Министерство образования и науки Российской Федерации
ФГБОУ ВО «Ивановский государственный университет»

Д. И. Молдаванский

ВВЕДЕНИЕ
В КОМБИНАТОРНУЮ ТЕОРИЮ ГРУПП

Учебное пособие
для студентов бакалавриата и магистратуры
направлений «Математика»
и «Математика и компьютерные науки»,
для аспирантов направления
«Математика и механика»

Иваново
Издательство «Ивановский государственный университет»
2018

УДК 512.54
ББК 22.144
М 75

Молдаванский, Д. И.

Введение в комбинаторную теорию групп [Электронный ресурс] : учеб. пособие для студентов бакалавриата и магистратуры направлений «Математика» и «Математика и компьютерные науки», для аспирантов направления «Математика и механика» / Д. И. Молдаванский. — Электрон. дан. — Иваново : Иван. гос. ун-т, 2018. — 1 электрон. опт. диск (DVD-ROM) ; 12 см. — Систем. требования: программа чтения файлов в формате PDF 1.4. — ISBN 978-5-7807-1244-2.

Целью пособия является первоначальное знакомство с понятиями и методами, лежащими в основе комбинаторной теории групп. Принятый в нем порядок изложения отличается от используемого в известной монографии В. Магнуса, А. Карраса и Д. Солитэра и, по мнению автора, позволяет быстрее овладеть основами теории. Изложение свойств свободных конструкций групп — обобщенных свободных произведений и HNN-расширений проводится более подробно, чем в существующей монографической литературе, и с учетом современного состояния исследований в данной области.

Предназначено студентам бакалавриата и магистратуры направлений «Математика» и «Математика и компьютерные науки», аспирантам направления «Математика и механика», преподавателям и научным работникам, интересующимся комбинаторной теорией групп.

Печатается по решению редакционно-издательского совета Ивановского государственного университета

Рецензенты:

кафедра высшей и прикладной математики
ФГБОУ ВО «Ивановский государственный
химико-технологический университет»
(зав. кафедрой доктор физико-математических наук,
профессор **Г. А. Зуева**)

кандидат физико-математических наук **О. Е. Сенкевич**
(компания ABBYY)

ISBN 978-5-7807-1244-2

ОГЛАВЛЕНИЕ

Предисловие

Предлагаемое пособие написано на основе ряда специальных курсов лекций, читавшихся в разное время для студентов и аспирантов математического факультета Ивановского государственного университета. Оно может быть полезным тем студентам, тематика выпускных работ (бакалаврских ВКР и магистерских диссертаций) которых относится к комбинаторной теории групп, одному из направлений научно-исследовательской работы, проводимой на факультете математики и компьютерных наук университета.

Комбинаторной теорией групп называют тот раздел общей теории групп, который характеризуется тем, что информация о строении и свойствах группы извлекается из вида ее задания порождающими и определяющими соотношениями. Каждая группа может быть задана таким образом, и в ряде случаев, когда для данной конкретной группы удалось найти ее задание (или, как иногда говорят, представление) порождающими и определяющими соотношениями, это позволяет получить дополнительную информацию об ее свойствах. С другой стороны, часто все, что нам известно об интересующей нас группе, это ее задание порождающими и определяющими соотношениями. Таковы, например, группы, которые строятся при помощи свободных конструкций групп, свободных произведений с объединяемыми подгруппами и HNN-расширений. В этих случаях такое задание является единственным источником информации о строении группы. Нахождение решений этой весьма нетривиальной задачи описания строения группы, заданной порождающими и определяющими соотношениями, и является предметом комбинаторной теории групп.

Систематическому изложению комбинаторной теории групп посвящены монографии [1] и [2]. При этом, книга [1] является предназначенным для начинающих подробным введением в предмет, тогда как [2] рассчитана на более продвинутого читателя, и является более углубленным изложением этой теории, содержащим ряд современных методов и результатов.

Данное пособие, как и книга [1], требует от читателя лишь владения основами теории групп в объеме стандартного университетского курса алгебры; все необходимые сведения можно, впрочем, найти в учебном пособии [3]. Для полноты информации в список литературы включено также несколько оригинальных статей, являющихся значительным вкладом в развитие данной теории.

Принятый в пособии порядок изложения основ теории отличается от используемого в [1] и, по мнению автора, позволяет быстрее овладеть основными понятиями и методами этого раздела теории групп. Настоятельно рекомендуется, тем не менее, сравнивать прочитанное с соответствующими разделами из [1] и, в особенности, выполнять упражнения и решать задачи, которые предлагаются в этой книге в весьма значительном количестве.

Пособие состоит из шести параграфов, четыре из которых, в свою очередь, разбиты на несколько разделов. Нумерация выделенных формул своя в каждом параграфе. Выделенные утверждения нумеруются тройкой чисел. Например, 2.4.1 — номер 1-ой теоремы из раздела 2.4 параграфа 2.

§ 1. Свободные группы

1.1. Построение свободной группы. Начнем с того, что фиксируется некоторый алфавит $A = \{a_1, a_2, \ldots, a_n\}$, т. е. набор символов или значков, которые различаются по их написанию. Здесь для обозначения алфавитных символов будут использоваться малые латинские буквы с индексами или без (например, a_1, a_2, b, x, y). Мощность множества алфавитных символов может быть произвольной; для удобства мы записываем алфавит в виде, указанном выше, считая, что n может быть произвольным ординальным числом.

Словом в алфавите A называется произвольная конечная последовательность символов этого алфавита, т. е. последовательность вида

$$a_{i_1}, a_{i_2}, \ldots, a_{i_r}$$

(где индексы $i_1, i_2, \ldots, i_r$ принадлежат множеству $\{1, 2, \ldots, n\}$). При записи слова мы будем опускать запятые, разделяющие алфавитные символы, и часто обозначать слово одной буквой. Так, если w обозначает слово указанного выше вида, мы пишем $w = a_{i_1} a_{i_2} \ldots a_{i_r}$. Если мы не хотим выписывать явный вид слова w, но хотим лишь указать, что w является словом в алфавите A, то будем писать $w = w(a_1, a_2, \ldots, a_n)$ или $w = w(a_i)$. Алфавитные символы, составляющие слово w, естественно называть также *буквами*, что мы и будем иногда делать.

Равенство двух слов означает совпадение соответствующих последовательностей. Более подробно, для произвольных слов

$$w = a_{i_1} a_{i_2} \ldots a_{i_r} \qquad \text{и} \qquad v = a_{j_1} a_{j_2} \ldots a_{j_s}$$

равенство $w = v$ имеет место тогда и только тогда, когда $r = s$ и для любого $k = 1, 2, \ldots, r$ алфавитные символы a_{i_k} и a_{j_k} совпадают, т. е. $i_k = j_k$. Это равенство слов называют также *графическим равенством*.

Количество r символов, составляющих слово $w = a_{i_1} a_{i_2} \ldots a_{i_r}$, будем называть *длиной* этого слова и записывать $l(w) = r$. Из сформулированных до сих пор соглашений следует, что длина любого слова является положительным целым числом. Тем не менее, удобно ввести в рассмотрение и *пустое слово*, т. е. слово, не содержащее ни одного символа. Пустое слово будем обозначать символом 1, а его длину считать равной нулю; таким образом, для любого слова w имеем: $l(w) = 0$ тогда и только тогда, когда $w = 1$.

Пусть $W(A)$ обозначает множество всех слов в алфавите A. На множестве $W(A)$ естественным образом возникает *операция умножения*, состоящая в простом приписывании одного слова к другому: если $u = a_{i_1}a_{i_2}\dots a_{i_r}$ и $v = a_{j_1}a_{j_2}\dots a_{j_s}$ — слова, то их произведением называется слово

$$uv = a_{i_1}a_{i_2}\dots a_{i_r}a_{j_1}a_{j_2}\dots a_{j_s}.$$

Очевидно, что эта операция ассоциативна, а пустое слово является нейтральным элементом. Таким образом, рассматриваемое вместе с этой операцией множество $W(A)$ оказывается полугруппой с единицей, т. е. — моноидом.

Операция умножения слов позволяет сформулировать определение *подслова* данного слова: слово v называется подсловом слова w, если $w = xvy$ для некоторых (возможно, пустых) слов x и y. Если при этом слово x пустое, то слово v будем называть *начальным подсловом* слова w, а если y пустое, — *конечным подсловом* слова w.

Очевидно, что моноид $W(A)$ не является группой: единственным обратимым элементом его является единица. Для получения группы необходимы дальнейшие построения.

Расширим алфавит A, присоединив к нему для каждого $i = 1, 2, \dots, n$ новый символ a_i^{-1}, соответствующий символу a_i. Следует подчеркнуть, что -1 (расположенная в этой записи на месте, занимаемом обычно показателем степени) здесь является лишь частью формального обозначения нового алфавитного символа. Этот расширенный алфавит называется *групповым*.

Всюду ниже термин “алфавит” будет обозначать только групповой алфавит. Поэтому введение нового обозначения не имеет смысла, и мы будем слова в групповом алфавите, полученном из алфавита A, по-прежнему называть словами в алфавите A, а множество всех таких слов обозначать через $W(A)$. Если договориться отождествлять запись a_i^1 с символом a_i исходного алфавита, то произвольный символ расширенного алфавита будет иметь вид a_i^ε, где $\varepsilon = \pm 1$. Таким образом, теперь произвольное слово из множества $W(A)$ записывается в виде $w = a_{i_1}^{\varepsilon_1}a_{i_2}^{\varepsilon_2}\dots a_{i_r}^{\varepsilon_r}$, где $\varepsilon_j = \pm 1$ для каждого $j = 1, 2, \dots, r$.

Кроме операции умножения слов, определяемой на этом (расширенном) множестве $W(A)$ точно так же, как это было сделано выше, введем здесь еще и операцию *формального обращения* слов: формально обратным к слову $w = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \dots a_{i_r}^{\varepsilon_r}$ будем называть слово

$$w^{-1} = a_{i_r}^{-\varepsilon_r} a_{i_{r-1}}^{-\varepsilon_{r-1}} \dots a_{i_1}^{-\varepsilon_1}.$$

Далее, введем *свободные элементарные преобразования* слов из множества $W(A)$; эти преобразования делятся на два типа.

Преобразование первого типа, называемое *вставкой*, заключается в том, что между соседними буквами данного слова, или перед первой буквой этого слова, или после его последней буквы вставляется слово $a_i^{\varepsilon} a_i^{-\varepsilon}$, где $\varepsilon = \pm 1$.

Преобразование второго типа называется *вычеркиванием* и состоит в вычеркивании из данного слова некоторого подслова вида $a_i^{\varepsilon} a_i^{-\varepsilon}$, где снова $\varepsilon = \pm 1$. Преобразование вычеркивания называют также (элементарным) *сокращением*.

Определим теперь на множестве $W(A)$ *отношение свободного равенства слов*, обозначаемое символом $\approx$:

Полагаем, что для произвольных слов $u, v \in W(A)$ утверждение $u \approx v$ является истинным, если существует конечная последовательность элементарных преобразований, переводящая слово u в слово v. Более подробно, это означает, что слово u свободно равно слову v тогда и только тогда, когда существует последовательность слов $w_0, w_1, \dots, w_m$ такая, что $w_0 = u$, $w_m = v$ и при $m > 0$ для каждого $i = 0, 1, \dots, m-1$ слово w_{i+1} получается из слова w_i некоторым свободным элементарным преобразованием.

Имеет место следующее утверждение:

1.1.1. Предложение. *Отношение свободного равенства является эквивалентностью на множестве $W(A)$. Кроме того, для любых слов u, v и w из того, что $u \approx v$, следует, что $wu \approx wv$ и $uw \approx vw$.*

В самом деле, свойство рефлексивности отношения свободного равенства (состоящего в том, что для любого слова u утверждение $u \approx u$ истинно) справедливо, так как для произвольного слова u последовательность, состоящая из единственного слова $w_0 = u$, удовлетворяет определению этого отношения (просто потому, что, поскольку $m = 0$, от такой последовательности определение отношения свободного равенства ничего не требует). Симметричность отношения $\approx$ очевидна в силу того, что если слово w_{i+1} получается из слова w_i некоторым свободным элементарным преобразованием, то и слово w_i получается из слова w_{i+1} некоторым свободным элементарным преобразованием. Очевидна и транзитивность этого отношения: если $u \approx v$ и $v \approx w$, то слово u можно преобразовать в слово w, преобразовав сначала u в v, а затем v – в w. Очевидно, наконец, если слово u переводится в слово v последовательностью w_0, w_1, $\ldots$, w_m, то слово wu можно преобразовать в слово wv последовательностью ww_0, ww_1, $\ldots$, ww_m и слово uw можно преобразовать в слово vw последовательностью w_0w, w_1w, $\ldots$, w_mw.

Напомним, что произвольному отношению эквивалентности $\sim$ на некотором множестве X соответствует разбиение этого множества на непересекающиеся классы эквивалентных элементов. Совокупность всех этих классов называется фактор-множеством множества X по отношению $\sim$ и обозначается через $X/\sim$.

Фактор-множество $W(A)/\approx$ множества $W(A)$ по эквивалентности $\approx$ будем обозначать через $F(A)$ или через $F(a_1, a_2, \ldots, a_n)$.

Таким образом, элементами множества $F(a_1, a_2, \ldots, a_n)$ являются всевозможные классы свободно равных между собой слов, т. е подмножества вида $[u] = \big\{w \in W(A) \bigm| u \approx w\big\}$. Слово u будем называть *представителем* класса $[u]$. В действительности, представителем класса может служить любой элемент этого класса: для любых слов u и v равенство $[u] = [v]$ выполнено тогда и только тогда, когда $u \approx v$.

Из предложения 1.1.1 вытекает, как легко видеть, что для любых слов u, u_1, v, v_1 из того, что $u \approx u_1$ и $v \approx v_1$, следует справедливость утверждения $uv \approx u_1v_1$. Это позволяет корректно определить на множестве $F(a_1, a_2, \ldots, a_n)$ операцию умножения, действующую по правилу: произведением двух классов считается класс, содержащий произведение их представителей (и, в силу предыдущего замечания, не зависящий от выбора представителей в перемножаемых классах). Более формально, для произвольных элементов $[u]$ и $[v]$ множества $F(A) = F(a_1, a_2, \ldots, a_n)$ полагаем $[u] \cdot [v] = [uv]$.

Очевидно, что эта операция ассоциативна, класс, представляемый пустым словом, является единицей и поскольку для любого $u \in W(A)$ имеют место свободные равенства $uu^{-1} \approx 1$ и $u^{-1}u \approx 1$ (где, напомним, u^{-1} — формально обратное к слову u), для каждого элемента $[u]$ множества $F(a_1, a_2, \ldots, a_n)$ в этом множестве существует обратный $[u^{-1}]$. Таким образом справедливо

1.1.2. Предложение. *Множество $F(a_1, a_2, \ldots, a_n)$ классов свободно равных слов, рассматриваемое вместе с операцией умножения классов, является группой.*

Группа $F(a_1, a_2, \ldots, a_n)$ из предложения 1.1.2 называется *свободной группой на алфавите* $\{a_1, a_2, \ldots, a_n\}$.

Таким образом, по построению группы $F = F(a_1, a_2, \ldots, a_n)$ произвольный элемент f этой группы является некоторым классом свободно равных слов. Допуская определенную вольность речи, удобно отождествлять элемент f с представителем этого класса и, следовательно, считать элементами группы F слова в алфавите $\{a_1, a_2, \ldots, a_n\}$. При этом, следует различать графическое равенство слов (т. е. совпадение соответствующих последовательностей) и их равенство как элементов группы F: если u и v — произвольные слова, то равенство в группе F *элементов* u и v означает свободное равенство слов u и v. Отметим, что при таком соглашении формальный смысл показателя -1 в записи алфавитного символа a_i^{-1} переходит в содержательное обозначение элемента, обратного к элементу a_i.

(Подобным соглашением мы по умолчанию пользуемся постоянно, отождествляя рациональное число с представляющей его дробью и считая, что, скажем, дроби $1/2$ и $5/10$ являются одним и тем же числом (хотя формально эти дроби следует считать различными). В действительности, рациональное число есть класс эквивалентных дробей, а соответствующее отношение эквивалентности в школьном курсе математики определяется как “правило равенства дробей”.)

Покажем, что в каждом классе свободно равных слов существует единственный представитель, являющийся словом определенного вида.

Слово w в алфавите $\{a_1, a_2, \ldots, a_n\}$ называется *несократимым*, если оно не содержит подслов вида $a_i^{\varepsilon} a_i^{-\varepsilon}$, где $\varepsilon = \pm 1$. Говоря более подробно, слово $w = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$ называется несократимым, если либо его длина r не превосходит 1, либо $r > 1$ и для любого номера j, $1 \leqslant j < r$, из того, что $\varepsilon_j + \varepsilon_{j+1} = 0$, следует, что $i_j \neq i_{j+1}$.

Очевидно, что слово w несократимо тогда и только тогда, когда нему неприменимо преобразование сокращения. Поскольку каждое сокращение слова уменьшает его длину на 2, первое утверждение следующей теоремы очевидно.

1.1.3. Теорема. *Любое слово в алфавите* $\{a_1, a_2, \ldots, a_n\}$ *свободно равно некоторому несократимому слову. Если несократимые слова* u *и* v *свободно равны, то они графически равны.*

Доказательство. Как было отмечено только что, доказательства требует лишь второе утверждение теоремы. Предположим, рассуждая от противного, что существуют свободно равные несократимые слова u и v, которые графически различны.

Так u и v свободно равны, существует конечная последовательность слов w_0, w_1, $\dots$, w_m такая, что $u = w_0$, $v = w_m$ и для любого номера $i = 0, 1, \dots, m-1$ слово w_{i+1} получается из слова w_i вставкой или вычеркиванием некоторого тривиального слова. Заметим, что поскольку $u \neq v$, хотя бы одно преобразование должно быть выполнено, т. е. $m \geqslant 1$. Будем считать, что из всех таких последовательностей нами выбрана та, у которой сумма $\sum_{i=0}^{m} l(w_i)$ длин всех ее членов минимальна.

Поскольку слово $w_0 = u$ несократимо, элементарное преобразование сокращения к нему неприменимо, и потому слово w_1 должно получаться из слова w_0 вставкой некоторого слова вида $a_i^{\varepsilon} a_i^{-\varepsilon}$, где $\varepsilon = \pm 1$. В частности, поэтому $l(w_0) < l(w_1)$. Аналогично, поскольку несократимое слово $w_m = v$ может быть получено из слова w_{m-1} только сокращением, имеет место неравенство $l(w_{m-1}) > l(w_m)$. Из этих замечаний следует, очевидно, существование такого номера k, $0 < k < m$, что $l(w_{k-1}) < l(w_k)$ и $l(w_k) > l(w_{k+1})$. Это означает, что слово w_k получается из слова w_{k-1} вставкой, т. е.

$$w_{k-1} = pq \quad \text{и} \quad w_k = p a_i^{\varepsilon} a_i^{-\varepsilon} q \tag{1}$$

для некоторых слов p и q, номера i, $1 \leqslant i \leqslant n$, и $\varepsilon = \pm 1$, а слово w_{k+1} получается из слова w_k сокращением, т. е.

$$w_k = r a_j^{\delta} a_j^{-\delta} s \quad \text{и} \quad w_{k+1} = rs \tag{2}$$

для некоторых слов r и s, номера j, $1 \leqslant j \leqslant n$, и $\delta = \pm 1$.

Будем предполагать, что $l(p) \leqslant l(r)$ (это не уменьшает степень общности, так как в противном случае мы можем, поменяв местами слова u и v, записать последовательность w_0, w_1, $\dots$, w_m в обратном порядке), и рассмотрим отдельно три случая. Искомое противоречие будет состоять в том, что, как будет показано, в каждом из этих случаев суммарная длина слов последовательности, преобразующей слово u в слово v, может быть уменьшена.

Случай 1. $l(p) \leqslant l(r) - 2$. Так как $w_k = p a_i^{\varepsilon} a_i^{-\varepsilon} q = r a_j^{\delta} a_j^{-\delta} s$, в этом случае начальное подслово длины $l(p) + 2$ слова w_k должно быть начальным подсловом слова r, т. е. $r = p a_i^{\varepsilon} a_i^{-\varepsilon} r_1$ для некоторого слова r_1 и потому $q = r_1 a_j^{\delta} a_j^{-\delta} s$. Подставляя это выражение для q в запись слова w_{k-1} из (1), а выражение для r — в запись слова w_{k+1} из (2), имеем

$$w_{k-1} = p r_1 a_j^{\delta} a_j^{-\delta} s \quad \text{и} \quad w_{k+1} = p a_i^{\varepsilon} a_i^{-\varepsilon} r_1 s.$$

Поэтому слово $w'_k = pr_1s$ получается из слова w_{k-1} вычеркиванием подслова $a_j^\delta a_j^{-\delta}$, а слово w_{k+1} получается из слова w'_k вставкой подслова $a_i^\varepsilon a_i^{-\varepsilon}$. Следовательно, в последовательности $w_0, w_1, \ldots, w_{k-1}, w'_k, w_{k+1}, \ldots, w_m$ каждое слово, начиная с w_1, получается из предыдущего свободным элементарным преобразованием. Но так как $w_k = ra_j^\delta a_j^{-\delta}s = pa_i^\varepsilon a_i^{-\varepsilon}r_1a_j^\delta a_j^{-\delta}s$, длина слова w'_k меньше длины слова w_k, что противоречит минимальности суммарной длины исходной последовательности.

Случай 2. $l(p) = l(r) - 1$. В этом случае из равенства $w_k = pa_i^\varepsilon a_i^{-\varepsilon}q = ra_j^\delta a_j^{-\delta}s$ следует, что поскольку слово r является начальным подсловом длины $l(p)+1$ слова w_k, должны выполняться равенства $r = pa_i^\varepsilon$ и $a_i^{-\varepsilon}q = a_j^\delta a_j^{-\delta}s$. Отсюда $j = i$, $\delta = -\varepsilon$ и $q = a_j^{-\delta}s = a_i^\varepsilon s$. Следовательно, слова $w_{k-1} = pq = pa_j^{-\delta}s$ и $w_{k+1} = rs = pa_j^{-\delta}s$ совпадают, и потому вычеркнув из последовательности $w_0, w_1, \ldots, w_m$ слова w_k и w_{k+1}, мы получим последовательность, также доказывающую свободное равенство слов u и v. Это снова противоречит минимальности суммарной длины исходной последовательности.

Случай 3. $l(p) = l(r)$. В этом случае сравнение выражений слова w_k из (1) и (2) сразу дает равенства $p = r$, $i = j$, $\varepsilon = \delta$ и $q = s$. Таким образом, $w_{k-1} = w_{k+1}$, и противоречие получается так же, как в случае 2. Теорема доказана.

Таким образом, любой элемент группы $F(a_1, a_2, \ldots, a_n)$ определяется единственным несократимым словом, и длиной элемента называют длину определяющего его несократимого слова. Кроме того, в силу принятого выше соглашения элементами группы $F(a_1, a_2, \ldots, a_n)$ можно считать несократимые слова. Отметим еще вытекающее из теоремы 1.1.3

1.1.4. Следствие. *Любой элемент группы $F(a_1, a_2, \ldots, a_n)$, определяемый непустым несократимым словом, отличен от единицы.*

1.2. Некоторые свойства группы $\mathbf{F(a_1, a_2, \ldots, a_n)}$. Из определения операции в группе $F(a_1, a_2, \ldots, a_n)$ следует, очевидно, что для любого слова $u = a_{i_1}^{\varepsilon_1}a_{i_2}^{\varepsilon_2}\ldots a_{i_r}^{\varepsilon_r}$ выполнено равенство

$$[u] = [a_{i_1}^{\varepsilon_1}a_{i_2}^{\varepsilon_2}\ldots a_{i_r}^{\varepsilon_r}] = [a_{i_1}]^{\varepsilon_1}[a_{i_2}]^{\varepsilon_2}\ldots[a_{i_r}]^{\varepsilon_r}.$$

Отсюда и из нашей договоренности элементы группы $F(a_1, a_2, \ldots, a_n)$ называть представляющими эти элементы словами получаем

1.2.1. Предложение. *Система элементов $a_1, a_2, \ldots, a_n$ свободной группы $F(a_1, a_2, \ldots, a_n)$ является системой порождающих этой группы.*

Следующее важное свойство свободных групп выражает

1.2.2. Теорема. *Для любой группы G и произвольного отображения $\tau\colon A \to G$ множества $A = \{a_1, a_2, \ldots, a_n\}$ алфавитных символов в группу G существует гомоморфизм φ группы $F = F(a_1, a_2, \ldots, a_n)$ в группу G такой, что для любого $i = 1, 2, \ldots, n$ образ относительно φ элемента a_i группы F совпадает с образом символа a_i относительно τ.*

Доказательство. Продолжим отображение τ множества A в группу G до обозначаемого тем же символом τ отображения в эту группу множества $W(A)$ всех слов в алфавите A. Для этого обозначим для каждого $i = 1, 2, \ldots, n$ через g_i элемент группы G, являющийся образом относительно τ символа a_i, и полагаем для любого непустого слова $u = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$

$$u\tau = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_r}^{\varepsilon_r}$$

(где в выражении, стоящем справа от знака равенства, выполняются операции умножения и взятия обратного в группе G), а образом пустого слова считаем единицу группы G. Элемент $u\tau$ группы G будем называть *значением слова u при отображении τ*.

Отметим, что из этого определения (и определения умножения слов) следует, очевидно, что для любых слов u и v из $W(A)$ имеет место равенство $(uv)\tau = u\tau \cdot v\tau$ (в правой части которого снова имеется в виду умножение в группе G).

Покажем, что значения любых свободно равных слов совпадают, т. е. для любых слов u и v таких, что $u \approx v$, выполнено равенство $u\tau = v\tau$. Ясно, что для этого достаточно установить совпадение значений двух слов, одно из которых получается из другого единственным свободным элементарным преобразованием. Но это практически очевидно, так как если $u = xa_j^{\varepsilon} a_j^{-\varepsilon} y$ и $v = xy$, имеем

$$u\tau = (xa_j^{\varepsilon} a_j^{-\varepsilon} y)\tau = x\tau \cdot (a_j\tau)^{\varepsilon} \cdot (a_j\tau)^{-\varepsilon} \cdot y\tau = x\tau \cdot y\tau = (xy)\tau = v\tau.$$

Определим теперь отображение φ группы F в группу G, для произвольного элемента $[u] \in F$ полагая $[u]\varphi = u\tau$. В силу только что сделанного замечания это определение корректно, поскольку назначаемый им образ элемента $[u]$ не зависит от выбора представителя этого класса свободно равных слов. Гомоморфность отображения φ проверяется непосредственно. Наконец, из нашей договоренности отождествлять классы классы свободно равных слов с их представителями следует, что для любого $j = 1, 2, \ldots, n$ имеем $a_j\varphi = [a_j]\varphi = a_j\tau$. Теорема доказана.

Критерий равенства элементов свободной группы установлен в теореме 1.1.3. Для получения критерия сопряженности элементов группы $F(a_1, a_2, \ldots, a_n)$ используется следующее понятие:

Несократимое слово $w = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$ называется *циклически несократимым*, если из того, что $\varepsilon_1 + \varepsilon_r = 0$, следует, что $i_1 \neq i_r$.

Из определения следует, что несократимое слово $w = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$ не является циклически несократимым в том и только в том случае, когда $i_1 = i_r$ и $\varepsilon_1 = -\varepsilon_r$. Поскольку это условие может выполняться лишь при $r > 2$, пустое слово, любое слово длины 1 и любое несократимое слово длины 2 циклически несократимы.

Элемент свободной группы, определяемый циклически несократимым словом, будем называть *циклически несократимым элементом.*

Очевидно, что если слово w циклически несократимо, то для любого целого числа $m > 0$ слово w^m является несократимым (и циклически несократимым) и потому (при $w \neq 1$) $l(w^m) = ml(w)$. Легко видеть также, что если элемент w не является циклически несократимым, то для любого целого числа $m > 0$ элемент w^m не является циклически несократимым.

Циклической перестановкой слова w называется произвольное слово вида yx, где x и y — такие подслова слова w, что $w = xy$.

Таким образом, список всех циклических перестановок слова $w = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$ имеет вид

$$a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}, \quad a_{i_2}^{\varepsilon_2} a_{i_3}^{\varepsilon_3} \ldots a_{i_r}^{\varepsilon_r} a_{i_1}^{\varepsilon_1}, \quad \ldots, \quad a_{i_r}^{\varepsilon_r} a_{i_1}^{\varepsilon_1} \ldots a_{i_{r-1}}^{\varepsilon_{r-1}}.$$

Легко видеть, что любая циклическая перестановка циклически несократимого слова являются циклически несократимым словом. Заметим также, что в силу очевидного равенства $yx = x^{-1}(xy)x$, справедливого в произвольной группе, элементы группы $F(a_1, a_2, \ldots, a_n)$, определяемые словами, одно из которых является циклической перестановкой другого, сопряжены. Для циклически несократимых элементов свободной группы справедливо и обратное утверждение:

1.2.3. Предложение. *В группе $F = F(a_1, a_2, \ldots, a_n)$ каждый элемент сопряжен с некоторым циклически несократимым элементом. Если циклически несократимые элементы u и v сопряжены, то один из них является циклической перестановкой другого.*

Доказательство Для доказательства первого утверждения достаточно заметить, что элемент w группы F, не являющийся циклически несократимым, сопряжен, очевидно, с некоторым элементом, длина которого равна $l(w) - 2$. Действительно, отсюда следует, что если среди элементов, сопряженных с данным, выбрать элемент, представляемый словом наименьшей длины, то этот элемент будет циклически несократимым.

Предположим, что циклически несократимые элементы u и v являются сопряженными в группе F, т. е. для некоторого несократимого слова w имеет место свободное равенство $u \approx w^{-1}vw$. Индукцией по длине слова w покажем, что тогда слово u совпадает с некоторой циклической перестановкой слова v.

Если $l(w) = 0$, т. е. $w = 1$, то это очевидно, так как в силу теоремы 1.1.3 свободное равенство несократимых слов равносильно их графическому равенству. Пусть $l(w) > 0$ и пусть для любой пары циклически несократимых слов, сопряженных с помощью слова меньшей длины, доказываемое утверждение справедливо.

Так как $l(w) > 0$, слово, стоящее в правой части свободного равенства $u \approx w^{-1}vw$ не может быть несократимым. Действительно, в противном случае с одной стороны, в силу теоремы 1.1.3 мы имели бы графическое равенство $u = w^{-1}vw$, а с другой стороны, поскольку слово w непусто, слово $w^{-1}vw$ не являлось бы циклически несократимым, что делает это равенство невозможным.

Поскольку слова v и w несократимы и слово v циклически несократимо, сокращения в слове $w^{-1}vw$ возможны только или на стыке слов w^{-1} и v, или на стыке слов v и w. В первом случае (второй рассматривается аналогично) это означает, что $w = a_i^{\varepsilon}x$ и $v = a_i^{\varepsilon}y$ для некоторых $i = 1, 2, \ldots, n$, $\varepsilon = \pm 1$ и подходящих слов x и y. Тогда $w^{-1}vw = x^{-1}a_i^{-\varepsilon}a_i^{\varepsilon}ya_i^{\varepsilon}x \approx x^{-1}(ya_i^{\varepsilon})x$. Таким образом, элемент u сопряжен при помощи элемента x с циклической перестановкой ya_i^{ε} слова v. Так как длина слова x меньше длины слова w, по индуктивному предположению слово u совпадает с некоторой циклической перестановкой слова ya_i^{ε}. Поскольку каждая циклическая перестановка слова ya_i^{ε} является некоторой циклической перестановкой слова v, слово u совпадает с некоторой циклической перестановкой слова v. Следовательно, индуктивный переход завершен, и предложение 1.2.3 полностью доказано.

1.2.4. Предложение. *Следующие утверждения справедливы для любой свободной группы $F = F(a_1, a_2, \ldots, a_n)$:*

(1) *Группа F является группой без кручения, т. е. порядок любого ее неединичного элемента бесконечен.*

(2) *Для любого нееденичного элемента u группы F множество натуральных чисел n, для которых в группе F существует корень n-ой степени из u (т. е. такой элемент x, что $u = x^n$) является конечным.*

(3) *Каждая нееденичная циклическая подгруппа группы F содержится в некоторой максимальной циклической подгруппе этой группы (т. е. в такой циклической подгруппе V, что для любой циклической подгруппы W группы F из включения $V \subseteq W$ следует равенство $V = W$).*

Доказательство. Пусть u — нееденичный элемент группы F и v — циклически несократимый элемент, сопряженный с u. Как было отмечено выше, для любого целого числа $m > 0$ слово v^m является несократимым и $l(v^m) = ml(v)$. Следовательно, для любого $m > 0$ имеем $v^m \neq 1$, и потому порядок элемента v бесконечен. Так как порядки сопряженных элементов совпадают, бесконечность порядка элемента u доказана.

Пусть снова u — нееденичный элемент группы F, v — циклически несократимый элемент, сопряженный с u и w — такой элемент группы F, что $u = w^{-1}vw$. Так как для любого натурального n и произвольного элемента $x \in F$ равенства $u = x^n$ и $v = (wxw^{-1})^n$ равносильны, корень n-ой степени из элемента u существует тогда и только тогда, когда существует корень n-ой степени из v. Таким образом, без потери общности можно считать, что элемент u циклически несократим.

Поэтому если элемент x (где слово x несократимо) удовлетворяет равенству $u = x^n$, то, как было замечено выше, элемент x должен быть также циклически несократимым. Следовательно, в силу теоремы 1.1.3 слова u и x^n графически совпадают, так что $l(u) = l(x^n) = nl(x)$ и потому число n является делителем числа $l(u)$. Так как множество натуральных делителей ненулевого целого числа конечно, утверждение (2) также доказано.

Пусть, наконец, U — циклическая подгруппа группы F, порождаемая элементом $u \neq 1$. Пусть n — наибольшее натуральное число, для которого корень n-ой степени из u существует. Обозначим этот корень через v, а через V — циклическую подгруппу, порожденную элементом v. Так как $u = v^n$, выполнено включение $U \subseteq V$, и остается показать, что V является максимальной циклической подгруппой.

Если W — циклическая подгруппа группы F, порождаемая элементом w и содержащая подгруппу V, то $v = w^k$ для некоторого целого числа k, которое можно считать положительным. Так как тогда $u = w^{kn}$, из выбора числа n следует, что $kn \leqslant n$, откуда имеем $k = 1$, $v = w$ и $V = W$. Предложение 1.2.4 полностью доказано.

1.2.5. Предложение. *Если элементы u и v свободной группы $F = F(a_1, a_2, \ldots, a_n)$ перестановочны, то оба они принадлежат некоторой циклической подгруппе этой группы. В частности, произвольная максимальная циклическая подгруппа группы F совпадает со своим централизатором.*

Доказательство. Для доказательства первого утверждения воспользуемся индукцией по сумме длин $l(u) + l(v)$ элементов u и v. В случае, когда $l(u) + l(v) = 0$, т. е. $u = v = 1$, принадлежность элементов u и v одной и той же циклической подгруппе очевидна. Предположим, что $l(u) + l(v) > 0$ и что для любой пары перестановочных элементов группы F, сумма длин которых меньше числа $l(u) + l(v)$, доказываемое утверждение справедливо.

Так как в случае, когда хотя бы один из элементов u и v равен 1, требуемое утверждение также очевидно, будем считать, что оба элемента неединичны (и, разумеется, представляющие их слова u и v несократимы). Поскольку элементы $x^{-1}ux$ и $x^{-1}vx$, сопряженные с элементами u и v при помощи одного и того же элемента x, перестановочны тогда и только тогда, когда перестановочны u и v, и лежат в некоторой циклической подгруппе тогда и только тогда, когда u и v лежат в одной и той же циклической подгруппе, можно без потери общности считать, что хотя бы один из перестановочных элементов u и v является циклически несократимым.

В самом деле, если, скажем, слово u не является циклически несократимым, то его несократимая запись имеет вид $u = a_i^{\varepsilon} u_1 a_i^{-\varepsilon}$. Так как $l(a_i^{-\varepsilon} u a_i^{\varepsilon}) = l(u_1) = l(u) - 2$ и $l(a_i^{-\varepsilon} v a_i^{\varepsilon}) \leqslant l(v) + 2$, сумма длин элементов u_1 и $a_i^{-\varepsilon} v a_i^{\varepsilon}$ не превосходит числа $l(u) + l(v)$. Поэтому в силу предыдущего замечания для индуктивного перехода можно использовать эти элементы. Если элемент u_1 не является циклически несократимым, к словам u_1 и $a_i^{-\varepsilon} v a_i^{\varepsilon}$ следует применить аналогичное преобразование. После нескольких таких шагов элемент u будет заменен циклически несократимым.

Считая элемент u циклически несократимым, перепишем равенство $uv = vu$ в виде $u = v^{-1}uv$. Так как элемент u циклически несократим и слово v непусто, к слову $v^{-1}uv$ должны быть применимы сокращения, причем они возможны только либо на стыке слов v^{-1} и u, либо на стыке слов u и v. В первом случае (второй рассматривается аналогично) это означает, что слова u и v должны начинаться с одного и того же алфавитного символа a_i^ε. Таким образом, у слов u и v имеется непустое общее начальное подслово, а потому существует и непустое общее начальное подслово x наибольшей длины, т. е. несократимые записи этих слов имеют вид $u = xu_1$ и $v = xv_1$, причем если оба подслова u_1 и v_1 непусты, то они начинаются с разных алфавитных символов.

Покажем, что в действительности хотя бы одно из слов u_1 и v_1 должно быть пустым.

Так как $v^{-1}uv = v_1^{-1}x^{-1}xu_1v$, слово u свободно равно слову $v_1^{-1}u_1v$. Если оба слова u_1 и v_1 непусты, то это слово несократимо, поскольку сокращение на стыке слов v_1^{-1} и u_1 невозможно в силу максимальности длины слова x, а сокращение на стыке слов u_1 и v невозможно, так последний символ слова u_1 совпадает с последним символом слова u. Следовательно, слова u и $v_1^{-1}u_1v$ совпадают графически, но это, в свою очередь, невозможно, так как в силу непустоты слова v_1 слово $v_1^{-1}u_1v$ не является циклически несократимым.

Таким образом, или $u_1 = 1$ и потому $v = uv_1$, или $v_1 = 1$ и потому $u = vu_1$.

В первом случае равенство $uv = vu$ может быть переписано в виде $uuv_1 = uv_1u$, откуда имеем, очевидно $uv_1 = v_1u$. Так как $l(u) + l(v_1) < l(u) + l(v)$, по индуктивному предположению элементы u и v_1 принадлежат некоторой циклической подгруппе W. Поскольку тогда и элемент $v = uv_1$ принадлежит этой подгруппе, для элементов u и v доказываемое утверждение справедливо.

Второй случай рассматривается совершенно так же. Поэтому индуктивный переход можно считать завершенным, и первое из утверждений предложения тем самым доказано.

Предположим теперь, что V — максимальная циклическая подгруппа группы F. Подгруппа V содержится в своем централизаторе, так как она абелева. С другой стороны, произвольный элемент u централизатора подгруппы V перестановочен с порождающим v этой подгруппы, и потому в силу доказанного существует циклическая подгруппа W группы F, содержащая элементы u и v. Так как v порождает подгруппу V, имеем включение $V \subseteq W$, откуда ввиду максимальности подгруппы V следует равенство $V = W$. Таким образом $u \in V$, так что все элементы централизатора подгруппы V принадлежат этой подгруппе, и совпадение V с ее централизатором доказано.

1.2.6. Предложение. *Свободная группа $F = F(a_1, a_2, \ldots, a_n)$ является группой с однозначным извлечением корней, т. е. для любых элементов u и v группы F и любого целого числа $m > 0$ из того, что $u^m = v^m$, следует, что $u = v$.*

Для доказательства заметим, прежде всего, что если элементы u и v группы F удовлетворяют равенству $u^m = v^m$, где $m > 0$, и один из этих элементов равен 1, то в силу первого утверждения предложения 1.2.4. равен 1 и другой элемент. Следовательно, можем считать, что элементы u и v отличны от 1.

Далее, поскольку для любого элемента $x \in F$ равенства $u^m = v^m$ и $(x^{-1}ux)^m = (x^{-1}vx)^m$ равносильны, можно, как и выше, без потери общности считать, что хотя бы один из элементов u и v является циклически несократимым. Так как степень элемента группы F является циклически несократимым элементом тогда и только тогда, когда этот элемент циклически несократим, то и другой из элементов u и v циклически несократим. Поэтому, как было отмечено выше, слова u^m и v^m несократимы и $l(u^m) = ml(u)$, $l(v^m) = ml(v)$. Следовательно, равенство $u^m = v^m$ означает графическое совпадение слов u^m и v^m, так что $l(u^m) = l(v^m)$ и потому $l(u) = l(v)$. Поскольку начальное подслово длины $l(u)$ слова u^m равно слову u и начальное подслово длины $l(v)$ слова v^m равно слову v имеем $u = v$, что и требовалось.

Из предложения 1.2.6 легко следует

1.2.7. Предложение. *Для любых элементов u и v свободной группы $F = F(a_1, a_2, \ldots, a_n)$ из того, что $u^k v^l = v^l u^k$ для некоторых ненулевых целых чисел k и l, следует, что $uv = vu$.*

В самом деле, переписав равенство $u^k v^l = v^l u^k$ в виде $u^k = (v^l u v^{-l})^k$, в силу предложения 1.2.6 будем иметь равенство $u = v^l u v^{-l}$. Поскольку его, в свою очередь, можно переписать в виде $v^l = (u^{-1} v u)^l$, получаем аналогично $v = u^{-1} v u$, что равносильно равенству $uv = vu$.

1.3. Абстрактное понятие свободной группы До сих пор свободными группами мы называли построенные выше конкретные группы $F(a_1, a_2, \ldots, a_n)$, элементами которых являются классы свободно равных слов в соответствующем алфавите. Абстрактное понятие свободной группы формулируется следующим естественным образом:

Группа G называется *свободной*, если она изоморфна некоторой группе $F(a_1, a_2, \ldots, a_n)$, т. е., говоря подробнее, если для некоторого алфавита

$\{a_1, a_2, \ldots, a_n\}$ существует изоморфизм группы $F(a_1, a_2, \ldots, a_n)$ на группу G.

Поскольку группа $F = F(a_1, a_2, \ldots, a_n)$ порождается элементами a_1, a_2, …, a_n (предложение 1.2.1), то в случае существования изоморфизма φ группы F на группу G группа G порождается элементами $g_1, g_2, \ldots, g_n$, где $g_i = a_i\varphi$ для $i = 1, 2, \ldots, n$. Эти элементы группы G естественно называть ее *свободными порождающими* и более развернутое определение свободной группы формулировать так:

Пусть G — некоторая группа, порождаемая элементами $g_1, g_2, \ldots, g_n$. Группа G называется *свободной группой с множеством* (*или системой*) *свободных порождающих* $g_1, g_2, \ldots, g_n$, если существует изоморфизм φ группы $F = F(a_1, a_2, \ldots, a_n)$ (в алфавите той же мощности, что и указанное множество порождающих группы G) на группу G такой, что $a_i\varphi = g_i$ для любого $i = 1, 2, \ldots, n$.

Полезно располагать "внутренним" по отношению к группе G определением понятия свободной группы. Оказывается, таким определением может служить любое из свойств, выражаемых следствием 1.1.4 и теоремой 1.2.2. Для соответствующих формулировок предварительно договоримся о следующем.

Напомним, что если группа G порождается элементами $g_1, g_2, \ldots, g_n$, то произвольный элемент g этой группы может быть выражен в виде произведения, каждый сомножитель которого равен одному из этих порождающих или элементу, обратному к порождающему, т. е. $g = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_r}^{\varepsilon_r}$, где $\varepsilon_j = \pm 1$ для каждого $j = 1, 2, \ldots, r$. Такое произведение будем называть *несократимым*, если в нем любые соседние сомножители не являются взаимно обратными, т. е. при $r > 1$ для любого j, $1 \leqslant j < r$, из того, что $\varepsilon_j + \varepsilon_{j+1} = 0$, следует, что $i_j \neq i_{j+1}$.

1.3.1. Теорема. *Для произвольной группы G с порождающими элементами g_1, g_2, …, g_n следующие утверждения попарно равносильны:*

(1) *Группа G является свободной с множеством свободных порождающих g_1, g_2, …, g_n.*

(2) *Для любой группы H и любого отображения τ в группу H множества порождающих $\{g_1, g_2, \ldots, g_n\}$ существует гомоморфизм $\rho : G \to H$ такой, что $g_i\rho = g_i\tau$ для любого $i = 1, 2, \ldots, n$;*

(3) *любое несократимое произведение, составленное из элементов g_1,*

g_2, …, g_n и содержащее хотя бы один сомножитель, является неединичным элементом группы G.

Доказательство. Покажем сначала, что из утверждения (1) следует (2). Если группа G является свободной с множеством свободных порождающих g_1, g_2, …, g_n, то в соответствии с определением существует изоморфизм φ группы $F = F(a_1, a_2, \ldots, a_n)$ на группу G такой, что $a_i\varphi = g_i$ для любого $i = 1, 2, \ldots, n$. Кроме того, в силу теоремы 1.2.2, для отображения τ множества $\{g_1, g_2, \ldots, g_n\}$ в группу H существует гомоморфизм ψ группы F в группу H такой, что для любого $i = 1, 2, \ldots, n$ выполнено равенство $a_i\psi = g_i\tau$. Очевидно, что отображение $\rho = \varphi^{-1}\psi$ является искомым гомоморфизмом группы G в группу H.

Предположим теперь утверждение (2) выполненным и покажем, что тогда выполнено и утверждение (3). Пусть $g = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_r}^{\varepsilon_r}$ — несократимое произведение, составленное из элементов g_1, g_2, …, g_n, причем $r \geqslant 1$. В силу утверждения 2 существует гомоморфизм ρ группы G в группу $F(a_1, a_2, \ldots, a_n)$ такой, что $g_i\rho = a_i$ для любого $i = 1, 2, \ldots, n$. Поскольку тогда образ $g\rho$ элемента g совпадает, очевидно, со словом $a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$, которое непусто и несократимо, в силу следствия 1.1.4 имеем $g\rho \neq 1$, и потому $g \neq 1$.

Покажем, наконец, что из утверждения (3) следует (1). Для этого мы должны показать, что если в группе G утверждение (3) выполнено, то существует изоморфизм φ группы $F = F(a_1, a_2, \ldots, a_n)$ на группу G такой, что $a_i\varphi = g_i$ для любого $i = 1, 2, \ldots, n$. Из теоремы 1.2.2 следует существование гомоморфизма φ группы F в группу G такого, что $a_i\varphi = g_i$ для любого $i = 1, 2, \ldots, n$. Поскольку элементы g_1, g_2, …, g_n порождают группу G, отображение φ сюръективно. Для доказательства его инъективности достаточно показать, что ядро этого гомоморфизма совпадает с единичной подгруппой группы F. Действительно, произвольный неединичный элемент группы F представим непустым несократимым словом вида $u = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$. Так как его образ $u\varphi = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_r}^{\varepsilon_r}$ является несократимым произведением с положительным числом сомножителей, в силу условия 3 $u\varphi \neq 1$ и потому u не входит в ядро гомоморфизма φ. Следовательно, отображение φ биективно, т. е. является изоморфизмом. Доказательство теоремы 1.3.1 закончено.

Для иллюстрации применения этой теоремы докажем следующее хорошо известное (см., напр., [3, стр.133]) утверждение:

1.3.2. Предложение. *Подгруппа G группы $GL_2(\mathbb{Z})$, порождаемая матрицами $a = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ и $b = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$, где $m \geqslant 2$ — некоторое целое число, является свободной группой с множеством свободных порождающих a, b.*

Доказательство. В силу теоремы 1.3.1 достаточно показать, что любое несократимое произведение w, составленное из элементов a, b и содержащее хотя бы один сомножитель, является неединичным элементом группы G.

Сгруппировав стоящие подряд сомножители вида $a^{\pm 1}$ или вида $b^{\pm 1}$, получим запись элемента w в виде произведения чередующихся степеней с ненулевыми показателями элементов a и b. При этом, если в записи w участвуют оба элемента a и b, переходя, если нужно к подходящей циклической перестановке, можем считать, что первым сомножителем этой записи является степень элемента a. (Напомним, что если элемент g некоторой группы записан в виде $g = xy$, то его циклическая перестановка yx является элементом, сопряженным с g, а сопряженные элементы равны или не равны единице одновременно.)

Таким образом, будем считать, что либо $w = a^k$, либо $w = b^k$ (где $k \neq 0$), либо запись элемента w имеет вид

$$w = u_1^{k_1} u_2^{k_2} \cdots u_r^{k_r},$$

где $r > 1$, k_1, k_2, …, k_r — ненулевые целые числа и для любого $i = 1, 2, \ldots r$ $u_i = a$, если i нечетно, и $u_i = b$, если i четно.

В двух первых случаях требуемое утверждение очевидно, так как матрицы $a^k = \begin{pmatrix} 1 & mk \\ 0 & 1 \end{pmatrix}$ и $b^k = \begin{pmatrix} 1 & 0 \\ mk & 1 \end{pmatrix}$ отличны от единичной.

Для рассмотрения основного случая введем последовательность целых чисел x_1, x_2, …, x_r, которая строится следующим образом:

Полагаем $x_1 = 1$, $x_2 = mk$, и если для некоторого $n \geqslant 3$ числа x_1, x_2, …, x_{n-1} уже определены, полагаем $x_n = x_{n-2} + mk_{n-1}x_{n-1}$.

Пусть еще для каждого $n = 1, 2, \ldots r$ $w_n = u_1^{k_1} u_2^{k_2} \cdots u_n^{k_n}$. Утверждается, что для любого $n = 1, 2, \ldots r$ первая строка матрицы w_n имеет вид

$$\begin{aligned} &(x_n \ x_{n+1}), \quad \text{если } n \text{ нечетное,} \\ &(x_{n+1} \ x_n), \quad \text{если } n \text{ четное.} \end{aligned}$$

.

Действительно, при $n = 1$ это очевидно. Предположим, что для некоторого $n < r$ это справедливо. Тогда при n нечетном первая строка матрицы $w_{n+1} = w_n b^{k_{n+1}}$ есть

$$(x_n \ x_{n+1}) \begin{pmatrix} 1 & 0 \\ mk_{n+1} & 1 \end{pmatrix} = (x_n + mk_{n+1}x_{n+1} \ x_{n+1}) = (x_{n+2} \ x_{n+1}),$$

а при n четном первая строка матрицы $w_{n+1} = w_n a^{k_{n+1}}$ есть

$$(x_{n+1} \ x_n) \begin{pmatrix} 1 & mk_{n+1} \\ 0 & 1 \end{pmatrix} = (x_{n+1} \ x_n + mk_{n+1}x_{n+1}) = (x_{n+1} \ x_{n+2}).$$

Доказательство неединичности матрицы завершается утверждением, что для любого номера $i = 1, 2, \dots r-1$ выполняется неравенство $|x_{i+1}| > |x_i|$.

В самом деле, при $i = 1$ это очевидно, и если для некоторого $i < r-1$ неравенство $|x_{i+1}| > |x_i|$ справедливо, то

$$\begin{aligned} |x_{i+2}| = |x_i + mk_{i+1}x_{i+1}| &\geqslant |mk_{i+1}x_{i+1}| - |x_i| \\ &\geqslant 2|x_{i+1}| - |x_i| = |x_{i+1}| + |x_{i+1}| + (x_{i+1}| - |x_i|) > |x_{i+1}|. \end{aligned}$$

Рассмотрим еще один пример доказательства того, что некоторая группа является свободной.

1.3.3. Предложение. *Пусть F — свободная группа с множеством свободных порождающих a, b. Подгруппа H группы F, порождаемая семейством элементов $c_i = a^{-i}ba^i$, где i — произвольное целое число, является свободной группой, свободно порождаемой этим семейством.*

В силу теоремы 1.3.1 для доказательства этого достаточно показать, что любое несократимое произведение $f = c_{i_1}^{\varepsilon_1} c_{i_2}^{\varepsilon_2} \dots c_{i_r}^{\varepsilon_r}$ (где $r \geqslant 1$), является неединичным элементом группы F. Для этого воспользуемся критерием неединичности элементов этой группы (следствие 1.1.4).

После замены каждого сомножителя этого произведения его выражением через порождающие a и b получится слово

$$(a^{-i_1}b^{\varepsilon_1}a^{i_1})(a^{-i_2}b^{\varepsilon_2}a^{i_2}) \dots (a^{-i_r}b^{\varepsilon_r}a^{i_r})$$

от этих порождающих, представляющее элемент f. Поскольку элементы a и b порождают группу F свободно, для доказательства неединичности элемента f достаточно показать, что свободно равное этому слову несократимое слово не может быть пустым. Для этого придется доказывать более точное утверждение:

Лемма. *Несократимое слово от порождающих a, b, свободно равное элементу*

$$f = c_{i_1}^{\varepsilon_1} c_{i_2}^{\varepsilon_2} \dots c_{i_r}^{\varepsilon_r}$$

(где $\varepsilon_j = \pm 1$ для каждого $j = 1, 2, \dots, r$ и при $r > 1$ для любого j, $1 \leqslant j < r$, из того, что $\varepsilon_j + \varepsilon_{j+1} = 0$, следует, что $i_j \neq i_{j+1}$), начинается с подслова вида $a^{-i_1} b^{\varepsilon_1}$ (и потому непусто).

Для доказательства леммы воспользуемся индукцией по числу r сомножителей произведения f. При $r = 1$ ее утверждение очевидно, поскольку слово $c_{i_1}^{\varepsilon_1} = a^{-i_1} b^{\varepsilon_1} a^{i_1}$ несократимо.

Пусть $r > 1$ и пусть для любых несократимых произведений, составленных из элементов $c_i = a^{-i} b a^i$, число сомножителей в которых меньше r, утверждение леммы справедливо. Так как произведение $f' = c_{i_2}^{\varepsilon_2} \dots c_{i_r}^{\varepsilon_r}$ несократимо и состоит из $r - 1$ сомножителей, по индуктивному предположению несократимое слово от порождающих a, b, свободно равное элементу f', имеет вид $a^{-i_2} b^{\varepsilon_2} x$ для некоторого слова x. Поэтому элемент $f = c_{i_1}^{\varepsilon_1} f'$ определяется словом $a^{-i_1} b^{\varepsilon_1} a^{i_1} a^{-i_2} b^{\varepsilon_2} x$, которое свободно равно слову $a^{-i_1} b^{\varepsilon_1} a^{i_1 - i_2} b^{\varepsilon_2} x$. Если $i_1 - i_2 \neq 0$, то это слово несократимо и начинается с подслова $a^{-i_1} b^{\varepsilon_1}$. Если же $i_1 = i_2$, то поскольку произведение $f = c_{i_1}^{\varepsilon_1} c_{i_2}^{\varepsilon_2} \dots c_{i_r}^{\varepsilon_r}$ несократимо, мы должны иметь $\varepsilon_1 = \varepsilon_2$, и потому слово $a^{-i_1} b^{2\varepsilon_1} x$ также несократимо и начинается с подслова $a^{-i_1} b^{\varepsilon_1}$.

Индуктивный переход завершен, и лемма доказана. Как отмечено выше, тем самым закончено доказательство предложения 1.3.3.

Условие 3 теоремы 1.3.1 используется и в доказательстве (разумеется, более сложном) классической теоремы Нильсена – Шрайера о подгруппах свободной группы (см., напр., [1]):

1.3.4. Теорема. *Каждая подгруппа свободной группы является свободной группой.*

Очевидно, что в соответствии с принятым выше общим определением система $a_1, a_2, \dots, a_n$ порождающих свободной группы $F(a_1, a_2, \dots, a_n)$ является системой ее свободных порождающих. Легко видеть, что группа $F(a_1, a_2, \dots, a_n)$ (а потому и любая свободная группа) обладает и другими системами свободных порождающих; в действительности, множество различных систем свободных порождающих этой группы (при

$n > 1$) бесконечно. Например, с помощью теоремы 1.3.1 нетрудно понять, что для любого целого числа k множество $a_1a_2^k, a_2, \ldots, a_n$ свободно порождает группу $F(a_1, a_2, \ldots, a_n)$. Тем не менее, справедливо

1.3.5. Предложение. *Любые два множества свободных порождающих свободной группы F имеют одну и ту же мощность.*

В самом деле, если группа F обладает бесконечным несчетным множеством A свободных порождающих, это следует из того, что мощность множества всевозможных конечных последовательностей, составленных из элементов бесконечного множества A, совпадает с мощностью A.

Остается показать, что предположение о существовании в группе F двух множеств свободных порождающих, одно из которых конечно и состоит из m элементов, а другое либо тоже конечно конечно и состоит из n элементов, где $n > m$, либо является счетным, приводит к противоречию. В силу теоремы 1.2.2 для получения противоречия достаточно располагать примером группы, которая порождается множеством, состоящим из n элементов, и не может быть порождена никаким своим подмножеством с меньшим числом элементов. Легко видеть, что такой группой является аддитивная группа n-мерного линейного пространства над полем $\mathbb{Z}_2$.

Предложение 1.3.5 позволяет ввести следующее понятие:

Мощность множества свободных порождающих свободной группы F называется *рангом* этой группы.

Таким образом, свободная группа ранга 1 является бесконечной циклической группой. Легко понять, что свободная группа ранга $r > 1$ не является абелевой и потому не является циклической. В ряде случаев полезно считать (для удобства формулировок) единичную группу свободной группой ранга 0 (с пустым множеством свободных порождающих).

Из предложения 1.3.3 следует, очевидно,

1.3.6. Предложение. *Свободная группа любого конечного или счетного ранга изоморфно вложима в свободную группу ранга 2.*

§ 2. Задание группы порождающими и определяющими соотношениями

2.1. Свободное представление группы. Задание группы порождающими и определяющими словами. Этот раздел начнем с формулировки практически очевидного следствия теоремы 1.2.2:

2.1.1. Предложение. *Любая группа изоморфна фактор-группе некоторой свободной группы.*

В самом деле, если G — группа, g_1, g_2, …, g_n — некоторое множество порождающих этой группы (где n, как и выше, может быть любым ординальным числом) и $F = F(a_1, a_2, \ldots, a_n)$ — свободная группа на алфавите с тем же числом символов, то в силу теоремы 1.2.2 существует гомоморфизм φ группы F в группу G такой, что для любого $i = 1, 2, \ldots, n$ выполнено равенство $a_i\varphi = g_i$. Так как элементы g_1, $g_2, \ldots$, g_n порождают группу G, гомоморфизм φ сюръективен, и потому группа G изоморфна фактор-группе F/N, где N — ядро гомоморфизма φ.

Фактор-группа F/N свободной группы F, изоморфная группе G, называется *свободным представлением группы* G. В силу предложения 2.1.1 каждая группа обладает свободным представлением. Очевидно также, что любая фактор-группа произвольной свободной группы является свободным представлением некоторой группы (например, — самой этой фактор-группы).

Поскольку группа своим свободным представлением определяется однозначно, его можно считать заданием этой группы. Говоря более подробно, для задания таким способом группы G следует фиксировать подходящий алфавит $\{a_1, a_2, \ldots, a_n\}$ и перечислить (в некотором смысле) все элементы нормальной подгруппы N группы $F = F(a_1, a_2, \ldots, a_n)$, фактор-группа F/N группы F по которой изоморфна группе G. Один из способов перечисления элементов подгруппы N основан на следующем понятии.

Пусть G —некоторая группа и M — подмножество группы G. *Нормальным замыканием подмножества M в группе G* называется наименьшая нормальная подгруппа группы G, содержащая все элементы из M. Эту подгруппу будем обозначать символом M^G. Более подробно, определение подгруппы M^G состоит из трех условий: M^G является нормальной подгруппой группы G; $M \subseteq M^G$; для любой нормальной подгруппы N группы G из включения $M \subseteq N$ следует включение

$M^G \subseteq N$. Равносильное определение, делающее очевидным существование нормального замыкания, состоит в том, что подгруппа M^G является пересечением всех нормальных подгрупп группы G, содержащих подмножество M.

Возвращаясь к определяющему группу G свободному представлению F/N, мы видим, что для описания подгруппы N достаточно указать в группе F множество элементов R, нормальным замыканием которого подгруппа N является. Следовательно, фактор-группу F/N можно описать следующим формальным выражением

$$\langle a_1, a_2, \ldots, a_n;\ R\rangle, \tag{1}$$

составленным из некоторого алфавита и некоторого множества слов в этом алфавите. Таким образом, мы приходим к следующему определению:

Выражение (1) называется *заданием или представлением группы G порождающими и определяющими словами*, если группа G изоморфна фактор-группе F/R^F группы $F = F(a_1, a_2, \ldots, a_n)$ по нормальному замыканию R^F множества R в группе F.

Для обозначения этого мы записываем $G = \langle a_1, a_2, \ldots, a_n;\ R\rangle$, алфавитные символы $a_1, a_2, \ldots, a_n$ называем *порождающими символами группы G*, а слова множества R — *определяющими словами группы G*. Легко видеть, что группа является свободной тогда и только тогда, когда она может быть задана представлением с пустым множеством определяющих слов.

Одной из групп, заданных представлением (1), т. е. изоморфных фактор-группе F/N, где $N = R^F$, является сама эта фактор-группа. Рассмотрим устройство этой группы более подробно.

По определению элементами фактор-группы F/N являются различные смежные классы $uN = \big\{ux \bigm| x \in N\big\}$, где $u \in F$. Так как элемент группы F, обозначаемый через u, является, напомним, классом слов $[u] = \big\{w \bigm| w \approx u\big\}$, свободно равных слову u, и, аналогично, каждый элемент $x \in N$ обозначает класс слов $[x] = \big\{y \bigm| y \approx x\big\}$, свободно равных слову x, то множество слов в алфавите $\{a_1, a_2, \ldots, a_n\}$, представляющих все элементы смежного класса uN, совпадает с множеством

$$\bigcup([u] \cdot [x]) = \bigcup [ux],$$

где x пробегает по всем представителям элементов подгруппы N.

Легко видеть, что совокупность всех таких подмножеств составляют *разбиение* множества W всех слов в алфавите $\{a_1, a_2, \ldots, a_n\}$, т. е. множество W является объединением всех попарно непересекающихся подмножеств вида $\bigcup[ux]$. В самом деле, произвольное слово u определяет элемент из смежного класса uN и потому принадлежит подмножеству $\bigcup[ux]$. Если слово v принадлежит подмножествам $\bigcup[u_1x]$ и $\bigcup[u_2x]$ для некоторых u_1 и u_2, то оно определяет общий элемент смежных классов u_1N и u_2N, откуда следует, что $u_1N = u_2N$ и потому $\bigcup[u_1x] = \bigcup[u_2x]$.

Как обычно, этому разбиению соответствует некоторое отношение эквивалентности. Получение явного описания этого отношения начнем с простого замечания общего характера.

2.1.2. Предложение. *Пусть G —некоторая группа и M — подмножество группы G. Нормальное замыкание M^G подмножества M в группе G совпадает с подгруппой, порождаемой всевозможными элементами вида $x^{-1}yx$, где $x \in G$ и $y \in M$.*

В самом деле, подгруппа, порожденная указанными элементами, является. как легко видеть, нормальной, содержит, очевидно. подмножество M и лежит в каждой нормальной подгруппе, содержащей M

Расширим список элементарных преобразований слов, добавив к свободным преобразованиям вставки и вычеркивания подслов вида r^ε, где $r \in R$ и $\varepsilon = \pm 1$. Отметим, что последовательность

$$xy,\ xrr^{-1}y,\ xr^{-1}y$$

показывает, что вставку или вычеркивание слова r^{-1} можно осуществить последовательностью, составленной из подходящих свободных элементарных преобразований и вычеркивания или вставки слова r.

Искомое отношение эквивалентности может быть описано следующим образом:

2.1.3. Предложение. *Слова u и v в алфавите $\{a_1, a_2, \ldots, a_n\}$ представляют один и тот же элемент группы F/N тогда и только тогда, когда существует переводящая слово u в слово v последовательность элементарных преобразований, состоящая из свободных элементарных преобразований и вставок или вычеркиваний подслов вида r^ε, где $r \in R$ и $\varepsilon = \pm 1$.*

Для доказательства части “тогда” этого утверждения достаточно заметить, что если слово v получается из u единственным элементарным преобразованием, то $uN = vN$. Это очевидно, если элементарное преобразование является свободным. Пусть $u = xr^{\varepsilon}y$ и $v = xy$ для некоторых слов x и y, элемента $r \in R$ и $\varepsilon = \pm 1$. Тогда $u = xr^{\varepsilon}y \equiv xy = v \pmod N$.

Обратно, если $uN = vN$, то $u = vw$ для некоторого слова w, определяющего элемент из подгруппы N. Из предложения 2.1.2 следует, что

$$w = (x_1^{-1} r_1^{\varepsilon_1} x_1)(x_2^{-1} r_2^{\varepsilon_2} x_2) \cdots (x_k^{-1} r_k^{\varepsilon_k} x_k)$$

для некоторых элементов $r_1, r_2, \ldots, r_k \in R$, $x_1, x_2, \ldots, x_k \in F$ и показателей $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_k$, равных ± 1. Поэтому v получается из u последовательностью элементарных вычеркиваний и свободных сокращений.

2.2. Задание группы порождающими и определяющими соотношениями. В силу предложения 2.1.3 элементами группы $F/N = \langle a_1, a_2, \ldots, a_n;\ R \rangle$ можно считать классы эквивалентных слов, соответствующие отношению эквивалентности, описанному в этом предложении. Как и в случае свободных групп, договоримся обозначать такой класс любым представляющим его словом. Тогда для любых слов u и v равенство $u = v$ элементов u и v группы F/N означает, что одно из этих слов получается из другого некоторой последовательностью элементарных преобразований, состоящей из свободных элементарных преобразований и вставок или вычеркиваний подслов вида r^{ε}, где $r \in R$ и $\varepsilon = \pm 1$.

Это равенство элементов u и v называется *соотношением*, выполненным в группе F/N или *выводимым* из определяющих слов ее представления. Если в группе F/N выводимо соотношение $u = 1$, то слово u называется *выводимым из множества слов R*.

Очевидно, что для любого слова $r \in R$ в группе F/N выполнено соотношение $r = 1$. Элементарные преобразования вставки и вычеркивания слова r можно рассматривать как замену правой или левой части этого соотношения на соответственно левую или правую часть. В более общей ситуации, когда слово r имеет вид $r = uv^{-1}$ для некоторых слов u и v, последовательность $u, uv^{-1}v = rv, v$ доказывает справедливость соотношения $u = v$. А последовательность

$$r = uv^{-1},\ vv^{-1},\ 1$$

показывает, что если в список элементарных преобразований слов добавить замену одной из частей соотношения другой его частью, то этими и свободными преобразованиями можно осуществить вставку и вычеркивание слова r.

Таким образом, если каждое слово $r \in R$ заменить соотношением вида $r = 1$ или $u = v$ (если $r = uv^{-1}$), то из полученной системы $\mathcal{R}$ соотношений будут выводимы (с помощью только что еще раз расширенной системы элементарных преобразований) все те и только те соотношения, которые выводимы из множества определяющих слов R. Поэтому систему $\mathcal{R}$ естественно называть *системой определяющих соотношений группы* $F/N = \langle a_1, a_2, \ldots, a_n;\ R\rangle$ и задавать эту группу также представлением вида

$$\langle a_1, a_2, \ldots, a_n;\ \mathcal{R}\rangle, \tag{2}$$

называемом *представлением порождающими и определяющими соотношениями.*

Например, группа $G = \langle a, b;\ a^2b^2\rangle$, заданная представлением с двумя порождающими и одним определяющим словом, может быть задана также представлением $\langle a, b;\ a^2b^2 = 1\rangle$ и представлением $\langle a, b;\ a^2 = b^{-2}\rangle$. Выбор для задания группы представления вида (1) или вида (2) определяется лишь соображениями удобства в данной конкретной ситуации. При этом, могут использоваться также представления, в которых участвуют и определяющие слова, и определяющие соотношения.

2.3. Вычисление представления группы порождающими и определяющими словами (определяющими соотношениями). Как уже было сказано выше, некоторую группу G будем называть *заданной представлением* (1), если она изоморфна соответствующей фактор-группе $F/N = \langle a_1, a_2, \ldots, a_n;\ R\rangle$. С учетом принятого в разделе 2.2 соглашения,как и в случае свободных групп, элементы a_1, a_2, ..., a_n составляют систему порождающих группы F/N. Поэтому при любом изоморфизме φ группы F/N на группу G образы $g_1 = a_1\varphi$, $g_2 = a_2\varphi$, ..., $g_n = a_n\varphi$ этих элементов составляют систему порождающих группы G, и в этом случае говорят, более подробно, что группа G *задается представлением* (1) *в системе порождающих* g_1, g_2, ..., g_n.

Нахождение представления группы в некоторой системе ее порождающих является весьма нетривиальной задачей, а если ее удается решить, то возникает задача с помощью найденного представления ответить на вопросы о строении группы (для чего это представление и вычислялось). С другой стороны, довольно часто группа так и возникает, как заданная некоторым представлением, и в этом случае это представление является единственным источником информации о строении и свойствах такой группы.

При решении этих задач весьма полезным является следующий критерий существования гомоморфизма группы F/N в некоторую группу, действующего на порождающих элементах F/N наперед заданным образом. Для его формулировки напомним понятие, введенное при доказательстве теоремы 1.2.2.

Произвольное отображение $\tau\colon A \to H$ множества

$$A = \{a_1, a_2, \ldots, a_n\}$$

алфавитных символов в некоторую группу H естественным образом продолжаемо до (обозначаемого тем же символом τ) отображения в эту группу множества $W(A)$ всех слов в алфавите A. А именно, если для каждого $i = 1, 2, \ldots, n$ $h_i = a_i\tau$ — элемент группы H, являющийся образом относительно τ символа a_i, то для любого непустого слова $u = a_{i_1}^{\varepsilon_1} a_{i_2}^{\varepsilon_2} \ldots a_{i_r}^{\varepsilon_r}$ полагаем

$$u\tau = g_{i_1}^{\varepsilon_1} g_{i_2}^{\varepsilon_2} \ldots g_{i_r}^{\varepsilon_r}$$

(где в выражении, стоящем справа от знака равенства, выполняются операции умножения и взятия обратного в группе H), а образом пустого слова считаем единицу группы H. Элемент $u\tau$ группы H будем называть *значением слова u при отображении τ*.

2.3.1. Теорема. *Пусть группа $F/N = \langle a_1, a_2, \ldots, a_n;\ R\rangle$ задана представлением с порождающими символами $a_1, a_2, \ldots, a_n$ и множеством R определяющих слов. Если при отображении τ множества порождающих символов этого представления в некоторую группу H значение каждого слова $r \in R$ равно единице, то существует гомоморфизм φ группы G в группу H такой, что для любого $i = 1, 2, \ldots, n$ образ относительно φ элемента a_i группы G совпадает с образом символа a_i относительно τ.*

Доказательство. Напомним, что группа F/N является фактор-группой группы $F = F(a_1, a_2, \ldots, a_n)$ по нормальному замыканию $N = R^F$ множества R в группе F. По теореме 1.2.2 существует гомоморфизм ψ группы F в группу H такой, что для любого $i = 1, 2, \ldots, n$ выполнено равенство $a_i\psi = a_i\tau$. При этом, образ любого элемента $u \in F$ относительно гомоморфизма ψ совпадает со значением слова u при отображении τ. Так как значение при отображении τ каждого слова $r \in R$ равно единице, отсюда с учетом предложения 2.1.2 вытекает, что подгруппа N лежит в ядре гомоморфизма ψ. Поэтому отображение φ группы $G = F/N$ в группу H, действующее по правилу $(uN)\varphi = u\psi$ $(u \in F)$, определено корректно и является гомоморфизмом. Поскольку элемент группы F/N, определяемый символом a_i, совпадает (в силу принятого соглашения) со смежным классом a_iN. гомоморфизм φ является искомым.

Для случая, когда группа задается представлением порождающими и определяющими соотношениями, теорема 2.3.1 должна быть переформулирована в следующем (очевидно, равносильном) виде:

2.3.2. Следствие. *Пусть группа $F/N = \langle a_1, a_2, \ldots, a_n;\ \mathcal{R}\rangle$ задана представлением с порождающими символами $a_1, a_2, \ldots, a_n$ и множеством $\mathcal{R}$ определяющих соотношений. Если при отображении τ множества порождающих этого представления в некоторую группу H у каждого соотношения из $\mathcal{R}$ значения левой и правой частей совпадают, то существует гомоморфизм φ группы G в группу H такой, что для любого $i = 1, 2, \ldots, n$ образ относительно φ элемента a_i группы G совпадает с образом символа a_i относительно τ.*

Очевидна также формулировка следствия из теоремы 2.3.1 применительно к представлениям, в которых участвуют и определяющие слова, и определяющие соотношения. Разумеется, эти утверждения применимы к любой группе, заданной представлением порождающими и определяющими словами (соотношениями).

Рассмотрим несколько примеров решения задач, упомянутых выше типов.

Пример 1. *Показать, что группа $G = \langle a;\ a^n = 1\rangle$ (т. е. группа, заданная представлением с единственным порождающим символом и единственным определяющим соотношением), где $n \geqslant 2$ — целое число, является циклической группой порядка n.*

Решение. Как было отмечено выше, группа G порождается элементом a и потому является циклической. Поскольку в этой группе выполнено соотношение $a^n = 1$, порядок элемента a не превосходит числа n. Так как порядок циклической группы совпадает с порядком порождающего ее элемента, остается показать, что порядок элемента a равен числу n. Это означает, что для любого положительного числа $m < n$ равенство $a^m = 1$ в группе G не выполняется, т. е. слово a^m не эквивалентно пустому слову.

Однако, распознавание того, существует или нет последовательность элементарных преобразований, переводящая одно слово в другое, является весьма нетривиальной задачей даже в случае такого простого представления. Вместо этого мы воспользуемся теоремой 2.3.1 (точнее, — следствием 2.3.2), для чего нам понадобится конкретная циклическая группа порядка n.

Такой группой является, например, группа $\mathbb{C}_n$ комплексных корней из 1 степени n. Хорошо известно, что ее порядок равен числу n и что она порождается элементом $z = \cos(2\pi/n) + i\sin(2\pi/n)$.

Зададим отображение τ множества $\{a\}$ порождающих символов из представления группы G в группу $\mathbb{C}_n$, полагая $a\tau = z$. Так как для любого целого числа m значением при отображении τ слова a^m является элемент z^m группы $\mathbb{C}_n$ и так как $z^n = 1$, то значения левой и правой частей определяющего соотношения $a^n = 1$ группы G равны. Поэтому в силу следствия 2.3.2 существует гомоморфизм φ группы G в группу $\mathbb{C}_n$ такой, что $a\varphi = z$. Так как для любого целого числа m элемент a^m при этом гомоморфизме переходит в элемент z^m, предположение о том, что для некоторого положительного числа $m < n$ в группе G выполнено равенство $a^m = 1$, приводит к равенству $z^m = 1$, что невозможно, поскольку порядок элемента z равен n.

Таким образом, порядок элемента a равен n, и утверждение о том, что группа G является циклической порядка n, доказано.

Пример 2. *Показать, что в группе $G = \langle a, b;\ a^{-1}ba = b^2 \rangle$ элементы a и b имеют бесконечный порядок.*

Решение. Зададим отображение τ множества $\{a, b\}$ порождающих символов из представления группы G в аддитивную группу группу $\mathbb{Z}$ целых чисел по правилу $a \mapsto 1$, $b \mapsto 0$. Так как тогда (с учетом аддитивности записи операции группы $\mathbb{Z}$)

$$(a^{-1}ba)\tau = -1 + 0 + 1 = 0$$

и $(b^2)\tau = 0 + 0 = 0$, определяющее соотношение группы G переходит в верное равенство в группе $\mathbb{Z}$. Поэтому в силу следствия 2.3.2 существует гомоморфизм φ группы G в группу $\mathbb{Z}$ такой, что $a\varphi = 1$ и $b\varphi = 0$.

Так как при гомоморфизме групп элемент конечного порядка переходит в элемент конечного порядка, а порядок элемента 1 группы $\mathbb{Z}$ бесконечен, бесконечность порядка элемента a доказана. Тем не менее, поскольку образом элемента b при гомоморфизме φ является нулевой элемент группы $\mathbb{Z}$, никакой информации о порядке элемента b этот гомоморфизм не дает.

Для доказательства бесконечности порядка элемента b попробуем, поступая аналогично, построить еще один гомоморфизм группы G в подходящую группу.

Рассмотрим для этого группу $GL_2(\mathbb{Q})$ всех обратимых 2×2-матриц над полем $\mathbb{Q}$ рациональных чисел и ее элементы

$$x = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \qquad \text{и} \qquad y = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

Так как для любого целого числа n $y^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix}$, порядок элемента y группы $GL_2(\mathbb{Q})$ бесконечен. Непосредственное вычисление показывает также, что в этой группе выполнено равенство $x^{-1}yx = y^2$. Поэтому в силу теоремы 2.3.1 существует гомоморфизм ψ группы G в группу $GL_2(\mathbb{Q})$, при котором элемент a переходит в x и элемент b переходит в y, что и доказывает бесконечность порядка элемента b. Очевидно, что из существования гомоморфизма ψ следует и бесконечность порядка элемента a.

Пример 3. Показать, что группа $G = \langle a, b;\ a^3, b^2, ab = ba^2 \rangle$ имеет порядок 6 и изоморфна группе S_3 подстановок 3-й степени.

Решение. Рассмотрим элементы $\alpha = (123)$ и $\beta = (12)$ группы S_3. Пусть также ι обозначает тождественную подстановку, т. е. — единицу этой группы. Непосредственно проверяется, что в группе S_3 выполнены равенства

$$\alpha^3 = \iota, \quad \beta^2 = \iota \quad \text{и} \quad \alpha\beta = \beta\alpha^2.$$

Поэтому в силу теоремы 2.3.1 существует гомоморфизм φ группы G в группу S_3 такой, что $a\varphi = \alpha$ и $b\varphi = \beta$.

Заметим, далее, что подстановки α и β порождают группу S_3. Действительно, так как $\alpha\beta\alpha^{-1} = (13)$ и $(12)(13)(12) = (23)$, подгруппе, порожденной подстановками α и β, принадлежат все транспозиции, а поскольку произвольная подстановка из S_3 раскладывается в произведение транспозиций, в этой подгруппе лежат все элементы группы S_3.

Из этого замечания следует, что гомоморфизм φ является сюръективным, и потому группа G должна содержать не менее шести элементов.

С другой стороны, мы покажем сейчас, что группа G не может иметь более шести элементов. Отметим сразу же, что тем самым будет доказано, что порядок группы G равен 6 и что отображение φ является изоморфизмом группы G на группу S_3 (поскольку всякое отображение конечного множества в любое множество с тем же числом элементов инъективно тогда и только тогда, когда оно сюръективно).

Отметим, прежде всего, что для любого целого числа n в группе Q выполнено соотношение $a^n b = ba^{2n}$. В самом деле, определяющее соотношение $ab = ba^2$ равносильно соотношению $b^{-1}ab = a^2$, возведя обе части которого в n-ю степень, получаем соотношение $b^{-1}a^n b = a^{2n}$, равносильное, в свою очередь, соотношению $a^n b = ba^{2n}$.

Покажем теперь, что произвольное слово w от порождающих символов a и b группы G эквивалентно слову вида $b^k a^l$, где k и l — некоторые неотрицательные целые числа. Для этого заметим сначала, что слово w эквивалентно слову, не содержащему вхождений символов a^{-1} и b^{-1}. Действительно, если $w = xa^{-1}y$ для некоторых слов x и y, то вставив после символа a^{-1} определяющее слово a^3 и вычеркнув тривиальное слово $a^{-1}a$, получим слово xa^2y, эквивалентное слову w и содержащее на один символ с отрицательным показателем степени меньше, чем у w. Аналогично, используя определяющее слово b^2, можно заменить вхождение символа b^{-1} на вхождение символа b. Очевидно, что конечная последовательность таких элементарных преобразований переведет слово w в эквивалентное ему слово без символов с отрицательным показателем.

Доказанное только что утверждение позволяет без потери общности предполагать, что наше исходное слово w не содержит вхождений символов a^{-1} и b^{-1}. Существование слова вида $b^k a^l$, эквивалентного слову w, будем доказывать индукцией по числу вхождений в это слово символа b.

Если это число равно нулю, т. е. символ b не входит в запись слова w, то $w = a^n$ для некоторого целого $n \geqslant 0$ и потому имеет требуемый вид при $k = n$ и $l = 0$. Таким образом, мы располагаем основанием индукции.

Предположим теперь, что символ b входит в запись слова w и что произвольное слово с меньшим, чем у w числом вхождений символа b эквивалентно слову требуемого вида. В частности, тогда слово w можно записать в виде $w = a^n bx$ для некоторого целого числа $n \geqslant 0$ и некоторого слова x. Поскольку в группе G выполнено соотношение $a^n b = ba^{2n}$, слово w эквивалентно слову $ba^{2n}x$. Так как число вхождений символа b в слово $a^{2n}x$ на 1 меньше, чем в слово w, по индуктивному предположению слово $a^{2n}x$ эквивалентно слову $b^k a^l$ для некоторых целых k и l. Тогда слово $ba^{2n}x$ эквивалентно слову $bb^k a^l = b^{k+1}a^l$. Таким образом, слово w эквивалентно слову требуемого вида, и индуктивный переход завершен.

Заметим, далее, что замена числа k его остатком от деления на 2 и числа l — его остатком от деления на 3 приводит к слову, эквивалентному слову $b^k a^l$. В самом деле, если $k = 2q + r$ для некоторых целых q и r, причем $0 \leqslant r < 2$, то вычеркнув в слове $b^k a^l$ q подслов b^2, получим слово $b^r a^l$. Аналогично, если $l = 3q_1 + s$ для некоторых целых q_1 и s, причем $0 \leqslant s < 3$, то слово $b^r a^l$ эквивалентно слову $b^r a^s$.

Итак, произвольное слово w от порождающих символов a и b группы G эквивалентно слову вида $b^k a^l$, где k и l — целые числа, удовлетворяющие неравенствам $0 \leqslant k < 2$ и $0 \leqslant l < 3$. Это означает, что в каждый класс эквивалентности входит хотя бы одно из шести слов данного вида. Поскольку различные классы попарно не пересекаются, число классов, т. е число элементов группы G не превосходит шести. Как было отмечено выше, отсюда следуют все утверждения из формулировки задачи.

Очевидно, что утверждение примера 3 равносильно тому, что группа S_3 в системе порождающих α, β может быть задана представлением $\langle a, b;\ a^3, b^2, ab = ba^2 \rangle$.

Пример 4. *Пусть группы A и B заданы представлениями*

$$\langle a_1, a_2, \ldots, a_m;\ R \rangle \quad \text{и} \quad \langle b_1, b_2, \ldots, b_n;\ S \rangle$$

соответственно. Показать, что прямое произведение $D = A \times B$ групп A и B может быть задано представлением

$$\langle a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n;\ R \cup S, \\ a_i b_j = b_j a_i \, (i = 1, 2, \ldots, m;\ j = 1, 2, \ldots, n) \rangle. \quad (3)$$

Решение. Напомним, прежде всего, что в соответствии с (внутренним) определением прямого произведения мы можем считать, что группа D содержит группы A и B в качестве подгрупп, $D = AB$, $A \cap B = 1$ и подгруппы A и B поэлементно перестановочны, т. е. для любых элементов $x \in A$ и $y \in B$ выполнено равенство $xy = yx$. Равенство $D = AB$ означает, что произвольный элемент g группы D представим в виде произведения ab, где $a \in A$ и $b \in B$, а из условия $A \cap B = 1$ следует, что такое представление элемента g является единственным. В частности, для любых элементов $a \in A$ и $b \in B$ равенство $ab = 1$ выполняется в том и только в том случае, когда $a = 1$ и $b = 1$.

Так как по условию группы A и B заданы указанными представлениями, существуют изоморфизмы φ_1 и φ_2 группы $F_1 = \langle a_1, a_2, \ldots, a_m;\ R \rangle$ на группу A и группы $F_2 = \langle b_1, b_2, \ldots, b_n;\ S \rangle$ на группу B (где F_1 и F_2 являются соответственно фактор-группами групп $F(a_1, a_2, \ldots, a_m)$ и

$F(b_1, b_2, \ldots, b_n)$ по нормальным замыканиям соответствующих множеств слов). Поскольку A и B являются подгруппами группы D, отображения φ_1 и φ_2 можно считать гомоморфизмами групп F_1 и F_2 в группу D.

Определим отображение τ множества порождающих символов представления (3) в группу D по следующему правилу:

$$a_i\tau = a_i\varphi_1\,(i = 1, 2, \ldots, m) \quad \text{и} \quad b_j\tau = b_j\varphi_2\,(j = 1, 2, \ldots, n)$$

и, как обычно, продолжим их до отображения соответствующих множеств слов. Так как отображения φ_1 и φ_2 гомоморфны, очевидно, что для любого слова $u = u(a_i)$ его значение $u\tau$ совпадает с $u\varphi_1$ и для любого слова $v = v(b_j)$ его значение $v\tau$ совпадает с $v\varphi_2$. Поскольку при гомоморфизмах групп единица переходит в единицу, отсюда следует, что значение при отображении τ любого слова из множества $R \cup S$ равно единице группы D. Кроме того, так как для любых $i = 1, 2, \ldots, m$ и $j = 1, 2, \ldots, n$ значение $a_i\tau$ слова a_i является элементом подгруппы A группы D и значение $b_j\tau$ слова b_j является элементом ее подгруппы B, из поэлементной перестановочности подгрупп G_1 и G_2 следует, что

$$(a_ib_j)\tau = a_i\tau \cdot b_j\tau = b_j\tau \cdot a_i\tau = (b_ja_i)\tau.$$

Таким образом, при отображении τ все определяющие соотношения из представления (3) переходят в равенства соответствующих элементов группы D. Поэтому из 2.3.2 следует существование такого гомоморфизма φ в группу D группы F, определяемой представлением (3), что $a_i\varphi = a_i\tau$ для любого $i = 1, 2, \ldots, m$ и $b_j\varphi = b_j\tau$ для любого $j = 1, 2, \ldots, n$. Покажем, что гомоморфизм φ в действительности является изоморфизмом.

Так как для любого слова w от порождающих символов представления (3) выполнено равенство $w\varphi = w\tau$, то для любого слова $u = u(a_i)$ имеем $u\varphi = u\tau = u\varphi_1$ и для любого слова $v = v(b_j)$ $v\varphi = v\tau = v\varphi_2$. Следовательно, подгруппы A и B группы D лежат в образе отображения φ, и так как группа D порождается этими подгруппами, она также содержится в образе отображения φ. Это означает сюръективность гомоморфизма φ, и нам остается показать, что ядро этого гомоморфизма совпадает с единичной подгруппой группы F.

Для этого заметим сначала, что (как легко видеть, используя определяющие соотношения $a_ib_j = b_ja_i$) произвольный элемент группы F может быть представлен словом вида uv, где $u = u(a_i)$ и $v = v(b_j)$. Поэтому, в частности, каждый элемент g группы F, принадлежащий ядру гомоморфизма φ, определяется некоторым словом вида uv, где $u = u(a_i)$ и $v = v(b_j)$. Отсюда $g\varphi = u\varphi \cdot v\varphi = u\varphi_1 \cdot v\varphi_2$, причем $u\varphi_1$ и $v\varphi_2$ — элементы группы D, принадлежащие подгруппам A и B соответственно. Так как $g\varphi = 1$, имеем $u\varphi_1 = 1$ и $v\varphi_2 = 1$. Из инъективности отображения φ_1 следует, что слово u определяет единицу группы A и потому соотношение $u = 1$ выводимо из множества R определяющих слов этой группы. Аналогично, соотношение $v = 1$ выводимо из множества S определяющих слов группы B. Поскольку все слова из множеств R и S являются определяющими словами и группы F, в этой группе также выводимы соотношения $u = 1$ и $v = 1$. Следовательно, $g = 1$, и утверждение о том, что ядро гомоморфизма φ совпадает с единичной подгруппой группы F, доказано.

Таким образом, отображение φ действительно является изоморфизмом группы F на группу D, а это и означает, что группа D определяется представлением (3).

2.4. Задание порождающими и определяющими соотношениями фактор-группы данной группы В этом разделе будет показано, как по заданию данной группы порождающими и определяющими соотношениями построить аналогичное задание фактор-группы этой группы. Для этого снова достаточно рассмотреть случай групп вида F/N.

2.4.1. Теорема. *Пусть нормальная подгруппа H группы*

$$F/N = \langle a_1, a_2, \ldots, a_n;\ R \rangle,$$

является нормальным замыканием некоторого множества элементов M и пусть S — множество слов, представляющих все элементы из M. Тогда фактор-группа группы F/N по подгруппе H определяется представлением $\langle a_1, a_2, \ldots, a_n;\ R \cup S \rangle$.

Доказательство. По теореме о соответствии между подгруппами некоторой группы и подгруппами ее фактор-группы подгруппа H фактор-группы F/N представима в виде $H = K/N$ для некоторой содержащей подгруппу N нормальной подгруппы K группы $F = F(a_1, a_2, \ldots, a_n)$, и потому в силу теоремы об изоморфизмах групп фактор-группа группы F/N по подгруппе H изоморфна фактор-группе F/K. Остается показать, что K совпадает с нормальным замыканием в группе F множества элементов $R \cup S$.

Так как для любого $s \in S$ смежный класс sN является элементом подмножества M и потому входит в подгруппу H, имеет место включение $S \subseteq K$. Поскольку, к тому же, подмножество R содержится в N и потому тоже лежит в K, нормальное замыкание в группе F множества $R \cup S$ содержится в подгруппе K. Произвольная нормальная подгруппа L группы F, содержащая подмножество $R \cup S$, содержит, очевидно, подгруппу $N = R^F$, и подгруппа L/N фактор-группы F/N является в ней нормальной и содержит подмножество M, а потому и подгруппу H, нормальное замыкание M. Так как из включения $K/N \subseteq L/N$ следует включение $K \subseteq L$, подгруппа K действительно является наименьшей нормальной подгруппой группы F, содержащей множество $R \cup S$, и теорема доказана.

§ 3. Преобразования Тице.

Как уже отмечалось, каждое представление определяет единственную (с точностью до изоморфизма) группу. С другой стороны, каждая группа может задаваться разными представлениями порождающими и определяющими соотношениями. Получить описание (в определенном смысле) всех представлений данной группы позволяют так называемые *преобразования Тице*, т. е. преобразования формального выражения вида

$$\langle a_1, a_2, \ldots, a_n;\ R\rangle \tag{1}$$

(где R — некоторое множество слов в алфавите $a_1, a_2, \ldots, a_n$) в другое выражение аналогичного вида. Эти преобразования относятся к следующим четырем типам.

Преобразование типа T1 состоит в присоединении к множеству R определяющих слов представления (1) слова w, выводимого из множества R. Таким образом, в результате этого преобразования представление (1) переходит в представление $\langle a_1, a_2, \ldots, a_n;\ R_1\rangle$, где $R_1 = R \cup \{w\}$.

Преобразование типа T2 является в определенном смысле обратным к преобразованию типа T1 и состоит в следующем: если некоторое слово w выводимо из множества $R_2 = R \setminus \{w\}$ всех остальных определяющих слов представления (1), то оно удаляется из множества определяющих слов (1), в результате чего получается представление $\langle a_1, a_2, \ldots, a_n;\ R_2\rangle$.

(Разумеется, эти преобразования могут оформляться как присоединение определяющего соотношения, выводимого в представлении (1) или удаление соотношения, выводимого из остальных определяющих слов (и соотношений).)

Преобразование типа T3 состоит в присоединении к порождающим символам представления (1) нового порождающего символа b с одновременным добавлением к множеству определяющих слов (соотношений) еще одного определяющего соотношения вида $b = w$, где $w = w(a_i)$ — слово в порождающих символах представления (1). Таким образом, в результате этого преобразования представление (1) переходит в представление $\langle a_1, a_2, \ldots, a_n, b\,;\ R,\ b = w\rangle$.

Обратным к преобразованию типа T3 является преобразование типа T4. Оно применимо к представлению (1), если одно из определяющих слов этого представления имеет вид xw^{-1}, где x — некоторый порождающий символ этого представления, не участвующий в записи ни слова w, ни любого другого определяющего слова (соотношения) из (1). В этом случае можно из представления удалить этот порождающий символ вместе с указанным определяющим соотношением.

Перечисленные преобразования называют *элементарными преобразованиями Тице.* В общем случае под преобразованием Тице понимается одновременное выполнение произвольного (возможно, бесконечного) набора однотипных элементарных преобразований.

Имеет место следующее утверждение:

Теорема. *Две группы, заданные представлениями, изоморфны тогда только тогда, когда одно из этих представлений можно перевести в другое некоторой конечной последовательностью преобразований Тице.*

Доказательство. Для доказательства того, что два представления, одно из которых получено из другого последовательностью преобразований Тице, определяют изоморфные группы, достаточно рассмотреть случай, когда эта последовательность состоит из единственного преобразования Тице.

Требуемое утверждение очевидно, если это преобразование относится к типу T1 или к типу T2, поскольку эти преобразования не изменяют соответствующего свободного представления группы. Случай преобразования типа T3 или T4 для простоты обозначений рассмотрим, считая его элементарным преобразованием; то же рассуждение проходит для произвольного преобразования.

Покажем, что группы, определяемые представлением (1) и представлением

$$\langle a_1, a_2, \ldots, a_n, b\,;\ R,\, b = w\rangle \tag{2}$$

(где $w = w(a_i)$) изоморфны.

Группа, определяемая представлением (1). является фактор-группой F/N, где $F = F(a_1, a_2, \ldots, a_n)$ и $N = R^F$ — нормальное замыкание множества R в группе F. Группа, определяемая представлением (2) является фактор-группой F_1/N_1, где $F_1 = F(a_1, a_2, \ldots, a_n, b)$ и $N_1 = R_1^{F_1}$ — нормальное замыкание множества $R_1 = R \cup \{bw^{-1}\}$ в группе F_1.

По теореме 2.3.1 существует гомоморфизм φ группы F_1 в группу F/N такой, что для любого $i = 1, 2, \ldots, n$ и $a_i\varphi = a_iN$ $b\varphi = wN$. Поскольку группа F/N порождается элементами $a_1N, a_2N, \ldots, a_nN$, гомоморфизм φ сюръективен, и потому группа F/N изоморфна фактор-группе F_1/K, где K — ядро гомоморфизма φ. Так как для любого элемента $u = u(a_i)$ выполнено равенство $u\varphi = uN$, справедливо включение $R \subseteq K$. Кроме того, $bw^{-1} \in K$, поскольку $(bw^{-1})\varphi = b\varphi \cdot w^{-1}\varphi = wN \cdot w^{-1}N = N$.

Так как N_1 является наименьшей нормальной подгруппой группы F_1, содержащей множество R_1, отсюда имеем $N_1 \subseteq K$. Покажем, что на самом деле подгруппа N_1 совпадает с K. Тем самым будет доказано, что группы F/N и F_1/N_1 изоморфны.

Пусть $v = v(a_i, b)$ — произвольный элемент из подгруппы K. Так как $bw^{-1} \in N_1$, имеет место сравнение $b \equiv w \pmod{N_1}$. Поэтому если слово $u = u(a_i)$ получено из слова v заменой каждого вхождения символа b словом w, имеем $u \equiv v \pmod{N_1}$. Поскольку $N_1 \subseteq K$, отсюда следует, что $u \in K$, т. е. $u\varphi = N$, и так как $u\varphi = uN$, получаем $u \in N$. В силу предложения 2.1.2 слово u свободно равно слову вида $(x_1^{-1} r_1^{\varepsilon_1} x_1)(x_2^{-1} r_2^{\varepsilon_2} x_2) \cdots (x_k^{-1} r_k^{\varepsilon_k} x_k)$, где $r_1, r_2, \ldots, r_k \in R$, и $x_1, x_2, \ldots, x_k$ — слова в алфавите $a_1, a_2, \ldots, a_n$ и $\varepsilon_i = \pm 1$. Следовательно, в группе F_1 слово u представляет элемент из подгруппы N_1, и так как $u \equiv v \pmod{N_1}$, имеет место включение $v \in N_1$. Равенство $N_1 = K$ доказано, и, следовательно, доказана часть “тогда” утверждения теоремы.

Предположим теперь, что изоморфные группы G и H заданы представлениями

$$\langle a_1, a_2, \ldots, a_m;\ R \rangle \tag{3}$$

и

$$\langle b_1, b_2, \ldots, b_n;\ S \rangle \tag{4}$$

соответственно. Покажем, что существуют последовательности преобразований Тице, приводящие каждое из этих представлений к одному и тому же представлению. Поскольку любая последовательность преобразований Тице обратима, теорема будет полностью доказана.

Фиксируем некоторый изоморфизм $\varphi\colon G \to H$ группы G на группу H и введем обозначения для образов относительно φ порождающих элементов $a_1, a_2, \ldots, a_m$ группы G: для любого $i = 1, 2, \ldots m$ пусть $a_i\varphi = u_i(b_1, b_2, \ldots, b_n)$. Аналогично, для обратного изоморфизма $\varphi^{-1}\colon H \to G$ полагаем $b_j\varphi^{-1} = v_j(a_1, a_2, \ldots, a_m)$ $(j = 1, 2, \ldots, n)$.

Применим к представлению (4) преобразование Тице типа T3, добавив порождающие символы $a_1, a_2, \ldots, a_m$ и определяющие соотношения $a_i = u_i(b_1, b_2, \ldots, b_n)$ $(i = 1, 2, \ldots, m)$. Результатом является представление

$$\begin{aligned}\langle a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n;& \\ S,\ a_i = u_i(b_1, b_2, \ldots, b_n)\,&(i = 1, 2, \ldots, m)\rangle.\end{aligned} \tag{5}$$

Для любого элемента $w = w(a_1, a_2, \ldots, a_m)$ группы G его φ-образ получается, очевидно, заменой каждого вхождения символа a_i словом u_i, $w\varphi = w(u_1, u_2, \ldots, u_m)$. Так как φ-образ произвольного определяющего слова $r \in R$, $r = r(a_1, a_2, \ldots, a_m)$ является единичным элементом группы H, соотношение $r(u_1, u_2, \ldots, u_m) = 1$ выводимо из множества S определяющих слов представления (4). Кроме того, из определяющих соотношений $a_i = u_i(b_1, b_2, \ldots, b_n)$ представления (5) выводимо соотношение $r(a_1, a_2, \ldots, a_m) = r(u_1, u_2, \ldots, u_m)$. Таким образом, из определяющих слов и определяющих соотношений представления (5) выводимо каждое слово из множества R.

Аналогично, для любого номера $(j = 1, 2, \ldots, n)$ в представлении (5) выводимо соотношение $v_j(a_1, a_2, \ldots, a_m) = v_j(u_1, u_2, \ldots, u_m)$, которое в силу равенства $b_j = v_j(a_1, a_2, \ldots, a_m)\varphi = v_j(u_1, u_2, \ldots, u_m))$ равносильно соотношению $b_j = v_j(a_1, a_2, \ldots, a_m)$.

Следовательно, представление

$$\langle a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n; R,\, S,\, a_i = u_i(b_1, b_2, \ldots, b_n) \\ (i = 1, 2, \ldots, m),\;\; b_j = v_j(a_1, a_2, \ldots, a_m)\,(j = 1, 2, \ldots, n)\rangle.$$

получается из представления (5) преобразованием Тице типа T1. Поскольку к этому же представлению приведут симметричные преобразования, примененные к представлению (3), теорема доказана.

§ 4. Об алгоритмических проблемах в теории групп

Практически любой вопрос о свойствах группы, заданной конечным представлением порождающими и определяющими соотношениями (т. е. представлением, состоящим из конечного множества порождающих символов и конечного множества определяющих слов (соотношений); группа, задаваемая конечным представлением, называется конечно определенной), может быть сформулирован, как проблема алгоритмической разрешимости, т. е. проблема существования алгоритма, разрешающего серию соответствующих однотипных задач. Первой из основных проблем разрешимости является проблема равенства слов (называемая также просто проблемой слов или проблемой тождества).

Пусть G — группа, определяемая данным конечным представлением. *Проблема равенства слов* заключается в существовании алгоритма, который для любых слов u и v в порождающих символах этого представления отвечает на вопрос, эквивалентны ли эти слова, т. е. — на вопрос, определяют ли слова u и v один и тот же элемент группы G. Проблема слов считается (алгоритмически) разрешимой, если такой алгоритм существует, и неразрешимой в противном случае. (Заметим, что поскольку слова u и v эквивалентны в группе G тогда и только тогда, когда слово uv^{-1} определяет единичный элемент этой группы, проблему слов можно сформулировать как проблему существования алгоритма, распознающего равенство произвольного слова пустому слову.)

Проблема сопряженности для группы G состоит в существовании алгоритма, который для любых слов u и v отвечал бы на вопрос, определяют ли эти слова сопряженные элементы группы G.

Следующая алгоритмическая проблема, *проблема изоморфизма*, относится к семейству всех конечных представлений и считается разрешимой, если существует алгоритм, который для любых двух конечных представлений отвечает на вопрос, изоморфны ли группы, определяемые этими представлениями.

Эти проблемы были сформулированы в 1911 году известным математиком Максом Дэном. В статье, содержащей их формулировку, была установлена разрешимость проблем тождества и сопряженности для некоторых групп, возникающих в топологии. Разрешимость этих проблем для свободных групп является очевидным следствием доказанных выше утверждений 1.1.3 и 1.2.3. По чисто формальным соображениям ближайшими к свободным группам, являются группы, определяемые единственным соотношением. Спустя 20 лет после публикации упомянутой только что работы Дэна его ученик В. Магнус доказал разрешимость проблемы тождества для групп с одним определяющим соотношением. Тем не менее, вопрос о разрешимости проблемы сопряженности для этих групп до сих пор остается нерешенным.

Первые примеры конечно определенных групп, алгоритмические проблемы тождества и сопряженности для которых являются неразрешимыми были построены П. С. Новиковым в начале 50-х годов прошлого века. Затем ученик П. С. Новикова С. И. Адян доказал, что практически каждое свойство конечно определенных групп алгоритмически нераспознаваемо. Это означает, в частности, что не существует алгоритма, который по произвольному конечному представлению устанавливал бы, является группа, определяемая этим представлением, единичной, т. е. изоморфной группе с представлением $\langle a;\ a = 1\rangle$. Тем самым доказана алгоритмическая неразрешимость проблемы изоморфизма.

§ 5. Обобщенные свободные произведения групп.

В этом параграфе формулируется определение конструкции обобщенного свободного произведения групп и излагаются ее основные свойства.

5.1. Определение свободного произведения двух групп с объединенными подгруппами. Пусть A и B — две группы, каждая из которых задана представлением порождающими и определяющими словами:

$$A = \langle a_1, a_2, \ldots, a_m;\ W\rangle, \tag{1}$$

$$B = \langle b_1, b_2, \ldots, b_n;\ V\rangle. \tag{2}$$

Пусть также H — подгруппа группы A, K — подгруппа группы B, изоморфная подгруппе H, и $\varphi\colon H \to K$ — некоторый изоморфизм группы H на группу K. *Свободным произведением групп A и B с подгруппами H и K, объединенными в соответствии с изоморфизмом φ*, называется группа G, задаваемая представлением вида

$$G = \langle a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n;\ W, V,\ h = h\varphi\ (h \in H)\rangle. \tag{3}$$

Для обозначения группы, получаемой таким образом, будем использовать запись $G = \big(A * B;\ H = K, \varphi\big)$.

Говоря более подробно, группа G задается представлением, множество порождающих символов которого является объединением (непересекающихся) множеств порождающих символов групп A и B, а определяющие соотношения группы G состоят из определяющих слов группы A, определяющих слов группы B и всевозможных соотношений вида $h = h\varphi$, где h — слово от порождающих $a_1, a_2, \ldots, a_m$, определяющее в группе A элемент из подгруппы H, и $h\varphi$ — слово от порождающих $b_1, b_2, \ldots, b_n$, определяющее в группе B соответствующий ему в силу отображения φ элемент из подгруппы K.

Разумеется, для каждого элемента группы H достаточно присутствия в (3) лишь одного соотношения вида $h = h\varphi$ (если этот элемент определяется словом h и также словом h_1, то легко видеть, что соотношение $h_1 = h_1\varphi$ выводимо из соотношения $h = h\varphi$ и множества слов $W \cup V$). Более того, такие соотношения в представлении (3) группы G можно оставить лишь для элементов из некоторого множества порождающих группы H, поскольку все остальные будут из них выводимы и потому могут быть удалены соответствующим преобразованием Тице.

Например, если A — бесконечная циклическая группа с порождающим a, B — бесконечная циклическая группа с порождающим b, подгруппа H порождается элементом a^2, подгруппа K порождается элементом b^3 и изоморфизм φ определяется отображением $a^2 \mapsto b^3$, то группа $G = \big(A * B;\ H = K, \varphi\big)$ задается представлением $\langle a, b;\ a^2 = b^3\rangle$. В самом деле, поскольку, например, для элемента a^4 подгруппы H имеем $a^4\varphi = (a^2\varphi)^2 = (b^3)^2 = b^6$, то в соответствии с определением в систему определяющих соотношений представления вида (3) группы G должно входить соотношение $a^4 = b^6$. Однако, очевидно, что оно выводимо из соотношения $a^2 = b^3$ и потому его можно удалить.

Изучение конструкции свободного произведения двух групп с объединенными подгруппами начнем с доказательства важного свойства, называемого *склеиваемостью или продолжаемостью гомоморфизмов*.

Пусть, как и выше, A и B — некоторые группы с подгруппами $H \leqslant A$ и $K \leqslant B$ и $\varphi\colon H \to K$ — изоморфизм группы H на группу K. Гомоморфизмы $\sigma\colon A \to T$ и $\tau\colon B \to T$ групп A и B в некоторую (одну и те же) группу T называются *согласованными с изоморфизмом* φ, если для произвольного элемента $h \in H$ выполняется равенство $h\sigma = h(\varphi\tau)$.

5.1.1. Теорема. *Пусть $G = (A{*}B;\ H = K, \varphi)$ — свободное произведение групп $A = \langle a_1, a_2, \ldots, a_m;\ W\rangle$ и $B = \langle b_1, b_2, \ldots, b_n;\ V\rangle$ с подгруппами H и K, объединенными в соответствии с изоморфизмом φ. Пусть σ и τ — гомоморфизмы групп A и B соответственно в некоторую группу T, согласованные с изоморфизмом φ. Тогда существует гомоморфизм ρ группы G в группу T такой, что $a_i\rho = a_i\sigma$ для любого $i = 1, 2, \ldots, m$ и $b_j\rho = b_j\tau$ для любого $j = 1, 2, \ldots, n$.*

(Разумеется символы a_i и b_j в левых частях этих равенств определяют элементы группы G, а в правых — элементы групп A и B.)

Доказательство. Определим отображение η множества порождающих символов представления (3) группы G в группу T, полагая для любых $i = 1, 2, \ldots, m$ и $j = 1, 2, \ldots, n$ $a_i\eta = a_i\sigma$ и $b_j\eta = b_j\tau$, и продолжим его (как в доказательстве теоремы 2.3.1) до отображения в группу T множества всех слов от этих символов. Так как σ — гомоморфизм, то для любого слова $w = w(a_1, a_2, \ldots, a_m)$ имеет место равенство $w\eta = w\sigma$, и потому из того, что $w \in W$, следует, что значение $w\eta$ слова w равно единице группы T. Аналогично, равно единице и η-значение каждого слова $v \in V$. Поскольку для любого слова $h \in H$ в силу согласованности гомоморфизмов σ и τ с изоморфизмом φ имеем $h\eta = h\sigma = h(\varphi\tau) = (h\varphi)\tau = (h\varphi)\eta$,

η-значения левой и правой частей любого соотношения вида $h = h\varphi$ совпадают. Существование требуемого гомоморфизма ρ гарантируется поэтому теоремой 2.3.1.

Поскольку множество W определяющих слов группы A содержится в множестве определяющих слов группы $G = \bigl(A * B;\ H = K, \varphi\bigr)$, в силу теоремы 2.3.1 существует гомоморфизм α группы A в группу G такой, что $a_i\alpha = a_i$ для любого $i = 1, 2, \ldots, m$. Аналогично, существует гомоморфизм β группы B в группу G такой, что для любого $j = 1, 2, \ldots, n$ выполнено равенство $b_j\beta = b_j$. Еще одно основное свойство конструкции свободного произведения двух групп с объединенными подгруппами состоит в том, что отображения α и β являются вложениями:

5.1.2. Теорема. *Пусть A, B и $G = \bigl(A * B;\ H = K, \varphi\bigr)$ — группы, заданные представлениями* (1), (2) *и* (3) *соответственно. Пусть α — гомоморфизм группы A в группу G, продолжающий тождественное вложение множества порождающих символов представления* (1) *в множество порождающих символов представления* (3), *и β — гомоморфизм группы B в группу G, продолжающий тождественное вложение множества порождающих символов представления* (2) *в множество порождающих символов представления* (3). *Тогда гомоморфизмы α и β являются инъективными.*

Доказательство. Обозначим через Γ декартово произведение множеств элементов групп A и B:

$$\Gamma = \bigl\{(x, y) \bigm| x \in A,\ y \in B\bigr\}.$$

Для каждого элемента $a \in A$ определим отображение σ_a множества Γ в себя, полагая для произвольного $(x, y) \in \Gamma$

$$(x, y)\sigma_a = (xa, y).$$

Непосредственно проверяется, что это отображение биективно и потому является элементом группы S_Γ всех биекций множества Γ в себя. Кроме того, для любых элементов $a_1, a_2 \in A$ и $(x, y) \in \Gamma$ имеем

$$(x, y)\sigma_{a_1a_2} = (x(a_1a_2), y) = ((xa_1)a_2, y) = ((x, y)\sigma_{a_1})\sigma_{a_2} = (x, y)(\sigma_{a_1}\sigma_{a_2}),$$

так что выполнено равенство $\sigma_{a_1a_2} = \sigma_{a_1}\sigma_{a_2}$. Это означает, что отображение $\sigma : A \to S_\Gamma$, сопоставляющее элементу $a \in A$ биекцию σ_a, является гомоморфизмом группы A в группу S_Γ. Так как для любых $a_1, a_2 \in A$ равенство $a_1\sigma = a_2\sigma$ равносильно тому, что $(x, y)\sigma_{a_1} = (x, y)\sigma_{a_2}$ для произвольного $(x, y) \in \Gamma$, а это, в свою очередь, равносильно равенству $a_1 = a_2$, гомоморфизм σ инъективен.

Аналогично, отображение τ_b, определяемое по правилу

$$(x, y)\tau_b = (x, yb) \quad ((x, y) \in \Gamma)$$

для каждого элемента $b \in B$, является элементом группы S_Γ и отображение $\tau\colon B \to S_\Gamma$, сопоставляющее элементу $b \in B$ отображение τ_b, является инъективным гомоморфизмом группы B в группу S_Γ.

Поскольку, как легко видеть, пересечение подгрупп $A\sigma$ и $B\tau$ группы S_Γ совпадает с единичной подгруппой, гомоморфизмы σ и τ не являются согласованными с изоморфизмом φ. Для исправления этой ситуации фиксируем систему представителей U левых смежных классов группы A по подгруппе H и систему представителей V левых смежных классов группы B по подгруппе K и определим отображение π множества Γ в себя следующим образом:

Возьмем произвольный элемент $(x, y) \in \Gamma$ и запишем его компоненты в виде $x = up$, $y = vq$ для подходящих однозначно определяемых элементов $u \in U$, $v \in V$, $p \in H$ и $q \in K$. Теперь полагаем

$$(x, y)\pi = (u(q\varphi^{-1}), v(p\varphi)).$$

Очевидно, что правая часть этого равенства является элементом множества Γ, так что π действительно отображает это множество в себя. Легко видеть также, что $\pi^2 = \mathrm{id}_\Gamma$ — тождественное отображение множества Γ. Поэтому π биективно, т. е. является элементом группы S_Γ.

Определим теперь отображение τ^* группы B в группу S_Γ, полагая для произвольного элемента $b \in B$

$$b\tau^* = \pi\tau_b\pi.$$

Так как $\pi = \pi^{-1}$, имеем $b\tau^* = \pi^{-1}\tau_b\pi = \pi^{-1}(b\tau)\pi = b(\tau\,\widehat{\pi})$, где $\widehat{\pi}$ — внутренний автоморфизм группы S_Γ, производимый элементом π. Следовательно, выполнено равенство $\tau^* = \tau\,\widehat{\pi}$, так что отображение τ^* является инъективным гомоморфизмом группы B в группу S_Γ.

Покажем, что гомоморфизмы σ и τ^* согласованы с изоморфизмом φ, т. е. для любого элемента $h \in H$ отображения $h\sigma = \sigma_h$ и $h(\varphi\tau^*) = \pi\tau_{h\varphi}\pi$ множества Γ в себя совпадают.

Снова возьмем произвольный элемент $(x, y) \in \Gamma$ и предположим, что его компоненты, как и выше, записаны в виде $x = up$ и $y = vq$, где $u \in U$, $v \in V$, $p \in H$ и $q \in K$.

По определению отображения σ_h имеем $(x, y)\sigma_h = (xh, y)$. С другой стороны, так как

$$(x, y)(\pi\tau_{h\varphi}\pi) = (((x, y)\pi)\tau_{h\varphi})\pi,$$

имеем последовательно

$$(x, y)\pi = (u(q\varphi^{-1}), v(p\varphi)),$$
$$(u(q\varphi^{-1}), v(p\varphi))\tau_{h\varphi} = (u(q\varphi^{-1}), v(p\varphi)(h\varphi)) = (u(q\varphi^{-1}), v((ph)\varphi),$$
$$(u(q\varphi^{-1}), v((ph)\varphi)\pi = (u(ph), vq) = (xh, y),$$

и требуемое равенство доказано.

По теореме 5.1.1 существует гомоморфизм ρ группы G в группу S_Γ такой, что $a_i\rho = a_i\sigma$ для любого $i = 1, 2, \ldots, m$ и $b_j\rho = b_j\tau^*$ для любого $j = 1, 2, \ldots, n$. Так как при гомоморфизме $\alpha\colon A \to G$ порождающий элемент a_i группы A переходит в порождающий элемент a_i группы G из равенства $a_i\rho = a_i\sigma$ следует равенство $a_i(\alpha\rho) = a_i\sigma$. Таким образом, гомоморфизмы $\alpha\rho$ и σ группы A в группу S_Γ действуют одинаково на каждый элемент системы порождающих группы A. Следовательно, $\alpha\rho = \sigma$, и так как отображение σ инъективно, отображение α является инъективным. Инъективность отображения β доказывается аналогично.

Теорема 5.1.2 фактически утверждает, что порожденная элементами $a_1, a_2, \ldots, a_m$ подгруппа группы $G = \bigl(A * B;\ H = K, \varphi\bigr)$ изоморфна группе A и подгруппа, порожденная элементами $b_1, b_2, \ldots, b_n$, изоморфна группе B. Возможность отождествлять изоморфные группы позволяет считать (когда это удобно), что эти подгруппы совпадают с группами A и B соответственно (и говорить о группах A и B как о *вложенных в группу G естественным образом*, называя их также *свободными сомножителями* группы G). Это позволяет придать теореме 5.1.1 следующую более компактную и более определенную формулировку:

5.1.3. Следствие (из теоремы 5.1.1)**.** *Пусть $G = (A*B;\ H = K, \varphi)$ — свободное произведение групп A и B с подгруппами H и K, объединенными в соответствии с изоморфизмом φ и пусть группы A и B вложены естественным образом в группу G. Пусть также σ и τ — гомоморфизмы групп A и B соответственно в некоторую группу T, согласованные с изоморфизмом φ. Тогда существует гомоморфизм ρ группы G*

в группу T, действие которого на подгруппе A совпадает с действием гомоморфизма σ и действие на подгруппе B совпадает с действием τ.

5.2. Несократимая запись элемента свободного произведения двух групп с объединенными подгруппами. Определение (3) группы $G = \big(A * B;\ H = K, \varphi\big)$ означает, в частности, что каждый неединичный элемент g этой группы представим некоторым словом w от порождающих символов $a_1, a_2, \ldots, a_m, b_1, b_2, \ldots, b_n$. Это слово можно записать в виде произведения $w = v_1 v_2 \cdots v_s$, где каждый сомножитель v_i является словом либо только от порождающих $a_1, a_2, \ldots, a_m$, либо только от порождающих $b_1, b_2, \ldots, b_n$ (и называется, соответственно, A-слогом или B-слогом слова w). причем при $s > 1$ любые соседние слоги v_i и v_{i+1} не являются одновременно A-слогами или B-слогами. Более того, можно предполагать, что при $s > 1$ каждый слог v_i, являющийся A-слогом, определяет в группе A элемент, не принадлежащий подгруппе H, и каждый слог v_i, являющийся B-слогом, определяет в группе B элемент, не принадлежащий подгруппе K.

Действительно, легко видеть, что в противном случае с использованием подходящего соотношения вида $h = h\varphi$, можно перейти к слову, определяющему тот же элемент g группы G и являющемуся произведением меньшего числа слогов.

Таким образом, каждый неединичный элемент g группы G определяется некоторым словом вида $v_1 v_2 \cdots v_s$ таким, что

1) каждый сомножитель v_i является либо A-слогом либо B-слогом;

2) если $s > 1$, то любые соседние слоги v_i и v_{i+1} не являются одновременно A-слогами или B-слогами;

3) если $s > 1$, то каждый слог v_i, являющийся A-слогом, определяет в группе A элемент, не принадлежащий подгруппе H, и каждый слог v_i, являющийся B-слогом, определяет в группе B элемент, не принадлежащий подгруппе K.

Слово, определяющее элемент $g \in G$ и удовлетворяющее условиям 1), 2) и 3), называют *несократимой записью* элемента g.

Из сказанного выше следует, что произвольный неединичный элемент свободного произведения G групп A и B с объединенными подгруппами

H и K обладает хотя бы одной несократимой записью. Несократимой записью единичного элемента будем считать пустое слово. Следовательно, имеет место

5.2.1. Предложение. *Для любого элемента группы*

$$G = \big(A * B;\ H = K, \varphi\big)$$

существует несократимая запись.

Третье из основных свойств конструкции свободного произведения двух групп с объединенными подгруппами дополняет утверждение предложения 5.2.1 и формулируемое следующим образом:

5.2.2. Теорема. *Если элемент группы* $G = \big(A * B;\ H = K, \varphi\big)$ *обладает несократимой записью, число слогов которой больше* 1*, то он отличен от единицы этой группы.*

Все известные доказательства этого утверждения (см., напр., [1], [2]) являются весьма объемными, и в силу этого здесь оно приводится без доказательства.

Если мы считаем группы A и B подгруппами группы G, то подгруппы H и K в группе G являются, очевидно, совпадающими, и потому имеет место включение $H \subseteq A \cap B$. В действительности, справедливо равенство $A \cap B = H$.

В самом деле, произвольный элемент $g \in G$, лежащий в подгруппе $A \cap B$, определяется некоторым словом u от порождающих $a_1, a_2, \ldots, a_m$ и некоторым словом v от порождающих $b_1, b_2, \ldots, b_n$. Если предположить, что g не входит в подгруппу $H = K$, то состоящая из двух слогов запись uv^{-1} единицы группы G окажется несократимой, что невозможно в силу теоремы 5.2.2.

Для выражения того факта, что группы A и B считаются подгруппами группы $G = (A * B;\ H = K, \varphi)$, обычно используется запись вида $G = \big(A * B;\ H\big)$ и в этом случае говорится о *свободном произведении групп* A *и* B *с* (*одной*) *объединенной подгруппой* H. Поскольку, в отличие от исходного определения, здесь не упоминается (но предполагается известным) изоморфизм, в соответствии с которым отождествляются подгруппы H и K, в таком виде эта конструкция используется, как правило, при изучении свойств, в формулировке которых этот изоморфизм не участвует.

Слоги несократимой записи элементов группы $G = \big(A * B;\ H\big)$ можно считать элементами групп A и B. Следовательно, в этой ситуации несократимой записью элемента $g \in G$ мы можем (и будем) называть представление этого элемента в виде произведения $g = x_1 x_2 \cdots x_s$, где $x_1,\ x_2,\ \ldots,\ x_s$ — элементы подгрупп A и B, причем при $s > 1$ любые соседние элементы не лежат в одной и той же из этих подгрупп (и потому ни один из этих элементов не входит в подгруппу H).

Вообще говоря, элемент группы $G = \big(A{*}B;\ H\big)$ может иметь несколько различных несократимых записей. Описание (в некотором смысле) всех несократимых записей данного элемента группы G содержится в следующем утверждении:

5.2.3. Предложение. *Пусть $G = \big(A * B;\ H\big)$ — свободное произведение групп A и B с объединенной подгруппой H. Пусть $f = x_1 x_2 \cdots x_r$ и $g = y_1 y_2 \cdots y_s$ — несократимые записи неединичных элементов f и g группы G. Равенство $f = g$ имеет место тогда и только тогда, когда $r = s$ и при $r = 1$ $x_1 = y_1$, а при $r > 1$ в подгруппе H найдутся элементы $h_1,\ h_2,\ \ldots,\ h_{r-1}$ такие, что*

$$\begin{aligned} x_1 &= y_1 h_1, \\ x_i &= h_{i-1}^{-1} y_i h_i \quad (1 < i < r), \\ x_r &= h_{r-1}^{-1} y_r \end{aligned}$$

Доказательство. Достаточность сформулированных условий очевидна. Доказательство необходимости, считая без потери общности, что $r \leqslant s$, проведем индукцией по r.

Если $f = g$ и $r = 1$, то следует показать лишь, что и $s = 1$. Пусть, напротив, $s \geqslant 2$. Тогда все сомножители $y_1,\ y_2,\ \ldots,\ y_s$ несократимой записи элемента g не входят в подгруппу H. Перепишем равенство $f = g$ в виде

$$x_1^{-1} y_1 y_2 \cdots y_s = 1. \tag{4}$$

Если элемент x_1 не лежит в той же подгруппе A или B, что и элемент y_1, то левая часть равенства (4) является состоящей из $s + 1$ сомножителя несократимой записью единичного элемента группы G, что противоречит теореме 5.2.2. Если элементы x_1 и y_1 принадлежат одной и той же подгруппе A или B, но элемент $x_1^{-1} y_1$ не входит в подгруппу H, то левая часть равенства (4) является несократимой записью единичного элемента группы G, состоящей из s сомножителей, что снова невозможно. Наконец, если $x_1^{-1}y_1 \in H$, то элемент $y_2' = (x_1^{-1}y_1)y_2$ принадлежит той же подгруппе A или B, что и элемент y_2, и не принадлежит подгруппе H. Поэтому левая часть равенства (4) имеет несократимую запись $y_2' \cdots y_s$, что при $s > 2$ опять противоречит теореме 5.2.2. Таким образом, $s = 2$, и равенство (4) принимает вид $(x_1^{-1}y_1)y_2 = 1$, откуда получаем включение $y_2 \in H$, что невозможно.

Предположим теперь, что $r > 1$ и что для любых двух элементов группы G, длина хотя бы одного из которых меньше, чем $r > 1$, доказываемое утверждение справедливо. Снова перепишем равенство $f = g$ в виде

$$x_r^{-1} \cdots x_2^{-1}x_1^{-1}y_1y_2 \cdots y_s = 1. \tag{5}$$

Из теоремы 5.2.2 следует, что запись левой части равенства (5) не может быть несократимой, и потому, как легко видеть, элементы x_1 и y_1 должны принадлежать одной и той же подгруппе A или B и элемент $x_1^{-1}y_1$ должен принадлежать подгруппе H. Обозначив этот элемент через h_1^{-1}, имеем $x_1 = y_1h_1$ и $h_1 \in H$. Полагаем теперь

$$f' = x_2 \cdots x_r \qquad \text{и} \qquad g' = y_2'y_3 \cdots y_s,$$

где $y_2' = h_1^{-1}y_2$. Из (5) следует, что элементы f' и g' равны, а указанные записи этих элементов являются, очевидно, несократимыми. Поэтому из индуктивного предположения следует, что $r-1 = s-1$, т. е. $r = s$. Кроме того, при $r = 2$ из (5) имеем $x_2 = h_1^{-1}y_2$, так что последовательность, состоящая из единственного члена h_1, является искомой. Если же $r > 2$, то по индуктивному предположению в подгруппе H существуют элементы $h_2, h_3, \ldots, h_{r-1}$ такие, что

$$\begin{aligned} x_2 &= y_2'h_2, \\ x_i &= h_{i-1}^{-1}y_ih_i \quad (2 < i < r), \\ x_r &= h_{r-1}^{-1}y_r. \end{aligned}$$

Очевидно, что последовательность элементов $h_1, h_2, \ldots, h_{r-1}$ является искомой, и предложение 5.2.3 доказано.

Из предложения 5.2.3 следует, в частности, что любые две несократимые записи элемента g группы $G = \big(A * B;\ H\big)$ содержат одно и то же число сомножителей. Это число мы будем называть *длиной элемента g* и обозначать через $l(g)$.

Таким образом, единственным элементом длины 0 в группе G является единица этой группы. Очевидно также, что для любого элемента $g \in G$ равенство $l(g) = 1$ выполнено тогда и только тогда, когда g является неединичным элементом одного из свободных сомножителей A или B.

(Следует отметить, что это определение длины элемента свободного произведения с объединенной подгруппой несколько отличается от принятого в ряде руководств, в частности, — в книге [1]. В этих руководствах вместо несократимой записи элементов группы $G = \big(A * B;\ H\big)$ вводится их *нормальная форма.* Для этого в группах A и B фиксируются системы представителей левых смежных классов по подгруппе H, причем в обеих системах представителем H выбирается 1. Тогда произвольный элемент $g \in G$ может быть записан в виде $g = c_1 c_2 \cdots c_n h$, где $n \geqslant 1$, $h \in H$ и c_1, $c_2, \ldots$, c_n — представители из выбранных систем, причем при $n > 1$ соседние представители c_i и c_{i+1} не лежат в одной и той же подгруппе A или B. Из теоремы 5.2.2 легко следует, что такая запись элемента g является единственной; она и называется нормальной формой этого элемента. Длиной элемента g называют число n представителей, образующих его нормальную форму. Очевидно, что эта длина отлична от длины, определенной здесь, лишь для элементов из подгруппы H. Поскольку несократимая запись элементов, как правило, оказывается более удобной, чем нормальная форма, здесь принимается определение длины, сформулированное выше.)

5.3. Циклически несократимые элементы и отношение сопряженности в свободном произведении двух групп с объединенными подгруппами. Заметим, что из предложения 5.2.3 следует также, что сомножители с одинаковыми номерами любых двух несократимых записей элемента g группы $G = \big(A * B;\ H\big)$ лежат в одной и той же подгруппе A или B. Это замечание позволяет ввести следующее понятие:

Элемент g группы $G = \big(A * B;\ H\big)$ называется *циклически несократимым*, если в его несократимой записи $g = x_1 x_2 \cdots x_r$ при $r > 1$ сомножители x_1 и x_r не лежат в одной и той же подгруппе A или B.

Отметим, что в соответствии с этим определением все элементы длины $\leqslant 1$ должны считаться циклически несократимыми. Очевидно также, что если длина r циклически несократимого элемента $g = x_1x_2\cdots x_r$ больше 1, то для любого положительного целого числа n запись

$$x_1x_2\cdots x_rx_1x_2\cdots x_r\cdots x_1x_2\cdots x_r$$

элемента g^n является несократимой и потому $l(g^n) = nl(g)$.

Понятие циклически несократимого элемента позволяет охарактеризовать классы сопряженных элементов свободного произведения двух групп с объединенной подгруппой. Соответствующее утверждение, известное как теорема Солитэра (см. [1, теорема 4.6]), приведем в следующей формулировке:

5.3.1. Теорема. *Каждый элемент группы $G = \big(A * B;\ H\big)$ сопряжен с некоторым циклически несократимым элементом. Если длины двух циклически несократимых элементов группы G различны, то эти элементы не являются сопряженными. Пусть f и g — циклически несократимые элементы группы G равной длины. Тогда*

1. *Если элемент f принадлежит подгруппе A и не сопряжен в ней ни с каким элементом из подгруппы H, то элементы f и g сопряжены в группе G тогда и только тогда, когда $g \in A$ и элементы f и g сопряжены в группе A. Аналогично, если элемент f принадлежит подгруппе B и не сопряжен в ней ни с каким элементом из подгруппы H, то элементы f и g сопряжены в группе G тогда и только тогда, когда $g \in B$ и элементы f и g сопряжены в группе B.*

2. *Если элемент $f \in A$ сопряжен с элементом из подгруппы H, то, заменяя его на сопряженный с ним, можем считать, что $f \in H$, и в этом случае элементы f и g сопряжены в группе G тогда и только тогда, когда существует такая последовательность элементов*
$$f = h_0, h_1, \ldots, h_n, h_{n+1} = g,$$
что для каждого $i = 0, 1, \ldots, n$ $h_i \in H$ и элемент h_i сопряжен с элементом h_{i+1} в одной из подгрупп A или B. Аналогичное утверждение справедливо для элемента $f \in B$, сопряженного с элементом из подгруппы H.

3. *Если длина элемента f больше 1, то элементы f и g сопряжены в группе G тогда и только тогда, когда элемент g сопряжен при помощи элемента из подгруппы H с некоторой циклической перестановкой f' элемента f.*

(*Циклической перестановкой* элемента $f \in G$, имеющего несократимую запись $f = y_1 y_2 \cdots y_m$, где $m > 1$, называется элемент вида $y_i y_{i+1} \cdots y_m y_1 \cdots y_{i-1}$, $i = 1, 2, \ldots, m$; таким образом, строго говоря, речь идет о циклической перестановке данной несократимой записи этого элемента.)

Доказательство. Легко видеть, что элемент наименьшей длины в множестве элементов, сопряженных с $g \in G$, является циклически несократимым. Отметим также, что достаточность условий в утверждениях пунктов 1, 2 и 3 очевидна и что из этих условий вытекает, что $l(f) = l(g)$. Докажем их необходимость.

Пусть f и g — циклически несократимые элементы группы G и пусть для некоторого элемента $u \in G$ с несократимой записью $u = x_1 x_2 \cdots x_r$ выполнено равенство $u^{-1} f u = g$.

Предположим сначала, что элемент f принадлежит подгруппе A и не сопряжен в ней ни с каким элементом из подгруппы H. Если $r > 1$ и элемент x_1 принадлежит подгруппе B, то запись

$$x_r^{-1} \cdots x_2^{-1} x_1^{-1} f x_1 x_2 \cdots x_r$$

элемента $u^{-1} f u$ является несократимой, а если элемент x_1 принадлежит подгруппе A, то поскольку $x_1^{-1} f x_1$ не входит в подгруппу H, запись

$$x_r^{-1} \cdots x_2^{-1} (x_1^{-1} f x_1) x_2 \cdots x_r$$

элемента $u^{-1} f u$ является несократимой. Так как в обоих случаях этот элемент не является циклически несократимым и потому не может совпадать с элементом g, имеем $r = 1$. Если $u = x_1$ не входит в подгруппу A, то поскольку f не входит в H, элемент $u^{-1} f u$ снова не является циклически несократимым. Таким образом, $u \in A$, так что $g \in A$ и элементы f и g сопряжены в группе A.

Случай, когда элемент f принадлежит подгруппе B и не сопряжен в ней ни с каким элементом из подгруппы H, рассматривается аналогично.

Пусть теперь элемент f принадлежит подгруппе H. Индукцией по длине r элемента u докажем существование такой последовательности

$h_0, h_1, \ldots, h_{r-1}, h_r$, что $h_0 = f$, $h_r = g$, элементы $h_0, h_1, \ldots, h_{r-1}$ лежат в подгруппе H и любые соседние члены этой последовательности h_i и h_{i+1} $(i = 0, 1, \ldots, r-1)$ сопряжены в одной из подгрупп A или B.

При $r = 1$ утверждение очевидно, поскольку последовательность h_0, h_1, где $h_0 = f$ и $h_1 = g$, обладает всеми требуемыми свойствами.

При $r > 1$ снова полагаем $h_0 = f$. Элемент $x_1^{-1}h_0x_1$ лежит в той же подгруппе A или B, что и элемент x_1. Поэтому если $x_1^{-1}h_0x_1$ не входит в подгруппу H, то запись

$$x_r^{-1} \cdots x_2^{-1}(x_1^{-1}fx_1)x_2 \cdots x_r$$

элемента $u^{-1}fu$ является несократимой, и потому этот элемент не является циклически несократимым.

Таким образом, элемент $h_1 = x_1^{-1}h_0x_1$ принадлежит подгруппе H. Полагая еще $v = x_2 \cdots x_r$, имеем $v^{-1}h_1v = g$. По индуктивному предположению существуют элементы $h_2, \ldots, h_{r-1}, h_r$ такие, что $h_r = g$, $h_2, \ldots, h_{r-1} \in H$ и для каждого $i = 1, 2, \ldots, r-1$ элементы h_i и h_{i+1} сопряжены в одной из подгрупп A или B. Очевидно, что последовательность $h_0, h_1, \ldots, h_{r-1}, h_r$ является искомой, индуктивный шаг завершен и утверждение пункта 2 доказано.

Предположим, наконец, что элемент f имеет несократимую запись вида $f = y_1y_2 \cdots y_m$, где $m > 1$. Покажем, что тогда элемент g сопряжен при помощи элемента из подгруппы H с некоторой циклической перестановкой элемента f. Заметим, что если длина r элемента u равна 1 и элемент x_1 лежит в подгруппе H, то справедливость этого очевидна. Поэтому мы можем считать, что в любом случае ($r = 1$ или $r > 1$) элемент x_1 не входит в подгруппу H.

Так как элемент f циклически несократим и $m > 1$, слоги y_1 и y_m несократимой записи этого элемента не лежат в одной и той же подгруппе A или B, и потому элемент x_1 лежит в одной и той же подгруппе в точности с одним из элементов y_1 и y_m. Заменив, если необходимо, элемент f на (сопряженный с ним) элемент $y_2y_3 \cdots y_my_1$, мы можем без потери общности считать, что элементы x_1 и y_1 лежат, а элементы x_1 и y_m не лежат в одной и той же подгруппе A или B. Если при этом элемент $x_1^{-1}y_1$ не входит в подгруппу H, то запись

$$x_r^{-1} \cdots x_2^{-1}(x_1^{-1}y_1)y_2 \cdots y_mx_1x_2 \cdots x_r$$

элемента $g = u^{-1}fu$ является несократимой. Но это невозможно, так как элемент с такой записью в любом случае ($r = 1$ или $r > 1$) не является циклически несократимым. Следовательно, элемент $x_1^{-1}y_1$ принадлежит подгруппе H. Обозначив его через h^{-1}, будем иметь $x_1 = y_1h$, откуда при $r = 1$ получаем

$$g = u^{-1}fu = x_1^{-1}y_1y_2\cdots y_mx_1 = h^{-1}(y_2\cdots y_my_1)h.$$

С учетом замечания, сделанного выше, это дает основание индукции по r. Если $r > 1$, полагаем $f' = y_2\cdots y_my_1$, $x_2' = hx_2$ и $u' = x_2'x_3\cdots x_r$. Тогда

$$\begin{aligned} g = u^{-1}fu = x_r^{-1}\cdots x_2^{-1}x_1^{-1}y_1y_2\cdots y_mx_1x_2\cdots x_r \\ = x_r^{-1}\cdots x_2^{-1}h^{-1}y_2\cdots y_my_1hx_2\cdots x_r = (u')^{-1}f'u'. \end{aligned}$$

Так как $l(u') = r - 1$, по индуктивному предположению элемент g сопряжен при помощи элемента из подгруппы H с некоторой циклической перестановкой элемента f'. Поскольку любая циклическая перестановка элемента f' совпадает с некоторой циклической перестановкой элемента f, это завершает индуктивный шаг, и теорема полностью доказана.

В случае, когда объединяемая подгруппа H расположена в центре каждой из групп A и B, то доставляемый теоремой 5.3.1. критерий сопряженности элементов группы $G = \big(A * B;\ H\big)$ приобретает, как нетрудно видеть, следующий более компактный вид:

5.3.2. Следствие. *Пусть $G = \big(A * B;\ H\big)$ и H является центральной подгруппой каждой из групп A и B. Пусть f и g — циклически несократимые элементы равной длины группы G. Тогда*

1. *если $l(f) = l(g) = 1$, то элементы f и g сопряжены в группе G тогда и только тогда, когда они лежат в одной и той же подгруппе A или B и сопряжены в этой подгруппе;*

2. *если $l(f) = l(g) > 1$, то элементы f и g сопряжены в группе G тогда и только тогда, когда один из них является циклической перестановкой другого.*

Так как порядки сопряженных элементов группы совпадают, из первого утверждения теоремы 5.3.1 вытекает следующее описание элементов конечного порядка свободного произведения групп с объединенными подгруппами:

5.3.3. Предложение. *Каждый элемент конечного порядка группы* $G = \big(A * B;\ H\big)$ *сопряжен с некоторым элементом из подгруппы* A *или из подгруппы* B. *В частности, свободное произведение с объединенной подгруппой двух групп без кручения является группой без кручения.*

Для доказательства достаточно напомнить, что если длина циклически несократимого элемента $g \in G$ больше 1, то для любого целого числа $n > 0$ имеет место равенство $l(g^n) = nl(g)$ и потому $g^n \neq 1$. Поэтому циклически несократимый элемент, сопряженный с элементом конечного порядка должен принадлежать одной из подгрупп A или B.

Теорема 5.3.1 позволяет также получить описание центра свободного произведения групп с объединенными подгруппами.

5.3.4. Предложение. *Пусть* $G = \big(A * B;\ H\big)$, *где* $H \neq A$ *и* $H \neq B$. *Центр* $Z(G)$ *группы* G *совпадает с пересечением* $Z(A) \cap Z(B)$ *центров подгрупп* A *и* B.

В самом деле, так как подгруппы A и B лежат в централизаторе подгруппы $Z = Z(A) \cap Z(B)$ и порождают группу G, справедливо включение $Z \subseteq Z(G)$. Обратно, пусть элемент $g \in G$ является центральным. Тогда он совпадает с любым элементом, сопряженным с ним, и так как каждый элемент группы G сопряжен с циклически несократимым, элемент g циклически несократим. Если в его несократимой записи $g = x_1 x_2 \cdots x_r$ число сомножителей $r > 1$, то элемент g не равен сопряженному с ним элементу $x_2 \cdots x_r x_1$. Следовательно, g входит в одну из подгрупп A и B.

Более того, элемент g принадлежит подгруппе H и потому входит и в подгруппу A, и в подгруппу B. В самом деле, если, скажем, $g \in A$ и $g \notin H$, то для произвольного элемента $b \in B \setminus H$ сопряженный с g элемент $b^{-1}gb$ имеет длину 3 и потому не может совпадать с g.

Поскольку элемент g перестановочен с каждым элементом группы G, из включения $g \in A$ следует, что $g \in Z(A)$, и из включения $g \in B$ следует, что $g \in Z(B)$. Таким образом, $g \in Z(A) \cap Z(B)$, и равенство $Z(G) = Z$ доказано.

В заключение этого раздела приведем описание вида элементов, не являющихся циклически несократимыми.

5.3.5. Предложение. *Пусть* $G = \big(A * B;\ H\big)$. *Произвольный элемент* $g \in G$, *не являющийся циклически несократимым, может быть* *представлен в виде*

$$g = u \cdot v \cdot u^{-1},$$

где u и v — неединичные элементы группы G с несократимыми записями $u = x_1x_2 \cdots x_r$ и $v = y_1y_2 \cdots y_s$, причем элемент v циклически несократим, элементы x_r и y_1 не принадлежат одной и той же подгруппе A или B и при $s > 1$ элемент $y_sx_r^{-1}$ (лежащий в той же подгруппе A или B, где находятся элементы x_r и y_s) не входит в подгруппу H.

Доказательство. Пусть $g = z_1z_2 \cdots z_n$ — несократимая запись элемента g. Если элемент g не является циклически несократимым, то $n \geqslant 3$ и сомножители z_1 и z_n его несократимой записи принадлежат одной и той же подгруппе A или B. Полагаем $z_n' = z_nz_1$ и $g' = z_2z_3 \cdots z_{n-1}z_n'$, так что $g = z_1g'z_1^{-1}$. Если элемент z_n' не входит в подгруппу H, то элемент g' циклически несократим, и очевидно, что элементы $u = z_1$ и $v = g'$ являются в этом случае искомыми.

Пусть $z_n' \in H$. Тогда запись $g' = z_2z_3 \cdots z_{n-1}'$, где $z_{n-1}' = z_{n-1}z_n'$, элемента g' является несократимой и потому его длина равна $n - 2$. Если $n - 2 = 1$, то элементы $u = z_1$ и $v = g'$ снова являются искомыми. Если же $n - 2 > 1$, то поскольку сомножители z_2 и z_{n-1}' лежат в одной и той же подгруппе A или B, элемент g' не является циклически несократимым. Поэтому по индукции можно считать, что существуют элементы $u' = x_1'x_2' \cdots x_r'$ и $v = y_1y_2 \cdots y_s$ (указанные записи которых несократимы) такие, что $g' = u' \cdot v \cdot (u')^{-1}$, элемент u' не входит в подгруппу H, элемент v циклически несократим, элементы x_r' и y_1 принадлежат разным подгруппам A или B и при $s > 1$ элемент $y_s(x_r')^{-1}$ не входит в подгруппу H. Тогда выражение

$$x_1'x_2' \cdots x_r'y_1(x_r')^{-1} \cdots (x_2')^{-1}(x_1')^{-1}$$

является несократимой записью элемента g', если $s = 1$, а при $s > 1$ несократимой записью этого элемента является выражение

$$x_1'x_2' \cdots x_r'y_1 \cdots y_{s-1}(y_s(x_r')^{-1}) \cdots (x_2')^{-1}(x_1')^{-1}$$

В любом случае элементы z_2 и x_1' лежат в одной и той же подгруппе A или B, и потому элементы z_1 и x_1' принадлежат разным подгруппам. Полагая теперь $u = z_1u'$, мы видим, что запись $u = z_1x_1'x_2' \cdots x_r'$ этого элемента несократима, и очевидно, что элементы u и v являются искомыми. Предложение доказано.

5.4. О некоторых гомоморфных образах свободного произведения двух групп с объединенными подгруппами. В этом разделе будет рассмотрен способ построения некоторых гомоморфных образов групп вида $G = (A * B;\ H = K, \varphi)$, предложенный в работе Г. Баумслага [4].

Пусть A и B — некоторые группы с подгруппами $H \leqslant A$ и $K \leqslant B$ и изоморфизмом $\varphi\colon H \to K$ этих подгрупп. Подгруппы R группы A и S группы B будем называть (H, K, φ)-*совместимыми*, если выполнено равенство $(H \cap R)\varphi = K \cap S$.

5.4.1. Предложение. *Пусть A и B — некоторые группы с изоморфными подгруппами $H \leqslant A$ и $K \leqslant B$ и $\varphi\colon H \to K$ — изоморфизм. Если нормальные подгруппы R и S групп A и B соответственно являются (H, K, φ)-совместимыми, то отображение $\varphi_{R,S}\colon HR/R \to KS/S$, определяемое по правилу*

$$(hR)\varphi_{R,S} = (h\varphi)S \qquad (h \in H), \tag{6}$$

этим правилом определено корректно и является изоморфизмом подгруппы HR/R фактор-группы A/R на подгруппу KS/S фактор-группы B/S.

Действительно, поскольку для произвольных элементов h_1 и h_2 из подгруппы H имеем

$$\begin{aligned} h_1R = h_2R \Rightarrow h_1^{-1}h_2 \in H \cap R \Rightarrow (h_1^{-1}h_2)\varphi \in K \cap S \Rightarrow \\ (h_1\varphi)^{-1}(h_2\varphi) \in K \cap S \Rightarrow (h_1\varphi)S = (h_2\varphi)S, \end{aligned}$$

отображение $\varphi_{R,S}$ определено корректно. Так как произвольный элемент xR фактор-группы A/R входит в подгруппу HR/R тогда и только тогда, когда $x \in HR$, т. е. $x = hr$ для некоторых элементов $h \in H$ и $r \in R$, то $xR = hR$, так что $HR/R = \big\{hR \bigm| h \in H\big\}$. Аналогично $KS/S = \big\{kS \bigm| k \in K\big\}$. Следовательно, отображение $\varphi_{R,S}$ правилом (6) определено для любого элемента подгруппы HR/R и потому действительно является отображением, причем сюръективным, подгруппы HR/R фактор-группы A/R на подгруппу KS/S фактор-группы B/S.

Если предположить, что для некоторых элементов h_1 и h_2 подгруппы H выполнено равенство $(h_1R)\varphi_{R,S} = (h_2R)\varphi_{R,S}$, т. е., в соответствии с (6), равенство $(h_1\varphi)S = (h_2\varphi)S$, то будем иметь, очевидно, $(h_1^{-1}h_2)\varphi \in K \cap S$.

Так как $K \cap S = (H \cap R)\varphi$, отсюда следует, что $(h_1^{-1}h_2)\varphi = h\varphi$ для некоторого $h \in H \cap R$, откуда в силу инъективности φ вытекает, что $h_1^{-1}h_2 = h$, и, поскольку $h \in R$, имеем $h_1R = h_2R$. Этим доказана инъективность отображения $\varphi_{R,S}$. Его гомоморфность проверяется непосредственно.

Из предложения 5.4.1 следует, что для любых групп A и B с подгруппами $H \leqslant A$ и $K \leqslant B$ и изоморфизмом $\varphi\colon H \to K$ и для произвольных нормальных (H, K, φ)-совместимых подгрупп $R \leqslant A$ и $S \leqslant B$ наряду с группой $G = \bigl(A * B;\ H = K, \varphi\bigr)$ мы можем построить свободное произведение

$$G_{R,S} = \bigl(A/R * B/S;\ HR/R = KS/S,\ \varphi_{R,S}\bigr)$$

групп A/R и B/S с подгруппами HR/R и KS/S, объединенными в соответствии с изоморфизмом $\varphi_{R,S}$. В следующем утверждении предполагается, что в каждую из групп G и $G_{R,S}$ свободные множители вложены естественным образом.

5.4.2. Теорема. *Пусть A и B — некоторые группы с изоморфными подгруппами $H \leqslant A$ и $K \leqslant B$ и $\varphi\colon H \to K$ — изоморфизм. Предположим также, что R и S — нормальные (H, K, φ)-совместимые подгруппы групп A и B соответственно. Тогда существует гомоморфизм $\rho_{R,S}$ группы $G = \bigl(A * B;\ H = K, \varphi\bigr)$ на группу*

$$G_{R,S} = \bigl(A/R * B/S;\ HR/R = KS/S,\ \varphi_{R,S}\bigr),$$

действие которого на подгруппе A совпадает с действием естественного гомоморфизма A на фактор-группу A/R и действие на подгруппе B совпадает с действием естественного гомоморфизма B на фактор-группу B/S. Ядро гомоморфизма $\rho_{R,S}$ совпадает с нормальным замыканием в группе G подмножества $R \cup S$.

Доказательство. В силу следствия 5.1.3 для доказательства того, что гомоморфизм $\rho_{R,S}$ с указанными свойствами существует, достаточно заметить, что естественные отображения σ группы A на фактор-группу A/R и τ группы B на фактор-группу B/S согласованы с изоморфизмом φ. Это действительно имеет место, так как для произвольного элемента $h \in H$ по определению естественного гомоморфизма имеем $h\sigma = hR$ и $h(\varphi\tau) = (h\varphi)S = (hR)\varphi_{R,S}$, а равенство $hR = (hR)\varphi_{R,S}$ входит в систему определяющих соотношений группы $G_{R,S}$.

Очевидно, что каждая из подгрупп R и S лежит в ядре $\operatorname{Ker}\rho_{R,S}$ гомоморфизма $\rho_{R,S}$, так что нормальное замыкание C их объединения $R \cup S$ содержится в $\operatorname{Ker}\rho_{R,S}$.

Наоборот, пусть неединичный элемент $g \in G$ с несократимой записью $g = x_1x_2 \cdots x_n$ входит в подгруппу $\operatorname{Ker}\rho_{R,S}$. Если $n = 1$, то элемент g входит в одну из подгрупп A или B, и так как отображение $\rho_{R,S}$ на этих подгруппах действует как соответствующий естественный гомоморфизм, равенство $g\rho_{R,S} = 1$ означает, что g входит в R или S соответственно. Таким образом, при $n = 1$ элемент g принадлежит подгруппе C.

Если $n > 1$, то сомножители записи $(x_1\rho_{R,S})(x_2\rho_{R,S}) \cdots (x_n\rho_{R,S})$ элемента $u = g\rho_{R,S}$ принадлежат попеременно подгруппам A/R и B/S группы $G_{R,S}$. Поскольку $u = 1$, из теоремы 5.2.2 следует, что эта запись не может быть несократимой, т. е. хотя бы один из ее сомножителей $x_i\rho_{R,S}$ должен входить в объединяемую подгруппу. Предположим, что $x_i \in A$ (случай $x_i \in B$ рассматривается аналогично). Поскольку тогда $x_i\rho_{R,S} = x_i\sigma = x_iR$ и $x_i\rho \in HR/R$, для некоторого $h \in H$ имеем $x_i \equiv h \pmod R$ и, следовательно, $x_i \equiv h \pmod C$. Пусть элемент g' получен из элемента g заменой в его несократимой записи сомножителя x_i на элемент h. Тогда $l(g') < l(g)$ и $g' \equiv g \pmod C$. Кроме того, $g' \in \operatorname{Ker}\rho_{R,S}$, так как $C \subseteq \operatorname{Ker}\rho_{R,S}$ и $g \in \operatorname{Ker}\rho_{R,S}$. Поэтому по индукции можно считать, что $g' \in C$. Следовательно, $g \in C$, и включение $\operatorname{Ker}\rho_{R,S} \subseteq C$ также доказано.

Таким образом, $\operatorname{Ker}\rho_{R,S} = C$, и теорема 5.4.2 доказана.

Поскольку действие гомоморфизма $\rho_{R,S}$ на подгруппе A группы G совпадает с действием естественного гомоморфизма A на фактор-группу A/R, имеем $A \cap \operatorname{Ker}\rho_{R,S} = R$ и, аналогично, $B \cap \operatorname{Ker}\rho_{R,S} = S$. Таким образом, справедливо

5.4.3. Следствие. *Для любых групп A и B с изоморфными подгруппами $H \leqslant A$ и $K \leqslant B$ и изоморфизмом $\varphi\colon H \to K$ и для любых нормальных (H, K, φ)-совместимые подгрупп R и S групп A и B соответственно существует нормальная подгруппа N группы $G = \bigl(A * B;\ H = K, \varphi\bigr)$ такая, что $A \cap N = R$ и $B \cap N = S$.*

Имеет место и обратное утверждение:

5.4.4. Предложение. *Для любой нормальной подгруппы N группы $G = \bigl(A * B;\ H = K, \varphi\bigr)$ пересечения $R = A \cap N$ и $S = B \cap N$ являются нормальными (H, K, φ)-совместимыми подгруппами групп A и B. Поэтому произвольный гомоморфизм группы G в какую-либо группу проходит через некоторый гомоморфизм вида $\rho_{R,S}$.*

Для доказательства (H, K, φ)-совместимости подгрупп R и S нам следует лишь установить справедливость равенства $(H \cap R)\varphi = K \cap S$.

Если элемент b группы B принадлежит образу при отображении φ подгруппы $H \cap R$, то $b = h\varphi$ для некоторого $h \in H \cap R$. Тогда $b \in K$, а так как в группе G выполнено равенство $h = h\varphi$, имеем $b = h$, так что $b \in N$ (поскольку $H \cap R \subseteq R \subseteq N$). Следовательно, $b \in K \cap N = K \cap B \cap N = K \cap S$. Таким образом, имеет место включение $(H \cap R)\varphi \subseteq K \cap S$.

Обратно, если $b \in K \cap S$, то $b = h\varphi$ для некоторого $h \in H$. Так как тогда $h = b$, имеем $h \in H \cap N = H \cap A \cap N = H \cap R$, откуда $b \in (H \cap R)\varphi$, и противоположное включение также справедливо.

Итак, (H, K, φ)-совместимость подгрупп R и S доказана, а нормальность каждой из них в соответствующем свободном множителе группы G очевидна. Остается заметить, что поскольку ядро гомоморфизма $\rho_{R,S} : G \to G_{R,S}$ содержится, очевидно, в подгруппе N, существует гомоморфизм τ группы $G_{R,S}$ на фактор-группу G/N такой, что естественный гомоморфизм группы G на фактор-группу G/N совпадает с произведением $\rho_{R,S}\tau$.

Отметим еще практически очевидное

5.4.5. Предложение. *Пусть A и B — некоторые группы с изоморфными подгруппами $H \leqslant A$ и $K \leqslant B$ и $\varphi\colon H \to K$ — изоморфизм. Пусть $\{(R_\lambda, S_\lambda)\}_{\lambda\in\Lambda}$ — некоторое семейство пар (H, K, φ)-совместимых подгрупп групп A и B (т. е. для каждого $\lambda \in \Lambda$ подгруппы $R_\lambda \leqslant A$ и $S_\lambda \leqslant B$ (H, K, φ)-совместимы). Тогда подгруппы $R = \bigcap_{\lambda\in\Lambda} R_\lambda$ и $S = \bigcap_{\lambda\in\Lambda} S_\lambda$ также являются (H, K, φ)-совместимыми.*

5.5. Внутреннее определение свободного произведения двух групп с объединенной подгруппой. Отождествление групп A и B с соответствующими подгруппами группы $G = \bigl(A * B;\ H\bigr)$, естественно приводит к вопросу о внутреннем определении свободного произведения двух групп с объединенной подгруппой. А именно, если T — некоторая группа с подгруппами A и B, спрашивается, при каких условиях эти подгруппы являются свободными сомножителями группы T, т. е., говоря подробнее, при каких условиях существует изоморфизм некоторой группы $G = \bigl(A * B;\ H = K, \varphi\bigr)$ на группу T, при котором подгруппы A и B группы G переходят соответственно в подгруппы A и B группы T?

Поскольку группа $G = \bigl(A * B;\ H = K, \varphi\bigr)$ порождается подгруппами A и B, для существования такого изоморфизма следует предполагать, прежде всего, что группа T порождается подгруппами A и B. Тогда произвольный элемент $x \in T$ совпадает с некоторым произведением элементов этих подгрупп, причем можно, очевидно, считать без потери общности, что если число сомножителей в таком произведении больше 1, то любые соседние сомножители не входят в одну и ту же подгруппу A или B. Такое выражение элемента x через элементы подгрупп A и B естественно называть *несократимым произведением*.

5.5.1. Теорема. *Пусть группа T порождается двумя своими подгруппами A и B. Если каждый элемент группы T, представимый несократимым произведением, число сомножителей в котором больше 1, отличен от единичного элемента, то группа T изоморфна свободному произведению групп A и B с объединенной подгруппой $H = A \cap B$.*

Для доказательства этого утверждения следует ввести в рассмотрение некоторые группы A_1 и B_1, изоморфные группам A и B соответственно, и зафиксировать изоморфизмы $\sigma : A_1 \to A$ и $\tau : B_1 \to B$. Если H_1 — прообраз подгруппы H относительно σ и K_1 — прообраз подгруппы H относительно τ, то полагая $h\varphi = (h\sigma)\tau^{-1}$ для произвольного $h \in H_1$, мы получаем изоморфизм φ подгруппы H_1 группы A_1 на подгруппу K_1 группы B_1. Так как отображения σ и τ согласованы, очевидно, с изоморфизмом φ, ввиду следствия 5.1.3 существует продолжающий их гомоморфизм ρ группы $G = \big(A_1 * B_1;\ H_1 = K_1, \varphi\big)$ в группу T. Сюръективность отображения ρ очевидна, поскольку группа G порождается подгруппами A и B, лежащими в образе этого отображения. Пусть элемент $g \in G$ с несократимой записью $g = x_1 x_2 \cdots x_s$ принадлежит ядру гомоморфизма ρ. Если $s > 1$, то запись элемента $g\rho$ в виде произведения ρ-образов элементов x_1, x_2, …, x_s является, как легко видеть, несократимой в группе T, и потому $g\rho \neq 1$. Таким образом, $s = 1$, т. е. элемент g лежит в одной из подгрупп A_1 или B_1, и так как действие ρ на этот элемент совпадает с действием одного из изоморфизмов σ или τ, $g = 1$. Следовательно, ρ — изоморфизм, и теорема 5.5.1 доказана.

С помощью этой теоремы легко доказать следующее утверждение, являющееся некоторым уточнением теоремы Х. Нейман (см., напр., [5, с. 512]).

5.5.2. Теорема. *Пусть $G = \big(A * B;\ H\big)$ — свободное произведение групп A и B с объединенной подгруппой H. Пусть A' и B' — такие подгруппы групп A и B соответственно, что $A' \cap H = B' \cap H$. Тогда подгруппа G' группы G, порожденная подгруппами A' и B', является* *свободным произведением групп A' и B' с объединенной подгруппой $H' = A' \cap H$. Кроме того, $A \cap G' = A'$ и $B \cap G' = B'$.*

Доказательство. Отметим, прежде всего, что

$$A' \cap B' = A' \cap A \cap B \cap B' = A' \cap H \cap B' = H'.$$

Легко видеть, далее, что для любого неединичного элемента g из подгруппы G' равное этому элементу несократимое произведение $x_1 x_2 \cdots x_r$ элементов множества $A' \cup B'$, порождающего группу G', является несократимой записью в группе G: при $r = 1$ это просто очевидно, а при $r > 1$ сомножители x_i принадлежат поочередно подгруппам A' и B', а потому — подгруппам A и B, и ни один из этих сомножителей не входит в подгруппу H', а потому не входит и в подгруппу H. Поэтому первое утверждение теоремы 5.5.2 вытекает непосредственно из теорем 5.2.2 и 5.5.1.

Если элемент $a \in A$ принадлежит подгруппе G', то ввиду замечания из предыдущего абзаца представляющее его несократимое произведение в этой подгруппе должно состоять из единственного сомножителя, который, как легко видеть, должен принадлежать подгруппе A': если $a \in B'$, то $a \in A \cap B' = A \cap B \cap B' = H \cap B' = H \cap A'$. Таким образом, $A \cap G' \subseteq A'$, и так как противоположное включение очевидно, равенство $A \cap G' = A'$ доказано. Равенство $B \cap G' = B'$ доказывается аналогично.

5.6. Обычное свободное произведение двух групп. Если в свободном произведении $G = \big(A * B;\ H = K, \varphi\big)$ групп A и B объединяемые подгруппы H и K являются единичными, группа G называется (обычным) *свободным произведением* групп A и B и записывается в виде $G = A * B$.

Разумеется, в этом частном случае конструкции свободного произведения двух групп с объединенными подгруппами все введенные в предыдущих разделах понятия и доказанные утверждения остаются справедливыми и, более того, приобретают более компактную и усиленную формулировку.

Так, группы A и B естественным образом вложимы в группу $G = A * B$ и $A \cap B = 1$. Каждый элемент $g \neq 1$ этой группы представим несократимой записью, которая здесь является произведением вида $g = x_1 x_2 \cdots x_s$, где элементы x_1, x_2, ..., x_s принадлежат поочередно подгруппам A и B, причем при $s > 1$ каждый из них отличен от единицы. Из предложения 5.2.3 следует

5.6.1. Предложение. *Каждый элемент свободного произведения $G = A * B$ групп A и B обладает единственной несократимой записью.*

Утверждение следствия 5.1.3 применительно к группе $G = A * B$ формулируется следующим образом:

5.6.2. Предложение. *Для любых гомоморфизмов σ и τ групп A и B в некоторую группу T существует гомоморфизм ρ группы $G = A * B$ в группу T, действие которого на подгруппе A совпадает с действием гомоморфизма σ и действие на подгруппе B совпадает с действием τ.*

Полученное в теореме 5.3.1 описание сопряженных элементов здесь принимает следующий вид:

5.6.3. Предложение. *Каждый элемент группы $G = A * B$ сопряжен с некоторым циклически несократимым элементом. Если длины двух циклически несократимых элементов группы G различны, то эти элементы не являются сопряженными. Циклически несократимые элементы длины 1 сопряжены в группе G тогда и только тогда, когда они лежат в одном и том же свободном множителе и сопряжены в нем. Циклически несократимые элементы, длина которых больше 1, сопряжены в группе G тогда и только тогда, когда один из них является циклической перестановкой другого.*

5.7. Обобщенное свободное произведение произвольного семейства групп. До сих пор нами рассматривалось свободное произведение двух групп с объединенными подгруппами. Более общая конструкция свободного произведения произвольного семейства групп может быть определена следующим образом.

Пусть Γ — граф с множеством вершин $V(\Gamma)$ и множеством ребер $E(\Gamma)$, любые две смежные вершины u и v которого различны и соединены единственным ребром (u, v). Предположим, что каждой вершине $v \in V(\Gamma)$ поставлена в соответствие некоторая группа G_v и для любых двух смежных вершин $u, v \in V(\Gamma)$ фиксированы подгруппы $H_{uv} \leqslant G_u$ и $H_{vu} \leqslant G_v$ и изоморфизм $\varphi_{uv} \colon H_{uv} \to H_{vu}$, причем $\varphi_{uv} = \varphi_{vu}^{-1}$. Предположим также, что каждая группа G_v задана множеством порождающих X_v и определяющих слов W_v (где при $u \neq v$ $X_u \cap X_v = \emptyset$). Пусть

$$G = \bigl(\Pi^*_{v \in V(\Gamma)} G_v;\ H_{uv} = H_{vu}, \varphi_{uv}\ ((u, v) \in E(\Gamma))\bigr) \qquad (7)$$

— группа, заданная представлением с множеством порождающих $X = \bigcup_{v\in V(\Gamma)} X_v$, множеством определяющих слов $W = \bigcup_{v\in V(\Gamma)} W_v$ и множеством всевозможных соотношений вида $h = h\varphi_{uv}$ для любого ребра $(u, v) \in E(\Gamma)$ и любого $h \in H_{uv}$. Если для каждой вершины $v \in V(\Gamma)$ гомоморфизм группы G_v в группу G, продолжающий тождественное вложение множества X_v в множество X, инъективен, то группу G будем называть (соответствующим графу Γ) *обобщенным свободным произведением семейства групп* $\bigl(G_v\bigr)_{v\in V(\Gamma)}$ *с объединенными в соответствии с изоморфизмами* φ_{uv} *подгруппами* H_{uv} *и* H_{vu} *(*$(u, v) \in E(\Gamma)$*)*.

Таким образом, введенное выше (в разделе 5.1) свободное произведение $G = \bigl(A * B;\ H = K, \varphi\bigr)$ двух групп с объединенными подгруппой является обобщенным свободным произведением, соответствующим графу с одним ребром и двумя (различными) вершинами. В отличие от этого частного случая, обобщенное свободное произведение, построенное по другим графам, существует далеко не всегда. Приведем соответствующий пример этого (см. [5, с. 548]).

Для построения примера используется группа $K = \langle a,\, b;\ a^{-1}ba = b^2\rangle$ с одним определяющим соотношением, входящая в семейство так называемых групп Баумслага – Солитэра. Можно показать, что эта группа не имеет кручения; в частности (см. пример 2 из раздела 2.3), циклические подгруппы, порождаемые элементами a и b, бесконечны. Отметим также, что очевидная индукция показывает, что для любого целого числа $n > 0$ соотношение $a^{-n}ba^n = b^{2^n}$ выводимо из соотношения $a^{-1}ba = b^2$.

Пример. *Пусть граф* Γ *является треугольником с вершинами* $1, 2, 3$. *Сопоставим вершине с номером* $i = 1,\, 2,\, 3$ *группу*

$$G_i = \langle x_i,\, y_i;\ x_i^{-1}y_ix_i = y_i^2\rangle.$$

Пусть также $H_{i,i+1}$ *— подгруппа группы* G_i*, порожденная элементом* y_i*, и* $H_{i+1,i}$ *— подгруппа группы* G_{i+1}*, порожденная элементом* x_{i+1}*, и пусть* $\varphi_{i,i+1}$ *— изоморфизм группы* $H_{i,i+1}$ *на группу* $H_{i+1,i}$*, определяемый отображением* $y_i \mapsto x_{i+1}$ *(где индексы приведены по модулю 3). Тогда группа*

$$G = \langle x_i,\, y_i\, (i = 1,\, 2,\, 3); \\ x_i^{-1}y_ix_i = y_i^2\, (i = 1,\, 2,\, 3),\ y_1 = x_2,\ y_2 = x_3,\ y_3 = x_1\rangle$$

является единичной.

Действительно, применяя к этому представлению группы G очевидные преобразования Тице и меняя обозначения (на более удобные), приходим к представлению

$$G = \langle a,\, b,\, c;\ a^{-1}ba = b^2,\ b^{-1}cb = c^2,\ c^{-1}ac = a^2\rangle.$$

Из соотношений $a^{-2}ba^2 = b^4$ и $c^{-1}ac = a^2$ получаем $c^{-1}a^{-1}cba^2 = b^4$. Последовательно используя вытекающие из определяющих соотношений равенства $cb = bc^2$, $a^{-1}b = b^2a^{-1}$ и $c^{-1}b^2 = b^2c^{-4}$, имеем

$$c^{-1}a^{-1}cb = c^{-1}a^{-1}bc^2 = c^{-1}b^2a^{-1}c^2 = b^2c^{-4}a^{-1}c^2,$$

и так как $a^{-1}c^2 = c^2a^{-4}$, отсюда следует, что $c^{-1}a^{-1}cb = b^2c^{-2}a^{-4}$. Поэтому равенство $c^{-1}a^{-1}cba^2 = b^4$ принимает вид $a^2c^2b^2 = 1$. Отсюда $b^{-1}a^2c^2b = a^2c^2$, т. е. $a^{-2}b^{-1}a^2c^2b = c^2$, и так как

$$a^{-2}b^{-1}a^2c^2b = b^{-4}c^2b = b^{-4}bc^4b^{-3}c^4,$$

имеем $b^3 = c^2$. Следовательно, элементы b и c^2 перестановочны, и потому из соотношения $b^{-1}cb = c^2$ следует, что $c = 1$. Теперь из соотношений $c^{-1}ac = a^2$ и $a^{-1}ba = b^2$ получаем $a = 1$ и $b = 1$.

(Заметим (см. [5]), что если граф является квадратом, вершинам которого поставлены в соответствие группы, изоморфные группе K, и объединяемые подгруппы определены аналогично, то обобщенное свободное произведение G этих четырех групп существует.)

С другой стороны, в работе А. Карраса и Д. Солитэра [6] показано, что если граф Γ является деревом, то группа (7) является обобщенным свободным произведением. Следуя [6], будем называть ее *древесным произведением* семейства групп $\left(G_v\right)_{v\in V(\Gamma)}$ с указанными объединениями. Основные свойства этой теоретико-групповой конструкции, доказанные в [6], формулируются следующим образом:

5.7.1. Теорема. *Пусть граф Γ является деревом и пусть G — древесное произведение семейства групп $\left(G_v\right)_{v\in V(\Gamma)}$ с объединенными в соответствии с изоморфизмами φ_{uv} подгруппами $H_{uv} \leqslant G_u$ и $H_{vu} \leqslant G_v$ $((u,v) \in E(\Gamma))$. Тогда справедливы следующие утверждения:*

1. *Для каждой вершины $v \in V(\Gamma)$ группа G_v вложима естественным образом в группу G.*

2. *Для любого поддерева Γ' дерева Γ подгруппа G' группы G, порожденная семейством подгрупп $\left(G_v\right)_{v\in V(\Gamma')}$, является древесным произведением групп этого семейства с теми же объединениями. В частности, для любых двух смежных вершин u и v графа Γ подгруппа G', порожденная подгруппами G_u и G_v является свободным произведением групп G_u и G_v с подгруппами H_{uv} и H_{vu}, объединенными в соответствии с изоморфизмом φ_{uv}.*

3. *Пусть снова Γ' — поддерево дерева Γ и G' — подгруппа группы G, порожденная семейством подгрупп $\left(G_v\right)_{v\in V(\Gamma')}$. Пусть также v — вершина дерева Γ, не входящая в поддерево Γ' и смежная с некоторой вершиной $u \in V(\Gamma')$. Тогда подгруппа L группы G, порожденная подгруппами G' и G_v является свободным произведением групп G' и G_v с подгруппами H_{uv} и H_{vu}, объединенными в соответствии с изоморфизмом φ_{uv}, $L = \left(G' * G_v;\ H_{uv} = H_{vu}, \varphi_{uv}\right)$.*

Предположим, что дерево Γ является звездой, т. е. существует вершина $u \in V(\Gamma)$, смежная с любой другой вершиной этого дерева. Если, к тому же, для любой вершины $v \in V(\Gamma) \setminus \{u\}$ подгруппа H_{uv} совпадает с некоторой, одной и той же, подгруппой H группы G_u, соответствующее древесное произведение G будем называть *свободным произведением семейства групп $\left(G_v\right)_{v\in V(\Gamma)}$ с одной объединенной подгруппой* и для его обозначения использовать запись $G = \left(\Pi^*_{v\in V(\Gamma)} G_v;\ H\right)$. Определенные выше для обобщенного свободного произведения двух групп понятия несократимой записи, длины и циклически несократимого элемента практически дословно распространяются на общий случай. В этом случая являются справедливыми (при подходящей переформулировке) и доказанные там утверждения.

Легко видеть, что элементы произвольного непустого множества можно считать вершинами некоторой звезды. Поэтому можно говорить о свободном произведении с одной объединенной единичной подгруппой произвольного семейства групп $\left(G_i\right)_{i\in I}$. Для этой конструкции, называемой, как и в случае двух свободных сомножителей, (обычным) свободным произведением групп и обозначаемой символом $G = \Pi^*_{i\in I} G_i$, справедливы (в соответствующей формулировке) все утверждения, содержащиеся в разделе 5.6.

Если множество I конечно и $I = \{1, 2, \ldots, n\}$, то для обозначения свободного произведения G такого семейства групп используют также (снова, как в случае двух сомножителей) запись $G = G_1 * G_2 * \cdots * G_n$. Из пункта 3 теоремы 5.7.1 следует, что при $n > 2$ имеет место равенство $G_1 * G_2 * \cdots * G_n = (G_1 * G_2 * \cdots * G_{n-1}) * G_n$; это позволяет использовать индукцию по числу свободных сомножителей.

Отметим также, что свободная группа $F = F(a_1, a_2, \ldots, a_n)$ с множеством свободных порождающих $\{a_1, a_2, \ldots, a_n\}$ является свободным произведением n бесконечных циклических групп,

$$F = A_1 * A_2 * \cdots * A_n,$$

где A_1, A_2,..., A_n — бесконечные циклические группы, порождаемые элементами a_1, a_2,..., a_n соответственно.

§ 6. HNN-расширения групп

В этом параграфе рассматривается еще одна теоретико-групповая свободная конструкция — расширение Хигмана – Неймана – Нейман или, короче, HNN-расширение.

6.1. Определение и начальные свойства HNN-расширений групп. Пусть G — некоторая группа с изоморфными подгруппами A и B и $\varphi\colon A \to B$ — фиксированный изоморфизм группы A на группу B. Если группа G задана представлением

$$G = \langle x_1, x_2, \ldots, x_r;\ W\rangle, \tag{1}$$

то группа G^*, задаваемая представлением

$$G^* = \langle x_1, x_2, \ldots, x_r, t;\ W,\ t^{-1}at = a\varphi\ (a \in A)\rangle, \tag{2}$$

множество порождающих символов которого состоит из порождающих символов представления (1) и еще одного символа t, а множество определяющих слов и соотношений состоит из множества слов W и всевозможных соотношений вида $t^{-1}at = b$, где a — слово от порождающих $x_1, x_2, \ldots, x_n$, определяющее в группе G элемент подгруппы A, а b — слово от порождающих $x_1, x_2, \ldots, x_r$, определяющее элемент подгруппы B, являющийся образом элемента a при отображении φ, называется *HNN-расширением группы G с проходной буквой t и связанными в соответствии с изоморфизмом φ подгруппами A и B*. Для обозначения этого будем записывать $G^* = \big(G, t;\ t^{-1}At = B, \varphi\big)$, а группу G называть *базовой группой HNN-расширения*.

Изучение свойств этой конструкции, как и в случае обобщенного свободного произведения двух групп, начнем с формулировки утверждения о продолжаемости гомоморфизмов.

6.1.1. Теорема. *Пусть $G^* = \big(G, t;\ t^{-1}At = B, \varphi\big)$ — заданное представлением (2) HNN-расширение группы G с проходной буквой t и связанными в соответствии с изоморфизмом φ подгруппами A и B. Пусть ρ — гомоморфизм группы G в некоторую группу H, причем в группе H имеется элемент h такой, что для любого $a \in A$ выполнено равенство $h^{-1}(a\rho)h = (a\varphi)\rho$. Тогда существует гомоморфизм θ группы G^* в группу H такой, что $t\theta = h$ и $x_i\theta = x_i\rho$ для любого $i = 1, 2, \ldots, r$.*

Доказательство этой теоремы проводится аналогично доказательству теоремы 5.1.1 с использованием теоремы 2.3.1.

Из теоремы 2.3.1 следует также, что тождественное отображение множества $\{x_1, x_2, \ldots, x_r\}$ порождающих символов представления (1) группы G в множество порождающих символов группы G^*, определяемой представлением (2), продолжаемо до гомоморфизма группы G в группу G^*. Следующее свойство конструкции HNN-расширения состоит в том, что этот гомоморфизм является инъективным.

6.1.2. Теорема. *Пусть $G^* = \big(G, t;\, t^{-1}At = B, \varphi\big)$ — заданное представлением* (2) *HNN-расширение группы G с проходной буквой t и связанными в соответствии с изоморфизмом φ подгруппами A и B. Тогда гомоморфизм группы G в группу G^*, продолжающий тождественное отображение множества $\{x_1, x_2, \ldots, x_r n\}$ порождающих группы G на соответствующее подмножество множества порождающих символов представления* (2)*, является вложением группы G в группу G^*.*

Теорема 6.1.2 является почти очевидным следствием теоремы 6.1.1 и следующего утверждения, доказанного Ф. Холлом (см. [5, стр. 537 –538]):

6.1.3. Предложение. *Для любой группы G с изоморфными подгруппами A и B и изоморфизмом $\varphi\colon A \to B$ существует вложение ρ группы G в некоторую группу H, содержащую такой элемент h, что для любого $a \in A$ выполнено равенство $h^{-1}(a\rho)h = (a\varphi)\rho$.*

Для доказательства теоремы 6.1.2 заметим, прежде всего, что из теоремы 6.1.1 следует, очевидно, что если ρ — вложение базовой группы G HNN-расширения $G^* = \big(G, t;\, t^{-1}At = B, \varphi\big)$ в некоторую группу H с таким элементом h, что для любого $a \in A$ выполнено равенство $h^{-1}(a\rho)h = (a\varphi)\rho$, то существует гомоморфизм θ группы G^* в группу H такой, что $t\theta = h$ и $x_i\theta = x_i\rho$ для любого $i = 1, 2, \ldots, n$. Далее, обозначим через τ гомоморфизм группы G в группу G^*, продолжающий тождественное отображение множества $\{x_1, x_2, \ldots, x_r\}$ порождающих группы G на соответствующее подмножество множества порождающих символов представления (2). Так как для любого $i = 1, 2, \ldots, n$ выполнено равенство $x_i(\tau\theta) = x_i\rho$, отображения $\tau\theta$ и ρ группы G в группу H совпадают. Инъективность отображения τ следует поэтому из инъективности отображения ρ.

Утверждение теоремы 6.1.2 означает, что подгруппа группы G^*, порожденная множеством $\{x_1, x_2, \ldots, x_r\}$, изоморфна группе G, и потому мы можем (и будем, когда это удобно) считать, что она совпадает с G (и говорить, что базовая группа G HNN-расширения G^* естественным образом вложена в группу G^*). При этом соглашении и утверждение теоремы 6.1.1 допускает более определенную формулировку:

6.1.4. Следствие. *Пусть* $G^* = \big(G, t;\, t^{-1}At = B, \varphi\big)$ *— заданное представлением* (2) HNN*-расширение группы* G *с проходной буквой* t *и связанными в соответствии с изоморфизмом* φ *подгруппами* A *и* B *и пусть группа* G *вложена в группу* G^* *естественным образом. Для любого гомоморфизма* ρ *группы* G *в некоторую группу* H*, содержащую такой элемент* h*, что для каждого* $a \in A$ *выполнено равенство* $h^{-1}(a\rho)h = (a\varphi)\rho$*, существует гомоморфизм* θ *группы* G^* *в группу* H*, при котором элемент* t *группы* G^* *переходит в элемент* h *и действие которого на подгруппе* G *совпадает с действием гомоморфизма* ρ*.*

6.2. Приведенная запись элементов HNN-расширения. Из определения (2) группы $G^* = \big(G, t;\, t^{-1}At = B, \varphi\big)$ следует, что произвольный элемент g этой группы может быть записан в виде

$$g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n, \tag{3}$$

где $n \geqslant 0$, $\varepsilon_i = \pm 1$ $(i = 1, 2, \ldots, n)$ и g_0, g_1, $\ldots$, g_n — слова от порождающих $x_1, x_2, \ldots, x_r$. Если при $n \geqslant 2$ для некоторого номера $i < n$ имеют место равенства $\varepsilon_i = -1$, $\varepsilon_{i+1} = 1$ и слово g_i определяет элемент из подгруппы A, то используя выполненное в группе G^* соотношение $t^{-1}g_i t = g_i'$ (где слово g_i' определяет образ относительно отображения φ элемента, определяемого словом g_i), мы можем преобразовать запись (3) элемента g в запись того же элемента, имеющую вид

$$g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots t^{\varepsilon_{i-1}} (g_{i-1} g_i' g_{i+1}) t^{\varepsilon_{i+2}} \cdots g_{n-1} t^{\varepsilon_n} g_n.$$

Аналогичное преобразование может быть выполнено, если $\varepsilon_i = 1$, $\varepsilon_{i+1} = -1$ и слово g_i определяет элемент из подгруппы B (а слово g_i' определяет прообраз относительно отображения φ элемента, определяемого словом g_i). Поскольку такие преобразования (называемые t*-редукциями*) уменьшает на 2 число вхождений буквы t в запись элемента g, произвольный элемент $g \in G^*$ обладает записью вида (3), к которой неприменимы никакие t-редукции. Такая запись элементов группы G^* называется *приведенной.*

Говоря более подробно, запись (3) элемента $g \in G^*$ называется приведенной, если либо $n = 0$, либо $n = 1$, либо $n \geqslant 2$ и для любого $i = 1, 2, \ldots, n-1$ из того, что $\varepsilon_i + \varepsilon_{i+1} = 0$, следует, что при $\varepsilon_i = -1$ слово g_i определяет элемент группы G, не принадлежащий подгруппе A, а при $\varepsilon_i = 1$ слово g_i определяет элемент группы G, не принадлежащий подгруппе B.

Предыдущие рассуждения доказывают справедливость следующего утверждения:

6.2.1. Предложение. *Каждый элемент HNN-расширения $G^* = \bigl(G, t;\ t^{-1}At = B, \varphi\bigr)$ обладает приведенной записью.*

Важное свойство конструкции HNN-расширения, называемое леммой Бриттона, формулируется следующим образом:

6.2.2. Теорема. *Произвольный элемент группы*

$$G^* = \bigl(G, t;\ t^{-1}At = B, \varphi\bigr),$$

обладающий приведенной записью вида (3)*, где $n \geqslant 1$, отличен от единицы.*

Эта теорема, как и теорема 5.2.2, приводится здесь без доказательства. Доказательство этих теорем можно найти в книге 2.

Предположение о том, что базовая группа G HNN-расширения $G^* = \bigl(G, t;\ t^{-1}At = B, \varphi\bigr)$ естественным образом вложена в группу G^*, позволяет считать, что в записи вида (3) элемента g группы G^* участвуют не слова от порождающих $x_1, x_2, \ldots, x_r$, а элементы g_0, g_1, …, g_n группы G. Поскольку для любого элемента a подгруппы A в группе G^* выполнено равенство $t^{-1}at = a\varphi$, и для любого элемента b подгруппы B в группе G^* выполнено равенство $tbt^{-1} = b\varphi^{-1}$, t-редукции состоят теперь просто в замене левой части соответствующего равенства его правой частью. Кроме того, в этом случае приведенность записи (3) элемента $g \in G^*$ означает, что при $n \geqslant 2$ для любого $i = 1, 2, \ldots, n-1$ из того, что $\varepsilon_i + \varepsilon_{i+1} = 0$, следует, что при $\varepsilon_i = -1$ элемент g_i не принадлежит подгруппе A и при $\varepsilon_i = 1$ этот элемент не принадлежит подгруппе B.

Из леммы Бриттона легко следует, что каждый элемент базовой группы G HNN-расширения обладает единственной приведенной записью, совпадающей с этим элементом.

В самом деле, если $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$ — приведенная запись элемента $g \in G$ и $n \geqslant 1$, то выполнено равенство

$$g_0' t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n = 1,$$

где $g_0' = g^{-1} g_0$, запись левой части которого является, очевидно, приведенной. Так как это противоречит лемме Бриттона, $n = 0$ и указанная запись элемента g имеет вид g_0, где $g_0 = g$.

В остальных случаях имеет место

6.2.3. Теорема. *Пусть* $G^* = \big(G, t;\, t^{-1}At = B, \varphi\big)$ *и пусть*

$$f = f_0 t^{\varepsilon_1} f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m \quad \text{и} \quad g = g_0 t^{\delta_1} g_1 t^{\delta_2} g_2 \cdots g_{n-1} t^{\delta_n} g_n$$

— приведенные записи ее элементов f и g, где $m \geqslant 1$ и $n \geqslant 1$. Равенство $f = g$ имеет место в группе G^* тогда и только тогда, когда $m = n$, $\varepsilon_i = \delta_i$ $(i = 1, 2, \ldots, n)$ и существует последовательность элементов c_0, c_1, $\ldots$, c_{2n-1} таких, что

$$\begin{aligned} &f_0 = g_0 c_0 \\ &f_i = c_{2i-1}^{-1} g_i c_{2i} \ (1 \leqslant i < n) \\ &f_n = c_{2n-1}^{-1} g_n, \end{aligned}$$

причем для любого $i = 0, 1, \ldots, n-1$ если $\varepsilon_{i+1} = 1$, то $c_{2i} \in A$, $c_{2i+1} \in B$ и $c_{2i}\varphi = c_{2i+1}$, а если $\varepsilon_{i+1} = -1$, то $c_{2i} \in B$, $c_{2i+1} \in A$ и $c_{2i+1}\varphi = c_{2i}$.

Доказательство. Если сформулированные условия выполнены, то поскольку тогда для любого $i = 0, 1, \ldots, n-1$ в группе G^* выполнено равенство $c_{2i} t^{\varepsilon_{i+1}} = t^{\varepsilon_{i+1}} c_{2i+1}$, имеем

$$\begin{aligned} f &= f_0 t^{\varepsilon_1} f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m \\ &= g_0 c_0 t^{\varepsilon_1} c_1^{-1} g_1 c_2 t^{\varepsilon_2} c_3^{-1} g_2 c_4 \cdots c_{2n-3}^{-1} g_{n-1} c_{2(n-1)} t^{\varepsilon_n} c_{2n-1}^{-1} g_n = g. \end{aligned}$$

Для доказательства необходимости условий, предполагая без потери общности, что $m \geqslant n$, воспользуемся индукцией по n. Перепишем равенство $f = g$ в виде

$$g_n^{-1} t^{-\delta_n} \cdots g_2^{-1} t^{-\delta_2} g_1^{-1} t^{-\delta_1} g_0^{-1} f_0 t^{\varepsilon_1} f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m = 1. \tag{4}$$

В силу леммы Бриттона запись левой части этого равенства не может быть приведенной. Так как записи элементов f и g являются приведенными, t-редукции в левой части (4) возможны лишь на стыке записей элементов g^{-1} и f. Это означает, что $\delta_1 = \varepsilon_1$ и элемент $c_0 = g_0^{-1} f_0$ принадлежит подгруппе A, если $\varepsilon_1 = 1$, или подгруппе B, если $\varepsilon_1 = -1$. Полагаем $c_1 = c_0\varphi$, если $\varepsilon_1 = 1$, и $c_1 = c_0\varphi^{-1}$, если $\varepsilon_1 = -1$. Тогда в любом случае $t^{-\delta_1} g_0^{-1} f_0 t^{\varepsilon_1} = c_1$, и при $n = 1$ равенство (4) принимает вид

$$g_1^{-1} c_1 f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m = 1.$$

Так как при $m > 1$ левая часть этого равенства является, очевидно, приведенной, что невозможно ввиду леммы Бриттона, имеем $m = 1$ и $f_1 = c_1^{-1} g_1$. Таким образом, при $n = 1$ выполнены равенства $m = n$ и $\varepsilon_1 = \delta_1$, а последовательность c_0, c_1 удовлетворяет требованиям формулировки предложения.

При $n > 1$ равенство (4), переписанное в виде

$$g_n^{-1} t^{-\delta_n} \cdots g_2^{-1} t^{-\delta_2} g_1^{-1} c_1 f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m = 1,$$

говорит о том, что элементы

$$f' = f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m \quad \text{и} \quad g' = g_1' t^{\delta_2} g_2 \cdots g_{n-1} t^{\delta_n} g_n,$$

где $g_1' = c_1^{-1} g_1$, совпадают. Поскольку указанные записи этих элементов приведены, по индуктивному предположению выполнены равенства $m - 1 = n - 1$, $\varepsilon_i = \delta_i$ $(i = 2, 3, \ldots, n)$ и существует последовательность элементов c_2, c_3, $\ldots$, c_{2n-1} таких, что

$$\begin{aligned} f_1 &= g_1' c_2 \\ f_i &= c a_{2i-1}^{-1} g_i c_{2i} \ (2 \leqslant i < n) \\ f_n &= c_{2n-1}^{-1} g_n, \end{aligned}$$

причем для произвольного $i = 1, 2, \ldots, n-1$ при $\varepsilon_{i+1} = 1$ $c_{2i} \in A$, $c_{2i+1} \in B$ и $c_{2i}\varphi = c_{2i+1}$, а при $\varepsilon_{i+1} = -1$ $c_{2i} \in B$, $c_{2i+1} \in A$ и $c_{2i+1}\varphi = c_{2i}$. Следовательно, для элементов f и g имеем $m = n$, для каждого $i = 1, 2, \ldots, n$ $\varepsilon_i = \delta_i$ и последовательность элементов c_0, c_1, $\ldots$, c_{2n-1} удовлетворяет требованиям формулировки предложения. Индуктивный шаг завершен, и теорема доказана.

Теорема 6.2.3 (вместе с замечанием после формулировки леммы Бриттона) говорит, в частности, о том, что любые две приведенные записи элемента $g \in G^*$ содержат одно и то же число вхождений проходной буквы t; это число будем называть *длиной элемента* g и обозначать через $l(g)$.

Таким образом, например, элемент $g \in G^*$ принадлежит подгруппе G тогда и только тогда, когда $l(g) = 0$.

6.3. Циклически приведенные элементы и сопряженность элементов HNN-расширения. Теорема 6.2.3 позволяет ввести еще одно понятие.

Элемент $g \in G^*$ с приведенной записью $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$ назовем *циклически приведенным*, если либо $n = 0$, либо $n = 1$, либо $n > 1$ и при $\varepsilon_1 + \varepsilon_n = 0$ элемент $g_n g_0$ не принадлежит подгруппе A, если $\varepsilon_n = -1$, и не принадлежит подгруппе B, если $\varepsilon_n = 1$. Так как из теоремы 6.3.1 легко следует, что любые две приведенные записи данного элемента удовлетворяют или не удовлетворяют сформулированным требованиям одновременно, это определение корректно.

Отметим, что если элемент $g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$ группы $g \in G^*$ является циклически приведенным длины $n \geqslant 1$, то для любого целого числа $k > 0$ к записи

$$g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n \\ \cdots g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$$

элемента g^k неприменимы t-редукции, и потому $l(g^k) = kl(g)$.

Понятие циклически приведенного элемента оказывается полезным при описании сопряженных элементов HNN-расширения.

6.3.1. Теорема. *Каждый элемент* g *группы*

$$G^* = \big(G, t;\ t^{-1}At = B, \varphi\big)$$

сопряжен с некоторым циклически приведенным элементом. Элемент, не сопряженный ни с каким элементом из подгруппы G, *сопряжен с циклически приведенным элементом вида* $t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$ $(n \geqslant 1)$. *Если два циклически приведенных элемента сопряжены в группе* G^*, *то их длины равны.*

Пусть f *и* g *— циклически приведенные элементы группы* G^*. *Тогда*

1. *Если хотя бы один из элементов* f *или* g *принадлежит подгруппе* G, *то эти элементы сопряжены в группе* G^* *тогда и только*

тогда, когда и другой содержится в G и если они не сопряжены в группе G, то для некоторого $r \geqslant 1$ существует последовательность чисел $\eta_1, \eta_2, \ldots, \eta_r$, равных ± 1, и существуют две последовательности $c_0, c_1, \ldots, c_{2r+1}$ и $d_0, d_1, \ldots, d_r$ элементов группы G такие, что

(1.1) *$c_0 = f$ и $c_{2r+1} = g$;*

(1.2) *для каждого $i = 0, 1, \ldots, r$ выполнено равенство $d_i^{-1} c_{2i} d_i = c_{2i+1}$;*

(1.3) *для любого $i = 1, 2, \ldots, r$ если $\eta_i = 1$, то $c_{2i-1} \in A$, $c_{2i} \in B$ и $c_{2i-1}\varphi = c_{2i}$, и если $\eta_i = -1$, то $c_{2i-1} \in B$, $c_{2i} \in A$ и $c_{2i}\varphi = c_{2i-1}$.*

В частности, если хотя бы один из элементов f или g принадлежит подгруппе G и не сопряжен в G ни с одним элементом из связанных подгрупп A и B, то эти элементы сопряжены в группе G^* тогда и только тогда, когда и другой содержится в G и они сопряжены в группе G.

2. *Если $f = t^{\varepsilon_1} f_1 t^{\varepsilon_2} f_2 \cdots f_{n-1} t^{\varepsilon_n} f_n$ и $g = t^{\delta_1} g_1 t^{\delta_2} g_2 \cdots g_{n-1} t^{\delta_n} g_n$ $(n \geqslant 1)$, то эти элементы сопряжены в группе G^* в точности тогда, когда элемент f сопряжен при помощи элемента d, принадлежащего подгруппе A, если $\varepsilon_1 = 1$, или подгруппе B, если $\varepsilon_1 = -1$, с некоторой циклической перестановкой $t^{\delta_i} g_i t^{\delta_{i+1}} g_{i+1} \cdots t^{\delta_n} g_n t^{\delta_1} \cdots t^{\delta_{i-1}} g_{i-1}$ элемента g.*

Доказательство. Существование циклически приведенного элемента, сопряженного с произвольным элементом g группы G^*, вытекает из того, что, как легко видеть, элемент g' наименьшей длины в классе сопряженных с g элементов является циклически приведенным. Если $g' = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$ — приведенная запись такого элемента и $n \geqslant 1$, то сопряженный с ним элемент

$$g_0^{-1} g' g_0 = t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} (g_n g_0)$$

имеет приведенную запись вида, указанного в формулировке предложения.

Заметим, что условия, сформулированные в каждом из пунктов 1 и 2, являются достаточными для сопряженности элементов f и g. Действительно, из условий (1.1) – (1.3) следует, что для любого $i = 1, 2, \ldots, r$

выполнено равенство $t^{-\eta_i}c_{2i-1}t^{\eta_i} = c_{2i}$, так что любые соседние члены последовательности $c_0, c_1, \ldots, c_{2r+1}$ сопряжены в группе G^*. Кроме того, произвольный циклически приведенный элемент положительной длины сопряжен, очевидно, с любой своей циклической перестановкой.

Доказательство необходимости начнем с рассмотрения случая, когда f и g — сопряженные в группе G^* циклически приведенные элементы группы G^*, причем $f \in G$. Тогда для некоторого элемента $d \in G^*$ с приведенной записью

$$d = d_0t^{\eta_1}d_1t^{\eta_2}d_2 \cdots d_{r-1}t^{\eta_r}d_r$$

выполнено равенство $d^{-1}fd = g$. Можно считать при этом, что среди элементов, удовлетворяющих этому равенству, длина r элемента d является наименьшей. Если $r = 0$, т. е. $d \in G$, то $g \in G$ и элементы f и g сопряжены в группе G. Будем далее считать, что $r \geqslant 1$ (и потому элементы f и g не сопряжены элементом из подгруппы G), и индукцией по r докажем, что существует последовательность $c_0, c_1, \ldots, c_{2r+1}$, которая вместе с последовательностями $\eta_1, \eta_2, \ldots, \eta_r$ и $d_0, d_1, \ldots, d_r$ удовлетворяет условиям (1.1), (1.2) и (1.3) (откуда будет следовать, в частности, что $g \in G$).

Перепишем равенство $d^{-1}fd = g$ в виде

$$d_r^{-1}t^{-\eta_r}d_{r-1}^{-1} \cdots d_2^{-1}t^{-\eta_2}d_1^{-1}t^{-\eta_1}d_0^{-1}fd_0t^{\eta_1}d_1t^{\eta_2}d_2 \cdots d_{r-1}t^{\varepsilon_r}d_r = g. \tag{4}$$

Поскольку элемент g является циклически приведенным, запись левой части этого равенства не может быть приведенной. Так как запись элемента d предполагалась приведенной, t-редукции возможны лишь в одном месте, а именно элемент $c_1 = d_0^{-1}fd_0$ должен входить в подгруппу A, если $\eta_1 = 1$, и — в подгруппу B, если $\eta_1 = -1$. Полагая $c_2 = c_1\varphi$ при $\eta_1 = 1$ и $c_2 = c_1\varphi^{-1}$ при $\eta_1 = -1$, будем иметь $c_2 \in B$, если $\eta_1 = 1$, и $c_2 \in A$, если $\eta_1 = -1$, а также $t^{-\eta_1}c_1t^{\eta_1} = c_2$. Поэтому при $r = 1$ равенство (4) принимает вид $d_1^{-1}c_2d_1 = g$, так что элемент g принадлежит подгруппе G и элементы $c_0 = f$, c_1, c_2 и $c_3 = g$ образуют искомую последовательность.

При $r > 1$ равенство (4), переписанное в виде

$$d_r^{-1}t^{-\eta_r}d_{r-1}^{-1} \cdots d_2^{-1}t^{-\eta_2}d_1^{-1}c_2d_1t^{\eta_2}d_2 \cdots d_{r-1}t^{\eta_r}d_r = g,$$

говорит о том, что элементы c_2 и g сопряжены при помощи элемента

$$d' = d_1t^{\eta_2}d_2 \cdots d_{r-1}t^{\eta_r}d_r$$

длины $r-1 \geqslant 1$. Поскольку из минимальности длины элемента d следует, как легко видеть, что c_2 и g не сопряжены в группе G, по индуктивному предположению существует последовательность $c_2, c_3, \ldots, c_{2r+1} = g$ элементов группы G такая, что для каждого $i = 1, 2, \ldots, r$ выполнено равенство $d_i^{-1} c_{2i} d_i = c_{2i+1}$ и для любого $i = 2, 3, \ldots, r$ если $\eta_i = 1$, то $c_{2i-1} \in A$, $c_{2i} \in B$ и $c_{2i-1}\varphi = c_{2i}$, и если $\eta_i = -1$, то $c_{2i-1} \in B$, $c_{2i} \in A$ и $c_{2i}\varphi = c_{2i-1}$.

Очевидно, что тогда $g \in G$ и последовательность $c_0, c_1, \ldots, c_{2r+1}$ является искомой. Тем самым завершен индуктивный шаг, и необходимость условия в первом утверждении пункта 1 доказана. Второе утверждение этого пункта является непосредственным следствием первого.

Предположим теперь, что приведенные записи циклически приведенных элементов f и g имеют вид

$$f = t^{\varepsilon_1} f_1 t^{\varepsilon_2} f_2 \cdots f_{m-1} t^{\varepsilon_m} f_m \quad \text{и} \quad g = t^{\delta_1} g_1 t^{\delta_2} g_2 \cdots g_{n-1} t^{\delta_n} g_n,$$

где $m \geqslant 1$ и $n \geqslant 1$. Если элемент f сопряжен в группе G^* с элементом g, то он сопряжен и с каждой циклической перестановкой элемента g. Для любой циклической перестановки

$$u_i = t^{\delta_i} g_i t^{\delta_{i+1}} g_{i+1} \cdots t^{\delta_n} g_n t^{\delta_1} \cdots t^{\delta_{i-1}} g_{i-1}$$

$(i = 1, 2, \ldots, n)$ этого элемента фиксируем элемент v_i наименьшей длины такой, что $f = v_i^{-1} u_i v_i$. Обозначим теперь через d тот из элементов v_1, v_2, $\ldots$, v_n, длина которого является наименьшей, и покажем, что $l(d) = 0$. При этом для простоты обозначений (и без потери общности) можно предполагать, что $d = v_1$, т. е. $f = d^{-1} g d$.

Пусть, напротив, приведенная запись элемента d имеет вид

$$d = d_0 t^{\eta_1} d_1 t^{\eta_2} d_2 \cdots d_{r-1} t^{\eta_r} d_r,$$

где $r > 0$. Так как элемент f циклически приведен, правая часть равенства

$$f = d_r^{-1} t^{-\eta_r} \cdots d_1^{-1} t^{-\eta_1} d_0^{-1} t^{\delta_1} g_1 t^{\delta_2} \cdots t^{\delta_n} g_n d_0 t^{\eta_1} d_1 \cdots t^{\eta_r} d_r \qquad (5)$$

не может быть приведенной, и потому к ней должна быть применима некоторая t-редукция. Поскольку записи элементов d и g предполагаются приведенными, это возможно лишь в следующих двух случаях:

а) $\eta_1 = \delta_1$ и d_0 принадлежит подгруппе A, если $\delta_1 = 1$, или d_0 принадлежит подгруппе B, если $\delta_1 = -1$;

б) $\delta_n = -\eta_1$ и $g_n d_0$ принадлежит подгруппе A, если $\delta_n = -1$, и $g_n d_0$ принадлежит подгруппе B, если $\delta_n = 1$.

В случае а) имеем $t^{-\eta_1} d_0 t^{\delta_1} = c$ для некоторого элемента $c \in G$, и если $n = 1$, равенство (5) принимает вид

$$f = d_r^{-1} t^{-\eta_r} d_{r-1}^{-1} \cdots t^{-\eta_2} (g_1^{-1} c d_1)^{-1} \cdot t^{\delta_1} g_1 \cdot (g_1^{-1} c d_1) t^{\eta_2} \cdots d_{r-1} t^{\eta_r} d_r,$$

из которого следует, что элементы f и g сопряжены при помощи элемента $d' = (g_1^{-1} c d_1) t^{\eta_2} \cdots d_{r-1} t^{\eta_r} d_r$ длины $r - 1$. Если $n > 1$, равенство (5) принимает вид

$$f = d_r^{-1} t^{-\eta_r} \cdots t^{-\eta_2} (g_1^{-1} c d_1)^{-1} \cdot t^{\delta_2} g_2 \cdots t^{\delta_n} g_n t^{\delta_1} g_1 \cdot (g_1^{-1} c d_1) t^{\eta_2} \cdots t^{\eta_r} h_r,$$

из которого следует, что элементы f и u_2 сопряжены при помощи элемента d'. В любом случае получаем противоречие с выбором элемента d.

В случае б) имеем $t^{\delta_n} g_n d_0 t^{\eta_1} = c$ для некоторого элемента $c \in G$, и если $n = 1$, равенство (5) принимает вид

$$f = d_r^{-1} t^{-\eta_r} d_{r-1}^{-1} \cdots t^{-\eta_2} (c d_1)^{-1} \cdot t^{\delta_1} g_1 \cdot (c d_1) t^{\eta_2} \cdots d_{r-1} t^{\eta_r} d_r,$$

из которого следует, что элементы f и g сопряжены при помощи элемента $d' = (c d_1) t^{\eta_2} \cdots d_{r-1} t^{\eta_r} d_r$ длины $r - 1$. Если $n > 1$, равенство (5) принимает вид

$$f = d_r^{-1} t^{-\eta_r} \cdots t^{-\eta_2} (c d_1)^{-1} \cdot t^{\delta_n} g_n t^{\delta_1} g_1 t^{\delta_2} g_2 \cdots t^{\delta_{n-1}} g_{n-1} \cdot \\ (c d_1) t^{\eta_2} \cdots t^{\eta_r} d_r,$$

из которого следует, что элементы f и u_n сопряжены при помощи элемента d', что снова противоречит выбору элемента d.

Таким образом, для некоторой циклической перестановки

$$u_i = t^{\delta_i} g_i t^{\delta_{i+1}} g_{i+1} \cdots t^{\delta_n} g_n \cdots t^{\delta_{i-1}} g_{i-1}$$

элемента g и некоторого элемента $d \in G$ выполнено равенство $f = d^{-1} u_i d$. Переписав это равенство в виде

$$f_m^{-1} t^{-\varepsilon_m} f_{m-1}^{-1} \cdots f_1^{-1} t^{-\varepsilon_1} d^{-1} t^{\delta_i} g_i t^{\delta_{i+1}} g_{i+1} \cdots t^{\delta_n} g_n \cdots t^{\delta_{i-1}} g_{i-1} d = 1,$$

мы видим, что в силу леммы Бриттона запись левой части не может быть приведенной. Единственной возможностью применимости к этой записи

t-редукции является условие $\varepsilon_1 = \delta_i$ и $d \in A$ при $\varepsilon_1 = 1$ или $d \in B$ при $\varepsilon_1 = -1$. Теорема полностью доказана.

Из первого утверждения теоремы 6.3.1 и замечания перед ее формулировкой вытекают, очевидно, следующие утверждения:

6.3.2. Следствие. *Произвольный элемент конечного порядка HNN-расширения $G^* = \bigl(G, t;\ t^{-1}At = B, \varphi\bigr)$ сопряжен в этой группе с некоторым элементом из подгруппы G. В частности, HNN-расширение группы без кручения является группой без кручения.*

6.3.3. Следствие. *Если в группе $G^* = \bigl(G, t;\ t^{-1}At = B, \varphi\bigr)$ степени g^m и g^n элемента g сопряжены и $|m| \neq |n|$, то элемент g сопряжен с некоторым элементом из подгруппы G.*

6.4. О некоторых гомоморфных образах HNN-расширения. Следующий аналог понятия пары совместимых подгрупп, введенного в разделе 5.4, фактически сформулирован в работе [7].

Пусть G — некоторая группа, A и B — изоморфные подгруппы группы G и $\varphi : A \to B$ — изоморфизм. Подгруппа H группы G называется (A, B, φ)-*совместимой*, если $(A \cap H)\varphi = B \cap H$.

Справедливы утверждения, аналогичные предложению 5.4.1 и теореме 5.4.2.

6.4.1. Предложение. *Пусть G — некоторая группа, A и B — изоморфные подгруппы группы G и $\varphi\colon A \to B$ — изоморфизм. Для любой нормальной (A, B, φ)-совместимой подгруппы H группы G отображение $\varphi_{_H}\colon AH/H \to BH/H$, определяемое по правилу $(aH)\varphi_{_H} = (a\varphi)H$ (где $a \in A$), этим правилом определено корректно и является изоморфизмом подгруппы AH/H фактор-группы G/H на ее подгруппу BH/H.*

Доказательство этого утверждения совершенно аналогично доказательству предложения 5.4.1.

Из предложения 6.4.1 следует, что наряду с HNN-расширением $G^* = \bigl(G, t;\ t^{-1}A\,t = B, \varphi\bigr)$ группы G можно построить HNN-расширение

$$G^*_H = \bigl(G/H, t_{_H};\ t_{_H}^{-1}AH/H\,t_{_H} = BH/H,\ \varphi_{_H}\bigr)$$

группы G/H с проходной буквой $t_{_H}$ и подгруппами AH/H и BH/H, связанными в соответствии с изоморфизмом $\varphi_{_H}$. Связь групп G^* и G^*_H описывается следующим образом:

6.4.2. Теорема. *Пусть G — некоторая группа, A и B — подгруппы группы G, $\varphi : A \to B$ — изоморфизм группы A на группу B. Для любой нормальной (A, B, φ)-совместимой подгруппы H группы G существует гомоморфизм $\rho_{_H}$ группы $G^* = \big(G, t;\ t^{-1}At = B, \varphi\big)$ на группу $G^*_{_H} = \big(G/H, t_{_H};\ t_{_H}^{-1}AH/H\, t_{_H} = BH/H,\ \varphi_{_H}\big)$, продолжающий естественное отображение подгруппы G группы G^* на подгруппу G/H группы $G^*_{_H}$ и переводящий проходную букву t в проходную букву $t_{_H}$. Ядро гомоморфизма $\rho_{_H}$ совпадает с нормальным замыканием H^{G^*} в группе G^* подгруппы H, а потому фактор-группа G^*/H^{G^*} изоморфна группе $G^*_{_H}$ и $G \cap H^{G^*} = H$.*

Доказательство. Существование гомоморфизма $\rho_{_H}$ группы G^* на группу $G^*_{_H}$, переводящего элемент t группы G^* в элемент $t_{_H}$ и действующего на подгруппе G как естественный гомоморфизм G на G/H, вытекает непосредственно из следствия 6.1.4.

Поскольку подгруппа H содержится в ядре гомоморфизма $\rho_{_H}$, включение $H^{G^*} \subseteq \operatorname{Ker} \rho_{_H}$ очевидно.

Для доказательства противоположного включения предположим, что элемент g с приведенной записью

$$g = g_0 t^{\varepsilon_1} g_1 t^{\varepsilon_2} g_2 \cdots g_{n-1} t^{\varepsilon_n} g_n$$

принадлежит подгруппе $\operatorname{Ker} \rho_{_H}$.

Если $n = 0$, то $g\rho_{_H} = g_0 H$ и потому $g \in H$.

Пусть $n > 0$ и пусть все элементы из ядра гомоморфизма $\rho_{_H}$, длина которых меньше n, лежат в подгруппе H^{G^*}. Так как $g\rho_{_H} = 1$, запись

$$g\rho_{_H} = (g_0H)t_{_H}^{\varepsilon_1}(g_1H)t_{_H}^{\varepsilon_2}(g_2H)\cdots(g_{n-1}H)t_{_H}^{\varepsilon_n}(g_nH)$$

не может быть приведенной в группе $G^*_{_H}$. Следовательно, $n > 1$ и для некоторого номера i, $0 < i < n$, мы должны иметь либо $\varepsilon_i = -1$, $\varepsilon_{i+1} = 1$ и $g_i \in AH$, либо $\varepsilon_i = 1$, $\varepsilon_{i+1} = -1$ и $g_i \in BH$.

В первом случае имеем $g_i \equiv a \pmod{H}$ для некоторого $a \in A$, и потому элемент g сравним по модулю подгруппы H^{G^*} с элементом g', который получается из элемента g заменой g_i на a. Так как $H^{G^*} \subseteq \operatorname{Ker}\rho_{_H}$, элемент g' тоже принадлежит ядру гомоморфизма $\rho_{_H}$, а так как $t^{-1}at = a\varphi$, то $l(g') < n$, и по индуктивному предположению $g' \in H^{G^*}$. Следовательно, и $g \in H^{G^*}$. Поскольку второй случай рассматривается аналогично, равенство $H^{G^*} = \operatorname{Ker} \rho_{_H}$ можно считать доказанным. Последние два утверждения теоремы 6.4.2 являются очевидными следствиями доказанных.

Из этой теоремы вытекают аналоги утверждений 5.4.3 и 5.4.4.

6.4.3. Следствие. *Для любой группы G с подгруппами A и B и изоморфизмом $\varphi\colon A \to B$ и для любой нормальной (A, B, φ)-совместимой подгруппы H группы G в группе $G^* = \bigl(G, t;\ t^{-1}A\,t = B, \varphi\bigr)$ существует нормальная подгруппа N такая, что $G \cap N = H$.*

6.4.4. Предложение. *Для любой нормальной подгруппы N группы $G^* = \bigl(G, t;\ t^{-1}A\,t = B, \varphi\bigr)$ пересечение $H = G \cap N$ является нормальной (A, B, φ)-совместимой подгруппой группы G. Поэтому произвольный гомоморфизм группы G^* в какую-либо группу проходит через некоторый гомоморфизм вида $\rho_{_H}$.*

В самом деле, если N — нормальная подгруппа группы G^* и $H = G \cap N$, то

$$(A \cap H)\varphi = (A \cap G \cap N)\varphi = (A \cap N)\varphi = t^{-1}(A \cap N)t = B \cap N.$$

Практически очевиден и следующий аналог утверждения 5.4.5:

6.4.5. Предложение. *Пусть G — группа с подгруппами A и B и изоморфизмом $\varphi\colon A \to B$. Пересечение любого семейства (A, B, φ)-совместимых подгрупп группы G является (A, B, φ)-совместимой подгруппой.*

6.5. HNN-расширение с произвольной системой проходных букв. Рассматриваемая выше конструкция HNN-расширения может быть обобщена следующим образом.

Пусть G — некоторая группа, заданная представлением

$$G = \langle x_1, x_2, \ldots, x_n;\ W\rangle, \tag{6}$$

и пусть $\{A_i\}_{i\in I}$ и $\{B_i\}_{i\in I}$ — два семейства подгрупп группы G с одним и тем же множеством индексов I. Предположим также, что для каждого $i \in I$ подгруппы A_i и B_i изоморфны и $\varphi_i\colon A_i \to B_i$ — фиксированный изоморфизм. Группа G^*, задаваемая представлением

$$G^* = \langle x_1, x_2, \ldots, x_n, t_i\,(i \in I);\ W,\ t_i^{-1}at_i = a\varphi_i\ (a \in A_i,\ i \in I)\rangle, \tag{7}$$

множество порождающих символов которого состоит из порождающих символов представления (6) и семейства символов t_i, а множество определяющих слов и соотношений состоит из множества слов W и для каждого $i \in I$ — из всевозможных соотношений вида $t_i^{-1}at_i = b$, где a —

слово от порождающих $x_1, x_2, \ldots, x_n$, определяющее элемент подгруппы A_i, а b — слово от порождающих $x_1, x_2, \ldots, x_n$, определяющее элемент $a\varphi_i$ подгруппы B_i, называется *HNN-расширением группы G с семейством проходных букв $\{t_i\}_{i\in I}$ и связанными в соответствии с изоморфизмами φ подгруппами A_i и B_i $(i \in I)$.*

Как и в случае HNN-расширения с одной проходной буквой, будем записывать $G^* = \bigl(G, t_i\,(i \in I);\, t_i^{-1}A_it = B_i, \varphi_i\,(i \in I)\bigr)$, а группу G называть *базовой группой HNN-расширения.*

Можно заметить сразу же, что если для каждого $i \in I$ ввести в рассмотрение группу $G_i^* = \bigl(G, t_i;\, t_i^{-1}A_it = B_i, \varphi_i\bigr)$ и считать базовую группу G подгруппой каждой группы G_i^*, то из представления (7) легко понять, что группа G^* является свободным произведением семейства групп $\{G_i^*\}_{i\in I}$ с одной объединенной подгруппой G. Поэтому свойства группы $G^* = \bigl(G, t_i\,(i \in I);\, t_i^{-1}A_it = B_i, \varphi_i\,(i \in I)\bigr)$ можно получать, используя результаты предыдущих разделов этого параграфа и параграфа 5. Например, из теоремы 5.5.2 (точнее, из ее аналога для свободного произведения с одной объединенной подгруппой произвольного семейства групп) следует, что подгруппа группы G^*, порождаемая семейством элементов $\{t_i\}_{i\in I}$, является свободной группой, свободно порождаемой этим семейством.

Список литературы

[1] *Магнус В., Каррас А., Солитэр Д.* Комбинаторная теория групп. М.: Наука, 1974.

[2] *Линдон Р., Шупп П.* Комбинаторная теория групп. М.: Мир, 1980.

[3] *Каргаполов М. И., Мерзляков Ю. И.* Основы теории групп: Учебное пособие. 5-е изд.,стер. – СПб.: издательство "Лань 2009.

[4] *Baumslag G.* On the residual finiteness of generalized free products of nilpotent groups // Trans.Amer.Math.Soc. 1963. Vol. 106. № 2. P. 193–209.

[5] *Neumann B. H.* An assay on free products of groups with amalgamations // Phil. Trans. Royal Soc. of London. 1954. Vol. 246. P. 503–554.

[6] *Karrass A., Solitar D.* The subgroups of a free product of two groups with an amalgamated subgroup // Trans. Amer. Math. Soc. 1970. Vol. 150. P. 227–255.

[7] *Baumslag B., Tretkoff M.* Residually finite HNN extensions // Communs in Algebra. 1978. Vol. 6. P. 179–194.