PROSTE GRUPE IN PREZENTACIJE GRUP

Neformalno: Kaj je prosta grupa na množici X?

$|X| = 1$: $F_X \cong \mathbb{Z}$

$|X| = 2$, $X = \{x, y\}$: $F_X = \{1, x, y, x^{-1}, y^{-1}, x^2, y^2, xy, yx, x^2y^{-3}x^{-5}y^4x, \ldots\}$

Množenje: $xyx^{-2} \cdot yx^{-1}y^{-1}x = xyx^{-2}yx^{-1}y^{-1}x$
$xyx^{-2} \cdot x^2y^{-1}x^{-5} = x^{-4}$

Formalno: Naj bo X poljubna množica. Definirajmo prosto grupo F_X na X.

$X = \emptyset$: $F_X = \{1\}$

$X \neq \emptyset$: Označimo z X^{-1} množico z isto kardinalnostjo kot X:
$X^{-1} = \{x^{-1} \,;\, x \in X\}$

Zaporedju $(x_1, x_2, x_3, \ldots)$, $x_i \in X \cup X^{-1} \cup \{1\}$, pri čemer so od nekega elementa dalje vsi elementi enaki 1, pravimo beseda.

Primer: Besedi $(1, 1, \ldots) =: 1$ pravimo prazna beseda.

Besedi pravimo reducirana beseda, če veljata še pogoja:

- Elementa x in x^{-1} nikoli ne nastopata zaporedoma:
  $(x_i = x \Rightarrow x_{i+1} \neq x^{-1})$ in $(x_i = x^{-1} \Rightarrow x_{i+1} \neq x)$

• Če je nek $x_n = 1$, so tudi $x_{n+1}, x_{n+2}, \ldots = 1$

Zaporedje $(x_1^{\varepsilon_1}, x_2^{\varepsilon_2}, \ldots, x_n^{\varepsilon_n}, 1, 1, \ldots)$, $\varepsilon_i \in \{-1, +1\}$, $x_i \in X$, pišemo kot $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_n^{\varepsilon_n}$.

Kot množica je F_X množica reduciranih besed.

Vpeljimo operacijo: Vzemimo dve reducirani besedi, $x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m}$ in $y_1^{\eta_1} y_2^{\eta_2} \cdots y_n^{\eta_n}$, $\varepsilon_i, \eta_i \in \{-1, +1\}$, $x_i, y_i \in X$. Denimo $m \leq n$.

Naj bo k najmanjše število, da $y_k^{\eta_k} = x_{m-k+1}^{-\varepsilon_{m-k+1}}$; če takega k ni, potem $k = m+1$.

$$x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m} \cdot y_1^{\eta_1} y_2^{\eta_2} \cdots y_n^{\eta_n} = \begin{cases} x_1^{\varepsilon_1} \cdots x_{m-k+1}^{\varepsilon_{m-k+1}} y_k^{\eta_k} \cdots y_n^{\eta_n} & ; \ k \leq m \\ y_{m+1}^{\eta_{m+1}} \cdots y_n^{\eta_n} & ; \ k = n+1 \text{ in } m < n \\ 1 & ; \ k = n+1 \text{ in } m = n \end{cases}$$

F_X grupa

Enota: 1

$(x_1^{\varepsilon_1} \cdots x_n^{\varepsilon_n})^{-1} = x_n^{-\varepsilon_n} \cdots x_1^{-\varepsilon_1}$

Asociativnost velja

F_X imenujemo **prosta grupa** na množici X.

$|X| = 1$: $F_X \cong \mathbb{Z}$

Neformalno: $X \subseteq F_X$

$$i: X \longrightarrow F_X$$
$$x \longmapsto x \quad (= (x, 1, 1, \ldots))$$

Izrek: Naj bo X množica in F_X prosta grupa na X ter $i: X \to F_X$, $i(x) = x$. Za vsako funkcijo $f: X \to G$, kjer je G grupa, obstaja natanko en homomorfizem $\varphi: F_X \to G$, da je $\varphi(i(x)) = f(x)$ za vsak $x \in X$.

$$\begin{tikzcd} X \arrow[r, "i_x"] \arrow[dr, "f"'] & F_X \arrow[d, dashed, "\varphi"] \\ & G \end{tikzcd}$$

Dokaz: $\varphi(x_1^{\varepsilon_1} \cdots x_m^{\varepsilon_m}) = f(x_1)^{\varepsilon_1} \cdots f(x_m)^{\varepsilon_m}$

Izrek: Vsaka grupa je homomorfna slika neke proste grupe.

Dokaz: Naj bo G grupa. Naj bo $X \subseteq G$ množica, ki generira G. Na X glejmo kot množico in zgradimo prosto grupo F_X na X. Po prejšnjem izreku obstaja homomorfizem $\varphi: F_X \to G$, $\varphi(x) = x$. φ je surjektiven, saj je $\operatorname{Im}\varphi$ podgrupa, ki vsebuje X.

$G = \operatorname{Im}\varphi$, $\varphi: F_X \to G$

$F_X / \operatorname{Ker}\varphi \cong G$

Definicija: Naj bo X množica in naj bo R neka množica reduciranih besed v X. Pravimo, da je grupa G **generirana z generatorji** $x \in X$ **in relacijami** $r = 1$, $r \in R$, če je G izomorfna grupi F_X / N_R, kjer je N_R edinka, generirana z množico R. V tem primeru rečemo, da je par $\langle X | R \rangle$ **prezentacija** R.

Naj bo $\langle X | R \rangle$ prezentacija G. Označimo $N = N_R$.

F_X / N je generiran z $x_i N$, $x_i \in X$.

$r \in R$: $r = x_1^{\varepsilon_1} x_2^{\varepsilon_2} \cdots x_m^{\varepsilon_m}$

$$(x_1N)^{\varepsilon_1}(x_2N)^{\varepsilon_2}\cdots(x_mN)^{\varepsilon_m} = \underbrace{x_1^{\varepsilon_1}x_2^{\varepsilon_2}\cdots x_m^{\varepsilon_m}}_{r}N = rN = N = 1$$

Definicija: Grupa G je **končno prezentirana**, če obstajata taka končna množica X in končna množica R, da je $\langle X \mid R\rangle$ prezentacija G.

Pišemo: $\langle X \mid R\rangle = \langle x_1,\dots,x_m \mid r_1 = \dots = r_n = 1\rangle$

Primer: Prezentacija proste grupe F_X je $\langle X \mid \emptyset\rangle$.

Primer: $\langle x \mid x^n = 1\rangle$ je prezentacija $\mathbb{Z}_n$.

Primer: $\langle x,y \mid \underset{[x,y]=1}{xy \overset{\shortparallel}{=} yx}\rangle$ je prezentacija $\mathbb{Z}\oplus\mathbb{Z}$.

Primer: Poskusimo najti prezentacijo D_{2n}.

$$D_{2n} = \{1, r, \dots, r^{n-1}, z, rz, \dots, r^{n-1}z\}$$

$r^n = 1$
$z^2 = 1$
$(rz)^2 = 1 \qquad (\Leftrightarrow zrz^{-1} = zrz = r^{-1})$

D_{2n} je prezentirana kot $\langle x,y \mid x^n = y^2 = (xy)^2 = 1\rangle$:

$F_{\{x,y\}}/N \cong D_{2n}$, N generirana z $x^n, y^n, (xy)^2$

Naj bo G katerakoli grupa, generirana z elementoma u, v, ki zadoščata $u^n = v^2 = (uv)^2 = 1$.

D_{2n} je taka grupa. Tudi $F_{\{x,y\}}/N$ je taka $(u = xN,\ v = yN)$.

1. korak: G je homomorfna slika $F_{\{x,y\}}/N$.

2. korak: $|G| \leq 2n$

Denimo, da je to res.

Po 1. koraku obstaja epimorfizem $\varphi: F_{\{x,y\}}/N \to D_{2n}$.

Po 2. koraku je $|F_{\{x,y\}}/N| \leq |D_{2n}|$.

Zato sledi, da je φ izomorfizem.

1. korak

Vemo: $\exists$ hom. φ iz $F_{\{x,y\}}$ v G

$$x \mapsto u, \; y \mapsto v$$

Jedro tega hom. φ vsebuje $x^n, y^2, (xy)^2$.

$\Rightarrow N \subseteq \operatorname{Ker}\varphi$

Zato obstaja hom. iz $F_{\{x,y\}}/N$ v $F_{\{x,y\}}/\operatorname{Ker}\varphi$,
$wN \to w \operatorname{Ker}\varphi$.

$F_{\{x,y\}}/\operatorname{Ker}\varphi \cong G$

Iz $N \subseteq \operatorname{Ker}\varphi$ sledi dobra definiranost.

2. korak

$u^{m_1} v^{n_1} u^{m_2} \cdots v^{n_r}, \quad m_i, n_i \in \mathbb{Z}$

$m_i \in \{0, 1, \ldots, m-1\}$
$n_i \in \{0, 1\}$

$v u^m v = (vuv)^m = (u^{-1})^m = u^{-m}$

Edini možni elementi so $1, u, \dots, u^{n-1}, v, uv, \dots, u^{n-1}v$.

$\Rightarrow |G| \leq 2n$

PROSTE ALGEBRE IN PREZENTACIJE ALGEBER

Algebra naj bo algebra nad poljem (zaradi preprostosti).

Elementi proste algebre so nekomutativni polinomi:

$1, X, Y, XY, YX, XY-YX, 3+7X^7Y-9YX^4Y, \dots$

$(XY+X)\cdot(YX-X) = XY^2X - X^2$

Naj bo X množica. Elementi prostega monoida X^* so besede, torej zaporedja $(x_1, x_2, \dots, x_m, 1, 1, \dots)$.

Pišemo: $x_1 x_2 \cdots x_m$, $XXYYX =: X^2Y^2X$

Vpeljemo množenje: $x_1 \cdots x_m \cdot y_1 \cdots y_n := x_1 \cdots x_m y_1 \cdots y_n$, $1 \cdot X = X$

S tem postane X^* monoid. Rečemo mu prosti monoid.

$F\langle X \rangle$ naj bo vektorski prostor nad F z bazo X^*.

$F\langle X \rangle$ postane algebra, če definiramo:

$(\sum \lambda_i w_i)\cdot(\sum \mu_j w_j) := \sum_{w_i w_j = w_k} \nu_k w_k$, $\nu_k = \sum_{w_i w_j = w_k} \lambda_i \mu_j$

$F\langle X \rangle$ imenujemo prosta algebra na množici X.

$$i: X \longrightarrow F\langle X\rangle$$
$$x \longmapsto x$$

$$\begin{tikzcd}
X \arrow[r, "i"] \arrow[dr, "f"'] & F\langle X\rangle \arrow[d, dashed, "\varphi"] \\
& A
\end{tikzcd}$$

Izrek: Naj bo X množica, A algebra in $f: X \to A$. Potem obstaja natanko en homomorfizem $\varphi: F\langle X\rangle \to A$, da je $\varphi \circ i = f$.

Dokaz: $\varphi(p(x_1, \dots, x_m)) := p(f(x_1), \dots, f(x_m))$

Torej je prosta algebra prosti objekt v kategoriji algeber nad F.

Posledica: Vsaka algebra je homomorfna slika neke proste algebre.

Dokaz: Naj bo A algebra. Naj bo $X \subseteq A$ katerakoli množica generatorjev A.

$$f: X \to A$$
$$x \mapsto x$$

Po izreku obstaja homomorfizem $\varphi: F\langle X\rangle \to A$, $\varphi(x) = x$.

$\operatorname{Im}\varphi$ vsebuje X, zato je φ epimorfizem.

$$A \cong F\langle X\rangle / I, \quad I = \operatorname{Ker}\varphi$$

Definicija: Naj bo X neprazna množica, naj bo F polje in naj bo R neka množica nekomutativnih polinomov iz X. Pravimo, da je algebra A definirana z generatorji $x \in X$ in relacijami $p = 0$, $p \in R$, če je A izomorfna $F\langle X\rangle/(R)$, kjer je (R) ideal $F\langle X\rangle$, generiran z R. V tem primeru rečemo, da je $F\langle X\rangle/(R)$ prezentacija algebre A.

Algebra A je končno generirana, če je $|X| < \infty$ in $|R| < \infty$.
$F\langle X\rangle/(R)$ pišemo kot $F\langle X_1,\dots,X_m \mid p_i(X_1,\dots,X_m)=0,\ i=1,\dots,n\rangle$.

Primer: Prosta algebra je algebra brez relacij ($R=\emptyset$).

Primer: $F\langle X,Y \mid XY=YX\rangle = F[X,Y]$ (navadni polinomi)

Primer: $F\langle X,Y \mid XY=1\rangle$

Primer: $M_2(F)$ kot algebra je generirana z E_{12}, E_{21}:

$$E_{11}=E_{12}\cdot E_{21}$$
$$E_{22}=E_{21}\cdot E_{12}$$

$$E_{12}^2=0$$
$$E_{21}^2=0$$
$$I=E_{12}\cdot E_{21}+E_{21}\cdot E_{12}$$

Ugibamo, da je prezentacija algebre $M_2(F)$ enaka:

$$F\langle X,Y \mid X^2=Y^2=0,\ XY+YX=1\rangle$$