МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РФ

Нижегородский государственный университет им. Н.И. Лобачевского

М.И. Кузнецов

ЗАДАНИЕ ГРУПП ОБРАЗУЮЩИМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ

Учебно-методическое пособие

Рекомендовано
методической комиссией механико-математического факультета
для студентов ННГУ, обучающихся по направлениям
010100 «Математика»,
010200 «Математика и компьютерные науки»

Нижний Новгород
2014

УДК 512.54 (075.8)
ББК В 144.3 (я 73-4)
К 89

К 89 Кузнецов М.И. ЗАДАНИЕ ГРУПП ОБРАЗУЮЩИМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ: Учебно-методическое пособие. – Нижний Новгород: Нижегородский госуниверситет, 2014. – 15 с.

Рецензент: к.ф.-м.н., доцент **М.Е. Елисеев**

Данное учебно-методическое пособие посвящено вопросам теории групп.
Учебно-методическое пособие «ЗАДАНИЕ ГРУПП ОБРАЗУЮЩИМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ» предназначено для студентов 2-го курса механико-математического факультета, изучающих курсы «Алгебра», «Фундаментальная и компьютерная алгебра».

Ответственный за выпуск:
председатель методической комиссии
механико-математического факультета ННГУ,
к.ф.-м.н., доцент **Н.А. Денисова**

УДК 512.54 (075.8)
ББК В 144.3 (я 73-4)

Содержание

1. Системы образующих группы

Пусть G – группа, S – подмножество в множество G. Пересечение всех подгрупп в G, содержащих S, является наименьшей подгруппой, содержащей S. Она обозначается через $< S >$ и называется *подгруппой, порожденной множеством* S. Из определения следует, что $< \emptyset >= \{e\}$. Элементами группы $< S >$ являются единица и всевозможные произведения $s_1 \dots s_n,\ n \geq 1$, где $s_i \in S$ или $s_i^{-1} \in S$. Количество сомножителей в самом коротком таком представлении для $g \in < S >$ будем называть длиной элемента g и обозначать через $\ell(g)$. Очевидно, $\ell(g) = 0$ тогда и только тогда, когда $g = e$ и $\ell(g_1 g_2) \leq \ell(g_1) + \ell(g_2)$. Рассмотрим примеры.

1.1. Пусть G – группа, $S = \{g\}$ – множество из одного элемента $g \in G$. Тогда подгруппа $< g >$ – циклическая подгруппа с образующим элементом g.

1.2. Любая подстановка n-й степени является произведением транспозиций. Следовательно, транспозиции составляют множество образующих группы S_n.

1.3. Индукцией по $n \geq 2$ покажем, что группа S_n порождается транспозициями

$$(1,2),\ (2,3),\ \dots,\ (n-1,n).$$

Для $n = 2$ утверждение очевидно. Предположим, что группа S_{n-1} порождается транспозициями

$$(1,2),\ (2,3),\ \dots,\ (n-2,n-1).$$

В частности, все транспозиции (i,j), такие, что $i < n,\ j < n$, можно записать в виде произведения транспозиций $(k-1,k),\ k \leq n-1$. Таким образом, достаточно доказать, что транспозиции $(i,n),\ i < n-1$, можно записать в виде произведения транспозиций $(i,j),\ i,\ j < n$, и транспозиции $(n-1,n)$. Это можно сделать так:

$$(i,n) = (i,n-1)(n-1,n)(i,n-1).$$

Следовательно, утверждение справедливо для n. Согласно принципу математической индукции утверждение справедливо для всех $n \geq 2$.

1.4. Пусть $G = SL_2(F),\ F$ – поле. Матрицы $x(\alpha) = \begin{pmatrix} 1 & \alpha \\ 0 & 1 \end{pmatrix}$, $y(\beta) = \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix}$, $\alpha,\ \beta \in F$, называются *трансвекциями*. Покажем, что группа G порождается трансвекциями.

Очевидно, $x(\alpha)^{-1} = x(-\alpha)$ и аналогично для $y(\beta)$. Напомним, что трансвекции соответствуют элементарным преобразованиям над матрицами, например, матрица $x(\alpha)A$ получается из матрицы 2-го порядка A прибавлением к 1-й строке 2-й строки, умноженной на α. Умножение матрицы A справа на матрицу $x(\alpha)$ или $y(\beta)$ равносильно выполнению элементарного преобразования над столбцами матрицы A. Как известно, любую матрицу элементарными преобразованиями можно привести к диагональному виду. Пусть $A \in G$. Существуют трансвекции $T_1, \dots, T_s,\ \ R_1, \dots, R_k$, такие что

$$T_1 \dots T_s A R_1 \dots R_k = \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix},$$

где $a,\ b \in F,\ ab = 1$ (так как все сомножители имеют определитель, равный 1). Таким образом, достаточно показать, что любая диагональная матрица из группы G является произведением трансвекций. Это действительно так (проверить!):

$$\begin{pmatrix} a & 0 \\ 0 & a^{-1} \end{pmatrix} = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -a^{-1} & 1 \end{pmatrix} \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix} \begin{pmatrix} 1 & -1 \\ 0 & 1 \end{pmatrix}.$$

2. Свободная группа

Пусть X – множество. Назовем *словом над* X формальное выражение $x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$, где $x_i \in X,\ i = 1,\dots,n, \varepsilon_i = \pm 1$. Пустое слово обозначается символом e. Слово называется *несократимым*, если в нем не встречаются рядом два символа x^ε и $x^{-\varepsilon}$. Любое слово можно привести (редуцировать) к несократимому слову, если сократить (убрать) все стоящие рядом символы x^ε и $x^{-\varepsilon}$ (этот процесс может состоять из нескольких шагов). Обозначим через $F(X)$ множество, состоящее из e и всех несократимых слов. На множестве $F(X)$ вводится операция умножения: чтобы перемножить два несократимых слова a и b, припишем к слову a слово b и редуцируем получившееся слово (т.е. в получившемся слове произведем сокращения). В результате получим несократимое слово ab, которое называется произведением слов a и b. В результате $F(X)$ превращается в группу с единичным элементом e. Обратным для элемента $a = x_1^{\varepsilon_1}x_2^{\varepsilon_2}\dots x_n^{\varepsilon_n}$ является элемент $a^{-1} = x_n^{-\varepsilon_n}x_{n-1}^{-\varepsilon_{n-1}}\dots x_1^{-\varepsilon_1}$. Группа $F(X)$ называется *свободной группой с множеством свободных порождающих* X, мощность множества S, $|S|$, называется *рангом* свободной группы $F(S)$.

2.1. Если $X = \{x\}$ – множество из одного элемента, то $F(X)$ – бесконечная циклическая группа с образующим элементом x.

2.2. Универсальное свойство свободной группы.

teoусть G – группа, порожденная множеством образующих S, X – некоторое множество, $F(X)$ – свободная группа над X, $\varphi : X \longrightarrow S$ – отображение. Существует единственный гомоморфизм $\Phi : F(X) \longrightarrow G$, такой что $\Phi(x) = \varphi(x)$ для любого $x \in X$. Если φ сюръективно, то Φ также сюръективно.

2.3. Пусть $F(x,\ y)$ – свободная группа ранга 2 с образующими $x,\ y$. Покажем, что свободная группа со счетным множеством образующих $S = \{s_0,\ s_1,\ s_2,\dots\}$, вкладывается в качестве подгруппы в $F(x,\ y)$. Согласно теореме, чтобы задать какой-либо гоморфизм φ группы $F(S)$ в $F(x,\ y)$, достаточно задать образы элементов множества S, причем в качестве $\varphi(s_i)$ можно выбрать любые элементы группы $F(x,\ y)$. Положим $\varphi(s_i) = z_i = x^i y x^i,\ i = 0,\ 1,\ 2,\dots$. Тем самым определен единственный гомоморфизм

$$\varphi : F(S) \longrightarrow F(x,\ y),\ s_{j_1}^{\varepsilon_1}\dots s_{j_k}^{\varepsilon_k} \mapsto z_{j_1}^{\varepsilon_1}\dots z_{j_k}^{\varepsilon_k} \in F(x,\ y).$$

Пусть $w = s_{j_1}^{\varepsilon_1}\dots s_{j_k}^{\varepsilon_k} \neq e$ – непустое редуцированное слово, т.е рядом не встречаются символы $s^\varepsilon,\ s^{-\varepsilon}$. Если все $j_1 = \dots = j_k = 0$, то $w = s_0^{\epsilon k}$ и $\varphi(w) = y^{\epsilon k} \neq e$. Аналогично, если в слове w встречаются стоящие рядом символы $s_0^\varepsilon,\ s_0^{\varepsilon'}$, то $\varepsilon = \varepsilon'$. Найдем $\varphi(w)$,

$$\varphi(w) = z_{j_1}^{\varepsilon_1}\dots z_{j_k}^{\varepsilon_k} = (x^{\varepsilon_1 j_1}y^{\varepsilon_1}x^{\varepsilon_1 j_1})(x^{\varepsilon_2 j_2}y^{\varepsilon_2}x^{\varepsilon_2 j_2})\cdots(x^{\varepsilon_k j_k}y^{\varepsilon_k}x^{\varepsilon_k j_k}).$$

Раскрывая скобки, соберем стоящие рядом множители x (частичная редукция по x). Получим

$$\varphi(w)=x^{\varepsilon_1 j_1}y^{\varepsilon_1}x^{\varepsilon_1 j_1+\varepsilon_2 j_2}y^{\varepsilon_2}x^{\varepsilon_2 j_2+\varepsilon_3 j_3}y^{\varepsilon_3}\cdot\ldots\cdot x^{\varepsilon_{k-1}j_{k-1}+\varepsilon_k j_k}y^{\varepsilon_k}x^{\varepsilon_k j_k}.$$

Дальнейшее редуцирование $\varphi(w)$ возможно, только когда некоторая степень x, стоящая между множителями y равна нулю, т.е. $\varepsilon_{t-1}j_{t-1}+\varepsilon_t j_t=0$ для некоторого t. Тогда либо $j_{t-1}=j_t=0$ (как отмечалось выше, в этом случае рядом стоят символы y в одинаковых степенях), либо $j_{t-1}=j_t$, $\varepsilon_{t-1}=-\varepsilon_t$ и, значит, в слове w стоят рядом символы $s_t^{\varepsilon_t}$, $s_t^{-\varepsilon_t}$, что противоречит неприводимости слова w. Таким образом, дальнейшее редуцирование слова $\varphi(w)$ в $F(x,\ y)$ невозможно и редуцирование закончено, т.е. мы получили редуцированную запись слова $\varphi(w)$. Мы видим, что редуцированное слово $\varphi(w)$ содержит k символов y^ε, поэтому $\varphi(w)\neq 0$. Следовательно, $\ker\varphi=\{e\}$, т.е. φ – инъективный гомоморфизм.

Таким образом, свободная группа с двумя свободными образующими содержит подгруппы, которые являются свободными группами с любым конечным или даже счетным множеством свободных образующих.

2.4.* Вложение свободной группы в $SL_2(Z)$.

Покажем, что группа с двумя свободными образующими $F(x,\ y)$ вкладывается в качестве подгруппы в группу матриц второго порядка с целыми коэффициентами $SL_2(\mathbb{Z})$. Более того, $F(x,\ y)$ может быть вложена в любую конгруэнц-подгруппу $\Gamma_q\subset SL_2(\mathbb{Z})$, состоящую из матриц, у которых все недиагональные элементы делятся на фиксированное натуральное число $q>1$, а все диагональные элементы сравнимы с 1 по модулю q, т.е. Γ_q – ядро гомоморфизма, который переводит матрицы с целыми коэффициентами в матрицы с коэффициентами из кольца классов вычетов $\mathbb{Z}_q$, заменяя целочисленные коэффициенты матрицы на их классы вычетов по $mod\ q$.

Мы покажем, что соответствие

$$x\mapsto u=\begin{pmatrix}1&q\\0&1\end{pmatrix},\ y\mapsto v=\begin{pmatrix}1&0\\q&1\end{pmatrix}$$

задает инъективный гомоморфизм $\varphi: F(x,\ y)\longrightarrow\Gamma_q$. Любой элемент группы $F(x,\ y)$ является произведением элементов a и b и, следовательно, может быть записан в виде $x^{a_1}y^{a_2}\cdot\ldots$, или $y^{a_1}x^{a_2}\cdot\ldots$. Рассмотрим элемент, начинающийся с x, $w=x^{a_1}y^{a_2}\cdot\ldots$, который оканчивается либо элементом $x^{a_{2s+1}}$, либо элементом $y^{a_{2s}}$(другой случай, когда элемент начинается с y, рассматривается аналогично). Заменяя x и y матрицами u и v, получим $z=(z_{ij})=\varphi(w)=u^{a_1}v^{a_2}\cdot\ldots$. Пусть w содержит n сомножителей вида x^a, y^a.

Покажем, что $max\ |z_{ij}| \geq n+1$. Отсюда будет следовать, что $z = \varphi(w) \neq E$ (E – единичная матрица). Рассмотрим произведение z_k первых k сомножителей в z,

$$z_k = \underbrace{u^{a_1} \cdot v^{a_2} \cdot \ldots}_{k} = \begin{pmatrix} c_1(k) & c_2(k) \\ d_1(k) & d_2(k) \end{pmatrix}.$$

Так как

$$u^a = \begin{pmatrix} 1 & aq \\ 0 & 1 \end{pmatrix},\ v^a = \begin{pmatrix} 1 & 0 \\ aq & 1 \end{pmatrix},$$

то для первой строки матрицы z_{k+1} получаем в случае $k = 2s-1$

$$z_{2s} = z_{2s-1} v^{a_{2s}} = (c_1(2s-1),\ c_2(2s-1)) \begin{pmatrix} 1 & 0 \\ a_{2s}q & 1 \end{pmatrix} = (c_1(2s),\ c_2(2s)),$$

где $c_1(2s) = c_1(2s-1) + a_{2s}qc_2(2s-1),\ c_2(2s) = c_2(2s-1)$, а в случае $k = 2s$

$$z_{2s+1} = z_{2s} v^{a_{2s+1}} = (c_1(2s),\ c_2(2s)) \begin{pmatrix} 1 & a_{2s+1}q \\ 0 & 1 \end{pmatrix} = (c_1(2s+1),\ c_2(2s+1)),$$

где $c_1(2s+1) = c_1(2s),\ c_2(2s+1) = c_2(2s) + a_{2s+1}qc_1(2s)$, таким образом, $c_1(2s) = c_1(2s+1),\ c_2(2s-1) = c_2(2s)$. Обозначим первую строку матрицы z_1 через $(f_1,\ f_2)$. Мы видим, что последовательность первых строк матриц z_k будет иметь следующий вид:

$$z_1 \sim (f_1,\ f_2),\ z_2 \sim (f_3,\ f_2), z_3 \sim (f_3, f_4),\ z_4 \sim (f_5,\ f_4), \ldots,$$

$$z_{2s-1} \sim (f_{2s-1},\ f_{2s}),\ z_{2s} \sim (f_{2s+1},\ f_{2s}),\ z_{2s+1} \sim (f_{2s+1}, f_{2s+2}) \ldots,$$

где посдедовательность чисел $\{f_k\}$ задается соотношением

$$f_{j+2} = f_j + a_{j+1}qf_{j+1}.$$

Индукцией по j покажем, что последовательность натуральных чисел $\{|f_j|\}$ возрастает.
1) проверим, что $|f_2| > |f_1|$. Действительно, $(f_1,\ f_2)$ – первая строка матрицы u, т.е. $f_1 = 1, f_2 = a_1q$. Очевидно,$|f_2| = |a_1|q \geq q > 1 = |f_1|$.
2) предположим, что $|f_{j+1}| > |f_j|$ и покажем, что $|f_{j+2}| > |f_{j+1}|$. Из формулы $f_{j+2} = f_j + a_{j+1}qf_{j+1}$ получаем

$$|f_{j+2}| \geq q|a_{j+1}||f_{j+1}| - |f_j| \geq 2|f_{j+1}| - |f_j| > |f_{j+1}|.$$

Учитывая, что числа $|f_j|$ натуральные, можно записать $|f_{j+1}| \geq |f_j| + 1$. Так как матрица z_k содержит элемент, равный f_{k+1}, и $|f_{k+1}| \geq |f_2| + k - 1 \geq 2 + k - 1 = k + 1$, то для $z = \varphi(w) = (z_{ij})\ \max |z_{ij}| \geq n + 1$. Утверждение доказано.

3. Копредставление группы

Пусть $G =< S >$ – группа с множеством образующих S. Согласно универсальному свойству свободной группы существует единственный сюръективный гомоморфизм Φ свободной группы $F(S)$ на группу G, соответствующий тождественному отображению φ множества S на себя. Применение Φ к формальному слову из $F(S)$ заключается в вычислении этого слова в группе G. Обозначим через H ядро гомоморфизма Φ, H состоит их всех несократимых слов в алфавите S, которые равны e группе G. Пусть L – такое множество соотношений из H (т.е. несократимых слов в алфавите X, лежащих в H), что H – наименьшая **нормальная** подгруппа в $F(X)$, содержащая L. Подгруппа H однозначно определяется множеством L: H состоит из всевозможных произведений элементов, сопряженных элементам из L или обратным элементам к элементам из L, т.е. множество элементов вида $ul^{\varepsilon}u^{-1}$, $l \in L$, $u \in F(X)$, $\varepsilon = \pm 1$, является множеством образующих подгруппы H. Множество L называется системой *определяющих соотношений* группы G над S. По теореме о гомоморфизмах $F(S)/H \cong G$, поэтому задание множества S и множества слов L определяет группу G с точностью до изоморфизма.Такое описание группы G называется *заданием группы образующими и определяющими соотношениями,* или, более кратко, *копредставлением* группы G. Иногда копредставление записывается так: $G \equiv (S||L)$. Определяющие соотношения часто записываются в виде $f = e$, где $f \in L$, а также в виде равенства двух слов $f = g$ в группе G. Последнее означает, что один из элементов fg^{-1}, gf^{-1} содержится в L. Группы, допускающие копредставление с конечным множеством определяющих соотношений L, называются *конечно определенными.*

3.1. Пусть $G = (S||L)$, где $S = \{a, b\}$, $L = \{a^2,\ b^2,\ (ab)^2\}$. Покажем, что группа G изоморфна четверной группе Клейна B_4. Напомним, что группа B_4 состоит из элементов $\{e,\ a,\ b,\ c\}$ с таблицей умножения $a^2 = b^2 = c^2 = e$, $ab = c$, $ac = b$, $bc = a$, группа B_4 коммутативна (так как $x^2 = e$ для любого $x \in B_4$). Элементы a, b порождают группу B_4. Применим универсальное свойство свободной группы для тождественного отображения $\varphi : S \longrightarrow S$. Пусть $H_1 = ker\Phi$. Для соответствующего сюръективного гомоморфизма $\Phi : F(S) \longrightarrow B_4$ $\Phi(a) = a$, $\Phi(b) = b$, $\Phi(ab) = \Phi(a)\Phi(b) = ab = c$. Пусть $H_1 = ker\Phi$. Обозначим через H наименьшую нормальную подгруппу в $F(S)$, содержащую множество L. Надо показать, что $H_1 = H$. Это будет означать, что L – множество определяющих соотношений для B_4. Так как в группе B_4 $\Phi(a^2) = a^2 = e$, $\Phi(b^2) = b^2 = e$, $\Phi((ab)^2) = (\Phi(ab))^2 = c^2 = e$, то a^2, b^2, $(ab)^2 \in H_1$. Поскольку H – наименьший нормальный делитель, содержащий L, то $H \subset H_1$. Обратно, $(\bar{a})^2 = (\bar{b})^2, (\bar{a}\bar{b})^2 = e$ в факторгруппе $G = F(S)/H$. Поэтому $\bar{a} = \bar{a}^{-1}$, $\bar{b} = \bar{b}^{-1}$, $\bar{a}\bar{b} = \bar{b}\bar{a}$, следовательно, G – абелева группа. Отсюда следует, что смежный класс по подгруппе H любого слова из $F(S)$ совпадает с одним из смежных классов $e,\ \bar{a},\ \bar{b},\ \bar{a}\bar{b}$. Таким образом, $|G| \leq 4$. С другой стороны, $|G| = |F(S)/H| = |(F(S)/H_1)/(H_1/H)| = |B_4|/|H_1/H| = 4|H_1/H|$. Отсюда получаем, что $|H_1/H| = 1$, т.е. $H_1 = H$.

Замечание. Приведенное рассуждение часто применяется для нахождения определяющих сооотношений. Предположим, что в группе G с множеством образующих S выполняются соотношения $L,\ L \subset F(S)$. Пусть H – наименьшая нормальная подгруппа свободной группы $F(S)$, содержащая L. Пусть $\Phi : F(S) \longrightarrow G$ - эпиморфизм, как в теореме 1. Очевидно, $H \subset Ker\ \Phi$. По основной теореме о гомоморфизмах Φ индуцирует эпиморфизм $\Phi^* : F(S)/H \longrightarrow G$. Следовательно, если $|G| = n$ и $|F(S)/H| \leq n$, то $G \cong F(S)/H$ и, значит, $G = (S||L)$, т. е. L – множество определяющих соотношений группы G над S.

3.2. Покажем, что группу S_3 можно задать образующими $a,\ b$ и определяющими соотношениями $a^2 = e,\ b^2 = e,\ (ab)^3 = e$, т.е. множество определяющих соотношений $L = \{a^2,\ b^2,\ (ab)^3\}$. Действительно, обозначим через $a,\ b$ транспозиции $(1,2),\ (1,3)$. Так как $(1,2),\ (1,3),\ (2,3)$ – образующие группы S_3 и $(2,3) = bab$, то $S = \{a,\ b\}$ – система образующих группы S_3. Легко проверить, что в S_3 $a^2 = e,\ b^2 = e, (ab)^3 = e$. Пусть H – наименьшая нормальная подгруппа $F(S)$, содержащая $L,\ G = (S||L)$. Группа G имеет две образующие a и b. Покажем, что $|G| \leq 6$. Любой элемент $g \in G$ имеет вид $g = a^{n_1}b^{m_1} \dots a^{n_k}b^{m_k},\ n_i,\ m_i \in \mathbb{Z}$. Так как $a^2 = b^2 = e$, то $a = a^{-1},\ b = b^{-1}$, поэтому можно считать, что $0 \leq n_i,\ m_i \leq 1$. Таким образом, в группе G есть элементы $e,\ a,\ b,\ ab,\ ba$. Элементов длины 3 может быть не больше одного: $aba = a(ab)^{-1} = a(ab)^2 = a(ab)(ab) = bab$. Покажем, что новых элементов длины 4 нет. Действительно, элементы длины 4 могут иметь вид $abab$ или $baba$, но $abab = (ab)^2 = (ab)^{-1} = ba$ и $baba = (ba)^2 = (ba)^{-1} = ab$, т. е. они имеют длину 2. Так как в G нет элементов длины 4, то нет и элементов большей длины. Таким образом, $|G| \leq 6$. Итак, S_3 порождается элементами $a,\ b$, в S_3 выполняются соотношения L, группа $G = (a,\ b||a^2,\ b^2,\ (ab)^3)$ имеет не более 6 элементов. Применяя замечание, получаем, что $S_3 = (a,\ b||a^2,\ b^2,\ (ab)^3)$.

3.3. Может оказаться, что определяющие соотношения таковы, что единственная группа, в которой они выполняются, состоит только из единичного элемента. Рассмотрим пример. Пусть группа G задается образующими $x,\ y$ и определяющими соотношениями $x^4 = e,\ yx^3 = x^2y,\ xy^5 = y^6x$. Из второго соотношения получаем $yx^3y^{-1} = x^2$. Возведем в квадрат, $yx^6y^{-1} = x^4 = e$. Отсюда $x^6 = e$, но по условию $x^4 = e$, следовательно, $x^2 = e$. Теперь из второго соотношения получаем $yx^3 = y$. Откуда $x^3 = e$. Так как $x^2 = e$, то $x = e$ Теперь из третьего определяющего соотношения получаем $y^5 = y^6$, т.е. $y = e$.

Итак, $x = y = e$, следовательно, $G = \{e\}$.

3.4. Если в некоторой группе K, порожденной множеством S, выполняются соотношения $L \subset F(S)$, $F(S)$ – свободная группа, то гомоморфизм $\varphi : F(S) \longrightarrow K$, тождественный на S, индуцирует сюръективеый гомоморфизм $\varphi^* : G = (S||L) \longrightarrow K$. Покажем, как это может быть использовано. Пусть $G = (x,\ y \mid\mid x^2 = y^2 = e)$.
1) Будет ли группа G коммутативной? Рассмотрим группу S_3. Эта группа порождается транспозициями $x = (1,\ 2),\ y = (2,\ 3)$ (см. п. 1.3.). Так как $x^2 = y^2 = e$ в S_3, то существует сюръективный гомоморфизм G на S_3. Поскольку S_3 неабелева, то и G – неабелева группа.
2) Будет ли группа G бесконечной? Рассмотрим группу D, порожденную двумя отражениями $\sigma_a,\ \sigma_b$ относительно двух прямых a и b на плоскости, пересекающихся в точке O. Выберем прямые так, чтобы угол α между ними не был рациональным кратным числа π, например, $\alpha = \pi\sqrt{2}$. Произведение отражений $\sigma_a\sigma_b$ является поворотом плоскости на угол 2α вокруг точки пересечения прямых. В силу выбора α $(\sigma_a\sigma_b)^n \neq 1$ для любого целого числа n. Следовательно, группа D бесконечна. Так как группа D порождается элементами $\sigma_a,\ \sigma_b$ и $\sigma_a^2 = \sigma_b^2 = 1$, то существует сюръективный гомоморфизм $\varphi : G \longrightarrow D,\ \varphi(x) = \sigma_a,\ \varphi(y) = \sigma_b$. Так как группа D бесконечна, то и G бесконечна.

3.5. *Группа кос* $B_n,\ n > 1$ задается образующими $\sigma_1, \ldots,\ \sigma_{n-1}$ и определяющими соотношениями $\sigma_i\sigma_j = \sigma_j\sigma_i$, когда $|i - j| > 1$, и $\sigma_i\sigma_{i+1}\sigma_i = \sigma_{i+1}\sigma_i\sigma_{i+1}$ (группа B_2 – свободная группа с одним свободным образующим элементом, т.е. бесконечная циклическая группа).
Группа S_n порождается транспозициями $\tau_i = (i,\ i+1),\ i = 1, \ldots, n-1$ (см. п.1.3.). Легко проверить, что τ_i удовлетворяют всем определяющим соотношениям для σ_i в B_n (проверьте!). Следовательно, существует сюръективный гомоморфизм $\varphi : B_n \longrightarrow S_n,\ \varphi(\sigma_i) = \tau_i$. Можно показать, что, добавляя к определяющим соотношениям группы B_n соотношение $\sigma_1^2 = 1$, получим определяющие соотношения группы S_n.

Группа кос была введена Э. Артином. Она играет важную роль в топологии "малой размерности"(low-dimensional topology) и, в частности, в теории узлов. Вообще, теория групп, заданных образующими и определяющими соотношениями, возникла в связи с проблемами топологии, и топологические методы играют в ней ключевую роль.

3.6. Основные алгоритмические проблемы теории групп.

Алгебраическая теория групп, заданных образующими и определяющими соотношениями, имеет дело со словами в групповых алфавитах и их преобразованиями, что естественно приводит к постановке алгоритмических проблем. В 1911 г. М. Дэн сформулировал три основные алгоритмические проблемы. Пусть G – группа, заданная множеством образующих $S = \{s_1,\ s_2, \ldots\}$ и определяющими соотношениями, $F(S)$ – свободная группа.

1. (Проблема слов) Существует ли алгоритм, который для любого слова $g \in F(S)$ выясняет за конечное число шагов, равно выражение g единице в группе G или нет.

2. (Проблема сопряженности) Существует ли алгоритм, который для любых слов $g_1,\ g_2 \in F(S)$ выясняет за конечное число шагов, сопряжены элементы, соответствующие словам g_1 и g_2 в группе G, или нет.

3. (Проблема изоморфизма) Существует ли алгоритм, который для произвольной группы G_1, заданной своим копредставлением, за конечное число шагов устанавливает, изоморфна G_1 группе G или нет.

Если для группы G алгоритм, решающий проблему, существует, то говорят, что соответствующая проблема разрешима для группы G. Проблема слов разрешима для многих классов групп, однако есть конечнопорожденные и конечно-определенные группы G, для которых проблема слов неразрешима (П.С. Новиков, 1952). Проблемы сопряженности и изоморфизма являются наиболее трудными. Известно, что проблема изоморфизма неразрешима даже для $G = \{e\}$, т.е. не существует алгоритма, выясняющего для любой группы G_1, заданной образующими и определяющими соотношениями, состоит G_1 только из единичного элемента или нет (С.И. Адян, 1955).

4. Задачи

4.1. Доказать, что
a) группа S_n порождается транспозициями $(1,2),\ (1,3),\dots,(1,n)$;
b) группа S_n порождается транспозицией $(1,2)$, и циклом $(1,2,\dots,n)$;
c) группа A_n порождается циклами длины 3.

4.2. Доказать, что группа $SL_n(F)$, F – поле, порождается трансвекциями $E+\alpha E_{ij}, \alpha\in F$ (см. пример 1.4.).

4.3. Доказать, что группа $SL_n(\mathbb{Z})$ порождается трансвекциями $E+\alpha E_{ij}, \alpha = \pm 1$. (Отсюда следует, что группа $SL_n(\mathbb{Z})$ конечно порождена.

4.4 Пусть $G = GL_2(\mathbb{C}),\ S=\{a,\ b\}$, где $a = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $b = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$. Подгруппа Q в G, порожденная множеством S, называется *группой кватернионов.* Доказать, что
a) Q – неабелева группа порядка 8;
b) каждая подгруппа в Q нормальна.

c) показать, что группы Q задается образующими $x,\ y,\ z,\ t$ и опеделяющими соотношениями $t^2=1,\ x^2=y^2=z^2=t,\ xy=z,\ yz=x,\ zx=y.$

4.5. *Группой диэдра* D_n называется подруппа группы ортогональных преобразований плоскости, порожденная отражениями относительно двух прямых, расположенных под углом π/n. Доказать, что
a) D_n имеет порядок $2n$;
b) группа симметрий правильного n-угольника изоморфна группе D_n.

4.6. Показать, что группа диэдра D_n задается образующими $a,\ b$ и определяющими соотношениями $L=\{a^2,\ b^2,\ (ab)^n\}$.

4.7. Доказать, что группа S_3 имеет копредставление $(a,\ b||a^2,\ b^3,\ (ab)^2)$.

4.8. Показать, что знакопеременная группа A_4 задается образующими $a = (2\ 3\ 4), b=(1\ 2)(3\ 4)$ и определяющими соотношениями $L=\{a^3,\ b^2, (ab)^3\}$.

4.9. Доказать, что для группы $B_4 = (a,\ b||a^2,\ b^2, (ab)^2)$ (см. п. 3.1.)разрешима проблема слов. (Указание: описать алгоритм редукции смежного класса слова g по наименьшей нормальной подгруппе H свободной группы $F(a,\ b)$, содержащей слова $a^2,\ b^2,\ (ab)^2$, к нормальному виду $e,\ \bar{a},\ \bar{b},\ \bar{a}\bar{b}$ (см. п. 3.1.). Два слова определяют один элемент группы B_4 тогда и только тогда, когда их смежные классы приводятся к одному каноническому виду.)

4.10. Доказать, что для группы D_3 (см. задачу 4.6.) разрешима проблема слов. (Указание: Найти канонический вид смежных классов слов свободной группы $F(a,\ b)$ по наименьшей нормальной подгруппе H, содержащей определяющие соотношения $a^2,\ b^2, (ab)^3$ и описать алгоритм приведения к каноническому виду.)

Литература

[1] Кострикин А.И. Введение в алгебру. Часть III. Основные структуры алгебры. М.: МЦНМО, 2009. - 272 с.

[2] Сборник задач по алгебре. Под. ред. А.И. Кострикина. М.: Факториал, 1995. - 454 с.

[3] Каргаполов М.И., Мерзляков Ю.И. Основы теории групп. - М.: Наука, 1977. - 240 с.

[4] Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. - М.: Наука, 1974. - 456 с.

Михаил Иванович **Кузнецов**

ЗАДАНИЕ ГРУПП ОБРАЗУЮЩИМИ И ОПРЕДЕЛЯЮЩИМИ СООТНОШЕНИЯМИ

Учебно-методическое пособие

Федеральное государственное автономное образовательное учреждение
высшего профессионального образования
«Нижегородский государственный университет им. Н.И. Лобачевского».
603950, Нижний Новгород, пр. Гагарина, 23.

Подписано в печать . .2014. Формат 60×84 1/16.
Бумага офсетная. Печать офсетная. Гарнитура Таймс.
Усл. печ. л. . Заказ № . Тираж 100 экз.
Отпечатано в типографии Нижегородского госуниверситета
им. Н.И. Лобачевского
603600, г. Нижний Новгород, ул. Большая Покровская, 37
Лицензия ПД № 18-0099 от 14.05.01