

### 3 Теория групп

#### 1. Свободные группы


Напомним (см. сур 1.1.1 из АТ1), что группа  $F = \langle x_i \mid i \in I \rangle$  из класса  $\mathcal{K}$  группы свободна в  $\mathcal{K}$  со св. порожд. мн-вом  $\{x_i \mid i \in I\}$ , если  $\forall G \in \mathcal{K}$  с порожд. мн-вом  $\{a_i \mid i \in I\}$  от-е  $x_i \mapsto a_i$  индуцирует гомоморфизм из  $F$  на  $G$ .

В §1.1 мы показали, что в классе абелевых групп есть свободные. Здесь мы покажем, что такие группы есть и в классе всех групп!

Пусть  $I$  - мн-во (не обяз. конечное), пусть  $X = \{x_i \mid i \in I\}$  и  $X^{-1} = \{x_i^{-1} \mid i \in I\}$  - два <sup>непересекающихся</sup> мн-ва символов

**Слово в алфавите**  $X$  - это пустая (обозн.  $1$ ) или конечная посл-сть символов из  $X \cup X^{-1}$ . Число эл-тов в слове - **длина** слова. Слово **сократимо**, если оно содержит стоящие рядом символы вида  $x_i^{\epsilon_i} x_i^{-\epsilon_i}$ , где  $\epsilon_i \in \{\pm 1\}$ , и **несократимо** в противном случае. Два слова  $u$  и  $v$  **эквивалентны** ( $u \sim v$ ), если  $v$  получается из  $u$  через конечное число вставок и сокращений слов вида  $x_i^{\epsilon_i} x_i^{-\epsilon_i}$ .

Предл. 1 Отн-е  $\sim$  экв-со отношением экв-со  
на мн-ве слов. В каждом классе этого отно-  
шения содержится ровно одно несократимое  
слово.

Д-130: Первое утв-е очевидно. Второе — см. п. а)  
в д-ве т. 14.1.1 из [КМ] 

Обозначим через  $[u]$  — класс всех слов, экв.  $u$ ,  
а через  $p(u)$  — несокр. слово из  $[u]$ .

Т. 1 Пусть  $X = \{x_i \mid i \in I\}$ . На мн-ве  $F(X) = \{[u] \mid u$   
— слова в алфавите  $X\}$  определим умножение,  
полагая  $[u][v] = [uv]$ . Это определение не зависит  
от выбора представителей. Отн-во этой операции  $F(X)$  —  
— группоид.

Л-во: Корректность операции вытекает из прелп. 1 и рав-ва  $p(uv) = p(p(u)p(v))$ , которое док-ся инд. по длине слова  $u$ .

Ассоциативность вытекает из того, что  $uv$  — это послед. выполнение ("сначала  $u$ , потом  $v$ ").

Кейтр. эл-т — это пустое слово  $\epsilon$ . Класс, обратный к классу  $[x_{i_1}^{\epsilon_1} \dots x_{i_m}^{\epsilon_m}]$ , — это  $[x_{i_m}^{-\epsilon_m} \dots x_{i_1}^{-\epsilon_1}]$ .

Группа  $G$  наз-ся **группой без кручения**, если в ней нет кеедир. эл-тов конечного порядка.

Упр 1 Докажите а)  $F(X)$  — группа без кручения  
б) если  $|X| \geq 2$ , то  $F(X)$  неабелева.

Т.2 Группа  $F(X)$  — свободная группа в классе всех групп со своб. порожд. мн-вом  $\{x_i \mid i \in I\}$ .

Д-во: Пусть гр.  $G$  порожд. мн-вом  $M = \{a_i \mid i \in I\}$

Пусть  $F = F(X)$ . Р-м от-е  $\varphi: F \rightarrow G$  по правилу  
 $[x_1^{\varepsilon_1} \dots x_m^{\varepsilon_m}] \rightarrow a_1^{\varepsilon_1} \dots a_m^{\varepsilon_m}$ , индуцированное от-ем

$x_i \rightarrow a_i$  мн-ва  $X$  на  $M$ . Корректность, соразмерность и то, что  $\varphi$  — гом. изм. вытекает из опр-ции  $\square$

Опр 2 Пусть  $G$  — группа,  $R \subseteq G$ . **Нормальная**  
**замкнутая** мн-ва  $R$  (в гр.  $G$ ) наз-ся наимень-  
шая нормальная в  $G$  подгруппа, содержащая  $R$ .  
Обозн:  $R^G$ .

Прем 2 1)  $R^G = \{ \prod_{i=1}^k g_i^{-1} r_i^{\varepsilon_i} g_i \mid g_i \in G, r_i \in R, \varepsilon_i = \pm 1, k \in \mathbb{N}_0 \}$

2) Если  $x \in R^G$ , то  $uxv \in R^G \Leftrightarrow uv \in R^G$ .  
 $\Delta$ -во: упр 2.

Пусть  $G$  — группа с нормальн. ин-вом  $M = \{a_i \mid i \in \mathbb{I}\}$ ,  
и  $\varphi: F(X) \rightarrow G$  гом-зм, индуц. ст. ст.  $x_i \rightarrow a_i, i \in \mathbb{I}$ .

Элементы  $\text{Ker} \varphi$  наз-ся **соотношениями**  
группы  $G$  в алфавите  $X$ . Если норм-во  $R$   
в  $H = \text{Ker} \varphi$  таково, что  $R^F = H$ , то  $R$  — **определя-**  
**ющие ин-ва соотношений** (гр.  $G$  в алфавите  $X$ )  
Так как  $G \simeq F/H$ , то пара  $X$  и  $R$  полно-

ство (с точностью до изоморфизма) определяет группу  $G$ . Таким  $G = \langle X \mid R \rangle$  называется

**представлением** группы  $G$  с помощью порождающих элементов и определяющих соотношений или **генерическим кодом** г.б.

Пример  $\mathbb{Z}_2 \times \mathbb{Z}_2 = \langle x, y \mid x^2, y^2, xy = yx \rangle$

Зам. Одна группа может иметь много представлений.

Упр 3 а)  $S_3 = \langle x, y \mid x^2, y^2, (xy)^3 \rangle$

б) Найти генерический код для группы  $A_4$ .  
в) Найти ген. код свободной абелевой группы ранга  $k$ .

Если  $|X| = |Y|$ , то  $F(X) \cong F(Y)$ . Несложно  
показать, что верно и обратное, т.е. модули  
два базиса свободной группы равносильны.

Размер базиса (т.е. порождающего мн-ва)  
свободной группы — **ранг**. Обозн.  $\text{rk}(F)$ .  
Через  $F_k$  будем обозн. свободную гр. ранга  $k$ ,  
а через  $F_\infty$  — свободную группу счётного ранга.

Предл 3 Группы  $F_2$  содержат в качестве  
подгрупп групп, изоморфные  $F_k \forall k \in \mathbb{N}$ ,  
а так же  $F_\infty$ .



Л-во: Пусть  $F_2 = F(x, y)$ . Р-м ин-во  $A$   
эл-тов  $x, y^{-1}xy, y^{-2}xy^2, \dots$  из  $F_2$

Заметим, что  $(y^{-r}xy^r)^{-1} = y^{-r}x^{-1}y^r$  и  
 $y^r x^\varepsilon y^r y^{-s} x^\delta y^s = y^{-r} x^\varepsilon y^{r-s} x^\delta y^s$ . Поэтому

в конечном слове вида  $a_{i_1}^{\varepsilon_1} \dots a_{i_m}^{\varepsilon_m}$

сокращение возникает  $\Leftrightarrow$  есть подслово

вида  $a_i^{\varepsilon} a_i^{-\varepsilon}$ . Поэтому  $\langle A \rangle$  — свободная

группа счетного ранга. Если  $A_k$  — ин-во

из  $A$ , сост. из первых  $k$  эл-тов, то  $\langle A_k \rangle = F_k$

Т. 4 Пусть  $m \in \mathbb{N}$  и  $m \geq 2$ . Погрешность, порожденная

в  $SL_2(\mathbb{Z})$  Трансформациями

$$a = E_{12}(m) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \text{ и } b = E_{21}(m) = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix},$$

порождается ими свободно.

Л-во: см. Л-во т. 14. 2.1 из [КМ].

Следствие Свободные группы не более чем счетного ранга линейны, т.е.

выражаются как подгруппы в некоторой группе матриц.

Л-во:  $F_2 \leq F_2 \leq SL_2(\mathbb{Z})$ , см. пред. 3 и т. 4.

