VOLNÉ GRUPY

Idea: co "největší" grupa generovaná danou množinou X

BYLO: $\langle X \rangle_G = \{ x_1^{k_1} \cdots x_n^{k_n} : x_1, \dots, x_n \in X,\ k_1, \dots, k_n \in \{\pm 1\} \}$

$\rightsquigarrow$ CHCI: grupa "slov", skládání slov za sebe,
pouze "krácení" vynucené axiomy grup

Konstrukce: def.: slovo nad abecedou $A \equiv$ konečná posloupnost znaků

Př.: $A = \{a, b\}$ $\rightsquigarrow$ slova $a, b, ab, ba, abbaaab, \dots$

povoluje se prázdné slovo ε

X množina $\rightsquigarrow$ $F_X := \left(\text{slova nad } X \cup X^{-1} / \sim ,\ *,\ ^{-1},\ \varepsilon \right)$

kde $w \sim w' \iff$ ze slova w získám slovo w' vsunutím/vypuštěním dvojice $x x^{-1}$, $x^{-1} x$

☺ je to ekvivalence

$[w] * [w'] := [ww']$ spojení posloupností

$[w]^{-1}$: $w = x_1^{k_1} \cdots x_n^{k_n} \Rightarrow [w]^{-1} = [x_n^{-k_n} \cdots x_1^{-k_1}]$

Značení: závorky [ ] se vypouštějí, $aa \rightsquigarrow a^2$, $a^{-1}a^{-1}a^{-1} \rightsquigarrow a^{-3}$ apod.

Př.: $X = \{a, b\}$ $\quad ab^{-1}a * a^{-1}a^{-1}bb = ab^{-1}aa^{-1}a^{-1}bb = ab^{-1}a^{-1}bb = ab^{-1}a^{-1}b^2$

☺ $F_{\{a\}} \simeq \mathbb{Z}$ ... slova nad $\{a, a^{-1}\}$ ... $aa \cdots a = a^k$, $a^{-1}a^{-1} \cdots a^{-1} = a^{-k}$, ε

... skládání slov $\equiv$ sčítání exponentů

$\rightsquigarrow$ izomorfismus je $a^k \leftrightarrow k$

☺ F_X není abelovská kdykoliv $|X| \geq 2$

... $ab \neq ba$ kdykoliv $a \neq b$

Tvrzení: G grupa, $f: X \to G$ zobrazení

$\Rightarrow \exists!\ \varphi: F_X \to G$ homomorfismus t.ž. $\varphi|_X = f$

Př.: $X=\{a,b\}$, $G=\mathbb{Z}$, $f: \{a,b\} \to \mathbb{Z}$, $a \mapsto 3$, $b \mapsto -2$ $\rightsquigarrow$ $\varphi: F_{\{a,b\}} \to \mathbb{Z}$

$\varepsilon \mapsto 0$

$a^2 \mapsto 3+3$

$a^k \mapsto 3k$

$b^\ell \mapsto -2\ell$

$a^{k_1} b^{\ell_1} a^{k_2} b^{\ell_2} \mapsto 3(k_1+k_2) + (-2)(\ell_1+\ell_2)$

atd.

Pozn.: důkaz nekomutativity: $G=S_3$, $a \mapsto (12)$, $b \mapsto (23)$, $ab \neq ba$ $\Rightarrow \varphi(a)\varphi(b) \neq \varphi(b)\varphi(a)$

Důkaz: má-li být φ hom., pak nutně musí platit:

$$\varphi(x_1^{k_1} \dots x_n^{k_n}) = \varphi(x_1)^{k_1} \dots \varphi(x_n)^{k_n} = f(x_1)^{k_1} \dots f(x_n)^{k_n}$$

$\rightsquigarrow$ pokud existuje, pak nejvýše jeden!

Snadné cvičení: ověřte, že takto definované φ je

1) dobře definované (různé zápisy jednoho slova!)
2) homomorfismus

□

Poznámka: Platí i opačná implikace:

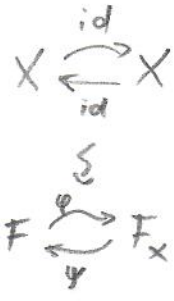
$F = \langle X \rangle$ grupa, $\forall G\ \forall f: X \to G\ \exists!\ \varphi: F \to G$ hom. t.ž. $\varphi|_X = f$

$\Rightarrow F \simeq F_X$

Idea důkazu: dosaďte $G = F_X$, dokažte, že to jediné φ je id_{F_X}.

$\mathrm{id}: X \to F_X$ $\overset{\text{předp.}}{\rightsquigarrow}$ $\varphi: F \to F_X$ hom. na

$\mathrm{id}: X \to F$ $\overset{\text{volná}}{\rightsquigarrow}$ $\psi: F_X \to F$ hom. na



$\varphi\psi|_X = \mathrm{id} \Rightarrow \varphi\psi = \mathrm{id}$

$\psi\varphi|_X = \mathrm{id} \Rightarrow \psi\varphi = \mathrm{id}$

↑ dílčí jen.

PREZENTACE GRUP

Idea: co "největší" grupa
- generovaná množinou X
- jejíž generátory splňují relace R

... např. $X=\{a,b\}$ $R=\{ab=ba\}$ ... dva komutující generátory

intuice: $\mathbb{Z}\times\mathbb{Z} = \langle (1,0), (0,1) \rangle$

... kde ji vzít? Vezmi volnou F_X, faktorizuj tak, aby byly splněny ty relace

možná definice: slova$/\sim$ kde $w \sim w'$ pomocí axiomů grup, relací v R

lépe: definovat vhodnou normální podgrupu F_X

Pozn.: rovnost $w_1 = w_2 \rightsquigarrow w_1 w_2^{-1} = 1$
$ab = ba \rightsquigarrow aba^{-1}b^{-1}$

def: X množina, $R \subseteq F_X$ množina slov

$\rightsquigarrow \langle X \mid R \rangle := F_X / \langle\langle R \rangle\rangle$ kde $\langle\langle R \rangle\rangle$ je nejmenší normální podgp. obsahující R

⋮

prezentace grupy

Př.: $\langle a_1, \dots, a_n \mid \emptyset \rangle = F_{\{a_1,\dots,a_n\}}$

Př.: $\langle a \mid a^n \rangle$ ... slova a^k, $k \in \mathbb{Z}$
vynucuji $a^n = 1$, čili také $a^{-n}, a^{2n}, \dots = 1$
... formálně: $\langle\langle a^n \rangle\rangle = \langle a^n \rangle = \{a^{kn} : k \in \mathbb{Z}\}$
... $F_{\{a\}} / \langle a^n \rangle \simeq \mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$
$a^k \longleftrightarrow k$

Př.: $\langle a,b \mid aba^{-1}b^{-1} \rangle \simeq \mathbb{Z}\times\mathbb{Z}$
$(k,\ell) \mapsto a^k b^\ell$
díky $ab=ba$ to bude 1) hom. 2) na
$\langle a,b \mid ab=ba \rangle$ neformální značení $w = w' \Leftrightarrow ww'^{-1} = 1$

Cv.: $\langle a,b,c \mid a^3, c^5, ab=ba, ac=ca, bc=cb \rangle \simeq ?$

$[\mathbb{Z}_3 \times \mathbb{Z} \times \mathbb{Z}_5]$

? Jak dokázat, že $\langle X|R\rangle \simeq G$?

... chci $f: X \to G$ t.ž. to jediné $\varphi: F_X \to G$

1) je na G ... stačí $G = \langle f(X)\rangle$
2) $\ker\varphi = \ll R \gg$

... prakticky :- najdi generátory G splňující dané relace
$\rightsquigarrow$ hom. $F_X \twoheadrightarrow G$ t.ž. $\ker\varphi \supseteq \ll R\gg$

- dokaž, že $|\langle X|R\rangle| \leq |G|$ výčtem slov

Př.: $\langle a,b \mid a^2, b^3, (ab)^2 \rangle \simeq S_3$

... $a=(1\,2)$, $b=(1\,2\,3)$ splňují dané relace

... výčet slov: $\varepsilon, a, b, b^2, ab, ba$ & 👁 všechna slova délky 3 lze upravit na kratší
($b^2 = b^{-1}$)

$(aba = a^{-1} \neq a,\ abb = ab^{-1} = ba, \ldots)$

Cv.: $D_{2n} \simeq \langle a,b \mid a^2, b^n, (ab)^2 \rangle$

Př.: $\langle a,b \mid a^2, b^2, aba = bab \rangle \simeq S_3$

... $a=(1\,2)$, $b=(2\,3)$ splňují dané relace

... výčet slov: $\varepsilon, a, b, ab, ba, aba$ & 👁 víc ne

Cv.: $S_n \simeq \langle a_1, \ldots, a_{n-1} : a_1^2, \ldots, a_{n-1}^2,\ a_i a_{i+1} a_i = a_{i+1} a_i a_{i+1},\ a_i a_j = a_j a_i \ \forall |i-j|>1 \rangle$

! Vidíme dvě velmi rozdílné prezentace S_3, je snadné vidět $\simeq$?

Jak vlastně rozhodovat, zda $w = w'$?

Špatné zprávy:

[Boone - Novikov] 1958 1955 Neexistuje algoritmus, který by pro dané X, R, w rozhodl, zda $w = 1$ v $\langle X | R \rangle$.

[Adian - Rabin]:

Neexistuje algoritmus, který by pro "Markovskou" vlastnost P a dané X, R rozhodl, zda $\langle X | R \rangle$ má vlast. P.

Př.: $P \equiv |\langle X, R \rangle| = 1$

$P \equiv \langle X, R \rangle$ je abelovská

apod.

Poznámka: každá (konečná) grupa má (konečnou) prezentaci:

$$G \simeq \langle G | R \rangle$$

← v podstatě multiplikační tabulka

kde $R = \{ abc^{-1} : \underbrace{a * b = c}_{\text{v } G} \}$

Cv.: kvaternionová grupa $Q_8 \simeq \langle a, b : aba = b, bab = a \rangle$

Cv.: $G = \langle X | R \rangle$, $H = \langle Y | S \rangle$ $\Rightarrow$ $G \times H \simeq \langle X \cup Y | R \cup S \cup \{ xyx^{-1}y^{-1} : \underset{y \in Y}{x \in X} \} \rangle$