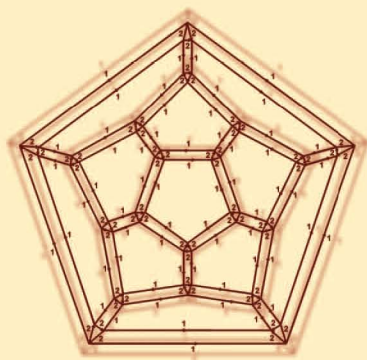


СОВРЕМЕННАЯ
МАТЕМАТИКА

О. В. Богопольский

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП



СОВРЕМЕННАЯ МАТЕМАТИКА

Редакционный совет:

А. В. Болсинов
А. В. Борисов
И. С. Мамаев
И. А. Тайманов
Д. В. Трещев

Вышли в свет:

П. И. Голод, А. У. Климык. Математические основы теории симметрии
М. Громов. Гиперболические группы
М. Громов. Знак и геометрический смысл кривизны
Дж. Д. Мур. Лекции об инвариантах Зайберга – Виттена
Дж. Милнор. Голоморфная динамика
И. Р. Шафаревич. Основные понятия алгебры
И. Добеши. Десять лекций по вейвлетам
Э. Столниц, Т. ДеРоуз, Д. Салезин. Вейвлеты в компьютерной графике
К. Кассель, М. Россо, В. Тураев. Квантовые группы и инварианты узлов
Ж. П. Рамис. Расходящиеся ряды и асимптотические теории
О. В. Богопольский. Введение в теорию групп

Готовятся к печати:

А. Д. Морозов. Введение в теорию фракталов
С. П. Новиков. Топология
Я. Песин. Теория размерности
А. И. Шафаревич. Введение в теорию квазиклассического квантования изотропных многообразий

О. В. Богопольский

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП



Москва ♦ Ижевск

2002

Интернет-магазин
MATHESIS

<http://shop.rcd.ru>

- физика
 - математика
 - биология
 - техника
-

Богопольский О. В.

Введение в теорию групп. — Москва-Ижевск: Институт компьютерных исследований, 2002, 148 стр.

Целью книги является быстрое и глубокое введение в теорию групп. В первой части излагаются основы теории, строится спорадическая группа Матге, объясняется ее связь с теорией кодирования и системами Штейнера. Во второй части рассматривается теория Басса-Серра групп, действующих на деревьях. Особенность книги — геометрический подход к теории конечных и бесконечных групп. Имеется большое количество примеров, упражнений и рисунков.

Для научных работников, аспирантов и студентов университетов.

ISBN 5-93972-165-6

© О. В. Богопольский, 2002

© Институт компьютерных исследований, 2002

<http://rcd.ru>

Оглавление

Предисловие	7
ГЛАВА 1. Введение в теорию конечных групп	8
§ 1. Основные определения	8
§ 2. Теорема Лагранжа. Нормальная подгруппа и фактор-группа	12
§ 3. Теоремы о гомоморфизмах	14
§ 4. Теорема Кэли	15
§ 5. Двойные смежные классы	16
§ 6. Действие группы на множестве	17
§ 7. Нормализатор и централизатор. Центр конечной p -группы неединичен	20
§ 8. Теорема Силова	21
§ 9. Прямые произведения групп	23
§ 10. Простые конечные группы	25
§ 11. Группа A_n проста при $n \geq 5$	26
§ 12. A_5 как группа вращений икосаэдра	27
§ 13. A_5 как первая нециклическая простая группа	28
§ 14. A_5 как проективная специальная линейная группа	30
§ 15. Теорема Жордана–Диксона	32
§ 16. Группа Матье M_{22}	34
§ 17. Группы Матье, системы Штейнера и теория кодирования	42
§ 18. Теория расширений	45
§ 19. Теорема Шура	47
§ 20. Группа Хигмэна–Симса	48
ГЛАВА 2. Введение в комбинаторную теорию групп	54
§ 1. Графы и графы Кэли групп	54
§ 2. Автоморфизмы деревьев	60
§ 3. Свободные группы	62
§ 4. Фундаментальная группа графа	67
§ 5. Задание группы порождающими и определяющими соотношениями	68
§ 6. Преобразования Титце	71

§ 7. Представление группы S_n	74
§ 8. Деревья и свободные группы	75
§ 9. Переписывающий процесс Райдемайстера–Шрайера	81
§ 10. Свободное произведение	83
§ 11. Свободное произведение с объединением	85
§ 12. Деревья и свободные произведения с объединением	87
§ 13. Действие группы $SL_2(\mathbb{Z})$ на гиперболической плоскости	89
§ 14. HNN-расширения	95
§ 15. Деревья и HNN-расширения	98
§ 16. Граф групп и его фундаментальная группа	98
§ 17. Связь свободных произведений с объединением и HNN-расширений	101
§ 18. Структура группы, действующей на дереве	102
§ 19. Теорема Куроша	106
§ 20. Накрытия графов	107
§ 21. S -графы и перечисление подгрупп свободных групп	111
§ 22. Фолдинги	113
§ 23. Пересечение двух подгрупп свободной группы	117
§ 24. Комплексы	119
§ 25. Накрытия комплексов	122
§ 26. Поверхности	126
§ 27. Теорема Зайферта–ван Кампена	132
§ 28. Теорема Грушко	133
§ 29. Хопфовы и финитно аппроксимируемые группы	135
Историческая справка	140
Список литературы	144

Предисловие

Эта книга — расширенная запись спецкурса по теории групп, читавшегося мной в Новосибирском государственном университете в 1996–2001 годах. Ее цель — не только изложить основы теории групп, но и описать некоторые нетривиальные конструкции и технику, используемые работающими специалистами. Основы даются в § 1–9 главы 1, а далее можно читать главы 1 и 2 независимо.

В первой главе мы стремимся быстро ввести начинающих в область классификации конечных простых групп. Показано, что такие сложные комбинаторные объекты, как группа Матье M_{22} и группа Хигмана–Симса HS , имеют естественное геометрическое описание. В § 17 объясняется связь групп Матье и систем Штейнера с теорией кодирования.

Во второй главе излагается теория Басса–Серра групп, действующих на деревьях. Эта теория содержит прозрачное и естественное объяснение многих результатов о свободных группах и свободных конструкциях. Объясняется также теория накрытий; внимательный читатель сможет увидеть мост от одной теории к другой. Надеюсь, что многочисленные примеры, упражнения и рисунки помогут читателю лучше разобраться в предмете.

Для понимания книги достаточно знать курс алгебры в объеме первого семестра университета (подстановки, поля, матрицы, векторные пространства, см. [13]). Дополнительно основы теории групп можно изучить по книге М. И. Каргаполова и Ю. И. Мерзлякова [10].

Я благодарю В. Г. Бардакова, А. В. Васильева, Е. П. Вдовина, А. В. Заварницына, В. Д. Мазурова, Д. О. Ревина, О. С. Тишкину и особенно В. А. Чуркина за чтение отдельных частей рукописи и многие ценные замечания. Я благодарю также М.-Т. Бохниг за помощь в оформлении книги.

г. Новосибирск,
11 мая 2002 г.

О. В. Богопольский

ГЛАВА 1

Введение в теорию конечных групп

§ 1. Основные определения

Говорят, что на множестве G определена *бинарная операция* \cdot , если для любых двух элементов a и b из G определен элемент $a \cdot b$ из G . Бинарная операция может обозначаться не только \cdot , но и любым другим символом, например $+$. Обычно пишут ab вместо $a \cdot b$.

Непустое множество G с определенной на нем бинарной операцией называется *группой*, если

- 1) $(ab)c = a(bc)$ для любых элементов a, b, c из G (операция *ассоциативна*);
- 2) существует такой элемент e из G (он называется *единицей*), что $ae = ea = a$ для любого a из G ;
- 3) для любого a из G существует такой элемент b из G (он называется *обратным к a*), что $ab = ba = e$.

Для обозначения единичного элемента используют также символ 1 , если операция обозначается точкой, и символ 0 , если операция обозначается плюсом.

1.1. Упражнение. 1) Докажите, что единица в любой группе G единственна и для любого a из G существует только один обратный к a элемент (он обозначается a^{-1}).

2) Докажите, что для любого элемента a из группы G отображение $\varphi_a: G \rightarrow G$, заданное правилом $\varphi_a(g) = ag$ ($g \in G$), является биекцией.

Группа G называется *абелевой*, или *коммутативной*, если $ab = ba$ для любых a, b из G . Множество \mathbb{Z} целых чисел с обычной операцией сложения является абелевой группой. Примеры 1.3 показывают, что существуют и неабелевы группы.

Группы G и G_1 называют *изоморфными* и пишут $G \cong G_1$, если существует *изоморфизм* $\varphi: G \rightarrow G_1$, то есть такое взаимно однозначное отображение φ из группы G на всю группу G_1 , что $\varphi(ab) = \varphi(a)\varphi(b)$ для любых a, b из G .

Благодаря ассоциативности в группе, произведение любых ее элементов a_1, a_2, \dots, a_n в заданном порядке не зависит от расстановки скобок и поэтому может быть записано как $a_1 a_2 \dots a_n$. Произведение n элементов, равных a , обозначается a^n . Полагают $a^0 = e$ и $a^n = (a^{-1})^{-n}$ для $n < 0$.

Если $a^n = e$ при некотором $n > 0$, то наименьшее такое n называют *порядком элемента a* и обозначают $|a|$. Если $a^n \neq e$ при любом $n > 0$, то говорят, что a — *элемент бесконечного порядка* и пишут $|a| = \infty$. Мощность $|G|$ группы G называют *порядком группы G* . Если эта мощность конечна, то группа называется *конечной*, в противном случае — *бесконечной*. Конечная группа G называется *p -группой*, если $|G| = p^k$ для некоторого простого числа p и натурального $k \geq 1$.

1.2. Упражнение.

- 1) Если $a^n = e$, то n делится на $|a|$.
- 2) Если a и b — перестановочные элементы, т. е. $ab = ba$, и их порядки взаимно просты, то $|ab| = |a| \cdot |b|$.

Непустое подмножество H группы G называется *подгруппой* группы G (пишут $H \leq G$), если для любых a, b из H элементы ab и a^{-1} также лежат в H . Подгруппа группы сама является группой относительно сужения на нее операции объемлющей группы. Если $H \leq G$ и $H \neq G$, то пишут $H < G$. Если $\{1\} < H < G$, то H называется *собственной* подгруппой группы G .

Следуя обозначениям учебника [13], далее мы используем следующее правило композиции двух отображений: $(fg)(x) = f(g(x))$. Таким образом, подстановки перемножаются справа налево.

1.3. Примеры.

1) Движением евклидовой плоскости называется любое отображение этой плоскости на себя, сохраняющее расстояния между точками.

Пусть F — произвольная фигура на евклидовой плоскости. Множество всех движений евклидовой плоскости, переводящих F на себя, с операцией «композиция двух движений», является группой. Эта группа называется *группой симметрий фигуры F* .

В группе симметрий правильного n -угольника имеется ровно $2n$ элементов: n вращений по часовой стрелке на углы $\frac{2\pi k}{n}$ ($k = 0, 1, \dots, n-1$) вокруг его центра и n отражений относительно прямых, проходящих через центр и одну из его вершин или середину одной из его сторон. Все вращения в группе симметрий правильного n -угольника образуют подгруппу, которая называется *группой вращений* данного n -угольника.

2) Множество всех подстановок на множестве $\{1, 2, \dots, n\}$ относительно умножения подстановок является группой. Она называется *симметрической группой степени n* и обозначается S_n . Все четные подстановки в S_n образуют подгруппу, которая обозначается A_n и называется *знакопеременной группой степени n* . Порядок группы S_n равен $n!$, а порядок группы A_n равен $n!/2$ при $n \geq 2$.

3) Множество $\text{GL}_n(K)$ всех невырожденных матриц размера $n \times n$ над полем K является группой относительно умножения матриц. Она называется *общей линейной группой*. Ее подгруппа $\text{SL}_n(K)$, состоящая из всех матриц с определителем 1, называется *специальной линейной группой*. Группа $\text{SL}_n(K)$ содержит подгруппу $\text{UT}_n(K)$, состоящую из всех матриц с единицами на главной диагонали и нулями под ней.

Известно (см, например, [13]), что конечное поле из q элементов единственно с точностью до изоморфизма и q может быть только степенью простого числа. Поэтому, если поле K состоит из q элементов, то вместо $\text{GL}_n(K)$ пишут $\text{GL}_n(q)$ и т. д.

1.4. Упражнение. *Группа симметрий правильного треугольника изоморфна группе S_3 .*

Если M — непустое подмножество группы G , то множество

$$\{a_1^{\epsilon_1} \cdots a_m^{\epsilon_m} \mid a_i \in M, \epsilon_i = \pm 1, m = 1, 2, \dots\}$$

называется подгруппой, *порожденной* множеством M , и обозначается $\langle M \rangle$. Очевидно, $\langle M \rangle$ — наименьшая подгруппа группы G , содержащая множество M .

Для сокращения записи вместо $\langle \{a, b, \dots, c\} \rangle$ пишут $\langle a, b, \dots, c \rangle$ и говорят, что эта подгруппа порождается элементами a, b, \dots, c . Допустимы и другие вольности в обозначениях. Например, если A и B — подмножества группы G , c — ее элемент, то вместо $\langle A \cup B \cup \{c\} \rangle$ пишут $\langle A, B, c \rangle$.

Группа называется *конечно порожденной*, если она может быть порождена конечным множеством элементов.

Группа G называется *циклической*, если в ней существует такой элемент a , что $G = \langle a \rangle$. В этом случае $G = \{a^n \mid n \in \mathbb{Z}\}$. Не исключено, что a^n совпадет с a^m при $n \neq m$. Примером бесконечной циклической группы является группа \mathbb{Z} всех целых чисел относительно обычной операции сложения (в качестве a можно взять 1 или -1).

Пусть $n \geq 1$ — натуральное число. Каждому целому числу i соответствует остаток от деления i на n , то есть такое целое число \bar{i} , что $0 \leq \bar{i} \leq n-1$ и $(i - \bar{i})$ делится на n . Легко проверить, что множество $Z_n = \{0, 1, \dots, n-1\}$ с операцией \oplus , определенной правилом $i \oplus j = \bar{i + j}$, является циклической группой, порожденной элементом 1.

1.5. Упражнение. Группа вращений правильного n -угольника изоморфна группе Z_n .

1.6. Теорема. Любая бесконечная циклическая группа изоморфна группе \mathbb{Z} , а любая конечная циклическая группа порядка n изоморфна группе Z_n .

Доказательство. Если $\langle a \rangle$ — бесконечная циклическая группа, то отображение $\varphi : \mathbb{Z} \rightarrow \langle a \rangle$, заданное правилом $\varphi(i) = a^i$, является изоморфизмом. Если $\langle a \rangle$ — циклическая группа порядка n , то отображение $\varphi : Z_n \rightarrow \langle a \rangle$, заданное тем же правилом $\varphi(i) = a^i$, является изоморфизмом. Проверим, например, взаимную однозначность этого отображения. Предположим противное: $a^i = a^j$ при некоторых $0 \leq i < j \leq n-1$. Тогда $a^{j-i} = e$ и в группе $\langle a \rangle$ были бы только элементы e, a, \dots, a^{j-i-1} . Но этих элементов меньше n — противоречие.

1.7. Теорема. Любая подгруппа циклической группы — циклическая.

Доказательство. Очевидно, единичная подгруппа — циклическая. Пусть H — неединичная подгруппа циклической группы $\langle a \rangle$, и пусть m — наименьшее положительное целое число с условием $a^m \in H$. Очевидно, $\langle a^m \rangle \leq H$. Докажем, что $\langle a^m \rangle = H$. Возьмем в H произвольный элемент, он имеет вид a^k . Поделим k на m с остатком: $k = mq + r$, $0 \leq r < m$. Тогда $a^r = a^k (a^m)^{-q} \in H$. В силу минимальности m отсюда следует, что $r = 0$. Тогда $a^k = (a^m)^q \in \langle a^m \rangle$.

1.8. Упражнение. 1) В циклической группе порядка n порядок любой подгруппы делит n и для любого делителя d числа n существует ровно одна подгруппа порядка d .

2) Число решений уравнения $x^k = e$ в циклической группе порядка n равно $\text{нод}(n, k)$ — наибольшему общему делителю чисел n и k .

Центром группы G называется подмножество

$$Z(G) = \{z \in G \mid zg = gz \text{ для любого } g \in G\}.$$

Очевидно, $Z(G)$ — подгруппа группы G , и группа G абелева тогда и только тогда, когда $Z(G) = G$.

Коммутатором элементов a и b называется элемент $aba^{-1}b^{-1}$. Он обозначается $[a, b]$. Коммутантом группы G называется ее подгруппа $G' = \langle [a, b] \mid a, b \in G \rangle$.

Говорят, что элемент a группы G сопряжен с элементом b посредством элемента g , если $a = gb g^{-1}$. Подгруппа A группы G сопряжена с подгруппой B посредством элемента g , если $A = \{gb g^{-1} \mid b \in B\}$.

Последнее множество обозначают gBg^{-1} . Легко понять, что порядки сопряженных элементов (подгрупп) равны.

Класс сопряженности элемента b — это множество всех элементов в G , сопряженных с b . Группа G разбивается на непересекающиеся классы сопряженности, один из которых равен $\{e\}$.

Любой изоморфизм группы G на себя называется *автоморфизмом*. Множество всех автоморфизмов группы G относительно их композиции является группой и обозначается $\text{Aut}(G)$.

1.9. Упражнение. 1) Докажите, что $\text{Aut}(\mathbb{Z}) \cong Z_2$.

2) Найдите центр, коммутант и группу автоморфизмов группы S_3 . Перечислите классы сопряженных элементов группы S_3 .

3) Докажите, что $S_n = \langle (12), (13), \dots, (1n) \rangle$.

4) Докажите, что группа \mathbb{Q} рациональных чисел относительно сложения не является конечно порожденной.

§ 2. Теорема Лагранжа. Нормальная подгруппа и фактор-группа

Пусть H — подгруппа группы G . Множества $gH = \{gh \mid h \in H\}$, где $g \in G$, называются *левыми смежными классами группы G по подгруппе H* . Аналогично определяются *правые смежные классы Hg* . Легко видеть, что

$$g_1H = g_2H \iff g_1^{-1}g_2 \in H.$$

2.1. Пример. Список всех левых смежных классов группы S_3 по подгруппе $\{e, (12)\}$:

$$\{e, (12)\}, \{(13), (123)\}, \{(23), (132)\}.$$

Список всех правых смежных классов группы S_3 по подгруппе $\{e, (12)\}$:

$$\{e, (12)\}, \{(13), (132)\}, \{(23), (123)\}.$$

Так как соответствие $xH \leftrightarrow Hx^{-1}$ взаимно однозначно, то мощность множества левых смежных классов совпадает с мощностью множества правых смежных классов. Она называется *индексом подгруппы H в группе G* и обозначается $|G : H|$.

2.2. Теорема (Лагранж). Если H — подгруппа конечной группы G , то

$$|G| = |H| \cdot |G : H|.$$

Доказательство. Так как $g \in gH$, то G есть объединение левых смежных классов G по H . Различные левые смежные классы не пересекаются: если $g_1H \cap g_2H \neq \emptyset$, то $g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in H$,

и тогда $g_1H = g_2h_2h_1^{-1}H = g_2H$. Осталось заметить, что эти классы равномошны. Биекция $H \rightarrow gH$ устанавливается правилом $h \mapsto gh$, $h \in H$.

2.3. Следствие. 1) *Порядок элемента конечной группы делит порядок этой группы.*

2) *Всякая группа простого порядка p изоморфна группе Z_p .*

Доказательство. Если G — конечная группа и $g \in G$, то $|g| = |\langle g \rangle|$ и $|\langle g \rangle|$ делит $|G|$. Если $|G| = p$ — простое число и $g \neq e$, то $|\langle g \rangle| = |G|$, и, значит, $G = \langle g \rangle \cong Z_p$.

Для непустых подмножеств A и B группы G определим их произведение: $AB = \{ab \mid a \in A, b \in B\}$. Пусть $H \leq G$, $g \in G$. Тогда произведение $\{g\}H$ совпадает с левым смежным классом gH . Кроме того, имеем $HH = H$.

Говорят, что подгруппа H нормальна в G и пишут $H \triangleleft G$, если $gH = Hg$ для любого $g \in G$. Пусть $H \triangleleft G$. Тогда произведение любых двух смежных классов G по H снова будет смежным классом:

$$g_1H \cdot g_2H = g_1(Hg_2)H = g_1(g_2H)H = g_1g_2H.$$

Множество всех смежных классов G по H относительно такого произведения образует группу. Ее единицей является класс H , а обратным к классу xH — класс $x^{-1}H$. Эта группа называется *фактор-группой* группы G по нормальной подгруппе H и обозначается G/H . По теореме Лагранжа, если G конечна, то $|G| = |H| \cdot |G/H|$.

2.4. Пример. Подгруппа $K = \{e, (12)(34), (13)(24), (14)(23)\}$ в S_4 нормальна и $S_4/K = \{K, (12)K, (13)K, (23)K, (123)K, (132)K\} \cong S_3$.

2.5. Упражнение. 1) *Докажите, что $Z(G) \triangleleft G$, $G' \triangleleft G$ и G/G' — абелева группа.*

2) *Если $H_1 \leq H \leq G$, то $|G : H_1| = |G : H| \cdot |H : H_1|$.*

3) *Если H — подгруппа индекса 2 в группе G , то $H \triangleleft G$.*

4) *Произведение двух подмножеств H_1, H_2 группы G может не быть подгруппой даже в случае, когда H_1 и H_2 — подгруппы. Если H_1 и H_2 — подгруппы и одна из них нормальна в G , то H_1H_2 — подгруппа в G . Если обе подгруппы H_1 и H_2 нормальны в G , то подгруппа H_1H_2 тоже нормальна в G .*

5) *Если A, B — конечные подгруппы группы G , то*

$$|AB| = \frac{|A| \cdot |B|}{|A \cap B|}.$$

§ 3. Теоремы о гомоморфизмах

Отображение φ из группы G в группу G_1 называется *гомоморфизмом*, если $\varphi(ab) = \varphi(a)\varphi(b)$ для любых $a, b \in G$. *Ядром* гомоморфизма φ называется множество $\text{Ker } \varphi = \{g \in G \mid \varphi(g) = e\}$. *Образом* гомоморфизма φ называется множество $\text{Im } \varphi = \{\varphi(g) \mid g \in G\}$.

3.1. Упражнение. Пусть $\varphi : G \rightarrow G_1$ — гомоморфизм. Тогда справедливы следующие утверждения.

- 1) $\varphi(e) = e$, $\varphi(g^{-1}) = (\varphi(g))^{-1}$ для $g \in G$.
- 2) Если $g \in G$ — элемент конечного порядка, то $|\varphi(g)|$ делит $|g|$.
- 3) $\text{Ker } \varphi \trianglelefteq G$, $\text{Im } \varphi \trianglelefteq G_1$.
- 4) Для непустых подмножеств A, B группы G выполняется¹

$$\varphi(A) = \varphi(B) \iff A \cdot \text{Ker } \varphi = B \cdot \text{Ker } \varphi.$$

3.2. Примеры. 1) Пусть K^* — мультипликативная группа поля K , то есть группа всех ненулевых элементов поля K относительно умножения. Отображение $\varphi : \text{GL}_n(K) \rightarrow K^*$, сопоставляющее матрице ее определитель, является гомоморфизмом с ядром $\text{SL}_n(K)$.

2) Пусть $H \trianglelefteq G$. Отображение $\varphi : G \rightarrow G/H$, заданное правилом $\varphi(g) = gH$, является гомоморфизмом с ядром H .

3.3. Теорема. Пусть $\varphi : G \rightarrow G_1$ — гомоморфизм на всю группу G_1 . Тогда

- 1) отображение из множества подгрупп группы G , содержащих $\text{Ker } \varphi$, в множество всех подгрупп группы G_1 , сопоставляющее подгруппам их образ относительно φ , является биекцией,
- 2) эта биекция сохраняет индексы:

$$\text{если } \text{Ker } \varphi \trianglelefteq H_1 \trianglelefteq H_2, \text{ то } |H_2 : H_1| = |\varphi(H_2) : \varphi(H_1)|,$$

- 3) эта биекция сохраняет нормальность:

$$\text{если } \text{Ker } \varphi \trianglelefteq H_1 \trianglelefteq H_2, \text{ то } H_1 \trianglelefteq H_2 \iff \varphi(H_1) \trianglelefteq \varphi(H_2).$$

Доказательство. 1) Это отображение *на*, так как полный прообраз подгруппы группы G_1 является подгруппой в G , содержащей $\text{Ker } \varphi$. Взаимная однозначность вытекает из пункта 4 упражнения 3.1 с учетом того, что $H \cdot \text{Ker } \varphi = H$ для любой подгруппы H группы G , содержащей $\text{Ker } \varphi$.

¹По определению полагают $\varphi(A) = \{\varphi(a) \mid a \in A\}$.

2) Отображение из множества левых смежных классов H_2 по H_1 в множество левых смежных классов $\varphi(H_2)$ по $\varphi(H_1)$, заданное правилом $xH_1 \mapsto \varphi(x)\varphi(H_1)$, является отображением *на*. Это отображение взаимно однозначно, так как из $\varphi(xH_1) = \varphi(yH_1)$ следует $xH_1 \cdot \text{Кер } \varphi = yH_1 \cdot \text{Кер } \varphi$, то есть $xH_1 = yH_1$.

3) Так как $H_1 \cdot \text{Кер } \varphi = H_1$ и $x \cdot \text{Кер } \varphi = \text{Кер } \varphi \cdot x$ для $x \in G$, то равенство $xH_1 = H_1x$ равносильно равенству $xH_1 \cdot \text{Кер } \varphi = H_1x \cdot \text{Кер } \varphi$, которое равносильно равенству $\varphi(x)\varphi(H_1) = \varphi(H_1)\varphi(x)$ ввиду пункта 4 упражнения 3.1.

3.4. Теорема. Если $\varphi : G \rightarrow G_1$ — гомоморфизм, то $G/\text{Кер } \varphi \cong \text{Im } \varphi$.

Указание. Изоморфизм задается правилом $g \text{Кер } \varphi \mapsto \varphi(g)$, $g \in G$.

3.5. Теорема. Пусть $A \leq B \leq G$, $A \trianglelefteq G$, $B \trianglelefteq G$. Тогда $B/A \trianglelefteq G/A$ и $(G/A)/(B/A) \cong G/B$.

Указание. Применить теорему 3.4 к гомоморфизму $\varphi : G/A \rightarrow G/B$, заданному правилом $gA \mapsto gB$.

3.6. Теорема. Пусть $H \trianglelefteq G$, $B \leq G$. Тогда $BH/H \cong B/B \cap H$.

Указание. Гомоморфизм $\varphi : BH \rightarrow B/B \cap H$, заданный правилом $bh \mapsto b(B \cap H)$, $b \in B$, $h \in H$, имеет ядро H .

В заключение приведем общепринятую терминологию. Гомоморфизм $\varphi : G \rightarrow G_1$ называется *эпиморфизмом*, если его образ равен G_1 . Гомоморфизм называется *мономорфизмом* (или *вложением*), если его ядро единично. Группа G *вкладывается* в группу G_1 , если существует вложение G в G_1 . Очевидно, изоморфизм является эпиморфизмом и мономорфизмом одновременно.

§ 4. Теорема Кэли

Далее $S(M)$ обозначает группу всех взаимно однозначных отображений — подстановок — множества M на себя. Если мощность множества M конечна и равна t , то группу $S(M)$ можно отождествить с группой S_t .

4.1. Теорема (Кэли). Пусть G — группа, H — ее подгруппа и M — множество всех левых смежных классов G по H . Зададим отображение $\varphi : G \rightarrow S(M)$ так, что для $g \in G$ подстановка $\varphi(g)$ переводит любой смежный класс xH в смежный класс gxH .

Тогда φ — гомоморфизм (не обязательно *на*) с ядром

$$\text{Кер } \varphi = \bigcap_{x \in G} xHx^{-1}.$$

Доказательство. Ясно, что $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$, так как $g_1g_2(xH) = g_1(g_2xH)$ для любого $x \in G$. Далее,

$$g \in \text{Ker } \varphi \iff (xH = gxH \text{ для всех } xH) \iff (g \in xHx^{-1} \text{ для всех } x).$$

В случае $H = \{1\}$ гомоморфизм φ из теоремы Кэли называется (*левым*) *регулярным представлением* группы G .

4.2. Следствие. 1) *Регулярное представление группы G является вложением группы G в группу $S(G)$. Образ любого неединичного элемента из G относительно этого вложения является подстановкой, сдвигающей все символы.*

Любая конечная группа G вкладывается в группу S_m , где $m = |G|$.

2) *Любая конечная группа G вкладывается в группу $\text{GL}_m(F)$, где F — поле, $m = |G|$.*

Доказательство. Первое утверждение вытекает из теоремы Кэли, а второе — из первого с учетом вложения S_m в $\text{GL}_m(F)$, заданного правилом $\sigma \mapsto A_\sigma$, где $(A_\sigma)_{ij} = 1$ при $\sigma(j) = i$ и $(A_\sigma)_{ij} = 0$ при $\sigma(j) \neq i$.

4.3. Упражнение. *Любая группа порядка 4 изоморфна группе Z_4 или группе $K = \{e, (12)(34), (13)(24), (14)(23)\}$.*

Решение. Пусть G — группа порядка 4. отождествим G с ее образом относительно регулярного представления в S_4 . Тогда любой неединичный элемент группы G является либо циклом длины 4, либо произведением двух независимых транспозиций (иначе появится неподвижный символ). Если в G есть цикл длины 4, то $G \cong Z_4$, а если нет, то $G \cong K$.

4.4. Следствие. *Всякая подгруппа H конечного индекса m группы G содержит подгруппу N , нормальную в G и индекса, делящегося на m и делящего $m!$.*

Доказательство. В качестве N можно взять подгруппу $\text{Ker } \varphi$, где φ из теоремы Кэли. Ее индекс в G равен порядку подгруппы $\text{Im } \varphi$ группы S_m и, следовательно, делит $m!$. Делимость на m выводится из включений $\text{Ker } \varphi \leq H \leq G$ с помощью пункта 2 упражнения 2.5.

§ 5. Двойные смежные классы

Пусть K и H — произвольные подгруппы группы G . Любое множество $KgH = \{kgh \mid k \in K, h \in H\}$, где $g \in G$, называется *двойным смежным классом группы G по подгруппам K и H* . Множество всех таких классов будем обозначать через $K \setminus G/H$.

5.1. Предложение. Пусть K и H — подгруппы группы G . Тогда

1) для произвольного $g \in G$ существует единственный двойной смежный класс группы G по подгруппам K и H , содержащий g ,

2) G разбивается в объединение двойных смежных классов по K и H ,

3) любой двойной смежный класс KgH есть объединение $|K : K \cap gHg^{-1}|$ различных левых смежных классов G по H .

Доказательство. 1) Очевидно, $g = ege \in KgH$. Если g принадлежит еще одному двойному смежному классу KxH , то $g = kxh$ для некоторых $k \in K$, $h \in H$, и, значит, $KgH = K(kxh)H = KxH$.

Пункт 2) следует из пункта 1).

3) Двойной смежный класс KgH есть объединение левых смежных классов kgH , когда k пробегает K . Пусть A — множество всех таких левых смежных классов, а B — множество всех левых смежных классов K по $K \cap gHg^{-1}$. Достаточно доказать, что отображение $\varphi : A \rightarrow B$, определенное правилом $kgH \mapsto k(K \cap gHg^{-1})$, где $k \in K$, является биекцией. Покажем, что это определение корректно и отображение φ взаимно однозначно. Пусть $k_1, k_2 \in K$. Тогда

$$\begin{aligned} k_1gH = k_2gH &\iff g^{-1}k_1^{-1}k_2g \in H \iff k_1^{-1}k_2 \in K \cap gHg^{-1} \iff \\ &\iff k_1(K \cap gHg^{-1}) = k_2(K \cap gHg^{-1}). \end{aligned}$$

То, что φ — отображение *на*, очевидно.

5.2. Теорема. Пусть K и H — подгруппы группы G . Пусть X — полная система представителей двойных смежных классов G по K и H (по одному из каждого класса). Тогда

$$|G : H| = \sum_{x \in X} |K : K \cap xHx^{-1}|. \quad (1)$$

Доказательство. Группа G разбивается на двойные смежные классы KxH с представителями $x \in X$. Каждый из них разбивается на $|K : K \cap xHx^{-1}|$ левых смежных классов G по H .

§ 6. Действие группы на множестве

Говорят, что группа G *действует* (слева) на множестве X , если для любых элементов $g \in G$ и $x \in X$ определен элемент $gx \in X$, причем $g_2(g_1x) = (g_2g_1)x$ и $ex = x$ для всех $x \in X$, $g_1, g_2 \in G$. Множество

$$Gx = \{gx \mid g \in G\}$$

называется *орбитой* элемента x . Очевидно, орбиты любых двух элементов из X либо совпадают, либо не пересекаются, так что множество X разбивается на непересекающиеся орбиты. Если орбита одна — все множество X , то говорят, что G действует *транзитивно* на X . Иначе говоря, группа G действует транзитивно на множестве X , если для любых двух элементов x, x' из X найдется элемент g из G такой, что $gx = x'$.

Стабилизатором элемента x из X называется подгруппа

$$\text{St}_G(x) = \{g \in G \mid gx = x\}.$$

Множеством неподвижных точек элемента g из G называется множество

$$\text{Fix}(g) = \{x \in X \mid gx = x\}.$$

6.1. Упражнение. *Стабилизаторы элементов из одной орбиты сопряжены.*

6.2. Предложение. *Мощность² орбиты Gx равна индексу стабилизатора $\text{St}_G(x)$ в группе G .*

Доказательство. Отображение из Gx в множество левых смежных классов G по $\text{St}_G(x)$, заданное правилом $gx \mapsto g\text{St}_G(x)$, является биекцией.

6.3. Примеры.

1) Любая группа G действует на множестве левых смежных классов по данной подгруппе H : смежный класс xH переходит под действием элемента g в смежный класс gxH . Это действие транзитивно. По сути дела, оно встречалось в теореме Кэли.

2) Пусть K — фиксированный куб в трехмерном евклидовом пространстве, G — группа всех движений этого пространства, сохраняющих ориентацию и переводящих K в K . В группе G имеется тождественное движение, вращения на 120° и 240° вокруг четырех осей, проходящих через противоположные вершины куба, вращения на 180° вокруг осей, проходящих через середины противоположных ребер, и вращения на 90° , 180° и 270° вокруг осей, проходящих через центры противоположных граней. Итак, мы нашли 24 элемента в группе G . Покажем, что других элементов в G нет. Группа G действует транзитивно на множестве K^0 вершин куба K , так как любые две вершины из K можно «соединить цепочкой соседних», а соседние можно перевести

²В случае конечных групп мы будем употреблять другой термин — *длина орбиты*.

друг в друга подходящим вращением. Стабилизатор вершины x должен оставлять на месте также наиболее удаленную от нее вершину x' . Поэтому он состоит из тождественного движения и вращений вокруг оси xx' на 120° и 240° . Следовательно, $|G| = |K^0| \cdot |\text{St}_G(x)| = 8 \cdot 3 = 24$ и, значит, все указанные выше вращения составляют группу G .

Группа G называется *группой вращений куба*. Докажем, что $G \cong S_4$. Вращения из G переставляют четыре самых длинных диагонали куба. Возникает гомоморфизм $\varphi : G \rightarrow S_4$. Ядро этого гомоморфизма равно $\{e\}$, так как только тождественное движение оставляет каждую диагональ куба на месте. Поэтому G изоморфна подгруппе группы S_4 . Сравнивая порядки этих групп, получаем, что $G \cong S_4$.

6.4. Теорема (Бернсайд). *Мощность множества орбит, получающихся при действии конечной группы G на множестве X , равна*

$$\frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

Доказательство. Подсчитывая мощность множества $\{(g, x) \mid gx = x\}$ двумя разными способами, получаем

$$\sum_{g \in G} |\text{Fix}(g)| = \sum_{x \in X} |\text{St}_G(x)| = \sum_{x \in X} \frac{|G|}{|Gx|}.$$

Так как элементы из одной и той же орбиты дают одинаковый вклад в последнюю сумму, то эта сумма равна мощности множества орбит, умноженной на $|G|$.

6.5. Упражнение. *Каждая грань куба раскрашивается одной из трех данных красок. Раскраски считаются одинаковыми, если они совмещаются некоторым вращением куба. Доказать, что существует ровно 57 различных раскрасок куба.*

Говорят, что группа G действует *k-транзитивно* на множестве X , если для любых двух наборов (x_1, \dots, x_k) и (x'_1, \dots, x'_k) элементов из X таких, что $x_i \neq x_j$ и $x'_i \neq x'_j$ при $i \neq j$ найдется элемент g из G с условием $gx_i = x'_i$, $i = 1, \dots, k$. Говорят, что G действует *точно* на X , если для всякого неединичного $g \in G$ существует $x \in X$ такой, что $gx \neq x$.

6.6. Пример. Группа S_n всех подстановок множества $\{1, 2, \dots, n\}$ действует на нем n -транзитивно, а ее подгруппа A_n четных подстановок действует на нем $(n-2)$ -транзитивно при $n \geq 3$. Первое очевидно. Второе следует из того, что если подстановка s переводит символы i_1, \dots, i_{n-2} в символы j_1, \dots, j_{n-2} , то подстановка $s \cdot (j_{n-1}j_n)$ тоже такова. Одна из этих подстановок четна.

В середине 80-х годов XX столетия была доказана гипотеза К. Жордана: если группа действует точно на множестве из n элементов и это действие k -транзитивно при некотором $k > 5$, то она изоморфна группе S_n или A_n . Исследования Э. Матье 4- и 5-транзитивных групп привели к открытию им первых пяти простых (см. § 10) спорадических групп. Мы займемся геометрическим построением одной из них — группы M_{22} — в § 16. Следующие два предложения понадобятся нам в § 16 и § 20.

6.7. Предложение. *Если группа G действует на множестве X точно и 2-транзитивно, то любая ее неединичная нормальная подгруппа N действует на X транзитивно.*

Доказательство. Предположим, что N действует на X не транзитивно. Тогда X есть объединение не менее двух непересекающихся N -орбит: Nx_1, Nx_2, \dots . Ввиду точности действия группы G , в одной из них более одного элемента. Допустим, что $nx_1 \neq x_1$ для некоторого $n \in N$. Так как G действует на X 2-транзитивно, то существует $g \in G$ такое, что $gx_1 = x_2$ и $g(nx_1) = x_1$. Тогда $Nx_2 \ni gng^{-1}x_2 = gnx_1 = x_1 \in Nx_1$ — противоречие.

Если группа G действует на множестве X , то любая ее подгруппа N тоже действует на X . Множества $Nx = \{nx \mid n \in N\}$, $x \in X$, называются N -орбитами. Если $N \trianglelefteq G$, то можно задать действие группы G на множестве всех N -орбит формулой $gNx = Ngx$, $x \in X$, $g \in G$.

6.8. Предложение. *Если группа G действует транзитивно на множестве X и $N \trianglelefteq G$, то G действует транзитивно на множестве всех N -орбит и мощности N -орбит равны.*

Доказательство. Пусть Nx и Nx' — две N -орбиты. Ввиду транзитивности существует такой элемент $g \in G$, что $gx = x'$. Тогда $gNx = Nx'$. Отображение $Nx \rightarrow Nx'$, заданное правилом $nx \mapsto gng^{-1}x'$, $n \in N$, является биекцией.

§ 7. Нормализатор и централизатор. Центр конечной p -группы неединичен

Нормализатором подгруппы H группы G называется подгруппа

$$N_G(H) = \{g \in G \mid gHg^{-1} = H\}.$$

Централизатором элемента $a \in G$ называется подгруппа

$$C_G(a) = \{g \in G \mid gag^{-1} = a\}.$$

Очевидно, $H \trianglelefteq N_G(H)$ и $\langle a \rangle \trianglelefteq Z(C_G(a))$.

7.1. Теорема. 1) *Мощность множества подгрупп группы G , сопряженных с данной подгруппой H , равна $|G : N_G(H)|$.*

2) *Мощность множества элементов группы G , сопряженных с данным элементом a , равна $|G : C_G(a)|$.*

Доказательство. 1) Группа G действует на множестве $M = \{xHx^{-1} \mid x \in G\}$ сопряжениями: подгруппа xHx^{-1} переходит под действием элемента $g \in G$ в подгруппу $gxHx^{-1}g^{-1}$. Легко понять, что это действие транзитивно и $\text{St}_G(H) = N_G(H)$. Тогда $|M| = |G : N_G(H)|$ по предложению 6.2.

2) Группа G действует на себе сопряжениями: элемент x переходит под действием элемента g в элемент gxg^{-1} . Очевидно, орбиты этого действия — это классы сопряженных элементов. Мощность орбиты элемента a равна $|G : \text{St}_G(a)| = |G : C_G(a)|$.

7.2. Теорема. *Центр конечной p -группы неединичен.*

Доказательство. Пусть G — конечная p -группа. Группа G разбивается в объединение классов сопряженных элементов, один из которых равен $\{e\}$. Так как мощности этих классов являются степенями числа p (по теореме 7.1) и сумма этих мощностей — степень p , то кроме $\{e\}$ имеется еще несколько одноэлементных классов. Объединение всех одноэлементных классов совпадает с $Z(G)$.

§ 8. Теорема Силова

Пусть $|G| = p^k m$, где p — простое число, $k \geq 1$ и $\text{нод}(p, m) = 1$. Подгруппа H группы G называется *силовской p -подгруппой*, если $|H| = p^k$.

8.1. Предложение. *Пусть q — степень простого числа p . Тогда $\text{UT}_n(q)$ является силовской p -подгруппой группы $\text{GL}_n(q)$.*

Доказательство. Первой строкой матрицы из $\text{GL}_n(q)$ может быть любая ненулевая строка длины n . Таких строк $(q^n - 1)$ штук. Если мы уже выбрали i первых линейно независимых строк, то $(i + 1)$ -я не должна попадать в их линейную оболочку и, следовательно, вариантов для ее выбора имеется $q^n - q^i$. Поэтому

$$|\text{GL}_n(q)| = \prod_{i=0}^{n-1} (q^n - q^i) = q^{\frac{n(n-1)}{2}} m, \quad (2)$$

где $\text{нод}(p, m) = 1$. Осталось заметить, что $|\text{UT}_n(q)| = q^{\frac{n(n-1)}{2}}$.

8.2. Лемма. Пусть H — силовская p -подгруппа конечной группы G_1 , K — подгруппа группы G_1 , порядок которой делится на p . Тогда существует такой элемент $x \in G_1$, что $K \cap xHx^{-1}$ — силовская p -подгруппа группы K .

Доказательство. Так как $|G_1 : H|$ не делится на p , то одно из слагаемых $|K : K \cap xHx^{-1}|$ в правой части формулы (1) тоже не делится на p . Кроме того, $K \cap xHx^{-1}$ — p -группа как подгруппа p -группы xHx^{-1} . Поэтому $K \cap xHx^{-1}$ является силовской p -подгруппой группы K .

8.3. Теорема (Силов). Пусть G — группа порядка $p^k m$, где p — простое число, $k \geq 1$ и $\text{нод}(p, m) = 1$. Тогда

- 1) в группе G существует силовская p -подгруппа,
- 2) любая p -подгруппа группы G содержится в некоторой силовской p -подгруппе,
- 3) любые две силовские p -подгруппы группы G сопряжены,
- 4) число силовских p -подгрупп делит m и сравнимо с 1 по модулю p .

Доказательство. По следствию 4.2 можно считать, что G — подгруппа группы $\text{GL}_n(p)$ при $n = |G|$. Первое утверждение следует из леммы 8.2 при $G_1 = \text{GL}_n(p)$, $H = \text{UT}_n(p)$, $K = G$, второе (третье) — при $G_1 = G$ и K равном (силовской) p -подгруппе группы G_1 .

Докажем четвертое утверждение. Пусть H — некоторая силовская p -подгруппа группы G . В силу 3) число силовских p -подгрупп группы G равно мощности множества $M = \{gHg^{-1} \mid g \in G\}$. По теореме 7.1 эта мощность равна $|G : N_G(H)|$ и, значит, делит m . Рассмотрим действие H сопряжением на M : группа gHg^{-1} переходит под действием элемента $h \in H$ в группу $hgHg^{-1}h^{-1}$. По предложению 6.2 длины всех орбит являются степенями p . Докажем, что только одна орбита $\{H\}$ имеет длину 1. Действительно, если бы $\{gHg^{-1}\}$ была другой орбитой длины 1, то $H \cdot gHg^{-1}$ была бы группой (докажите!) порядка p^l при $l > k$ по пункту 5 упражнения 2.5. Противоречие. Осталось заметить, что мощность множества M равна сумме длин всех орбит.

8.4. Пример. Группа S_3 содержит три силовских 2-подгруппы: $\{e, (12)\}$, $\{e, (13)\}$ и $\{e, (23)\}$. Их полные прообразы относительно гомоморфизма $\varphi : S_4 \rightarrow S_3$ с ядром K (см. 2.4) равны

$$K \cup (12)K, K \cup (13)K, K \cup (23)K$$

и являются силовскими 2-подгруппами в S_4 . По теореме Силова число силовских 2-подгрупп в S_4 не может быть больше трех.

Рассмотрим S_4 как группу вращений куба (см. пример 2 в п. 6.3). Эти вращения переставляют три квадратных сечения куба, проходящих через его центр. Возникает гомоморфизм из S_4 в S_3 с ядром, состоящим из тождественного отображения и трех вращений на 180° вокруг осей, проходящих через центры противоположных граней. Геометрически, каждая силовская 2-подгруппа группы S_4 состоит из всех вращений куба, оставляющих на месте одно из этих сечений, и изоморфна группе симметрий квадрата.

8.5. Упражнение. Если p — простой делитель $|G|$, то в G существует элемент порядка p .

8.6. Теорема. Мультипликативная группа конечного поля — циклическая.

Доказательство. Пусть K^* — мультипликативная группа конечного поля K и P — ее произвольная силовская p -подгруппа, $|P| = p^k$. По следствию из теоремы Лагранжа порядки элементов из P являются делителями числа p^k . Если бы в P не существовало элемента порядка p^k , то для всех $g \in P$ выполнялось бы $g^{p^{k-1}} = 1$. Однако, в поле K уравнение $x^{p^{k-1}} = 1$ имеет не более p^{k-1} корней. Поэтому в P существует элемент порядка p^k .

Пусть $|K^*| = p_1^{k_1} \cdots p_s^{k_s}$ — разложение на простые числа. По доказанному в K^* существуют элементы порядков $p_1^{k_1}, \dots, p_s^{k_s}$. Ввиду пункта 2 упражнения 1.2 их произведение имеет порядок $|K^*|$ и, значит, порождает группу K^* .

§ 9. Прямые произведения групп

Из нескольких групп G_1, \dots, G_n можно построить группу $G = G_1 \times \dots \times G_n$, состоящую из всех последовательностей вида (g_1, \dots, g_n) , где $g_i \in G_i$, с умножением $(g_1, \dots, g_n) \cdot (g'_1, \dots, g'_n) = (g_1 g'_1, \dots, g_n g'_n)$. Эту группу называют *прямым произведением* групп G_1, \dots, G_n . Ее единицей является элемент (e_1, \dots, e_n) , где e_i — единица группы G_i .

Положим $U_i = \{(e_1, \dots, e_{i-1}, g, e_{i+1}, \dots, e_n) \mid g \in G_i\}$. Тогда U_i — подгруппа группы G , изоморфная группе G_i , и выполняются формулы

$$G = \left\langle \bigcup_{i=1}^n U_i \right\rangle, \tag{3}$$

$$U_i \trianglelefteq G, \tag{4}$$

$$U_i \cap \left\langle \bigcup_{j \neq i} U_j \right\rangle = \{1\} \quad \text{для всех } i. \tag{5}$$

9.1. Теорема. Пусть G — группа, U_1, \dots, U_n — ее подгруппы такие, что выполнены формулы (3)–(5). Тогда $G \cong U_1 \times \dots \times U_n$.

Доказательство. Пусть $a \in U_i, b \in U_j, i \neq j$. Тогда $a(ba^{-1}b^{-1}) = (aba^{-1})b^{-1} \in U_i \cap U_j = \{1\}$, и, значит, $ab = ba$. Ввиду (3) и доказанной перестановочности, каждый элемент $g \in G$ можно записать в виде $g = u_1 \dots u_n$, где $u_i \in U_i$. Эта запись однозначна: если $g = u'_1 \dots u'_n$, где $u'_i \in U_i$, то снова, пользуясь перестановочностью, получаем $(u'_1)^{-1}u_1 = u_2^{-1}u'_2 \dots u_n^{-1}u'_n$. Ввиду (5), отсюда следует, что $u'_1 = u_1$. Аналогично получаем, что $u_i = u'_i$ для всех $i = 1, \dots, n$. Это позволяет определить отображение $\varphi : G \rightarrow U_1 \times \dots \times U_n$ по правилу: $\varphi(g) = (u_1, \dots, u_n)$, если $g = u_1 \dots u_n, u_i \in U_i$. Легко проверить, что φ — изоморфизм.

Если выполняются условия этой теоремы, то будем говорить, что группа G разлагается в прямое произведение своих подгрупп U_1, \dots, U_n .

9.2. Упражнение. Любая группа порядка 6 изоморфна группе Z_6 или S_3 .

Решение. Пусть G — группа порядка 6, H — ее силовская 2-подгруппа, F — ее силовская 3-подгруппа. Очевидно, $F \trianglelefteq G$. Если $H \trianglelefteq G$, то $G \cong H \times F \cong Z_2 \times Z_3 \cong Z_6$. Если $H \not\trianglelefteq G$, то $\bigcap_{x \in G} xHx^{-1} = \{1\}$, и по теореме Кэли $G \cong S_3$.

9.3. Упражнение. Если n, m — взаимно простые натуральные числа, то $Z_{nm} \cong Z_n \times Z_m$.

Конечная циклическая группа называется *примарной циклической*, если ее порядок есть степень некоторого простого числа. Из упражнения 9.3 следует, что всякая конечная циклическая группа разлагается в прямое произведение примарных циклических групп. Следующая теорема обобщает это утверждение.

9.4. Теорема. Всякая конечно порожденная абелева группа разлагается в прямое произведение конечного числа бесконечных циклических и примарных циклических групп. Количество бесконечных циклических и набор порядков примарных циклических групп в любом таком разложении одни и те же.

Доказательство этой теоремы, а также сведения о нильпотентных и разрешимых группах, обобщающих абелевы, имеются, например, в книге [10]. Мы не касаемся этих важных тем, поскольку наша цель — познакомиться с некоторыми нетривиальными примерами простых конечных групп.

§ 10. Простые конечные группы

Группа G называется *простой*, если она неединична и в ней нет собственных нормальных подгрупп. Примером простой группы является циклическая группа простого порядка.

Подобно тому, как для любого натурального числа n существует цепочка

$$1 = n_0 < n_1 < \dots < n_k = n,$$

где $n_i \mid n_{i+1}$ и n_{i+1}/n_i — простые числа, для любой конечной группы G существует цепочка

$$\{1\} = G_0 < G_1 < \dots < G_k = G,$$

где $G_i \trianglelefteq G_{i+1}$ и G_{i+1}/G_i — простые группы. При $\{1\} < G$ ее можно получить последовательными уплотнениями цепочки $\{1\} < G$. Операция уплотнения заключается в следующем: если имеется цепочка $\{1\} = H_0 < H_1 < \dots < H_s = G$ и H_{i+1}/H_i — не простая группа, то взяв в ней собственную нормальную подгруппу H/H_i , можно заменить фрагмент $H_i < H_{i+1}$ фрагментом $H_i < H < H_{i+1}$.

Аналогия между числами и группами нарушается тем, что группа G восстанавливается не всегда однозначно по фактор-группам G_{i+1}/G_i . Простой пример дают две цепочки

$$\{1\} < Z_2 < Z_4 \quad \text{и} \quad \{e\} < \{e, (12)(34)\} < K,$$

где K — группа Клейна из примера 2.4.

Таким образом, для того, чтобы понять строение конечных групп, необходимо изучить не только простые группы, но и способы сборки групп из меньших групп. Следующая теорема полезна тем, что позволяет вести индуктивные рассуждения.

10.1. Теорема. Пусть H — минимальная по включению неединичная нормальная подгруппа конечной группы G . Тогда $H \cong U_1 \times \dots \times U_k$, где все U_i изоморфны одной и той же простой группе.

Доказательство проведем индукцией по порядку группы G . Если группа G проста, то доказывать нечего. Пусть G не проста. Тогда $|H| < |G|$. Пусть V — некоторая минимальная неединичная нормальная подгруппа группы H . По индуктивному предположению V разлагается в прямое произведение изоморфных простых групп. Достаточно доказать с помощью теоремы 9.1, что H разлагается в прямое произведение групп, изоморфных V .

Для любого $g \in G$ имеем $gVg^{-1} \trianglelefteq gHg^{-1} = H$. Группа, порожденная всеми подгруппами gVg^{-1} , нормальна в G и лежит в H . Поэтому

она должна совпадать с H . Пусть X — минимальное по включению подмножество в G такое, что $H = \langle xVx^{-1} \mid x \in X \rangle$. Для каждого $x_0 \in X$ пересечение $x_0Vx_0^{-1} \cap \langle xVx^{-1} \mid x \in X \setminus \{x_0\} \rangle$ нормально в H и строго меньше, чем $x_0Vx_0^{-1}$ (ввиду минимальности X). Так как $x_0Vx_0^{-1}$ — минимальная неединичная нормальная подгруппа в H , то это пересечение равно $\{1\}$. Поэтому H разлагается в прямое произведение групп xVx^{-1} по всем $x \in X$.

10.2. К 1985 году у некоторых известных специалистов по конечным группам возникла уверенность в справедливости следующего утверждения.

Всякая конечная простая группа изоморфна либо циклической группе простого порядка, либо знакопеременной группе A_n при $n \geq 5$, либо простой группе лиева типа, либо одной из 26 sporadicических групп (см. табл. 1).

По группам лиева типа мы рекомендуем книгу [36], по sporadicским группам — книгу [24], описание упомянутых групп имеется в [39]. Доказательство этого утверждения все еще не опубликовано (2002 год). История вопроса освещена в книге [49].

Далее мы докажем, что группа A_n проста при $n \geq 5$, приведем примеры простых групп двух последних типов и затронем проблему восстановления группы G по ее нормальной подгруппе H и фактор-группе G/H .

§ 11. Группа A_n проста при $n \geq 5$

11.1. Лемма. 1) При $n \geq 3$ группа A_n порождается всеми своими тройными циклами.

2) При $n \geq 5$ группа A_n порождается всеми своими подстановками³ вида $(ij)(kl)$.

Доказательство. Группа A_n состоит из тех подстановок из S_n , которые разлагаются в произведении четного числа транспозиций (возможно, зависимость). Осталось заметить, что $(ij)(ik) = (ikj) = (ij)(ab) \cdot (ab)(ik)$ и $(ij)(kl) = (ijk)(jkl)$.

11.2. Упражнение. Пусть α и β — произвольные подстановки из S_n . Запись подстановки $\alpha\beta\alpha^{-1}$ в виде произведения независимых циклов получается из записи для β заменой в ней каждого символа i на символ $\alpha(i)$. В частности, количество и длины независимых циклов в записях подстановок β и $\alpha\beta\alpha^{-1}$ совпадают.

³Здесь и далее разные буквы в подстановке обозначают разные числа.

11.3. Теорема (Галуа). Пусть $n \geq 5$. Тогда

1) A_n — единственная собственная нормальная подгруппа группы S_n ,

2) A_n — простая группа.

Доказательство. 1) Пусть N — собственная нормальная подгруппа группы S_n и пусть σ — некоторая неединичная подстановка из N . Тогда существует i такое, что $\sigma(i) \neq i$. Выберем $j \neq i, \sigma(i)$. Тогда для $\tau = (ij)$ подстановка $\rho = \sigma\tau\sigma^{-1}\tau^{-1}$ неединична и принадлежит N . Далее, ρ есть произведение транспозиций $\sigma\tau\sigma^{-1}$ и τ и, поэтому, является либо тройным циклом, либо подстановкой вида $(ab)(cd)$ (см. доказательство леммы 11.1). Так как подгруппа N нормальна, то по упражнению 11.2 она содержит либо все тройные циклы, либо все подстановки вида $(ab)(cd)$, и, значит, $N = A_n$.

2) По теореме 10.1, $A_n = U_1 \times \dots \times U_k$, где все U_i изоморфны одной и той же простой группе U . Тогда $n!/2 = |U|^k$ и из теоремы Чебышева⁴ следует, что $k = 1$.

Однако, можно завершить доказательство и без теоремы Чебышева. Так как $n \geq 5$, то $|U|$ чётно, и по упражнению 8.5 группа U_1 содержит элемент ρ порядка 2. Такой ρ всегда раскладывается в произведение независимых транспозиций: $\rho = \tau_1\tau_2 \cdots \tau_k$. Тогда $\rho = \tau_1\rho\tau_1^{-1}$, и, значит, $\rho \in U_1 \cap \tau_1 U_1 \tau_1^{-1}$. Так как группы U_1 и $\tau_1 U_1 \tau_1^{-1}$ просты, нормальны в $A_n = \tau_1 A_n \tau_1^{-1}$ и их пересечение неединично, то $U_1 = \tau_1 U_1 \tau_1^{-1}$. Тогда U_1 нормальна в группе $\langle A_n, \tau_1 \rangle = S_n$, и из 1) следует, что $U_1 = A_n$.

§ 12. A_5 как группа вращений икосаэдра

Пусть I — фиксированный икосаэдр в трехмерном евклидовом пространстве (рис. 1), G — группа всех движений этого пространства, сохраняющих ориентацию и переводящих I в I . В группе G имеется тождественное движение, вращения на $k \cdot 72^\circ$ ($k = 1, 2, 3, 4$) вокруг шести осей, проходящих через противоположные вершины икосаэдра, вращения на 180° вокруг осей, проходящих через середины противоположных ребер, и вращения на 120° и 240° вокруг осей, проходящих через центры противоположных граней. Итак, мы нашли 60 движений в группе G . Покажем, что других движений в G нет.

Группа G действует транзитивно на множестве I^0 вершин I , так как любые две вершины из I можно «соединить цепочкой соседних», а соседние можно перевести друг в друга подходящим вращением. Стабилизатор вершины N оставляет на месте также вершину S как наиболее

⁴При $m \geq 2$ между m и $2m$ содержится хотя бы одно простое число. Элементарное доказательство этой теоремы приведено в послесловии к [21]).

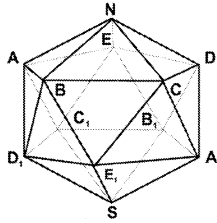


Рис. 1

удаленную от N . Поэтому он состоит из пяти вращений вокруг оси NS , включая тождественное. Следовательно, $|G| = |I^0| \cdot |\text{St}_G(N)| = 12 \cdot 5 = 60$, и, значит, все указанные выше вращения составляют группу G .

Группа G называется *группой вращений икосаэдра*. Докажем, что $G \cong A_5$. Для этого разобьем 30 ребер икосаэдра на пять шестерок. Каждая шестерка состоит из ребер, параллельных или перпендикулярных друг другу. Например, $\{NA, SA_1, CD, C_1D_1, BE_1, B_1E\}$ — одна из таких шестерок. Другие полностью определяются своими начальными ребрами NB, NC, ND и NE и мы их не будем выписывать. Занумеруем эти шестерки числами от 1 до 5 в соответствии с указанным порядком.

Вращения из G переставляют эти шестерки как множества, так как они переводят ребра икосаэдра в ребра и сохраняют отношения параллельности и перпендикулярности. Возникает гомоморфизм $\varphi : G \rightarrow S_5$. Вращению вокруг оси NS на 72° в подходящем направлении соответствует подстановка (12345) . Вращению вокруг оси, проходящей через центры граней (BE_1D_1) и (B_1ED) , на 120° в подходящем направлении, соответствует подстановка (123) . Поэтому $\text{Im } \varphi$ содержит подгруппу $H = \langle (12345), (123) \rangle$. Докажем, что $H = A_5$. Очевидно, $H \leq A_5$ и $|H|$ делится на 15, так как H содержит элементы порядков 3 и 5. По следствию 4.4 в H существует подгруппа H_1 нормальная в A_5 и индекса не большего 4!. Поскольку A_5 — простая группа, то $H_1 = H = A_5$. Так как $G/\text{Ker } \varphi \cong \text{Im } \varphi \cong H = A_5$ и $|G| = |A_5|$, то $G \cong A_5$.

§ 13. A_5 как первая нециклическая простая группа

13.1. Упражнение. Если G — нециклическая группа порядка меньше 60, то G не проста.

Решение. Ввиду теоремы Силова и неединичности центра конечной p -группы, можно исключить те группы, у которых существует единственная силовская p -подгруппа для некоторого p (такая подгруппа

нормальна). С помощью теоремы Силова и следствия 4.4 исключаются также группы порядков 12, 24, 36 и 48. Остаются группы порядков 30 и 56.

Разберем случай, когда $|G| = 56$. Предположим, что в G не одна, а восемь силовских 7-подгрупп. Так как они попарно пересекаются по единице, то общее число элементов в них равно $1 + 8(7 - 1) = 49$. Остаются еще 7 элементов, которые вместе с единичным образуют единственную силовскую 2-подгруппу.

Случай, когда $|G| = 30$ разбирается аналогично, но мы приведем другое доказательство. Отождествим группу G с образом ее регулярного представления в S_{30} . Гомоморфизм из G в группу $\{\pm 1\}$, сопоставляющий четным подстановкам 1, а нечетным -1 , является эпиморфизмом, так как имеющийся в G элемент порядка 2 является произведением 15 независимых транспозиций (по утверждению 1 следствия 4.2) и, значит, нечетен. Поэтому ядро этого гомоморфизма имеет индекс 2 в G и G не проста.

13.2. Теорема. *Если G — простая группа порядка 60, то $G \cong A_5$.*

Доказательство. Из теоремы Силова следует, что G имеет ровно шесть силовских 5-подгрупп. Обозначим их через H_i , $i = 1, \dots, 6$. Индекс $N_G(H_i)$ в G равен числу сопряженных с H_i подгрупп, то есть шести, и, значит, $|N_G(H_i)| = 10$. Пусть $H_1 = \langle a \rangle$, и пусть $\langle b \rangle$ — некоторая силовская 3-подгруппа в G . Порядок группы $\langle a, b \rangle$ делится на 15 и, следовательно, она совпадает с G (иначе по следствию 4.4 в G нашлась бы собственная нормальная подгруппа).

Рассмотрим действие группы G сопряжениями на множестве ее силовских 5-подгрупп. Элемент b не стабилизирует ни одну из H_i , так как в $N_G(H_i)$ нет элементов порядка 3. Поэтому b переставляет по циклу некоторые три силовские 5-подгруппы и переставляет по циклу оставшиеся три. Действие b изображается подстановкой $\bar{b} = (123)(***)$. Элемент a стабилизирует H_1 и (докажите!) переставляет по циклу остальные пять подгрупп. В частности, \bar{a} оставляет символ 1 на месте и некоторая степень \bar{a} переводит 2 в 3. Поэтому, заменяя порождающий a на его степень, можно считать, что $\bar{a} = (23ijk)$. Переобозначая, можно считать также, что $i = 4, j = 5, k = 6$. Для второго цикла в \bar{b} имеются всего две возможности: $(***) = (456)$ и $(***) = (465)$. Первая приводит к тому, что $\overline{a^{-1}b} = (163)$. В частности, элемент $a^{-1}b$ оставляет при сопряжении группу H_2 на месте. Но в $N_G(H_2)$ нет элементов порядка 3. Поэтому реализуется только вторая возможность.

Итак, возникает гомоморфизм из G в S_6 , заданный на порождающих правилом: $a \mapsto (23456)$, $b \mapsto (123)(465)$. Так как G проста, то ядро этого гомоморфизма единично, и, значит, $G \cong \langle (23456), (123)(465) \rangle$.

В частности, G единственна с точностью до изоморфизма. С другой стороны, $|A_5| = 60$ и A_5 проста. Поэтому $G \cong A_5$.

13.3. Упражнение. *Занумеруйте диаметры икосэдра числами от 1 до 6 и найдите его вращения a и b , переставляющие диаметры, как в доказательстве теоремы. Выведите отсюда, что $\langle (23456), (123)(465) \rangle \cong A_5$.*

Поучительно и другое доказательство. Пусть P — силовская 2-подгруппа группы G . Ее порядок равен 4, а порядок ее нормализатора $N_G(P)$ равен 4 или 12 (если $|N_G(P)| = 20$, то G была бы не проста по следствию 4.4). Докажем, что в G во всяком случае есть подгруппа порядка 12.

Предположим, что $|N_G(P)| = 4$. Тогда в группе G имеется 15 силовских 2-подгрупп. Если эти подгруппы попарно пересекаются по единице, то общее число элементов в них равно $1 + (4 - 1) \cdot 15 = 46$. Так как силовских 5-подгрупп в G имеется ровно 6, то общее число элементов в них равно $1 + (5 - 1) \cdot 6 = 25$. Получаем противоречие с тем, что $|G| = 60$. Поэтому найдутся две силовские 2-подгруппы P_i и P_j с пересечением порядка 2. Ввиду пункта 3 упражнения 2.5, $P_i \cap P_j \trianglelefteq \langle P_i, P_j \rangle$, и, следовательно, $\langle P_i, P_j \rangle$ — собственная подгруппа группы G . По следствию 4.4 она имеет индекс больший 4 и строго содержит P_i . Поэтому $|\langle P_i, P_j \rangle| = 12$.

Итак, в группе G во всяком случае найдется подгруппа порядка 12. Ввиду простоты G , из теоремы Кэли следует, что G вкладывается в S_5 . Поэтому можно считать, что G — подгруппа индекса 2 в S_5 . Тогда $G \trianglelefteq S_5$ и $G \cong A_5$ по теореме Галуа.

§ 14. A_5 как проективная специальная линейная группа

Проективной специальной линейной группой $\text{PSL}_n(K)$ над полем K называется фактор-группа группы $\text{SL}_n(K)$ по ее центру. Аналогично определяется группа $\text{PGL}_n(K)$. Напомним, что если поле K конечно и состоит из q элементов, то вместо $\text{SL}_n(K)$ мы пишем $\text{SL}_n(q)$ и т. д.

Поскольку центр группы $\text{SL}_n(q)$ состоит из всех скалярных матриц с определителем 1 (докажите!), то его порядок d равен числу элементов a из мультипликативной группы поля таких, что $a^n = 1$. По теореме 8.6 мультипликативная группа конечного поля — циклическая. Поэтому $d = \text{нод}(q - 1, n)$ ввиду пункта 2 упражнения 1.8. Из формулы (2) с учетом первого примера из пункта 3.2 следует формула

$$|\text{PSL}_n(q)| = \frac{1}{d(q-1)} \prod_{i=0}^{n-1} (q^n - q^i).$$

14.1. Теорема. $\text{PSL}_2(5) \cong \text{PSL}_2(4) \cong A_5$.

Доказательство. 1) Пусть V — векторное пространство столбцов высоты 2 над \mathbb{F}_5 — полем вычетов по модулю 5. Каждый ненулевой вектор из V пропорционален одному из следующих векторов:

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}, \begin{pmatrix} 1 \\ 3 \end{pmatrix}, \begin{pmatrix} 1 \\ 4 \end{pmatrix},$$

а сами эти вектора попарно не пропорциональны. Поэтому V содержит ровно шесть прямых, проходящих через нулевой вектор. Группа $\text{SL}_2(5)$ действует на множестве этих прямых по следующему правилу: прямая $\{kv \mid k \in \mathbb{F}_5\}$, где $0 \neq v \in V$, переводится матрицей $A \in \text{SL}_2(5)$ в прямую $\{kAv \mid k \in \mathbb{F}_5\}$. Скалярные матрицы и только они оставляют каждую прямую на месте. Поэтому группа $\text{PSL}_2(5)$ действует на множестве этих прямых точно. В группе $\text{PSL}_2(5)$ имеются элементы \bar{A} и \bar{B} , являющиеся образами матриц $A = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$ и $B = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Легко проверить, что при подходящей нумерации прямых \bar{A} действует на них, как подстановка (23456), а \bar{B} — как подстановка (123)(465). Возникает гомоморфизм из подгруппы $\langle \bar{A}, \bar{B} \rangle$ группы $\text{PSL}_2(5)$ на группу $\langle (23456), (123)(465) \rangle \cong A_5$ (см. упражнение 13.3). Так как $|\text{PSL}_2(5)| = 60 = |A_5|$, то этот гомоморфизм является изоморфизмом и $\langle \bar{A}, \bar{B} \rangle = \text{PSL}_2(5) \cong A_5$.

2) Пусть V — векторное пространство столбцов высоты 2 над полем $\mathbb{F}_4 = \{0, 1, x, y\}$.⁵ Пространство V содержит ровно пять прямых, проходящих через нулевой вектор. Они имеют направляющие вектора

$$\begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ x \end{pmatrix}, \begin{pmatrix} 1 \\ y \end{pmatrix}.$$

Как и выше, группа $\text{PSL}_2(4)$ действует точно на множестве этих прямых. В группе $\text{PSL}_2(4)$ имеются элементы \bar{A} и \bar{B} , являющиеся образами матриц $A = \begin{pmatrix} x & y \\ x & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$. Легко проверить, что при подходящей нумерации прямых \bar{A} действует на них как подстановка (12345), а \bar{B} — как подстановка (123). Осталось вспомнить (см. § 12), что $\langle (12345), (123) \rangle = A_5$ и завершить доказательство, как в 1).

14.2. Упражнение. $\text{PSL}_2(2) \cong S_3$, $\text{PSL}_2(3) \cong A_4$.

⁵Докажите, что в \mathbb{F}_4 выполняются следующие равенства: $1+1 = x+x = y+y = 0$, $x+1 = y$, $x \cdot x = y$, $y \cdot y = x$, $x \cdot y = 1$.

§ 15. Теорема Жордана–Диксона

15.1. Критерий простоты. Пусть группа G точно и 2-транзитивно действует на множестве X . Тогда G проста, если выполнены следующие условия:

- 1) G совпадает со своим коммутантом G' ,
- 2) в стабилизаторе $\text{St}(x)$ некоторого элемента $x \in X$ содержится такая подгруппа A , что
 - а) A — абелева,
 - б) $A \trianglelefteq \text{St}(x)$,
 - в) $G = \langle gAg^{-1} \mid g \in G \rangle$.

Доказательство. Пусть N — неединичная нормальная подгруппа группы G . По предложению 6.8 группа N действует транзитивно на X , и, следовательно, $G = N \text{St}(x)$. Докажем, что $G = NA$. В силу в) каждый элемент g из G записывается в виде $g = g_1 a_1 g_1^{-1} \dots g_k a_k g_k^{-1}$, где $a_i \in A$, $g_i \in G$. По доказанному каждый элемент g_i записывается в виде $g_i = n_i s_i$, где $n_i \in N$, $s_i \in \text{St}(x)$. Тогда образ элемента g при факторизации по N совпадает с образом элемента $a = s_1 a_1 s_1^{-1} \dots s_k a_k s_k^{-1}$. В силу б) имеем $a \in A$, и, значит, $g \in Na \subseteq NA$. Наконец, $G = G^G = (NA)^G \leq N$, так как при факторизации по N образ любого коммутатора $[n_1 a_1, n_2 a_2]$, где $n_i \in N$, $a_i \in A$, равен образу коммутатора $[a_1, a_2]$, то есть 1 в силу абелевости A .

15.2. Теорема (Жордан–Диксон). Пусть K — поле, $n \geq 2$. Группа $\text{PSL}_n(K)$ проста за исключением двух случаев: $\text{PSL}_2(2)$ и $\text{PSL}_2(3)$.

Доказательство. Пусть V — векторное пространство столбцов высоты n над полем K со стандартным базисом e_1, \dots, e_n . Пусть X — множество всех прямых пространства V , проходящих через 0. Для $0 \neq v \in V$ обозначим через \bar{v} прямую из X с направляющим вектором v . Через \bar{M} обозначим образ матрицы $M \in \text{SL}_n(K)$ в группе $G = \text{PSL}_n(K)$. Определим действие группы G на множестве X правилом $\bar{M}\bar{v} = \overline{Mv}$ и докажем, что это действие удовлетворяет условиям критерия простоты.

Предположим, что \bar{M} стабилизирует каждую прямую из X . Тогда $M e_i = \lambda_i e_i$ и $M(e_1 + \dots + e_n) = \lambda(e_1 + \dots + e_n)$ для некоторых λ_i и λ из K . Пользуясь линейностью, получаем отсюда, что $\lambda_1 = \dots = \lambda_n = \lambda$. Поэтому M — скалярная матрица и $\bar{M} = 1$. Итак, действие G на X точно. Это действие 2-транзитивно, так как прямые \bar{e}_1 и \bar{e}_2 можно перевести в любые две прямые \bar{v}_1 и \bar{v}_2 элементом \bar{M} , где M — такая матрица из $\text{SL}_n(K)$, у которой первый и второй столбец пропорциональны v_1 и v_2 .

Докажем, что $(\mathrm{PSL}_n(K))' = \mathrm{PSL}_n(K)$. Так как из $N \trianglelefteq H$ и $H = H'$ следует, что $(H/N)' = H/N$, то достаточно доказать, что $(\mathrm{SL}_n(K))' = \mathrm{SL}_n(K)$. При $n \geq 3$ это вытекает из пунктов 1) и 2) упражнения 15.3, а при $n = 2$ из пунктов 1) и 3) с учетом того, что при $|K| > 3$ в $\mathrm{SL}_2(K)$ существует нескальная диагональная матрица.

Пусть x — прямая с направляющим вектором e_n . Её стабилизатор $\mathrm{St}(x)$ в группе G состоит из всех \overline{B} таких, что столбец Be_n пропорционален столбцу e_n , то есть $\mathrm{St}(x) = \{\overline{B} \mid B_{1n} = \dots = B_{n-1,n} = 0\}$. Пусть A — подгруппа группы $\mathrm{St}(x)$, состоящая из всех \overline{B} таких, что B отличается от единичной матрицы только элементами, стоящими на местах $(n, 1), \dots, (n, n-1)$. Легко проверить, что A — абелева группа и $A \trianglelefteq \mathrm{St}(x)$. Равенство $\mathrm{PSL}_n(K) = \langle gAg^{-1} \mid g \in \mathrm{PSL}_n(K) \rangle$ следует из того, что в A лежат образы трансвекций вида $t_{ni}(\alpha)$ и из пунктов 1) и 4) упражнения 15.3.

15.3. Упражнение. 1) Группа $\mathrm{SL}_n(K)$ порождается всеми своими трансвекциями $t_{ij}(\alpha)$,

$$2) [t_{ik}(\alpha), t_{kj}(\beta)] = t_{ij}(\alpha\beta) \text{ при различных } i, j, k,$$

3) $[t_{ij}(\alpha), d] = t_{ij}(\alpha(1 - \frac{d_i}{d_j}))$, где d — диагональная матрица из $\mathrm{GL}_n(K)$ с элементами d_1, \dots, d_n на главной диагонали.

4) $M_\sigma t_{ij}(\alpha) M_\sigma^{-1} = t_{\sigma(i)\sigma(j)}(\alpha)$, где $\sigma \in S_n$ и M_σ — матрица, у которой на местах $(\sigma(1), 1), \dots, (\sigma(n), n)$ стоят 1, а на остальных местах — 0.

Как изменится эта формула, если в M_σ заменить одну 1 на -1 ?

15.4. Замечания. 1) Группы $\mathrm{PSL}_n(q)$ при $n \geq 2$, q — простым и $(n, q) \neq (2, 2), (2, 3)$ входят в серию конечных простых групп лиева типа (см. [36, 39]). Все они, кроме конечного числа, не изоморфны знакопеременным группам. Это вытекает из сравнения их порядков. Например, $|\mathrm{PSL}_2(7)| = 168 \neq |A_m|$ ни при каком m . Отметим следующие неожиданные изоморфизмы⁶:

$$\begin{aligned} \mathrm{PSL}_2(4) \cong \mathrm{PSL}_2(5) \cong A_5, \quad \mathrm{PSL}_2(7) \cong \mathrm{PSL}_3(2), \\ \mathrm{PSL}_2(9) \cong A_6, \quad \mathrm{PSL}_4(2) \cong A_8. \end{aligned}$$

Простые группы A_8 и $\mathrm{PSL}_3(4)$ имеют одинаковые порядки, но не изоморфны. Это следует из того, что в A_8 есть элемент порядка 15 (например, (12345)(678), а в $\mathrm{PSL}_3(4)$ такого элемента нет. Действительно, пусть $A = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & x \end{pmatrix}$, где x — порождающий мультипликативной

⁶Их можно разглядеть в группах Матье.

группы поля из четырех элементов. Достаточно доказать, что элемент $\bar{A} \in \text{PSL}_3(4)$ имеет порядок 5 и его централизатор совпадает с $\langle \bar{A} \rangle$. Последнее сводится к проверке того, что из равенства $BA = ABZ$, где $B \in \text{SL}_3(4)$, Z — скалярная матрица из $\text{SL}_3(4)$, следует включение $B \in \langle A \rangle$.

Можно доказать, что $\text{PSL}_3(4)$ — группа наибольшего порядка из серии групп $\text{PSL}_n(q)$, порядок которой совпадает с порядком группы из серии групп A_m .

2) Оказывается, все нециклические простые группы порядка, не превосходящего 1000, имеют порядки 60, 168, 360, 504 и 660 и изоморфны $\text{PSL}_2(q)$ при $q = 4$ и 5 (это доказано в § 13 и § 14), 7, 9, 8 и 11 соответственно.

В следующем параграфе мы определим одну из 26 спорадических групп — группу Матье M_{22} и докажем ее простоту. Эта группа не изоморфна A_n и $\text{PSL}_n(q)$ ни при каких n и q , однако в ее конструкции активно участвует группа $\text{PSL}_3(4)$.

§ 16. Группа Матье M_{22}

Пусть \mathbb{F}_q — поле из q элементов, V — векторное пространство размерности 3 над \mathbb{F}_q , x_1, x_2, x_3 — его база. *Проективная плоскость* $\mathbb{P}_2(q)$ — это множество всех одномерных подпространств пространства V . Его элементы называются *точками*, а подмножества, соответствующие двумерным подпространствам пространства V — *проективными прямыми*. Для краткости мы будем называть их прямыми: из контекста будет ясно, когда идет речь о прямых V , и когда о прямых $\mathbb{P}_2(q)$.

Обозначим через \bar{v} точку $\mathbb{P}_2(q)$, соответствующую прямой в V с направляющим вектором v . Через $l(\bar{v}_1, \bar{v}_2)$ обозначим прямую $\mathbb{P}_2(q)$, соответствующую плоскости в V , натянутой на вектора v_1, v_2 . Так как в V ровно $(q^3 - 1)$ ненулевых векторов и на каждой прямой в V лежит ровно $(q - 1)$ ненулевых векторов, то в V имеется ровно $\frac{q^3 - 1}{q - 1} = q^2 + q + 1$ прямых. Поэтому в $\mathbb{P}_2(q)$ имеется ровно $q^2 + q + 1$ точек. Их можно записать в виде $\bar{x}_1 + a_2\bar{x}_2 + a_3\bar{x}_3$, $\bar{x}_2 + a_3\bar{x}_3$ и \bar{x}_3 , где $a_2, a_3 \in \mathbb{F}_q$. Существует биективное соответствие между множеством плоскостей и множеством прямых в V : каждой плоскости соответствует «ортогональная» ей прямая. Поэтому плоскостей в V , а значит и прямых в $\mathbb{P}_2(q)$, имеется тоже $q^2 + q + 1$.

16.1 Упражнение. На каждой прямой в $\mathbb{P}_2(q)$ лежит ровно $q + 1$ точка.

Обозначим образ матрицы $A \in \text{GL}_3(q)$ в группе $\text{PGL}_3(q)$ через \overline{A} . Группа $\text{PGL}_3(q)$ естественно действует на множестве точек $\mathbb{P}_2(q)$: для $\overline{a_1x_1 + a_2x_2 + a_3x_3}$ из $\mathbb{P}_2(q)$ и \overline{A} из $\text{PGL}_3(q)$ положим

$$\overline{A} \cdot \overline{a_1x_1 + a_2x_2 + a_3x_3} = \overline{b_1x_1 + b_2x_2 + b_3x_3},$$

где

$$A \cdot \begin{pmatrix} a_1 \\ a_2 \\ a_3 \end{pmatrix} = \begin{pmatrix} b_1 \\ b_2 \\ b_3 \end{pmatrix}.$$

16.2. Упражнение. Докажите, что это действие корректно определено, точно, дважды транзитивно и переводит прямые в прямые.

16.3. Определение. Автоморфизмом проективной плоскости $\mathbb{P}_2(q)$ называется любая перестановка точек $\mathbb{P}_2(q)$, переводящая прямые в прямые.

Через $\text{Aut}(\mathbb{P}_2(q))$ обозначим группу всех автоморфизмов плоскости $\mathbb{P}_2(q)$. В силу упражнения 16.2 можно считать, что $\text{PGL}_3(q) \leq \text{Aut}(\mathbb{P}_2(q))$.

Определим теперь систему M , состоящую из точек и блоков (стандартных и нестандартных).

Точки M — это точки $\mathbb{P}_2(4)$ и еще одна точка, обозначаемая символом ∞ .

Стандартные блоки — это прямые $\mathbb{P}_2(4)$, пополненные точкой ∞ .

Нестандартные блоки (овалы) — это образы овала

$$O = \{\overline{x_1}, \overline{x_2}, \overline{x_3}, \overline{x_1 + x_2 + x_3}, \overline{x_1 + ax_2 + a^{-1}x_3}, \overline{x_1 + a^{-1}x_2 + ax_3}\}$$

под действием элементов группы $\text{PSL}_3(4)$. Мы рассматриваем группу $\text{PSL}_3(4)$ как подгруппу группы $\text{PGL}_3(4)$.

Множество всех точек системы M обозначим через M^0 , а множество всех ее блоков — через M^1 .

16.4. Упражнение. Проверьте, что любые три точки овала O не лежат на одной прямой.

Отсюда следует, что любые три точки произвольного овала не лежат на одной прямой.

16.5. Определение. Автоморфизмом системы M назовем любую перестановку точек M , переводящую блоки в блоки (возможно, стандартные в нестандартные и наоборот).

Обозначим через $\text{Aut}(M)$ группу всех автоморфизмов M , а через M_{22} — группу всех четных автоморфизмов M .

16.6. Теорема. *Группа Маттье M_{22} проста.*

Мы докажем эту теорему с помощью семи лемм.

Пусть $\mathbb{F}_4 = \{0, 1, a, a^{-1}\}$ — поле из 4 элементов. Напомним, что $1 + 1 = a + a = a^{-1} + a^{-1} = 0$, $1 + a = a^{-1}$ и $a^3 = 1$. Пусть f — автоморфизм поля \mathbb{F}_4 , переставляющий a и a^{-1} . Он задает биекцию из V в V , переводящую произвольную точку $a_1x_1 + a_2x_2 + a_3x_3$ в точку $f(a_1)x_1 + f(a_2)x_2 + f(a_3)x_3$. Поскольку эта биекция переводит прямые в прямые и плоскости в плоскости, то она индуцирует автоморфизм f^* проективной плоскости $\mathbb{P}_2(4)$, который задается формулой

$$f^*(\overline{a_1x_1 + a_2x_2 + a_3x_3}) = \overline{f(a_1)x_1 + f(a_2)x_2 + f(a_3)x_3}.$$

Группа G называется *расщепляемым расширением группы H посредством группы F* , если $H \trianglelefteq G$ и в G существует подгруппа $F_1 \cong F$ такая, что $H \cap F_1 = \{1\}$ и $HF_1 = G$. В этом случае пишут $G = H \rtimes F$.

16.7. Лемма. $\text{Aut}(\mathbb{P}_2(4)) = \text{PGL}_3(4) \rtimes \langle f^* \rangle$.

Доказательство. Пусть $\alpha \in \text{Aut}(\mathbb{P}_2(4))$. Умножая α на элементы группы $\text{PGL}_3(4)$ и на f^* , приведем α к 1. Так как $\text{PGL}_3(4)$ действует транзитивно на множестве точек $\mathbb{P}_2(4)$, то можно считать, что

1) α фиксирует \bar{x}_1 .

Пусть Δ — множество из пяти прямых, проходящих через \bar{x}_1 (рис. 2).

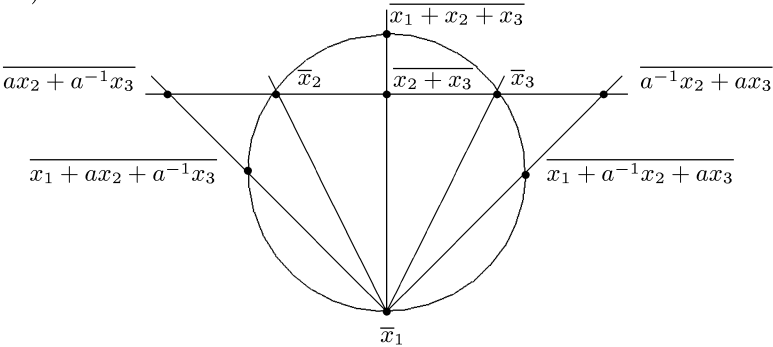


Рис. 2

Стабилизатор \bar{x}_1 в $\text{PGL}_3(4)$ действует на Δ 2-транзитивно⁷, а f^* переставляет прямые $l(\bar{x}_1, \overline{a^{-1}x_2 + ax_3})$ и $l(\bar{x}_1, \overline{ax_2 + a^{-1}x_3})$, оставляя остальные три прямые из Δ на месте. Пусть l_1 и l_2 — любые две пря-

⁷ *Указание.* Посмотрите, куда переходят прямые $l(\bar{x}_1, \bar{x}_2)$ и $l(\bar{x}_1, \bar{x}_3)$ под действием элемента (a_{ij}) из $\text{PGL}_3(4)$, где $a_{11} = 1$, $a_{21} = a_{31} = 0$.

мые из Δ , g — элемент группы $\text{PGL}_3(4)$, стабилизирующий \bar{x}_1 и переводящий l_1 и l_2 в прямые $l(\bar{x}_1, a^{-1}x_2 + ax_3)$ и $l(\bar{x}_1, ax_2 + a^{-1}x_3)$ соответственно. Тогда преобразование $g^{-1}f^*g$ переставляет прямые l_1 и l_2 и оставляет остальные три прямые из Δ на месте. Так как группа перестановок множества Δ порождается транспозициями, то можно считать, что

2) α оставляет на месте каждую прямую из Δ .

Пусть $Q_{bc} = \begin{pmatrix} 1 & b & c \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$. Группа $\{\bar{Q}_{bc} \mid b, c \in \mathbb{F}_4\}$ фиксирует \bar{x}_1 и оставляет каждую прямую из Δ на месте. Кроме того, она действует транзитивно на множестве остальных 16 прямых $\mathbb{P}_2(4)$. Это следует из того, что каждая такая прямая пересекает прямые $l(\bar{x}_1, \bar{x}_2)$ и $l(\bar{x}_1, \bar{x}_3)$ по точкам вида $b\bar{x}_1 + x_2$ и $c\bar{x}_1 + x_3$, и, следовательно, является \bar{Q}_{bc} -образом прямой $k = l(\bar{x}_2, \bar{x}_3)$. Поэтому можно считать, что

3) α оставляет прямую k на месте.

Ввиду 2) α фиксирует k поточечно. Элемент \bar{A} , где $A = \text{diag}(a, 1, 1)$, тоже фиксирует k поточечно и еще фиксирует \bar{x}_1 . Кроме того, \bar{A} переставляет по циклу три точки прямой $m = l(\bar{x}_1, \bar{x}_2)$, отличные от \bar{x}_1 и \bar{x}_2 . Поэтому, умножив α на подходящую степень элемента \bar{A} , можно считать, что

4) α фиксирует прямые k и m поточечно.

Любая прямая, не проходящая через точку $k \cap m$, α -инвариантна, так как пересекает $k \cup m$ в двух точках. Через любую точку, отличную от точки $k \cap m$, можно провести две такие прямые. Поэтому все точки $\mathbb{P}_2(4)$ фиксируются α , и, значит, $\alpha = 1$.

Подгруппа $\text{PGL}_3(4)$ нормальна в группе $\text{Aut}(\mathbb{P}_2(4))$, так как для любого элемента $\bar{A} \in \text{PGL}_3(4)$ выполняется $f^*\bar{A}(f^*)^{-1} = \bar{A}^*$, где A^* — матрица, получающаяся из A применением к ее элементам автоморфизма f .

16.8. Лемма.

1) $\text{St}_{\text{PSL}_3(4)}(O) = \text{St}_{\text{PGL}_3(4)}(O) \cong A_6$.

2) $\text{St}_{\text{Aut}(\mathbb{P}_2(4))}(O) \cong S_6$.

Доказательство. Докажем, что $\text{St}_{\text{PSL}_3(4)}(O) \cong A_6$. Заметим сначала, что группа $G = \text{St}_{\text{PSL}_3(4)}(O)$ действует точно на шести точках овала O : если элемент $\bar{A} \in G$ фиксирует точки $\bar{x}_1, \bar{x}_2, \bar{x}_3$ и $\overline{x_1 + x_2 + x_3}$, то матрица $A \in \text{SL}_3(4)$ скалярна, значит, $\bar{A} = 1$.

Рассмотрим матрицы

$$A = \begin{pmatrix} 1 & 0 & 1 \\ 0 & 0 & 1 \\ 0 & 1 & 1 \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 0 & a^{-1} \\ 0 & 0 & 1 \\ 0 & 1 & a \end{pmatrix}, \quad C = \begin{pmatrix} 0 & 0 & 1 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}.$$

Легкие вычисления показывают, что $\overline{A}, \overline{B}, \overline{C} \in G$. Более того, \overline{A} и \overline{B} стабилизируют \overline{x}_1 и действуют на множестве $O \setminus \{\overline{x}_1\}$ как тройной цикл и как цикл длины пять. Обозначим через $G_{\overline{x}_1}$ стабилизатор \overline{x}_1 в G . Так как тройной цикл и цикл длины пять в группе S_5 порождают подгруппу A_5 , то $G_{\overline{x}_1} \cong A_5$.

Элемент \overline{C} сдвигает \overline{x}_1 в область действия цикла длины 5. Поэтому G действует транзитивно на O , и, значит, $|G| = |G_{\overline{x}_1}| \cdot |O| \geq 360$. Отсюда G изоморфна либо S_6 , либо подгруппе индекса 2 в S_6 . В первом случае в G существовал бы элемент, фиксирующий точки $\overline{x}_1, \overline{x}_2, \overline{x}_3$ и $\overline{x}_1 + \overline{x}_2 + \overline{x}_3$, и переставляющий $\overline{x}_1 + a\overline{x}_2 + a^{-1}\overline{x}_3$ и $\overline{x}_1 + a^{-1}\overline{x}_2 + a\overline{x}_3$. Однако, это невозможно ввиду начала доказательства. Во втором случае $G \cong A_6$ ввиду пункта 3 упражнения 2.5 и теоремы Галуа.

Аналогично доказывается, что $\text{St}_{\text{PGL}_3(4)}(O) \cong A_6$, и, значит, $\text{St}_{\text{PSL}_3(4)}(O) = \text{St}_{\text{PGL}_3(4)}(O)$. Второе утверждение леммы вытекает из первого с учетом леммы 16.7 и того, что f^* действует на O как транспозиция, переставляющая последние две точки O .

Доопределим действие f^* и $\text{PGL}_3(4)$ на M , положив $f^*\infty = \infty$ и $\overline{A}\infty = \infty$ для любого элемента $\overline{A} \in \text{PGL}_3(4)$. Сразу отметим, что элементы из $\text{PSL}_3(4)$ и f^* переводят блоки в блоки. Для элементов из $\text{PSL}_3(4)$ это очевидно. Также очевидно, что f^* переводит стандартные блоки в стандартные. То, что f^* переводит нестандартные блоки в нестандартные следует из того, что для любого $\overline{A} \in \text{PSL}_3(4)$ выполняется равенство $f^*\overline{A}O = f^*\overline{A}(f^*)^{-1} \cdot f^*O = f^*\overline{A}(f^*)^{-1}O = \overline{A^*}O$ и $\overline{A^*} \in \text{PSL}_3(4)$.

16.9. Лемма. *Через любые три точки в $\mathbb{P}_2(4)$, не лежащие на одной прямой, проходит единственный овал.*

Доказательство. Пусть $\overline{v}_i = \overline{a_{1i}x_1 + a_{2i}x_2 + a_{3i}x_3}$, $i = 1, 2, 3$, — три точки, не лежащие на одной прямой. Разделив элементы последнего столбца матрицы $A = (a_{ji})$ на $\det(A)$, можно считать, что $\overline{A} \in \text{PSL}_3(4)$ и $\overline{v}_i = \overline{A}\overline{x}_i$, $i = 1, 2, 3$. Поэтому достаточно доказать, что точки $\overline{x}_1, \overline{x}_2, \overline{x}_3$ принадлежат единственному овалу O . Предположим, что эти точки принадлежат еще овалу $\overline{B}O$. Так как $\text{St}_{\text{PSL}_3(4)}(O) \cong A_6$ и группа A_6 действует на O 4-транзитивно (см. п. 6.6), то существует такой элемент $\overline{S} \in \text{St}_{\text{PSL}_3(4)}(O)$, что $\overline{S} \cdot \overline{B}\overline{x}_i = \overline{x}_i$, $i = 1, 2, 3$. Тогда матрица $\overline{S}\overline{B}$ равна некоторой степени матрицы $\overline{D} = \text{diag}(1, a, a^{-1})$ с точностью до скалярного множителя. Так как $\overline{D}O = \overline{S}O = O$, то и $\overline{B}O = O$.

16.10. Лемма. $\text{St}_{M_{22}}(\infty) = \text{PSL}_3(4)$.

Доказательство. Группа $\text{St}_{M_{22}}(\infty)$ состоит из тех четных биекций множества точек плоскости $\mathbb{P}_2(4)$ на себя, которые

1) сохраняют блоки M , лежащие в $\mathbb{P}_2(4)$ (это $\text{PSL}_3(4)$ -образы овала O),

2) сохраняют блоки M , проходящие через ∞ , то есть сохраняют прямые $\mathbb{P}_2(4)$.

Отсюда и из леммы 16.7 вытекает, что

$$\text{St}_{M_{22}}(\infty) \leq \text{Aut}(\mathbb{P}_2(4)) = \text{PGL}_3(4) \rtimes \langle f^* \rangle = \text{PSL}_3(4) \rtimes (\langle \bar{A} \rangle \rtimes \langle f^* \rangle),$$

где $A = \text{diag}(a, 1, 1)$. Легко доказать, что $\langle \bar{A} \rangle \rtimes \langle f^* \rangle \cong S_3$.

Чтобы вычислить $\text{St}_{M_{22}}(\infty)$ точно, надо выделить в группе $\text{PSL}_3(4) \rtimes (\langle \bar{A} \rangle \rtimes \langle f^* \rangle)$ только те четные биекции, которые удовлетворяют условию 1).

Ясно, что $\text{PSL}_3(4)$ подходит, так как, если какой-то элемент из $\text{PSL}_3(4)$ осуществлял бы нечетную перестановку точек $\mathbb{P}_2(4)$, то в $\text{PSL}_3(4)$ существовала бы подгруппа индекса 2 (пересечение $\text{PSL}_3(4)$ и группы четных подстановок), что противоречит простоте $\text{PSL}_3(4)$.

Элемент \bar{A} не подходит, так как $|\bar{A}O \cap O| = 3$ и из леммы 16.9 следует, что $\bar{A}O$ — не овал. Аналогично доказывается, что элемент $(\bar{A})^2$ не подходит.

Элемент f^* стабилизирует 7 точек $\mathbb{P}_2(4)$ (это точки $\bar{x}_1, \bar{x}_2, \bar{x}_3, \overline{x_1 + x_2}, \overline{x_1 + x_3}, \overline{x_2 + x_3}$ и $\overline{x_1 + x_2 + x_3}$)⁸, а остальные 14 точек разбивает на 7 пар, переставляя точки в каждой паре. Поэтому f^* — нечетная биекция и не входит в M_{22} . Остальные два элемента порядка 2 группы $\langle \bar{A} \rangle \rtimes \langle f^* \rangle$ сопряжены с f^* и, значит, тоже нечетны и не входят в M_{22} .

16.11. Лемма. *Существует элемент $g \in M_{22}$, переставляющий \bar{x}_1 и ∞ .*

Доказательство. Всякую точку $\bar{z} = \overline{a_1x_1 + a_2x_2 + a_3x_3}$ из $\mathbb{P}_2(4)$ можно представить единственным образом в каноническом виде:

$$\bar{z} = \bar{x}_1, \text{ если } a_2 = a_3 = 0,$$

$$\bar{z} = \overline{ux_1 + x_2}, \text{ если } a_2 \neq 0, a_3 = 0,$$

$$\bar{z} = \overline{ux_1 + x_3}, \text{ если } a_2 = 0, a_3 \neq 0,$$

$$\bar{z} = \overline{ux_1 + vx_2 + v^{-1}x_3}, \text{ если } a_2 \neq 0 \text{ и } a_3 \neq 0.$$

Определим биекцию $\varphi : M^0 \rightarrow M^0$ по правилу:

$$\varphi(\bar{x}_1) = \infty, \varphi(\infty) = \bar{x}_1,$$

$$\varphi(\overline{ux_1 + x_2}) = \overline{ux_1 + x_2},$$

⁸Эти 7 точек образуют проективную подплоскость $\mathbb{P}_2(2)$ плоскости $\mathbb{P}_2(4)$.

$$\varphi(\overline{ux_1 + x_3}) = \overline{ux_1 + x_3},$$

$$\varphi(\overline{ux_1 + vx_2 + v^{-1}x_3}) = \overline{(u+1)x_1 + vx_2 + v^{-1}x_3}$$

при $u \in \mathbb{F}_4$, $v \in \mathbb{F}_4 \setminus \{0\}$.

Ясно, что φ^2 — тождественное преобразование. Стандартные блоки, проходящие через \bar{x}_1 (см. рис. 2), инвариантны относительно φ , стандартный блок, проходящий через \bar{x}_2 и \bar{x}_3 , переходит в овал O . Поэтому φ можно рассматривать как инверсию в M по аналогии с инверсией в евклидовой плоскости, пополненной бесконечно удаленной точкой.

Докажем, что $\varphi \in \text{Aut}(M)$, то есть φ переводит блоки в блоки. Сначала проверим, что стандартные блоки, не проходящие через \bar{x}_1 , переходят в нестандартные. Таких блоков 16 штук — ровно столько, сколько прямых в $\mathbb{P}_2(4)$, не проходящих через \bar{x}_1 . Каждый такой блок является \overline{Q}_{bc} -образом блока $l = l(\bar{x}_2, \bar{x}_3) \cup \{\infty\}$ при подходящих $b, c \in \mathbb{F}_4$ (см. доказательство леммы 16.7). Непосредственные вычисления показывают, что преобразования \overline{Q}_{bc} и φ перестановочны. Тогда для любого стандартного блока l' , не проходящего через \bar{x}_1 , получаем, что $\varphi(l') = \varphi(\overline{Q}_{bc} l) = \overline{Q}_{bc} \varphi(l) = \overline{Q}_{bc} O$ является нестандартным блоком.

Осталось проверить, что произвольный овал P под действием φ переходит в некоторый блок. Ввиду перестановочности преобразований \overline{Q}_{bc} и φ достаточно проверить это для подходящего овала $\overline{Q}_{bc} P$. Через пары точек овала P проходят 15 прямых. Выберем одну из них, не проходящую через точку \bar{x}_1 . Заменяя P подходящим овалом $\overline{Q}_{bc} P$, можно считать, что это прямая $k = l(\bar{x}_2, \bar{x}_3)$. Пусть $H = \langle \overline{H}_1, \overline{H}_2 \rangle$, где

$$H_1 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & a & 0 \\ 0 & 0 & a^{-1} \end{pmatrix}, \quad H_2 = \begin{pmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{pmatrix}.$$

Группа H оставляет k на месте и любая пара точек из k переводится подходящим элементом из H в одну из пар $\{\bar{x}_2, \bar{x}_3\}$, $\{\bar{x}_2, \bar{x}_2 + x_3\}$, $\{\bar{x}_2 + x_3, a\bar{x}_2 + a^{-1}x_3\}$. Так как φ поэлементно перестановочно с H , то можно считать, что P пересекается с k по одной из этих пар. Из упражнения 16.12 следует, что φ переводит овал P в некоторый блок.

Итак, $\varphi \in \text{Aut}(M)$. Однако, $\varphi \notin M_{22}$, так как φ осуществляет нечетную перестановку точек M : φ — элемент порядка 2, оставляющий на месте 8 точек из 22. Автоморфизм f^* , как отмечалось выше, тоже нечетен. Поэтому $f^*\varphi \in M_{22}$ и, кроме того, $f^*\varphi(\bar{x}_1) = \infty$ и $f^*\varphi(\infty) = \bar{x}_1$.

16.12. Упражнение. Докажите с помощью леммы 16.9, что через каждую пару точек $\mathbb{P}_2(4)$ проходит ровно 4 овала. Выпишите все овалы, проходящие через пары точек $\{\bar{x}_2, \bar{x}_3\}$, $\{\bar{x}_2, \bar{x}_2 + x_3\}$,

$\{\overline{x_2 + x_3}, \overline{ax_2 + a^{-1}x_3}\}$, и проверьте, что они переходят в блоки под действием φ .

16.13. Лемма. *Группа M_{22} действует 3-транзитивно на множестве M^0 точек системы M .*

Доказательство. Легко понять, что если группа G действует транзитивно на множестве X и стабилизатор G_x некоторого элемента $x \in X$ действует $(k - 1)$ -транзитивно на множестве $X \setminus \{x\}$, то G действует k -транзитивно на X . Поэтому, ввиду леммы 16.10, достаточно доказать, что M_{22} действует транзитивно на множестве M^0 . Последнее очевидно, так как точку ∞ можно перевести в точку \bar{x}_1 элементом $f^*\varphi$, а \bar{x}_1 можно перевести в любую точку $\mathbb{P}_2(4)$ элементом из $\text{PSL}_3(4)$.

16.14. Упражнение. *Группа M_{22} действует транзитивно на множестве M^1 блоков системы M .*

Указание. Подгруппа $\text{PSL}_3(4)$ группы M_{22} действует транзитивно на множестве стандартных блоков и на множестве нестандартных блоков (по лемме 16.9), а преобразование $f^*\varphi \in M_{22}$ переводит нестандартный блок O в стандартный блок $l(\bar{x}_2, \bar{x}_3) \cup \{\infty\}$.

16.15. Определение. *Группа N действует регулярно на множестве X , если N действует транзитивно на X и стабилизатор в N любого элемента из X единичен.*

16.16. Лемма. *Пусть группа G действует 2-транзитивно на множестве X и N — неединичная конечная нормальная подгруппа в G . Если N действует регулярно на X , то $|X| = p^k$, где p — простое число.*

Доказательство. Пусть x — произвольный элемент из X , G_x — стабилизатор x в G . Так как G действует 2-транзитивно на X , то G_x действует транзитивно на $X \setminus \{x\}$. Поэтому для любых неединичных элементов $n_1, n_2 \in N$ существует такой элемент $g \in G_x$, что $g(n_1 x) = n_2 x$, и, значит, $gn_1 g^{-1} x = n_2 x$. Так как N действует на X регулярно, то $gn_1 g^{-1} = n_2$. В частности, все неединичные элементы из N имеют одинаковый порядок и, следовательно, N — p -группа. Из регулярности также следует, что $|X| = |N|$, и доказательство закончено.

Доказательство теоремы 16.6. Пусть N — неединичная нормальная подгруппа в M_{22} . Ввиду предложения 6.7 и леммы 16.13, N действует транзитивно на M^0 . Поэтому $M_{22} = N \cdot \text{St}_{M_{22}}(\infty)$. Так как $|M^0| = 22$ не является степенью простого числа, то по лемме 16.16 группа N действует не регулярно на M^0 , то есть $\text{St}_{M_{22}}(\infty) \cap N \neq \{1\}$. Остаток заметить, что $\text{St}_{M_{22}}(\infty) \cap N \trianglelefteq \text{St}_{M_{22}}(\infty)$, и что группа $\text{St}_{M_{22}}(\infty) = \text{PSL}_3(4)$ проста. Тогда $\text{St}_{M_{22}}(\infty) \leq N$, и, следовательно, $M_{22} = N$.

16.17. Упражнение. $|M_{22}| = |\mathrm{PSL}_3(4)| \cdot 22 = 2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$.
Группа M_{22} не изоморфна A_n и $\mathrm{PSL}_n(q)$ ни при каких n и q .

§ 17. Группы Матье, системы Штейнера и теория кодирования

Системой Штейнера $S(v, k, t)$ называется множество X из v элементов (*точек*) с таким набором его k -элементных подмножеств (*блоков*), что каждое t -элементное подмножество множества X содержится в единственном блоке.

Системы Штейнера естественно обобщают проективные плоскости $\mathbb{P}_2(q)$, блоками которых являются проективные прямые.

Автоморфизмом системы Штейнера называется такая перестановка ее точек, которая индуцирует перестановку ее блоков.

Систему Штейнера $S(v, k, t)$, $t \geq 2$, можно преобразовать в систему Штейнера $S(v-1, k-1, t-1)$, удалив из множества X некоторую точку x и взяв в качестве блоков только те $(k-1)$ -элементные подмножества, которые получаются удалением точки x из блоков системы $S(v, k, t)$. Если система Штейнера S получается из системы Штейнера \tilde{S} таким образом, то \tilde{S} называется *расширением* S . В § 16 мы, фактически, построили расширение $M = S(22, 6, 3)$ системы Штейнера $\mathbb{P}_2(4) = S(21, 5, 2)$. Оказывается, можно расширять эти системы и дальше:

$$S(21, 5, 2) \prec S(22, 6, 3) \prec S(23, 7, 4) \prec S(24, 8, 5),$$

причем эти системы Штейнера определены с точностью до изоморфизма, а система $S(24, 8, 5)$ далее не расширяется. Группы Матье M_v являются группами четных автоморфизмов этих систем при $v = 22, 23$ и 24 (при $v = 23$ и 24 все автоморфизмы будут четными).

В конструкции системы $S(24, 8, 5)$ участвуют овалы, подплоскости $\mathbb{P}_2(2)$ и симметрические разности пар прямых проективной плоскости $\mathbb{P}_2(4)$. Ниже мы опишем другую конструкцию системы $S(24, 8, 5)$, использующую теорию кодирования.

Пусть F^n — векторное пространство размерности n над полем $F = \{0, 1\}$. Вектора из F^n будем называть *словами* и записывать в виде последовательностей длины n , состоящих из букв 0 и 1. Через $\mathbf{0}$ обозначим слово, состоящее из n нулей, а через $\mathbf{1}$ — слово, состоящее из n единиц.

Для u и v из F^n через $d(u, v)$ обозначим число мест, где буквы слов u и v не совпадают. Функция d определяет расстояние между словами u и v и называется *метрикой Хэмминга*, а число $d(\mathbf{0}, u)$ — *весом*

слова u . *Носителем* слова $u \in F^n$ называется множество номеров его единичных букв.

17.1. Определение. *Бинарным s -кодом, исправляющим ошибки,* называется любое непустое подмножество $C \subseteq F^n$ такое, что

$$d(u, v) \geq 2s + 1 \quad \text{при } u, v \in C, u \neq v.$$

Для $r \in \mathbb{N}$ и $u \in F^n$ положим $B(u, r) = \{v \in F^n \mid d(u, v) \leq r\}$. Тогда условие этого определения можно переписать в виде

$$B(u, s) \cap B(v, s) = \emptyset \quad \text{при } u, v \in C, u \neq v.$$

Бинарный s -код C называется *совершенным*, если

$$\cup_{u \in C} B(u, s) = F^n.$$

Представим, что мы передаем (скажем, по Internet) сообщение, закодированное словами из C . Помехи или неисправности на линии могут привести к ошибкам: в некоторых словах какие-то 0 заменятся на 1, а 1 — на 0. В результате могут получиться слова вовсе не из C . Однако, если в каждом слове сделано не более s ошибок, то абонент, зная код C , может исправить все ошибки и полностью восстановить сообщение. Для этого он должен каждое полученное слово \bar{u} заменить на ближайшее к нему в смысле метрики Хэмминга слово u из C .

Задача теории кодирования состоит в том, чтобы найти наиболее эффективные коды, исправляющие как можно больше ошибок.

17.2 Примеры. 1) Любое подпространство C пространства F^n является бинарным s -кодом при $s = \left\lfloor \left(\min_{\mathbf{0} \neq u \in C} d(\mathbf{0}, u) - 1 \right) / 2 \right\rfloor$.

Такой код называется *линейным* или (n, m) -кодом, где $m = \dim C$. *Группой автоморфизмов линейного кода $C \subseteq F^n$* называется группа всех линейных преобразований пространства F^n , которые переставляют стандартные⁹ базисные вектора $e_i, i = 1, \dots, n$, и оставляют подпространство C на месте.

Расширением линейного кода $C \subseteq F^n$ называется код

$$\bar{C} = \{(c_0, c_1, \dots, c_n) \mid (c_1, \dots, c_n) \in C, \sum_{i=0}^n c_i = 0\},$$

лежащий в F^{n+1} .

⁹ i -я координата вектора e_i равна 1, остальные — нули.

2) Пусть $k \geq 1$, $n = 2^k - 1$. *Бинарным кодом Хэмминга* называется $(n, n-k)$ -код $C = \{u \in F^n \mid uH = 0\}$, где H — матрица размера $n \times k$, чьи строки — все ненулевые вектора пространства F^k в некотором порядке. Отсюда следует, что вес ненулевых слов из C не меньше 3, и, значит, C является 1-кодом. Код Хэмминга является совершенным 1-кодом, так как

$$|B(u, 1)| = 1 + n = 2^k, \quad |C| = 2^{n-k} \quad \text{и} \quad |\cup_{u \in C} B(u, 1)| = 2^n = |F^n|.$$

17.3. Упражнение. Докажите, что подпространство $C \subseteq F^7$, порожденное строками матрицы

$$\begin{pmatrix} 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 & 1 \end{pmatrix},$$

является $(7, 4)$ -кодом Хэмминга.

Этот код *циклический*, так как вместе с каждым словом (c_1, c_2, \dots, c_7) содержит его циклический сдвиг (c_2, \dots, c_7, c_1) . Множество $\{1, 2, \dots, 7\}$ и носители слов веса 3 кода C образуют систему Штейнера $S(7, 3, 2)$, которую можно отождествить с проективной плоскостью $\mathbb{P}_2(2)$. Отсюда следует (докажите!), что группы автоморфизмов $(7, 4)$ -кода Хэмминга, системы Штейнера $S(7, 3, 2)$ и проективной плоскости $\mathbb{P}_2(2)$ изоморфны одной и той же простой группе $\text{PSL}_3(2)$ порядка 168.

17.4. Теорема. Множество $X = \{1, 2, \dots, 8\}$ и носители слов веса 4 в расширенном $(8, 4)$ -коде Хэмминга \overline{C} образуют систему Штейнера $S(8, 4, 3)$.

Доказательство. Выписав все 16 слов этого кода, можно убедиться, что он содержит слова $\mathbf{0}$, $\mathbf{1}$ и 14 слов веса 4. Носители различных слов u и v из \overline{C} веса 4 не имеют общего подмножества мощности 3, иначе в \overline{C} было бы слово $u+v$ веса 2. Так как носители всех слов веса 4 из \overline{C} содержат $4 \cdot 14 = 56$ трехэлементных подмножеств множества X , и всего в X имеется $C_8^3 = 56$ трехэлементных подмножеств, то каждое из них содержится в единственном носителе.

Пусть C' — код, полученный из кода C (см. п. 17.3) обращением порядка следования букв, $\overline{C'}$ — его расширение. Построим теперь бинарный линейный код $G_{24} \subseteq F^{24}$, беря в качестве кодовых слов линейные комбинации векторов $(a, a, 0)$, $(0, b, b)$, (x, x, x) , где $a \in C$, $b \in C$, $x \in C'$. набросок доказательства следующей теоремы имеется в [34].

17.5. Теорема. *Минимальный вес ненулевых слов кода G_{24} равен 8. Множество $\{1, \dots, 24\}$ и носители слов веса 8 кода G_{24} образуют систему Штейнера $S(24, 8, 5)$.*

Отбрасывая последние символы в словах кода G_{24} , можно получить *бинарный код Голея* (открыт в 1949 году). Бинарный код Голея является совершенным $(23, 12)$ -кодом, исправляющим 3 ошибки (см. [34], [24]). Минимальный вес его ненулевых слов равен 7. Множество $\{1, \dots, 23\}$ и носители этих слов образуют систему Штейнера $S(23, 7, 4)$. Отсюда можно вывести, что группа автоморфизмов бинарного кода Голея изоморфна группе Матье M_{23} .

§ 18. Теория расширений

18.1. Определение. Группа G называется *расширением группы H посредством группы F* , если $H \trianglelefteq G$ и $G/H \cong F$.

Задача теории расширений состоит в восстановлении группы G по группам H , F и еще некоторым данным.

Мы будем отождествлять группы G/H и F с помощью фиксированного изоморфизма. В каждом смежном классе $\sigma \in F$ выберем представитель $t(\sigma)$. Далее всегда в единичном классе выбирается единичный представитель, т.е. $t(1) = 1$. Так как элемент $t(\sigma)t(\tau)$ лежит в смежном классе $\sigma\tau$, то существует элемент $f(\sigma, \tau) \in H$ такой, что

$$t(\sigma)t(\tau) = f(\sigma, \tau)t(\sigma\tau). \quad (6)$$

С каждым $\rho \in F$ можно связать автоморфизм $T(\rho) : H \rightarrow H$ такой, что

$$T(\rho)(h) = t(\rho)ht(\rho)^{-1}, \quad h \in H. \quad (7)$$

Очевидно, выполняются условия

$$T(1) = 1 \quad \text{и} \quad f(\sigma, 1) = f(1, \tau) = 1. \quad (8)$$

Из (6) и (7) следует формула

$$T(\sigma)T(\tau) = \widehat{f(\sigma, \tau)}T(\sigma\tau), \quad (9)$$

где $\widehat{f(\sigma, \tau)}$ — автоморфизм группы H , переводящий любой элемент $h \in H$ в элемент $f(\sigma, \tau)hf(\sigma, \tau)^{-1}$.

18.2. Упражнение. *Применив закон ассоциативности к произведению $t(\sigma)t(\tau)t(\rho)$, выведите формулу*

$$f(\sigma, \tau) = T(\sigma)(f(\tau, \rho)) \cdot f(\sigma, \tau\rho) \cdot f(\sigma\tau, \rho)^{-1}. \quad (10)$$

18.3. Определение. Пара функций $f : F \times F \rightarrow H$ и $T : F \rightarrow \text{Aut}(H)$ называется *системой факторов и автоморфизмов* для групп H и F , если выполняются формулы (8), (9) и (10).

18.4. Теорема. Пусть (f, T) — система факторов и автоморфизмов для групп H и F . Тогда существует группа G такая, что $H \trianglelefteq G$, $G/H \cong F$, и существует система представителей $\{t(\sigma)\}_{\sigma \in F}$ смежных классов G по H такая, что система факторов и автоморфизмов, построенная по ней, совпадает с (f, T) .

Доказательство. На множестве $H \times F$ определим умножение по правилу $(x, \sigma) \cdot (y, \tau) = (x \cdot T(\sigma)(y) \cdot f(\sigma, \tau), \sigma\tau)$. Можно проверить, что получилась группа. Обозначим эту группу через G и рассмотрим гомоморфизм $\varphi : G \rightarrow F$, заданный правилом $\varphi(x, \sigma) = \sigma$. Его образ совпадает с F , а ядро — с подгруппой $\{(h, 1) \mid h \in H\}$. Отождествляя эту подгруппу с H , получаем $G/H \cong F$. Мы оставляем читателю проверить, что система факторов и автоморфизмов, построенная по системе представителей $\{(1, \sigma)\}_{\sigma \in F}$, совпадает с (f, T) .

18.5. Определение. Группа G называется *расщепляемым расширением* группы H посредством группы F , если $H \trianglelefteq G$ и в G существует подгруппа $F_1 \cong F$ такая, что $H \cap F_1 = \{1\}$ и $HF_1 = G$. Говорят также, что G — *полупрямое произведение* групп H и F , и пишут $G = H \rtimes F$. Очевидно, $F \cong G/H$.

18.6. Примеры. 1) $S_n = A_n \rtimes Z_2$ при $n \geq 2$.
2) $S_4 = K \rtimes S_3$ (см. 2.4).

18.7. Упражнение. По теореме 14.1 имеем $\text{SL}_2(5)/\{\pm E\} \cong A_5$, где E — единичная матрица. Покажите, что $\text{SL}_2(5)$ не является расщепляемым расширением Z_2 посредством A_5 .

Указание. Если это не так, то $\text{SL}_2(5) \cong Z_2 \times A_5$ и тогда в $\text{SL}_2(5)$ не существовало бы элемента порядка 4, однако он там есть.

18.8. Предложение. Пусть G — расширение группы H посредством группы F , (f, T) — система факторов и автоморфизмов этого расширения, построенная по системе представителей $\{t(\sigma)\}_{\sigma \in F}$. Это расширение расщепляемо тогда и только тогда, когда существует функция $h : F \rightarrow H$ такая, что $h(1) = 1$ и

$$f(\sigma, \tau) = T(\sigma)(h(\tau)^{-1}) \cdot h(\sigma)^{-1} \cdot h(\sigma\tau). \quad (11)$$

Доказательство. Предположим, что данное расширение расщепляемо. Тогда существует система представителей $\{t'(\sigma)\}_{\sigma \in F}$, образующая группу. Так как произведение $t'(\sigma)t'(\tau)$ лежит в смежном классе $\sigma\tau$ и в этой группе, то оно равно $t'(\sigma\tau)$. В частности, $t'(1) = 1$.

Определим функцию h с помощью равенств $t'(\sigma) = h(\sigma)t(\sigma)$, $\sigma \in F$. Тогда

$$h(\sigma\tau)t(\sigma\tau) = h(\sigma)t(\sigma) \cdot h(\tau)t(\tau) = h(\sigma) \cdot T(\sigma)(h(\tau)) \cdot f(\sigma, \tau)t(\sigma\tau),$$

откуда и следует формула (11). Так как $t(1) = t'(1) = 1$, то $h(1) = 1$.

Наоборот, если существует функция $h : F \rightarrow H$ такая, что $h(1) = 1$ и выполняется формула (11), то система представителей $\{h(\sigma)t(\sigma)\}_{\sigma \in F}$ образует группу, и, значит, данное расширение расщепляемо.

§ 19. Теорема Шура

19.1. Лемма (Фраттини). Пусть G — конечная группа, $H \trianglelefteq G$ и P — силовская p -подгруппа группы H . Тогда $G = H \cdot N_G(P)$.

Доказательство. Для произвольного $g \in G$ подгруппа gPg^{-1} лежит в группе H и является в ней силовской p -подгруппой. По теореме Силова $gPg^{-1} = hPh^{-1}$ для некоторого $h \in H$. Отсюда $h^{-1}g \in N_G(P)$ и $g \in H \cdot N_G(P)$.

19.2. Лемма. Пусть H — конечная абелева группа, F — произвольная конечная группа и $\text{нод}(|H|, |F|) = 1$. Тогда любое расширение группы H посредством группы F расщепляемо.

Доказательство. Пусть G — расширение группы H посредством группы F , и пусть (f, T) — некоторая система факторов и автоморфизмов этого расширения. Согласно п. 18.8 достаточно доказать, что существует функция $h : F \rightarrow H$ с условием $h(1) = 1$, для которой выполняется формула (11). Так как H — абелева группа, то мы будем использовать аддитивную форму записи. Определим функцию $\tilde{f} : F \rightarrow H$ правилом

$$\tilde{f}(\sigma) = \sum_{\tau \in F} f(\sigma, \tau).$$

Суммируя равенства (10)

$$f(\sigma, \tau) = T(\sigma)(f(\tau, \rho)) + f(\sigma, \tau\rho) - f(\sigma\tau, \rho)$$

по всем $\rho \in F$, получим

$$|F| \cdot f(\sigma, \tau) = T(\sigma)(\tilde{f}(\tau)) + \tilde{f}(\sigma) - \tilde{f}(\sigma\tau).$$

Умножая это равенство на целое n такое, что $n|F| \equiv 1 \pmod{|H|}$, получаем равенство

$$f(\sigma, \tau) = T(\sigma)(n\tilde{f}(\tau)) + n\tilde{f}(\sigma) - n\tilde{f}(\sigma\tau).$$

Теперь ясно, что в качестве h можно взять функцию $(-n\tilde{f})$.

19.3. Теорема (Шур). Пусть H и F — конечные группы и $\text{нод}(|H|, |F|) = 1$. Тогда любое расширение группы H посредством группы F расщепляемо.

Доказательство. Положим $n = |F|$, $m = |H|$. Пусть G — произвольное расширение группы H посредством группы F . Достаточно доказать, что G содержит подгруппу порядка n . Сделаем это индукцией по m . При $m = 1$ утверждение тривиально. Пусть $m > 1$. Можно считать, что H — собственная подгруппа группы G .

Рассмотрим сначала случай, когда H содержит собственную подгруппу H_1 , нормальную в G . Тогда $(G/H_1)/(H/H_1) \cong F$, и по индукции в G/H_1 содержится подгруппа N/H_1 порядка n . Снова по индукции в N содержится подгруппа порядка n .

Теперь рассмотрим противоположный случай: H — минимальная собственная нормальная подгруппа в G . Пусть P — некоторая силовская p -подгруппа группы H . Тогда

$$F \cong G/H = N_G(P)H/H \cong N_G(P)/N_G(P) \cap H = N_G(P)/N_H(P).$$

Если $|N_H(P)| < |H|$, то по индукции в $N_G(P)$ найдется подгруппа порядка n . Если же $|N_H(P)| = |H|$, то $|N_G(P)| = |F| \cdot |H| = |G|$, то есть $N_G(P) = G$. Тогда подгруппа P , а значит и ее центр $Z(P)$ нормальны в G . Так как центр конечной p -группы всегда неединичен, то $Z(P) = H$ ввиду минимальности H , и, значит, H — абелева группа. По лемме 19.2 расширение G расщепляемо.

§ 20. Группа Хигмэна–Симса

Напомним, что группа Матье M_{22} определялась нами как группа четных автоморфизмов системы Штейнера $M = S(22, 6, 3)$. Множество точек M^0 этой системы состоит из 21 точки, входящей в $\mathbb{P}_2(4)$, и дополнительной точки ∞ ; $|M^0| = 22$. Множество ее блоков M^1 состоит из 21 стандартного блока и $56 = |\text{PSL}_3(4)| / |\text{St}_{\text{PSL}_3(4)}(O)|$ нестандартных блоков (овалов); $|M^1| = 77$.

Построим граф Γ , имеющий $100 = 1 + 22 + 77$ вершин: $\Gamma^0 = \{*\} \cup M^0 \cup M^1$, вершина $*$ соединена с каждой вершиной $m \in M^0$, вершина $m \in M^0$ соединяется с вершиной $B \in M^1$, если и только если m — точка блока B , вершина $B \in M^1$ соединяется с вершиной $B_1 \in M^1$, если и только если блоки B и B_1 не пересекаются. Других соединений нет.

Группа Хигмэна–Симса HS определяется как группа всех автоморфизмов этого графа, осуществляющих четные перестановки его вершин: $HS = \text{Aut}^+(\Gamma)$. Любой автоморфизм системы M индуцирует автоморфизм графа Γ , переводящий вершину $*$ в себя. Поэтому можно

считать, что группа M_{22} и автоморфизмы φ, f^* системы M , определенные в § 16, лежат в $\text{Aut}(\Gamma)$. Более того, $M_{22} \leq \text{Aut}^+(\Gamma)$, т. к. группа M_{22} проста и $|\text{Aut}(\Gamma) : \text{Aut}^+(\Gamma)| \leq 2$.

Мы докажем сейчас теорему о простоте группы HS , опираясь на леммы 20.8 и 20.9, которые будут доказаны позже.

20.1. Теорема. *Группа Хигмэна – Симса HS проста. Ее порядок равен $|M_{22}| \cdot 100$.*

Доказательство. Пусть $\{1\} \neq N \trianglelefteq \text{Aut}^+(\Gamma)$. По лемме 20.9 имеем $\text{St}_{\text{Aut}^+(\Gamma)}(*) = M_{22}$. Так как $M_{22}N = NM_{22}$, то $M_{22}(N*) = NM_{22}* = (N*)$, и, значит, орбита $(N*)$ есть объединение орбит группы M_{22} . Так как длины орбит группы M_{22} равны 1, 22 и 77, а длины N -орбит равны и делят 100 (см. пункты 16.13, 16.14 и 6.8, 20.8), то длина орбиты $(N*)$ равна 1 или 100. Длина каждой N -орбиты не может равняться 1, так как N действует на Γ^0 точно. Поэтому N действует транзитивно и $\text{Aut}^+(\Gamma) = N \text{St}_{\text{Aut}^+(\Gamma)}(*) = NM_{22}$. Так как $N \cap M_{22} \trianglelefteq M_{22}$ и M_{22} проста, то либо $N \cap M_{22} = M_{22}$, либо $N \cap M_{22} = \{1\}$. В первом случае $\text{Aut}^+(\Gamma) = N$, во втором $|N| = 100$. Но в группе порядка 100 имеется единственная силовская подгруппа порядка 25. Ее можно взять в качестве N и получить противоречие. Итак, группа HS проста. Утверждение о ее порядке следует из лемм 20.8 и 20.9.

Прежде, чем доказывать основные леммы 20.8 и 20.9, докажем несколько вспомогательных лемм.

20.2. Лемма. *Число точек пересечения в $\mathbb{P}_2(4)$ произвольной прямой l с произвольным овалом O_i равно 0 или 2.*

Доказательство. Пусть $\bar{x} \in l \cap O_i$. Так как пять прямых, проходящих через точку \bar{x} , содержат все точки $\mathbb{P}_2(4)$ и на каждой из них не более двух точек овала O_i , то каждая из этих прямых содержит кроме \bar{x} еще ровно одну точку из O_i .

Множество всех прямых l таких, что $O_i \cap l = \emptyset$, обозначим через L_i .

20.3. Лемма. *Никакие три прямые из L_i не пересекаются в одной точке.*

Доказательство. Если бы эти прямые пересекались в одной точке, то две другие прямые, проходящие через эту точку, содержали бы овал, что невозможно.

Определим на V (см. начало § 16) скалярное произведение по праву:

$$(a_1x_1 + a_2x_2 + a_3x_3, b_1x_1 + b_2x_2 + b_3x_3) = a_1b_1 + a_2b_2 + a_3b_3.$$

Преобразование множества всех подпространств пространства V , заключающееся в переходе к ортогональному дополнению, индуцирует преобразование α проективной плоскости $\mathbb{P}_2(4)$, переводящее ее точки в прямые, а прямые в точки. Более точно, если \bar{v} — точка, а l — прямая $\mathbb{P}_2(4)$, то

$$\alpha(\bar{v}) = l \iff (\forall \bar{w} \in l \quad (\bar{v}, \bar{w}) = 0) \iff \alpha(l) = \bar{v}.$$

20.4. Упражнение. 1) $\alpha^2(\bar{v}) = \bar{v}$, $\alpha^2(l) = l$.

2) $\bar{v} \in l \iff \alpha(\bar{v}) \ni \alpha(l)$,

3) $\alpha \bar{B} \alpha^{-1} = (\bar{B}^\top)^{-1}$ для любой матрицы $B \in \text{SL}_3(4)$.

Последнее вытекает из формулы $(\bar{v}, \bar{w}) = ((\bar{B}^\top)^{-1} \bar{v}, \bar{B} \bar{w})$.

Расширяя прямую l до стандартного блока $l \cup \{\infty\}$, можно считать, что α определено на множестве точек $\mathbb{P}_2(4)$ и стандартных блоков системы M .

Определим теперь α -образ произвольного овала O_i формулой

$$\alpha(O_i) = \mathbb{P}_2(4) \setminus \bigcup_{\bar{v} \in O_i} \alpha(\bar{v}).$$

Положим еще $\alpha(*) = \infty$ и $\alpha(\infty) = *$. Наша ближайшая цель — доказать, что α — автоморфизм графа Γ .

20.5. Лемма. Для любых овалов O_i, O_j и прямой l справедливы следующие утверждения:

1) $\alpha(O_i)$ — овал,

2) $\alpha^2(O_i) = O_i$,

3) $O_i \cap l = \emptyset \iff \alpha(l) \in \alpha(O_i)$,

4) $O_i \cap O_j = \emptyset \iff \alpha(O_i) \cap \alpha(O_j) = \emptyset$.

Доказательство. Нетрудно вычислить, что

$$\alpha(O) = \{ \overline{ax_1 + x_2 + x_3}, \quad \overline{a^{-1}x_1 + x_2 + x_3}, \quad \overline{x_1 + ax_2 + x_3},$$

$$\overline{x_1 + a^{-1}x_2 + x_3}, \quad \overline{x_1 + x_2 + ax_3}, \quad \overline{x_1 + x_2 + a^{-1}x_3} \} = \bar{A} \cdot O,$$

где

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

Поэтому 1) выполнено: если $O_i = \overline{B} \cdot O$, где $\overline{B} \in \text{PSL}_3(4)$, то

$$\begin{aligned} \alpha(O_i) &= \mathbb{P}_2(4) \setminus \bigcup_{\overline{v} \in O} \alpha(\overline{B} \overline{v}) = \mathbb{P}_2(4) \setminus \bigcup_{\overline{v} \in O} \overline{(B^\top)^{-1}} \cdot \alpha(\overline{v}) = \\ &= \overline{(B^\top)^{-1}} \cdot \alpha(O) = \overline{(B^\top)^{-1} A} \cdot O. \end{aligned}$$

2) Имеем $\alpha^2(O_i) = \overline{B(A^\top)^{-1} A} \cdot O = \overline{B} \cdot O = O_i$, так как $\overline{(A^\top)^{-1} A} \cdot O = O$, что проверяется непосредственно.

3) $O_i \cap l = \emptyset \iff (\forall \overline{v} \in O_i \ \overline{v} \notin l) \iff (\forall \overline{v} \in O_i \ \alpha(l) \notin \alpha(\overline{v})) \iff \alpha(l) \in \alpha(O_i)$.

4) Предположим, что $O_i \cap O_j = \emptyset$, но $\overline{v} \in \alpha(O_i) \cap \alpha(O_j)$. Ввиду 3), $\alpha(\overline{v}) \cap O_i = \emptyset$ и $\alpha(\overline{v}) \cap O_j = \emptyset$. Так как овалы O_i, O_j и прямая $l = \alpha(\overline{v})$ попарно не пересекаются, то вне них в $\mathbb{P}_2(4)$ имеются еще 4 точки, которые мы обозначим y_1, y_2, y_3, y_4 . По упражнению 20.6 существует такая точка $x \in l$, что прямым, соединяющих x с точками y_k , не менее 3.

Обозначим некоторые три такие прямые через l_1, l_2, l_3 . Так как $l \in L_i$, то, ввиду леммы 20.3, максимум только одна из них может лежать в L_i . Аналогично максимум только одна из них может лежать в L_j . Поэтому одна из этих прямых, скажем $l_1 = l(x, y_1)$, не лежит в $L_i \cup L_j$, и, значит, пересекает O_i и O_j . Тогда на l лежат 6 точек: x, y_1 и точки из $l_1 \cap O_i$ и $l_1 \cap O_j$ — противоречие. Обратная импликация следует из 2).

20.6. Упражнение. Для любой прямой l в $\mathbb{P}_2(4)$ и четырех точек y_1, y_2, y_3, y_4 , не лежащих на l , существует такая точка $x \in l$, что прямым, соединяющих x с точками y_k , не менее 3.

20.7. Следствие. α — автоморфизм графа Γ порядка 2.

Теперь в нашем распоряжении имеются три автоморфизма порядка 2: α, φ, f^* , и мы легко докажем лемму 20.8. Эта лемма имеет общематематическое значение: она уничтожает разницу между множеством (вершину $*$ можно отождествить с множеством M^0), его подмножествами (блоками) и элементами (точками).

20.8. Лемма. Группа $\text{Aut}^+(\Gamma)$ действует транзитивно на множестве Γ^0 .

Доказательство. По лемме 16.13 и упражнению 16.14 группа M_{22} имеет три орбиты при действии на Γ^0 : $\{*\}$, M^0 и M^1 . Группа $\text{Aut}^+(\Gamma)$ действует транзитивно на Γ^0 , так как $M_{22} \leq \text{Aut}^+(\Gamma)$ и автоморфизм $(f^* \varphi \alpha)^2$ переводит точку $*$ в овал O , а автоморфизм $(\alpha f^* \varphi)^2$ переводит точку ∞ в овал $\alpha(O)$. Эти автоморфизмы четные, так как квадрат любой подстановки четен.

20.9. Лемма. $\text{St}_{\text{Aut}^+(\Gamma)}(*) = M_{22}$.

Доказательство. Легко понять, что группу $\text{St}_{\text{Aut}(\Gamma)}(*)$ можно отождествить с группой $\text{Aut}(M)$. В группе $\text{Aut}(M)$ имеется подгруппа M_{22} индекса 2. Так как M_{22} проста, то $M_{22} \leq \text{Aut}^+(\Gamma)$. Во втором смежном классе группы $\text{Aut}(M)$ по подгруппе M_{22} есть элемент φ (см. конец п. 16.11). По лемме 20.10, $\varphi \notin \text{Aut}^+(\Gamma)$. Поэтому $\text{St}_{\text{Aut}^+(\Gamma)}(*) = M_{22}$.

20.10. Лемма. Автоморфизм φ осуществляет нечетную перестановку вершин графа Γ .

Доказательство. Пусть Φ — множество φ -инвариантных овалов. Докажем сначала¹⁰, что $|\Phi|$ делится на 4. Так как φ поэлементно перестановочно с группой $\bar{Q} = \{\bar{Q}_{bc} \mid b, c \in \mathbb{F}_4\}$ (см. § 16), то группа \bar{Q} действует на множестве Φ . Достаточно доказать, что длина каждой \bar{Q} -орбиты в Φ делится на 4. Так как $|\bar{Q}| = 16$, то достаточно доказать, что стабилизатор любого овала в группе \bar{Q} имеет порядок 1, 2 или 4. Согласно лемме 16.8 стабилизатор овала в группе $\text{PSL}_3(4)$ изоморфен группе A_6 , в которой 2-силовские подгруппы изоморфны группе $\langle (12)(34), (1234)(56) \rangle$ порядка 8. Так как в \bar{Q} нет элементов порядка 4, то стабилизатор овала в группе \bar{Q} не может иметь порядок 8 (и тем более 16).

Пусть $|\Phi| = 4n$. Учитывая, что φ оставляет на месте ровно 5 стандартных блоков (они проходят через \bar{x}_1 , так как $\varphi(\infty) = \bar{x}_1$), 8 точек из M^0 и вершину $*$, получаем, что общее число неподвижных относительно φ вершин графа Γ равно $(14 + 4n)$. Так как $\varphi^2 = id$, то на остальных его $(86 - 4n)$ вершинах φ действует как произведение $(43 - 2n)$ транспозиций. Поэтому φ — нечетный автоморфизм графа Γ .

¹⁰В [3] доказано, что $|\Phi| = 16$.

Таблица 1. Спорадические группы

Группа	Порядок	Первые исследователи
M_{11}	$2^4 \cdot 3^2 \cdot 5 \cdot 11$	Mathieu
M_{12}	$2^6 \cdot 3^3 \cdot 5 \cdot 11$	Mathieu
M_{22}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11$	Mathieu
M_{23}	$2^7 \cdot 3^2 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
M_{24}	$2^{10} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \cdot 23$	Mathieu
J_2	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	Hall, Janko
Suz	$2^{13} \cdot 3^7 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Suzuki
HS	$2^9 \cdot 3^2 \cdot 5^3 \cdot 7 \cdot 11$	Higman, Sims
McL	$2^7 \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11$	McLaughlin
Co_3	$2^{10} \cdot 3^7 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_2	$2^{18} \cdot 3^6 \cdot 5^3 \cdot 7 \cdot 11 \cdot 23$	Conway
Co_1	$2^{21} \cdot 3^9 \cdot 5^4 \cdot 7^2 \cdot 11 \cdot 13 \cdot 23$	Conway, Leech
He	$2^{10} \cdot 3^3 \cdot 5^2 \cdot 7^3 \cdot 17$	Held/Higman, McKay
Fi_{22}	$2^{17} \cdot 3^9 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	Fischer
Fi_{23}	$2^{18} \cdot 3^{13} \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \cdot 23$	Fischer
Fi'_{24}	$2^{21} \cdot 3^{16} \cdot 5^2 \cdot 7^3 \cdot 11 \cdot 13 \cdot 17 \cdot 23 \cdot 29$	Fischer
HN	$2^{14} \cdot 3^6 \cdot 5^6 \cdot 7 \cdot 11 \cdot 19$	Harada, Norton/Smith
Th	$2^{15} \cdot 3^{10} \cdot 5^3 \cdot 7^2 \cdot 13 \cdot 19 \cdot 31$	Thompson/Smith
B	$2^{41} \cdot 3^{13} \cdot 5^6 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot 31 \cdot 47$	Fischer/Sims, Leon
M	$2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$	Fischer, Griess
J_1	$2^3 \cdot 3 \cdot 5 \cdot 7 \cdot 11 \cdot 19$	Janko
$O'N$	$2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31$	O'Nan/Sims
J_3	$2^7 \cdot 3^5 \cdot 5 \cdot 17 \cdot 19$	Janko/Higman, McKay
Ly	$2^8 \cdot 3^7 \cdot 5^6 \cdot 7 \cdot 11 \cdot 31 \cdot 37 \cdot 67$	Lyons/Sims
Ru	$2^{14} \cdot 3^3 \cdot 5^3 \cdot 7 \cdot 13 \cdot 29$	Rudvalis/Conway, Wales
J_4	$2^{21} \cdot 3^3 \cdot 5 \cdot 7 \cdot 11^3 \cdot 23 \cdot 29 \cdot 31 \cdot 37 \cdot 43$	Janko/Norton, Parker, Benson, Conway, Thackray

ГЛАВА 2

Введение в комбинаторную теорию групп

§ 1. Графы и графы Кэли групп

Для понимания строения группы полезно изучить ее действие на подходящем геометрическом объекте. Эта идея будет развиваться в следующих параграфах. В данном параграфе мы напомним некоторые определения из главы 1 и введем новые понятия, связанные с графами и действиями групп на них. Далее разность множеств X и Y обозначается $X - Y$.

1.1. Определение. Говорят, что группа G действует на множестве M слева, если для любых элементов $g \in G$ и $m \in M$ определен элемент $gm \in M$, причем $g_2(g_1m) = (g_2g_1)m$ и $1m = m$ для всех $m \in M$, $g_1, g_2 \in G$.

Действие транзитивно, если для любых двух элементов m, m' из M найдется элемент g из G с условием $gm = m'$. Действие точно, если для любого неединичного элемента g из G существует элемент m из M такой, что $gm \neq m$. Ядром действия называется подгруппа

$$\{g \in G \mid gm = m \text{ для всех } m \in M\}.$$

Очевидно, действие точно, если его ядро единично. Орбитой элемента m из M называется множество $\mathcal{O}(m) = \{gm \mid g \in G\}$. Два элемента m, m' из M называются G -эквивалентными, если они лежат в одной орбите. Стабилизатором элемента m из M называется подгруппа $\text{St}_G(m) = \{g \in G \mid gm = m\}$.

Иногда мы будем использовать и правые действия.

1.2. Определение. Говорят, что группа G действует на множестве M справа, если для любых элементов $g \in G$ и $m \in M$ определен элемент $mg \in M$, причем $(mg_1)g_2 = m(g_1g_2)$ и $m1 = m$ для всех $m \in M$, $g_1, g_2 \in G$.

1.3. Замечание. *Имея левое действие группы G на множестве M , можно построить правое (и наоборот), положив $tg = g^{-1}m$.*

1.4. Определение. *Граф X состоит из непустого множества вершин X^0 , множества ребер X^1 и трех отображений $\alpha : X^1 \rightarrow X^0$, $\omega : X^1 \rightarrow X^0$ и $\bar{\cdot} : X^1 \rightarrow X^0$ (взятие начала ребра, конца ребра и взятие обратного ребра), удовлетворяющих условию: для любого $e \in X^1$ имеем $\overline{\bar{e}} = e$, $\bar{e} \neq e$ и $\alpha(e) = \omega(\bar{e})$.*

Граф X называется *конечным*, если множества его вершин и ребер конечны. Естественным образом определяется понятие *подграфа* графа. *Прямым произведением* графов X и Y (обозначается $X \times Y$) называется граф с множеством вершин $X^0 \times Y^0$, множеством ребер $X^1 \times Y^1$ и условием $\alpha((e, e')) = (\alpha(e), \alpha(e'))$, $\omega((e, e')) = (\omega(e), \omega(e'))$, $\overline{(e, e')} = (\bar{e}, \bar{e}')$ при $(e, e') \in X^1 \times Y^1$.

Морфизмом из графа X в граф Y называется отображение p из множества вершин и ребер графа X в множество вершин и ребер графа Y , которое переводит вершины в вершины, ребра в ребра и удовлетворяет условиям $p(\alpha(e)) = \alpha(p(e))$, $p(\omega(e)) = \omega(p(e))$, $p(\bar{e}) = \overline{p(e)}$. Сокращенно пишут $p : X \rightarrow Y$. Биактивный морфизм называется *изоморфизмом*. Изоморфизм графа на себя называется *автоморфизмом*. Если в графе X выделяется вершина x , то пишут (X, x) . Запись $p : (X, x) \rightarrow (Y, y)$ означает, что $p : X \rightarrow Y$ — морфизм и $p(x) = y$.

Звездой вершины x графа X называется множество ребер графа X с началом в x . *Валентность* вершины x — это мощность ее звезды. Морфизм p из графа X в граф Y называется *локально инъективным*, если ограничение p на звезду любой вершины графа X инъективно.

Граф X называется *ориентированным*, если в каждой паре $\{e, \bar{e}\}$ его взаимно обратных ребер выбрано одно из них и названо *положительно ориентированным*, а другое названо *отрицательно ориентированным*. Множество всех положительно (отрицательно) ориентированных ребер обозначается через X_+^1 (через X_-^1). Множество X_+^1 называется *ориентацией* графа X .

Графы изображаются в виде объектов, состоящих из точек и линий, соответствующих парам взаимно обратных ребер. Для выделения положительно ориентированных ребер на линиях ставят стрелки.

Введем два вида графов: C_n ($n \in \mathbb{Z}$, $n \geq 1$) и C_∞ . Вершинами графа C_n являются числа $0, 1, \dots, n-1$, ребрами — символы e_i, \bar{e}_i ($0 \leq i \leq n-1$), причем $\alpha(e_i) = i$, $\omega(e_i) = i+1$ (сложение по модулю n). Вершинами графа C_∞ являются все целые числа, ребрами — символы e_i, \bar{e}_i ($i \in \mathbb{Z}$), причем $\alpha(e_i) = i$, $\omega(e_i) = i+1$ (рис. 3).

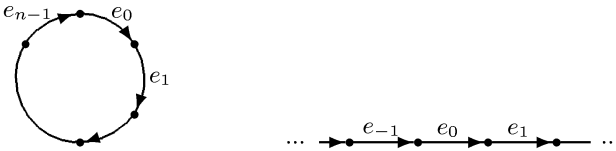


Рис. 3

Последовательность $l = e_1 e_2 \dots e_n$ ребер графа X называется *путем* длины n в графе X , если $\omega(e_i) = \alpha(e_{i+1})$, $i = 1, \dots, n - 1$. Говорят, что l — путь из вершины $\alpha(e_1)$ в вершину $\omega(e_n)$, и что $\alpha(e_1)$ и $\omega(e_n)$ — его начало и конец. Любую вершину графа X считаем тоже путем (*вырожденным*) длины 0 с началом и концом в этой вершине. Для пути $l = e_1 e_2 \dots e_n$ обозначим через l^{-1} путь $\bar{e}_n \dots \bar{e}_2 \bar{e}_1$. Для вырожденного пути l положим $l^{-1} = l$. Говорят, что l — *путь без возвращений*, если он либо вырожден, либо $l = e_1 e_2 \dots e_n$ и $e_{i+1} \neq \bar{e}_i$, $i = 1, \dots, n - 1$. Путь l *замкнут*, если его начало и конец совпадают.

Если конец пути $l = e_1 \dots e_k$ совпадает с началом пути $l' = e'_1 \dots e'_n$ то *произведение* этих путей определяется как путь $ll' = e_1 \dots e_k e'_1 \dots e'_n$.

Граф X *связен*, если для любых двух его вершин u и v существует путь из u в v . *Циклом* в графе называется любой подграф, изоморфный графу \mathcal{C}_n . *Деревом* — это связный граф без циклов. Очевидно, для любых двух вершин u и v произвольного дерева T существует единственный путь без возвращений из u в v .

1.5. Упражнение. Пусть $p : X \rightarrow T$ — локально инъективный морфизм из связного графа X в дерево T . Тогда p инъективен и X — дерево.

1.6. Предложение. Пусть T — максимальное по включению поддерево связного графа X . Тогда T содержит все вершины X .

Доказательство. Если это не так, то в силу связности графа X существует ребро y с началом в T и концом вне T . Присоединяя к T ребра y , \bar{y} и вершину $\omega(y)$, получим большее поддерево, что противоречит максимальности T .

Следующее упражнение сложное, но его легко можно решить, прочитав § 3 и § 4.

1.7. Упражнение. Мощность множества ребер связного графа X , не входящих в его максимальное поддерево T , не зависит от выбора T . Если X — конечный связный граф с ориентацией X^1_+ , то

число положительно ориентированных ребер графа X , не входящих в T , равно $|X_+^1| - |X^0| + 1$.

1.8. Определение. Говорят, что группа G действует слева на графе X , если определены левые действия группы G на множествах X^0 и X^1 так, что $g\alpha(e) = \alpha(ge)$ и $g\bar{e} = \overline{ge}$ для всех $g \in G$ и $e \in X^1$.

Это действие без инверсий ребер, если $ge \neq \bar{e}$ для всяких $e \in X^1$ и $g \in G$.

Действие называется свободным, если $gv \neq v$ для всяких $v \in X^0$ и неединичных $g \in G$.

В теории Басса–Серра, излагаемой далее, требуется, чтобы группа действовала без инверсий ребер на некотором графе. Покажем, что это не является серьезным ограничением: если группа G действует на графе X , то G действует без инверсий ребер на его барицентрическом разбиении $B(X)$ и это действие хорошо связано с исходным.

Определим неформально барицентрическое разбиение графа X как граф $B(X)$, получающийся из X «разбиением» каждого ребра e на два ребра e_n и e_k и добавлением вершины v_e , соответствующей «сердине» ребра e . При этом мы считаем, что $(\bar{e})_k = \bar{e}_n$, $(\bar{e})_n = \bar{e}_k$, $v_e = v_{\bar{e}}$ (рис. 4).

Определим действие группы G на графе $B(X)$, полагая $ge_n = (ge)_n$, $ge_k = (ge)_k$, $gv_e = v_{ge}$ и сохраняя действие G на вершинах графа $B(X)$, являющихся вершинами графа X .

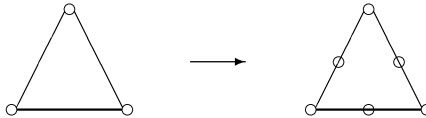


Рис. 4

1.9. Упражнение. Действие группы G на графе $B(X)$ — без инверсий ребер.

Пусть группа G действует на графе X без инверсий ребер. Для $x \in X^0 \cup X^1$ обозначим через $\mathcal{O}(x)$ орбиту x относительно действия группы G : $\mathcal{O}(x) = \{gx \mid g \in G\}$. Определим фактор-граф $G \backslash X$ как граф с вершинами $\mathcal{O}(v)$, где $v \in X^0$, и ребрами $\mathcal{O}(e)$, где $e \in X^1$, причем считаем, что

- 1) $\mathcal{O}(v)$ — начало $\mathcal{O}(e)$, если существует $g \in G$ такое, что gv — начало e ,
- 2) обратным к ребру $\mathcal{O}(e)$ является ребро $\mathcal{O}(\bar{e})$.

Ребра $\mathcal{O}(e)$ и $\mathcal{O}(\bar{e})$ не совпадают, так как G действует без инверсий ребер на X . Отображение $p : X \rightarrow G \backslash X$, заданное правилом $p(x) = \mathcal{O}(x)$, $x \in X^0 \cup X^1$, является морфизмом графов. Назовем этот морфизм *проекцией*.

1.10. Пример. На рис. 5 справа изображен фактор-граф графа, изображенного слева, по действию группы Z_3 его вращений на углы, кратные 120° .

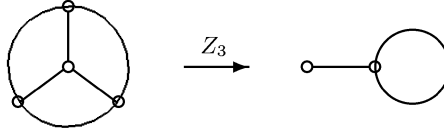


Рис. 5

1.11. Упражнение. Для любого ребра e' фактор-графа $G \backslash X$ и произвольной вершины v графа X , проецирующейся в начало e' , существует ребро e графа X с началом в v , проецирующееся на e' .

1.12. Предложение. Пусть X — связный граф, на котором без инверсий ребер действует группа G . Для любого поддерева T' фактор-графа $G \backslash X$ существует поддерево T в X такое, что $p|_T : T \rightarrow T'$ — изоморфизм.

Доказательство. Множество поддеревьев в X , проецирующихся инъективно в T' , индуктивно по включению (это означает, что объединение любой возрастающей цепи таких поддеревьев лежит в этом множестве). Пусть T — некоторый его максимальный элемент¹. Достаточно доказать, что $p(T) = T'$. Если это не так, то существует ребро e' с началом в $p(T)$ и концом в разности $T' - p(T)$. Воспользовавшись упражнением 1.11, можно увеличить T и прийти к противоречию.

Поддерево T из предложения 1.12 называется *поднятием* в X поддерева T' .

1.13. Определение. Пусть G — группа, S — подмножество G . Обозначим через $\Gamma(G, S)$ ориентированный граф с множеством вершин G , множеством положительно ориентированных ребер $G \times S$ и функциями α и ω , заданными правилами $\alpha((g, s)) = g$ и $\omega((g, s)) = gs$, где $(g, s) \in G \times S$. Обратным к ребру (g, s) считаем ребро (gs, s^{-1}) , вторую компоненту которого в таком окружении воспринимаем как формальный знак, а не как элемент группы G . Тогда $(gs, s^{-1}) \notin G \times S$ даже

¹Он существует по лемме Цорна.

в случае, когда элемент s^{-1} лежит в S . *Меткой* ребра (g, t) называется элемент t .

Группа G действует левым умножением на $\Gamma(G, S)$. Более точно, если $g \in G$, то вершина g' переходит под действием g в вершину gg' , ребро (g', t) — в ребро (gg', t) . Очевидно, что это действие без инверсий ребер и свободно.

1.14. Упражнение. Граф $\Gamma(G, S)$ *связен* $\iff \langle S \rangle = G$.

1.15. Определение. Если $\langle S \rangle = G$, то граф $\Gamma(G, S)$, построенный выше, называется *графом Кэли* группы G относительно порождающего множества S .

1.16. Примеры. Графы C_n и C_∞ изоморфны графам Кэли циклических групп Z_n и Z относительно порождающих множеств, состоящих из одного элемента.

На рис. 6 изображен граф Кэли группы $Z_6 = \langle x \rangle$ относительно порождающего множества $\{x^2, x^3\}$ и граф Кэли группы S_3 относительно порождающего множества $\{(12), (123)\}$.

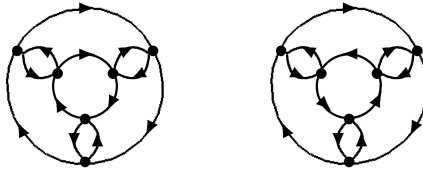


Рис. 6

Пусть $n \geq 1$ — произвольное целое число или $n = \infty$. *Диэдральная группа* D_n — это группа автоморфизмов графа C_n . Любой такой автоморфизм полностью определяется образом ребра e_0 . Пусть a и b такие автоморфизмы, что $a(e_0) = \overline{e_{-1}}$, $b(e_0) = e_1$ (при конечном n индексы берутся по модулю n). Тогда группа D_n состоит из автоморфизмов b^k и $b^k a$, где $0 \leq k \leq n - 1$ при n конечном и $k \in \mathbb{Z}$ при $n = \infty$. Автоморфизмы b^k можно мыслить как вращения (при n конечном) или переносы (при $n = \infty$), автоморфизмы $b^k a$ — как отражения.

1.17. Упражнение. Докажите, что $D_3 \cong S_3$. Как выглядит граф Кэли группы D_n относительно порождающего множества $\{a, b\}$ при конечном n ?

На рис. 7 изображены графы Кэли группы D_∞ относительно порождающих множеств $\{a, b\}$ и $\{a, c\}$, где $c = ab$, а также граф Кэли группы $Z \times Z$ относительно произвольного порождающего ее множества $\{x, y\}$.

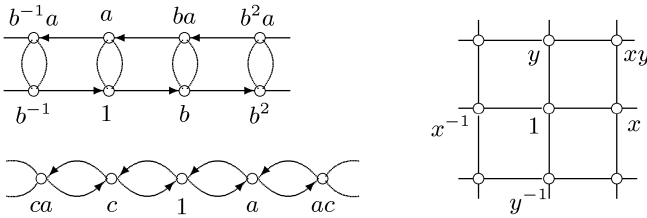


Рис. 7

1.18. Упражнение. *Группа автоморфизмов графа Кэли группы G , сохраняющих метки его ребер, изоморфна группе G .*

1.19. Упражнение. *Проверьте, что граф, изображенный на обложке книги, является графом Кэли знакопеременной группы A_5 .*

§ 2. Автоморфизмы деревьев

Во многих важных случаях группы действуют на деревьях. Поэтому необходимо изучить автоморфизмы деревьев.

Пусть X — дерево. *Геодезическая* в X — это любой путь без возвращений в X . Очевидно, для любых двух непересекающихся поддеревьев X_1 и X_2 дерева X существует единственная геодезическая, начало которой лежит в X_1 , конец в X_2 , а ее ребра не лежат ни в X_1 , ни в X_2 . Геодезическую с началом в вершине u и концом в вершине v обозначим через $u - v$, а ее длину через $l(u, v)$.

Пусть τ — автоморфизм дерева X . Для любой вершины (ребра) v дерева X обозначим через v^τ образ v относительно τ . Заметим, что $l(u, v) = l(u^\tau, v^\tau)$. Положим

$$|\tau| = \min_{v \in X^0} l(v, v^\tau).$$

Минимальное поддерево дерева X , содержащее все вершины u такие, что $l(u, u^\tau) = |\tau|$, обозначим через $\overset{\circ}{\tau}$ при $|\tau| = 0$ и через $\overset{\tau}{\tau}$ при $|\tau| > 0$. Следующая теорема иллюстрируется рис. 9.

2.1. Теорема. *Пусть τ — автоморфизм дерева X . Справедливы следующие утверждения.*

1) *Если $|\tau| = 0$, то любая вершина u и любое ребро дерева $\overset{\circ}{\tau}$ неподвижны относительно τ . Пусть P — произвольная вершина из X*

и Q — вершина из $\overset{\circ}{\tau}$, ближайшая к P . Тогда $P-Q$ и $Q-P^\tau$ — геодезические равной длины, произведение которых является геодезической, соединяющей P и P^τ .

2) Если $|\tau| > 0$ и τ действует без инверсий ребер, то дерево $\vec{\tau}$ изоморфно дереву \mathcal{C}_∞ . Автоморфизм τ действует на $\vec{\tau}$ переносом на длину $|\tau|$. Пусть P — произвольная вершина дерева X , Q — вершина из $\vec{\tau}$, ближайшая к P . Тогда геодезическая $P-P^\tau$ пересекает дерево $\vec{\tau}$ по геодезической $Q-Q^\tau$ и $l(P, P^\tau) = |\tau| + 2l(P, Q)$.

Доказательство. Мы докажем лишь утверждение 2, оставив доказательство утверждения 1 читателю. Пусть A — произвольная вершина такая, что $l(A, A^\tau) = |\tau|$. Тогда последнее ребро геодезической $A-A^\tau$ не является обратным к первому ребру геодезической $A^\tau-A^{\tau^2}$. В противном случае (см. рис. 8) при $|\tau| = 1$ была бы инверсия ребра, а при $|\tau| > 1$ для вершины B геодезической $A-A^\tau$ с $l(A, B) = 1$ было бы $l(B, B^\tau) = l(A, A^\tau) - 2 < |\tau|$, что противоречит определению $|\tau|$.

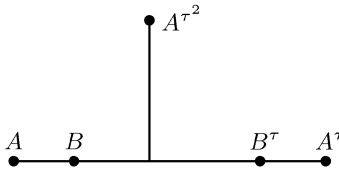


Рис. 8

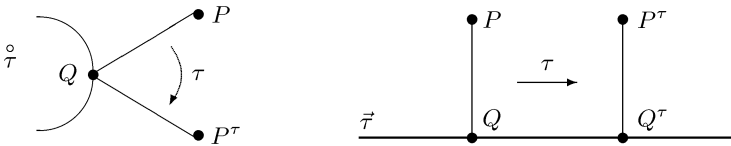


Рис. 9

Теперь ясно, что бесконечный путь $T = \dots - A^{\tau^{-1}} - A - A^\tau - \dots$, составленный из геодезических $A^{\tau^n} - A^{\tau^{n+1}}$ ($n \in \mathbb{Z}$), изоморфен дереву \mathcal{C}_∞ и τ действует на нем переносом на длину $|\tau|$. Если P — произвольная вершина вне T и Q — вершина из T , ближайшая к P (см. рис. 9 справа), то $l(P, P^\tau) = l(P, Q) + l(Q, Q^\tau) + l(Q^\tau, P^\tau) = |\tau| + 2l(P, Q) > |\tau|$. Отсюда $\vec{\tau} = T$ и утверждение 2 доказано.

Ввиду этой теоремы оправдана следующая терминология.

2.2. Определение. Автоморфизм τ дерева X , действующий без инверсий ребер, называется *поворотом*, если $|\tau| = 0$ и *переносом*, если $|\tau| > 0$. При $|\tau| > 0$ поддерево $\bar{\tau}$ называется *магистралью* для τ .

2.3. Упражнение. Пусть ν и τ — автоморфизмы дерева X , $n \in \mathbb{Z}$. Тогда

- 1) $|\nu^{-1}\tau\nu| = |\tau|$,
- 2) $|\tau^n| = |n||\tau|$, если τ действует без инверсий ребер.

2.4. Упражнение. Пусть T_1, \dots, T_n — конечный набор поддеревьев дерева X и $T_i \cap T_j \neq \emptyset$ для всех i и j . Тогда $\bigcap_{i=1}^n T_i \neq \emptyset$.

2.5. Предложение. Пусть τ_1, \dots, τ_n — конечный набор автоморфизмов дерева X . Если τ_i и $\tau_j\tau_i$ — повороты для всех i и j , то $\bigcap_{i=1}^n \overset{\circ}{\tau}_i \neq \emptyset$.

Доказательство. Докажем, что любые два поддерева $\overset{\circ}{\tau}_i$ и $\overset{\circ}{\tau}_j$ имеют непустое пересечение. Тогда утверждение будет следовать из упражнения 2.4. Напомним, что согласно определению композиции отображений $P^{\tau_j\tau_i} = \tau_j(\tau_i(P))$.

Предположим, найдутся два непересекающихся поддерева $\overset{\circ}{\tau}_i$ и $\overset{\circ}{\tau}_j$. Пусть $P - Q$ — геодезическая, соединяющая их. Так как $P^{\tau_j\tau_i} = P^{\tau_j}$, то геодезические $P - P^{\tau_j\tau_i}$ и $P - P^{\tau_j}$ совпадают. По теореме 2.1 середина Q этой геодезической лежит в $\overset{\circ}{\tau}_j\tau_i$ и $\overset{\circ}{\tau}_j$. Отсюда $Q = Q^{\tau_j} = Q^{\tau_j\tau_i}$, следовательно $Q = Q^{\tau_i}$ и $Q \in \overset{\circ}{\tau}_i \cap \overset{\circ}{\tau}_j$ — противоречие.

2.6. Следствие. Для любой конечной группы автоморфизмов дерева, действующей без инверсий ребер, существует вершина, неподвижная относительно всех элементов этой группы.

§ 3. Свободные группы

Ключевую роль в комбинаторной теории групп играют свободные группы. Достаточно сказать, что произвольная группа является фактор-группой подходящей свободной группы (теорема 3.14). В этом параграфе будет доказано существование свободных групп с произвольным базисом. В дальнейшем будет доказано, что свободные группы и только они действуют свободно и без инверсий ребер на деревьях.

Для произвольного подмножества X группы обозначим через X^{-1} ее подмножество $\{x^{-1} \mid x \in X\}$.

3.1. Определение. Пусть F — группа, X — ее линейно упорядоченное подмножество такое, что $X \cap X^{-1} = \emptyset$. Группа F называ-

ется *свободной группой с базисом* X , если любой ее неединичный элемент f представляется единственным способом в виде произведения $f = x_1 x_2 \cdots x_n$, где $x_i \in X \cup X^{-1}$ и $x_i x_{i+1} \neq 1$ для всех i . Такая запись называется *приведенной относительно* X . При этом мы договариваемся, что единичному элементу соответствует пустая приведенная запись.

Из этого определения, в частности, следует, что X порождает F . Очевидно, бесконечная циклическая группа Z свободна. Она имеет базис, состоящий из одного элемента.

3.2. Теорема. *Для всякого множества X существует свободная группа с базисом X .*

Доказательство. Пусть X — произвольное множество. Положим $X^{-1} = \{x^{-1} \mid x \in X\}$, где x^{-1} обозначает новый символ, соответствующий элементу x . Можно считать, что $X \cap X^{-1} = \emptyset$. Считаем также, что запись $(x^{-1})^{-1}$ обозначает элемент x . Множество $X^\pm = X \cup X^{-1}$ назовем *алфавитом*, а его элементы — *буквами*. Слово — это конечная последовательность букв, записанных одна за другой: $x_1 x_2 \dots x_n$, $n \geq 0$, $x_i \in X^\pm$. При $n = 0$ имеем *пустое слово*. Подсловом слова называется любая подпоследовательность его подряд идущих букв.

Пусть W — множество всех слов в алфавите X^\pm . Обозначим *длину слова* f (т. е. число букв, из которого оно состоит) через $|f|$. Для слов f и g из W определим их произведение как слово fg , получающееся приписыванием слова g справа к слову f . Очевидно, W — не группа при $X \neq \emptyset$.

Далее мы введем отношение эквивалентности на W и определим произведение классов эквивалентности так, что получится группа с нужным свойством. Скажем, что слово u эквивалентно слову v , если существует конечная последовательность слов $u = f_1, f_2, \dots, f_k = v$ такая, что каждое f_{i+1} получается из f_i вставкой или вычеркиванием подслова вида xx^{-1} , где $x \in X^\pm$. Назовем такую последовательность связывающей для слов u и v . Пусть $[F]$ обозначает множество классов эквивалентности слов из W . Класс, содержащий слово f , обозначим через $[f]$. Слово g называется *приведенным*, если оно не содержит подслов вида xx^{-1} , где $x \in X^\pm$.

3.3. Предложение. *Каждый класс $[f]$ содержит единственное приведенное слово.*

Доказательство. Существование приведенного слова в классе $[f]$ очевидно. Единственность докажем с помощью метода, который называется «редукция пиков». Предположим, что существуют два различных приведенных слова u и v в классе $[f]$. Из всех последовательностей,

связывающих u и v , выберем последовательность $u = f_1, f_2, \dots, f_k = v$, для которой сумма $\sum_{i=1}^{i=k} |f_i|$ минимальна. Так как слова u и v приведены и различны, то $|f_1| < |f_2|$ и $|f_{k-1}| > |f_k|$. Поэтому существует такое i , что $1 < i < k$ и $|f_{i-1}| < |f_i|$ и $|f_i| > |f_{i+1}|$. Предположим, что f_i получается из f_{i-1} вставкой подслова xx^{-1} , а f_{i+1} получается из f_i вычеркиванием подслова yy^{-1} . Если подслова xx^{-1} и yy^{-1} не пересекаются, то можно сначала в f_{i-1} вычеркнуть подслово yy^{-1} , а затем вставить подслово xx^{-1} . В результате тройка f_{i-1}, f_i, f_{i+1} заменится на тройку f_{i-1}, f'_i, f_{i+1} с меньшей суммой длин слов — противоречие. Если же подслова xx^{-1} и yy^{-1} пересекаются, то $f_{i-1} = f_{i+1}$ и мы можем убрать два члена последовательности. Снова получили противоречие с минимальностью.

Зададим на множестве $[F]$ всех классов умножение, полагая $[f][g] = [fg]$. Докажем, что $[F]$ — свободная группа с базисом $[X] = \{[x] \mid x \in X\}$. Ассоциативность умножения очевидна, единичным элементом является класс $[\emptyset]$. Обратным к классу $[f] = [x_1 \cdots x_n]$, где $x_i \in X \cup X^{-1}$, является класс $[x_n^{-1} \cdots x_1^{-1}]$. Далее, $[f] = [x_1] \cdots [x_n]$ и эта запись приведена относительно $[X]$ тогда и только тогда, когда слово $x_1 \dots x_n$ приведено. Так как в каждом классе имеется ровно одно приведенное слово, то единственность приведенной записи элементов $[F]$ относительно $[X]$ доказана. Осталось заметить, что мощность $[X]$ равна мощности X .

3.4. Упражнение. Произвольная свободная группа с базисом X изоморфна построенной выше свободной группе $[F]$ с базисом $[X]$.

Далее свободную группу с базисом X будем обозначать через $F(X)$. На практике удобно обращаться с элементами группы $F(X)$ как со словами в алфавите $X \cup X^{-1}$, считая два слова равными, если соответствующие им приведенные слова совпадают.

Дадим другое, категорное, определение свободной группы.

3.5. Определение. Пусть F — группа и X — подмножество в F . Тогда F — свободная группа с базисом X , если для любой группы G любое отображение $\varphi : X \rightarrow G$ имеет единственное продолжение $\varphi^* : F \rightarrow G$, являющееся гомоморфизмом.

3.6. Теорема. Определения 3.1 и 3.5 свободной группы эквивалентны.

Доказательство. Пусть F — свободная группа с базисом X в смысле определения 3.1, и пусть φ — отображение из X в некоторую

группу G . Продолжим φ до гомоморфизма из группы F в группу G по следующему правилу. Для $x \in X$ положим $\varphi^*(x^{-1}) = (\varphi(x))^{-1}$. Пусть теперь f — произвольный элемент из F . Возьмем его произвольную запись $f = x_1 \cdots x_n$, где $x_1, \dots, x_n \in X^\pm$, и положим $\varphi^*(f) = \varphi^*(x_1) \cdots \varphi^*(x_n)$. Это определение корректно, так как от одной записи элемента f к другой можно перейти конечным числом вставок и вычеркиваний подслов вида xx^{-1} , где $x \in X^\pm$. Очевидно, отображение $\varphi^* : F \rightarrow G$ является гомоморфизмом, причем единственным, продолжающим φ .

Пусть теперь F — свободная группа с базисом X в смысле определения 3.5. Тогда тождественное вложение $X \rightarrow \langle X \rangle$ можно продолжить до гомоморфизма $F \rightarrow \langle X \rangle$, и, значит, до гомоморфизма $F \rightarrow F$ с образом $\langle X \rangle$. Так как имеется еще тождественный гомоморфизм $F \rightarrow F$, то, в силу единственности продолжения, имеем $F = \langle X \rangle$.

Единственность приведенной записи элементов группы F относительно X следует из рассмотрения гомоморфизма $F \rightarrow [F]$, продолжающего отображение $x \mapsto [x]$, $x \in X$.

3.7. Упражнение. *Свободная группа с базисом $\{a, b\}$ имеет также базис $\{ab, bab\}$.*

3.8. Теорема. *Любые два базиса свободной группы F равносильны.*

Доказательство. Пусть X — некоторый базис свободной группы F . Пусть $Z_2 = \{0, 1\}$ — группа вычетов по модулю 2 и H — группа относительно сложения, состоящая из всех функций $f : X \rightarrow Z_2$, принимающих значение 1 только для конечного числа элементов $x \in X$. Складываются такие функции покомпонентно: $(f + g)(x) = f(x) + g(x)$, $x \in X$.

Сопоставим каждому $x \in X$ функцию f_x , принимающую значение 1 на x и 0 на остальных элементах из X . Возникающее отображение продолжается до эпиморфизма $\varphi : F \rightarrow H$. Подгруппа $\text{Ker } \varphi$ состоит из всех слов, в которых для каждого $x \in X$ общее число вхождений x и x^{-1} четно. Докажем, что $\text{Ker } \varphi = \langle f^2 \mid f \in F \rangle$. Включение правой части в левую очевидно. Обратное включение следует индукцией по длине слова из $\text{Ker } \varphi$ ввиду формул $xixv = (xi)^2 \cdot u^{-1}v$ и $x^{-1}uxv = x^{-2}(xu)^2 \cdot u^{-1}v$. Итак, $H \cong F / \langle f^2 \mid f \in F \rangle$, откуда следует, что мощность H не зависит от выбора X . С другой стороны, из определения H следует, что $|H| = 2^{|X|}$, если X конечно и $|H| = |X|$, если X бесконечно. Поэтому мощность базиса — инвариант группы F .

3.9. Определение. *Ранг свободной группы — это мощность любого ее базиса.*

Обозначим ранг свободной группы F через $\text{rk}(F)$.

3.10. Следствие. *Две свободные группы изоморфны тогда и только тогда, когда их ранги равны.*

3.11. Следствие. *Если $\psi : F(Y) \rightarrow F(X)$ — эпиморфизм, то $|Y| \geq |X|$.*

Доказательство. Пусть $\varphi : F(X) \rightarrow H$ — эпиморфизм из доказательства теоремы 3.8. Группу H можно рассматривать как векторное пространство над полем из двух элементов. Базисом этого векторного пространства является множество $\{f_x \mid x \in X\}$. Так как множество $\varphi(\psi(Y))$ порождает H , то $|Y| \geq |X|$.

3.12. Упражнение. *В свободной группе ранга $n \geq 2$ существуют свободные подгруппы всех конечных рангов.*

Указание. В группе $F(a, b)$ подмножество $\{a, b^{-1}ab, \dots, b^{-r}ab^r\}$ порождает свободную подгруппу ранга $r + 1$.

3.13. Упражнение. *Пусть $\varphi : G \rightarrow F(X)$ — эпиморфизм из группы G на свободную группу $F(X)$. Для каждого элемента $x \in X$ выберем элемент x' в полном прообразе $\varphi^{-1}(x)$. Положим $X' = \{x' \mid x \in X\}$. Докажите, что $\langle X' \rangle$ — свободная группа, изоморфная группе $F(X)$.*

Следующая теорема позволяет изучать произвольные группы с помощью свободных групп и их подгрупп. Мы разовьем этот подход в § 5.

3.14. Теорема. *Произвольная группа G является фактор-группой подходящей свободной группы.*

Доказательство. Пусть Y — произвольное множество, порождающее группу G . По теореме 3.6 существует гомоморфизм из свободной группы $F(Y)$ в группу G , продолжающий тождественное отображение $Y \rightarrow Y$. Очевидно, этот гомоморфизм является эпиморфизмом.

3.15. Определение. *Ранг произвольной группы G — это минимум из мощностей базисов свободных групп F таких, что G — гомоморфный образ F , или, что то же самое, минимум из мощностей порождающих группу G множеств².*

Докажем, что этот минимум достигается на некотором порождающем множестве. Если хотя бы одно порождающее множество конечно, то это очевидно. Если же все порождающие множества бесконечны, то их мощности совпадают с мощностью группы G и минимум равен $|G|$. Действительно, пусть X — некоторое бесконечное порождающее группу G множество. Тогда каждый элемент из G есть произведение конечного числа элементов из $X \cup X^{-1}$. Поскольку мощность множества всех

²Ввиду следствия 3.11, это определение обобщает определение 3.9.

конечных подмножеств бесконечного множества равна его мощности, имеем $|G| = |X|$.

Ранг группы G обозначим через $rk(G)$.

§ 4. Фундаментальная группа графа

Пусть X — связный граф с выделенной вершиной x . Рассмотрим множество $P(X, x)$ всех путей в X с началом и концом в x . Для любых двух путей $p = e_1 \dots e_k$ и $q = e'_1 \dots e'_n$ из $P(X, x)$ определено их произведение $pq = e_1 \dots e_k e'_1 \dots e'_n$, лежащее снова в $P(X, x)$. Вырожденный путь x можно рассматривать как единичный элемент и считать, что он имеет пустую запись. Однако, так мы не получим группу при $X^1 \neq \emptyset$ ввиду отсутствия обратных путей к невырожденным. Ситуацию можно исправить, если рассматривать пути $e_1 \dots e_i e \bar{e}_{i+1} \dots e_m$ и $e_1 \dots e_i e_{i+1} \dots e_m$ как одинаковые.

Более точно, скажем, что пути p_1 и p_2 из $P(X, x)$ *гомотопны*, если от p_1 к p_2 можно перейти с помощью конечного числа вставок и вычеркиваний подпутей вида $e\bar{e}$. Множество $P(X, x)$ разбивается на классы гомотопных путей. Обозначим через $[p]$ гомотопический класс пути p и для любых двух классов $[p]$ и $[q]$ положим $[p] \cdot [q] = [pq]$.

4.1. Упражнение. Докажите, что

- 1) произведение гомотопических классов определено корректно, то есть не зависит от выбора представителей в классах,
- 2) в каждом классе имеется ровно один путь без возвратений.

Теперь легко проверить, что множество гомотопических классов путей из $P(X, x)$ относительно такого произведения образует группу. Эта группа называется *фундаментальной группой графа X относительно вершины x* и обозначается $\pi_1(X, x)$.

4.2. Замечание.

1) Аналогично можно определить гомотопический класс $[p]$ произвольного (не обязательно замкнутого) пути p в X , произведение путей p и q в X при условии, что конец p совпадает с началом q , и произведение их гомотопических классов. Множество гомотопических классов всех путей в X относительно такого частичного произведения называется *фундаментальным группоидом графа X* .

2) Если x_1 — другая вершина графа X , то $\pi_1(X, x_1) \cong \pi_1(X, x)$. Изоморфизм задается правилом $[p] \mapsto [qpq^{-1}]$, где q — фиксированный путь из x в x_1 .

Докажем, что фундаментальная группа связного графа свободна. Выберем максимальное поддерево T в X . Для каждой вершины $v \in X^0$

существует единственный путь без возвращений из x в v , проходящий в T . Обозначим этот путь через p_v . Тогда для любого ребра $e \in X^1$ определен путь $p_e = p_{\alpha(e)} e p_{\omega(e)}^{-1}$. Заметим, что $[p_e] = [p_{\bar{e}}]^{-1}$.

4.3. Теорема. Пусть X — связный граф, $x \in X^0$, T — его максимальное поддереве. Ориентируем X произвольным образом. Тогда $\pi_1(X, x)$ — свободная группа с базисом $S = \{[p_e] \mid e \in X_+^1 - T^1\}$.

Доказательство. Если $p = e_1 e_2 \dots e_k$ — замкнутый путь в X с началом в x , то $[p] = [p_{e_1}][p_{e_2}] \dots [p_{e_k}]$. Так как $[p_e] = 1$ для $e \in T^1$, то группа $\pi_1(X, x)$ порождается множеством S . Докажем единственность приведенной записи элементов группы $\pi_1(X, x)$ относительно S .

Пусть $[p] = [p_{e_1}][p_{e_2}] \dots [p_{e_k}]$ — приведенная запись элемента $[p]$ относительно множества S . Это означает, что $e_i \in X^1 - T^1$ и $e_{i+1} \neq \bar{e}_i$ для всех i . Поэтому сокращения подпутей в пути $p_{e_1} p_{e_2} \dots p_{e_k}$ могут происходить только на стыках путей p_{e_i} , $p_{e_{i+1}}$ и не затрагивают ребер e_i . Следовательно, путь p гомотопен пути без возвращений вида $t_1 e_1 t_2 e_2 \dots e_k t_{k+1}$, где все пути t_i проходят в дереве T . Так как в каждом гомотопическом классе существует только один путь без возвращений, то приведенная запись единственна.

Если $f : X \rightarrow Y$ — морфизм графов и $p = e_1 \dots e_n$ — путь в X , то определен путь $f(p) = f(e_1) \dots f(e_n)$ в Y .

4.4. Упражнение. Пусть X и Y — связные графы, $f : (X, x) \rightarrow (Y, y)$ — морфизм. Тогда отображение $f_* : \pi_1(X, x) \rightarrow \pi_1(Y, y)$, заданное правилом $f_*([p]) = [f(p)]$, является гомоморфизмом.

В § 20 мы определим накрытия графов — специальные морфизмы f , для которых гомоморфизм f_* является вложением.

§ 5. Задание группы порождающими и определяющими соотношениями

В этом параграфе мы обсудим способ задания групп порождающими и определяющими соотношениями. Он позволяет не только компактно задавать группы, но и изучать многие их свойства, а также строить группы с заранее заданными свойствами. Такие задания групп возникают естественно во многих областях теории групп и топологии.

5.1. Определение. Пусть F — группа и R — ее подмножество. Нормальным замыканием множества R в группе F называется наименьшая нормальная подгруппа группы F , содержащая R .

Обозначим это нормальное замыкание через R^F . Очевидно, при непустом R имеем

$$R^F = \left\{ \prod_{i=1}^k f_i^{-1} r_i^{\varepsilon_i} f_i \mid f_i \in F, r_i \in R, \varepsilon_i = \pm 1, k \geq 0 \right\}.$$

Следующее простое замечание облегчает запись многих доказательств.

5.2. Замечание. Если $r \in R^F$, то

$$urv \in R^F \iff uv \in R^F.$$

5.3. Пусть группа G порождается системой $A = \{a_i\}_{i \in I}$ и пусть F — свободная группа с базисом $X = \{x_i\}_{i \in I}$. Отображение $X \rightarrow A$, $x_i \mapsto a_i$ ($i \in I$) продолжается до эпиморфизма $\varphi : F \rightarrow G$. Тогда $G \cong F/N$, где $N = \text{Ker } \varphi$. Если R — такое подмножество F , что $N = R^F$, то запись $\langle X \mid R \rangle$ определяет группу G с точностью до изоморфизма и называется ее *представлением*. Такая запись удобна, так как часто, даже в случаях, когда N не конечно порождена³, удается отыскать конечное множество R со свойством $N = R^F$. Представление $\langle X \mid R \rangle$ называется *конечным*, если множества X и R конечны. Существуют конечно порожденные группы, не имеющие конечного представления [57, 25].

5.4. Пример. Группа S_3 имеет представление $\langle x, y \mid x^2, y^2, (xy)^3 \rangle$.

Действительно, зададим гомоморфизм $\varphi : F(x, y) \rightarrow S_3$ правилом $\varphi(x) = (12)$, $\varphi(y) = (23)$. Тогда φ является эпиморфизмом и в его ядре лежат элементы $x^2, y^2, (xy)^3$. Докажем, что $\text{Ker } \varphi$ совпадает с нормальным замыканием множества этих элементов, используя замечание 5.2. Пусть $x^{k_1} y^{l_1} \dots x^{k_s} y^{l_s} x^{k_{s+1}} \in \text{Ker } \varphi$, где все показатели не равны нулю, кроме, может быть, первого и последнего. Вычеркивая подслово вида $x^{\pm 2}$ и $y^{\pm 2}$, можно считать, что все ненулевые показатели равны 1. Далее, вычеркивая подслово вида $xuxuxu$ и $yxuxux$, можно прийти к словам длины не более 5 с показателями при буквах x и y равными 1. Из них только пустое слово (оно равно 1) лежит в $\text{Ker } \varphi$. Утверждение доказано.

³По теореме 22.5, если $F(X)$ — свободная группа конечного ранга, то любая ее неединичная нормальная подгруппа N , имеющая бесконечный индекс в $F(X)$, не является конечно порожденной.

В § 7 мы выведем представление группы S_n для любого n с помощью индукции по n и теорем 5.7 и 5.8.

Иногда вместо слов r из R в записи представления пишут равенства $r = 1$ или даже $u = v$, если r имеет вид uv^{-1} . Часто систему порождающих A группы G отождествляют с множеством X ее представления⁴. Тогда множество $\{r = 1 \mid r \in R\}$ называют *множеством определяющих соотношений группы G* , а задание группы G представлением $\langle X \mid R \rangle$ называют *заданием порождающими и определяющими соотношениями*. При этом пишут $G = \langle X \mid R \rangle$ и слова в алфавите X^\pm отождествляют с элементами группы G .

Если u, v — два слова в алфавите X^\pm , задающие одинаковые элементы группы G , то говорят, что $u = v$ — *соотношение* в группе G . Произвольное соотношение $u = v$ в группе G является *следствием* определяющих (*выводится* из них) в том смысле, что слово uv^{-1} в $F(X)$ является произведением некоторых слов, сопряженных к словам из R^\pm . Доказать или опровергнуть, что два данных слова в алфавите X^\pm задают одинаковые элементы группы G иногда весьма непросто. В общем случае эта проблема, называемая *проблемой равенства слов*, алгоритмически неразрешима даже в классе конечно представленных групп [17, 31]. Однако, если группа конечно представлена и финитно аппроксимируема, то проблема равенства слов в ней разрешима (см. § 29).

5.5. Упражнение. Пусть n — целое число, по модулю большее 1. Группа G , порожденная в $\text{GL}_2(\mathbb{Q})$ матрицами

$$A = \begin{pmatrix} 1 & 0 \\ 0 & n \end{pmatrix}, \quad B = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},$$

имеет представление $\langle a, b \mid a^{-1}ba = b^n \rangle$.

Решение. Значением слова $a^{k_1}b^{l_1} \dots a^{k_s}b^{l_s}$ на матрицах A, B назовем его образ в G при отображении $a \mapsto A, b \mapsto B$. Говоря о соотношениях в G , будем использовать алфавит $\{A, B\}^\pm$.

Прежде всего заметим, что соотношение $A^{-1}BA = B^n$ справедливо. Теперь докажем, что любое соотношение между матрицами A и B выводится из этого соотношения. Пусть $w = a^{k_1}b^{l_1} \dots a^{k_s}b^{l_s}$ — произвольное слово такое, что его значение на матрицах A и B равно единичной матрице E . Перепишем это слово в виде $(a^{p_1}b^{l_1}a^{-p_1})(a^{p_2}b^{l_2}a^{-p_2}) \dots (a^{p_s}b^{l_s}a^{-p_s})a^{p_s}$, где $p_i = k_1 + k_2 + \dots + k_i$. Воспользовавшись тем, что при $k > l$ соотношение $a^{-k}ba^k = (a^{-l}ba^l)^{n^{(k-l)}}$ является следствием соотношения $a^{-1}ba = b^n$, можно привести слово w к виду $w_1 = a^{-l}b^l a^l \cdot a^{p_s}$. При этом значение слова w_1 на матрицах A и B по-прежнему равно E .

⁴Если элементы в A повторяются, то один и тот же порождающий может одновременно обозначаться различными буквами из X .

Простые матричные вычисления показывают, что $t = p_s = 0$, то есть $w_1 = 1$.

5.6. Упражнение. 1) Конечная диэдральная группа D_n имеет представление $\langle a, b \mid a^2 = 1, b^n = 1, a^{-1}ba = b^{-1} \rangle$.

2) Бесконечная диэдральная группа D_∞ имеет представление $\langle a, b \mid a^2 = 1, a^{-1}ba = b^{-1} \rangle$.

Пусть $\varphi : X \rightarrow G'$ — отображение из множества X в группу G' . Для произвольного слова $r = x_1 \dots x_n$ в алфавите X^\pm положим $\varphi(r) = \varphi(x_1) \cdots \varphi(x_n)$, считая, что $\varphi(x^{-1}) = (\varphi(x))^{-1}$ при $x \in X$.

5.7. Теорема. Пусть группа G задана порождающими и определяющими соотношениями $\langle X \mid R \rangle$, и пусть G' — другая группа. Если отображение $\varphi : X \rightarrow G'$ таково, что $\varphi(r) = 1$ для всех $r \in R$, то φ продолжается до гомоморфизма $G \rightarrow G'$.

Доказательство. Произвольный элемент $g \in G$ записывается (возможно неоднозначно) в виде $g = x_1 \cdots x_k$, где все x_i из X^\pm . Поэтому искомое продолжение естественно задать правилом $g \mapsto \varphi(x_1) \cdots \varphi(x_k)$. Для проверки корректности этого определения достаточно заметить, что если $x_1 \cdots x_k = 1$ в G , то $\varphi(x_1) \cdots \varphi(x_k) = 1$ в G' . Это вытекает из того, что все слова из $R^{F(X)}$ отображаются под действием φ в 1.

Придадим другую форму этой теореме.

5.8. Теорема. Пусть группы G и G' заданы порождающими и определяющими соотношениями $\langle X \mid R \rangle$ и $\langle X' \mid R' \rangle$. Если отображение $\varphi : X \rightarrow X'$ таково, что все слова $\varphi(r)$ ($r \in R$) лежат в нормальном замыкании множества R' в $F(X')$, то φ продолжается до гомоморфизма $G \rightarrow G'$.

§ 6. Преобразования Титце

В этом параграфе мы докажем, что если группа G имеет два конечных представления, то от одного к другому можно перейти с помощью конечной последовательности преобразований Титце.

Согласно пункту 5.3 будем говорить, что представление $\langle X \mid R \rangle$ группы G происходит из эпиморфизма $\varphi : F(X) \rightarrow G$, если $\text{Ker } \varphi = R^{F(X)}$. Эпиморфизм φ и множество R не определяют друг друга однозначно. Например, представление $\langle x \mid x^3 \rangle$ группы $Z_3 = \{0, 1, 2\}$ вычетов по модулю 3 происходит из двух эпиморфизмов φ_1 и φ_2 из $F(x)$ в Z_3 , заданных правилами $\varphi_1(x) = 1$ и $\varphi_2(x) = 2$ соответственно.

6.1. Упражнение. *Покажите, что представление $\langle x, y \mid x^{-5}y^2, x^6y^{-3} \rangle$ тоже задает группу Z_3 .*

Пусть $\langle X \mid R \rangle$ — некоторое представление группы G . Предположим, что оно происходит из эпиморфизма φ . Определим преобразования Титце вида I, II, I' и II'.

I. Пусть r — произвольный элемент из $R^{F(X)}$. Тогда $\langle X \mid R \cup \{r\} \rangle$ тоже является представлением группы G и происходит из φ . Переход от первого представления ко второму запишем в виде

$$\langle X \mid R \rangle \xrightarrow{I} \langle X \mid R \cup \{r\} \rangle.$$

II. Пусть $y \notin X^\pm$ — новая буква, w — произвольный элемент из $F(X)$. Тогда имеется переход

$$\langle X \mid R \rangle \xrightarrow{II} \langle X \cup \{y\} \mid R \cup \{y^{-1}w\} \rangle.$$

Последнее представление тоже является представлением группы G . Докажем, что оно происходит из эпиморфизма $\varphi': F(X \cup \{y\}) \rightarrow G$, заданного правилами $\varphi'(x) = \varphi(x)$ для $x \in X$ и $\varphi'(y) = \varphi(w)$. Обозначим через N нормальное замыкание множества $R \cup \{y^{-1}w\}$ в группе $F(X \cup \{y\})$. Ясно, что $N \subseteq \text{Ker } \varphi'$. Докажем обратное включение. Пусть g — произвольное слово из $\text{Ker } \varphi'$. По замечанию 5.2 имеем $uy^{\pm 1}v \in N \iff uw^{\pm 1}v \in N$. Поэтому можно считать, что g не содержит букв y и y^{-1} . Тогда $g \in \text{Ker } \varphi \subseteq N$.

Преобразования I, II и обратные к ним преобразования I', II' называются *преобразованиями Титце*. Будем писать $\langle X_1 \mid R_1 \rangle \rightarrow \langle X_2 \mid R_2 \rangle$, если от $\langle X_1 \mid R_1 \rangle$ к $\langle X_2 \mid R_2 \rangle$ можно перейти конечной последовательностью преобразований Титце. Для произвольного множества слов W и пары букв x и y обозначим через $W_{x \rightarrow y}$ множество, полученное из W заменой букв x и x^{-1} на буквы y и y^{-1} в каждом слове $w \in W$.

6.2. Упражнение.

- 1) Если R_1 и R_2 конечны и $R_1^{F(X)} = R_2^{F(X)}$, то $\langle X \mid R_1 \rangle \rightarrow \langle X \mid R_2 \rangle$.
- 2) Пусть R конечно, $x \in X$ и $y \notin X^\pm$ — новая буква. Тогда $\langle X \mid R \rangle \rightarrow \langle X_{x \rightarrow y} \mid R_{x \rightarrow y} \rangle$.

Докажем только второе утверждение, опираясь на первое. Имеем $\langle X \mid R \rangle \xrightarrow{II} \langle X \cup \{y\} \mid R \cup \{y^{-1}x\} \rangle \rightarrow \langle X \cup \{y\} \mid R_{x \rightarrow y} \cup \{x^{-1}y\} \rangle \xrightarrow{II'} \langle X_{x \rightarrow y} \mid R_{x \rightarrow y} \rangle$. Второй переход возможен ввиду утверждения 1. Равенство соответствующих нормальных замыканий следует из того, что любое слово uxv можно переписать в виде $uyv \cdot v^{-1}(y^{-1}x)v$.

6.3. Теорема (Титце). *Два конечных представления $\langle X | R_1 \rangle$ и $\langle Y | R_2 \rangle$ задают одну и ту же группу G тогда и только тогда, когда от одного к другому можно перейти конечным числом преобразований Титце.*

Доказательство. Пусть представления $\langle X | R_1 \rangle$ и $\langle Y | R_2 \rangle$ задают группу G и происходят из эпиморфизмов φ_1 и φ_2 . В силу упражнения 6.2 можно считать, что $X \cap Y = \emptyset$. Для каждого $y \in Y$ выберем $w_y \in F(X)$ такое, что $\varphi_1(w_y) = \varphi_2(y)$. Для каждого $x \in X$ выберем $w_x \in F(Y)$ такое, что $\varphi_1(x) = \varphi_2(w_x)$. Имеем

$$\begin{aligned} \langle X | R_1 \rangle &\xrightarrow{II} \dots \xrightarrow{II} \langle X \cup Y | R_1 \cup \{y^{-1}w_y \mid y \in Y\} \rangle \xrightarrow{I} \dots \xrightarrow{I} \\ &\xrightarrow{I} \langle X \cup Y | R_1 \cup R_2 \cup \{y^{-1}w_y \mid y \in Y\} \cup \{x^{-1}w_x \mid x \in X\} \rangle. \end{aligned}$$

Среднее представление в этой цепочке происходит из эпиморфизма $\varphi_1 \cup \varphi_2$. Переход к последнему представлению возможен ввиду включений $R_2 \subseteq \text{Ker } \varphi_2 \subseteq \text{Ker } (\varphi_1 \cup \varphi_2)$ и $x^{-1}w_x \in \text{Ker } (\varphi_1 \cup \varphi_2)$. Вследствие симметрии, представление $\langle Y | R_2 \rangle$ приводится к тому же виду. Поэтому $\langle X | R_1 \rangle \rightarrow \langle Y | R_2 \rangle$. Обратное утверждение теоремы очевидно.

Отметим, что не существует алгоритма, позволяющего узнавать, задают ли два разных представления одну и ту же группу [1, 58]. Тем самым поиск (или доказательство отсутствия) соответствующей цепочки преобразований Титце становится своего рода искусством. Чтобы овладеть этим искусством, необходимо научиться выводить нужные следствия из данного множества соотношений. В следующих примерах мы будем возводить соотношения в степень, перемножать различные соотношения и подставлять одни соотношения в другие. Последнее означает, что если имеются соотношения $w = uv$ и $p = q$, то можно подставить q вместо p и получить соотношение $w = uqv$.

6.4. Примеры.

1) Фундаментальная группа⁵ узла «трилистник» (рис. 10) имеет представление $\langle x, y \mid xux = yxy \rangle$. Покажем, что эта группа представима в виде нетривиального свободного произведения с объединением⁶.

$$\begin{aligned} \langle x, y \mid xux = yxy \rangle &\rightarrow \langle x, y, a, b \mid xux = yxy, a = xy, b = yx \rangle \rightarrow \\ &\rightarrow \langle x, y, a, b \mid xux = yxy, a^3 = b^2, a = xy, b = yx, x = a^{-1}b, y = b^{-1}a^2 \rangle \rightarrow \\ &\rightarrow \langle x, y, a, b \mid a^3 = b^2, x = a^{-1}b, y = b^{-1}a^2 \rangle \rightarrow \langle a, b \mid a^3 = b^2 \rangle. \end{aligned}$$

⁵Определение фундаментальной группы (узла) можно посмотреть, например, в книгах [42, 56].

⁶Эта конструкция возникнет в § 11.

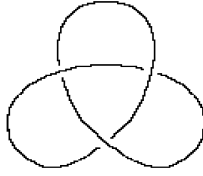


Рис. 10

2) Покажем, что представление

$$\langle a, b \mid ab^2a^{-1} = b^3, ba^2b^{-1} = a^3 \rangle$$

задает единичную группу.

Введем новые порождающие и соотношения:

$$b_1 = aba^{-1}, b_2 = ab_1a^{-1}, b_3 = ab_2a^{-1}.$$

Выводим следствия:

$$bb_2^{-1} = a, b_3 = bb_2^{-1} \cdot b_2 \cdot b_2b^{-1} = bb_2b^{-1},$$

$$b^3 = b_1^2, b_1^3 = b_2^2, b_2^3 = b_3^2,$$

$$b_3^8 = b_2^{12} = b_1^{18} = b^{27},$$

$$b_2^8 = b_1^{12} = b^{18}.$$

Так как $b_3 = bb_2b^{-1}$, то отсюда следует, что $b^{27} = b^{18}$. Далее, $1 = b^9 = b_1^6 = b_2^4$. Так как $b_2 = a^2ba^{-2}$, то $b^4 = 1$. Из $b^9 = 1 = b^4$ следует $b = 1$. Тогда и $a = 1$.

6.5. Упражнение. Выведите из упражнения 5.6, что

1) конечная диэдральная группа D_n имеет представление $\langle a, c \mid a^2 = 1, c^2 = 1, (ac)^n = 1 \rangle$,

2) бесконечная диэдральная группа D_∞ имеет представление $\langle a, c \mid a^2 = 1, c^2 = 1 \rangle$.

§ 7. Представление группы S_n

7.1. Теорема. Группа S_n имеет представление

$$\langle t_1, \dots, t_{n-1} \mid t_i^2 = 1, t_i t_{i+1} t_i = t_{i+1} t_i t_{i+1}, t_i t_j = t_j t_i \ (|i - j| > 1) \rangle.$$

Доказательство проведем индукцией по n . При $n = 1, 2$ теорема очевидна. Сделаем индукционный переход от $n-1$ к n . Пусть G — группа с данным представлением. По теореме 5.7 отображение $t_i \mapsto (i, i+1)$ задает эпиморфизм $\varphi : G \rightarrow S_n$. Достаточно доказать, что $|G| \leq |S_n|$. Рассмотрим подгруппу $H = \langle t_2, \dots, t_{n-1} \rangle$ группы G . По индукции S_{n-1} имеет представление

$$\langle s_1, \dots, s_{n-2} \mid s_i^2 = 1, s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1}, s_i s_j = s_j s_i \ (|i-j| > 1) \rangle$$

и, следовательно (по теореме 5.8), существует гомоморфизм $S_{n-1} \rightarrow H$, заданный правилом $s_i \mapsto t_{i+1}$, $1 \leq i \leq n-2$.

Поэтому $|H| \leq |S_{n-1}|$. Мы докажем, что $|G| \leq |S_n|$, если докажем, что $|G : H| \leq n$. Положим $H_0 = H$, $H_i = H t_1 t_2 \dots t_i$ ($1 \leq i \leq n-1$). В силу того, что $t_i^{-1} = t_i$, достаточно доказать, что множество $H_0 \cup H_1 \cup \dots \cup H_{n-1}$ замкнуто относительно умножений справа на t_1, \dots, t_{n-1} . Имеем $H_i t_i = H_{i-1}$, $H_i t_{i+1} = H_{i+1}$. Положим $u_i = t_1 t_2 \dots t_i$. При $j \geq i+2$ выполняются равенства $H_i t_j = H u_i t_j = H t_j u_i = H u_i = H_i$. При $j \leq i-1$ имеем $u_i = u_{j-1} t_j t_{j+1} v$, где v перестановочно с t_j . Следовательно, $H_i t_j = H u_{j-1} t_j t_{j+1} v \cdot t_j = H u_{j-1} (t_j t_{j+1} t_j) v = H u_{j-1} (t_{j+1} t_j t_{j+1}) v = H t_{j+1} u_{j-1} t_j t_{j+1} v = H_i$.

7.2. Упражнение. *Группа A_n имеет представление*

$$\langle s_3, \dots, s_n \mid s_i^3 = 1, (s_i s_j)^2 = 1 \ (3 \leq i \neq j \leq n) \rangle.$$

Это представление происходит из эпиморфизма $F(s_3, \dots, s_n) \rightarrow A_n$, заданного правилом $s_i \mapsto (12i)$, где $3 \leq i \leq n$.

§ 8. Деревья и свободные группы

В этом параграфе мы докажем теорему Нильсена–Шрайера о том, что подгруппа свободной группы свободна. Это позволит нам находить представления подгрупп групп по представлениям самих групп. Метод доказательства использует деревья, что неудивительно, если взглянуть на рис. 11, где изображена часть графа Кэли группы $F(x, y)$ относительно порождающего множества $\{x, y\}$. Развитие этого метода приводит к теории Басса–Серра групп, действующих на деревьях. Она позволяет единообразно рассматривать конструкции свободного произведения с объединением и HNN-расширения, играющие важную роль в теории групп и топологии.

Для понимания дальнейшего следует вспомнить определения из § 1. Условимся, что все действия в этом параграфе левые.

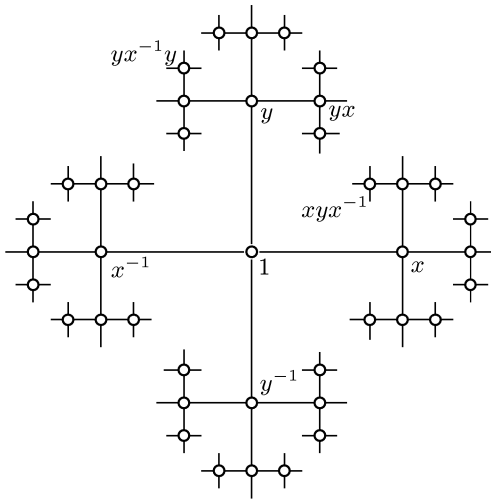


Рис. 11

8.1. Предложение. Пусть $\Gamma(G, S)$ — граф, определенный группой G и подмножеством $S \subseteq G$. Тогда $\Gamma(G, S)$ — дерево $\iff G$ — свободная группа с базисом S .

Доказательство. Для ребра $e = (g, t)$, где $t \in S \cup S^{-1}$, определим его метку $s(e) = t$. Тогда $\omega(e) = \alpha(e)s(e)$ и для любого пути $e_1 \dots e_n$ имеем $\omega(e_n) = \alpha(e_1)s(e_1) \dots s(e_n)$.

Пусть G — свободная группа с базисом S . В силу упражнения 1.14 граф $\Gamma(G, S)$ связан. Предположим, что в $\Gamma(G, S)$ существует замкнутый путь без возвратов $e_1 \dots e_n$. Тогда $\omega(e_n) = \alpha(e_1)$ и, следовательно, $s(e_1) \dots s(e_n) = 1$. Так как S — базис группы G , то существует такое k , что $s(e_k) = (s(e_{k+1}))^{-1}$. Тогда ребра e_k и e_{k+1} противоположны — противоречие. Итак, граф $\Gamma(G, S)$ является деревом. Доказательство обратного утверждения оставляем читателю.

8.2. Следствие. Свободная группа G действует свободно и без инверсий ребер на некотором дереве (а именно, левыми умножениями на своем графе Кэли $\Gamma(G, S)$, где S — базис G).

Справедливо и обратное утверждение.

8.3. Теорема. Пусть G — группа, действующая свободно и без инверсий ребер на дереве X . Тогда G свободна и ее ранг равен мощно-

сти множества положительно ориентированных ребер фактор-графа $G \setminus X$ (при любом выборе ориентации), лежащих вне некоторого (любого выбранного) его максимального поддерева.

В частности, если фактор-граф $G \setminus X$ конечен, то

$$rk(G) = |(G \setminus X)_+^1| - |(G \setminus X)^0| + 1.$$

Доказательство. Пусть $p : X \rightarrow X'$ — каноническая проекция дерева X на фактор-граф $X' = G \setminus X$. Выберем в X' максимальное поддерево T' и поднимем его до некоторого поддерева T в X . Отметим, что разные вершины дерева T не эквивалентны относительно действия G и каждая вершина из X эквивалентна некоторой (единственной) вершине из T . Ориентируем X' произвольным образом и поднимем эту ориентацию в X , то есть считаем, что ребро из X положительно ориентировано тогда и только тогда, когда его образ в X' положительно ориентирован.

Пусть E' — множество положительно ориентированных ребер X' , не входящих в T' . По упражнению 1.11 для каждого ребра $e' \in E'$ существует его поднятие с началом в некоторой вершине из T . Такое поднятие единственно, иначе из этой вершины v выходят два эквивалентных ребра и тогда элемент, переводящий одно ребро в другое, фиксирует v , что противоречит свободе действия G на X . Обозначим это поднятие через e и заметим, что конец e лежит вне T (иначе e лежит в T и тогда e' лежит в T'). Пусть E — множество всех положительно ориентированных ребер в X с началом в T и концом вне T . Легко понять, что p отображает E на E' биективно.

Конец каждого ребра $e \in E$ эквивалентен единственной вершине $v(e) \in T$. Элемент из G , переводящий $v(e)$ в конец ребра e , тоже единствен в силу свободы действия G на X . Обозначим его через g_e .

Докажем, что G — свободная группа с базисом $S = \{g_e \mid e \in E\}$. Поддерева gT ($g \in G$) попарно не пересекаются, множество их вершин совпадает с множеством вершин дерева X . Поэтому любое положительно ориентированное ребро f из X , не входящее в объединение этих поддереваев, соединяет некоторые два из них, скажем g_1T и g_2T . Стянем каждое поддерево gT в одну вершину и обозначим эту вершину через (gT) . Получится дерево X_T , в котором ребро f соединяет вершины (g_1T) и (g_2T) . В силу предложения 8.1 достаточно доказать, что $X_T \cong \Gamma(G, S)$. Изоморфизм задается отображением вершин $(g_1T) \mapsto g_1$, $(g_2T) \mapsto g_2$ и ребер $f \mapsto (g_1, s)$, где $s = g_1^{-1}g_2$. Элемент s лежит в S , т. к. ребро $g_1^{-1}f$ соединяет поддерева T и $g_1^{-1}g_2T$.

Последнее утверждение теоремы следует из упражнения 1.7.

8.4. Следствие (Теорема Нильсена–Шрайера). *Любая подгруппа свободной группы свободна.*

Доказательство. Пусть G — свободная группа с базисом S . По следствию 8.2 группа G действует свободно и без инверсий ребер на дереве $\Gamma(G, S)$. Если $H \leq G$, то H тоже действует свободно и без инверсий ребер на том же дереве. По теореме 8.3 группа H свободна.

8.5. Следствие (Формула Шрайера). *Если G — свободная группа конечного ранга и H — ее подгруппа конечного индекса n , то*

$$\mathbf{rk}(H) - 1 = n(\mathbf{rk}(G) - 1).$$

Доказательство. Пусть S — некоторый базис группы G , $H \setminus G$ — множество правых смежных классов группы G по подгруппе H . Группа H действует на вершинах и положительно ориентированных ребрах дерева $\Gamma(G, S)$ по следующим правилам: $g \xrightarrow{h} hg$, $(g, s) \xrightarrow{h} (hg, s)$. Здесь $h \in H$, $g \in G$, $s \in S$. Поэтому фактор-граф $Y = H \setminus \Gamma(G, S)$ задается формулами $Y^0 = H \setminus G$, $Y_+^1 = (H \setminus G) \times S$, причем ребро (Hg, s) соединяет вершины Hg и Hgs . По теореме 8.3 имеем $\mathbf{rk}(H) = n \cdot \mathbf{rk}(G) - n + 1$.

Изучим более подробно фактор-граф $Y = H \setminus \Gamma(G, S)$. Используя этот граф и понятие фундаментальной группы, мы получим другое доказательство следствия 8.4. Меткой ребра $e = (Hg, t)$, где $t \in S \cup S^{-1}$, назовем элемент $s(e) = t$. Меткой пути $l = e_1 \dots e_k$ назовем произведение $s(l) = s(e_1) \dots s(e_k)$. Меткой вырожденного пути считаем единицу. Если произведение путей l_1 и l_2 определено, то, очевидно, $s(l_1 l_2) = s(l_1) s(l_2)$.

8.6. Замечание. *В звезде каждой вершины графа Y метки различных ребер различны и пробегают множество $S \cup S^{-1}$.*

8.7. Предложение. *Группа H состоит из меток всех путей в графе Y с началом и концом в вершине H .*

Доказательство. Пусть $l = e_1 \dots e_k$ — путь в Y с началом и концом в вершине H . Как и раньше имеем $\omega(e_i) = \alpha(e_i) s(e_i)$ и $\omega(e_k) = \alpha(e_k) s(e_k) = \alpha(e_1) s(e_1) \dots s(e_k) = \alpha(e_1) s(l)$. Так как $\omega(e_k) = \alpha(e_1) = H$, то $s(l) \in H$.

Наоборот, пусть $h = s_1 \dots s_k \in H$, где $s_i \in S^\pm$ для всех i . Положим $e_1 = (H, s_1)$ и $e_i = (H s_1 \dots s_{i-1}, s_i)$ при $2 \leq i \leq k$. Тогда $l = e_1 \dots e_k$ — путь с началом и концом в H такой, что $s(l) = h$.

Наша ближайшая цель — показать, что H порождается метками некоторых «простейших» путей в Y .

Выберем максимальное поддерево Δ в Y и выделим вершину y , равную смежному классу H . Для каждой вершины $v \in Y^0$ существует единственный путь без возвращений из y в v , проходящий в Δ . Обозначим этот путь через p_v . Тогда для любого ребра $e \in Y^1$ определен путь $p_e = p_{\alpha(e)} e p_{\omega(e)}^{-1}$.

8.8. Теорема. *В предыдущих обозначениях H — свободная группа с базисом $\{s(p_e) \mid e \in Y_+^1 - \Delta^1\}$.*

Доказательство. Зададим отображение $s : \pi_1(Y, y) \rightarrow G$ правилом $[p] \mapsto s(p)$. Так как метки гомотопных путей равны, то отображение s корректно определено. По предложению 8.7 это отображение является гомоморфизмом на H . Взаимная однозначность s вытекает из того, что неединичный гомотопический класс содержит невырожденный путь без возвращений и метка такого пути неединична (по замечанию 8.6). Теперь утверждение теоремы следует из теоремы 4.3.

8.9. Определение. Пусть G — свободная группа с базисом S и H — ее подгруппа. Система представителей \mathcal{T} правых смежных классов G по H называется *шрайеровой*, если из того, что $t \in \mathcal{T}$ имеет приведенную форму $s_1 s_2 \cdots s_n$ ($s_i \in S \cup S^{-1}$) следует, что $s_1 \cdots s_i \in \mathcal{T}$ для каждого $0 \leq i \leq n$. Такую систему будем называть коротко *шрайеровой трансверсалью для H в G* .

В частности, $1 \in \mathcal{T}$. Для $g \in G$ обозначим через \bar{g} такой элемент из \mathcal{T} , что $Hg = H\bar{g}$.

8.10. Теорема. 1) *Для любой подгруппы H свободной группы G с базисом S существует шрайерова трансверсаль в G . Более точно, пусть Δ — произвольное максимальное поддерево в фактор-графе $Y = H \backslash \Gamma(G, S)$. Тогда множество*

$$\mathcal{T}(\Delta) = \{s(p_v) \mid v \in Y^0\}$$

является шрайеровой трансверсалью для H в G .

2) *Соответствие $\Delta \mapsto \mathcal{T}(\Delta)$ задает биекцию из множества максимальных поддеревьев в Y в множество шрайеровых трансверсалей для H в G .*

3) *Пусть \mathcal{T} — произвольная шрайерова трансверсаль для H в G . Тогда H имеет базис*

$$\{ts(\bar{ts})^{-1} \mid t \in \mathcal{T}, s \in S \text{ и } ts(\bar{ts})^{-1} \neq 1\}.$$

Доказательство. 1) Так как v пробегает множество правых смежных классов группы G по подгруппе H и $v = Hs(p_v)$, то $\mathcal{T}(\Delta)$ — система представителей этих классов. Осталось заметить, что для пути

$p_v = e_1 e_2 \dots e_n$ в дереве Δ его метка $s(p_v) = s(e_1) s(e_2) \dots s(e_n)$ является приведенным словом и любое начальное подслово этого слова является меткой соответствующего начального подпути пути p_v .

2) Пусть \mathcal{T} — произвольная шрайерова трансверсаль для H в G . Пусть $t = s_1 \dots s_k$ — произвольный элемент из \mathcal{T} , записанный в приведенной форме. Сопоставим ему путь $l_t = e_1 \dots e_k$ в Y такой, что $\alpha(e_1) = H$, $s(e_i) = s_i$. Пусть $\Delta(\mathcal{T})$ — подграф в Y , образованный всеми ребрами, входящими в пути l_t ($t \in \mathcal{T}$), обратными к ним ребрами, а также их началами и концами. Легко понять, что $\Delta(\mathcal{T})$ — максимальное поддерево в Y , и что соответствия $\Delta \mapsto \mathcal{T}(\Delta)$ и $\mathcal{T} \mapsto \Delta(\mathcal{T})$ задают взаимно обратные отображения.

3) Третье утверждение следует из теоремы 8.8. В самом деле, пусть Δ — максимальное поддерево в Y , соответствующее системе \mathcal{T} . Для любого пути $p_e = p_{\alpha(e)} e p_{\omega(e)}^{-1}$ имеем $s(p_e) = t s t_1^{-1}$, где $t = s(p_{\alpha(e)})$, $s = s(e)$, $t_1 = s(p_{\omega(e)})$. По первому утверждению $t, t_1 \in \mathcal{T}$, а по предложению 8.7 имеем $t s t_1^{-1} \in H$, т. е. $t_1 = \bar{t} s$. Осталось заметить, что $(e \in Y_+^1 \iff s(e) \in S)$ и $(e \in \Delta^1 \iff s(p_e) = 1)$ и сослаться на теорему 8.8.

8.11. Примеры.

1) Множество $\{a^n b^m \mid n, m \in \mathbb{Z}\}$ является шрайеровой трансверсалью для коммутанта свободной группы $F(a, b)$. Имеем $\overline{a^n b^m \cdot a} = a^{n+1} b^m$, $\overline{a^n b^m \cdot b} = a^n b^{m+1}$. Поэтому этот коммутант имеет базис

$$\{a^n b^m a b^{-m} a^{-(n+1)} \mid n, m \in \mathbb{Z}, m \neq 0\}.$$

2) Пусть H — подгруппа свободной группы $F(a, b)$, состоящая из всех слов с четной суммой показателей при a и при b . Легко понять, что $\{1, a, b, ab\}$ — шрайерова трансверсаль для H в группе $F(a, b)$. Обозначим через Γ граф Кэли группы $F(a, b)$ относительно базиса $\{a, b\}$. Размеченный фактор-граф $H \setminus \Gamma$ изображен на рис. 12 слева (например, вершины Hab и Hb соединены ребром с меткой a , поскольку $Haba = Hb$). Выберем в нем максимальное поддерево Δ , состоящее из жирных ребер и их концов. Тогда H имеет базис

$$a^2, b^2, ab^2 a^{-1}, abab^{-1}, bab^{-1} a^{-1}.$$

Заметим, что H является ядром гомоморфизма $\varphi : F(a, b) \rightarrow Z_2 \times Z_2$, отображающего a в порождающий первого множителя и b — в порождающий второго.

3) Пусть H — ядро гомоморфизма $\varphi : F(a, b) \rightarrow S_3$, заданного правилом $a \mapsto (12)$, $b \mapsto (13)$. Множество $\{1, a, b, ab, ba, aba\}$ является

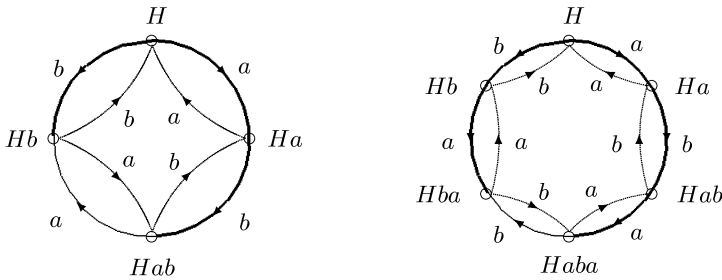


Рис. 12

шрайеровой трансверсалью для H в $F(a, b)$. Группа H имеет базис

$$\{a^2, ab^2a^{-1}, aba^2b^{-1}a^{-1}, ababa^{-1}b^{-1}, b^2, ba^2b^{-1}, baba^{-1}b^{-1}a^{-1}\}.$$

8.12. Замечание. Группа автоморфизмов графа $H \setminus \Gamma$, сохраняющих метки ребер, изоморфна группе $Z_2 \times Z_2$ в первом примере и группе S_3 во втором.

Следующее упражнение обобщает последние два примера.

8.13. Упражнение.

1) Представим диэдральную группу D_n как фактор-группу группы $F(a, c)$ по нормальному замыканию множества $\{a^2, c^2, (ac)^n\}$. Пусть H – ядро канонического гомоморфизма $\varphi : F(a, c) \rightarrow D_n$. Докажите, что при $n = 2k$ в качестве шрайеровой трансверсали для H в группе $F(a, c)$ можно взять множество всех начальных подслов слов $(ac)^k$ и $(ca)^{k-1}c$, при $n = 2k + 1$ – множество всех начальных подслов слов $(ac)^ka$ и $(ca)^k$. Найдите базис группы H .

2) Представим бесконечную диэдральную группу D_∞ как фактор-группу группы $F(a, c)$ по нормальному замыканию множества $\{a^2, c^2\}$. Найдите базис ядра канонического гомоморфизма $F(a, c) \rightarrow D_\infty$.

§9. Переписывающий процесс Райдемайстера – Шпрайера

Пусть F – свободная группа с базисом X , $H \leq F$, T – шрайерова система представителей правых смежных классов F по H . Для $t \in T$ и $x \in X \cup X^{-1}$ положим $\gamma(t, x) = tx(tx)^{-1}$. Неединичные элементы $\gamma(t, x)$, где $t \in T$, $x \in X$, образуют базис свободной группы H .

Обозначим этот базис через Y , и пусть H^* — свободная группа с базисом $Y^* = \{y^* \mid y \in Y\}$. Отображение $y \mapsto y^*$ определяет изоморфизм $\tau : H \rightarrow H^*$.

Для $\omega \in H$ элемент $\tau(\omega)$ можно вычислить, пользуясь следующим замечанием. Пусть $\omega = x_1 \cdots x_n \in H$, $x_i \in X \cup X^{-1}$. Тогда

$$\omega = \gamma(1, x_1) \cdot \gamma(\overline{x_1}, x_2) \cdot \dots \cdot \gamma(\overline{x_1 \cdots x_{i-1}}, x_i) \cdot \dots \cdot \gamma(\overline{x_1 \cdots x_{n-1}}, x_n).$$

Учитывая, что $\gamma(t, x^{-1}) = \gamma(\overline{tx^{-1}}, x)^{-1}$, можно записать ω через базис Y и, значит, $\tau(\omega)$ через базис Y^* . Этот процесс переписывания ω через базис Y называется переписывающим процессом Райдемайстера–Шрайера.

9.1. Теорема. Пусть группа G имеет представление $\langle X \mid R \rangle$ и $\varphi : F(X) \rightarrow G$ — связанный с этим представлением эпиморфизм. Пусть G_1 — подгруппа группы G и H — ее полный прообраз. Тогда в обозначениях выше G_1 имеет представление $\langle Y^* \mid R^* \rangle$, где $R^* = \{\tau(trt^{-1}) \mid t \in T, r \in R\}$.

Доказательство. Пусть N — нормальное замыкание R в $F(X)$. Тогда $G_1 \cong H/N \cong H^*/\tau(N)$. Подгруппа N состоит из всех конечных произведений элементов вида $fr^\varepsilon f^{-1}$, где $f \in F$, $r \in R$, $\varepsilon = \pm 1$. Пусть $f = ht$, где $t \in T$, $h \in H$. Тогда $\tau(fr^\varepsilon f^{-1}) = \tau(htr^\varepsilon t^{-1}h^{-1}) = \tau(h)(\tau(trt^{-1}))^\varepsilon \tau(h^{-1})$, что и доказывает теорему.

9.2. Следствие. Подгруппа конечного индекса в конечно представленной (конечно порожденной) группе конечно представлена (конечно порождена).

9.3. Пример. Пусть φ — гомоморфизм из группы трилистника $G = \langle a, b \mid a^2 = b^3 \rangle$ в группу S_3 , заданный правилом $a \mapsto (12)$, $b \mapsto (123)$. Найдем конечное представление его ядра H .

В качестве шрайеровых представителей правых смежных классов G по H выберем $1, b, b^2, a, ab, ab^2$. Порождающими группы H будут элементы

$$\left. \begin{aligned} 1 \cdot a \cdot (\overline{a})^{-1} &= 1, \\ x &= b \cdot a \cdot (\overline{ba})^{-1} = bab^{-2}a^{-1}, \\ y &= b^2 \cdot a \cdot (\overline{b^2a})^{-1} = b^2ab^{-1}a^{-1}, \\ z &= a \cdot a \cdot (\overline{a^2})^{-1} = a^2, \\ u &= ab \cdot a \cdot (\overline{aba})^{-1} = abab^{-2}, \\ v &= ab^2 \cdot a \cdot (\overline{ab^2a})^{-1} = ab^2ab^{-1}, \end{aligned} \right| \begin{aligned} 1 \cdot b \cdot (\overline{b})^{-1} &= 1, \\ b \cdot b \cdot (\overline{b^2})^{-1} &= 1, \\ w &= b^2 \cdot b \cdot (\overline{b^3})^{-1} = b^3, \\ a \cdot b \cdot (\overline{ab})^{-1} &= 1, \\ ab \cdot b \cdot (\overline{ab^2})^{-1} &= 1, \\ s &= ab^2 \cdot b \cdot (\overline{ab^3})^{-1} = ab^3a^{-1}. \end{aligned}$$

Для нахождения определяющих соотношений нам нужно переписать соотношения вида trt^{-1} , где $t \in \{1, b, b^2, a, ab, ab^2\}$, $r = b^3a^{-2}$ как слова в порождающих x, y, z, u, v, w, s . Имеем

$$r = wz^{-1}, \quad brb^{-1} = wv^{-1}x^{-1}, \quad b^2rb^{-2} = wu^{-1}y^{-1},$$

$$ara^{-1} = sz^{-1}, \quad (ab)r(ab)^{-1} = sy^{-1}u^{-1}, \quad (ab^2)r(ab^2)^{-1} = sx^{-1}v^{-1}.$$

Используя преобразования Титце, можно исключить порождающие w, v, u, s , подставив во все соотношения вместо них слова $z, x^{-1}z, y^{-1}z, z$. В итоге мы получим следующее представление группы $H: \langle x, y, z \mid yz = zy, xz = zx \rangle$. Отсюда следует, что $H \cong F(z) \times F(x, y)$.

9.4. Упражнение. Докажите, что ядро гомоморфизма

$$\varphi : \langle s, t \mid s^3, t^3, (st)^3 \rangle \rightarrow Z_3 = \langle a \mid a^3 \rangle,$$

переводящего s и t в a , изоморфно $Z \times Z$.

Рассматривая граф Кэли (рис. 13), построенный по представлению $\langle s, t \mid s^3, t^3, (st)^3 \rangle$, можно убедиться в этом непосредственно.

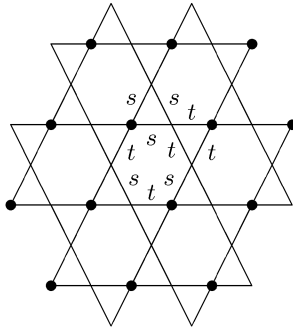


Рис. 13

9.5. Упражнение. Вычислите представление группы A_n , пользуясь представлением группы S_n в теореме 7.1.

§ 10. СВОБОДНОЕ ПРОИЗВЕДЕНИЕ

В этом параграфе мы определим свободное произведение групп A и B . Взяв изоморфные копии этих групп, можно считать, что $A \cap B = \{1\}$. *Нормальной формой* называется выражение вида $g_1g_2 \dots g_n$, где

$n \geq 0$, $g_i \in (A \cup B) - \{1\}$ ($1 \leq i \leq n$) и соседние элементы не принадлежат одновременно A или B . Число n называется *длиной* этой нормальной формы. Нормальная форма нулевой длины отождествляется с единицей. Зададим на множестве всех нормальных форм умножение индукцией по сумме длин перемножаемых форм: для любой нормальной формы x положим $1 \cdot x = x \cdot 1 = x$; для нормальных форм $x = g_1 \dots g_n$ и $y = h_1 \dots h_m$ при $n \geq 1$, $m \geq 1$ положим

$$x \cdot y = \begin{cases} g_1 \dots g_n h_1 \dots h_m, & \text{если } g_n \in A, h_1 \in B \\ & \text{или } g_n \in B, h_1 \in A, \\ g_1 \dots g_{n-1} z h_2 \dots h_m, & \text{если } g_n, h_1 \in A \text{ или } g_n, h_1 \in B \\ & \text{и } z = g_n h_1 \neq 1, \\ g_1 \dots g_{n-1} \cdot h_2 \dots h_m, & \text{если } g_n, h_1 \in A \text{ или } g_n, h_1 \in B \\ & \text{и } g_n h_1 = 1. \end{cases}$$

10.1. Упражнение. Докажите, что множество всех нормальных форм с операцией умножения, заданной выше, является группой.

Эта группа называется *свободным произведением* групп A и B и обозначается $A * B$. Группы A и B естественно вкладываются в группу $A * B$. Это приводит нас к следующему предложению.

10.2. Предложение. Пусть A и B — подгруппы группы G такие, что любой неединичный элемент $g \in G$ представляется единственным способом в виде произведения $g = g_1 g_2 \dots g_n$, где $g_i \in (A \cup B) - \{1\}$ ($1 \leq i \leq n$) и соседние элементы не принадлежат одновременно A или B . Тогда $G \cong A * B$.

10.3. Теорема. Пусть $A = \langle X | R \rangle$, $B = \langle Y | S \rangle$ и $X \cap Y = \emptyset$. Тогда $A * B = \langle X \cup Y | R \cup S \rangle$.

Доказательство. Обозначим через $[R]$, $[S]$ и $[R \cup S]$ нормальные замыкания множеств R , S и $R \cup S$ в группах $F(X)$, $F(Y)$ и $F(X \cup Y)$. Пусть $\varphi : F(X) \rightarrow A$ и $\psi : F(Y) \rightarrow B$ — гомоморфизмы с ядрами $[R]$ и $[S]$ соответственно. Пусть $\theta : F(X \cup Y) \rightarrow A * B$ — гомоморфизм, совпадающий с φ на X и с ψ на Y . Достаточно доказать, что $\text{Ker } \theta = [R \cup S]$. Включение правой части в левую очевидно. Докажем обратное включение. Пусть $g = g_1 g_2 \dots g_n \in \text{Ker } \theta$, $g_i \in (F(X) \cup F(Y)) - \{1\}$ и соседние множители не лежат одновременно в $F(X)$ или в $F(Y)$. Так как $\theta(g_1) \theta(g_2) \dots \theta(g_n) = 1$ в $A * B$, то существует такое i , что $\theta(g_i) = 1$ и, значит, $g_i \in [R]$ или $g_i \in [S]$. Кроме того, $\theta(g_1 \dots g_{i-1} g_{i+1} \dots g_n) = 1$, откуда индукцией по n заключаем, что $g_1 \dots g_{i-1} g_{i+1} \dots g_n \in [R \cup S]$. Следовательно, $g \in [R \cup S]$.

10.4. Пример. $D_\infty \cong Z_2 * Z_2$.

Хотя это следует из упражнения 6.5, мы приведем другое доказательство. Положим $c = ba$, где a и b — автоморфизмы графа \mathcal{C}_∞ , определенные в п. 1.16. Тогда a и c можно мыслить как отражения графа \mathcal{C}_∞ относительно начала и середины ребра e_0 . В частности, a и c имеют порядок 2. При $n \geq 0$ автоморфизмы $(ca)^n$, $(ca)^n c$, $a(ca)^n c$, $a(ca)^n$ переводят ребро e_0 в ребра e_n , \bar{e}_n , $e_{-(n+1)}$, $\bar{e}_{-(n+1)}$, соответственно. Поскольку любой автоморфизм графа \mathcal{C}_∞ полностью определяется образом ребра e_0 , все выписанные выше элементы различны и составляют группу D_∞ . По предложению 10.2 имеем $D_\infty \cong \langle a \rangle * \langle c \rangle$.

§ 11. Свободное произведение с объединением

Пусть даны группы G и H с выделенными в них изоморфными подгруппами A и B . Фиксируем изоморфизм $\varphi : A \rightarrow B$. Группа F , равная фактор-группе группы $G * H$ по нормальному замыканию множества $\{\varphi(a)a^{-1} \mid a \in A\}$, называется *свободным произведением G и H с объединением по A и B* . Для обозначения F используют записи

$$\langle G * H \mid a = \varphi(a) (a \in A) \rangle, \quad G \underset{A=B}{*} H, \quad G \underset{A}{*} H,$$

указывая в двух последних случаях изоморфизм φ .

Можно интерпретировать F как результат склейки A и B в свободном произведении $G * H$. Ниже мы определим A -нормальную форму и покажем, что произвольному элементу группы F соответствует единственная A -нормальная форма. Отсюда будет следовать, что G и H естественно вкладываются в F . Пусть $i : G * H \rightarrow F$ — канонический гомоморфизм. Любой элемент $f \in F$ записывается в виде $f = i(x_0)i(x_1) \cdots i(x_n)$, где $x_i \in G \cup H$. Условимся вместо этой записи использовать запись $f = x_0 x_1 \cdots x_n$.

Выберем систему представителей T_A правых смежных классов G по A и систему представителей T_B правых смежных классов H по B . Считаем, что представители подгрупп A и B равны 1. Любой $x \in G$ единственным образом записывается в виде $x = \tilde{x}\bar{x}$, где $\tilde{x} \in A$, $\bar{x} \in T_A$.

11.1. Определение. *A -нормальной формой* называется последовательность (x_0, x_1, \dots, x_n) такая, что

- 1) $x_0 \in A$,
- 2) $x_i \in T_A - \{1\}$ или $x_i \in T_B - \{1\}$ при $i \geq 1$, причем x_i и x_{i+1} лежат в разных системах представителей.

B -нормальная форма определяется аналогично, для нее $x_0 \in B$.

11.2. Пример. Пусть $G = \langle a \mid a^{12} = 1 \rangle$, $H = \langle b \mid b^{15} = 1 \rangle$, A и B — подгруппы порядка 3 в G и H , изоморфизм $\varphi : A \rightarrow B$ переводит a^4 в b^5 . Тогда свободное произведение G и H с объединением по A и B имеет представление $\langle a, b \mid a^{12} = 1, b^{15} = 1, a^4 = b^5 \rangle$. Пусть $T_A = \{1, a, a^2, a^3\}$, $T_B = \{1, b, b^2, b^3, b^4\}$. Запишем элемент $f = a^3ba^5$ в виде произведения множителей, составляющих A -нормальную форму. Для этого будем выделять представители справа налево и заменять элементы из A соответствующими элементами из B , и наоборот: $f = a^3ba^4 \cdot a = a^3b^6 \cdot a = a^3b^5 \cdot ba = a^3a^4 \cdot ba = a^4a^3ba$.

11.3. Теорема. *Любой элемент $f \in F = G \underset{A=B}{*} H$ представляется единственным способом в виде произведения $f = x_0x_1 \cdots x_n$, где (x_0, x_1, \dots, x_n) — A -нормальная форма.*

Доказательство. Существование такого представления доказывается индукцией с помощью постепенного выделения представителей справа налево.

Докажем единственность. Пусть W_A — множество всех A -нормальных форм, W_B — множество всех B -нормальных форм. Пусть $\varphi_* : W_A \rightarrow W_B$ — биекция, сопоставляющая набору (x_0, x_1, \dots, x_n) набор $(\varphi(x_0), x_1, \dots, x_n)$. Зададим действие группы G на множестве W_A . Пусть $g \in G$, $\tau = (x_0, x_1, \dots, x_n) \in W_A$. Положим

$$g \cdot \tau = \begin{cases} (gx_0, x_1, \dots, x_n), & \text{если } g \in A, \\ (\overline{gx_0}, \overline{gx_0}, x_1, \dots, x_n), & \text{если } g \notin A, x_1 \in H, \\ (gx_0x_1, x_2, \dots, x_n), & \text{если } g \notin A, x_1 \in G, \\ & gx_0x_1 \in A, \\ (\overline{gx_0x_1}, \overline{gx_0x_1}, x_2, \dots, x_n), & \text{если } g \notin A, x_1 \in G, \\ & gx_0x_1 \notin A. \end{cases}$$

11.4. Упражнение. *Покажите, что эти формулы действительно задают действие группы G на множестве W_A .*

Аналогично зададим действие группы H на множестве W_B . Биекция φ_* позволяет перенести это действие на множество W_A : $h \cdot \tau = \varphi_*^{-1}(h \cdot \varphi_*(\tau))$, $\tau \in W_A$, $h \in H$. Действия групп G и H на множестве W_A продолжаются до действия свободного произведения $G * H$ на W_A . Так как элементы $\varphi(a)a^{-1}$, где $a \in A$, лежат в ядре этого действия, то имеется естественное действие группы F на множестве W_A .

Пусть $f \in F$ и $f = x_0x_1 \cdots x_n$, где (x_0, x_1, \dots, x_n) — A -нормальная форма. Вычислим образ формы $(1) \in W_A$ под действием элемента f . Обозначим $f_i = x_0x_1 \cdots x_i$. Тогда $f \cdot (1) = f_{n-1} \cdot (1, x_n) = = f_{n-2} \cdot (1, x_{n-1}, x_n) = \cdots = f_0 \cdot (1, x_1, \dots, x_{n-1}, x_n) = (x_0, x_1, \dots, x_{n-1}, x_n)$.


Таким образом, элементу f соответствует единственная A -нормальная форма. Иногда саму запись $x_0x_1 \cdots x_n$ называют *нормальной формой элемента f* .

11.5. Следствие. Пусть $F = G \underset{A=B}{*} H$. Канонический гомоморфизм $i : G * H \rightarrow F$ индуцирует вложение групп G и H в группу F . Подгруппы $i(G)$ и $i(H)$ порождают группу F , их пересечение равно $i(A)$, что совпадает с $i(B)$.

Далее мы будем обозначать образы групп G, H, A и B в группе F теми же буквами.

11.6. Следствие. Пусть $G = G_1 \underset{A}{*} G_2$. Если $g \in G$ и $g = g_1g_2 \cdots g_n$, где $n \geq 1$, $g_i \in G_1 - A$ или $g_i \in G_2 - A$ в зависимости от четности i , то $g \neq 1$.

§ 12. Деревья и свободные произведения с объединением

Сегментом называется связный граф, состоящий из двух вершин и двух противоположных ребер: 

12.1. Теорема. Пусть $G = G_1 \underset{A}{*} G_2$. Тогда существует дерево X , на котором G действует без инверсий ребер так, что $G \setminus X$ — сегмент. При этом в X существует сегмент \tilde{T} , являющийся поднятием сегмента $G \setminus X$, стабилизаторы двух вершин и ребра которого в группе G равны G_1, G_2 и A соответственно.

Доказательство. Положим $X^0 = G/G_1 \cup G/G_2$, $X^1_+ = G/A$ (здесь все смежные классы левые). Положим $\alpha(gA) = gG_1$, $\omega(gA) = gG_2$, и пусть \tilde{T} — сегмент с вершинами G_1, G_2 и положительно ориентированным ребром A . Определим действие группы G на X левым умножением. Докажем, что граф X связан. Без ограничения общности достаточно доказать, что его вершина вида gG_1 связана путем с вершиной G_1 . Запишем элемент g в виде $g_1g_2 \cdots g_n$, где $g_i \in G_1$ или $g_i \in G_2$ в зависимости от четности i . Тогда вершины $g_1 \cdots g_{i-1}G_1$ и $g_1 \cdots g_iG_1$ при $g_i \in G_1$ совпадают, а при $g_i \in G_2$ соединены ребрами с вершиной $g_1 \cdots g_{i-1}G_2 (= g_1 \cdots g_iG_2)$. Теперь связность легко следует индукцией по n .

Докажем отсутствие циклов в графе X . Предположим, что в X существует замкнутый путь без возвращений $e_1 \dots e_n$. Сдвигая его на элемент из G , можно считать без ограничения общности, что $\alpha(e_1) = G_1$. Так как соседние вершины являются смежными классами по разным подгруппам, то n четно, и существуют такие элементы $x_i \in G_1 - A$, $y_i \in G_2 - A$, что $\alpha(e_2) = x_1 G_2$, $\alpha(e_3) = x_1 y_1 G_1$, \dots , $\alpha(e_n) = x_1 y_1 \dots x_{n/2} G_2$, $\omega(e_n) = x_1 y_1 \dots x_{n/2} y_{n/2} G_1$. Так как $\omega(e_n) = \alpha(e_1) = G_1$, то мы получаем противоречие с единственностью нормальной формы элемента в группе $G_1 *_A G_2$.

12.2. Замечание. В графе X , построенном выше, все ребра с началом в вершине gG_1 имеют вид gg_1A , где g_1 пробегает множество представителей левых смежных классов группы G_1 по подгруппе A . Валентность вершины gG_1 равна индексу $|G_1 : A|$. Стабилизатор вершины gG_1 равен gG_1g^{-1} . Аналогичные утверждения справедливы для вершины вида gG_2 .

12.3. Теорема. Пусть группа G действует без инверсий ребер на дереве X и фактор-граф $G \setminus X$ — сегмент. Пусть \tilde{T} — любое его поднятие, G_P , G_Q и G_e — стабилизаторы вершин P , Q и ребра e этого поднятия. Тогда гомоморфизм $\varphi : G_P *_e G_Q \rightarrow G$, тождественный на G_P и G_Q , является изоморфизмом.

Доказательство. 1) Докажем, что $G = \langle G_P, G_Q \rangle$. Обозначим $G' = \langle G_P, G_Q \rangle$ и предположим, что $G' < G$. Графы $G' \cdot \tilde{T}$ и $(G - G') \cdot \tilde{T}$ не пересекаются. Действительно, равенство $g'P = gQ$, где $g' \in G'$, $g \in G - G'$, невозможно, так как вершины P и Q не эквивалентны относительно действия G . Аналогично невозможно равенство $g'Q = gP$. Равенство $g'R = gR$, где $R \in \{P, Q\}$, тоже невозможно, так как из него следовало бы, что $g \in g'R \subseteq G'$. Осталось заметить, что $X = G \cdot \tilde{T}$ — связный граф, и поэтому его нельзя представить в виде объединения двух непересекающихся непустых подграфов. Противоречие.

2) Докажем, что гомоморфизм φ инъективен. Обозначим $\tilde{G} = G_P *_e G_Q$, и пусть \tilde{X} — дерево, построенное по \tilde{G} как в доказательстве теоремы 12.1. Зададим морфизм $\psi : \tilde{X} \rightarrow X$ правилом $gG_r \mapsto \varphi(g) \cdot r$, где $r \in \{P, Q, e\}$, $g \in \tilde{G}$. Этот морфизм является изоморфизмом: сюръективность вытекает из того, что $X = G \cdot \tilde{T}$ и $G = \langle G_P, G_Q \rangle$, инъективность следует из упражнения 1.5, замечания 12.2 и инъективности ограничений $\varphi|_{G_P}$, $\varphi|_{G_Q}$.

Пусть $g \in \tilde{G} - G_P$. Тогда вершины G_P и gG_P дерева \tilde{X} различны. Поэтому вершины P и $\varphi(g) \cdot P$ дерева X тоже различны. Следовательно $\varphi(g) \neq 1$ и инъективность φ доказана.

Приведем *другое доказательство* инъективности φ . Достаточно доказать, что $g_n \dots g_2 g_1 \neq 1$ в G при $n \geq 2$, где $g_i \in G_P - G_e$ или $g_i \in G_Q - G_e$ в зависимости от четности i . Без ограничения общности считаем, что $g_1 \in G_P - G_e$. Тогда g_1 фиксирует P и не фиксирует Q . Имеем $d(P, g_1 Q) = d(g_1 P, g_1 Q) = d(P, Q) = 1$, в частности, $d(Q, g_1 Q) = 2$. Поэтому можно представить себе, что g_1 действует на дереве X как поворот вокруг вершины P . При этом любой путь без возвратов, проходящий через вершины P и Q , переходит в путь без возвратов, проходящий через вершины P и $g_1 Q$. Аналогично g_2 действует на дереве X как поворот вокруг вершины Q . Опираясь на эти замечания, можно доказать по индукции, что $d(Q, g_i \dots g_2 g_1 Q)$ равно i при i четном и $i + 1$ при i нечетном. Поэтому $g_n \dots g_2 g_1 \neq 1$.

12.4. Пример. Группа D_∞ действует без инверсий ребер на барицентрическом разбиении графа C_∞ (см. § 1 и рис. 14).

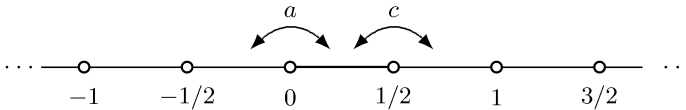


Рис. 14

Фактор-граф изоморфен сегменту. В качестве поднятия этого сегмента можно взять сегмент с вершинами 0 и 1/2. Стабилизаторы этих вершин равны $\langle a \rangle$ и $\langle c \rangle$, где $c = ba$. Стабилизатор ребра поднятия равен $\{1\}$. Поэтому $D_\infty \cong \langle a \rangle * \langle c \rangle$.

12.5. Упражнение. Пусть $\varphi: G \rightarrow H$ — эпиморфизм и пусть $H = H_1 *_{H_3} H_2$. Тогда $G = G_1 *_{G_3} G_2$, где $G_i = \varphi^{-1}(H_i)$.

§ 13. Действие группы $SL_2(\mathbb{Z})$ на гиперболической плоскости

Далее \mathbb{C} обозначает поле комплексных чисел. Каждое комплексное число z однозначно записывается в виде $z = x + iy$, где $x, y \in \mathbb{R}$, $i^2 = -1$. Числа x, y и $\sqrt{x^2 + y^2}$ обозначаются через $\text{Re}(z)$, $\text{Im}(z)$ и $|z|$ и называются вещественной частью, мнимой частью и модулем числа z соответственно.

Гиперболической плоскостью \mathbb{H}^2 называется множество $\{z \in \mathbb{C} \mid \text{Im}(z) > 0\}$, которое иногда удобно отождествлять с открытой верхней полуплоскостью евклидовой плоскости. Его элементы будем называть *точками*.

Гиперболическими прямыми называются открытые полуокружности и полупрямые (в евклидовом смысле) в \mathbb{H}^2 , замыкания которых пересекают вещественную ось под прямым углом (рис. 15).

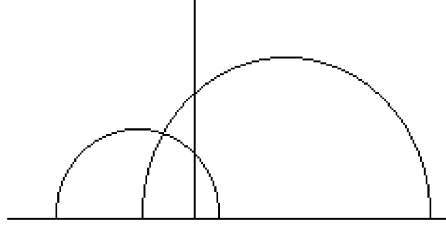


Рис. 15

13.1. Упражнение. 1) *Через любые две точки в \mathbb{H}^2 проходит единственная гиперболическая прямая.*

2) *Для любой гиперболической прямой l и любой точки $z \in \mathbb{H}^2$ вне этой прямой существует бесконечно много гиперболических прямых, проходящих через z и не пересекающих l .*

Дробно-линейным преобразованием плоскости \mathbb{H}^2 называется отображение $\mathbb{H}^2 \rightarrow \mathbb{H}^2$ вида $z \mapsto \frac{az+b}{cz+d}$, где $a, b, c, d \in \mathbb{R}$, $ad - bc = 1$. Следующее упражнение показывает, что образ \mathbb{H}^2 при таком отображении действительно лежит в \mathbb{H}^2 .

13.2. Упражнение. *Если $a, b, c, d \in \mathbb{R}$, $ad - bc = 1$ и $\text{Im}(z) > 0$, то число $\text{Im}\left(\frac{az+b}{cz+d}\right)$ превосходит число $\text{Im}(z)$ в $1/|cz+d|^2$ раз. В частности, это число положительно.*

Группа $\text{SL}_2(\mathbb{R})$ действует на \mathbb{H}^2 по правилу

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} : z \mapsto \frac{az+b}{cz+d}.$$

Ядро этого действия равно $\{\pm E\}$. Поэтому группу $\text{PSL}_2(\mathbb{R}) = \text{SL}_2(\mathbb{R})/\{\pm E\}$ можно отождествить с группой всех дробно-линейных

преобразований плоскости \mathbb{H}^2 . Группу $PSL_2(\mathbb{Z})$ можно рассматривать как подгруппу группы $PSL_2(\mathbb{R})$.

13.3. Упражнение. *Образ луча $\{z + it \mid t \geq 0\}$, где $z \in \mathbb{H}^2$, под действием матрицы $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ из $SL_2(\mathbb{R})$ является либо лучом (при $c = 0$), либо дугой окружности (при $c \neq 0$), замыкание которой содержит вещественную точку a/c .*

13.4. Упражнение. 1) *Группа $PSL_2(\mathbb{R})$ действует транзитивно и точно на множестве всех гиперболических прямых.*

2) *Группа $PSL_2(\mathbb{R})$ порождается преобразованиями $z \mapsto z + b$ ($b \in \mathbb{R}$), $z \mapsto az$ ($a \in \mathbb{R}, a > 0$), $z \mapsto -\frac{1}{z}$.*

3) *Группа $PSL_2(\mathbb{Z})$ порождается преобразованиями $\psi : z \mapsto z + 1$ и $\varphi : z \mapsto -\frac{1}{z}$.*

Пусть M обозначает объединение внутренности бесконечного гиперболического треугольника $XY\infty$ с частью своей границы, выделенной на рис. 16 жирной линией. Более точно,

$$M = \{z \mid 1 < |z|, -1/2 < \operatorname{Re}(z) \leq 1/2\} \cup \{e^{i\alpha} \mid \pi/3 \leq \alpha \leq \pi/2\}.$$

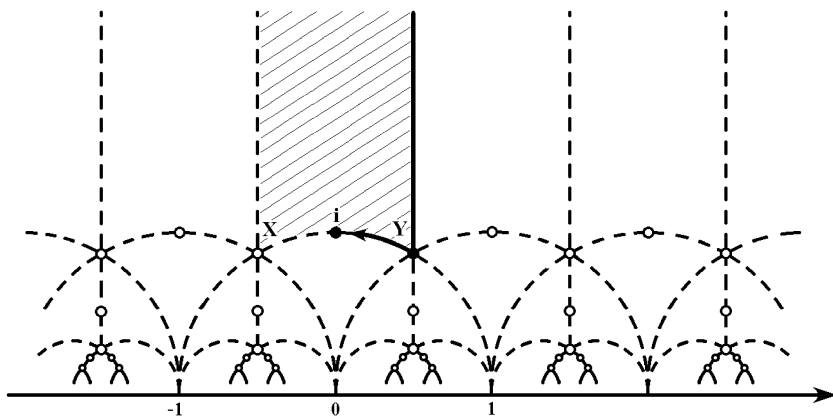


Рис. 16

13.5. Теорема. *Множество M является фундаментальной областью для действия группы $PSL_2(\mathbb{Z})$ на \mathbb{H}^2 , то есть относительно этого действия любая точка из \mathbb{H}^2 эквивалентна некоторой точке из M и различные точки из M не эквивалентны.*

Доказательство. 1) Докажем сначала, что любую точку z из \mathbb{H}^2 можно перевести в некоторую точку из \mathcal{M} подходящим элементом из $\mathrm{PSL}_2(\mathbb{Z})$.

Для данной точки $z \in \mathbb{H}^2$ среди всех ее образов под действием группы $\mathrm{PSL}_2(\mathbb{Z})$ выберем тот образ z' , у которого мнимая часть максимальна. Это возможно, так как при $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ число $\mathrm{Im}\left(\frac{az+b}{cz+d}\right)$ превосходит число $\mathrm{Im}(z)$ в $1/|cz+d|^2$ раз, а неравенство $|cz+d| \leq 1$ выполняется лишь для конечного множества пар (c, d) целых чисел.

Так как преобразование ψ не изменяет мнимой части, можно считать, что $-1/2 < \mathrm{Re}(z') \leq 1/2$. Из условия $\mathrm{Im}(z') \geq \mathrm{Im}(\varphi(z'))$ следует, что $|z'| \geq 1$. Итак, точка z' лежит в множестве \mathcal{M} или на дуге $\{e^{i\alpha} \mid \pi/2 < \alpha < 2\pi/3\}$. В последнем случае можно применить преобразование $z \mapsto -\frac{1}{z}$ и перевести z' в \mathcal{M} .

2) Докажем, что различные точки из \mathcal{M} не эквивалентны. Предположим, что $z' = \frac{az+b}{cz+d}$, где $z, z' \in \mathcal{M}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$. Если $c = 0$, то $a = d = \pm 1$, и, значит, $b = 0$, $z = z'$. Пусть $c \neq 0$. Имеем

$$\begin{aligned} (cz' - a)(cz + d) &= cz'(cz + d) - a(cz + d) = \\ &= c(az + b) - a(cz + d) = cb - ad = -1. \end{aligned}$$

Отсюда $|z' - a/c| \cdot |z + d/c| = 1/c^2$. Числа a/c и d/c вещественны, поэтому $|z' - a/c| \geq \mathrm{Im}(z' - a/c) = \mathrm{Im}(z') \geq \sqrt{3}/2$. Аналогично $|z + d/c| \geq \sqrt{3}/2$. Отсюда $|c| \leq 2/\sqrt{3}$. Так как c — ненулевое целое число, то $c = \pm 1$ и $|z' \mp a| \cdot |z \pm d| = 1$. При любых $w \in \mathcal{M}$ и $n \in \mathbb{Z}$ имеем $|w + n| \geq 1$, причем равенство возможно только при $n = -1, 0$. Это дает конечное число вариантов для a, b, c и d . Все они приводят к противоречию, если предположить, что $z \neq z'$.

13.6. Упражнение. Если матрица $g \in \mathrm{SL}_2(\mathbb{Z}) - \{\pm E\}$ стабилизирует точку $z \in \mathcal{M}$, то выполняется один из следующих случаев (матрицы $-E, A$ и B определены в теореме 13.7):

- 1) $z = e^{i\pi/2}$, g — степень матрицы A ,
- 2) $z = e^{i\pi/3}$, g — степень матрицы B .

13.7. Теорема. Объединение образов дуги $T = \{e^{i\alpha} \mid \pi/3 \leq \alpha \leq \pi/2\}$ под действием группы $\mathrm{SL}_2(\mathbb{Z})$ является деревом⁷. Группа $\mathrm{SL}_2(\mathbb{Z})$ действует на этом дереве без инверсий ребер так, что различные

⁷Точнее, геометрической реализацией дерева, так как наше определение дерева — комбинаторное.

точки дуги T не эквивалентны, ее стабилизатор и стабилизаторы ее концов $e^{i\pi/2}$ и $e^{i\pi/3}$ порождаются матрицами $-E = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$, $A = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ и $B = \begin{pmatrix} 0 & 1 \\ -1 & 1 \end{pmatrix}$ порядков 2, 4 и 6 соответственно. В частности,

$$SL_2(\mathbb{Z}) \cong Z_4 *_{Z_2} Z_6.$$

Доказательство. Докажем, что множество $X = SL_2(\mathbb{Z}) \cdot T$ является деревом. Связность X вытекает из того⁸, что $SL_2(\mathbb{Z}) = \langle A, B \rangle$ и матрицы A и B стабилизируют концы дуги T (аналогично доказывается связность X в теореме 12.1). Отсутствие пересечений различных образов T по внутренним точкам следует из теоремы 13.5 и упражнения 13.6. Предположим теперь, что некоторые образы T , рассмотренные как ребра графа, образуют цикл. Тогда эти образы ограничивают некоторую компактную область D в \mathbb{H}^2 . Так как образы \mathcal{M} покрывают \mathbb{H}^2 , то во внутренности D существует точка w , лежащая во внутренности некоторого сдвига $g\mathcal{M}$. По упражнению 13.3 из точки w во внутренности области $g\mathcal{M}$ идет либо луч, либо дуга, стремящаяся к точке на вещественной оси. И луч, и дуга должны пересечь границу области D . Получили противоречие с тем, что внутренние точки из \mathcal{M} не эквивалентны граничным. Итак, X — дерево. Остальные утверждения теоремы проверяются легко, последнее следует из теоремы 12.3.

13.8. Упражнение. Пусть $C = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$. Докажите, что $\langle -E, C \rangle \cong D_2$, $\langle A, C \rangle \cong D_4$, $\langle B, C \rangle \cong D_6$. Выведите отсюда, что $GL_2(\mathbb{Z}) \cong D_4 *_{D_2} D_6$.

Следующие четыре теоремы мы приводим без доказательств.

Свободное произведение с объединением $G_1 *_{G_3} G_2$ называется *нетривиальным*, если $G_3 \neq G_1$ и $G_3 \neq G_2$.

13.9. Теорема (Серр [61]). При $n \geq 3$ группы $SL_n(\mathbb{Z})$ и $GL_n(\mathbb{Z})$ не представимы в виде нетривиального свободного произведения с объединением.

Пусть F_n — свободная группа с базисом $X = \{x_1, x_2, \dots, x_n\}$, $\text{Aut}(F_n)$ — группа ее автоморфизмов. Группа $\text{Aut}(F_n)$ является таким же классическим объектом в теории групп, что и группа $GL_n(\mathbb{Z})$. Известно (см. [53]), что существует эпиморфизм $\text{Aut}(F_n) \rightarrow GL_n(\mathbb{Z})$, заданный следующим правилом: элементу $\alpha \in \text{Aut}(F_n)$ сопоставляется

⁸Известно, что $SL_2(\mathbb{Z})$ порождается трансвекциями $t_{12}(1)$ и $t_{21}(1)$ равными $B^{-1}A$ и BA^{-1} .

матрица $\bar{\alpha}$, такая, что ее элемент $\bar{\alpha}_{ij}$ равен сумме показателей при букве x_i в слове $\alpha(x_j)$. Обозначим через $\text{SAut}(F_n)$ полный прообраз группы $\text{SL}_n(\mathbb{Z})$ при этом эпиморфизме.

13.10. Теорема (Богопольский [5]).

1) При $n \geq 3$ группы $\text{Aut}(F_n)$ и $\text{SAut}(F_n)$ не представимы в виде нетривиального свободного произведения с объединением.

2) Группа $\text{Aut}(F_2)$ разлагается единственным способом, с точностью до сопряжения сомножителей, в нетривиальное свободное произведение с объединением.

Заметим, что теорема 13.9 следует из первого утверждения теоремы 13.10 в силу упражнения 12.5

Доказательства следующих теорем Ихары и Нагао содержатся в [61].

Пусть p — простое число. Через $\mathbb{Z}[1/p]$ обозначим подкольцо кольца \mathbb{Q} рациональных чисел, состоящее из всех чисел вида n/p^k , где $n \in \mathbb{Z}$, $k \in \{0, 1, \dots\}$. Кольцо $\mathbb{Z}[1/p]$ называется *кольцом p -ичных дробей*.

13.11. Теорема (Ихара).

$$\text{SL}_2(\mathbb{Z}[1/p]) \cong \text{SL}_2(\mathbb{Z}) \underset{\Gamma_0(p)}{*} \text{SL}_2(\mathbb{Z}),$$

где $\Gamma_0(p)$ — подгруппа группы $\text{SL}_2(\mathbb{Z})$, состоящая из всех матриц вида $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$, в которых $c \equiv 0 \pmod{p}$.

Пусть K — произвольное коммутативное ассоциативное кольцо с единицей. Обозначим через $B(K)$ подгруппу группы $\text{GL}_2(K)$, состоящую из всех матриц вида $\begin{pmatrix} a & b \\ 0 & d \end{pmatrix}$.

13.12. Теорема (Нагао). Пусть $k[t]$ — кольцо многочленов от переменной t над полем k . Тогда

$$\text{GL}_2(k[t]) = \text{GL}_2(k) \underset{B(k)}{*} B(k[t]).$$

13.13. Теорема (Санов). Для любого целого $m \geq 2$ матрицы

$$t_{12}(m) = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}, \quad t_{21}(m) = \begin{pmatrix} 1 & 0 \\ m & 1 \end{pmatrix}$$

порождают в $\text{SL}_2(\mathbb{Z})$ свободную группу ранга 2.

Доказательство. В обозначениях теоремы 13.7 имеем $t_{12}(m) = (B^{-1}A)^m$ и $t_{21}(m) = (BA^{-1})^m$. Остается заметить, что любое непустое приведенное слово от слов $(B^{-1}A)^m$ и $(BA^{-1})^m$ имеет неединичную нормальную форму в свободном произведении с объединением из теоремы 13.7.

Другое доказательство этой теоремы, использующее прямые матричные вычисления, изложено в [10].

§ 14. HNN-расширения

Пусть G — группа, A и B — ее изоморфные подгруппы и $\varphi : A \rightarrow B$ — фиксированный изоморфизм. Пусть $\langle t \rangle$ — бесконечная циклическая группа, порожденная элементом t , не входящим в G . Группа G^* , равная фактор-группе группы $G * \langle t \rangle$ по нормальному замыканию множества $\{t^{-1}at(\varphi(a))^{-1} \mid a \in A\}$, называется *HNN-расширением* группы G относительно A , B и φ . Группа G называется *базой* HNN-расширения G^* , t — *проходной буквой*, A и B — *ассоциированными подгруппами*. Для обозначения группы G^* используют записи

$$\langle G, t \mid t^{-1}at = \varphi(a) \ (a \in A) \rangle \quad \text{и} \quad G_A^*,$$

указывая в последнем случае изоморфизм φ .

Ниже мы покажем, что произвольный элемент в группе G^* имеет единственную нормальную форму. Отсюда будет следовать, что группы G и $\langle t \rangle$ канонически вкладываются в G^* . Если отождествить эти группы с их образами в G^* , то окажется, что подгруппы A и B сопряжены элементом t , причем ограничение на A автоморфизма, индуцированного сопряжением элементом t , совпадает с изоморфизмом φ .

Пусть $i : G * \langle t \rangle \rightarrow G^*$ — канонический гомоморфизм. Любой элемент $x \in G^*$ записывается в виде $x = i(g_0)i(t)^{\varepsilon_1}i(g_1) \cdots i(t)^{\varepsilon_n}i(g_n)$, где $g_i \in G$, $\varepsilon_j = \pm 1$. Условимся вместо этой записи использовать запись $x = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$.

Выберем систему представителей T_A правых смежных классов G по A и систему представителей T_B правых смежных классов G по B . Считаем, что представители классов A и B равны 1. Если $g \in G$, то через \bar{g} обозначим представитель смежного класса Ag , лежащий в T_A , а через \hat{g} — представитель смежного класса Bg , лежащий в T_B .

Буква g с индексом будет обозначать элемент группы G . Буква ε с индексом или без будет обозначать 1 или -1 .

14.1. Определение. *Нормальной формой* называется последовательность $(g_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n)$ в которой

- 1) g_0 — произвольный элемент из G ,
- 2) если $\varepsilon_i = -1$, то $g_i \in T_A$,
- 3) если $\varepsilon_i = 1$, то $g_i \in T_B$,
- 4) нет последовательных вхождений $t^\varepsilon, 1, t^{-\varepsilon}$.

Пользуясь соотношениями $t^{-1}a = \varphi(a)t^{-1}$ и $tb = \varphi^{-1}(b)t$, где $a \in A$, $b \in B$, можно каждый элемент из G^* привести к виду $g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$, где последовательность $(g_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n)$ — нормальная форма.

14.2. Пример. Рассмотрим HNN-расширение $G^* = \langle a, b, t \mid t^{-1}a^2t = b^3 \rangle$ с базой $G = F(a, b)$ и ассоциированными подгруппами $A = \langle a^2 \rangle$ и $B = \langle b^3 \rangle$. Пусть T_A — множество всех приведенных слов в $F(a, b)$ вида u, au , где u не начинается с $a^{\pm 1}$. Пусть T_B — множество всех приведенных слов в $F(a, b)$ вида v, vb, vb^2 , где v не начинается с $b^{\pm 1}$. Вычислим нормальную форму, соответствующую элементу $x = b^2 t^{-1} a^{-4} t b^5 a b t^{-1} a^4 b^3 a$, двигаясь справа налево. Поскольку представитель класса $A a^4 b^3 a$ равен $b^3 a$ и $t^{-1} a^4 = b^6 t^{-1}$, имеем $x = b^2 t^{-1} a^{-4} t b^5 a b^7 t^{-1} b^3 a$. Поскольку представитель класса $B b^5 a b^7$ равен $b^2 a b^7$ и $t b^3 = a^2 t$, то $x = b^2 t^{-1} a^{-2} t b^2 a b^7 t^{-1} b^3 a = b a b^7 t^{-1} b^3 a$, где $(b a b^7, t^{-1}, b^3 a)$ — уже нормальная форма.

14.3. Теорема. Пусть $G^* = \langle G, t \mid t^{-1} a t = \varphi(a) \ (a \in A) \rangle$ — HNN-расширение группы G с ассоциированными подгруппами A и B . Тогда выполняются следующие утверждения.

- 1) Каждый элемент x группы G^* имеет единственное представление $x = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$, где последовательность $(g_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n)$ — нормальная форма⁹.
- 2) Группа G вкладывается в группу G^* посредством отображения $g \mapsto g$. Если в записи $x = g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$, где $n \geq 1$, нет вхождений $t^{-1} g_i t$, где $g_i \in A$ и нет вхождений $t g_j t^{-1}$, где $g_j \in B$, то $x \neq 1$ в G^* .

Утверждение о вложении G в G^* доказали Хигман, Х. Нейман и Б. Нейман. В их честь эта конструкция называется HNN-расширением. Остальную часть утверждения 2 доказал Бриттон и эта часть называется леммой Бриттона.

Доказательство первого утверждения идейно повторяет доказательство теоремы 11.3. Существование нужного представления доказывается с помощью постепенного выделения представителей справа налево и замен $t^{-1}a = \varphi(a)t^{-1}$ при $a \in A$ и $tb = \varphi^{-1}(b)t$ при $b \in B$. Для доказательства единственности определим действие группы G^* на множестве W всех нормальных форм так, чтобы образ формы (1), содер-

⁹Поэтому саму запись $g_0 t^{\varepsilon_1} g_1 \cdots t^{\varepsilon_n} g_n$ также называют нормальной формой элемента x .

жащей только единицу, под действием элемента x был равен искомой нормальной форме для x .

Пусть $\tau = (g_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n) \in W$. Для элементов $g \in G$, t и t^{-1} определим их действия на τ следующими формулами:

$$g \cdot \tau = (gg_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n),$$

$$t \cdot \tau = \begin{cases} (\varphi^{-1}(g_0)g_1, t^{\varepsilon_2}, g_2, \dots, t^{\varepsilon_n}, g_n), & \text{если } \varepsilon_1 = -1, g_0 \in B, \\ (\varphi^{-1}(b), t, \widehat{g_0}, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n) & \text{в противном случае,} \end{cases}$$

где b — такой элемент из B , что $g_0 = b\widehat{g_0}$,

$$t^{-1} \cdot \tau = \begin{cases} (\varphi(g_0)g_1, t^{\varepsilon_2}, g_2, \dots, t^{\varepsilon_n}, g_n), & \text{если } \varepsilon_1 = 1, g_0 \in A, \\ (\varphi(a), t^{-1}, \overline{g_0}, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n) & \text{в противном случае,} \end{cases}$$

где a — такой элемент из A , что $g_0 = a\overline{g_0}$.

Первая формула задает действие группы G на множестве W . Вторая и третья формулы задают действие группы $\langle t \rangle$ на W (упражнение 14.4). Поэтому мы имеем действие группы $G * \langle t \rangle$ на W . Ее подгруппа N , равная нормальному замыканию множества $\{t^{-1}at\varphi(a)^{-1} \mid a \in A\}$, действует на W тождественно (упражнение 14.5). Поэтому $G \cap N = \{1\}$, и, значит, G вкладывается в $G^* = (G * \langle t \rangle) / N$. Тождественность действия N позволяет определить также действие группы G^* на W . То, что любому элементу $x \in G^*$ соответствует единственная нормальная форма, следует из упражнения 14.6. Второе утверждение теоремы вытекает из первого и процесса приведения элемента из G^* к нормальной форме.

14.4. Упражнение. Докажите, что композиция действий элементов t и t^{-1} на W тождественна.

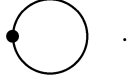
14.5. Упражнение. Докажите, что действия элементов $t^{-1}at$ и $\varphi(a)$ на W совпадают для любых a из A .

14.6. Упражнение. Пусть $x \in G^*$ и $x = g_0 t^{\varepsilon_1} g_1 \dots t^{\varepsilon_n} g_n$, где $(g_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n)$ — нормальная форма. Докажите, что образ нормальной формы (1) под действием элемента x равен форме $(g_0, t^{\varepsilon_1}, g_1, \dots, t^{\varepsilon_n}, g_n)$.

14.7. Следствие. Пусть $G^* = \langle G, t \mid t^{-1}at = \varphi(a) (a \in A) \rangle$ — HNN-расширение группы G с ассоциированными подгруппами A и B . Тогда канонический гомоморфизм $i : G * \langle t \rangle \rightarrow G^*$ индуцирует вложение групп G и $\langle t \rangle$ в группу G^* . отождествим эти группы с их образами в G^* . Тогда подгруппы A и B сопряжены в G^* элементом t , причем ограничение на A автоморфизма, индуцированного сопряжением элементом t , совпадает с изоморфизмом φ .

§ 15. Деревья и HNN-расширения

Петлей называется граф, состоящий из одной вершины и двух противоположных ребер, имеющих начало и конец в этой вершине:



15.1. Теорема. Пусть $G = \langle H, t \mid t^{-1}at = \varphi(a) \ (a \in A) \rangle$ — HNN-расширение группы H с ассоциированными подгруппами A и $\varphi(A)$. Тогда существует дерево X , на котором G действует без инверсий ребер так, что $G \setminus X$ — петля. При этом в X существует сегмент \tilde{Y} , отображающийся на эту петлю, стабилизаторы двух вершин и ребра которого в группе G равны H , tHt^{-1} и A соответственно.

Доказательство. Положим $X^0 = G/H$, $X^1_+ = G/A$ (здесь все смежные классы — левые), $\alpha(gA) = gH$, $\omega(gA) = gtH$ и пусть \tilde{Y} — сегмент с вершинами H , tH и положительно ориентированным ребром A . Определим действие группы G на графе X левым умножением. Дальнейшее доказательство аналогично доказательству теоремы 12.1 и мы оставляем его читателю.

15.2. Теорема. Пусть группа G действует без инверсий ребер на дереве X и фактор-граф $Y = G \setminus X$ — петля. Пусть \tilde{Y} — любой сегмент в X , отображающийся на эту петлю, G_P , G_Q и G_e — стабилизаторы вершин P , Q и ребра e этого сегмента. Пусть $x \in G$ — произвольный элемент такой, что $Q = xP$. Положим $G'_e = x^{-1}G_e x$ и пусть $\varphi : G_e \rightarrow G'_e$ — изоморфизм, индуцированный сопряжением элементом x . Тогда $G'_e \leq G_P$ и гомоморфизм

$$\langle G_P, t \mid t^{-1}at = \varphi(a) \ (a \in G_e) \rangle \rightarrow G,$$

тождественный на G_P и переводящий t в x , является изоморфизмом.

Доказательство аналогично доказательству теоремы 12.3.

§ 16. Граф групп и его фундаментальная группа

В этом параграфе мы дадим определение фундаментальной группы графа групп, обобщающее понятия свободного произведения с объединением и HNN-расширения.

16.1. Определение. Граф групп (\mathbb{G}, Y) состоит из связного графа Y , наборов групп $\{G_v \mid v \in Y^0\}$, $\{G_e \mid e \in Y^1\}$ и вложений $\{\alpha_e : G_e \rightarrow G_{\alpha(e)} \mid e \in Y^1\}$ с условием $G_e = G_{\bar{e}}$.

Группы G_v при $v \in Y^0$ называются *вершинными*, группы G_e при $e \in Y^1$ — *реберными*. Иногда удобно использовать вложение $\omega_e : G_e \rightarrow G_{\omega(e)}$, заданное равенством $\omega_e = \alpha_{\bar{e}}$.

Обозначим через $F(\mathbb{G}, Y)$ фактор-группу свободного произведения всех групп G_v ($v \in Y^0$) и свободной группы с базисом $\{t_e | e \in Y^1\}$ по нормальному замыканию множества элементов $t_e^{-1} \alpha_e(g) t_e \cdot (\alpha_{\bar{e}}(g))^{-1}$ и $t_e t_{\bar{e}}$ ($e \in Y^1, g \in G_e$).

Далее мы определим фундаментальную группу графа групп (\mathbb{G}, Y) относительно вершины и относительно максимального поддерева графа Y . Будет доказано, что эти определения дают изоморфные группы.

16.2. Определение. Пусть P — произвольная вершина графа Y . *Фундаментальной группой* $\pi_1(\mathbb{G}, Y, P)$ графа групп (\mathbb{G}, Y) относительно вершины P называется подгруппа группы $F(\mathbb{G}, Y)$, состоящая из всех элементов вида $g_0 t_{e_1} g_1 t_{e_2} \dots t_{e_n} g_n$, где $e_1 e_2 \dots e_n$ — замкнутый путь в Y с началом в P , $g_0 \in G_P, g_i \in G_{\omega(e_i)}, 1 \leq i \leq n$.

16.3. Определение. *Фундаментальной группой* $\pi_1(\mathbb{G}, Y, T)$ графа групп (\mathbb{G}, Y) относительно максимального поддерева T графа Y называется фактор-группа группы $F(\mathbb{G}, Y)$ по нормальному замыканию множества элементов t_e ($e \in T^1$).

16.4. Примеры.

1) Если $G_v = \{1\}$ для всех $v \in Y^0$, то $\pi_1(\mathbb{G}, Y, P) \cong \pi_1(Y, P)$, где $\pi_1(Y, P)$ — фундаментальная группа графа Y относительно вершины P , определенная в § 4.

2) Если $Y = \overset{P}{\bullet} \xrightarrow{e} \overset{Q}{\bullet}$ — сегмент, то группа $\pi_1(\mathbb{G}, Y, P)$ изоморфна свободному произведению групп G_P и G_Q с объединением по $\alpha_e(G_e)$ и $\alpha_{\bar{e}}(G_e)$.

3) Если $Y = \overset{P}{\bullet} \circlearrowright e$ — петля, то группа $\pi_1(\mathbb{G}, Y, P)$ изоморф-

на HNN-расширению с базой G_P и ассоциированными подгруппами $\alpha_e(G_e)$ и $\alpha_{\bar{e}}(G_e)$.

4) Для произвольного графа групп (\mathbb{G}, Y) его фундаментальная группа $\pi_1(\mathbb{G}, Y, T)$ получается многократным применением¹⁰ конструкции HNN-расширения к фундаментальной группе дерева групп $\pi_1(\mathbb{G}, T, T)$, которая сама строится из фундаментальной группы сегмента групп (при $|T^0| > 1$) с помощью конструкции свободного произведения с объединением.

¹⁰Количество применений равно числу пар противоположных ребер графа Y , не входящих в дерево T .

16.5. Теорема. Пусть (\mathbb{G}, Y) — граф групп, P — вершина, T — максимальное поддереве графа Y . Ограничение p канонического гомоморфизма $F(\mathbb{G}, Y) \rightarrow \pi_1(\mathbb{G}, Y, T)$ на подгруппу $\pi_1(\mathbb{G}, Y, P)$ является изоморфизмом на $\pi_1(\mathbb{G}, Y, T)$.

Доказательство. Для любой вершины v графа Y , отличной от P , существует единственный путь без возвратов $e_1 e_2 \dots e_k$ в дереве T из P в v . Соответствующий ему элемент $t_{e_1} t_{e_2} \dots t_{e_k}$ группы $F(\mathbb{G}, Y)$ обозначим через γ_v . Положим $\gamma_P = 1$. Определим отображение q' из множества порождающих группы $\pi_1(\mathbb{G}, Y, T)$ в группу $\pi_1(\mathbb{G}, Y, P)$ правилами $g \mapsto \gamma_v g \gamma_v^{-1}$ при $g \in G_v, v \in Y^0$ и $t_e \mapsto \gamma_{\alpha(e)} t_e \gamma_{\omega(e)}^{-1}$ при $e \in Y^1$. Теорема вытекает из следующего упражнения.

16.6. Упражнение. 1) Отображение q' продолжается до гомоморфизма $q: \pi_1(\mathbb{G}, Y, T) \rightarrow \pi_1(\mathbb{G}, Y, P)$.

2) Гомоморфизмы $q \circ p$ и $p \circ q$ тождественны.

16.7. Следствие. Фундаментальные группы $\pi_1(\mathbb{G}, Y, P)$ и $\pi_1(\mathbb{G}, Y, T)$ изоморфны при всех возможных выборах вершины P и максимального поддерева T в графе Y .

Класс изоморфности этих групп обозначается через $\pi_1(\mathbb{G}, Y)$.

16.8. Приведенная запись. Пусть (\mathbb{G}, Y) — граф групп с выделенным максимальным поддеревом T в Y . Пусть $g \in G_v, g' \in G_u$, где $u, v \in Y^0$. Скажем, что элементы g и g' эквивалентны (относительно T), если $g' = \omega_{e_k} \alpha_{e_k}^{-1} \dots \omega_{e_1} \alpha_{e_1}^{-1}(g)$, где $e_1 \dots e_k$ — путь без возвратов в дереве T из v в u . Считаем также, что g эквивалентно g .

Фиксируем некоторую ориентацию Y_+^1 графа Y . Тогда любой элемент $x \in \pi_1(\mathbb{G}, Y, T)$ можно записать в виде $g_1 g_2 \dots g_n$, где каждый g_i принадлежит некоторой вершинной группе или равен $t_e^{\pm 1}$ при $e \in Y_+^1 - T^1$. Такая запись называется *приведенной*, если в ней

1) соседние элементы не эквивалентны элементам одной и той же вершинной группы (в частности, соседние элементы не лежат в одной и той же вершинной группе),

2) нет вхождений вида $t_e t_e^{-1}$ и $t_e^{-1} t_e$,

3) нет вхождений вида $t_e^{-1} g t_e$, где g — элемент некоторой вершинной группы, эквивалентный элементу из $\alpha_e(G_e)$,

4) нет вхождений вида $t_e g t_e^{-1}$, где g — элемент некоторой вершинной группы, эквивалентный элементу из $\omega_e(G_e)$.

Заметим, что если исходная запись $g_1 g_2 \dots g_n$ не приведена, то ее можно укоротить, воспользовавшись соотношениями группы $\pi_1(\mathbb{G}, Y, T)$. Это обеспечивает существование приведенной записи для любого элемента $x \in \pi_1(\mathbb{G}, Y, T)$. Как показывает следующий пример, элемент может иметь несколько приведенных записей.

16.9. Пример. Пусть Y — граф с вершинами u, v и ребрами $e_1, \bar{e}_1, e_2, \bar{e}_2$ такими, что $\alpha(e_1) = \alpha(e_2) = u, \omega(e_1) = \omega(e_2) = v$. Положим $G_u = \langle a \mid a^{12} = 1 \rangle, G_v = \langle b \mid b^{18} = 1 \rangle, G_{e_1} = \langle c \mid c^2 = 1 \rangle, G_{e_2} = \langle d \mid d^3 = 1 \rangle$; $\alpha_{e_1}(c) = a^6, \omega_{e_1}(c) = b^9, \alpha_{e_2}(d) = a^4, \omega_{e_2}(d) = b^6$. Пусть T — максимальное поддерево графа Y , содержащее вершины u, v и ребра e_1, \bar{e}_1 . Тогда

$$\pi_1(\mathbb{G}, Y, T) = \langle a, b, t \mid a^{12} = 1, b^{18} = 1, a^6 = b^9, t^{-1}a^4t = b^6 \rangle.$$

Элемент $bt^{-1}a^3ta^6b^3t^{-1}$ имеет приведенные записи $bt^{-1}a^{-1}$ и $b^{-5}t^{-1}a^3$.

16.10. Теорема. Если элемент g фундаментальной группы $\pi_1(\mathbb{G}, Y, T)$ имеет приведенную запись, отличную от 1, то $g \neq 1$. В частности, группы G_v ($v \in Y^0$) канонически вкладываются в группу $\pi_1(\mathbb{G}, Y, T)$.

Доказательство ведется индукцией по числу ребер графа Y с учетом утверждений 16.4. База индукции имеется ввиду следствий 11.5, 11.6 и теоремы 14.3.

§ 17. СВЯЗЬ СВОБОДНЫХ ПРОИЗВЕДЕНИЙ с объединением и HNN-расширений

Пусть $G = \langle H, t \mid t^{-1}at = \varphi(a) \ (a \in A) \rangle$ — HNN-расширение. Докажем, что ядро эпиморфизма $\theta : G \rightarrow \langle t \rangle$, заданного правилом $t \mapsto t, h \mapsto 1 \ (h \in H)$, является свободным произведением с объединением.

Пусть \mathcal{C}_∞ — граф, введенный в § 1. Напомним, что вершинами графа \mathcal{C}_∞ являются все целые числа, ребрами — символы e_n, \bar{e}_n ($n \in \mathbb{Z}$), причем $\alpha(e_n) = n, \omega(e_n) = n + 1$. Вершине n сопоставим группу $H_n = \{h_n \mid h \in H\}$, являющуюся n -й копией группы H , каждому ребру сопоставим группу A . Вложения группы A , соответствующей ребру e_n , в вершинные группы H_n и H_{n+1} зададим правилами $a \mapsto (\varphi(a))_n$ и $a \mapsto a_{n+1}$.

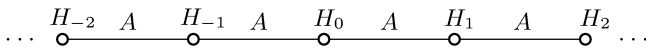


Рис. 17

Фундаментальная группа F построенного графа групп (рис. 17) имеет представление

$$\langle \ast_{i \in \mathbb{Z}} H_i \mid a_{n+1} = (\varphi(a))_n \ (a \in A, n \in \mathbb{Z}) \rangle.$$

Пусть $\langle t \rangle$ — бесконечная циклическая группа, порожденная элементом t . Образует полупрямое произведение $F \rtimes \langle t \rangle$, задав действие t на F правилом $t^{-1}h_it = h_{i+1}$ ($h_i \in H_i, i \in \mathbb{Z}$).

17.1. Теорема. $F \rtimes \langle t \rangle \cong G$.

Доказательство следует из того, что группа $F \rtimes \langle t \rangle$ порождается подгруппой H_0 и элементом t и все ее соотношения выводятся из соотношений группы H_0 и соотношений $t^{-1}a_0t = (\varphi(a))_0$ ($a \in A$).

17.2. Упражнение. Пусть $A \leq C, B \leq D$ и $\varphi : A \rightarrow B$ — изоморфизм. Гомоморфизм из свободного произведения с объединением $G = \langle C * D \mid a = \varphi(a) (a \in A) \rangle$ в HNN-расширение $F = \langle C * D, t \mid t^{-1}at = \varphi(a) (a \in A) \rangle$, заданный правилом $c \mapsto t^{-1}ct$ ($c \in C$), $d \mapsto d$ ($d \in D$), является вложением.

Указание. Этот гомоморфизм переводит неединичную приведенную запись из G в неединичную приведенную запись из F .

17.3. Упражнение. Выведите следствие 11.6 из теоремы 14.3 и упражнения 17.2.

§ 18. Структура группы, действующей на дереве

18.1. Определение. Пусть $p : X \rightarrow Y$ — морфизм из дерева в связный граф и пусть T — максимальное поддерево в Y . Пару (\tilde{T}, \tilde{Y}) поддеревьев дерева X назовем *поднятием пары графов* (T, Y) , если $\tilde{T} \subseteq \tilde{Y}$ и

- 1) любое ребро из $\tilde{Y}^1 - \tilde{T}^1$ имеет начало или конец в \tilde{T} ,
- 2) p отображает \tilde{T} изоморфно на T и p отображает $\tilde{Y}^1 - \tilde{T}^1$ биективно на $Y^1 - T^1$.

Для вершины $v \in Y^0$ ($= T^0$) обозначим через \tilde{v} ее прообраз в \tilde{T}^0 , а для ребра $e \in Y^1$ обозначим через \tilde{e} его прообраз в \tilde{Y}^1 (см. рис. 18).

Ввиду теоремы 16.10 мы отождествляем вершинные группы графа групп (\mathbb{G}, Y) с их каноническими образами в фундаментальной группе $\pi_1(\mathbb{G}, Y, T)$.

18.2. Теорема. Пусть $G = \pi_1(\mathbb{G}, Y, T)$ — фундаментальная группа графа групп (\mathbb{G}, Y) относительно максимального поддерева T . Тогда группа G действует без инверсий ребер на некотором дереве X так, что фактор-граф $G \backslash X$ изоморфен графу Y и стабилизаторы вершин и ребер дерева X сопряжены с каноническими образами в G групп вида G_v ($v \in Y^0$) и $\alpha_e(G_e)$ ($e \in Y^1$) соответственно.

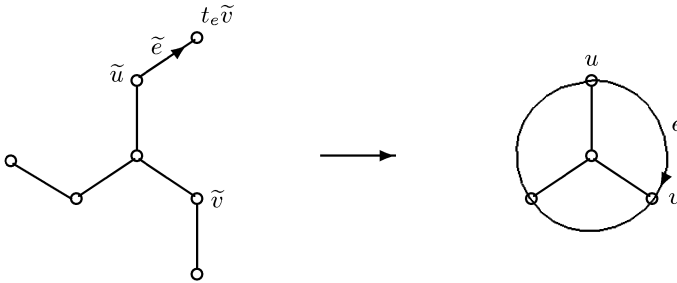


Рис. 18

Более того, для проекции $p : X \rightarrow Y$, связанной с этим действием, существует такое поднятие (\tilde{T}, \tilde{Y}) пары (T, Y) , что

1) стабилизатор любой вершины $\tilde{v} \in \tilde{T}^0$ (ребра $\tilde{e} \in \tilde{Y}^1$ с началом в \tilde{T}^0) в группе G равен группе G_v (группе $\alpha_e(G_e)$),

2) если конец ребра $\tilde{e} \in \tilde{Y}^1$ не лежит в \tilde{T}^0 , то элемент t_e^{-1} переводит этот конец в \tilde{T}^0 .

Доказательство аналогично доказательству теоремы 12.1. Поэтому мы лишь определим графы X, \tilde{T}, \tilde{Y} и действие группы G на X .

Выберем произвольную ориентацию графа Y . Для каждой вершины $v \in Y^0$ отождествим группу G_v с ее каноническим образом в группе G . Для каждого ребра $e \in Y^1_+$ отождествим группу G_e с каноническим образом подгруппы $\alpha_e(G_e)$ в группе G . Напомним, что $t_e = 1$ в группе G тогда и только тогда, когда $e \in T^1$.

Граф X определяется следующим образом (все объединения раздельные, все смежные классы левые):

$$X^0 = \bigcup_{v \in Y^0} G/G_v, \quad X^1_+ = \bigcup_{e \in Y^1_+} G/G_e,$$

$$\alpha(gG_e) = gG_{\alpha(e)}, \quad \omega(gG_e) = gt_e G_{\omega(e)} \quad (g \in G, e \in Y^1_+).$$

Группа G действует на графе X левым умножением.

Валентность вершины gG_v равна $\sum |G_v : \alpha_e(G_e)|$, где сумма берется по всем ребрам $e \in Y^1$ с началом v .

Поднятие \tilde{T} дерева T определяется естественным образом:

$$\tilde{T}^0 = \bigcup_{v \in T^0} \{G_v\}, \quad \tilde{T}^1_+ = \bigcup_{e \in T^1_+} \{G_e\}.$$

В граф \tilde{Y} кроме вершин и ребер графа \tilde{T} входят еще вершины $t_e G_{\omega(e)}$ и ребра G_e ($e \in Y_+^1 - T_+^1$), а также обратные к ним ребра.

18.3. Следствие. *Любая конечная подгруппа фундаментальной группы $\pi_1(\mathbb{G}, Y, T)$ сопряжена с подгруппой некоторой ее вершинной группы.*

Доказательство вытекает из теоремы 18.2 и следствия 2.6.

18.4. Пусть G — произвольная группа, X — дерево, и пусть G действует на X без инверсий ребер. Пусть $Y = G \backslash X$ — фактор-граф, T — некоторое его максимальное поддерево, $p : X \rightarrow Y$ — каноническая проекция и (\tilde{T}, \tilde{Y}) — любое поднятие пары (T, Y) .

Определим граф групп (\mathbb{G}, Y) следующим образом. Для каждой вершины или ребра y графа Y положим G_y равным стабилизатору $\text{St}_G(\tilde{y})$ соответствующего поднятия \tilde{y} . Для каждого ребра $e \in Y^1 - T^1$ такого, что $\omega(\tilde{e}) \notin \tilde{T}^0$, выберем произвольный элемент $t_e \in G$ такой, что $\omega(\tilde{e}) = t_e \omega(e)$ (напомним, что $\omega(e) \in \tilde{T}^0$). Положим $t_{\bar{e}} = t_e^{-1}$.

Для каждого $e \in Y^1$ зададим вложение $\omega_e : G_e \rightarrow G_{\omega(e)}$ следующим образом:

$$\omega_e(g) = \begin{cases} g, & \text{если } \omega(\tilde{e}) \in \tilde{T}^0, \\ t_e^{-1} g t_e, & \text{если } \omega(\tilde{e}) \in \tilde{Y}^0 - \tilde{T}^0. \end{cases}$$

18.5. Теорема. *Пусть группа G действует без инверсий ребер на дереве X . Тогда существует естественный изоморфизм из группы G на группу $\pi_1(\mathbb{G}, Y, T)$, определенную в пункте 18.4. Этот изоморфизм продолжает тождественные изоморфизмы $\text{St}_G(\tilde{v}) \rightarrow G_v$ ($v \in Y^0$) и переводит t_e в t_e ($e \in Y^1 - T^1$).*

Доказательство аналогично доказательству теоремы 12.3 (см. также теорему 15.2).

18.6. Замечание. Пусть (\mathbb{G}, Y) — граф групп и X — дерево, построенное по нему в доказательстве теоремы 18.2. Любая подгруппа H фундаментальной группы $\pi_1(\mathbb{G}, Y, T)$ действует на X и по теореме 18.5 сама является фундаментальной группой некоторого графа групп. Мы не будем уточнять строение H в общем случае. Разберем лишь пример 18.7 и докажем теорему Куроша, относящуюся к частному случаю графов групп.

18.7. Пример. Пусть φ — гомоморфизм из группы трилистника $G = \langle a, b \mid a^2 = b^3 \rangle$ в группу S_3 , заданный правилом $a \mapsto (12)$, $b \mapsto (123)$. Найдем представление его ядра H в виде фундаментальной группы некоторого графа групп.

Сама группа G является фундаментальной группой сегмента групп $\langle b \rangle \langle b^3 \rangle = \langle a^2 \rangle \langle a \rangle$. Часть соответствующего дерева X изображена на рис. 19 слева. Вершинами этого дерева являются левые смежные классы группы G по подгруппам $\langle a \rangle$ и $\langle b \rangle$, положительно ориентированными ребрами — левые смежные классы группы G по подгруппе $\langle a^2 \rangle (= \langle b^3 \rangle)$. Вершины $g\langle b \rangle$ и $g\langle a \rangle$ соединяются положительно ориентированным ребром $g\langle a^2 \rangle$. Группа H действует на дереве X левыми умножениями и соответствующий фактор-граф Y изображен на рис. 19 справа.

Действительно, так как $\{1, b, b^2, a, ba, b^2a\}$ — система представителей смежных классов G по H , то любая вершина вида $g\langle a \rangle$ H -эквивалентна вершине $\langle a \rangle$, $b\langle a \rangle$ или $b^2\langle a \rangle$, а сами эти вершины не H -эквивалентны. Аналогично, так как $\{1, b, b^2, a, ab, ab^2\}$ — тоже система представителей смежных классов G по H , то любая вершина вида $g\langle b \rangle$ H -эквивалентна вершине $\langle b \rangle$ или $a\langle b \rangle$, а сами эти вершины не H -эквивалентны. Поэтому мы имеем 5 классов эквивалентности A, D, E, B, C вершин дерева X . Их представителями являются вершины $\langle a \rangle, b\langle a \rangle, b^2\langle a \rangle, \langle b \rangle, a\langle b \rangle$.

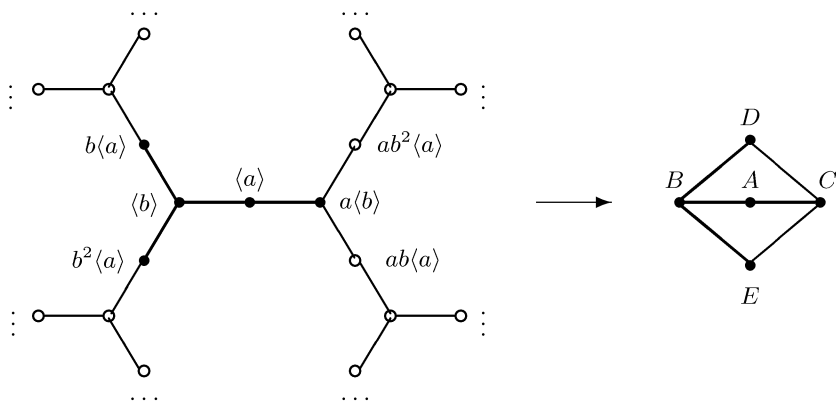


Рис. 19

Легко понять также, что имеется ровно 6 классов эквивалентности положительно ориентированных ребер дерева X . Их представителями являются положительно ориентированные ребра, входящие в минимальное поддерево \tilde{Y} , содержащее вершины $b\langle a \rangle, b^2\langle a \rangle, ab\langle a \rangle, ab^2\langle a \rangle$.

Вершины $b\langle a \rangle$ и $ab^2\langle a \rangle$ H -эквивалентны, так как $ab^2a^{-1}b^{-1} \cdot b\langle a \rangle = ab^2\langle a \rangle$ и $ab^2a^{-1}b^{-1} \in H$. Поэтому они проецируются в одну вершину D . Аналогично вершины $b^2\langle a \rangle$ и $ab\langle a \rangle$ проецируются в одну вершину E .

Пусть T — максимальное поддереву графа Y , в которое входят все его вершины и ребра, кроме ребер CD , CE и обратных к ним. В качестве его поднятия \tilde{T} в дереве X выберем минимальное поддереву, содержащее вершины $b\langle a \rangle$, $b^2\langle a \rangle$ и $a\langle b \rangle$. Тогда (\tilde{T}, \tilde{Y}) — поднятие пары (T, Y) . Легко подсчитать, что стабилизаторы всех вершин дерева \tilde{T} и всех ребер дерева \tilde{Y} в группе H равны $\langle a^2 \rangle$. Поэтому каждой вершине и ребру графа Y надо сопоставить группу $\langle a^2 \rangle$. Все вложения реберных групп в соответствующие вершинные группы тождественные, так как $\langle a^2 \rangle$ — центр группы G .

Итак, мы построили граф групп (\mathbb{H}, Y) , фундаментальная группа которого относительно максимального поддереву T изоморфна H . Отсюда выводим, что H имеет представление

$$\langle x, t_1, t_2 \mid t_1^{-1}xt_1 = x, t_2^{-1}xt_2 = x \rangle,$$

в котором элементы x, t_1, t_2 соответствуют элементам $a^2, ab^2a^{-1}b^{-1}, aba^{-1}b^{-2}$. Элементы $ab^2a^{-1}b^{-1}$ и $aba^{-1}b^{-2}$ переводят, соответственно, вершины $b\langle a \rangle$ и $b^2\langle a \rangle$ дерева \tilde{T} в вершины $ab^2\langle a \rangle$ и $ab\langle a \rangle$ дерева \tilde{Y} .

§ 19. Теорема Куроша

Теорема Куроша является частным случаем следующей теоремы при $A = \{1\}$.

19.1. Теорема. Пусть H — свободное произведение групп H_i ($i \in I$), амальгамированных по общей подгруппе¹¹ A . Пусть G — такая подгруппа группы H , что $G \cap xAx^{-1} = \{1\}$ для любого $x \in H$. Тогда существует свободная группа F и системы представителей X_i двойных смежных классов $G \setminus H/H_i$ такие, что G является свободным произведением группы F и групп $G \cap xH_ix^{-1}$ по всем $i \in I, x \in X_i$.

Доказательство. Пусть X — дерево, на котором действует фундаментальная группа H , построенное как в доказательстве теоремы 18.2. Имеем $X^0 = H/A \cup (\cup_{i \in I} H/H_i)$, $X^1_+ = \cup_{i \in I} (H/A \times \{i\})$. Началом ребра (hA, i) является вершина hA , концом — вершина hH_i . Группа G действует на этом дереве левыми умножениями. Для того, чтобы понять строение группы G , воспользуемся пунктами 18.4 и 18.5.

¹¹Иными словами, H — фундаментальная группа графа групп, изображенного на рис. 20. Вложения реберных групп A в вершинную группу A тождественные.

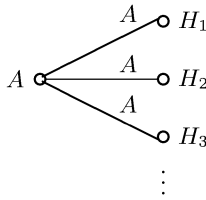


Рис. 20

Пусть $Y = G \backslash X$ — фактор-граф, T — некоторое его максимальное поддереву, $p : X \rightarrow Y$ — каноническая проекция и (\tilde{T}, \tilde{Y}) — любое поднятие пары (T, Y) в дерево X .

Множество вершин дерева \tilde{T} является максимальным множеством левых смежных классов xA и xH_i ($i \in I$), не эквивалентных относительно действия группы G . Таким образом, существуют системы представителей X_A и X_i двойных смежных классов $G \backslash H/A$ и $G \backslash H/H_i$ такие, что $\tilde{T}^0 = \{xA \mid x \in X_A\} \cup \bigcup_{i \in I} \{xH_i \mid x \in X_i\}$.

Стабилизатор в G вершины вида xA равен $G \cap xAx^{-1} = \{1\}$. Стабилизатор в G вершины вида xH_i равен $G \cap xH_i x^{-1}$. Стабилизатор в G любого ребра графа X единичен, так как ребра имеют вид xA . Теперь утверждение теоремы следует из пунктов 18.4 и 18.5.

Для каждого ребра $\tilde{e} \in \tilde{Y}^1$ с концом вне \tilde{T}^0 выберем элемент $t_e^{-1} \in G$, переводящий этот конец в \tilde{T}^0 . Тогда F имеет базис, состоящий из всех таких элементов t_e .

19.2. Упражнение. Рассмотрим гомоморфизм $SL_2(\mathbb{Z}) = Z_4 *_{Z_2} Z_6 \rightarrow Z_{12}$, заданный естественными вложениями множителей в группу Z_{12} . Докажите, что его ядро является свободной группой ранга 2.

19.3. Замечание. С помощью теории концов групп Столлингс доказал следующую теорему: группа G является фундаментальной группой конечного графа конечных групп¹² тогда и только тогда, когда в ней есть свободная подгруппа конечного индекса и конечного ранга (см. [56, 62]).

§ 20. Накрытия графов

20.1. Определение. Морфизм графов $f : X \rightarrow Y$ называется *накрытием*, если f отображает множество вершин и множество ребер графа X на множество вершин и множество ребер графа Y так, что

¹²Это означает, что граф конечен и вершинные группы тоже конечны.

звезда любой вершины $v \in X^0$ отображается биективно на звезду вершины $f(v)$.

Слоем в X называется полный прообраз любой вершины или ребра из Y .

20.2. Примеры. 1) Для каждого целого $n \geq 1$ существует накрытие из графа C_∞ в граф C_n (эти графы определены в § 1).

2) Существуют накрытия из графов, изображенных на рис. 12, 22 и 38, на граф, изображенный на рис. 21.

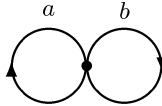


Рис. 21

3) Пусть $\Gamma(G, S)$ — граф Кэли группы G относительно порождающего множества S . Любая подгруппа H группы G действует левым умножением на $\Gamma(G, S)$. Фактор-отображение $\Gamma(G, S) \rightarrow H \backslash \Gamma(G, S)$ является накрытием. Граф $\{1\} \backslash \Gamma(G, S)$ совпадает с $\Gamma(G, S)$, граф $\mathcal{R}(S) = G \backslash \Gamma(G, S)$ имеет одну вершину и $|S|$ пар взаимно обратных ребер.

Пусть $f : X \rightarrow Y$ — накрытие графов и p — путь в Y . *Поднятием* пути p называется любой путь l в X такой, что $f(l) = p$.

20.3. Упражнение. Пусть $f : X \rightarrow Y$ — накрытие. Тогда выполняются следующие утверждения.

1) Для любого пути p в графе Y и любой вершины v графа X , отображающейся в начало p , существует единственное поднятие пути p , имеющее начало в v .

2) Если пути l_1 и l_2 в X гомотопны, то их проекции $f(l_1)$ и $f(l_2)$ гомотопны. Наоборот, если пути p_1 и p_2 в Y гомотопны, то их поднятия в X , имеющие общее начало, гомотопны. В частности, эти поднятия имеют общий конец.

Напомним некоторые обозначения из § 4. Пусть Y — связный граф с выделенной вершиной y , T — максимальное поддерево в Y . Для каждой вершины v графа Y существует единственный путь без возвращений из y в v , проходящий в T . Обозначим этот путь через p_v . Тогда для любого ребра $e \in Y^1$ определен путь $p_e = p_{\alpha(e)} e p_{\omega(e)}^{-1}$. В § 4 доказано, что $\pi_1(Y, y)$ — свободная группа с базисом $\{[p_e] \mid e \in Y_+^1 - T^1\}$, где Y_+^1 — некоторая (произвольная) ориентация графа Y .

Пусть X и Y — связные графы, $f : (X, x) \rightarrow (Y, y)$ — морфизм. Согласно упражнению 4.4 отображение $f_* : \pi_1(X, x) \rightarrow \pi_1(Y, y)$, заданное правилом $f_*([l]) = [f(l)]$, является гомоморфизмом.

20.4. Упражнение. Пусть X и Y — связные графы, $f : (X, x) \rightarrow (Y, y)$ — накрытие. Если p — путь в Y , гомотопический класс которого лежит в $f_*(\pi_1(X, x))$, то его поднятие l с началом в x замкнуто.

Мы говорим, что накрытие $f : (X, x) \rightarrow (Y, y)$ соответствует подгруппе H группы $\pi_1(Y, y)$, если $f_*(\pi_1(X, x)) = H$.

20.5. Теорема. В следующих утверждениях мы предполагаем, что все графы связны.

1) Если $f : (X, x) \rightarrow (Y, y)$ — накрытие, то гомоморфизм $f_* : \pi_1(X, x) \rightarrow \pi_1(Y, y)$ является вложением.

2) Для каждой подгруппы $H \leq \pi_1(Y, y)$ существует накрытие $f : (X, x) \rightarrow (Y, y)$ такое, что $f_*(\pi_1(X, x)) = H$.

3) Пусть $f_1 : (X_1, x_1) \rightarrow (Y, y)$ и $f_2 : (X_2, x_2) \rightarrow (Y, y)$ — накрытия такие, что $f_{1*}(\pi_1(X_1, x_1)) = f_{2*}(\pi_1(X_2, x_2)) = H$. Тогда существует изоморфизм $p : (X_1, x_1) \rightarrow (X_2, x_2)$ такой, что $f_1 = f_2 p$.

3') Пусть $f_1 : (X_1, x_1) \rightarrow (Y, y)$ и $f_2 : (X_2, x_2) \rightarrow (Y, y)$ — накрытия такие, что $f_{1*}(\pi_1(X_1, x_1)) \leq f_{2*}(\pi_1(X_2, x_2))$. Тогда существует накрытие $p : (X_1, x_1) \rightarrow (X_2, x_2)$ такое, что $f_1 = f_2 p$.

4) Пусть $f : (X, x) \rightarrow (Y, y)$ — накрытие. Граф X является деревом тогда и только тогда, когда $f_*(\pi_1(X, x)) = \{1\}$. Если X — дерево, то группа $\pi_1(Y, y)$ действует на нем свободно и фактор-граф изоморфен графу Y .

5) Пусть H — нормальная подгруппа группы $\pi_1(Y, y)$ и $f : (X, x) \rightarrow (Y, y)$ — накрытие, соответствующее H . Тогда фактор-группа $\pi_1(Y, y)/H$ действует на X свободно, орбиты этого действия — слои, и фактор-граф по этому действию изоморфен Y .

Доказательство. 1) Обозначим через 1_x и 1_y вырожденные пути в X и Y с началами в x и y . Пусть $[l] \in \pi_1(X, x)$ и предположим, что $f_*([l]) = [1_y]$. Тогда пути $f(l)$ и 1_y гомотопны. По упражнению 20.3 их поднятия l и 1_x гомотопны, следовательно $[l] = 1$.

2) Пусть $\{t_i \mid i \in I\}$ — система представителей правых смежных классов группы $\pi_1(Y, y)$ по подгруппе H , причем представитель H равен t_1 , где $t_1 = 1$. Положим $X^0 = \{(v, i) \mid v \in Y^0, i \in I\}$, $X^1 = \{(e, i) \mid e \in Y^1, i \in I\}$, $\alpha((e, i)) = (\alpha(e), i)$, $\omega((e, i)) = (\omega(e), j)$, где индекс j такой, что $Ht_j = Ht_i[p_e]$, и положим $(\bar{e}, i) = (\bar{e}, j)$. Выделим в графе X вершину $x = (y, 1)$ и определим отображение $f : X \rightarrow Y$ по правилу $f((v, i)) = v$, $f((e, i)) = e$, $v \in X^0$, $e \in X^1$. Очевидно, f — накрытие.

Докажем, что граф X связан. Выберем в Y максимальное поддереве T . Пусть $(T_i)_{i \in I}$ — система подграфов графа X , каждый T_i состоит

из вершин и ребер, первая компонента которых лежит в T , вторая равна i . Легко понять, что каждый граф T_i изоморфен T и, значит, связан. Ясно также, что $\bigcup_{i \in I} T_i^0 = X^0$. Поэтому достаточно доказать, что для любых $i, j \in I$ графы T_i и T_j соединены путем в X . Пусть $g = e_1 \dots e_s$ — путь в Y с началом и концом y такой, что $Ht_i[g] = Ht_j$. Тогда $[g] = [p_{e_1}] \dots [p_{e_s}]$. Определим последовательность $(i_1, i_2, \dots, i_{s+1})$ правилами $i_1 = i$, $Ht_{i_{k+1}} = Ht_{i_k}[p_{e_k}]$, $1 \leq k \leq s$. Тогда $i_{s+1} = j$ и путь $(e_1, i_1) \dots (e_s, i_s)$ соединяет вершины $(y, i) \in T_i$ и $(y, j) \in T_j$. Итак, граф X связан и $f : X \rightarrow Y$ — накрытие.

Заметим, что произвольный путь $(e_1, 1)(e_2, i_2) \dots (e_s, i_s)$ в X с началом в вершине $x = (y, 1)$ замкнут тогда и только тогда, когда путь $g = e_1 e_2 \dots e_s$ в Y с началом y замкнут и $H \cdot 1 \cdot [p_{e_1}] \dots [p_{e_s}] = H \cdot 1$, то есть $[g] \in H$. Поэтому $f_*(\pi_1(X, x)) = H$.

3) Определим отображение $p : X_1 \rightarrow X_2$ следующим образом. Пусть x — произвольная вершина (ребро) графа X_1 . Выберем произвольный путь l_1 в X_1 с начальной вершиной x_1 и конечной вершиной (ребром) x . По упражнению 20.3.1 существует единственный путь l_2 в X_2 с началом x_2 такой, что $f_1(l_1) = f_2(l_2)$. Положим $p(x)$ равным конечной вершине (ребру) пути l_2 .

Докажем, что это определение не зависит от выбора пути l_1 . Достаточно разобрать случай, когда x — вершина. Пусть l'_1 — другой путь в X_1 с начальной вершиной x_1 и конечной вершиной x . Пусть l'_2 — путь в X_2 с началом x_2 такой, что $f_1(l'_1) = f_2(l'_2)$.

Скажем, что пути a и b отличаются на путь c , если путь ca гомотопен пути b . Так как l_1 и l'_1 отличаются на замкнутый путь, то $f_1(l_1)$ и $f_1(l'_1)$ отличаются на путь, гомотопический класс которого лежит в H . По упражнению 20.4 поднятия l_2 и l'_2 этих путей в X_2 тоже отличаются на замкнутый путь. В частности, конечные вершины путей l_2 и l'_2 совпадают.

Из определения следует, что $p : X_1 \rightarrow X_2$ — морфизм и $f_1 = f_2 p$. Аналогично можно определить морфизм $q : X_2 \rightarrow X_1$. Так как $qp = id|_{X_1}$ и $pq = id|_{X_2}$, то p — изоморфизм.

Утверждение 3') доказывается аналогично.

4) Так как f_* — вложение, то условие $f_*(\pi_1(X, x)) = \{1\}$ равносильно условию $\pi_1(X, x) = \{1\}$. Последнее означает, что в X нет циклов. Оставшееся утверждение вытекает из утверждения 5.

5) Ввиду утверждения 3 считаем, что граф X определен как в доказательстве утверждения 2. Тогда левое действие группы $\pi_1(Y, y)/H$ на X можно задать следующим образом. Пусть (u, i) — вершина или ребро графа X , Hg — смежный класс H в $\pi_1(Y, y)$. Скажем, что Hg переводит (u, i) в (u, j) , если $Ht_j = Hgt_i$. Доказательство того, что это

действие обладает нужными свойствами несложно и мы оставляем его читателю.

20.6. Следствие. Пусть X и Y — связные графы и $f : X \rightarrow Y$ — накрытие. Тогда мощность прообраза любой вершины или ребра из Y равна индексу подгруппы $f_*(\pi_1(X, x))$ в группе $\pi_1(Y, f(x))$.

Эта мощность называется кратностью накрытия f .

Доказательство следует из конструкции накрытия в доказательстве утверждения 2 с учетом утверждений 1 и 3 теоремы 20.5.

С помощью накрытий легко доказывается теорема Нильсена — Шрайера о подгруппах свободных групп.

20.7. Теорема. Любая подгруппа свободной группы свободна. Если G — свободная группа конечного ранга и H — ее подгруппа конечного индекса n , то

$$rk(H) - 1 = n(rk(G) - 1).$$

Доказательство. Пусть G — свободная группа, H — ее подгруппа. Отождествим G с группой $\pi_1(Y, y)$, где Y — граф с единственной вершиной y и $rk(G)$ положительно ориентированными ребрами. По теореме 20.5 существует накрытие $f : (X, x) \rightarrow (Y, y)$ такое, что вложение f_* отождествляет группу $\pi_1(X, x)$ с группой H . По теореме 4.3 группа $\pi_1(X, x)$ свободна.

Если $|G : H| = n$, то кратность накрытия f равна n и, следовательно, $|X^0| = n$, $|X^1_+| = n \cdot rk(G)$. Из теоремы 4.3 и упражнения 1.7 (при условии конечности $rk(G)$ и n) вытекает, что $\pi_1(X, x)$ — свободная группа ранга $n \cdot rk(G) - n + 1$.

§ 21. S -графы и перечисление подгрупп свободных групп

Пусть S — фиксированное множество и $F(S)$ — свободная группа с базисом S .

Разметкой ребер произвольного графа X назовем любое отображение $s : X^1 \rightarrow S \cup S^{-1}$ такое, что $s(\bar{e}) = (s(e))^{-1}$ при $e \in X^1$. Меткой пути $l = e_1 \dots e_k$ в графе X назовем произведение $s(l) = s(e_1) \dots s(e_k)$ в $F(S)$. Меткой вырожденного пути считаем единицу. Заметим, что если произведение путей l_1 и l_2 определено, то $s(l_1 l_2) = s(l_1) s(l_2)$. Так как метки гомотопных путей совпадают, то (для связного X) отображение $s : \pi_1(X, x) \rightarrow F(S)$, заданное правилом $[p] \mapsto s(p)$, корректно определено и является гомоморфизмом. Здесь p — произвольный путь в X с началом и концом в x , $[p]$ — его гомотопический класс. Группу $s(\pi_1(X, x))$ назовем s -фундаментальной группой графа X .

Наша ближайшая цель — определить такой класс размеченных графов, для которых гомоморфизм s будет взаимно однозначен.

21.1. Определение. *Связный граф X с выделенной вершиной x назовем S -графом, если задана разметка его ребер $s: X^1 \rightarrow S \cup S^{-1}$, отображающая звезду любой его вершины биективно на $S \cup S^{-1}$.*

Простейшим примером S -графа является граф $\mathcal{R}(S)$, состоящий из одной вершины v и $|S|$ пар взаимно обратных ребер, с фиксированной биективной разметкой $\mathcal{R}(S)^1 \rightarrow S \cup S^{-1}$. Очевидно, его s -фундаментальная группа совпадает с $F(S)$. Другие примеры S -графов получаются из накрытий $f: (X, x) \rightarrow (\mathcal{R}(S), v)$, где X — связный граф, если пометить каждое ребро e графа X той буквой, которой помечено ребро $f(e)$. Легко понять, что всякий S -граф получается таким образом.

21.2. Предложение. *Пусть X — S -граф с выделенной вершиной x и разметкой s . Тогда гомоморфизм $s: \pi_1(X, x) \rightarrow F(S)$, заданный правилом $[p] \mapsto s(p)$, взаимно однозначен.*

Доказательство. Любой неединичный гомотопический класс из $\pi_1(X, x)$ содержит невырожденный путь без возвращений, а метка такого пути неединична.

Таким образом, s -фундаментальная группа S -графа (X, x) свободна и имеет базис $\{s(p_e) \mid e \in X_+^1 - T^1\}$ по теореме 4.3.

Скажем, что два S -графа S -изоморфны, если существует изоморфизм из одного графа в другой, переводящий выделенную вершину в выделенную и сохраняющий метки ребер. Из теоремы 20.5 и следствия 20.6 вытекает следующее предложение.

21.3. Предложение. *1) Для каждой подгруппы H группы $F(S)$ существует единственный с точностью до S -изоморфизма S -граф¹³ с s -фундаментальной группой, равной H .*

2) Индекс H в $F(S)$ равен числу вершин S -графа, соответствующего H .

21.4. Теорема (М. Холл). *Число подгрупп данного конечного индекса n в конечно порожденной группе G конечно.*

Доказательство. Так как группа G конечно порождена, то существует свободная группа $F(S)$ конечного ранга и эпиморфизм $\theta: F(S) \rightarrow G$. Прообразы разных подгрупп индекса n в G относительно θ различны и имеют индекс n в $F(S)$. Количество же подгрупп индекса n в группе $F(S)$ равно числу классов S -изоморфности S -графов с n вершинами и потому конечно.

¹³Такой S -граф назовем *соответствующим* подгруппе H .

21.5. Пример. В группе $F(a, b)$ имеются ровно три подгруппы индекса 2:

$$\langle ba^{-1}, a^2, ab \rangle, \langle a, b^2, bab^{-1} \rangle, \langle b, a^2, aba^{-1} \rangle.$$

Они соответствуют S -графам, изображенным на рис. 22.

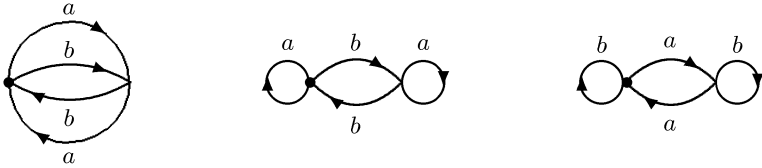


Рис. 22

21.6. Упражнение. Найдите базисы всех 13 подгрупп индекса 3 в группе $F(a, b)$.

§ 22. Фолдинги

Пусть $F(S)$ — свободная группа с базисом S и пусть H — ее подгруппа, порожденная словами h_1, \dots, h_n в алфавите $S \cup S^{-1}$. Объясним, как построить S -граф, соответствующий H (см. предложение 21.3).

Пусть Γ_0 — граф с одной вершиной x и n петлями. Разделим i -ю петлю на столько сегментов, какова длина слова h_i ($i = 1, \dots, n$). Каждый сегмент ориентируем и пометим буквой из $S \cup S^{-1}$ так, чтобы вдоль i -й петли читалось слово h_i . Таким образом, получится граф Γ_1 с разметкой, s -фундаментальная группа которого относительно x равна H . Однако, граф Γ_1 может не быть S -графом, в частности, по той причине, что из некоторой его вершины могут выходить два ребра с одинаковыми метками. Если это случится для некоторой пары ребер, то мы отождествим их в одно ребро с той же меткой. Такая операция называется *фолдингом*. Фолдинг не изменяет s -фундаментальную группу, но уменьшает число ребер в графе. Пусть Γ_2 — граф, полученный из графа Γ_1 последовательным применением фолдингов пока это возможно. Граф Γ_2 все еще может не быть S -графом по той причине, что из некоторой его вершины не выходит ребро с меткой s для некоторого $s \in S \cup S^{-1}$. В таком случае приклеим к этой вершине подходящее бесконечное поддерево из графа Кэли $\Gamma(S)$ (см. пример 22.1). Такая подклейка тоже не изменяет s -фундаментальную группу. Осуществляя все такие подклейки (их число конечно, если множество S конечно), получим искомый S -граф, соответствующий подгруппе H .

22.1. Пример. На рис. 23 изображена процедура построения S -графа, соответствующего подгруппе $\langle a^2, aba^{-1} \rangle$ группы $F(a, b)$.

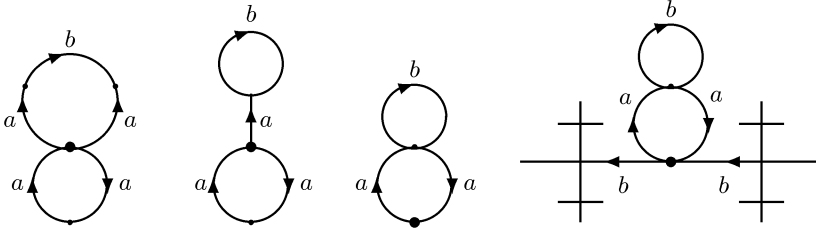


Рис. 23

22.2. Лемма. Пусть N — нормальная подгруппа свободной группы $F(S)$ и (X, x) — соответствующий ей S -граф. Тогда группа автоморфизмов графа X , сохраняющих метки ребер, действует транзитивно на множестве его вершин. Эта группа изоморфна группе $F(S)/N$.

Доказательство. Пусть $f : (X, x) \rightarrow (\mathcal{R}(S), v)$ — накрытие, соответствующее подгруппе N группы $F(S)$ и сохраняющее метки ребер. По утверждению 5 теоремы 20.5 фактор-группа $F(S)/N$ действует на X свободно, орбиты этого действия — слои, и фактор-граф по этому действию изоморфен $\mathcal{R}(S)$. Так как граф $\mathcal{R}(S)$ имеет только одну вершину, то это действие транзитивно на X^0 . Метки ребер при этом действии сохраняются, так как орбиты этого действия — слои. Последнее утверждение леммы следует из того, что автоморфизм S -графа X , сохраняющий метки его ребер и фиксирующий некоторую его вершину, тождествен.

Приведем еще одно доказательство транзитивности, не опирающееся на теорему 20.5. Пусть v — произвольная вершина графа X и l — некоторый путь из x в v . Построим автоморфизм φ графа X , сохраняющий метки его ребер и переводящий x в v .

Пусть w — произвольная вершина графа X . Выберем произвольный путь g из x в w . Так как X — S -граф, то существует единственный путь g' с началом в v и меткой, равной метке пути g . Положим $\varphi(w)$ равным конечной вершине пути g' .

Докажем, что это определение не зависит от выбора пути g . Пусть g_1 — другой путь из x в w . Через g'_1 обозначим путь с началом в v и меткой, равной метке пути g_1 . Тогда

$$s(lg') = s(l)s(g) = s(l) \cdot s(gg_1^{-1}) \cdot s(l)^{-1} \cdot s(l)s(g_1).$$

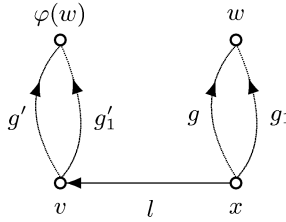


Рис. 24

Так как $s(gg_1^{-1}) \in N$ и $N \trianglelefteq F(S)$, то $s(l) \cdot s(gg_1^{-1}) \cdot s(l)^{-1} = s(n)$ для некоторого замкнутого пути n с началом в x . Тогда $s(lg') = s(n)s(l)s(g'_1) = s(nlg'_1)$. Так как метки путей lg' и nlg'_1 и их начала совпадают, то и концы этих путей совпадают. Поэтому концы путей g' и g'_1 тоже совпадают.

Если e — ребро графа X , то положим $\varphi(e)$ равным ребру с началом в $\varphi(\alpha(e))$ и с меткой, равной метке ребра e . Нетрудно понять, что φ является автоморфизмом графа X и $\varphi(x) = v$.

22.3. Определение. *Ядром связного графа X относительно его вершины x называется наименьший подграф, содержащий все пути без возвращения из x в x .*

Обозначим это ядро через $C(X, x)$. Очевидно, тождественное вложение $C(X, x)$ в X индуцирует изоморфизм групп $\pi_1(C(X, x), x)$ и $\pi_1(X, x)$. Следующее упражнение показывает, что для получения ядра графа надо выкинуть из него «лишние» поддеревья.

22.4. Упражнение. *Ядро $C(X, x)$ совпадает с наименьшим подграфом C графа X , содержащим x , для которого существует такое множество $\{T_i \mid i \in I\}$ попарно непересекающихся поддеревьев, что $X = C \cup (\bigcup_{i \in I} T_i)$ и $C \cap T_i$ — вершина, зависящая от i .*

22.5. Теорема. *Если $F(S)$ — свободная группа конечного ранга и N — ее неединичная подгруппа, то индекс N в $F(S)$ конечен тогда и только тогда, когда группа N конечно порождена.*

Доказательство. В одну сторону утверждение вытекает из следствия 9.2.

Предположим, что $\{1\} \neq N \trianglelefteq F(S)$ и группа N конечно порождена. Пусть (X, x) — S -граф, соответствующий группе N . Так как N конечно порождена и неединична, то ядро $C(X, x)$ этого графа конечно и содержит цикл. По лемме 22.2 деревья, фигурирующие в упражнении 22.4, отсутствуют, и, значит, $X = C(X, x)$. Индекс подгруппы N в группе $F(S)$ равен числу вершин графа X .

Будем говорить, что подгруппа H группы L выделяется в L свободным множителем, если существует такая подгруппа M в L , что $H * M = L$.

22.6. Определение. Говорят, что группа G обладает *свойством М. Холла*, если любая ее конечно порожденная подгруппа H выделяется свободным множителем в некоторой подгруппе L конечного индекса в G .

22.7. Теорема. *Свободная группа конечного ранга обладает свойством М. Холла.*

Доказательство. Пусть F — свободная группа с конечным базисом S , H — ее конечно порожденная подгруппа и (X, x) — S -граф, соответствующий подгруппе H . Ядро $C = C(X, x)$ этого графа конечно, так как группа H конечно порождена. Покажем, что граф C вкладывается с сохранением меток ребер в некоторый конечный S -граф (C_1, x) .

Любое ребро с меткой s назовем s -ребром. Для каждого s -ребра e_1 с началом вне C и концом в C существует единственный путь $e_1 e_2 \dots e_k$ такой, что $e_2, \dots, e_{k-1} \in C^1$, конец ребра e_k лежит вне C и метки всех e_i равны s . Действительно, войдя в некоторую вершину графа C , можно только по одному s -ребру выйти из нее. Зацикливаний не происходит (т.е. вершины $\alpha(e_1), \alpha(e_2), \dots$ не повторяются), поскольку в каждую вершину входит только одно s -ребро. Так как C конечен, то за конечное число шагов мы выйдем из C . Аналогично можно понять, что пути, соответствующие разным начальным ребрам, не имеют общих ребер, и что ребру \bar{e}_k соответствует путь $\bar{e}_k \bar{e}_{k-1} \dots \bar{e}_1$. Теперь замкнем начало и конец построенных путей (см. рис. 25). Формально заменим каждую пару соответствующих ребер e_1, e_k одним ребром e таким, что $\alpha(e) = \alpha(e_k)$, $\omega(e) = \omega(e_1)$, и пометим это ребро меткой s . При этом считаем, что пара \bar{e}_k, \bar{e}_1 заменяется ребром \bar{e} .

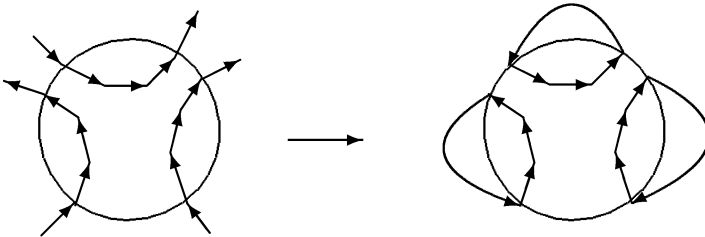


Рис. 25

В результате получим конечный S -граф (C_1, x) , содержащий ядро (C, x) . Тогда в качестве L можно взять группу $s(\pi_1(C_1, x))$. Действительно, любое максимальное поддерево графа C является максимальным поддеревом графа C_1 . Согласно теореме 4.3 это означает, что некоторый базис группы $H = s(\pi_1(C, x))$ включается в подходящий базис группы $s(\pi_1(C_1, x))$. Группа $s(\pi_1(C_1, x))$ имеет конечный индекс в $F(S)$ по предложению 21.3.

22.8. Упражнение. Найдите базис некоторой подгруппы конечного индекса свободной группы $F(a, b)$, содержащей подгруппу $\langle a^2, aba^{-1} \rangle$ в качестве свободного множителя.

22.9. Упражнение. Выведите теорему 22.5 из теоремы 22.7.

Следующая теорема характеризует конечно порожденные группы со свойством М. Холла. Ее первая часть вытекает из статьи Данвуди [44], вторая часть доказана Богопольским в [6].

22.10. Теорема.

1) Конечно порожденная группа со свойством М. Холла изоморфна фундаментальной группе конечного графа конечных групп.

2) Фундаментальная группа G конечного графа конечных групп обладает свойством М. Холла тогда и только тогда, когда каждая подгруппа любой ее вершинной группы выделяется свободным множителем в некоторой подгруппе конечного индекса группы G . Последнее можно проверить алгоритмически.

§ 23. Пересечение двух подгрупп свободной группы

В этом параграфе мы научимся находить базис пересечения двух подгрупп свободной группы по базисам этих подгрупп.

23.1. Теорема. Пусть G и H — две подгруппы свободной группы $F(S)$ и пусть (X, x) и (Y, y) — S -графы с s -фундаментальными группами G и H соответственно. Определим новый размеченный граф (Z, z) правилами: $Z^0 = X^0 \times Y^0$, $z = (x, y)$,

$$Z^1 = \{(e, e') \mid (e, e') \in X^1 \times Y^1, s(e) = s(e')\},$$

$$\alpha((e, e')) = (\alpha(e), \alpha(e')), \quad \omega((e, e')) = (\omega(e), \omega(e')), \quad \overline{(e, e')} = (\bar{e}, \bar{e}'), \\ s((e, e')) = s(e) \text{ при } (e, e') \in Z^1.$$

Пусть \tilde{Z} — компонента связности графа Z , содержащая вершину z . Тогда (\tilde{Z}, z) — S -граф с s -фундаментальной группой $G \cap H$.

Доказательство. Очевидно, (\tilde{Z}, z) является S -графом. Пусть $p = (e_1, e'_1)(e_2, e'_2) \dots (e_k, e'_k)$ — произвольный замкнутый путь в графе \tilde{Z} с началом в вершине z . Тогда $e_1 e_2 \dots e_k$ и $e'_1 e'_2 \dots e'_k$ — замкнутые пути в графах X и Y с началами x и y соответственно. Их метки равны $s(p)$. Поэтому $s(p) \in G \cap H$. Наоборот, если g — произвольный элемент из $G \cap H$, то существует замкнутый путь p в графе \tilde{Z} с началом в вершине z , метка которого равна g . Теорема доказана.

23.2. Пример. Пересечение подгрупп $G = \langle ba^{-1}, a^2, ab \rangle$ и $H = \langle a, b^2, bab^{-1} \rangle$ свободной группы $F(a, b)$ имеет базис $\{a^2, b^2, ab^2a^{-1}, abab, baba\}$. В качестве S -графов, соответствующих группам G и H , можно взять первые два графа на рис. 22. Обозначим их вершины слева направо буквами x, x', y, y' . S -граф, соответствующий группе $G \cap H$, изображен на рис. 26.

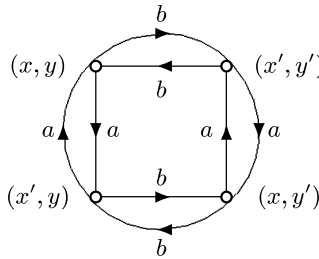


Рис. 26

23.3. Упражнение. Найдите базисы подгрупп индексов 2 и 3 в группе $F(a, b)$, пересекающихся по ядру гомоморфизма $\varphi: F(a, b) \rightarrow S_3$, заданного правилом $a \mapsto (12), b \mapsto (123)$.

Говорят, что группа G обладает свойством Хаусона, если пересечение любых двух ее конечно порожденных подгрупп конечно порождено.

23.4. Теорема. Любая свободная группа обладает свойством Хаусона.

Доказательство. Пусть F — свободная группа с базисом S , и пусть G, H — две ее конечно порожденные подгруппы. Можно считать, что базис S конечен, взяв вместо F группу $\langle G, H \rangle$. Заметим, что подгруппа группы F конечно порождена тогда и только тогда, когда ядро соответствующего ей S -графа конечно. Поэтому в обозначениях теоремы 23.1 достаточно доказать, что $C(\tilde{Z}, z)$ является подграфом графа $C(X, x) \times C(Y, y)$. Последнее вытекает из следующего рассуждения. Пусть $(e_1, e'_1) \dots (e_k, e'_k)$ — путь без возвратов в графе \tilde{Z} из z в z .

Тогда $s((e_i, e'_i)) \neq s(\overline{(e_{i+1}, e'_{i+1})})$ для $i = 1, \dots, k - 1$. Отсюда $s(e_i) \neq s(\overline{e_{i+1}})$ и $s(e'_i) \neq s(\overline{e'_{i+1}})$, и, значит, $e_1 \dots e_k$ и $e'_1 \dots e'_k$ — пути без возвращений из x в x и из y в y в графах X и Y соответственно.

Хана Нойман доказала следующую теорему.

23.5. Теорема. Пусть G и H — две конечно порожденные подгруппы свободной группы. Тогда

$$rk(G \cap H) - 1 \leq 2(rk(G) - 1)(rk(H) - 1).$$

До сих пор (2002 год) не решена *проблема Ханы Нойман*: можно ли убрать 2 в предыдущем неравенстве? Эта и многие другие проблемы комбинаторной и геометрической теории групп обсуждаются в [66].

Не все конечно порожденные группы обладают свойством Хаусона. Например, этим свойством не обладает группа $A \underset{A'=B'}{*} B$, где A и B — свободные группы рангов 2, A' и B' — их коммутанты. Оказывается, даже в классе групп с одним определяющим соотношением имеются группы, не обладающие свойством Хаусона.

23.6. Предложение. Группа $G = \langle a, b \mid a^{-1}b^2a = b^2 \rangle$ не обладает свойством Хаусона.

Доказательство. Положим $H = \langle a, b^{-1}ab \rangle$. Из нормальной формы элементов группы G , рассмотренной как HNN-расширение с базой $\langle b \rangle$, следует, что любое непустое приведенное слово от элементов $a, b^{-1}ab$ и обратных к ним неединично. Поэтому H — свободная группа ранга 2. Кроме того, $H \trianglelefteq G$, так как $bab^{-1} = b^{-1}(b^2ab^{-2})b = b^{-1}ab$. Аналогично $L = \langle ba, ab \rangle$ — свободная группа ранга 2 и $L \trianglelefteq G$. Поэтому подгруппа $H \cap L$ нормальна в H , неединична (так как $a^{-1}b^{-1}ab \in H \cap L$) и имеет бесконечный индекс в H (так как при эпиморфизме $G \rightarrow \mathbb{Z}$, заданном правилом $a \mapsto 1, b \mapsto -1$, образ H равен \mathbb{Z} , образ L равен $\{0\}$). По теореме 22.5 группа $H \cap L$ не конечно порождена.

23.7. Упражнение. Докажите, что группа $H \cap L$ является нормальным замыканием в H элемента $a^{-1}b^{-1}ab$ и совпадает с коммутантом группы G .

23.8. Упражнение. Обладает ли свойством Хаусона группа $G = \langle a, b \mid a^{-1}b^2a = b^3 \rangle$?

§ 24. КОМПЛЕКСЫ

Термины *граф* и *одномерный комплекс* — синонимы. *Циклическим путем* в графе называется любая циклически упорядоченная последовательность его ребер $e_1e_2 \dots e_n$ такая, что $\omega(e_i) = \alpha(e_{i+1})$ ($1 \leq i \leq n - 1$) и $\omega(e_n) = \alpha(e_1)$. Согласно этому определению циклические пути

$e_1e_2 \dots e_n$ и $e_2e_3 \dots e_n e_1$ равны. Скажем, что вершина v лежит на этом циклическом пути, если v является началом некоторого его ребра. Число таких ребер назовем числом вхождений v в данный путь. Обратным к циклическому пути $e_1e_2 \dots e_n$ называется циклический путь $\overline{e_n e_{n-1} \dots e_1}$. Из контекста будет ясно, когда речь идет об обычном пути, и когда о циклическом.

24.1. Определение. *Двумерный комплекс* K состоит из одномерного комплекса $K^{(1)}$, множества K^2 *двумерных клеток*, или *граней*, и двух отображений ∂ и $\bar{}$, определенных на K^2 . Отображение ∂ сопоставляет двумерной клетке D некоторый циклический путь ∂D в $K^{(1)}$, называемый *границей* клетки D . Отображение $\bar{}$ сопоставляет клетке D клетку \overline{D} с условием, что циклический путь $\partial(\overline{D})$ является обратным к циклическому пути ∂D . При этом $\overline{\overline{D}} = D$ и $\overline{D} \neq D$.

Клетка \overline{D} называется *обратной* к клетке D . Через K^0 , K^1 , K^2 обозначим множество вершин, ребер и граней комплекса K . Естественным образом вводится понятие подкомплекса комплекса и морфизма из комплекса в комплекс. Путем в K называется любой путь в $K^{(1)}$. Комплекс K *связен*, если его подкомплекс $K^{(1)}$ связан.

Путь p в K называется *контурным путем для клетки* D , если его ребра, рассмотренные в циклическом порядке, образуют границу клетки D .

Пути p и q в K называются *элементарно гомотопными*, если для некоторого ребра e и путей s, t имеем $p = se\bar{e}t$, $q = st$ или $p = st$, $q = se\bar{e}t$, или $p = sr_1t$, $q = sr_2t$, где $r_1r_2^{-1}$ является контурным путем некоторой клетки.

Пути p и q в K называются *гомотопными в* K , если существует конечная последовательность путей p_1, p_2, \dots, p_s , в которой $p = p_1$, $q = p_s$ и соседние пути элементарно гомотопны. Класс путей, гомотопных пути p в K , обозначим через $[p]$. Напомним, что класс путей, гомотопных пути p в графе $K^{(1)}$, мы обозначаем через $[p]$. Очевидно, $[p] \subseteq [p]$.

Пусть теперь K — связный комплекс и x — его фиксированная вершина. Обозначим через $P(K, x)$ множество всех замкнутых путей в K с началом в x . Определим произведение классов путей из $P(K, x)$ формулой $[p] \cdot [q] = [pq]$.

24.2. Упражнение. *Докажите, что это произведение определено корректно, то есть не зависит от выбора представителей в классах.*

Легко проверить, что множество классов путей из $P(K, x)$ относительно такого произведения образует группу. Эта группа называется *фундаментальной группой комплекса K относительно вершины x* и обозначается $\pi_1(K, x)$.

24.3. Замечание. Фундаментальная группа подкомплекса не обязательно вкладывается в фундаментальную группу комплекса. Примером служит комплекс L , состоящий из одной вершины x , двух ребер e, \bar{e} и двух клеток D, \bar{D} таких, что $\partial D = e$. Очевидно, $\pi_1(L^{(1)}, x) = Z$, $\pi_1(L, x) = \{1\}$.

Имеется естественный эпиморфизм $\varphi : \pi_1(K^{(1)}, x) \rightarrow \pi_1(K, x)$, заданный правилом $[p] \mapsto [p]$. Группа $\pi_1(K^{(1)}, x)$ свободна (по теореме 4.3), поэтому достаточно изучить $\text{Ker } \varphi$.

Выберем максимальное поддерево T и ориентацию K_+^1 в $K^{(1)}$. Для каждой вершины v комплекса K существует единственный путь без возвращений из x в v , проходящий в T . Обозначим этот путь через p_v . Тогда для любого ребра $e \in K^1$ определен путь $p_e = p_{\alpha(e)} e p_{\omega(e)}^{-1}$. Заметим, что $[p_{\bar{e}}] = [p_e]^{-1}$. Пусть теперь D — произвольная двумерная клетка. Выберем некоторую вершину v на границе этой клетки и выберем¹⁴ контурный путь $\partial_v(D)$ для клетки D с началом в v . Положим $[p_D] = [p_v \partial_v(D) p_v^{-1}]$. Можно считать, что $[p_{\bar{D}}] = [p_D]^{-1}$. Напомним, что группа $\pi_1(K^{(1)}, x)$ свободна и элементы $[p_e]$ ($e \in K_+^1 - T^1$) образуют ее базис. Поэтому класс $[p_D]$ можно выразить в виде слова от этих элементов и обратным к ним: $[p_D] = [p_{c_1}] \cdots [p_{c_s}]$, где c_1, \dots, c_s — те ребра, которые останутся в $\partial_v(D)$ после вычеркивания ребер, входящих в T^1 . Обозначим это слово через r_D .

24.4. Теорема. Пусть K — связный комплекс, x — его вершина, T — максимальное поддерево в $K^{(1)}$ и K_+^1 — некоторая ориентация графа $K^{(1)}$. Тогда группа $\pi_1(K, x)$ имеет представление с множеством порождающих $\{[p_e] \mid e \in K_+^1 - T^1\}$ и множеством определяющих соотношений $\{r_D \mid D \in K^2\}$.

Доказательство. Достаточно доказать, что $\text{Ker } \varphi$ совпадает с нормальным замыканием N множества $\{[p_D] \mid D \in K^2\}$ в группе $\pi_1(K^{(1)}, x)$. Включение $N \subseteq \text{Ker } \varphi$ очевидно. Для доказательства обратного включения достаточно проверить, что если пути p и q из $P(K, x)$ элементарно гомотопны в K , то $[p]$ отличается от $[q]$ на элемент из N . Если $p = se\bar{e}t$, $q = st$, то $[p] = [q]$. Пусть $p = sr_1t$, $q = sr_2t$, где

¹⁴Таких путей может быть несколько, если ∂D «проходит через» v несколько раз.

$r_1 r_2^{-1}$ — контурный путь клетки D . Предположим, что на границе этой клетки выбиралась вершина v , $\partial_v(D) = e_1 e_2 \dots e_n$ и $r_1 r_2^{-1} = e_k \dots e_n e_1 \dots e_{k-1}$. Положим $f = e_1 e_2 \dots e_{k-1}$. Тогда $[p][q]^{-1} = [s r_1 r_2^{-1} s^{-1}] = [s f^{-1} p_v^{-1} \cdot p_v \partial_v(D) p_v^{-1} \cdot p_v f s^{-1}]$, т. е. элемент $[p][q]^{-1}$ сопряжен с $[p_D]$ и, значит, лежит в N .

24.5. Теорема. *Для всякой группы G существует двумерный комплекс K , фундаментальная группа которого изоморфна G .*

Доказательство. Построим комплекс K по некоторому представлению $\langle S | R \rangle$ группы G . Комплекс K имеет единственную вершину x , ребра e_s ($s \in S \cup S^{-1}$) и грани D_r и \overline{D}_r ($r \in R$). При этом считаем, что $\overline{e}_s = e_{s^{-1}}$. Если $r = s_1 s_2 \dots s_n$, где $s_i \in S \cup S^{-1}$, то положим $\partial D_r = e_{s_1} e_{s_2} \dots e_{s_n}$. Из теоремы 24.4 (или прямо из определения фундаментальной группы комплекса) следует, что $\pi_1(K, x) \cong G$.

Комплекс, построенный по представлению \mathcal{G} как в этом доказательстве, будет обозначаться $K(\mathcal{G})$.

§ 25. Накрытия комплексов

Звездой вершины v двумерного комплекса K называется система, состоящая из всех его ребер с началом в v и клеток, на границе которых лежит v , причем каждая клетка учитывается с кратностью, равной числу вхождений v в ее границу.

25.1. Определение. Морфизм двумерных комплексов $f : X \rightarrow Y$ называется *накрытием*, если f отображает множество вершин, ребер и клеток комплекса X на множество вершин, ребер и клеток комплекса Y так, что звезда любой вершины $v \in X^0$ отображается биективно на звезду вершины $f(v)$.

25.2. Замечание. Утверждения 1, 2, 3, 3' и 5 теоремы 20.5 остаются справедливыми, если в них заменить слово граф словом комплекс. Их доказательства проходят с небольшими изменениями и дополнениями. Например, в доказательстве утверждения 2 надо положить $X^2 = \{(D, i) \mid D \in Y^2, i \in I\}$. Для каждой клетки $D \in Y^2$ выберем ее контурный путь l_D . Тогда контурным путем клетки (D, i) объявим поднятие пути l_D с началом в вершине $(\alpha(l_D), i)$. Необходимо также заменить символы $[,]$ на символы $\left[, \right]$.

Справедливо также следующее обобщение следствия 20.6.

25.3. Следствие. Пусть X и Y — связные комплексы и $f : (X, x) \rightarrow (Y, y)$ — накрытие. Тогда мощность прообраза любой вершины, ребра или клетки из Y равна индексу подгруппы $f_*(\pi_1(X, x))$ в группе $\pi_1(Y, y)$.

Эта мощность называется *кратностью накрытия* f .

В примерах, приведенных ниже, говоря о том, что комплекс состоит из некоторых ребер и клеток, мы подразумеваем, что в него входят и обратные к описанным ребра и клетки. Мы отождествляем также группу с ее представлением.

25.4. Примеры. 1) Пусть $A = \langle a \mid a^2 = 1 \rangle$ и $B = \langle b \mid b^3 = 1 \rangle$ — циклические группы порядков 2 и 3. На рис. 27 изображены накрытия $f : \widetilde{K(A)} \rightarrow K(A)$ и $g : \widetilde{K(B)} \rightarrow K(B)$, соответствующие единичным подгруппам этих групп. Эти накрытия имеют кратности 2 и 3 соответственно. Комплекс $\widetilde{K(A)}$ имеет две пары взаимно обратных клеток, изображенных верхней и нижней полусферами. В комплексе $\widetilde{K(B)}$ имеется еще одна пара, изображенная средним сечением.

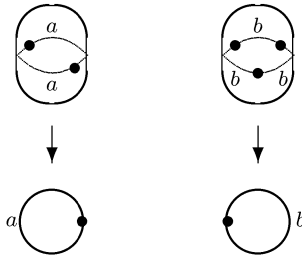


Рис. 27

2) Рассмотрим свободное произведение $A * B = \langle a, b \mid a^2 = 1, b^3 = 1 \rangle$. Пусть Y — комплекс, получающийся соединением вершин комплексов $K(A)$ и $K(B)$ ориентированным ребром t . Очевидно, $\pi_1(Y, y) \cong A * B$. На рис. 28 изображен комплекс X из накрытия $h : X \rightarrow Y$, соответствующего единичной подгруппе группы $\pi_1(Y, y)$. Комплекс X состоит из подкомплексов, изоморфных комплексам $\widetilde{K(A)}$ и $\widetilde{K(B)}$, соединенных поднятиями ребра t , и имеет в целом древесную структуру.

3) Рассмотрим свободное произведение с объединением $G = \langle a, b \mid a^2 = b^3 \rangle$. Пусть Y — комплекс, получающийся «приклеиванием

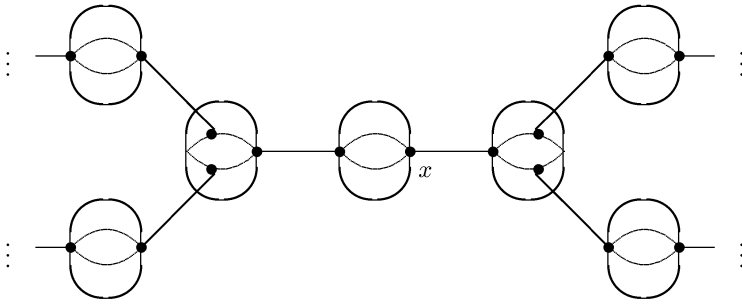


Рис. 28

клетки» D , изображенной на рис. 29 слева, к графу Γ , изображенному справа. Это означает, что граница клетки D отождествляется в соответствии с метками ребер с некоторым циклическим путем в Γ . Очевидно, $\pi_1(Y, y) \cong G$. Обозначим через H ядро гомоморфизма $\varphi : G \rightarrow S_3$, заданного правилом $a \mapsto (12)$, $b \mapsto (123)$. На рис. 30 изображен комплекс X из накрытия $f : (X, x) \rightarrow (Y, y)$, соответствующего подгруппе H . Это накрытие имеет кратность 6. Комплекс X состоит из трех копий двукратного (т.к. $a^2 \in \text{Ker } \varphi$ и $a \notin \text{Ker } \varphi$) накрытия a -петли графа Γ и из двух копий трехкратного (т.к. $b^3 \in \text{Ker } \varphi$ и $b \notin \text{Ker } \varphi$) накрытия b -петли графа Γ , соединенных шестью поднятиями ребра t , а также из шести копий клетки D , приклеенных к тем циклическим путям, вдоль которых читается циклическое слово $a^2tb^{-3}t^{-1}$. Ориентированные ребра комплекса X помечены символами a , b и t в зависимости от того, поднятиями каких ребер они являются.

Мы рекомендуем читателю формально построить комплекс X методом из доказательства утверждения 2 теоремы 20.5 с учетом замечания 25.2.

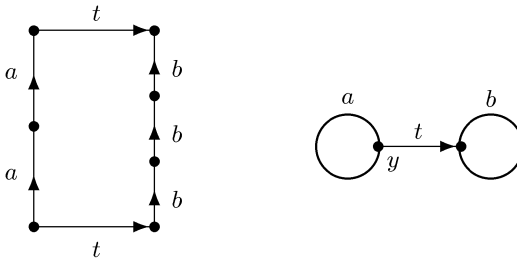


Рис. 29

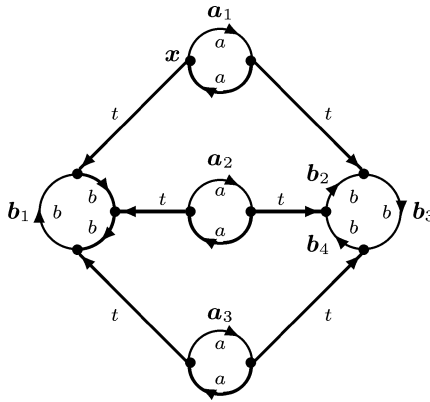


Рис. 30

Вычислим представление фундаментальной группы комплекса \$X\$ с выделенной вершиной \$x\$. На рис. 30 жирной линией выделено максимальное поддерево \$T\$ в \$X\$. Обозначим ориентированные \$a\$-ребра, не входящие в \$T\$, через \$a_1, a_2, a_3\$. Обозначим ориентированные \$b\$-ребра, не входящие в \$T\$, через \$b_1, b_2, b_3, b_4\$. Для краткости записи будем отождествлять ребро \$e\$ с элементом фундаментальной группы \$[p_e]\$. Тогда группа \$\pi_1(X, x)\$ порождается элементами \$a_1, a_2, a_3, b_1, b_2, b_3, b_4\$. Определяющими соотношениями являются слова, которые получаются из контурных путей клеток вычеркиванием всех ребер, входящих в \$T\$. Например, если контурный путь клетки начинается в вершине \$x\$ и вдоль него читается слово \$a^2tb^{-3}t^{-1}\$, то возникает соотношение \$a_1b_1^{-1}\$. Рассматривая шесть контурных путей, вдоль которых читается слово \$a^2tb^{-3}t^{-1}\$, получаем следующие определяющие соотношения:

$$\begin{aligned} a_1b_1^{-1}, & \quad a_1b_2^{-1}b_4^{-1}b_3^{-1}, \\ a_2b_1^{-1}, & \quad a_2b_4^{-1}b_3^{-1}b_2^{-1}, \\ a_3b_1^{-1}, & \quad a_3b_3^{-1}b_2^{-1}b_4^{-1}. \end{aligned}$$

Применяя преобразования Титце, выводим следующее представление группы \$\pi_1(X, x)\$:

$$\langle b_1, b_3, b_4 \mid b_1^{-1}b_3^{-1}b_1b_3 = 1, b_1^{-1}b_4^{-1}b_1b_4 = 1 \rangle.$$

Группа \$H\$ имеет такое же представление и порождается словами, получающимися из меток путей \$p_{b_1}, p_{b_3}, p_{b_4}\$ вычеркиванием букв \$t\$ и \$t^{-1}\$. Итак, группа \$H\$ порождается элементами \$b^3, a^{-1}bab^{-2}, b^2a^{-1}bab^{-1}\$.

25.5. Упражнение. Выразите эти порождающие группы H через порождающие, найденные в пункте 18.7.

25.6. С помощью накрытий легко вывести теорему 19.1. Для простоты изложения ограничимся случаем, когда G — подгруппа группы H , где H — свободное произведение групп H_i ($i \in I$). Построим комплексы (K_i, x_i) по представлениям групп H_i . Пусть K — комплекс, состоящий из комплексов K_i , выделенной вершины x и ориентированных ребер t_i , соединяющих x с x_i . Очевидно, $\pi_1(K, x) \cong H$. Пусть $f : (\tilde{K}, \tilde{x}) \rightarrow (K, x)$ — накрытие, соответствующее подгруппе G . Комплекс \tilde{K} состоит из разнообразных накрытий комплексов K_i , соединенных поднятиями ребер t_i с поднятиями вершины x . Выбрав максимальные поддеревья в этих накрытиях и дополнив их всеми поднятиями ребер t_i , t_i^{-1} и вершины x , получим подграф T в \tilde{K} .

Если T — дерево, то G — свободное произведение подгрупп, сопряженных с подгруппами групп H_i . Сопрягающие элементы соответствуют путям в T из \tilde{x} в фиксированные вершины накрытий комплексов K_i . Если же T — не дерево, то возникает дополнительный свободный множитель F . Мы оставляем читателю разобраться в деталях этого доказательства.

§ 26. Поверхности

В этом параграфе мы дадим комбинаторное определение поверхности, в отличие от геометрического, принятого в дифференциальной геометрии. Поэтому мы используем термин *конечность*, а не *компактность*.

26.1. Определение. Двумерный комплекс, состоящий из конечного числа вершин, ребер и клеток называется *конечным*. *Характеристикой Эйлера* конечного двумерного комплекса K называется число

$$\chi(K) = |K^0| - |\dot{K}^1| + |\dot{K}^2|,$$

где $|K^0|$ — число вершин, $|\dot{K}^1|$ — число пар взаимно обратных ребер и $|\dot{K}^2|$ — число пар взаимно обратных клеток комплекса K .

Элементарными преобразованиями комплекса K называются следующие преобразования.

(1) «Разбиение ребра».

Пусть ребро e идет из вершины v_1 в вершину v_2 . Удалим из комплекса K ребра e , \bar{e} и добавим новые ребра e_1 , e_2 и \bar{e}_1 , \bar{e}_2 , а также

добавим новую вершину v так, что e_1 идет из v_1 в v , а e_2 — из v в v_2 . В границах клеток ребро e заменим на произведение e_1e_2 , а ребро \bar{e} на произведение $\bar{e}_2\bar{e}_1$.

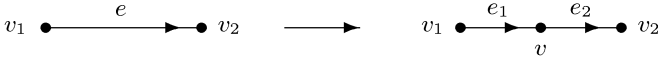


Рис. 31

(2) «Разбиение клетки».

Пусть D — клетка с контурным путем p_1p_2 , где p_1, p_2 — некоторые пути. Удалим из комплекса K клетки D, \bar{D} и добавим новое ребро e , идущее из начала пути p_2 в начало пути p_1 , обратное ему ребро \bar{e} , а также клетки D_1, D_2 с контурными путями $p_1e, \bar{e}p_2$ и обратные к ним клетки.

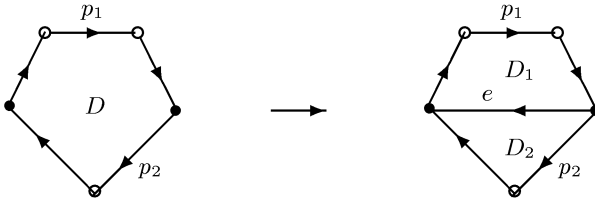


Рис. 32

(3) «Слияние ребер» и «слияние клеток» — преобразования, обратные преобразованиям (1) и (2).

Комплексы K_1 и K_2 называются *эквивалентными*, если от K_1 к K_2 можно перейти с помощью конечного числа элементарных преобразований.

26.2. Упражнение. *Фундаментальные группы эквивалентных связных комплексов изоморфны. Характеристики Эйлера эквивалентных конечных комплексов равны.*

Ребра e_1 и e_2 , выходящие из одной вершины комплекса, называются *соседними*, если e_2 следует за \bar{e}_1 в границе некоторой клетки.

26.3. Определение. *Поверхность* — это двумерный комплекс K с непустым множеством клеток, обладающий следующими свойствами.

- (1) K связан.
- (2) Каждое ребро входит в границу некоторой клетки.

(3) Общее число вхождений каждого ребра в границы всех клеток не более двух¹⁵.

(4) Звезда любой вершины v конечна и для некоторой нумерации ее ребер e_1, e_2, \dots, e_n ребра e_i и e_{i+1} оказываются соседними, $1 \leq i \leq n - 1$.

Ребро называется *краевым*, если оно входит в границу только одной клетки, и притом один раз. Вершины краевых ребер называются *краевыми*, остальные — *внутренними*. *Край поверхности* — это ее подкомплекс, состоящий из краевых ребер и вершин.

26.4. Упражнение. 1) *Вершина v на поверхности краевая тогда и только тогда, когда в обозначениях из (4) ребра e_1 и e_n краевые. Если эти ребра не краевые, то они соседние.*

2) *Каждая компонента связности края конечной поверхности является циклом, т. е. изоморфна некоторому графу C_n из пункта 1.4. Компонентами края бесконечной поверхности могут быть еще графы вида C_∞ .*

26.5. Определение. Поверхность называется *ориентируемой*, если из каждой пары D, \bar{D} ее клеток можно выбрать по представителю так, чтобы каждое ребро, не лежащее на крае, входило ровно один раз в границу некоторого представителя и не входило в границу других представителей.

26.6. Упражнение. *Элементарные преобразования переводят конечную поверхность в конечную поверхность, сохраняют характеристику Эйлера, число компонент края и ориентируемость.*

26.7. Примеры. 1) Пусть S — поверхность, состоящая из двух вершин v_1, v_2 , двух пар ребер e_1, \bar{e}_1 и e_2, \bar{e}_2 , а также двух пар клеток D_1, \bar{D}_1 и D_2, \bar{D}_2 таких, что $\alpha(e_1) = v_1, \omega(e_1) = v_2, \alpha(e_2) = v_2, \omega(e_2) = v_1, \partial(D_1) = e_1 e_2, \partial(D_2) = \bar{e}_1 \bar{e}_2$. Любая поверхность, эквивалентная поверхности S , называется *сферой* (см. рис. 33, слева).

Пусть P — поверхность, состоящая из одной вершины v , одной пары ребер e, \bar{e} и одной пары клеток D, \bar{D} таких, что $\partial D = ee$. Любая поверхность, эквивалентная поверхности P , называется *проективной плоскостью*.

Очевидно, существует накрытие $f : S \rightarrow P$ кратности 2, поверхность S ориентируема, поверхность P неориентируема.

2) Пусть M — поверхность, состоящая из одной внутренней вершины v , одной краевой вершины u , трех пар ребер $\sigma, \bar{\sigma}, \rho, \bar{\rho}, \gamma, \bar{\gamma}$ и

¹⁵Если границы некоторых двух клеток совпадают, то мы считаем вхождения в каждую из них. Ребро может входить дважды в границу одной клетки, но тогда оно не должно входить в границы других клеток.



Рис. 33

одной пары клеток D, \bar{D} таких, что σ идет из v в u , ρ — из u в u , γ — из v в v и $\partial D = \sigma\rho\bar{\sigma}\gamma^2$.

Поверхность M неориентируема. Любая поверхность, эквивалентная поверхности M , называется *листом Мебиуса* (см. рис. 33, справа).

Опишем неформально один из способов построения конечных поверхностей. Пусть A — некоторый конечный алфавит. Возьмем многоугольник D на плоскости, зададим ориентацию его ребер и пометим эти ориентированные ребра буквами из A так, чтобы каждая буква возникла не более двух раз. Тогда поверхность получается «склеиванием» ребер, помеченных одинаковыми буквами (см. рис. 34).

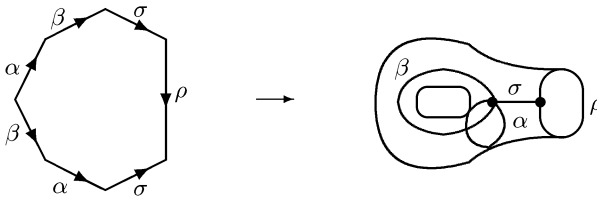


Рис. 34

Следующая теорема показывает, что с точностью до элементарных преобразований любая конечная поверхность может быть получена этим способом.

26.8. Теорема. *Любую конечную поверхность, не являющуюся сферой, можно привести при помощи элементарных преобразований к поверхности K такой, что K имеет только одну внутреннюю вершину, на каждой компоненте ее края имеется ровно одна вершина и одна пара противоположных ребер, в каждую краевую вершину из внутренней идет ровно одно ребро; все остальные ребра начинаются*

и заканчиваются во внутренней вершине, K имеет только одну пару взаимно обратных клеток D, \overline{D} .

Обозначим через $\rho_1, \overline{\rho_1}, \dots, \rho_r, \overline{\rho_r}$ все краевые ребра, через $\sigma_1, \dots, \sigma_r$ — ребра, ведущие из внутренней вершины в начала ребер ρ_1, \dots, ρ_r . Тогда клетка D имеет контур

$$\prod_{i=1}^r \sigma_i \rho_i \overline{\sigma_i} \prod_{j=1}^g \gamma_j^2, \quad g > 0, \quad (-)$$

или

$$\prod_{i=1}^r \sigma_i \rho_i \overline{\sigma_i} \prod_{j=1}^g [\alpha_j, \beta_j], \quad (r, g) \neq (0, 0), \quad (+)$$

где $\gamma_1, \dots, \gamma_g$, соответственно, $\alpha_1, \beta_1, \dots, \alpha_g, \beta_g$ — ребра с началом и концом во внутренней вершине и $[\alpha_j, \beta_j] = \alpha_j \beta_j \overline{\alpha_j} \overline{\beta_j}$.

Доказательство этой теоремы имеется, например, в книгах [56] и [65]. Заметим, что в случае $(-)$ поверхность неориентируема и $\chi(K) = (1+r) - (r+r+g) + 1 = 2 - r - g$. В случае $(+)$ поверхность ориентируема и $\chi(K) = (1+r) - (r+r+2g) + 1 = 2 - r - 2g$.

Число g называется *родом* поверхности в обоих случаях. Сфера имеет род 0. Отсюда и из упражнения 26.6 вытекает следующая теорема.

26.9. Теорема. *Ориентируемость, число компонент края и род образуют полный набор инвариантов конечных поверхностей. Фундаментальная группа конечной неориентируемой поверхности рода g с r компонентами края имеет представление*

$$\langle s_1, \dots, s_r, c_1, \dots, c_g \mid \prod_{i=1}^r s_i \prod_{j=1}^g c_j^2 \rangle, \quad g > 0.$$

Фундаментальная группа конечной ориентируемой поверхности рода g с r компонентами края имеет представление¹⁶

$$\langle s_1, \dots, s_r, a_1, b_1, \dots, a_g, b_g \mid \prod_{i=1}^r s_i \prod_{j=1}^g [a_j, b_j] \rangle.$$

¹⁶Здесь $[a, b] = aba^{-1}b^{-1}$.

26.10. Теорема. Если $f : K \rightarrow S$ — накрытие из связного комплекса в поверхность, то K тоже является поверхностью. При этом K — поверхность без края тогда и только тогда, когда S — поверхность без края. Если поверхности K и S конечны и n — кратность накрытия f , то $\chi(K) = n \cdot \chi(S)$.

Доказательство следует непосредственно из определений и мы оставляем его читателю.

Далее T_g обозначает конечную ориентируемую поверхность рода g без края. Следующая теорема вытекает из теоремы 26.10 и аналогична теореме 20.7.

26.11. Теорема. Любая подгруппа фундаментальной группы поверхности изоморфна фундаментальной группе некоторой поверхности. Если H — подгруппа конечного индекса n в группе $\pi_1(T_g, x)$, то $H \cong \pi_1(T_{g_1}, x_1)$, где $g_1 - 1 = n(g - 1)$.

В заключение приведем нетривиальные примеры накрытий поверхностей. На рис. 35 изображены два различных накрытия $T_3 \rightarrow T_2$ кратности 2.

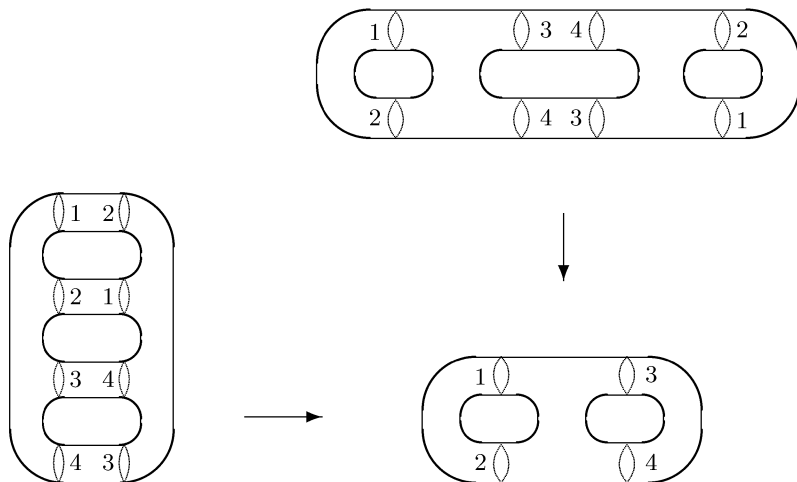


Рис. 35

Эти накрытия получены путем «утолщения» накрытий из графов на рис. 22 в граф на рис. 21.

26.12. Упражнение. *Перечислите все подгруппы индекса 2 в группе $\pi_1(T_2, x) = \langle a_1, b_1, a_2, b_2 \mid [a_1, b_1][a_2, b_2] \rangle$.*

Фундаментальные группы поверхностей наследуют многие свойства свободных групп. Это неудивительно, так как свободная группа ранга n изоморфна фундаментальной группе сферы с $n + 1$ дырой; более того, фундаментальная группа любой поверхности с краем изоморфна свободной группе. Техника *расслоений* и *ламинаций*, развитая при исследовании гомеоморфизмов поверхностей (см. [37]), может быть успешно применена к исследованию групп автоморфизмов этих групп (см. [29, 30], где вводятся *трейн-треки*).

Отметим еще одну параллель. Свободные группы действуют свободно на деревьях, группы $\pi_1(T_g, x)$ — на плоскости. Это следует из того, что единичной подгруппе группы $\pi_1(T_g, x)$ соответствует накрытие $f: P \rightarrow T_g$, где P — плоскость, разбитая на клетки (см. [65]). Удивительно, что группы $\pi_1(T_g, x)$ действуют свободно на *R-деревьях* — естественных обобщениях симплициальных деревьев, введенных в § 1 (см. [47]).

§ 27. Теорема Зайферта–ван Кампена

27.1. Теорема. *Пусть K — комплекс, являющийся объединением связных подкомплексов $K_i, i \in I$, таких, что выполняются следующие условия.*

$$(1) K_s \cap K_t = \bigcap_{i \in I} K_i \text{ для любых } s \neq t.$$

(2) *Пересечение $\bigcap_{i \in I} K_i$ является связным подкомплексом.*

(3) *Тождественное вложение $\bigcap_{i \in I} K_i$ в K_j индуцирует вложение фундаментальных групп для каждого $j \in I$.*

Пусть x — произвольная вершина комплекса $\bigcap_{i \in I} K_i$. Тогда группа $\pi_1(K, x)$ изоморфна свободному произведению групп $\pi_1(K_i, x)$ с объединением по подгруппе $\pi_1(\bigcap_{i \in I} K_i, x)$.

Доказательство выведем из теоремы 24.4. Обозначим $K_0 = \bigcap_{i \in I} K_i$, считая, что $0 \notin I$. Выберем ориентацию K_{0+}^1 в $K_0^{(1)}$ и продолжим ее до ориентации K_{i+}^1 в каждом $K_i^{(1)}$. Выберем также максимальное поддерево T_0 в $K_0^{(1)}$ и продолжим его до максимального поддерева T_i в каждом $K_i^{(1)}$. Объединение этих поддеревьев — максимальное поддерево в $K^{(1)}$. Соответственно, объединение базисов $\{[p_e] \mid e \in K_{i+}^1 - T_i^1\}$

всех свободных групп $\pi_1(K_i^{(1)}, x)$ является базисом свободной группы $\pi_1(K^{(1)}, x)$ (см. теорему 4.3). Положим

$$X_i = \{[p_e] \mid e \in K_{i+}^1 - T_i^1\}, \mathcal{R}_i = \{r_D \mid D \in K_i^2\}.$$

По теореме 24.4 имеем $\pi_1(K_i, x) = \langle X_i \mid \mathcal{R}_i \rangle$ и $\pi_1(K, x) = \langle \bigcup_{i \in I} X_i \mid \bigcup_{i \in I} \mathcal{R}_i \rangle$.

Осталось заметить, что $X_i \cap X_j = X_0$ при $i \neq j$ (в силу (1)) и подгруппа, порожденная множеством X_0 в каждом $\pi_1(K_i, x)$, канонически изоморфна (в силу (3)) группе $\pi_1(K_0, x)$.

27.2. Упражнение. *С помощью рис. 35 докажите, что $\pi_1(T_2, x) \cong A \underset{C}{*} B$, где каждая группа A, B, C изоморфна свободной группе ранга 3.*

§ 28. Теорема Грушко

28.1. Теорема. *Пусть $\psi : F \rightarrow \underset{i \in I}{*} G_i$ — эпиморфизм из конечно порожденной¹⁷ свободной группы F на свободное произведение групп $G_i, i \in I$. Тогда существует такое разложение группы F в свободное произведение $\underset{i \in I}{*} F_i$, что $\psi(F_i) = G_i$ для каждого i .*

Доказательство. Пусть S — базис F , \mathcal{R} — граф с единственной вершиной x и положительно ориентированными ребрами, находящимися во взаимно однозначном соответствии с элементами из S . Для каждого $s \in S$ запишем элемент $\psi(s)$ в нормальной форме в $G = \underset{i \in I}{*} G_i$. Если

$\psi(s) = g_1 g_2 \cdots g_t$ — такая запись, то мы разобьем соответствующее s ребро e на t ребер: $e = e_1 e_2 \dots e_t$; при этом пометим каждое ребро e_i элементом g_i . Возникает новый граф K . Определим метку $\varphi(p)$ любого пути p в K как произведение меток ребер, из которых он состоит. Эта разметка индуцирует гомоморфизм $\varphi^* : \pi_1(K, x) \rightarrow G$.

В дальнейшем к комплексу K будут добавляться новые ребра с метками 1 и двумерные клетки. После каждого шага новый комплекс обозначаем снова через K . Для каждого $i \in I$ определим подкомплекс K_i в K следующим образом: $K_i^0 = K^0, K_i^1 = \{e \in K^1 \mid \varphi(e) \in G_i\}, K_i^2 = \{D \in K^2 \mid \partial D \subseteq K_i^1\}$.

Для исходного комплекса K выполняются следующие свойства.

(1) Группы $\pi_1(K, x)$ и F можно отождествить так, что φ^* отождествится с ψ .

¹⁷Эта теорема справедлива и без предположения о конечной порожденности группы F .

- (2) $\bigcup_{i \in I} K_i = K$.
 (3) $K_s \cap K_t = \bigcap_{i \in I} K_i$ при $s \neq t$.
 (4) $\bigcap_{i \in I} K_i$ есть объединение попарно непересекающихся деревьев.

Мы будем производить изменения так, чтобы и новые комплексы K обладали этими свойствами. Свойство (2) является аналогом равенства $\langle \bigcup_{i \in I} G_i \rangle = G$. Будем добиваться стягиваемости пересечения $\bigcap_{i \in I} K_i$ в точку, что является аналогом равенства $\bigcap_{i \in I} G_i = \{1\}$.

Предположим, что пересечение $\bigcap_{i \in I} K_i$ несвязно. *Связкой* назовем путь p в некотором K_i , начало и конец которого лежат в разных компонентах связности пересечения $\bigcap_{i \in I} K_i$, и такой, что $\varphi(p) = 1$. По лемме 28.2 (см. далее) существует связка p . Добавим к K ребро e с тем же началом и концом, что и у связки p , и добавим клетку с границей $p\bar{e}$. Доопределим φ , полагая $\varphi(e) = 1$. Новый комплекс K обладает свойствами (1)–(4) и новое пересечение $\bigcap_{i \in I} K_i$ имеет на одну компоненту связности меньше, чем старое.

Поэтому за конечное число шагов мы построим комплекс K , для которого пересечение $\bigcap_{i \in I} K_i$ связно, и, значит, по свойству (4) является деревом. Так как $K^0 \subseteq \bigcap_{i \in I} K_i$, то комплекс K_i связан для каждого $i \in I$. По теореме Зайферта – ван Кампена имеем $\pi_1(K, x) = \ast_{i \in I} \pi_1(K_i, x)$. Положим $F_i = \pi_1(K_i, x)$. Тогда $F = \ast_{i \in I} F_i$ и $\psi(F_i) \subseteq G_i$. Поскольку ψ отображает F на G , то $\psi(F_i) = G_i$.

28.2. Лемма. *Если $\bigcap_{i \in I} K_i$ несвязно, то существует связка.*

Доказательство. Пусть v — вершина, не лежащая в той компоненте связности пересечения $\bigcap_{i \in I} K_i$, в которой лежит x . Выберем в K путь p из x в v . Так как ψ — эпиморфизм, то существует замкнутый путь q с началом в x такой, что $\varphi(p) = \varphi(q)$. Тогда путь $r = q^{-1}p$ идет из x в v и $\varphi(r) = 1$. Так как $\bigcup_{i \in I} K_i = K$, то r можно представить в виде $r = r_1 r_2 \cdots r_k$, где каждый путь r_j лежит в некотором $K_{i(j)}$ и соседние r_j не лежат в одном K_i . Так как $\varphi(r) = 1$ и $\varphi(r_j) \in G_{i(j)}$, то из нормальной формы элемента в свободном произведении следует, что $\varphi(r_s) = 1$ для некоторого r_s . Если $\alpha(r_s)$ и $\omega(r_s)$ лежат в разных компонентах связности пересечения $\bigcap_{i \in I} K_i$, то r_s — связка. Предположим, что $\alpha(r_s)$ и $\omega(r_s)$ лежат в одной компоненте связности. Выберем путь r'_s в

этой компоненте, идущий из $\alpha(r_s)$ в $\omega(r_s)$. Так как $\varphi(r'_s) \in \bigcap_{i \in I} G_i = \{1\}$, то можно заменить r_s на r'_s в r , сохранив свойство $\varphi(r) = 1$. Так как r'_s — путь в $\bigcap_{i \in I} K_i$, то можно уменьшить k , присоединив r'_s к соседнему множителю. Таким образом, за конечное число шагов мы найдем связку.

28.3. Следствие. Если $G = \underset{i=1}{*}^n G_i$, то $\mathbf{rk}(G) = \sum_{i=1}^n \mathbf{rk}(G_i)$.

Доказательство. Пусть F — свободная группа, ранг которой равен рангу группы G , и пусть $\psi : F \rightarrow G$ — эпиморфизм. По теореме Грушко существует разложение $F = F_1 * \dots * F_n$ такое, что $\psi(F_i) = G_i$ для всех i . Тогда утверждение следует из неравенств $\sum_{i=1}^n \mathbf{rk}(G_i) \geq \mathbf{rk}(G) = \mathbf{rk}(F) = \sum_{i=1}^n \mathbf{rk}(F_i) \geq \sum_{i=1}^n \mathbf{rk}(G_i)$.

§ 29. Хопфовы и финитно аппроксимируемые группы

Группа G называется *хопфовой*, если любой эпиморфизм $\theta : G \rightarrow G$ имеет единичное ядро. Проблема существования конечно представленных нехопфовых групп возникла в топологии (Хопф, 1931). Простейшие примеры таких групп даются в следующей теореме Баумслэга–Солитэра [26].

29.1. Теорема. Пусть m, n — пара целых взаимно простых чисел, не равных $0, 1, -1$. Тогда группа $G = \langle b, t \mid t^{-1}b^m t = b^n \rangle$ нехопфова.

Доказательство. Определим гомоморфизм $\theta : G \rightarrow G$, полагая $\theta(t) = t, \theta(b) = b^m$. Так как применение θ к определяющему соотношению $t^{-1}b^m t = b^n$ равносильно возведению обеих его частей в степень m , то θ определен корректно. Поскольку t и b^m лежат в образе θ , b^n тоже лежит в образе θ . Так как n и m взаимно просты, то b лежит в образе θ , и, значит, θ — эпиморфизм. Имеем

$$\theta([t^{-1}bt, b]) = [t^{-1}b^m t, b^m] = [b^n, b^m] = 1$$

и

$$[t^{-1}bt, b] = t^{-1}btbt^{-1}b^{-1}tb^{-1} \neq 1$$

по лемме Бриттона. Поэтому ядро эпиморфизма θ неединично.

Далее мы докажем, что группа $G = \langle b, t \mid t^{-1}bt = b^n \rangle$ хопфова при любом целом n . Часть графа Кэли этой группы при $n = 2$ изображена на рис. 36. Видно, что с «фасада» этот граф выглядит как плоскость, а с «торца» — как дерево, валентность каждой вершины которого равна 3.

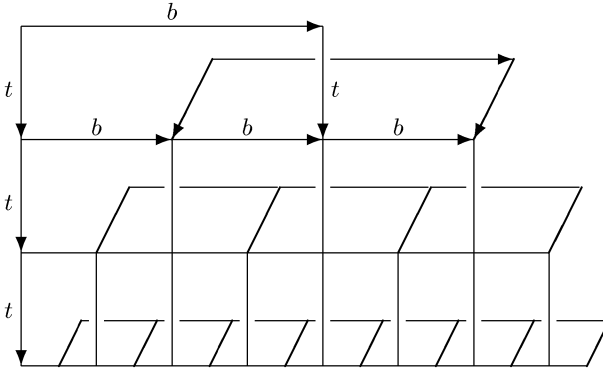


Рис. 36

29.2. Определение. Группа G называется *финитно аппроксимируемой*, если для каждого неединичного элемента g из G существует конечная группа K и гомоморфизм $\varphi : G \rightarrow K$ такой, что $\varphi(g) \neq 1$.

29.3. Упражнение. 1) *Группа G финитно аппроксимируема тогда и только тогда, когда пересечение всех ее нормальных подгрупп конечного индекса равно $\{1\}$.*

2) *Любая подгруппа финитно аппроксимируемой группы финитно аппроксимируема.*

Свойство финитной аппроксимируемости применяется при решении некоторых алгоритмических проблем.

29.4. Теорема. *Проблема равенства слов в конечно представленной финитно аппроксимируемой группе G разрешима.*

Доказательство. Пусть $\langle X \mid R \rangle$ — конечное представление группы G , g — произвольное слово в алфавите $X \cup X^{-1}$ и \bar{g} — его образ при естественном гомоморфизме из $F(X)$ в G . Мы хотим узнать, равен ли элемент \bar{g} единичному элементу в G . Для этого одновременно устраиваем два процесса. Первый процесс перечисляет все слова, равные 1 в

группе G (для этого надо перечислять слова из нормального замыкания множества R в $F(X)$), второй перечисляет образы данного g при всех гомоморфизмах из G во все конечные группы (почему это возможно?). Если $\bar{g} = 1$, то мы поймем это за конечное число шагов в первом процессе, если $\bar{g} \neq 1$, то это станет ясно из второго процесса.

29.5. Теорема. *Группа $GL_n(\mathbb{Z})$ финитно аппроксимируема.*

Доказательство. Для любого натурального числа m существует гомоморфизм $\varphi_m : GL_n(\mathbb{Z}) \rightarrow GL_n(\mathbb{Z}_m)$, при котором элементы матрицы заменяются на соответствующие им вычеты по модулю m . Для неединичной матрицы $A \in GL_n(\mathbb{Z})$ ее образ относительно φ_m неединичен при $m > \max |A_{ij}|$.

Следующая более общая теорема доказана А. И. Мальцевым [15].

29.6. Теорема. *Всякая конечно порожденная группа матриц над полем финитно аппроксимируема.*

29.7. Теорема. *Любая свободная группа финитно аппроксимируема.*

Доказательство. Пусть $F(X)$ — свободная группа с базисом X и g — произвольный неединичный элемент из $F(X)$. В его записи участвует только конечное число элементов из X . Пусть X_1 — множество этих элементов. Рассмотрим гомоморфизм $\varphi : F(X) \rightarrow F(X_1)$ такой, что $\varphi(x) = x$ при $x \in X_1$ и $\varphi(x) = 1$ при $x \in X - X_1$. Тогда $\varphi(g) \neq 1$. Поэтому достаточно рассмотреть случай, когда базис X конечен. По упражнению 3.12 свободные группы всех конечных рангов вкладываются в свободную группу $F(a, b)$. Поэтому достаточно доказать финитную аппроксимируемость группы $F(a, b)$. Но эта группа финитно аппроксимируема, так как она вкладывается в группу $SL_2(\mathbb{Z})$, что следует из теоремы Санова 13.13 или упражнения 19.2.

Приведем исходное доказательство Шрайера, иллюстрирующее тезис, что все гениальное просто. Пусть $g = x_1x_2 \dots x_n$ — непустое приведенное слово в алфавите $X \cup X^{-1}$. Определим гомоморфизм $\varphi : F(X) \rightarrow S_{n+1}$, для которого $\varphi(g) \neq 1$. Порождающие из X , не входящие в g и g^{-1} , отобразим в тождественную подстановку. Остальные порождающие из X отобразим в подстановки так, чтобы x_i переводил символ $i + 1$ в i , независимо от того, порождающий это или обратный к нему. Это условие определяет подстановки неоднозначно, но оно непротиворечиво, поскольку элементы x_i и x_{i+1} не взаимно обратны. Независимо от того, как мы доопределим подстановки для всех x_i , произведение $x_1x_2 \dots x_n$ будет переводить символ $n + 1$ в символ 1.

произвольности n , K содержится в пересечении всех подгрупп конечного индекса группы G . Так как G финитно аппроксимируема, то это пересечение равно $\{1\}$, следовательно $K = \{1\}$.

29.11. Следствие (см. [15]). *Всякая конечно порожденная группа матриц над полем хопфова.*

Доказательство непосредственно вытекает из теорем 29.6 и 29.9.

29.12. Следствие. *Для каждого целого n группа $\langle a, b \mid a^{-1}ba = b^n \rangle$ хопфова.*

Доказательство вытекает из упражнения 5.5 и следствия 29.11.

Историческая справка

I. Первый значительный вклад в теорию групп внес Эварист Галуа (1811–1832) при исследовании вопроса о разрешимости в радикалах алгебраических уравнений (см. [8] и [13, 20]). Именно Галуа впервые ввел понятие группы и попытался понять как они устроены. До него группы в виде подстановок корней уравнения возникали также в работах Лагранжа (1771), Руффини (1799) и Абеля (1825).

В 1830–1832 годах Галуа пришел к понятиям нормальной подгруппы, разрешимой группы, простой группы и сформулировал¹⁹ теоремы о простоте знакопеременной группы A_n степени $n \geq 5$ и о простоте проективной специальной линейной группы $\text{PSL}_2(q)$ при простом $q \geq 4$.

Исключительная роль конечных простых групп объясняется тем, что из них может быть построена любая конечная группа. Долгое время исследования групп велись в терминах групп подстановок. В частности, изучался вопрос о кратно транзитивных группах подстановок. Именно на этом пути Эмиль Матье открыл в 1861 году две простые группы M_{12} и M_{24} . Из них легко получаются простые группы M_{11} , M_{22} и M_{23} . Эти пять групп Матье являются спорадическими (исключительными) группами, так как они не входят в три бесконечные серии простых конечных групп: циклические группы простого порядка, знакопеременные группы степени ≥ 5 и простые группы лиева типа (о них можно прочитать в книге [36]). Удивительно, что шестая спорадическая группа J_1 была открыта Звонимиром Янко только в 1965 году.

Всплеск активности в этой области произошел благодаря трем выдающимся событиям.

В 1954 году Ричард Брауэр предложил исследовать группы по централизаторам инволюций. Одной из важных теорем в этом направлении является теорема Брауэра – Фаулера о том, что существует только конечное число конечных простых групп с данным централизатором инволюции.

В 1955 году появилась работа Клода Шевалле о конечных группах лиева типа.

¹⁹В имеющихся бумагах Галуа не все утверждения строго доказаны. Некоторые утверждения неверны, но даже они подчеркивают силу его мысли. Так лемма 1 из дополнения \mathcal{N} к его «Мемуару о решении уравнений» при некоторых необходимых ограничениях превращается в теорему Силова о количестве силовских p -подгрупп.

В 1962 году Джон Томпсон и Уолтер Фейт доказали свою знаменитую теорему, согласно которой любая группа нечетного порядка разрешима.

Открытие группы Янко J_1 послужило сигналом к настоящей охоте на спорадические группы. Их открывали примерно по одной штуке в год в течение 16 лет. Изумительные по красоте конструкции предложил Джон Конвей. Он построил простые группы Co_3 , Co_2 и Co_1 из группы автоморфизмов замечательной 24-мерной решетке Лича, которая появилась при исследовании плотных упаковок сфер. В 1981 году Роберт Грисс построил 26-ю спорадическую группу — группу Грисса–Фишера F_1 , которую он назвал сначала Монстром, а затем Дружественным гигантом (ее порядок равен примерно 10^{54}).

В середине 80-х годов XX века у специалистов по конечным группам возникла уверенность, что спорадических групп существует ровно 26 и классификационная теорема (см. пункт 10.2 в главе 1) может быть доказана. Однако, до сих пор (2002 год) полное доказательство все еще не опубликовано. Более подробно с историей этого вопроса можно ознакомиться по книгам [49], [40] и [24].

II. Принято считать, что комбинаторная теория групп — это теория, изучающая группы, заданные порождающими и определяющими соотношениями. Её истоки находятся в работах Шварца, Клейна, Фукса, Пуанкаре и Шоттки, в которых группы возникали как дискретные группы геометрических преобразований. И все же решающим пунктом в становлении комбинаторной теории групп является статья Вальтера фон Дика 1882 года, где доказано существование свободной группы (термин введен позднее Дэном) и показано, что произвольная группа получается из подходящей свободной группы наложением некоторых определяющих соотношений. Следующим важным этапом является работа Титце 1908 года, где исследуется вопрос об изоморфизме групп, заданных различными системами порождающих и определяющих соотношений. Эта работа была вдохновлена открытием Пуанкаре в 1895 году понятия фундаментальной группы топологического пространства и работами Виртингера по теории узлов. Четыре работы Дэна 1910, 1911, 1912 и 1914 годов углубляют и продолжают работу Титце. В этих работах он формулирует проблемы равенства слов, сопряженности слов и изоморфизма групп, заданных множествами порождающих и определяющих соотношений. Используя геометрические методы, Дэн находит чисто алгебраическое решение проблемы равенства слов для фундаментальной группы ориентируемой поверхности, заданной следующим представлением:

$$\langle a_1, b_1, \dots, a_g, b_g \mid a_1^{-1}b_1^{-1}a_1b_1 \dots a_g^{-1}b_g^{-1}a_gb_g = 1 \rangle.$$

Найденный им алгоритм (сейчас он называется алгоритмом Дэна) применим к очень широкому классу групп — так называемым гиперболическим группам, интенсивное исследование которых началось после появления в 1987 году работы М. Громова [50]. Макс Дэн предложил также конструкцию графа, называемого теперь графом Кэли группы. Истоки этой идеи имеются уже в работе Кэли 1878 года. Разница в подходах Кэли и Дэна состоит в том, что Кэли, исходя из «цветных» графов строит группы, Дэн же строит графы по представлениям групп. Эти графы адекватно отражают строение группы и применяются, например, в теории Басса–Серра групп, действующих на деревьях. Этапом бури и натиска можно назвать статьи Нильсена 1917–1924 годов (две из них были написаны и опубликованы во время его службы в германском флоте). В статье 1921 года Нильсен приводит некоторый метод (сейчас он называется методом Нильсена), из которого следует, что конечно порожденная подгруппа свободной группы также свободна. В полной общности результат о свободе произвольных подгрупп свободных групп был получен Шрайером в 1927 году. Исключительно сложной по комбинаторному доказательству является работа Нильсена 1924 года, где он находит конечное представление группы автоморфизмов свободной группы конечного ранга. Более прозрачное доказательство было получено Маккулом только в 1975 году. Следующей важной вехой в развитии комбинаторной теории групп являются статьи Райдемайстера 1926 года и Шрайера 1927 года, где развивается метод нахождения представлений подгрупп в группе, заданной порождающими и определяющими соотношениями. Райдемайстер проинтерпретировал этот метод через накрытия топологических пространств, Шрайер — через граф смежных классов группы по ее подгруппе, что, в принципе, одно и то же. Исследование фундаментальных групп топологических пространств привело к кристаллизации понятий свободного произведения групп (Артин, 1926, Шрайер, 1927), свободного произведения с объединением (Шрайер, 1927) и HNN-расширения (Хигман, Б. Нейман и Х. Нейман, 1949). Чисто алгебраическим путем А. Г. Курош получает теорему о строении подгрупп свободных произведений групп (1934), а И. А. Грушко (1940) и Б. Нейман (1943) развивают метод Нильсена для свободных произведений групп.

В 1968–69 годах Ж.-П. Серр прочитал курс лекций в Коллеж де Франс, посвященный исследованию групп, действующих на деревьях. Записки этих лекций были подготовлены им в сотрудничестве с Х. Бассом. Развитая ими теория, называемая теперь *теорией Басса–Серра*, содержит прозрачное и естественное объяснение многих результатов о свободных группах и свободных конструкциях с геометрической точки зрения. Для специалистов по комбинаторной теории групп

французский вариант этой книги [60] и более поздний английский [61] стали своего рода Библией, в которой объяснено, как группы, деревья и действие порождают мир комбинаторной теории групп.

Многие классические результаты комбинаторной теории групп (но не теория Басса–Серра) содержатся в переводных книгах Магнуса, Карраса, Солитера [55] и Линдона, Шуппа [53]. С историей комбинаторной теории групп до 1980 года можно ознакомиться по книге Чандлера, Магнуса [38]. Успехи в решении алгоритмических проблем теории групп до 1984 года отражены в обзоре С. И. Адяна и Г. С. Маканина [2]. Полезная и разнообразная информация содержится также в обзорах А. Ю. Ольшанского и А. Л. Шмелькина [19], Р. И. Григорчука и П. Ф. Курчанова [9], Д. Коллинза и Х. Цишанга [11].

В последние 15 лет на небосклоне комбинаторной теории групп наблюдаются вспышки новых идей и теорий, источником которых является геометрия и топология. Вот некоторые из них²⁰:

- ★ *трейн-треки* (М. Бествина, М. Хэндель [29, 30]),
- ★ *\mathbb{R} -деревья* (И. Рипс (не опубликовано); М. Бествина, М. Фейн [28]; Д. Габорэ, Г. Левитт, Ф. Полен [47]),
- ★ *теория концов групп* (истоки у Дж. Столлингса [62]; М. Данвуди [43]; М. Бествина, М. Фейн [27]; И. Рипс, З. Села [59]; Б. Бовдич [32]; М. Данвуди, М. Сагеев [45]; М. Данвуди, Э. Свенсон [46]),
- ★ *гиперболические группы* (М. Громов [50], см. также книги [48, 33]),
- ★ *автоматные группы* (Дж. Кэннон, С. Леви, М. Паттерсон, У. Терстон, Д. Хольт, Д. Эпстейн [35]).

Нерешенные проблемы теории групп фиксируются в книге [14] и на сайте [66].

²⁰Мы упоминаем только ключевые работы.

Список литературы

- [1] Адян С. И. *Неразрешимость некоторых алгоритмических проблем теории групп*. Труды Моск. матем. о-ва, 1957, т. 6, 231–298.
- [2] Адян С. И., Маканин Г. С. *Исследования по алгоритмическим вопросам алгебры*. Труды МИАН СССР, 1984, т. 168, 197–217.
- [3] Богопольский О. В. *Введение в теорию конечных групп*. Учеб. пособие. Новосибирск: Новосиб. гос. ун-т, 1997.
- [4] Богопольский О. В. *Комбинаторная теория групп. Часть I*. Учеб. пособие. Новосибирск: Новосиб. гос. ун-т, 2000.
- [5] Богопольский О. В. *О древесной разложимости групп автоморфизмов свободных групп*. Алгебра и логика, 1987, т. 26, № 2, 131–149.
- [6] Богопольский О. В. *Конечно порожденные группы со свойством М. Холла*. Алгебра и логика, 1992, т. 31, № 3, 227–275.
- [7] Борисов В. В. *Простые примеры групп с неразрешимой проблемой тождества*. Мат. заметки, 1969, т. 6, №5, 521–532.
- [8] Галуа Эварист. *Сочинения*. М.-Л.: НКТП, 1936.
- [9] Григорчук Р. И., Курчанов П. Ф. *Некоторые вопросы теории групп, связанные с геометрией*. В кн.: Итоги науки и техн. Современ. пробл. матем. Фундам. направления, т. 58, М.: ВИНТИ, 1990 (стр. 191–256).
- [10] Каргаполов М. И., Мерзляков Ю. И. *Основы теории групп*. 3-е изд. М.: Наука, 1982.
- [11] Коллинз Д., Цишанг Х. *Комбинаторная теория групп и фундаментальные группы*. В кн.: Итоги науки и техн. Современ. пробл. матем. Фундам. направления, т. 58, М.: ВИНТИ, 1990 (стр. 5–190).
- [12] Кострикин А. И. *Вокруг Бернсайда*. М.: Наука, 1986.
- [13] Кострикин А. И. *Введение в алгебру*. (В трех частях.) М.: Физматлит, 2000.
- [14] *Коуровская тетрадь: Нерешенные вопросы теории групп*. 15-е изд. Новосибирск, 2002.
- [15] Мальцев А. И. *Об изоморфном представлении бесконечных групп матрицами*. Мат. сб., 1940, т. 8, № 3, 405–422.

- [16] Марков А. А. *Невозможность некоторых алгоритмов в теории ассоциативных систем*. Докл. АН СССР, 1947, т. 55, № 7, 587–590.
- [17] Новиков П. С. *Об алгоритмической неразрешимости проблемы тождества слов в теории групп*. Труды МИАН СССР, 1955, т. 44, 3–143.
- [18] Ольшанский А. Ю. *Геометрия определяющих соотношений*. М.: Наука, 1989.
- [19] Ольшанский А. Ю., Шмелькин А. Л. *Бесконечные группы*. В кн.: Итоги науки и техн. Современ. пробл. матем. Фундам. направления, т. 37, М.: ВИНТИ, 1989 (стр. 5–113).
- [20] Постников М. М. *Теория Галуа*. М.: Физматлит, 1963.
- [21] Серпинский В. *250 задач по элементарной теории чисел*. М.: Просвещение, 1968.
- [22] Чуркин В. А. *К теории групп, действующих на деревьях*. Алгебра и логика, 1983, т. 22, № 2, 218–225.
- [23] Шафаревич И. Р. *Основные понятия алгебры*. Ижевск: Регулярная и хаотическая динамика, 1999.
- [24] Aschbacher M. *Sporadic groups*. Cambridge tracts in mathematics, 104, Cambridge, Univ. Press, 1994.
- [25] Baumslag G. *Multiplicators and metabelian groups*. J. London Math. Soc. Series A, 1976, V. 22, N 3, 305–312.
- [26] Baumslag G., Solitar D. *Some two-generator, one-relator non-Hopfian groups*. Bull. Amer. Math. Soc., 1962, V. 68, N 3, 199–201.
- [27] Bestvina M., Feighn M. *Bounding the complexity of simplicial group actions*. Invent. Math., 1991, V. 103, 449–469.
- [28] Bestvina M., Feighn M. *Stable actions of groups on real trees*. Invent. Math., 1995, V. 121, 287–321.
- [29] Bestvina M., Handel M. *Train tracks and automorphisms of free groups*. Annals of Math., 1992, V. 135, N 2, 1–53.
- [30] Bestvina M., Handel M. *Train tracks for surface homeomorphisms*. Topology, 1995, V. 34, N 1, 109–140.
- [31] Boone W. W. *The word problem*. Ann. of Math., 1959, V. 70, N 2, 207–265.
- [32] Bowditch B. H. *Cut points and canonical splittings of hyperbolic groups*. Acta Math., 1998, V. 180, N 2, 145–186.
- [33] Bridson M., Haefliger A. *Metric spaces of non-positive curvature*. Boston–Heidelberg: Springer–Verlag, 1999.

- [34] Cameron P. J., van Lint J. H. *Graph theory, coding theory and block designs*. London Math. Soc. Lecture Note Ser., 19, Cambridge Univ. Press, 1975. (Пер. на рус. яз.: Камерон П., Дж. ван Линт. *Теория графов, теория кодирования и блок-схемы*. М.: Наука, 1980.)
- [35] Cannon J., Epstein D., Holt D., Levy S., Paterson M., Thurston W. *Word processing in groups*. Boston: Jones and Barlett, 1992.
- [36] Carter R. W. *Simple groups of Lie type*. New York: Wiley, 1989. (Reprint of the 1972 original.)
- [37] Casson A., Bleiler S. *Automorphisms of surfaces after Nielsen and Thurston*. Cambridge–New York: Cambridge Univ. Press, 1988. (Имеется перевод: Кассон Э., Блейлер С. *Теория автоморфизмов поверхностей по Нильсену и Терстону*. М.: ФАЗИС, 1998.)
- [38] Chandler B., Magnus W. *The history of combinatorial group theory*. Berlin, New York, Heidelberg: Springer–Verlag, 1982. (Пер. на рус. яз.: Чандлер Б., Магнус В. *Развитие комбинаторной теории групп*. М.: Мир, 1985.)
- [39] Conway J. H., Curtis R. T., Norton S. P., Parker R. A., Wilson R. A. *Atlas of finite groups*. Oxford: Clarendon Press, 1985.
- [40] Conway J. H., Sloane N. J. A. *Sphere packing, lattices and groups*. Grundlehren der math. Wissenschaften 290, A Series of Comprehensive Studies in Math., New York: Springer–Verlag, 1988. (Пер. на рус. яз.: Конвей Дж., Слоэн Н. *Упаковки шаров, решетки и группы*. М.: Мир, 1990.)
- [41] Coxeter H. S. M., Moser W. O. J. *Generators and relations for discrete groups*. 3–rd ed., Berlin–Heidelberg–New York: Springer–Verlag, 1972. (Пер. на рус. яз.: Коксетер Г. С. М., Мозер У. О. Дж. *Порождающие элементы и определяющие соотношения дискретных групп*. М.: Наука, 1980.)
- [42] Crowell R. H., Fox R. H. *Introduction to knot theory*. Boston–New York–Toronto: GINN and Co., 1963. (Пер. на рус. яз.: Кроуэлл Р., Фокс Р. *Введение в теорию узлов*. М.: Мир, 1967.)
- [43] Dunwoody M. J. *The accessibility of finitely presented groups*. Invent. Math., 1985, V. 81, 449–457.
- [44] Dunwoody M. J. *Folding sequences*. In: The Epstein birthday shrift, Geometry and topology monographs, International Press, 1998, V. 1, 139–158.
- [45] Dunwoody M. J., Sageev M. E. *JSJ-decompositions for finitely presented groups over slender subgroups*. Invent. Math., 1999, V. 135, 25–44.

- [46] Dunwoody M. J., Swenson E. L. *The algebraic torus theorem*. Invent. Math., 2000, V. 140, 605–637.
- [47] Gaboriau D., Levitt G., Paulin F. *Pseudogroups of isometries of \mathbb{R} and Rips' theorem on free actions on \mathbb{R} -trees*. Israel J. of Math., 1994, V. 87, 403–428.
- [48] Ghys E., de la Harpe P. (editors). *Sur les Groupes Hyperboliques d'après Mikhael Gromov*. Progr. Math., V. 83, Boston–Basel–Berlin: Birkhäuser, 1990. (Пер. на рус. яз.: *Гиперболические группы по Михаэлю Грому*. М.: Мир, 1992.)
- [49] Gorenstein D. *Finite simple groups. An introduction to their classification*. New York: Plenum Publ. Corp., 1982. (Пер. на рус. яз.: Горенштейн Д. *Конечные простые группы. Введение в их классификацию*. М.: Мир, 1985.)
- [50] Gromov M. *Hyperbolic groups*. In: *Essays in group theory*. (S. M. Gersten ed.) MSRI Publ. 8, Springer–Verlag, 1987, 75–263. (Пер. на рус. яз.: Громов М. *Гиперболические группы*. Москва–Ижевск: Институт компьютерных исследований, 2002.)
- [51] Huppert B., Blackburn N. *Finite groups III*. (A series of Comprehensive Studies in Math., 243) Berlin–Heidelberg–New York: Springer–Verlag, 1982.
- [52] Lang S. *Algebra*. Reading, Mass.: Addison–Wesley, 1965. (Пер. на рус. яз.: Ленг С. *Алгебра*. М.: Мир, 1968.)
- [53] Lyndon R. C., Schupp P. E. *Combinatorial group theory*. Ergebnisse der Mathematik, 89, Berlin–Heidelberg–New York: Springer–Verlag, 1977. (Пер. на рус. яз.: Линдон Р., Шупп П. *Комбинаторная теория групп*. М.: Мир, 1980.)
- [54] Magnus W. *Das Identitäts Problem für Gruppen mit einer definierenden Relation*. Math. Ann., 1932, Bd. 106, 295–307.
- [55] Magnus W., Karrass A., Solitar D. *Combinatorial group theory*. New York: Wiley, 2-nd ed. New York: Dover, 1976. (Пер. на рус. яз.: Магнус В., Каррас А., Солитар Д. *Комбинаторная теория групп*. М.: Наука, 1974.)
- [56] Massey W. S. *Algebraic topology: An Introduction*. New York: Harcourt, Brace and World, 1967. (Пер. на рус. яз. в кн.: Масси У., Столлингс Дж. *Алгебраическая топология. Введение*. М.: Мир, 1977.)
- [57] Neumann B. H. *Some remarks on infinite groups*. J. London Math. Soc., 1937, V. 12, 120–127.
- [58] Rabin M. O. *Recursive unsolvability of group theoretic problems*. Annals of Math., 1958, V. 67, N 1, 172–194.

- [59] Rips E., Sela Z. *Cyclic splitting of finitely presented groups and the canonical JSJ decomposition*. Annals of Math., 1997, V. 146, N 1, 53–109.
- [60] Serre J.-P. *Arbres, amalgames et SL_2* . Notes Collège de France, 1968/69. (Пер. на рус. яз.: Серр Ж.-П. *Деревья, амальгамы и SL_2* . Математика, 1974, т. 18, № 1, 3–51.)
- [61] Serre J.-P. *Trees*. Berlin–Heidelberg–New York: Springer–Verlag, 1980.
- [62] Stallings J. R. *Group theory and three dimensional manifolds*. Yale Math. monographs, N 4, New Heaven: Yale Univ. Press, 1971.
- [63] Stallings J. R. *Topology of finite graphs*. Invent. Math., 1983, V. 71, 551–565.
- [64] Suzuki M. *Group theory I*. Berlin–Heidelberg–Tokyo: Springer–Verlag, 1986.
- [65] Zieschang H., Vogt E., Coldewey H.-D. *Surfaces and planar discontinuous groups*. Berlin–Heidelberg–New York: Springer–Verlag, 1980. (Пер. на рус. яз.: Цишанг Х., Фогт Э., Колдевай Х.-Д. *Поверхности и разрывные группы*. М.: Наука, 1988.)
- [66] <http://www.grouptheory.org>

Богопольский Олег Владимирович

ВВЕДЕНИЕ В ТЕОРИЮ ГРУПП

Дизайнер М. В. Ботя

Технический редактор А. В. Ширококов

Корректор М. А. Ложкина

Подписано в печать 19.08.02. Формат $60 \times 84^{1/16}$.
Печать офсетная. Усл. печ. л. 8,6. Уч. изд. л. 8,75.
Гарнитура Таймс. Бумага офсетная №1. Заказ №40.

АНО «Институт компьютерных исследований»
426034, г. Ижевск, ул. Университетская, 1.

Лицензия на издательскую деятельность ЛУ №084 от 03.04.00.

<http://rcd.ru> E-mail: borisov@rcd.ru
