KOMBINATORICKÁ TEORIE GRUP

1. Volná grupa

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).

$$\begin{tikzcd} X \arrow[r, phantom, "\subseteq"] \arrow[dr, "f"'] & F \arrow[d, "\exists!\varphi"] \\ & G \end{tikzcd}$$

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 $w = x_0, \dots, x_{n-1}$, 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 $v = x_0, \dots, x_{n-1}$ a $w = y_0, \dots, y_{m-1}$ budeme rozumět slovo $v^\wedge w = x_0, \dots, x_{n-1}, y_0, \dots, y_{n-1}$.

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 $w = x_0, \dots, x_{n-1}$ položme $w^{-1} = x_{n-1}^{-1}, \dots, x_0^{-1}$.

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. $\square$

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 $x_0, \dots, x_{n-1}$ nad X.

Důkaz. Je-li podmínka (1.2) splňena, 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 $x_0, \dots, x_{n-1}$ pak platí

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

odkud plyne (1.2). $\square$

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

2. Nielsenovsky redukovaná množina

3. Nielsen

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 3.1. *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. $\square$

4. HNN-rozšíření a amalgámy grup

4.1. **HNN-rozšíření.** Budeme užívat následující značení: Je-li dána grupa G s prezentací $\langle X \mid R \rangle$, označíme symbolem $\langle G; Y \mid S \rangle$ grupu s prezentací $\langle X \cup Y \mid R \cup S \rangle$, přitom automaticky 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

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

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

Fixujme si jedno takové HNN-rozšíření G_φ. Níže budeme pracovat s posloupnostmi tvaru g_0, $t^{\varepsilon_1}, \dots, t^{\varepsilon_n}$, 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* této posloupnosti.

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, $t^{\varepsilon_1}, \dots$, t^{ε_n}, $g_n \in \mathcal{V}$ je v *redukovaném tvaru* pokud neobsahuje štěp.

Lemma 4.1. *Každý prvek $g \in G_\varphi$ je součinem posloupnosti v 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 redukovaném tvaru. Nechť je to posloupnost g_0, $t^{\varepsilon_1}, \dots, t^{\varepsilon_n}$, g_n. Pro spor předpokládejme, že posloupnost není v redukovaném tvaru. Potom obsahuje štěp t^{ε_i}, g_i, $t^{\varepsilon_{i+1}}$, který lze nahradit prvkem $\varphi^{-\varepsilon_i}$. Tak dostaneme posloupnost g_0, $t^{\varepsilon_1}, \dots, t^{\varepsilon_{i-1}}$, $g_{i-1}\varphi^{-\varepsilon_i}(g_i)g_{i+1}$, $t^{\varepsilon_{i+2}}, \dots, t^{\varepsilon_n}$, g_n z $\mathcal{V}$ délky $n-2$ jejímž součinem je opět prvek g. To je ve sporu s minimalitou délky původně zvolené posloupnosti. $\square$

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, reprezentanty zvolených pravých rozkladových tříd podle podgrup A, resp. B, takové, že $Ag \in Ag^A$, resp. $Bg \in Bg^B$.

Definice. Řekneme, že posloupnost $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n \in \mathcal{V}$ 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 4.2. *Buď $g \in G_\varphi$ součinem posloupnosti g_0, $t^{\varepsilon_1}, \dots,$ t^{ε_n}, g_n v redukovaném tvaru. Potom je g součinem nějaké posloupnosti h_0, $t^{\varepsilon_1}, \dots,$ t^{ε_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 $n \geq 0$. 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 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^{ε_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 posloupnosti $g_0\varphi(a), t^{\varepsilon_1}$, h_1^A, $t^{\varepsilon_2}, \dots,$ t^{ε_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 $g_1 \in A$. To by ale znamenalo existenci štěpu $t^{\varepsilon_1}, g_1, t^{\varepsilon_2}$ v posloupnosti g_0, $t^{\varepsilon_1}, \dots,$ t^{ε_n}, g_n v redukovaném tvaru což vede ke sporu. 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 4.3 (O normálním tvaru)**.** *Každý prvek G_φ je součinem právě jedné posloupnosti v normálním tvaru.*

Důkaz. Vzhledem k Lemmatu 4.1 je každý prvek $g \in G_\varphi$ součinem posloupnosti v redukovaném tvaru a podle Lemmatu 4.2 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^{ε_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, $t^{\varepsilon_1}, \ldots, t^{\varepsilon_n}$, $g_n \in \mathcal{W}$. Nejprve rozložme $g_0 = b_0 g_0^B$ (kde $b_0 \in B$) a definujme

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

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

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

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

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

Protože je posloupnost $g_0, t^{\varepsilon_1}, \ldots, t^{\varepsilon_n}, g_n$ 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

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

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

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

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^{ε_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. $\square$

Věta 4.4 (Brittonovo lemma)**.** *Předpisem, který prvku $g \in G$ přiřadí součin redukované posloupnosti g délky nula je definováno vnoření $G \hookrightarrow G_\varphi$. Je-li $g_0, t^{\varepsilon_1}, \dots, t^{\varepsilon_n}, g_n$ posloupnost v 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 4.2 plyne, že je-li $g \in G_\varphi$ součinem posloupnosti v redukovaném tvaru kladné délky je také součinem posloupnosti v normálním tvaru kladné délky. Z Věty 4.3 potom plyne, že tento součin je různý od jedné. $\square$

Lemma 4.5. *Nechť H je podgrupa grupy G a nechť $\varphi\colon A \to B$ je izomorfismus dvou podgrup grupy H. Potom je H_φ podgrupa grupy G_φ.*

Důkaz. Buď $h \in H_\varphi$ různý od jednotky. Potom je h součinem posloupnosti h_0, t^{ε_1}, $h_1, \dots,$ t^{ε_n}, h_n v redukovaném tvaru. Dle Brittonova lemmatu je součin této posloupnosti v grupě B_φ různý od jednotky, odkud plyne dokazované. $\square$

S HNN-rozšířením můžeme pracovat i v případě, že máme dán 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 $\boldsymbol{\varphi}_J = \{\varphi_j\colon A_j \to B_j \mid j \in J\}$ izomorfismů. Potom grupu

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

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, $t_{j_1}^{\varepsilon_1}, \dots, t_{j_n}^{\varepsilon_n}$, g_n, kde $g_i \in G$, $\varepsilon_i \in \{-1, 1\}$ a $j_i \in J$. Číslo n nazveme *délkou* této posloupnosti.

Definice. *Štěp* buď posloupnost tvaru $t_j^{\varepsilon}, g, t_j^{-\varepsilon}$ taková, že buďto $\varepsilon = -1$ a $g \in A_j$ nebo $\varepsilon = 1$ a $g \in B_j$ pro některé $j \in J$. Řekneme, že posloupnost g_0, $t_{j_1}^{\varepsilon_1}, \dots, t_{j_n}^{\varepsilon_n}$, $g_n \in \mathcal{V}_J$ je v *redukovaném tvaru* pokud neobsahuje štěp.

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

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

Je-li množina J nekonečná, snadno nahlédneme, že

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

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

Věta 4.6. *Předpisem, který prvku $g \in G$ přiřadí součin redukované posloupnosti g délky nula je definováno vnoření grupy G do $G_{\boldsymbol{\varphi}_J}$. Součin posloupnosti v redukovaném tvaru kladné délky je různý od jedné.*

4.2. **Amalgámy grup.**

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 danou prezentací

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

Snadno také nahlédneme, že grupa P je kolimitou diagramu

$$\begin{tikzcd} A \arrow[r, "j_0"] \arrow[d, "j_1"'] & G_0 \\ G_1 & \end{tikzcd}$$

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 $\{\varphi(a)a^{-1} \mid a \in A_0\}$.

Lemma 4.7. *Buď*

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

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

$$\begin{cases} \Phi(g) = t^{-1}gt & \text{pokud } g \in G_0 \\ \Phi(g) = g & \text{pokud } g \in G_1 \end{cases} \tag{4.1}$$

faktorizovat přes homomorfismus $\Psi\colon P \to (G_0 * G_1)_\varphi$.

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

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

□

Lemma 4.7 spočívá v komutativitě diagramu

$$\begin{tikzcd} G_0 * G_1 \arrow[d, "\Pi"'] \arrow[dr, "\Phi"] & \\ P \arrow[r, "\Psi"'] & (G_0 * G_1)_\varphi \end{tikzcd},$$

kde $\Pi\colon (G_0 * G_1) \to P$ je kanonická projekce s jádrem N.

Definice. Pro $i = 0, 1$ označme $G'_i = G_i \setminus A_i$. Řekneme, že posloupnost $g_0, \dots, g_n$ prvků volného součinu $G_0 * G_1$ je v *redukovaném tvaru*, jestliže

(i) každý z prvků g_i leží v některé z množin G'_0, G'_1;
(ii) je-li $g_i \in G'_j$, potom $g_{i+1} \in G'_{2-j}$;

Délkou poslopnosti v redukovaném tvaru rozumnějme číslo n

Lemma 4.8. *Každý prvek $g \in P \setminus \Pi(A_0)$ je součinem posloupnosti v redukovaném tvaru.*

Důkaz. Buď $g_0, \dots, g_n$ 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 $g_0 \notin G'_j$, pro vhodné $j \in \{0, 1\}$ a tedy zvolená posloupnost je redukovaná v P. Předpokládejme, že $n > 0$. Pokud by $g_i \in A_0$ pro některé $0 \le i \le n$, mohli bychom zvolenou posloupnost nahradit kratší posloupností $g_0, \dots,\ g_{i-2},\ g_{i-1}\varphi(g_i)g_{i+1},\ g_{i+2}, \dots,\ g_n$, která je opět v redukovaném tvaru. Pokud by $g_i \in A_1$ pro některé $0 \le i \le n$, mohli bychom analogicky zvolenou posloupnost nahradit kratší posloupností $g_0, \dots\ g_{i-2},\ g_{i-1}\varphi^{-1}(g_i)g_{i+1},\ g_{i+2}, \dots,\ g_n$ 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 redukovaném tvaru v P. □

Následující věta je analogií Brittonova lemmatu pro amalgám grup.

Věta 4.9. *Platí následující:*

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

Důkaz. Z první části Brittonova lemmatu snadno nahlédneme, že předpisy (4.1) 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 redukované posloupnosti délky 0 je různý od jedné. Buď $g_0, \dots, g_n$ redukovaná posloupnost kladné délky a g její součin. Z definice redukované posloupnosti je vidět, že obraz $\Psi(g) = \Psi(g_0) \cdots \Psi(g_n)$ je součinem redukované posloupnosti kladné délky v HNN-rozšíření $(G_0 * G_1)_\varphi$ a proto, podle Brittonova lemmatu, různý od jedné. Odtud plyne, že $g \neq 1$. Tím je dokázána část (b). $\square$

Z Věty 4.9 a z Lemmatu 4.8 okamžitě plyne, že:

Důsledek 4.10. *Zobrazení $\Psi\colon P \to (G_1 * G_2)_\varphi$ popsané v Lemmatu 4.7 je vnoření.*

...

Ještě tu bude více o vztahu HNN-rozšíření a amalgámů, konkrétně jak vnořit amalgám do HNN-rozšíření. Dále jek definovat amalgám více než dvou grup.

...

5. O vnoření spočetných grup

Věta 5.1. *Každou spočetnou grupu G můžeme vnořit do grupy H_φ generované dvěma prvky. Má-li navíc grupa G prezentaci s n-relacemi, existuje prentace grupy H_φ se dvěma generátory a n-relacemi.*

Důkaz. Uvažme prezentaci

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

grupy G, kde $X = \{g_1, g_2, \dots\}$ a $\Delta = \{\delta_1, \delta_2, \dots\}$ jsou spočetné (ne nutně nekonečné) množiny. Položme $H = G * \langle a, b \rangle$. Všimněmě si, že množina

$$A = \{b^{-i}ab^i \mid i \in \mathbb{N}_0\}$$

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

$$B = \{b, g_i a^{-i} b a^i \mid i \in \mathbb{N}\}.$$

Přiřazeními $b \mapsto a$, $a \mapsto b$ a $g_i \mapsto 1$, pro $i \in \mathbb{N}$, definujeme projekci grupy H na $\langle a, b \rangle$. Přitom obrazem množiny B je N-redukovaná množina A a proto je B bazí podgrupy 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

$$H_\varphi = \langle H; t \mid t^{-1}bt = a, t^{-1}g_i a^{-i} b a^i t = b^{-i} a b^i,\ i \in \mathbb{N} \rangle.$$

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

$$g_i = tb^{-i}ab^it^{-1}a^ib^{-1}a^{-i} = \underbrace{t^{i+1}a^{-1}t^{-i}at^iat^{-(i+1)}a^ita^{-1}t^{-i}a^{-i}}_{w_i}, \tag{5.1}$$

pro každé $i \in \mathbb{N}$, je grupa H_φ generovaná dvojicí prvků a, t. 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 (5.1), dostaneme prezentaci

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

grupy H_φ. Speciálně má-li grupa G prezentaci s n-relacemi $\delta_1, \ldots, \delta_n$, má grupa H_φ konečnou prezentaci s generátory a, t a n-relacemi $\gamma_1, \ldots, \gamma_n$. □

6. 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.

6.1. **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 6.1. *Nechť $H \le G \le E$ je řetízek grup. Je-li H benigní v E, potom je H benigní také v G.*

Důkaz. Podle Lemmatu 4.5 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 6.2. *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

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

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. $\square$

Lemma 6.3. *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 $G_{H_i} = \langle G, t_i \mid t_i^{-1}ht_i = h_i, h_i \in H_i\rangle$. 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

$$G_{H_{\pm1}} = \langle G; t_{-1}, t_1 \mid t_i^{-1}ht_i = h_i,\ h_i \in H_i,\ i = -1, 1\rangle$$

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):

$$\begin{tikzcd}
G \arrow[r] \arrow[d] & G_{H_{-1}} \arrow[r] \arrow[d] & E_{-1} \arrow[dd] \\
G_{H_1} \arrow[r] \arrow[d] & G_{H_{\pm1}} \arrow[dr] & \\
E_1 \arrow[rr] & & P
\end{tikzcd}$$

Položme $G_{H_{-1}\cap H_1} = \langle G; s \mid s^{-1}hs,\ h \in H_{-1} \cap H_1\rangle$. 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 $\varphi\colon G_{H_{-1}\cap H_1} \to G_{H_{\pm1}}$. 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 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 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}, t_{-1}^{-1}. Protože původní posloupnost $\boldsymbol{g}$ je v 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 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. □

Buď X podmnožina grupy G. Symbolem $\mathrm{Gp}(X)$ označíme podgrupu grupy G generovanou množinou X. Jsou-li navíc dány prvky $a_1, a_2, \ldots$ grupy G, budeme značit *$Gp(X; a_1, a_2, \ldots)$* podgrupu generovanou množinou X a danými prvky.

Lemma 6.4. *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 $G_{H_i} = \langle G, t_i \mid t_i^{-1} h t_i = h,\, h \in H_i \rangle$ 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

$$\mathrm{Gp}(H_0 \cup H_1) = \mathrm{Gp}(t_i^{-1} G t_i,\, i = 0, 1) \cap G. \tag{6.1}$$

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 $0 \le i < m$ 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 6.2 benigní v P. Z rovnosti (6.1) a Lemmatu 6.3 pak plyne, že $\mathrm{Gp}(H_0 \cup H_1)$ je benigní v P a vzhledem k Lemmatu 6.2 je benigní v G. □

6.2. **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 6.5. *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. $\square$

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 6.6 (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 6.6.

Tvrzení 6.7. *Existuje rekurzivně spočetná podmnožina přirozených čísel S, která není rekurzivní.*

Důkaz. Buď $X = \{x_0, x_1, \dots\}$ 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. $p_0 = 3$, $p_1 = 5$, $p_2 = 7$, $p_3 = 11, \dots$ atd. a posloupnosti $\boldsymbol{t} = t_0, \dots, t_n \in \mathbb{N}_0^{n+1}$ 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 $\boldsymbol{t} = t_0, \dots, t_n \in \mathbb{N}_0^{n+1}$ značme $\boldsymbol{x}^{\boldsymbol{t}} = x_0^{t_0} \cdots x_n^{t_n}$. Nyní, pro libovolný polynom

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

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

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

Položme

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

Postupně můžeme generovat všechny polynomy $P(x_0, \dots, x_n) \in P[X]$, pro každý spočítat $\gamma(P)$ a dosadit výslednou hodnotu za x_0. Dále budeme do výsledného polynonu v proměnných $x_1, \dots, x_n$ 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 $\mathbb{Z} \smallsetminus S$ rekurzivně spočetná a existují $n \in \mathbb{N}_0$ a polynom $P \in \mathbb{Z}[x_0, \dots, x_n]$ tak, že $z \in \mathbb{Z} \smallsetminus S$ právě když má $P(z, x_1, \dots, x_n)$ kořen v $\mathbb{Z}^n$. Odtud plyne, že $\gamma(P) \in \mathbb{Z} \smallsetminus S$ právě když má polynom $P(\gamma(P), x_1, \dots, x_n)$ kořen v $\mathbb{Z}^n$, což však nastane právě když $\gamma(P) \in S$. To je hledaný spor. $\square$

Definice. *Elementární formulí* rozumějme formuli $\varphi(x_0, \dots, x_m)$ 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 $\varphi_0, \dots, \varphi_t$ rozumíme formuli

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

Lemma 6.8. *Pro každé $n \in \mathbb{N}_0$ a každý polynom $P \in \mathbb{Z}[x_0, \dots, x_n]$ existují nezáporné celé číslo m a konjunkce elementárních formulí Φ_P tak, že $P(x_0, \dots, x_n) = y_m$ právě když $\Phi_P(x_0, \dots, x_n, y_0, \dots, y_m)$ pro nějaké $(y_0, \dots, y_{m-1}) \in \mathbb{Z}^m$.*

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 $P \in \mathbb{Z}[x_0, \dots, x_n]$ je tvaru

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

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 $P_1(x_0, \dots, x_n) = y_k$ právě když $\Phi_{P_1}(x_0, \dots, x_n, y_2, \dots, y_k)$ pro nějaké $(y_2, \dots, y_{k-1}) \in \mathbb{Z}^{k-2}$, resp. $P_0(x_0, \dots, x_{n-1}) = y_{m-1}$ právě když $\Phi_{P_0}(x_0, \dots, x_n, y_{k+1}, \dots, y_{m-1})$ pro nějaké $(y_{k+1}, \dots, y_{m-2}) \in \mathbb{Z}^{m-k-2}$. 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 6.9. *Pro každé $n \in \mathbb{N}_0$ a každý polynom $P \in \mathbb{Z}[x_0, \dots, x_n]$ existují nezáporné celé číslo m a konjunkce elementárních formulí Ψ_P tak, že $P(x_0, \dots, x_n) = 0$ právě když $\Psi_P(x_0, \dots, x_n, y_0, \dots, y_m)$ pro nějaké $(y_0, \dots, y_m) \in \mathbb{Z}^{m+1}$.*

Důkaz. Položme

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

□

Lemma 6.10. *Buď dána konjunkce elementárních formulí*

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

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

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 6.11. *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 6.8 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 6.10 určena polynomem P_Φ a tedy je diofantická. □

6.3. **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 6.12. *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*

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

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

$$t_i^{-1}(H \cap A_i) t_i = H \cap B_i \tag{6.2}$$

pro každé $i \in I$. Potom

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

Důkaz. Položme

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

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 redukované posloupnosti v $H_{\boldsymbol{\varphi}}$ je 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 redukovaná posloupnost v HNN-rozšíření $H_{\boldsymbol{\varphi}}$. Pokud by tato posloupnost nebyla redukovaná v G_{φ}, 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 (6.2) však žádná z těchto možností nemůže nastat.

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

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 6.13. *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

$$t_i^{-d} w_{\boldsymbol{z}} t_i^{d} = w_{\boldsymbol{z}+d\boldsymbol{e}_i}, \tag{6.3}$$

$$t_{ij}^{-d} w_{\boldsymbol{z}} t_{ij}^{d} = w_{\boldsymbol{z}+d\boldsymbol{e}_i+d\boldsymbol{e}_j}. \tag{6.4}$$

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 (6.3) plyne, že $G^{\varphi} \subseteq H^{\varphi} \cap F_m$. Navíc, z (6.3) snadno odvodíme, že $G^{\varphi} = t_j^{-1} G^{\varphi} t_j$ pro každé $j \neq i$- Proto vzhledem k Lemmatu 6.12 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 6.2 benigní. Z Lemmatu 6.3 plyne, že je také G^φ benigní v F_m^* a tedy je benigní v také v F_m.

Označme $\mathbf{0} = (0, \dots, 0) \in \mathbb{Z}^{m+1}$. 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 (6.3) a (6.4) dostaneme podobně jako v předchozím případě použitím Lemmatu 6.12, 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 6.12 a vztahů (6.3), (6.4) 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).

$$\begin{tikzcd}
F_m * \langle t_k \rangle \arrow[d, "\pi"'] \arrow[dr, "\psi'_{j;ik}"] & \\
\mathrm{Gp}(F_m, t_k) \arrow[r, "\psi_{j;ik}"] & \mathrm{Gp}(F_m, t_k).
\end{tikzcd}$$

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

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

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 $\psi_{j;ik}^{-1}$ grupy $\mathrm{Gp}(F_m, t_k)$. Z definujících předpisů obou zobrazení je vidět, že $\psi_{j;ik}$ a $\psi_{j;ik}^{-1}$ 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 $s_{j;ik}^{-1} b_j s_{j;ik}^{-1} = a_j b_j c_j$ a $s_{j;ik}^{-1} c_i s_{j;ik} = t_k c_i$, resp. $s_{i;jk}^{-1} b_i s_{i;jk}^{-1} = a_i b_i c_i$ a $s_{i;jk}^{-1} c_j s_{i;jk} = t_k c_j$ 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 $\boldsymbol{z} = (z_0, \ldots, z_m) \in \mathbb{Z}^{m+1}$ platí

$$s_{j;ik}^{-d} w_{\boldsymbol{z}} s_{j;ik}^{d} = w_{\boldsymbol{z}+d\boldsymbol{e}_j+dz_i\boldsymbol{e}_k} \text{ a } s_{i;jk}^{-d} w_{\boldsymbol{z}} s_{i;jk}^{d} = w_{\boldsymbol{z}+d\boldsymbol{e}_i+dz_j\boldsymbol{e}_k}. \tag{6.5}$$

Položme

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

Z rovností (6.3) a (6.5) 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 (6.5) plyne, že $s_{j;ik}^{-1} G^\varphi s_{j;ik} = G^\varphi$ a $s_{i;jk}^{-1} G^\varphi s_{i;jk} = G^\varphi$. Podle Lemmatu 6.12 je potom

$$H^\varphi = H_*^\varphi \cap F_m^*. \tag{6.6}$$

Z rovností (6.3) je vidět, že $t_l^{-1} G^\varphi t_l^{-1} = G^\varphi$ pro každé $l \neq i, j, k$, odkud vhledem k Lemmatu 6.12 plyne, že

$$G^\varphi = H^\varphi \cap F_m. \tag{6.7}$$

Protože, H_*^φ a F_m a F_m^* jsou konečně generované podgrupy konečně prezentované grupy F_m^{**}, dotaneme z rovnosti (6.6), že H^φ je benigní v F_m^* a následně z rovnosti (6.7), že G^φ je benigní v F_m. □

Lemma 6.14. *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 6.11 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

$$G^\Phi = \bigcap_{i=0}^{t} G^{\varphi_t}. \tag{6.8}$$

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 $g = w_{\boldsymbol{z}_0}^{\varepsilon_0} \dots w_{\boldsymbol{z}_k}^{\varepsilon_k} \in G^\varphi$ právě když $\varphi(w_j)$ pro všechna $j \in \{0, \dots, k\}$. Odtud vidíme, že $g = w_{\boldsymbol{z}_0}^{\varepsilon_0} \dots w_{\boldsymbol{z}_k}^{\varepsilon_k} \in G^\Phi$ 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 (6.8) ověřena. Z této rovnosti a z Lemmatu 6.3 plyne, že G^Φ je benigní v F_m.

Nyní ověřme rovnost

$$G^S = \mathrm{Gp}(G^\Phi, a_i, b_i, c_i,\ 1 \le i \le m) \cap F_0. \tag{6.9}$$

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 $1 \le i \le m$). 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 $0 \le j \le m$ platí $\Phi(\boldsymbol{z}_j)$ a tedy $z_0^j \in S$. Proto $\pi(G^\Phi) = G^S$. Označme $F_m^\Phi = \mathrm{Gp}(G^\Phi, a_i, b_i, c_i,\ 1 \le i \le m)$. Potom

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

což je (6.9). Z Lemmatu 6.4 plyne, že F_m^Φ je benigní podgrupou F_m. Z Lemmatu 6.3 pak dostaneme, že G^S je benigní v F_m a tedy je benigní i v F_0. $\square$

Věta 6.15 (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 6.14.

Důkaz. Podle Tvrzení 6.7 existuje rekurzivně spočetná nerekurzivní podmnožina S přirozených čísel. Podle Lemmatu 6.14 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

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

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

$$a^z b c^z \in G \text{ právě když } t^{-1}(a^z b c^z) t = a^z b c^z. \tag{6.10}$$

Kdyby měla grupa H řešitelný problém slov, dokázali bychom na základě (6.10) rozhodnout, zda celé číslo z leží v S, což je spor s tím, že množina S není rekurzivní. □

6.4. **Higmanova vnořovací věta.** V poslední části této kapitoly dokážeme Higmanovu vnořovací větu. Základem našeho důkazu, podobně jako v případě věty Novikov-Booneovy, bude Lemma 6.14. Nejprve si však ukažme další užitečnou vlastnost benigních podgrup.

Lemma 6.16. *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.*

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

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

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

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

$$Q = \langle P \times \overline{G}/\overline{N}; s \mid s^{-1}(u, 1)s = (u, \Phi(u)), u \in U\rangle. \tag{6.11}$$

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 (6.11) nahradit její konečnou podmnožinou $\Gamma = \{s^{-1}(u,1)s \mid u \in A \cup t^{-1}At\}$. Ukážeme, že

$$Q = \langle B \times \overline{A}, s \mid \Delta \times \mathbf{1}, \Gamma \rangle \tag{6.12}$$

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 (6.12). 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. $\square$

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

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

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 6.17. *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

$$t_\lambda^{-1} g_v t_\lambda = g_{v^\wedge\lambda}. \tag{6.13}$$

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 6.2 a 6.3 dostaneme, že G je benigní podgrupa F, tedy dokazovné. Protože $g_\emptyset = hd$, plyne z (6.13) inkluze

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

Zbývá ukázat opačnou inkluzi. Podle Lemmatu 6.12 k tomu stačí ověřit pro každé $\lambda \in A$ rovnost

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

Z rovnosti (6.13) 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 $g_{w_1}^{\varepsilon_1}, \dots, g_{w_m}^{\varepsilon_m}$ slovo nad B v redukovanéme 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 6.18 (Higmanova)**.** *Konečně generovaná grupa je rekurzivně prezentovaná právě když je vnořitelná do konečně prezentované grupy.*

Důkaz. Z úvah uvozojících formulaci Higmanovy věty plyne, že každá konečně generovaná podgrupa konečně prezentované grupy je rekurzivně prezentovaná. Zbývá ukázat opačnou implikaci. Podle Věty 5.1 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 6.17 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 6.17 ukážeme, že

$$G_\Delta = U_\Delta \cap G. \tag{6.14}$$

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 (6.14) pak plyne, že

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

Podle Lemmat 6.14, resp. 6.17 jsou podgrupy U_Δ, resp. G benigní v F. Pomocí Lemmat 6.1 - 6.4 odtud odvodíme, že $\mathrm{Gp}(\Delta)$ je benigní podgrupa $\langle a, b\rangle$. Podle Lemmatu 6.16 je pak grupa $\langle a, b \mid \Delta\rangle$ vnořitelná do konečně prezentované grupy. $\square$

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

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

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

$$t^{-1}(a_0^{-n} b a_0^n)t = a_1^{-n} b a_1^n \tag{6.15}$$

právě když $n \in S$ (pokud totiž $n \notin S$, je $t^{-1}, (a_0^{-n} b a_0^n), t, (a_1^{-n} b a_1^n)^{-1}$ 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 (6.15) a tak zda $n \in S$. To je ve sporu s tím, že množina S není rekurzivní.