3 Теория групп

1. Свободные группы

Напомним (см. опр 1.1.1 из АТ1п), что группа $F = \langle x_i \mid i \in I \rangle$ из класса $\mathcal{K}$ групп 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 <u>на</u> 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). Положим $X = \{x_i \mid i \in I\}$ и $X^{-1} = \{x_i^{-1} \mid i \in I\}$ — два $\underbrace{\text{мн-ва}}_{}$ непересекающихся 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 $x_i^{\varepsilon_i} x_i^{-\varepsilon_i}$, где $\varepsilon_i \in \{\pm 1\}$, 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 $x_i^{\varepsilon_i} x_i^{-\varepsilon_i}$.

Предл. 1 Отн-е $\sim$ явл-ся отношением экв-сти на мн-ве слов. В каждом классе этого отношения содержится ровно одно несократимое слово.

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

Обозначим через $[u]$ — класс всех слов, экв. u, а через $\rho(u)$ — 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-но этой операции $F(X)$ — группа.

Д-во: Корректность опр-ния операции вытекает из предл. 1 и рав-ва $\rho(uv) = \rho(\rho(u)\rho(v))$, которое док-ся инд. по длине слова u.

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

Нейтр. эл-т — это пустое слово 1. Класс, обратный к классу $[x_{i_1}^{\varepsilon_1}\dots x_{i_m}^{\varepsilon_m}]$, — это $[x_{i_m}^{-\varepsilon_m}\dots x_{i_1}^{-\varepsilon_1}]$.

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

Упр 1 Докажите а) $|X| \geq 2 \Rightarrow F(X)$ неабелева;

б) $F(X)$ — группа без кручения

Указ. Если $u \neq 1$, то $\rho(u^n) > \rho(u)$ и $\rho(u^{-1})$ при $n \geq 2$.

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 $\varphi: F \to G$ по правилу $[x_1^{\varepsilon_1} \ldots x_m^{\varepsilon_m}] \to a_1^{\varepsilon_1} \ldots a_m^{\varepsilon}$, индуцированное от-ем $x_i \to a_i$ мн-ва X на M. Корректность, сюръективность и то, что φ — гом. эм вытекает из опр-ний ∎

Опр 2 Пусть G — группа, $R \subseteq G$. Нормальным замыканием мн-ва R (в гр. G) наз-ся наименьшая нормальная в G подгруппа, содержащая R.
Обозн: R^G.

Предл 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 $uxv \in R^G \Leftrightarrow uv \in R^G$.

Д-во: упр 2.

Пусть G — группа с порожд. мн-вом $M = \{a_i \mid i \in I\}$, и $\varphi : F(X) \to G$ гом-зм, индуц. отобр. $x_i \to a_i$, $i \in I$.

Элементы $Ker\varphi$ наз-ся соотношениями группы G в алфавите X. Если подмн-во R в $H = Ker\varphi$ таково, что $R^F = H$, то R — определяющие мн-во соотношений (гр. G в алфавите X).

Так как $G \cong F/H$, то пара X и R полно-

стью (с точностью до изоморфизма) определяет группу G. Запись $G = \langle X \mid R \rangle$ называется **представлением** группы G с помощью порождающих эл-тов и определяющих соотношений или **генетическим кодом** гр. G.

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

Зам. Одна группа может иметь мн-во представлений.

Упр3 а) $S_3 = \langle x, y \mid x^2, y^2, (xy)^3 \rangle$

Указ. Исп. предл. 2

б) Найти генетический код для группы A_4.

в) Найти ген. код. своб. абелевой группы ранга k.

Если $|X|=|Y|$, то $F(X)\simeq F(Y)$. Можно показать (см. т. 3.8 из [БГП]), что верно и обратное, т.е. любые два базиса свободной группы равномощны.

Размер базиса (т.е. порождающего мн-ва) свободной группы — ранг. Обозн. $\mathrm{rk}(F)$.

Через F_k будем обозн. свободную гр. ранга k, и через F_∞ — свободную группу счётного ранга.

Теор. 3 Группа F_2 содержит в качестве подгрупп группы, изоморфные F_k $\forall k\in\mathbb{N}$, а также F_∞.

__Д-во:__ Пусть $F_2 = F(\{x, y\})$. Р-м мн-во A эл-тов $\underset{a_0}{x}, \underset{a_1}{y^{-1}xy}, \underset{a_2}{y^{-2}xy^2}, \ldots\ldots$ из гр 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 $a_{i_1}^{\varepsilon_1} \ldots a_{i_m}^{\varepsilon_m}$ сокращение возникает $\Longleftrightarrow$ есть подслово вида $a_i^{\varepsilon_i} a_i^{-\varepsilon_i}$. Поэтому $\langle A \rangle$ — свободная группа счетного ранга. Если A_k — подмн-во из A, сост. из первых k эл-тов, то $\langle A_k \rangle = F_k$ $\blacksquare$

Т. 4 Пусть $m \in \mathbb{N}$ и $m \geq 2$. Подгруппа, порождённая в $SL_2(\mathbb{Z})$ трансвекциями

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

порождается ими свободно.

Δ-во: см. Д-во т. 14.2.1 из [КМ].

Следствие Свободные группы не более чем счётного ранга линейны, т.е. вкладываются как подгруппы в некоторую группу матриц.

Δ-во: $F_{\aleph_0} \leq F_2 \leq SL_2(\mathbb{Z})$, см. Т. 3 и 4 $\blacksquare$