymbol{z}_0}^{\varepsilon_0} \dots w_{\boldsymbol{z}_k}^{\varepsilon_k} \in G^\Phi$, kde $\boldsymbol{z}_j = (z_0^j, \dots, z_m^j)$. Potom pro každé $0 \leq j \leq m$ platí $\Phi(\boldsymbol{z}_j)$ a tedy $z_0^j \in S$. Proto $\pi(G^\Phi) = G^S$. Označme $F_m^\Phi = \mathrm{Gp}(G^\Phi, a_i, b_i, c_i,\ 1 \leq i \leq m)$. Potom

$$F_m^\varphi \cap F_0 = \pi(F_m^\varphi) = \pi(G^\Phi) = G^S,$$

což je (5.9). Z Lemmatu 5.4 plyne, že F_m^Φ je benigní podgrupou F_m. Z Lemmatu 5.3 pak dostaneme, že G^S je benigní v F_m a tedy je benigní i v F_0. □

Věta 5.15 (Novikov-Booneova)**.** *Existuje konečně prezentovaná grupa H, která nemá řešitelný problém slov.*

Později si ukážeme, že Novikov-Booneova věta je přímým důsledkem Higmanovy vnořovací věty. Relativně snadno ji však můžeme dokázat již z Lemmatu 5.14.

Důkaz. Podle Tvrzení 5.7 existuje rekurzivně spočetná nerekurzivní podmnožina S přirozených čísel. Podle Lemmatu 5.14 je

$$G = \mathrm{Gp}(a^z b c^z \mid z \in S)$$

benigní podgrupou grupy $F = \langle a, b, c\rangle$. Proto existuje konečně prezentovaná grupa H obsahující HNN-rozšíření

$$F_G = \left\langle F; t \mid t^{-1} g t = g,\ g \in G \right\rangle.$$

Snadno ověříme, že je množina

$$B = \{a^z b c^z \mid z \in \mathbb{Z}\}$$

N-redukovaná a tedy tvoří volnou bázi grupy $\mathrm{Gp}(B)$. Odtud plyne, že $a^z b c^z \in G$ právě když $z \in S$. Je však

$$a^z b c^z \in G \text{ právě když } t^{-1}(a^z b c^z) t = a^z b c^z. \tag{5.10}$$

Kdyby měla grupa H řešitelný problém slov, dokázali bychom na základě (5.10) rozhodnout, zda celé číslo z leží v S, což je spor s tím, že množina S není rekurzivní. □

5.4. **Higmanova vnořovací věta.** V poslední části této kapitoly dokážeme Higmanovu vnořovací větu. Základem našeho důkazu, podobně jako v případě věty Novikov-Booneovy, bude Lemma 5.14. Nejprve si však ukažme další užitečnou vlastnost benigních podgrup.

Lemma 5.16. *Buď H benigní podgrupa konečně generované grupy G. Označme N normální podgrupu grupy G generovanou podgrupou H, tj. $N = G^{-1}HG$. Potom je faktor-grupu G/N možné vnořit do konečně prezentované grupy.*

Důkaz. Buď $\overline{G}$ izomorfní kopie grupy G. Pro $g \in G$ označme $\overline{g}$ odpovídající prvek v $\overline{G}$. Podobně označme $\overline{H}$, resp. $\overline{N}$ podgrupy $\overline{G}$ odpovídající podgrupám H, resp. N grupy G. V grupě

$$G_H = \left\langle G; t \mid t^{-1}ht = h,\, h \in H \right\rangle$$

uvažme podgrupu $U = \mathrm{Gp}(G, t^{-1}Gt)$ na kterou můžeme nahlížet jako na amalgám grup G a $t^{-1}Gt$ podle společné podgrupy H. Buď $\pi\colon G \to G/N$ přirozená projekce a $\overline{\pi}\colon G \to \overline{G}/\overline{N}$ zobrazení dané přiřazením $g \mapsto \overline{\pi(g)}$. Jádrem projekce $\overline{\pi}$ je normální podgrupa N obshující H. Proto je možné zobrazení $\overline{\pi}$ spolu se zobrazením $t^{-1}Gt \to \overline{G}/\overline{N}$, které přiřadí každému prvku jednotku v grupě $\overline{G}/\overline{N}$ jednoznačně rozšířit na projekci $\Phi\colon U \to \overline{G}/\overline{N}$.

Podle předpokladu je možné vnořit grupu G_H do konečně prezentované grupy P. Přiřazením $(u, 1) \mapsto (u, \Phi(u))$ je definován izomorfismus grupy $U \times \mathbf{1}$ na podgrupu kartézského součinu $P \times \overline{G}/\overline{N}$. Uvažme HNN-rozšíření

$$Q = \left\langle P \times \overline{G}/\overline{N}; s \mid s^{-1}(u,1)s = (u, \Phi(u)), u \in U \right\rangle. \tag{5.11}$$

Je evidentní, že grupu G/N můžeme vnořit do grupy Q. K dokončení důkazu tedy stačí ověřit, že grupa Q je konečně prezentovaná. Podle předpokladu jsou grupy G a P konečně generované. Buď A konečná množina generátorů grupy G a B konečná množina generátorů grupy P obsahující t a množinu A. Buď

$$P = \langle B \mid \Delta \rangle$$

konečná prezentace grupy P. Potom je grupa Q generovaná prvkem s a sjednocením $(B \times \mathbf{1}) \cup (\mathbf{1} \times \overline{A})$, kde $\overline{A}$ odpovídá obrazu množiny A v $\overline{G}/\overline{N}$ a grupa U je generovaná konečnou množinou $A \cup t^{-1}At$. Proto můžeme množinu relací v prezentaci (5.11) nahradit její konečnou podmnožinou $\Gamma = \{s^{-1}(u,1)s \mid u \in A \cup t^{-1}At\}$. Ukážeme, že

$$Q = \left\langle B \times \overline{A}, s \mid \Delta \times \mathbf{1}, \Gamma \right\rangle \tag{5.12}$$

K tomu stačí ukázat, že relace definující podgrupu $\mathbf{1} \times \overline{G}/\overline{N}$ v Q, tedy relace $(1, \overline{w}) = 1$, kde w je slovo nad A jehož součin a je prvkem N, jsou důsledky relací $(\Delta \times \mathbf{1}) \cup \Gamma$ v prezentaci (5.12). Protože $N = G^{-1}HG$, stačí se omezit na relace, kde $a \in H$. Důsledkem relací definujících

Δ je rovnost $a = t^{-1}at$. Důsledky relací Γ jsou rovnosti $s^{-1}(a,1)s = (a,\Phi(a)) = (a,\overline{a})$ a $s^{-1}(t^{-1}at,1)s = (a,1)$. Odtud dostaneme

$$(a,\overline{a}) = s^{-1}(a,1)s = s^{-1}(t^{-1}at,1)s = (a,1).$$

Po krácení prvkem $(a,1)$ dostaneme rovnost $(1,\overline{a}) = 1$, což zbývalo ověřit. □

Nyní budeme směřovat k důkazu hlavní věty této kapitoly. Uvažme volnou grupu $D = \langle a,b\rangle$. Připomeňme, že slovem nad množinou $\{a,b\}$ rozumíme posloupnost $x_0,\dots,x_{n-1}$, kde každé x_i je jedním ze znaků a, b, a^{-1}, b^{-1}. Soubor všech slov nad množinou $\{a,b\}$ označme $\mathcal{W}_{\{a,b\}}$. Definujme

$$\gamma(a) = 1,\ \gamma(b) = 2,\ \gamma(a^{-1}) = 3,\ \gamma(b^{-1}) = 4$$

a slovu $w = x_0,\dots,x_{n-1}$ přiřaďme přirozené číslo

$$\gamma(w) = 10^{n-1}\gamma(x_0) + 10^{n-2}\gamma(x_1) + \cdots + 10\gamma(x_{n-2}) + \gamma(x_{n-1}),$$

tj. číslo takové, že $\gamma(x_0)\dots\gamma(x_{n-1})$ je zápis hodnoty $\gamma(w)$ v desítkové soustavě. Například

$$\gamma(a^2b^{-1}a^{-3}b^3) = \gamma(aab^{-1}a^{-1}a^{-1}a^{-1}bbb) = 114333222.$$

Máme tak efektivně popsáno vnoření $\gamma\colon \mathcal{W}_{\{a,b\}} \to \mathbb{N}$. Pro podmnožinu Δ množiny $\mathcal{W}_{\{a,b\}}$ položme $\gamma(\Delta) = \{\gamma(w) \mid w \in \Delta\}$.

Lemma 5.17. *Buď $F = \langle a,b,c,d,e,h\rangle$. Pro každé $w \in \mathcal{W}_{\{a,b\}}$ položme*

$$g_w = whc^{\gamma(w)}de^{\gamma(w)}.$$

Potom je

$$G = \mathrm{Gp}(g_w \mid w \in \mathcal{W}_{\{a,b\}})$$

benigní podgrupou grupy F.

Důkaz. Položme $A = \{a,\ b,\ a^{-1},\ b^{-1}\}$. Pro každé $\lambda \in A$ převedeme Nielsenovou transformací $\lambda h \to h$ množinu

$$B_\lambda = \{a,b,c^{10},c^{\gamma(\lambda)}de^{\gamma(\lambda)},e^{10},\lambda h\}$$

na množinu která je N-redukovaná. Odtud plyne, že množina B_λ volně generuje podgrupu F_λ grupy F. Proto adjunkcí stabilizujících prvků

t_λ, $\lambda \in A$, splňujících relace

$$\begin{aligned} t_\lambda^{-1} a t_\lambda &= a, \\ t_\lambda^{-1} b t_\lambda &= b, \\ t_\lambda^{-1} c t_\lambda &= c^{10}, \\ t_\lambda^{-1} d t_\lambda &= c^{\gamma(\lambda)} d e^{\gamma(\lambda)}, \\ t_\lambda^{-1} e t_\lambda &= e^{10}, \\ t_\lambda^{-1} h t_\lambda &= \lambda h \end{aligned}$$

dostaneme HNN-rozšíření grupy F, které označíme F^*. Z těchto relací snadno odvodíme, že pro každé $v \in \mathcal{W}_{\{a,b\}}$ a každé $\lambda \in A$ platí

$$t_\lambda^{-1} g_v t_\lambda = g_{v^\wedge\lambda}. \tag{5.13}$$

Protože je grupa F^* konečně prezentovaná, jsou její konečně generované podgrupy $\mathrm{Gp}(hd, t_a, t_{a^{-1}}, t_b, t_{b^{-1}})$ a F benigní. Ukážeme, že

$$G = \mathrm{Gp}(hd, t_a, t_{a^{-1}}, t_b, t_{b^{-1}}) \cap F,$$

odkud vzhledem k Lemmatům 5.2 a 5.3 dostaneme, že G je benigní podgrupa F, tedy dokazovné. Protože $g_\emptyset = hd$, plyne z (5.13) inkluze

$$G \subseteq \mathrm{Gp}(hd, t_a, t_{a^{-1}}, t_b, t_{b^{-1}}) \cap F.$$

Zbývá ukázat opačnou inkluzi. Podle Lemmatu 5.12 k tomu stačí ověřit pro každé $\lambda \in A$ rovnost

$$t_\lambda^{-1} G t_\lambda = F_\lambda \cap G.$$

Z rovnosti (5.13) plyne, že

$$t_\lambda^{-1} G t_\lambda = \mathrm{Gp}(t_\lambda^{-1} B t_\lambda) = \mathrm{Gp}(g_{v^\wedge\lambda} \mid v \in \mathcal{W}_{\{a,b\}}),$$

tedy je to podgrupa G generovaná těmi g_w pro které končí slovo w znakem λ. Naopak, $g_w \in F_\lambda$ právě když $\gamma(w) \equiv \gamma(\lambda) \pmod{10}$ což nastane právě když slovo w končí znakem λ. Odtud plyne inkluze

$$t_\lambda^{-1} G t_\lambda \subseteq F_\lambda \cap G.$$

Množina $B = \{g_w \mid w \in \mathcal{W}_{\{a,b\}}\}$ je N-redukovaná a tedy volně generuje grupu G. Navíc, je-li $g_{w_1}^{\varepsilon_1}, \ldots, g_{w_m}^{\varepsilon_m}$ slovo nad B v redukovaném tvar, potom se v jeho redukovaném součinu v F úseky $(hc^{\gamma(w_i)}d)^{\varepsilon_i}$ nezkrátí. Buď nyní w slovo v redukovaném tvaru jehož součin leží v F_λ. Obsahuje-li slovo w úsek jehož součin je $(hc^{\gamma(w_i)}d)^{\varepsilon_i}$, potom nutně $\gamma(w_i) \equiv \gamma(\lambda) \pmod{10}$, a tedy slovo w končí znakem λ. Odtud plyne, že

$$F_\lambda \cap G \subseteq t_\lambda^{-1} G t_\lambda.$$

□

Dříve než zformulujeme Higmanovu větu o vnoření, musíme definovat rekurzivně generovanou grupu: Grupa G je *rekurzivně prezentovaná* má-li prezentaci

$$G = \langle X \mid \Delta \rangle$$

v níž X je konečná množina a $\gamma(\Delta)$ je rekurzivně spočetná množina. Intuitivně, grupa je rekurzivně prezentovaná, pokud je konečně generovaná a existuje algoritmus, který postupně najde všechny její definující relace. Tento algoritmus snadno modifikujeme tak, aby našel všechny slova nad množinou generátorů X jejichž součin je v grupě G roven jednotce. Odtud je vidět, že konečně generovaná podgrupa rekurzivně prezentované grupy je rekurzivně prezentovaná.

Věta 5.18 (Higmanova)**.** *Konečně generovaná grupa je rekurzivně prezentovaná právě když je vnořitelná do konečně prezentované grupy.*

Důkaz. Z úvah uvozujících formulaci Higmanovy věty plyne, že každá konečně generovaná podgrupa konečně prezentované grupy je rekurzivně prezentovaná. Zbývá ukázat opačnou implikaci. Podle Věty 4.1 je možné každou spočetnou grupu G vnořit do grupy H_φ generované dvěma prvky. Navíc v důkaze této věty je popsáno, jak efektivně transformovat množinu relací z prezentace grupy G na množinu relací v prezentaci grupy H_φ. Odtud je vidět, že je-li grupa G rekurzivně prezentovaná, je také grupa H_φ rekurzivné prezentovaná. Proto se ve zbytku důkazu můžeme omezit na rekurzivně prezentované grupy generované dvěma prvky.

Podobně jako v Lemmatu 5.17 buď $F = \langle a, b, c, d, e, h \rangle$ a $G = \mathrm{Gp}(g_w \mid w \in \mathcal{W}_{\{a,b\}})$. Buď Δ libovolná podmnožina $\mathcal{W}_{\{a,b\}}$. Položme

$$G_\Delta = \mathrm{Gp}(g_w \mid w \in \Delta) \text{ a } U_\Delta = \mathrm{Gp}(a, b, h, c^\alpha d e^\alpha,\ \alpha \in \gamma(\Delta)).$$

Podobně jako v závěru důkazu Lemmatu 5.17 ukážeme, že

$$G_\Delta = U_\Delta \cap G. \tag{5.14}$$

Přímo z definice množiny U_Δ je vidět, že $\{g_w \mid w \in \Delta\} \subseteq U_\Delta$, odkud plyne inkluze $G_\Delta \subseteq U_\Delta \cap G$. Naopak, úseky tvaru $(hc^{\gamma(w_i)}d)^{\varepsilon_i}$ se v redukovaných tvarech prvků z U_Δ nekrátí, odkud plyne, že je-li prvek z $U_\Delta \cap G$ součinem redukované posloupnosti $g_{w_1}^{\varepsilon_1}, \ldots, g_{w_m}^{\varepsilon_m}$, jsou $\gamma(w_i) \in \Delta$ a tedy slova w_i jsou z Δ. Proto $U_\Delta \cap G \subseteq G_\Delta$. Nyní,

$$\begin{aligned} &\mathrm{Gp}(G_\Delta; c, d, e, h) = \mathrm{Gp}(\{g_w \mid w \in \Delta\}; c, d, e, h) = \\ &= \mathrm{Gp}(\{w \mid w \in \Delta\}; c, d, e, h) = \mathrm{Gp}(\Delta) * \langle c, d, e, h \rangle. \end{aligned}$$

Proto

$$\mathrm{Gp}(G_\Delta; c, d, e, h) \cap \langle a, b \rangle = (\mathrm{Gp}(\Delta) * \langle c, d, e, h \rangle) \cap \langle a, b \rangle = \mathrm{Gp}(\Delta).$$

Z rovnosti (5.14) pak plyne, že

$$\mathrm{Gp}(\Delta) = \mathrm{Gp}(U_\Delta \cap G; c, d, e, h) \cap \langle a, b\rangle.$$

Podle Lemmat 5.14, resp. 5.17 jsou podgrupy U_Δ, resp. G benigní v F. Pomocí Lemmat 5.1 - 5.4 odtud odvodíme, že $\mathrm{Gp}(\Delta)$ je benigní podgrupa $\langle a, b\rangle$. Podle Lemmatu 5.16 je pak grupa $\langle a, b \mid \Delta\rangle$ vnořitelná do konečně prezentované grupy. □

Na závěr této kapitoly se podívejme na to, jak pomocí Higmanovy vnořovací věty ukázat existenci konečně prezentované grupy s neřešitelným problémem slov. Buď $F = \langle a_0, a_1, b_0, b_1\rangle$ volná grupa a uvažme její podgrupy

$$G_i = \mathrm{Gp}(a_i^{-n} b a_i^n \mid n \in \mathbb{N}),\ i = 0, 1,$$

které jsou volně generované N-redukovanými množinami $\{a_i^{-n} b a_i^n \mid n \in \mathbb{N}\}$, $i = 0, 1$. Buď S rekurzivně spočetná množina přirozených čísel, která není rekurzivní. HNN-rozšíření

$$H = \left\langle F; t \mid t^{-1}(a_0^{-n} b a_0^n)t = a_1^{-n} b a_1^n,\ n \in S\right\rangle$$

je rekurzivně prezentované a proto je vnořitelné do konečně prezentované grupy E. Přitom z Brittonova lemmatu plyne, že

$$t^{-1}(a_0^{-n} b a_0^n)t = a_1^{-n} b a_1^n \tag{5.15}$$

právě když $n \in S$ (pokud totiž $n \notin S$, je $t^{-1}, (a_0^{-n} b a_0^n), t, (a_1^{-n} b a_1^n)^{-1}$ HNN-redukovaná posloupnost a její součin je proto různý od jednotky). Kdyby grupa E měla řešitelný problém slov, existoval by algoritmus jež pro dané $n \in \mathbb{N}$ rozhodne zda platí rovnost (5.15) a tak zda $n \in S$. To je ve sporu s tím, že množina S není rekurzivní.

Dalším důsledkem Higmanovy vnořovací věty je existence konečně generované grupy, která není rekurzivně prezentovaná.

Důsledek 5.19. *Existuje grupa generovaná dvěma prvky nekonečného řádu, která není rekurzivně prezentovaná.*

Důkaz. Existuje jen spočetně mnoho vzájemně neizomorfních konečně prezentovaných grup a každá obsahuje jen spočetně mnoho konečně generovaných podgrup. Podle Důsledku 4.2 existuje $2^{\aleph_0}$ vzájemně neizomorfních grup generovaných dvěma prvky nekonečného řádu. Proto je mezi nimi grupa, kterou nelze vnořit do konečně prezentované grup. Ta podle Higmanovy vnořovací věty nemá rekurzivně spočetnou prezentaci. □