G - grupa

Def. Podzbiór $S \subset G$ jest zbiorem generatorów dla G jeśli każdy $g \in G$ przedstawia się jako $g = s_1 s_2 \cdots s_n$ dla pewnego n, oraz dla pewnych $s_i \in S \cup S^{-1}$ $[S^{-1} = \{s^{-1} : s \in S\}]$.

Chcemy opisywać i badać grupy za pomocą ich opisu (zwanego prezentacją) w formie zbioru generatorów S oraz układu pewnych równości pomiędzy kombinacjami generatorów.

Np. $S = \{s\}$, równość $s^k = 1$, opisywałaby grupę $\mathbb{Z}_n$

$S = \{a, b\}$, równość $ab = ba$, opisywałoby grupę $\mathbb{Z}^2$.

Zanim do tego dojdziemy, opiszemy sobie rodzinę grup posiadających zbiór generatorów S dla których nie zachodzą żadne extra relacje, z wyjątkiem tych które muszą zachodzić w każdej grupie (np. $s_1 s_2 s_2^{-1} s_1^{-1} = 1$).

Def. Niech S będzie układem generatorów grupy G.
G jest grupą wolną względem S jeśli dla dowolnej grupy H, dowolne odwzorowanie $\phi : S \to H$ rozszerza się do homomorfizmu $\Phi : G \to H$.

UWAGA: Jeśli Φ istnieje, to jest jednoznacznie zdeterminowane przez ϕ, dzięki temu że S generuje G.

Def. G jest grupą wolną jeśli jest wolna względem pewnego układu generatorów S.

FAKT 1. Grupy wolne względem równolicznych zbiorów S_1, S_2 generatorów są izomorficzne.

dowód:

Niech $b: S_1 \to S_2$ bijekcja. Możemy ją też traktować jako $b: S_1 \to G_2$.

Ponieważ G_1 wolna względem S_1, mamy rozszerzenie $\beta: G_1 \to G_2$ – homomorfizm.

Podobnie dla $a: S_2 \to S_1$ odwrotnego do b mamy rozszerzający homomorfizm $\alpha: G_2 \to G_1$.

Złożenie $\alpha\beta: G_1 \to G_1$ rozszerza id_{S_1}, więc z jedyności rozszerzenia $\alpha\beta = id_{G_1}$. Podobnie $\beta\alpha = id_{G_2}$.

Zatem $\alpha = \beta^{-1}$, czyli β jest izomorfizmem. □

OZN. Ponieważ grupa wolna jest jednoznacznie wyznaczona przez swój układ generatorów S (z definicji), będziemy stosować oznaczenie F_S.

Grupę wolną względem n-elementowego zbioru generatorów będziemy też oznaczać F_n.

TERMINOLOGIA: baza grupy wolnej

zbiór generujący grupę w sposób wolny

zbiór wolnych generatorów

FAKT 2. Grupy wolne względem różnolicznych (skończonych) zbiorów generatorów nie są izomorficzne.

dowód: Zliczamy

surjektywne homomorfizmy $h: F_S \to \mathbb{Z}_2$.

Każdy $h: F_S \to \mathbb{Z}_2$ jest zadany przez odwzorowanie $\chi: S \to \mathbb{Z}_2$, przy czym h jest surjektywny jeśli $\chi \not\equiv 0$.

Takich χ jest

tyle ile podzbiorów S minus 1

czyli $2^{|S|}-1$ gdy $|S|$ skończone

zaś $2^{|S|}$ gdy S nieskończone

Dla skończonych S to kończy dowód. $\square$

FAKT 3. Dla dowolnej grupy G o zbiorze S generatorów liczba podgrup indeksu 2 jest $\leq 2^{|S|}-1$.

WNIOSEK. Grupa F_K nie posiada zbioru generatorów złożonego z mniej niż K elementów.

DEF. Rangą grupy G nazywamy minimalną moc zbioru generatorów.
OZN. $rk(G)$.

WNIOSEK. $rk(F_K) = K$ dla dowolnego naturalnego K.

KONSTRUKCJA GRUPY F_S.

S - zbiór, $S^{-1} = \{x^{-1} : x \in S\}$ - zbiór formalnych odwrotności

($S \cap S^{-1} = \emptyset$, $S \to S^{-1}$ zadane przez $x \mapsto x^{-1}$ różnowartościowe)

STOSUJEMY TEŻ KONWENCJĘ: $(x^{-1})^{-1} = x$.

- słowo w nad alfabetem $S \cup S^{-1}$ to skończony ciąg $x_1 \cdots x_k$ elementów z $S \cup S^{-1}$; słowo puste oznaczamy 1, długość słowa - liczba elementów ciągu, $|1| = 0$.

- słowa potrafimy składać: $w = x_1 \cdots y_k$, $u = y_1 \cdots y_m$ to $wu = x_1 \cdots y_k y_1 \cdots y_m$.

- elementarna operacja - wstawienie słowa aa^{-1} dla pewnego $a \in S \cup S^{-1}$ w dowolnym miejscu w słowie w

  (np. $w = w_1 w_2 \rightsquigarrow w_1 aa^{-1} w_2$)

  lub usunięcie takiego podsłowa występującego w słowie w

  ($w = w_1 aa^{-1} w_2 \rightsquigarrow w_1 w_2$)

- Słowa są <u>równoważne</u> jeśli jedno można przeprowadzić na drugie za pomocą skończonego ciągu elementarnych operacji

- zbiór klas równoważności słów tworzy grupę, właśnie F_S

  (S utożsamiamy z klasami równoważności słów długości 1)

Opiszemy tę grupę jawniej by móc wykazać że jest grupą wolną nad S.

DEF. Słowo w nad $S \cup S^{-1}$ jest <u>zredukowane</u> jeśli nie występuje w nim żadne podsłowo postaci aa^{-1}: $a \in S \cup S^{-1}$.

LEMAT. W każdej klasie równoważności słów nad $S \cup S^{-1}$ występuje dokładnie jedno słowo zredukowane.

dowód:

istnienie – wystarczy zredukować dowolne słowo w z tej klasy kolejno usuwając z niego podsłowa postaci aa^{-1}

jedyność – pokażmy że różne zredukowane słowa nie są równoważne.

- Nie wprost, niech u, v – zredukowane różne słowa nad $S \cup S^{-1}$, i załóżmy że $u = w_1, w_2, \ldots, w_n = v$ jest ciągiem takim że każde w_{i+1} jest uzyskane z w_i przez jedną elementarną operację.
- Niech $N = \sum |w_i|$, i niech powyższy ciąg będzie taki, że N jest dla niego minimalne wśród wszystkich takich ciągów.
- ponieważ u, v zredukowane, mamy $|w_2| > |w_1|$, $|w_{n-1}| > |w_n|$

Zatem istnieje i ($1 < i < n$) takie że
$|w_i| > |w_{i-1}|$, $|w_i| > |w_{i+1}|$.

- w_{i-1} jest uzyskane z w_i przez usunięcie aa^{-1} z pewnej pozycji zaś w_{i+1} przez usunięcie bb^{-1} z pewnej pozycji

PRZYPADKI. (1) jeśli powyższe pozycje pokrywają się, to $w_{i-1} = w_{i+1}$, wbrew założeniu o minimalności N

(2) jeśli aa^{-1} bb^{-1} nie pokrywają się ale zachodzą na siebie to w_i zawiera podsłowo $cc^{-1}c$, zaś oba w_{i-1}, w_{i+1} powstają z w_i przez zastąpienie tego słowa przez c, skąd znowu $w_{i-1} = w_{i+1}$, sprzeczność z minimalnością N

(3) jeśli podsłowa aa^{-1}, bb^{-1} w w_i nie zachodzą, możemy w ciągu zastąpić w_i przez w_i' powstałe przez usunięcie obu podsłów; wówczas $N' = N - 4$ wbrew minimalności N. $\square$

Konstrukcja:

F_S = słowa nad $S \cup S^{-1}$ / kombinacje elementarnych operacji $w_1 x x^{-1} w_2 \longleftrightarrow w_1 w_2$

mnożenie: $[w_1] \cdot [w_2] := [w_1 w_2]$ — dobrze określone

jedynka: $[1]$ $\quad$ 1 - słowo puste

odwrotność $\quad [a_1 \cdots a_k]^{-1} = [a_k^{-1} a_{k-1}^{-1} \cdots a_1^{-1}]$

Łączność — wynika z LEMATU

WNIOSEK. F_S = zredukowane słowa nad $S \cup S^{-1}$ | jawny opis grupy F_S

mnożenie = konkatenacja + redukcje na styku

FAKT. F_S jest wolna względem S $\quad [S = \{[s] : s \in S\} \subset F_S]$

| Def. G jest wolna względem $\underbrace{S}_{\text{układu generatorów}}$ jeśli
| $\forall H \quad \forall \phi : S \to H \quad \exists$ rozszerzenie $\overline{\Phi} : F_S \to H$.

Dowód: S oczywiście generuje F_S.

Niech $\phi : S \to H$ dane.

Na zredukowanych słowach $w = s_{i_1}^{\varepsilon_1} \cdots s_{i_k}^{\varepsilon_k}$ dookreślamy (w jedyny możliwy sposób)

$$\overline{\Phi}(w) = \phi(s_{i_1})^{\varepsilon_1} \cdots \phi(s_{i_k})^{\varepsilon_k}$$

i sprawdzamy że jest to homomorfizm grupowy. $\square$