Т.М. Банникова, Н.А. Баранова

Теория групп в задачах и упражнениях

Ижевск
2009

Федеральное агентство по образованию
Государственное образовательное учреждение
высшего профессионального образования
«Удмуртский государственный университет»

Т.М. Банникова, Н.А. Баранова

Теория групп в задачах и упражнениях

Учебно-методическое пособие

Ижевск 2009

УДК 511(075)
ББК 22.13я7
Б 232

Рекомендовано к изданию учебно-методическим советом УдГУ.
Рецензент: к.ф.-м.н., доцент кафедры прикладной математики и информатики ИжГТУ Ицков А.Г.

Банникова Т.М., Баранова Н.А.
Б 232 Теория групп в задачах и упражнениях: учебно-методическое пособие. Ижевск, 2009. 105 с.

Учебно-методическое пособие подготовлено на кафедре алгебры и топологии Удмуртского государственного университета и рекомендуется студентам 1 и 2 курса направления 511200 «Математика. Прикладная математика». (бакалавриат).

В учебно-методическом пособии рассматриваются основные вопросы теории групп, содержатся примеры и упражнения, демонстрирующие использование изложенной теории для решения конкретных задач. По каждой теме курса специально подобрана система упражнений, что способствует лучшему усвоению излагаемого материала. Теоретический материал снабжен системой упражнений для самостоятельного доказательства, которую можно также использовать для организации практических и лабораторных занятий по курсу «Алгебры».

Учебно-методическое пособие может быть также полезно студентам всех специальностей и направлений факультетов ФИТиВТ и МФ при изучении элементов теории групп в соответствующих курсах.

Оглавление

ВВЕДЕНИЕ

Теория групп составляет важную часть в курсе алгебры. Понятие группы является одним из фундаментальных в математическом образовании.

В настоящее время основы теории групп являются стала составной частью подготовки не только бакалавров математиков, но и специалистов в области физики, химии и информатики. Основные идеи теории групп изучаются студентами и в рамках таких фундаментальных математических дисциплин как «Алгебра», «Алгебра и геометрия», «Геометрия и алгебра» и других.

Представленный в учебно-методическом пособии материал дает начальное представление о теории групп и доступен студентам младших курсов математических специальностей.

Несмотря на наличие разнообразной научной литературы и учебных пособий по теории чисел, в них практически отсутствует сопровождение теоретической информации необходимым количеством задач и упражнений для организации самостоятельной работы студентов. Настоящее пособие пытается частично восполнить этот пробел.

В пособии рассматриваются основные вопросы теории групп, содержатся примеры и упражнения, демонстрирующие использование изложенной теории для решения конкретных задач. По каждой теме курса специально подобрана система упражнений, что способствует лучшему усвоению излагаемого

материала. Теоретический материал снабжен системой упражнений для самостоятельного доказательства, который можно также использовать для организации практических и лабораторных занятий по курсу «Алгебра».

Данное пособие охватывает весь материал теории групп, включенный в ныне действующую университетскую программу подготовки бакалавров-математиков. Оно, разумеется, не может заменить подробных учебников и не является специализированным задачником. Предлагаемые задачи имеют различную сложность и преследуют следующие дидактические цели: от первого знакомства с понятием теории групп до их серьезного изучения.

Список литературы, которую авторы использовали, приведен в конце пособия, и его можно рекомендовать для изучения других проблем теории групп, не освещенных в данном пособии.

1. Основные определения и примеры групп

Определение. *Декартовым произведением* двух множеств называется пара элементов a, b, где $a \in M$, $b \in M$. Декартово произведение обозначается

$$M \times M = \{(a, b) \colon a \in M, b \in M\}.$$

Определение. *Бинарной операцией* на множестве M называется отображение

$$M \times M \to M,$$
$$(a, b) \to c,$$

заданное по какому-либо правилу.

Определение. Бинарная операция *ассоциативна*, если для любых $a, b, c \in M$

$$(a * b) * c = a * (b * c).$$

Упражнение 1. Доказать обобщенный закон ассоциативности, т.е. для любого n выполнено

$$a_1 * a_2 * \ldots * a_n = a_1 * (a_2 * a_3) * \ldots * (a_{n-1} * a_n).$$

Указание. Использовать метод математической индукции.

Упражнение 2. Ассоциативна ли операция $*$ на множестве M, если

а) $M = \mathbb{N}$, $x * y = x^y$;

б) $M = \mathbb{Z}$, $x * y = x^2 + y^2$;

в) $M = \mathbb{R}$, $x * y = \sin x \cdot \sin y$.

Ответ. а) нет; б) да; в) нет.

Определение. $(M, *)$ — множество элементов произвольной математической природы с определенной на ней ассоциативной бинарной операцией называется *полугруппой*.

Упражнение 3. Сколько существует неизоморфных между собой полугрупп порядка 2?

Определение. Элемент $e \in M$ называется *нейтральным*, если для всех $a \in M$

$$a * e = e * a = a.$$

Определение. Полугруппа с нейтральным элементом называется *моноидом*.

Определение. Элемент b называется *обратным* для a, если

$$a * b = b * a = e.$$

Упражнение 4. Доказать, что если в полугруппе существует нейтральный элемент, то он единственный.

Упражнение 5. Правым (левым) нулем полугруппы называется такой элемент z, что $az = z$ ($za = z$) при любом a. Доказать, что если в полугруппе имеются как правые, так и левые нули, то все они совпадают, так что существует единственный двусторонний нуль.

Указание. Рассмотреть $z_1 z_2$, где z_1 — какой-либо левый нуль, z_2 — правый нуль.

Упражнение 6. Правой (левой) единицей полугруппы называется такой элемент u, что $au = a$ ($ua = a$) при любом a. Доказать, что если в полугруппе имеются как правые так и левые единицы, то все они совпадают, так что существует единственная двусторонняя единица.

Указание. Рассмотреть $u_1 u_2$, где u_1 — какая-либо левая единица, u_2 — правая единица.

Упражнение 7. Может ли элемент полугруппы быть одновременно правым нулем и левой единицей?

Ответ. Да, только в полугруппе, в которой произведение равно правому сомножителю.

Упражнение 8. Доказать, что если в полугруппе существует обратный элемент, то он единственный.

Определение. Моноид, для которого выполняется условие: для всех $a \in M$, существует $b \in M$:

$$a * b = b * a = e$$

называется *группой*.

Сформулируем определение группы другим способом.

Определение. Множество элементов M с определенной на нем бинарной операцией, удовлетворяющей следующим условиям:

1. для всех a, b, c: $a * b * c = a * (b * c)$, $\forall\ a, b, c \in M$;
2. существует e: $\forall\ a \in M$, $a * e = e * a$;
3. для всех $a \in M$ существует $b \in M$: $a * b = b * a = e$

называется *группой*.

Определение. Группа, для которой выполняется следующее условие: для всех $a, b \in M$: $a * b = b * a$ называется *коммутативной* (или абелевой) группой.

Если множество M имеет бесконечное число элементов, то группа имеет бесконечный порядок.

Если множество M имеет конечное число элементов (n-элементов), то группа называется *конечной группой* и ее порядок равен n, т. е. $|M| = n$.

Упражнение 9. На множестве M^2, где M — множество, определена операция $\circ$ по правилу $(x, y) \circ (z, t) = (x, t)$. Является ли M^2 полугруппой относительно этой операции? Существует ли в M^2 нейтральный элемент?

Ответ. Да; не существует, если $|M| > 1$.

Определение. Отображение из одной группы в другую

$$\varphi : (G, *) \to (F, \circ)$$

называется *гомоморфизмом* (Hom), если оно удовлетворяет следующему условию: для любых $g_1, g_2 \in G$

$$\varphi(g_1 * g_2) = \varphi(g_1) \circ \varphi(g_2).$$

Упражнение 10. Докажите следующие свойства гомоморфизма:

1) $\varphi(e_G) = e_F$;

2) $\varphi(g^{-1}) = \big(\varphi(g)\big)^{-1}$.

Определение. Взаимно-однозначный гомоморфизм называется *изоморфизмом*

Определение. *Ядром* гомоморфизма называется следующее множество:

$$\operatorname{Ker} \varphi = \{g \in G : \varphi(g) = e_F\}.$$

Определение. *Образом* гомоморфизма называется следующее множество:

$$\operatorname{Im} \varphi = \{f \in F : \exists\ g \in G,\ f = \varphi(g)\}.$$

Обобщим для гомоморфизма и изоморфизма хорошо известные вам свойства и определения, характерные для функций.

Определение. $\varphi : (G, *) \to (F, 0)$ называется

а) *инъективным* гомоморфизмом, если для любых $g_1, g_2 \in G$, $\varphi(g_1) \neq \varphi(g_2)$;

б) *сюръективным* гомоморфизмом, если для любого $f \in F$ существует $g \in G$: $f = \varphi(g)$;

в) биективным гомоморфизмом или изоморфизмом, если условия а) и б) выполняются одновременно.

Определение. *Композицией* двух гомоморфизмов

$$\varphi_1(G, *) \to (F, \circ), \quad \varphi_2(F, *) \to (H, \cdot)$$

называется гомоморфизм, заданный по правилу

$$\varphi_1 \circ \varphi_2(g) = \varphi_1 \left(\varphi_2(g)\right).$$

Утверждение. *Рассмотрим гомоморфизм*

$$\varphi_1(G, *) \to (F, \circ), \quad \varphi_2(F, \circ) \to (G, *).$$

φ_1 и φ_2 будут являться взаимообразными тогда и только тогда, когда

$$\varphi_1 \circ \varphi_2 = \mathrm{id}_F, \quad \varphi_2 \circ \varphi_1 = \mathrm{id}_G.$$

И в этом случае гомоморфизмы φ_1 и φ_2 являются изоморфизмами.

Данное утверждение доказывается аналогично свойству функций, поэтому проведите его самостоятельно.

Упражнение 11. Сколько элементов содержит полугруппа, состоящая из всех степеней матрицы

$$\begin{Vmatrix} -1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 0 & 0 \end{Vmatrix}?$$

Является ли эта полугруппа группой?

Ответ. а) 3; б) нет.

Упражнение 12. Сколько существует неизоморфных между собой полугрупп порядка 2?

Упражнение 13. Какие из указанных множеств квадратных вещественных матриц фиксированного порядка образуют группу:

а) множество симметрических (кососимметрических) матриц относительно сложения;

б) множество невырожденных матриц относительно сложения;

в) множество матриц с фиксированным определителем d относительно умножения;

г) множество диагональных матриц относительно сложения;

д) множество верхних треугольных матриц относительно умножения;

е) множество верхних нильтреугольных матриц относительно сложения.

Ответ. а), в) при $d \neq 1$; г) при $\lambda < 0$.

Упражнение 14. Пусть X — множество точек кривой $y = x^3$, l — прямая, проходящая через точки $a, b \in X$ (касательная к X при $a = b$), c — ее третья точка пересечения с X и m — прямая, проходящая через начало координат O и точку c (касательная к X при $c = 0$).

Положим $a \oplus b = d$, где d — третья точка пересечения m и X или O, если m касается X в точке O. Доказать, что $(X, \oplus)$ — коммутативная группа.

Упражнение 15. Доказать, что, конечная полугруппа с правыми сокращениями (т. е. из $ba = ca$ следует $b = c$) и хотя бы с одной левой единицей есть группа.

Указание. Рассмотрев Ga, где G — данная полугруппа, показать, что $Ga = G$, т. е. уравнение $xa = b$ разрешается в G при любых a и b. В частности, $xa = e$, где e — левая единица. Однозначность очевидна.

Упражнение 16. Построить пример конечной полугруппы с правыми сокращениями, не являющейся группой.

Ответ. Полугруппа, в которой произведение равно левому сомножителю.

Упражнение 17. Построить пример бесконечной коммутативной полугруппы с единицей и с сокращениями, не являющейся группой.

Ответ. Полугруппа натуральных чисел относительно умножения.

Упражнение 18. Доказать, что непрерывные строго воз-

растающие на отрезке $[0,1]$ функции φ со значениями $\varphi(0)=0$, $\varphi(1)=1$ составляют группу относительно суперпозиции.

Упражнение 19. Установить изоморфизм группы вещественных чисел относительно сложения и группы положительных чисел относительно умножения.

Ответ. Изоморфизм осуществляется показательной функцией.

Упражнение 20. Какие из отображений групп $f:\mathbb{C}^*\to\mathbb{R}^*$ являются гомоморфизмами:

а) $f(z)=|z|$; б) $f(z)=2|z|$;

в) $f(z)=\dfrac{1}{|z|}$; г) $f(z)=1+|z|$;

д) $f(z)=|z^2|$; е) $f(z)=1$; ж) $f(z)=2$?

Ответ. а), д), е).

Упражнение 21. Для каких групп G отображение $f:G\to G$, определенное правилом: а) $f(x)=x^2$, б) $f(x)=x^{-1}$ является гомоморфизмом? При каком условии эти отображения являются изоморфизмами?

Ответ. Для коммутативных групп.

Упражнение 22. Разбить на классы попарно изоморфных групп следующий набор групп:

$\mathbb{Z}$; $n\mathbb{Z}$; $\mathbb{Q}$; $\mathbb{R}$; $\mathbb{C}$; $\mathbb{Q}^*$; $\mathbb{R}^*$; $\mathbb{C}^*$; $\mathbb{UT}_2(A)$,

где A — одно из колец $\mathbb{Z},\mathbb{Q},\mathbb{R},\mathbb{C}$;

G — группа матриц вида $\begin{Vmatrix} x & y \\ -y & x \end{Vmatrix}$,

$(x, y \in \mathbb{R})$ относительно сложения;

G^* — группа ненулевых матриц вида $\begin{Vmatrix} x & y \\ -y & x \end{Vmatrix}$,

$(x, y \in \mathbb{R})$ относительно умножения;

$E(A)$ — группа вещественных чисел вида e^a $(a \in A)$,

где A — одно из колец $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$;

$\mathbb{UT}_2(A)$ — группа унитарных матриц второго порядка.

Ответ.

$\{\mathbb{Z}, n\mathbb{Z}, \mathbb{UT}_2(\mathbb{Z}), E(\mathbb{Z})\}$, $\{\mathbb{Q}, \mathbb{UT}_2(\mathbb{Q}), E(\mathbb{Q})\}$,
$\{\mathbb{R}, \mathbb{UT}_2(\mathbb{R}), E(\mathbb{R})\}$, $\{\mathbb{C}, \mathbb{UT}_2(\mathbb{C}), G, E(\mathbb{C})\}$,
$\{\mathbb{Q}^*\}$, $\{\mathbb{R}^*\}$, $\{\mathbb{C}^*, \mathbb{G}^*\}$.

Упражнение 23. Найти все изоморфизмы между группами $(\mathbb{Z}_4, +)$ и $(\mathbb{Z}_5^*, \cdot)$.

Ответ. $[k] \mapsto [2^k]$ и $[k] \mapsto [3^k]$.

Упражнение 24. Доказать, что группа порядка 6 либо коммутативна, либо изоморфна группе $\mathbb{S}_3$.

Указание. Рассмотреть отдельно два случая:

1) если в группе для любого x: $x^2 = e$;

2) если в группе существует x: $x^2 \neq e$.

Тогда найти некоммутирующие элементы x и y, для которых $x^2 = y^3 = 1$.

Упражнение 25. Найти группы гомоморфизмов:

а) $\mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_6)$; б) $\mathrm{Hom}(\mathbb{Z}_{12}, \mathbb{Z}_{18})$;

в) $\mathrm{Hom}(\mathbb{Z}_6, \mathbb{Z}_{12})$; г) $\mathrm{Hom}(A_1 + A_2, B)$;

д) $\mathrm{Hom}\,(A, B_1 + B_2)$; е) $\mathrm{Hom}\,(\mathbb{Z}_n, \mathbb{Z}_k)$;

ж) $\mathrm{Hom}\,(\mathbb{Z}, \mathbb{Z}_n)$; з) $\mathrm{Hom}\,(\mathbb{Z}_n, \mathbb{Z})$; и) $\mathrm{Hom}\,(\mathbb{Z}, \mathbb{Z})$.

Упражнение 26. Найти все гомоморфные отображения:

а) $\mathbb{Z}_6 \to \mathbb{Z}_6$; б) $\mathbb{Z}_6 \to \mathbb{Z}_{18}$; в) $\mathbb{Z}_{18} \to \mathbb{Z}_6$;

г) $\mathbb{Z}_{12} \to \mathbb{Z}_{15}$; д) $\mathbb{Z}_6 \to \mathbb{Z}_{25}$.

Упражнение 27. Доказать, что если группа G гомоморфно отображена на группу G', причем $a \mapsto a'$, то

а) порядок a делится на порядок a';

б) порядок G делится на порядок G'.

2. Фактор-группы

Пусть G — группа, H — подгруппа $H \subset G$. Пусть $g \in G$.

Рассмотрим множества, заданные следующим образом:

$gH = \{gh | h \in H\}$ — *левый класс смежности*;

$Hg = \{hg | h \in H\}$ — *правый класс смежности*.

Каждый элемент класса называется *представителем* этого класса.

Пусть $x, y \in G$, $xH = yH$, следовательно для всех $h \in H$ существует $h_1 \in H$: $x \cdot h = y \cdot h_1$, тогда

$x^{-1} \cdot x \cdot h \cdot h_1^{-1} = x^{-1} \cdot y \cdot h_1 \cdot h_1^{-1}$, следовательно

$h \cdot h_1^{-1} = x^{-1} \cdot y \in H$, т. к. H — подгруппа.

Это позволяет другим путем прийти к понятию смежных классов.

Именно, с подгруппой H свяжем отношение эквивалентности левой смежности (соответственно правой смежности), полагая по определению

$a \sim b$ тогда и только тогда, когда $a^{-1}b \in H$ — левая смежность;

$a \sim b$ тогда и только тогда, когда $ab^{-1} \in H$ — правая смежность.

Упражнение 28. Доказать, что заданное таким образом отношение является отношением эквивалентности, т.е. симметрично, рефлексивно, транзитивно.

Группа G разбивается на непересеченные классы эквивалентности, т. е. левые смежные классы попарно не пересекаются, и то же верно для правых. Докажите это самостоятельно.

Упражнение 29. Доказать, что левые и правые классы смежности равномощны и их мощность совпадает с мощностью H.

Доказательство. Введем отображение
$\psi\colon gH \to Hg^{-1}$ и докажем, что оно взаимно однозначно, т.е. рассмотрим цепочку отображений

$$gH \xrightarrow{\varphi} Hg^{-1} \xrightarrow{\psi} (g^{-1})^{-1}H = gH, \quad \psi \circ \varphi = \mathrm{id},$$

следовательно ψ и φ — биекция.

Мощность множества смежных классов не зависит от того, левые или правые классы рассматриваются.

Определение. Мощность множества смежных классов называется *индексом* подгруппы $|G : H|$.

Теорема (Лагранжа). *Если* H *— подгруппа конечной группы* G*, то* $|G| = |H| * |G : H|$.

Доказательство. Каждый класс gH и Hg равномощны подгруппе H $(h \in H)$:

$$\left.\begin{array}{l} h \to gh \\ h \to hg \end{array}\right. \text{ — взаимно однозначные соответствия;}$$

$$\left.\begin{array}{c} \varphi : gh \to H, \quad \psi : H \to gH \\ \forall h \in H, \quad gh \to h, \quad h \to gh \\ \varphi \circ \psi = \mathrm{id}, \quad \psi \circ \varphi = \mathrm{id} \end{array}\right| \Rightarrow |gh| = |H|.$$

Таким образом, порядок конечной группы G можно посчитать, умножив мощность каждого класса на число $|G : H|$ всех классов. Доказательство завершено.

Упражнение 30. Доказать, что порядок подгруппы всегда делит порядок группы.

Упражнение 31. Доказать, что порядок всякого элемента делит порядок группы.

Упражнение 32. Доказать, что $|Z : (n)| = n$.

Упражнение 33. Доказать, что Q — не содержит собственных подгрупп конечного индекса.

Упражнение 34. Доказать, что $|Z : (n)| = n$.

Упражнение 35. Доказать, что Q — не содержит собственных подгрупп конечного индекса.

Упражнение 36. Доказать, что $A, B \subset G$ — подгруппы $A \subseteq B$. $|G : B|$, $|B : A|$ — конечны тогда и только тогда, когда $|G : A|$ — конечен, $|G : A| = |G : B| \cdot |B : A|$ — обобщение теоремы Лагранжа.

Упражнение 37. Доказать, что любая подгруппа индекса 2 является нормальной.

Упражнение 38. Найти фактор-группы:
а) $\mathbb{Z}/n\mathbb{Z}$; б) $\mathbb{T}_n/\mathbb{T}_3$; в) $4\mathbb{Z}/12\mathbb{Z}$; г) $\mathbb{R}^*/\mathbb{R}_+$.

3. Нормальная подгруппа

Особенно важную роль в группах играют те подгруппы, относительно которых левые и правые смежные классы совпадают.

Определение. $H \subset G$ — подгруппа группы G называется *нормальной* $H \lhd G$, если для всех $x \in G$: $Hx = xH$ или $x^{-1}Hx = H$.

Определение. Говорят, что элемент a сопряжен с элементом b посредством элемента x, если $a = x^{-1}bx$.

Определение. Операция в G устойчива относительно от-

ношения эквивалентности, если для любых $x, x_1 \in G$, $y, y_1 \in G$ из $x \sim x_1$, $y \sim y_1$ следует $x * y \sim x_1 * y_1$.

Теорема. *Групповая операция в G устойчива относительно введенного отношения эквивалентности тогда и только тогда, когда $H \lhd G$.*

Доказательство. Докажем необходимость. Пусть операция в G — устойчива относительно отношения эквивалентности для всех $g \in G$, для всех $h \in H$, $e \sim h$, т.е. $eH = hH = H$, $g \sim g$ — рефлекисвность. Следовательно, по свойству устойчивости операции $eg \sim hg$, следовательно $(eg)^{-1} \cdot hg \in H$, откуда $H \lhd G$.

Докажем достаточность. $H \lhd G$, это означает, что необходимо доказать следующее:

$$\left.\begin{array}{l} xH = x_1H \\ yH = y_1H \end{array}\right| \quad \Leftrightarrow \quad xyH = x_1y_1H\,.$$

$(xH)(yH) = (x_1H)(y_1H) = x_1(Hy_1)H = x_1y_1H$.

Доказательство завершено.

Определение. Операцией *умножения* на множестве классов эквивалентности называется $(xH)(yH) = xyH$.

Из доказанного выше видно, что операция определена корректно.

Утверждение. *Пусть $H \lhd G$, следовательно ${}^{G}\!/_{H}$ — группа.*

Докажите это утверждение самостоятельно.

Утверждение. *Пусть* $\varphi : G \xrightarrow{\text{Hom}} M$, *тогда* $\operatorname{Ker}\varphi \lhd G$.

Доказательство. Пусть $x \in G$, $h \in \operatorname{Ker}\varphi$, Докажем, что $x^{-1}hx \in \operatorname{Ker}\varphi$.

$\varphi(x^{-1}hx) = \varphi(x^{-1})\varphi(h)\varphi(x) = \big(\varphi(x)\big)^{-1} e_M \cdot \varphi(x) =$

$= \varphi(x^{-1} \cdot x) = \varphi(e_G) = e_M$.

Доказательство завершено.

Следствие. ${}^{G}\!/_{\operatorname{Ker}\varphi}$ — группа.

Определение. Группы, не содержащие собственных нормальных подгрупп, называются *простыми*.

Примеры.

1) Любая подгруппа абелевой группы нормальна.

2) $A_n \lhd S_n$.

3) p — простое, Z_p — простая.

4) $|G : H| = 2$, следовательно $H \lhd G$.

Упражнение 39. Найти фактор-группы:

а) $\mathbb{Z}/n\mathbb{Z}$; б) $\mathbb{T}_{12}/\mathbb{T}_3$; в) $4\mathbb{Z}/12\,\mathbb{Z}$; г) $\mathbb{R}^*/\mathbb{R}_+$.

Ответ.

а) $\mathbb{Z}_n$; б) $\mathbb{Z}_4$; в) $\mathbb{Z}_3$; г) $\mathbb{Z}_2$.

Упражнение 40. Доказать, что в группе $\mathbb{Q}/\mathbb{Z}$

а) каждый элемент имеет конечный порядок;

б) для каждого натурального n имеется в точности одна подгруппа порядка n.

Указание. В единственную подгруппу порядка n попадают все смежные классы вида $\frac{k}{n}$, где k — любое целое число.

4. Первая теорема об изоморфизме групп

Пусть G — группа, H — нормальная подгруппа группы G, ${}^{G}\!/_{H}$ – фактор-группа, т.е ${}^{G}\!/_{H} = \{gH | g \in G\}$.

Определение. Зададим отображение следующим образом:

$$\mathscr{P} : G \to {}^{G}\!/_{H},$$
$$g \to gH.$$

Данное отображение называется *канонической проекцией или естественным отображением.*

Упражнение 41. Доказать, что $\mathscr{P}$ — эпиморфизм групп и $\operatorname{Ker} \mathscr{P} = H$.

Доказательство. Докажем, что $\mathscr{P}$ — Hom .

Пусть $g_1, g_2 \in G$. По определению $\mathscr{P}(g_1) = g_1 H$, $\mathscr{P}(g_2) = g_2 H$.

$\mathscr{P}(g_1 g_2) = g_1 \cdot g_2 H = g_1 H \cdot g_2 H = \mathscr{P}(g_1) \cdot \mathscr{P}(g_2)$.

Докажем, что $\mathscr{P}$ — эпиморфизм.

Пусть $gH \in {}^{G}\!/_{H}$, $\mathscr{P}(g) = gH \in \operatorname{Im} \mathscr{P}$.

Пусть $g \in \operatorname{Ker} \mathscr{P}$, $\mathscr{P}(g) = e_{{}^{G}\!/_{H}} = H$, тогда $g \in H$, $\operatorname{Ker} \mathscr{P} \subset H$.

Пусть $g \in H$. $\mathscr{P}(g) = gH = H$, тогда $H \subset \operatorname{Ker} \mathscr{P}$, следовательно $\operatorname{Ker} \mathscr{P} = H$. Доказательство завершено.

Теорема (1-ая теорема об изоморфизме). *Пусть* $\varphi : G \xrightarrow{\text{Hom}} F$, *тогда* ${}^{G}\!/_{\text{Ker}\,\varphi} \approx \text{Im}\,\varphi$.

Доказательство. Диаграмма 1-ой теоремы:

где f — изоморфизм.

Зададим f следующим образом.

Для всех $gH \in {}^{G}\!/_{H}$, $f(gH) = \varphi(g)$ — по определению. Необходимо проверить:

1. Корректность определения f;
2. f — Hom;
3. f — эпиморфизм;
4. f — мономорфизм.

Перейдем к последовательному доказательству перечисленных выше утверждений.

1. $g'H = gH \xrightarrow{f} \varphi(g)$, $g'H = gH \xrightarrow{f} \varphi(g')$. Докажем, что образы равных классов тоже равны, т.е. $\varphi(g) = \varphi(g')$.

$g' \in gH$, тогда и только тогда, когда существует $h \in H$: $g' = gh$. $\varphi(g') = \varphi(gh) = \varphi(g)\varphi(h) = \varphi(g)$ (где φ — Hom, $gH = \operatorname{Ker}\varphi$).

2. Для всех g_1H, g_2H, $f\big((g_1H)(g_2H)\big) = f(g_1H)f(g_2H)$ — докажем.

   $f\big((g_1H)(g_2H)\big) = f(g_1g_2H) = \varphi(g_1g_2) = (\varphi - \text{Hom}) =$
   $= \varphi(g_1)\varphi(g_2) = f(g_1H)f(g_2H)$.

3. Пусть $\varphi(g) \in \operatorname{Im}\varphi$, существует gH: $f(gH) = \varphi(g)$, следовательно f — сюрьекция, т. е. эпиморфизм.

4. Пусть $f(g_1H) = f(g_2H)$, докажем, что $g_1H = g_2H$. $f(g_1H) = \varphi(g_1)$, $f(g_2H) = \varphi(g_2)$, следовательно

   $\varphi(g_1) = \varphi(g_2)$; $\varphi(g_1)^{-1}\varphi(g_1) = \varphi(g_1)^{-1}\varphi(g_2)$,

   $\varphi(g_1^{-1}g_1) = e_F = \varphi(g_1^{-1}g_2)$, следовательно $g_1^{-1}g_2 \in H$, тогда $g_1 \sim g_2$, откуда $g_1H = g_2H$, следовательно f — инъекция.

Эта теорема позволяет избавиться от фактор-группы и рассмотреть изоморфную ей группу. Проиллюстрируем это на конкретных примерах.

Пример 1. $\varphi : Z \to C^*$.
$k \to \varphi(k) = \cos\frac{2\pi k}{n} + \sin\frac{2\pi k}{n} = \varepsilon_k$, $n > 0$.

Нетрудно проверить, что φ — Hom. Каждому целому числу ставим в соответствие корень n-степени из 1 с индексом k.

$\varphi(k_1+k_2)=\varepsilon_{k_1+k_2}$, $\varphi(k_1+k_2)=\varphi(k_1)\varphi(k_2)=\varepsilon_{k_1}\varepsilon_{k_2}$,

$\operatorname{Ker}\varphi=\{k|\varphi(k)=1\}=nZ$.

Множество всех чисел кратных n.

$\operatorname{Im}\varphi=T_n$ — множество корней n-степени из 1.

По первой теореме об изоморфизме ${}^{Z}\!/_{nZ}\approx T_n$.

Пример 2. $\varphi: C^*\to C^*$.

$z\to\dfrac{z}{|z|}=\varphi(z)$.

$\operatorname{Ker}\varphi=\{z:\varphi(z)=1\}$.

$\dfrac{z}{|z|}=1\ \Leftrightarrow\ z=|z|$.

Равенство выполнится, если $z\in R_+$, $\operatorname{Ker}\varphi\in R_+$,

$\operatorname{Im}\varphi=\left\{\dfrac{z}{|z|}=1\right\}=T$, следовательно ${}^{C^*}\!/_{R_+}\approx T$.

Аналогично докажите следующее утверждение.

Упражнение 42. Пусть H_n — множество чисел с аргументами вида $2\pi k/n$ ($k\in\mathbb{Z}$). Доказать, что

а) $\mathbb{R}/\mathbb{Z}\simeq\mathbb{T}$; б) $\mathbb{C}^*/\mathbb{T}\simeq\mathbb{R}_+$; в) $\mathbb{T}/\mathbb{T}_n\simeq\mathbb{T}$;

г) $\mathbb{C}^*/\mathbb{T}_n\simeq\mathbb{C}^*$; д) $\mathbb{C}^*/H_n\simeq\mathbb{T}$;

е) $H_n/\mathbb{R}_+\simeq\mathbb{T}_n$; ж) $H_n/\mathbb{T}_n\simeq\mathbb{R}_+$.

Указание. Рассмотреть отображения:

а) $x\mapsto\cos 2\pi x+i\sin 2\pi x$; б) $z\mapsto|z|$;

в) $z\mapsto z^n$; г) $z\mapsto z^n$; д) $z\mapsto\left(\dfrac{z}{|z|}\right)^n$;

е) $z\mapsto\dfrac{z}{|z|}$; ж) $z\mapsto|z|$.

Упражнение 43. Доказать, что фактор-группа груп-

пы $\mathbb{S}_4$ по нормальной подгруппе $\{e, (12)(34), (13)(24), (14)(23)\}$ изоморфна группе $\mathbb{S}_3$.

Указание. Группа $\mathbb{S}_4$ действует на кубе. Отсюда, если занумеровать три пары противоположных граней куба числами 1, 2, 3, мы получаем действие группы на множестве 1, 2, 3. Проверить, что ядром этого действия является подгруппа $\mathbb{V}_4$.

5. Вторая теорема об изоморфизме групп

Теорема (2-ая теорема об изоморфизме). *Если* $H \lhd G$, $A \lhd G$, $H \subseteq A$, *то* ${}^{(G/H)}/_{(A/H)} \approx {}^{A}/_{H}$.

Доказательство. Пусть $\varphi : {}^{G}/_{H} \to {}^{A}/_{H}$, $\varphi(xH) = xA$ для всех $x \in G$.

Корректность: $xH = yH$, следовательно $x^{-1}y \in H \subset A$, откуда $xA = yA$.

φ — сохраняет умножение, т. е. φ — Hom.

$\varphi(xH \cdot yH) = \varphi(xyH) = xyA = xA \cdot yA$.

Очевидно $\operatorname{Ker}\varphi = {}^{A}/_{H}$, тогда ${}^{A}/_{H} \lhd {}^{G}/_{H}$ — ${}^{(G/H)}/_{(A/H)} \approx {}^{G}/_{A}$.

6. Группы, порожденные множеством

Упражнение 44. G — группа, H_1, H_2 — подгруппы, тогда $H_1 \cap H_2$ — подгруппа.

Упражнение 45. $H_\alpha \subset G$ — подгруппа. J — множество индексов $\bigcap\limits_{\alpha \in J} H_\alpha$ — подгруппа.

Пусть $M \subset G$ — подмножество группы G.

Определение. Пересечение всех подгрупп, содержащих M, называется *подгруппой*, порождённой множеством M.

M — называется *порождающим множеством* подгруппы (M), а элементы множества M называются *порождающими элементами.*

Теорема 1. *M — подмножество группы G, тогда*

$$(M) = \{a_1^{\varepsilon_1}, a_2^{\varepsilon_2}, \ldots, a_m^{\varepsilon_m} | a_i \in M, \varepsilon_i = \pm 1, m = 1, 2, \ldots\}$$

Доказательство. Обозначим правую часть через H, т. к. подгруппа (M) содержит все a_i из M, то $H \subseteq M$.

С другой стороны для всех h при $m = 1$, $\varepsilon = 1$, для всех $a_1 \in H$ следует, что $M \subseteq H$.

Очевидно, что H — подгруппа, содержащая M, и $M = H$,

Пример 3. $S_3 = \{e, (12), (13), (23), (123), (132)\}$.

Найдите все нетривиальные подгруппы:

$H_1 = \{e, (12)\}$;

$H_2 = \{e, (13)\}$;

$H_3 = \{e, (23)\}$, $A_3 = \{e, (123), (132)\}$,

$\langle N_1 \rangle = A_3$, $\quad \langle N_2 \rangle = S_3$;

$M_1 = \{(123), (132)\}$, $\quad M_2 = \{(12), (123)\}$;

M_2 — не $\min$, т. к. ${}^{M_2}\!/_{(12)} = M_2'$;

$\langle M_2' \rangle = A_3 \neq S_3$, $\quad {}^{M_2}\!/_{(123)} = M_2''$;

$\langle M_2'' \rangle \neq S_3$.

Определение. Система образующих называется *минимальной системой образующих*, если из множества S нельзя удалить ни одного элемента без того, чтобы это множество не перестало быть системой образующих.

Пример 4.

$Z = (1)$;

$Z(n) = (1(\mathrm{mod}\ n))$;

$Q = \left(\frac{1}{n} | n = 1, 2, \ldots\right)$.

Пример 5.

$Z^* = (-1)$;

$Q^* = (-1, 2, 3, 5, 7, 11, \ldots)$.

Антиподом порождающих множеств является подгруппа Фраттини.

Определение. $H \subset G$ — подгруппа называется *максимальной* среди подгрупп со свойством G, если

1) $H \subset G$;

2) не существует H' со свойством G: $H \subset H' \subset G$.

Если G такое свойство, что им обладают все подгруппы, то H называется просто *максимальным*. Вообще говоря, максимальных подгрупп может не существовать.

Определение. Подгруппа Фраттини $\Phi(G)$ группы G — это пересечение всех ее максимальных подгрупп, если они существуют. В противном случае, это сама группа G.

Определение. Элемент $x \in G$ называется *непорождающим элементом* группы G, если его можно удалить из любого множества порождающих элементов группы G, в которое он входит.

Теорема 2. *Множество S всех непорождающих элементов группы G совпадает с подгруппой Фраттини.*

Пример 6. В $Z(p)$ — $\max$, $\Phi(Z) = 0$.

В Q — для всех элемент порождает $\Phi(Q) = 0$.

Упражнение 46. Доказать, что

а) если в коммутативной группе элементы a, b связаны соотношениями $a^3 = b^5 = (ab)^7 = e$, то $a = b = e$;

б) подгруппа, порожденная в $\mathbb{S}_7$ перестановками $(1\,2\,3)$ и $(1\,4\,5\,6\,7)$, не является разрешимой;

в) группа с порождающими элементами x_1, x_2 и определяющими соотношениями $x_1^3 = x_2^5 = (x_1x_2)^7 = e$ не является разрешимой.

Упражнение 47. Доказать, что если между элементами a и b группы выполнены соотношения $a^3 = b^2 = 1$, $b^{-1}ab = a^2$, то $a = 1$.

Упражнение 48. Показать, что группа, порожденная элементами a, b с соотношениями $a^2 = b^7 = 1$, $a^{-1}ba = b^{-1}$, конечна.

Упражнение 49. Доказать, что группа, заданная порождающими элементами x_1 и x_2 и определяющими соотношения-

ми: а) $x_1^2 = x_2^2 = (x_1x_2)^2 = 1$; б) $x_1^2 = x_2^2 = 1$, $x_1^{-1}x_2x_1 = x_2^2$, изоморфна $\mathbb{S}_3$.

7. Цикличсекие группы

Пусть G — группа $\{x\} = M$, $x \in G$,

$$\langle M\rangle = \langle x\rangle = \{x \dots xx^{-1} \dots | x^n, n \in Z\}.$$

Определение. Подгруппа, порожденная одним элементом, называется *циклической*.

Примеры — Z, Z_n.

Определение. Если для каждого положительного числа n, $x^n \neq e$, то говорят, что элемент x имеет *бесконечный порядок* и обозначают $|x| = \infty$.

Определение. Наименьшее натуральное число n, для которого $x^n = e$, называется *порядком* элемента x.

Упражнение 50. Пусть $a \in \mathbb{Z}$ — целое число и $|x| = n$, тогда $x^a = e$ тогда и только тогда, когда $a \equiv 0(\mathrm{mod}\ n)$.

Доказательство. Пусть $a = nk$, $x^a = (x^n)^k = e$, т. к. $x^n = e$.

Пусть $x^a = e$, $a = nq + r$, $0 \leqslant r < n$, $e = a^{nq+r} = a^r = e$ — противоречит определению порядка, следовательно $a \equiv 0(\mathrm{mod}\ n)$.

Упражнение 51. Пусть $|x| = n$; $a, b \in \mathbb{Z}$, $x^a = x^b$ тогда и только тогда, когда $a \equiv b(\mathrm{mod}\ n)$.

Доказательство. $x^{a-b} = e$; $a - b \equiv 0 (\mathrm{mod}\ n)$, следовательно $a \equiv b (\mathrm{mod}\ n)$.

Упражнение 52. Найти порядок элемента группы:

а) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \in \mathbb{S}_5$; б) $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 4 & 5 & 1 & 6 \end{pmatrix} \in \mathbb{S}_6$;

в) $\frac{-\sqrt{3}}{2} + \frac{1}{2}i \in \mathbb{C}^*$; г) $\frac{1}{\sqrt{2}} - \frac{1}{2}i \in \mathbb{C}$;

д) $\begin{Vmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \end{Vmatrix} \in \mathbb{CL}_4(\mathbb{R})$;

е) $\begin{Vmatrix} 0 & i \\ 1 & 0 \end{Vmatrix} \in \mathbb{GL}_2(\mathbb{C})$; ж) $\begin{Vmatrix} -1 & a \\ 0 & 1 \end{Vmatrix} \in \mathbb{GL}_2(\mathbb{C})$.

Указание. а) 6; б) 5; в) 12; г) 8; д) 4; е) 8; ж) 2.

Упражнение 53. Доказать, что

а) элемент $\frac{3}{5} + \frac{4}{5}i$ группы $\mathbb{C}^*$ имеет бесконечный порядок;

б) число $\frac{1}{\pi} \operatorname{arctg} \frac{4}{3}$ иррационально.

Упражнение 54. Сколько элементов порядка 6 содержится в группе:

а) $\mathbb{C}^*$; б) $\mathbb{S}_5$; в) $\mathbb{A}_5$?

Упражнение 55. Доказать, что во всякой группе

а) элементы xy и yx имеют один и тот же порядок;

б) элементы x и yxy^{-1} имеют один и тот же порядок;

в) элементы xyz и zyx могут иметь разные порядки.

Указание.

а) Умножить равенство $(xy)^n = e$ слева на y справа на x;

б) использовать а);

в) рассмотреть перестановки $(1\,2\,3)$, $(1\,2)$ и $(1\,3)$.

Упражнение 56. Пусть элементы x и y группы G имеют конечный порядок и $xy = yx$. Доказать, что

а) если порядки элементов x и y взаимно просты, то порядок произведения xy равен произведению их порядков;

б) существуют показатели k и l такие, что порядок произведения xy равен наименьшему общему кратному порядков x и y;

в) верны ли эти утверждения для некоммутирующих элементов x и y?

Указание.

а) Для взаимно простых чисел p и q существуют u и v такие, что $pu + qv = 1$;

б) следует из а).

Упражнение 57. Доказать, что

а) если элемент x группы G имеет бесконечный порядок, то $x^k = x^l$ тогда и только тогда, когда $k = l$;

б) если элемент x группы G имеет порядок n, то $x^k = x^l$ тогда и только тогда, когда $n|k - l$;

в) если элемент x группы G имеет порядок n, то $x^k = e$ тогда и только тогда, когда $n|k$.

Упражнение 58. Найти порядок элемента x^k, если порядок элемента x равен n.

Ответ. $^{n}/_{\text{НОД}(n,k)}$.

Теорема 3. *Пусть* $H = \langle x \rangle \subset G$, *тогда:*

1) *если* $|x| = \infty$, *то* G — *бесконечная циклическая группа, и* $H \approx Z$;

2) *если* $|x| = n$, *то* H — *конечная циклическая группа, и*

$H \approx Z_n = {}^{Z}/_{nZ}$ — *группа классов вычетов.*

$H = \{x^0 = e, x, x^2, \ldots, x^{n-1}\}$.

Доказательство. Пусть $\varphi : Z \to H$; $a \to \varphi(a) = x^a$; φ — $\operatorname{Hom} \varphi(a+b) = \varphi(a) + \varphi(b)$ (из правил действия со степенями). φ — эпиморфизм (сюръекция Hom).

Так как H — циклическая группа, то $\operatorname{Im} \varphi = H$.

1) Если $|x| = \infty$, то $x^a = e$ тогда и только тогда, когда $a = 0$. Следовательно, $\operatorname{Ker} \varphi = \{0\}$ — нулевая подгруппа.

2) Пусть $|x| = n < \infty$, $x^a = e$ тогда и только тогда, когда $a \equiv 0 (\operatorname{mod} n)$. $\operatorname{Ker} \varphi = nZ$ (по первой теореме об изоморфизме).

${}^{Z}/_{\operatorname{Ker} \varphi} \approx \operatorname{Im} \varphi = H$.

1. ${}^{Z}/_{\{0\}} = Z$.

2. $^{Z}/_{nZ} \approx H$.

Осталось показать, что все элементы можно записать:

$H = \{x^0 = e, x, x^2, \ldots, x^{n-1}\}$, но т. к. $0, 1, \ldots, n-1$ не сравнимы друг с другом, то $x^0, x, x^2, \ldots, x^{n-1}$ — различные элементы.

Следствие. Порядок элемента равен порядку циклической группы, порожденной этим элементом.

Следствие. Порядок элемента делит порядок группы.

Теорема 4. *Пусть* $G = \langle x \rangle$ — *циклическая группа.*

1. Любая подгруппа $H \subset G$ — сама циклическая.

2. Любой элемент бесконечной циклической группы, кроме единственного, имеет бесконечный порядок.

3. Пусть $|G| = n$, тогда между всеми делителями $^{d}/_{n}$ и всеми подгруппами G существует взаимнооднозначное соответствие, причем

   $$^{d}/_{n} \leftrightarrow H_d\,,\ |H_d| = d \text{ и } H_d = \left\langle x^{\frac{n}{d}} \right\rangle,\ H_d = \left\{ e, x^{\frac{2n}{d}}, \ldots, x^{\frac{d-1}{d}n} \right\}.$$

4. Пусть $|G| = n$, тогда число образующих циклической группы G равно $\varphi(n)$, где φ — функция Эйлера.

5. $\Phi(d) = \{x \in G \mid |x| = d\}$, $|\Phi(d)| = \varphi(d)$.

   $\sum\limits_{d|n} \varphi(d) = |G| = n$.

Доказательство.

1. Любая подгруппа циклической группы циклическая.

Пусть $G = \langle x \rangle$, H — подгруппа.

1) $H = \{e\}$ — циклическая.

2) $H \neq \{e\}$, существует $y \in G$, $y \neq e$, $y \in H$, существует $n \in Z$: $y = x^n$, т. к. H — подгруппа $y^{-1} = x^{-n} \in H$, n — целое положительное число.

Пусть m — наименьшее положительное число, для которого $x^m \in H$, $x^{m-1} \notin H$, $\langle x^m \rangle \subset H$.

Докажем, что $H \subset \langle x^m \rangle$.

Пусть $z \in H$, $z = x^a$, $a \in \mathbb{Z}$, $a = mq + r$, $0 \leqslant r < m$;
$x^r = x^{a-mq} = x^a \cdot (x^m)^{-q} \in H$, т. к. $x^a \in H$, $(x^m)^{-q} \in H$,
следовательно $r = 0$, $a = mq$, $z = x^a = (x^m)^q$,
$H \subset \langle x^m \rangle = H = \{x^m\}$.

2. Пусть $G = \langle x \rangle$, $|x| = \infty$, пусть $y \in G$, $y \neq e$. Докажем, что $|y| = \infty$. Пусть существует $n < \infty$: $|y| = n$, $\Leftrightarrow$ $y^n = e$; существует k: $y = x^k$, следовательно $y^n = x^{nk} = 1$, тогда $|x| < \infty$ — противоречие.

3. Пусть d — делитель n. Поставим ему в соответствие циклическую группу $H = \left\langle x^{\frac{n}{d}} \right\rangle$,

$|H| = d$, $G = \langle x \mid x^n = 1 \rangle = \{1, x, \ldots, x^{n-1}\}$.

Пусть $H \subset G$ — произвольная подгруппа. $H = \langle x^m \rangle$, m — минимальное положительное число $x^m \in H$.

Докажем, что m делит n, $n = mq + r$, $0 \leqslant r < n$.

$x^r = x^{n-mq} = x^n(x^m)^{-q} \in H$, следовательно $r = 0$, ($x^n = e \in H$, $(x^m)^{-q} \in H$). $n = md$, $|x^m| = d$, $(x^m)^k = 1 \;\; mk \equiv 0(\mathrm{mod}\ n)$.

Наименьшее положительное $k = d$.

$y^m = |\langle x^m \rangle| = d$, $\langle x^m \rangle = |H|$, $H = \{1, x^m, (x^m)^2, \ldots, (x^m)^{d-1}\}$.

Пусть d — произвольный делитель числа n. Следовательно $n = md$. Рассмотрим циклическую группу $H = \langle x^m \rangle$.

Просто рассмотрев последовательные степени элемента x^m, получим: $x^m, x^{2m}, \ldots, x^{(d-1)m}$ — единицу не дают $(x^m)^d = 1$. С другой стороны получим тот же самый результат.

4. Пусть $|G| = n$, тогда число образующих циклическую группу G равно $\varphi(n)$, где φ — функция Эйлера.

$G = \langle x | x^n = 1 \rangle = \{1, x, \ldots, x^{n-1}\}$.

Докажем, что $|x^k| = n$ тогда и только тогда, когда

$(k, n) = 1$; $k = 0, 1, \ldots, n-1$.

Пусть $(x^k)^m = 1$, тогда $x^{km} = 1$, $km \equiv 0(\mathrm{mod}\ n)$.

Пусть $(k, n) = 1$, тогда $m \equiv 0(\mathrm{mod}\ n)$, $m \geqslant n$, т.е. x^k — образующая группы G. Пусть $|x^k| = n$ и $(k, n) = d > 1$.

$k = k_1 \cdot d$, $n = n_1 \cdot d$. $(x^k)^{n_1} = x^{k_1(d \cdot n_1)} = (x^n)^{k_1} = 1$.

$y = x_k$, $|y| \leqslant n_1$ — противоречие, следовательно $(k, n) = 1$.

Доказать данное утверждение можно было другим способом, а именно задать изоморфизм по следующему правилу.

$G \approx T_n = \{1, \varepsilon_1, \varepsilon_1^2, \ldots, \varepsilon_1^{n-1}\}$, $x^m \to \varepsilon_1^m$.

Таким образом, можно сделать вывод, что изоморфизм сохраняет порядок элемента.

Упражнение 59. Доказать, что φ — изоморфизм, $|\varphi(y)| = |y|$.

5. $\Phi(d_1) \cap \Phi(d_2) = \emptyset$, $d_1 \neq d_2$ по 4-му свойству теоремы, следовательно $|\Phi(d) = \varphi(d)|$, $|G| = \sum\limits_{d|n} \varphi(d)$.

Упражнение 60. Описать правые классы смежности при разложении группы G по подгруппе H:

a) G — циклическая группа $\mathbb{Z}_8$ восьмого порядка, H — ее подгруппа четвертого порядка;

b) $G = \mathbb{S}_3$, H — подгруппа, порожденная транспозицией (12);

c) G — группа вращений куба, H — ее подгруппа, совмещающая с собой одну из граней куба;

d) G — группа всех невырожденных вещественных матриц, H — подгруппа матриц с определителем 1.

Ответ.

a) $H = \{1, a^2, a^4, a^6\}$, $Ha = \{a, a^3, a^5, a^7\}$, где a — образующая.

b) $H = \{1, (12)\}$, $H\sigma = \{(123), (13)\}$, $H\sigma^2 = \{(132)(23)\}$, $\sigma = (123)$.

c) H — циклическая группа порядка 4. Элементы, составляющие один класс смежности, — вращения, переводящие исходную грань в какую-либо другую.

d) Классы смежности — множества матриц с фиксированным определителем.

Упражнение 61. Доказать, что если порядок конечной

абелевой группы делится на простое число p, то в группе найдется элемент порядка p.

Указание. Для циклической группы доказывается непосредственно. Для нециклической — применить метод индукции, рассмотрев циклическую подгруппу и фактор-группу по ней.

Упражнение 62. В циклической группе $\langle a\rangle$ порядка n найти все элементы g, удовлетворяющие условию $g^k = e$, и все элементы порядка k при

а) $n = 24$, $k = 6$; б) $n = 24$, $k = 4$;

в) $n = 100$, $k = 20$;

г) $n = 100$, $k = 5$; д) $n = 360$; $k = 30$;

е) $n = 360$, $k = 12$; ж) $n = 360$, $k = 7$.

Указание. Если $x^k = e$ и $x = a^l$, то $a^{kl} = e$, откуда $kl|n$ и $l|\text{НОД}(n,k)$; элемент a^k имеет порядок $n/\text{НОД}(n,k)$ и поэтому удовлетворяет условию при $\text{НОД}(n,l) = n/k$.

Упражнение 63. Найти все подгруппы в циклической группе порядка:

а) 24; б) 100; в) 360; г) 125; д) p^n (p — простое число).

Указание. Во всех случаях $\{\langle a^d\rangle | d|n\}$, где n — порядок группы.

Упражнение 64. Какие из групп $\langle g\rangle$, порожденных элементом $g \in G$, изоморфны:

а) $G = \mathbb{G}^*$, $g = -\frac{1}{\sqrt{2}} + \frac{1}{\sqrt{2}}i$; б) $G = \mathbb{GL}_2(\mathbb{C})$, $g = \begin{Vmatrix} 0 & 1 \\ i & 0 \end{Vmatrix}$;

в) $G = \mathbb{S}_6$, $g = (3\,2\,6\,5\,1)$; г) $G = \mathbb{C}^*$, $g = 2 - i$;
д) $G = \mathbb{R}^*$, $g = 10$; е) $G = \mathbb{C}^*$; $g = \cos\frac{6\pi}{5} + i\sin\frac{6\pi}{5}$;
ж) $G = \mathbb{Z}$, $g = 3$?

Ответ.

а) $\simeq$ б); в) $\simeq$ е) г) $\simeq$ д) $\simeq$ ж).

Упражнение 65. Доказать, что

а) во всякой группе четного порядка имеется элемент порядка 2;

б) группа, в которой все элементы имеют порядок 2, коммутативна.

Указание. а) Если в группе G нет элементов порядка 2, то $G = \{(x, x^{-1})\ (x \neq e)\} \cup \{e\}$ и G нечетен;

Упражнение 66. Доказать, что всякая конечная подгруппа группы $\mathbb{C}^*$ — циклическая.

Указание. Если порядок подгруппы H равен n, то $x^n = e$ для любого $x \in H$, откуда $H \subset \mathbb{T}_n$.

Упражнение 67. Найти все подгруппы в группах

а) $\mathbb{S}_3$; б) $\mathbb{D}_4$; в) $\mathbb{Q}_8$; г) $\mathbb{A}_4$.

Ответ.

а) E, $\mathbb{S}_3$, $\langle(i\,j)\rangle$, $\langle(1\,2\,3)\rangle$;

б) E, $\mathbb{D}_4$, $\langle(1\,3)\rangle$, $\langle(2\,4)\rangle$, $\langle(1\,2)(3\,4)\rangle$, $\langle(1\,3)(2\,4)\rangle$, $\langle(1\,4)(2\,3)\rangle$, $\langle(1\,2\,3\,4)\rangle$, $\mathbb{V}_4$;

в) E, $\mathbb{Q}_8$, $\langle i\rangle$, $\langle j\rangle$, $\langle k\rangle$;

г) E, $\mathbb{A}_4$, $\langle(1\,2)(3\,4)\rangle$, $\langle(1\,3)(2\,4)\rangle$, $\langle(1\,4)(2\,3)\rangle$, $\mathbb{V}_4$, $\langle(1\,2\,3)\rangle$, $\langle(1\,2\,4)\rangle$, $\langle(1\,3\,4)\rangle$, $\langle(2\,3\,4)\rangle$.

8. Действия с подмножествами группы

Пусть G — группа, $H, N, M \subset G$ — подмножества.
$N \cdot M = \{n \cdot m | n \in N, m \in M\}$ (по определению).
$M^{-1} = \{m^{-1} | m \in M\}$.

1. Ассоциативность умножения: $H \cdot (N \cdot M) = (H \cdot N) \cdot M$;
2. $(M^{-1})^{-1} = M$;
3. $(N \cdot M)^{-1} = M^{-1} \cdot N^{-1}$;
4. Если $H \subset G$ — подгруппа группы G, то $H \cdot H = H$; $H^{-1} \cdot H = H$; $H^{-1} = H$;
5. Если $H^{-1} \cdot H \subset H$, следовательно H — подгруппа G, и $H \neq \emptyset$;
6. Если $H \lhd G$, M — произвольное подмножество, то $H \cdot M = M \cdot H$;
7. Если $H \lhd G$, K — произвольная подгруппа, то $H \cdot K$ — подгруппа G.

Доказательство. 4. 1) Для любых $h_1, h_2 \in H$, т. к. H — подгруппа, следовательно $H \cdot H \subseteq H$, $e \in H$, для всех $h \in H$: $e \cdot h \in H \cdot H$, значит $H \subseteq H \cdot H$, $(e \cdot h = h)$.

2) $H^{-1} = H$; $H^{-1} \subseteq H$, т. к. обратный элемент, принадлежащий своей подгруппе.

$H \subset H^{-1}$, для всех $h = (h^{-1})^{-1} \in H$.

3) $H^{-1} \cdot H = H$ (доказывается по аналогии с 1), 2)).

5. Пусть $H^{-1} \cdot H \subset H$.

Докажем, что H — подгруппа, для всех $x, y \in H$, $x \cdot y^{-1} \in H$.

Пусть $h \in H$, $h^{-1} \in H^{-1}$, $h^{-1} \cdot h = e \in H^{-1} \cdot H \subset H$,

т. к. $e \in H$: $h^{-1} = h^{-1} \cdot e \in H^{-1} \cdot H \subset H$,

следовательно $h^{-1} \in H$.

Пусть $a \cdot b \in H \cdot K$, $a \in H$, $b \in K$:

$(a \cdot b)^{-1} = b^{-1} \cdot a^{-1} = (b^{-1} \cdot a^{-1} \cdot b) \in H$, т. к. $H \lhd G$.

$b^{-1} \in K$, следовательно $(a \cdot b)^{-1} \in H \cdot K$.

Пусть $a_1 \cdot b_1, a_2 \cdot b_2 \in H \cdot K$:

$(a_1 \cdot b_1)(a_2 \cdot b_2) = a_1(b_1 \cdot b_1^{-1}) \cdot b_1 \cdot b_2$, т.к. $H \lhd G$,

то $b_1 \cdot a_2 \cdot b^{-1} \in H$ и $b_1 \cdot b_2 \in K$.

Следовательно $(a_1 \cdot b_1)(a_2 \cdot b_2) \in H \cdot K$.

Замечание. Произведение двух подгрупп не обязательно будет подгруппой, если ни одна из них нормальной не является

Пример 7. $H = \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix}$ — множество диагональных матриц.

$$K = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}, \quad K^2 = \begin{pmatrix} -1 & -1 \\ 1 & 0 \end{pmatrix} \quad K^3 = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix};$$

$$H \cdot K = \left\{ \begin{pmatrix} 0 & b_1 \\ -b_2 & -b_2 \end{pmatrix}; \quad \begin{pmatrix} -b_1 & -b_1 \\ b_2 & 0 \end{pmatrix}; \quad \begin{pmatrix} b_1 & 0 \\ 0 & b_2 \end{pmatrix} \right\};$$

Если $b_1 \neq b_2$:

$$\begin{pmatrix} 0 & b_1 \\ -b_2 & -b_2 \end{pmatrix}; \quad \begin{pmatrix} -b_1 & -b_1 \\ b_2 & 0 \end{pmatrix} = \begin{pmatrix} b_1 \cdot b_2 & 0 \\ b_1 \cdot b_2 - b_2^2 & b_1 \cdot b_2 \end{pmatrix} \notin H \cdot K,$$

следовательно $H \cdot K$ — не группа.

9. Третья теорема об изоморфизме

Теорема 5. *$H, K \subset G$ — подгруппа группы $GH \lhd G$, ${}^{KH}\!/_{H} \approx {}^{K}\!/_{K \cap H}$.*

Доказательство. Пусть $\varphi : G \xrightarrow{\text{Hom}} S$, $\operatorname{Ker}\varphi = H$ (например: $\mathscr{P}\colon G \to {}^{G}\!/_{H}$ — естественный гомоморфизм).

$\operatorname{Im}\varphi \subset S$ — подгруппа.

Рассмотрим сужение φ, т. е. $\varphi'\colon K \to \operatorname{Im}\varphi$:

$\operatorname{Im}\varphi' = P \subset \operatorname{Im}\varphi \subset S$, $\varphi'(K) = \varphi(K)$;

$\operatorname{Ker}\varphi' = K \cap H$ — очевидно, а следовательно по 1-ой теореме об изоморфизме $P \approx {}^{K}\!/_{K \cap H}$.

Пусть $z \in P$, существует $c \in K$: $\varphi(c) = z$, но полный прообраз z, т. е. $\varphi^{-1}(z)$ — это смежный класс с H, и объединение всех этих прообразов есть подгруппа KH группы G. Образ $\varphi(KH) = P$, т. к. H — ядро прообраза, т. е. $\operatorname{Ker}\varphi = H \subset KH$.

$P \approx {}^{K}\!/_{K \cap H}$, следовательно ${}^{KH}\!/_{H} \approx {}^{K}\!/_{K \cap H}$ (по 1-ой теореме об изоморфизме), получаем $\varphi\colon KH \to \operatorname{Im}\varphi = P$.

10. Автоморфизмы и эндоморфизмы групп

Пусть G — группа.

Определение. Изоморфизм $\varphi : G \to G$ называется *автоморфизмом.*

Пример 8. Пусть G — поле комплексных чисел.

$\varphi : \mathbb{C} \to \mathbb{C}$;

$z \to \overline{z}$.

Так как $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$, то φ — Hom .

Очевидно, что φ — биекция, следовательно φ — автоморфизм.

Пример 9. Докажите, что это отображение является автоморфизмом самостоятельно: $R^* \to R^*$, $x \to x^{-1}$.

Пример 10. Пусть G — группа, для любого $g \in G$ определим автоморфизм по следующему правилу:

$$\varphi_g : G \to G$$
$$x \to g^{-1}xg.$$

Данный автоморфизм называется *внутренним автоморфизмом*, а элементы — сопряженными. Докажите, что внутренний автоморфизм действительно является автоморфизмом самостоятельно.

При этом автоморфизме подгруппа H группы G переходит в сопряженную ей подгруппу $g^{-1}Hg$. Левый класс смежно-

сти aH в множество $g^{-1}aHg = (g^{-1}ag)g^{-1}Hg$, которое является левым классом смежности по подгруппе $g^{-1}Hg$, порожденной элементом $x^{-1}ax$.

Пространство классов смежности по подгруппе H изоморфно пространству классов смежности по подгруппе $g^{-1}Hg$. (К сопряженным группам мы будем возвращаться, например, изучая действие группы на множестве).

Введем обозначения:

$\operatorname{Aut} G$ — множество всех автоморфизмов группы G;

$\operatorname{Inn} G$ — множество всех внутренних автоморфизмов группы G.

$\operatorname{Inn} G \subset \operatorname{Aut} G$ — подмножество всех автоморфизмов группы G

Утверждение. $\operatorname{Aut} G$ — *группа.* $\operatorname{Inn} G$ — *подгруппа группы* $\operatorname{Aut} G$. $\operatorname{Inn} G \lhd \operatorname{Aut} G$.

Доказательство.

1. Для всех $\varphi, \psi \in \operatorname{Aut} G$ определим бинарную операцию следующим образом: $\varphi \cdot \psi = \varphi \circ \psi$. Докажите, что относительно этой операции множество всех автоморфизмов образует группу самостоятельно.

2. Теперь перейдем к доказательству того, что множество внутренних автоморфизмов образует подгруппу группы всех автоморфизмов. Пусть $\varphi_{g_1}, \varphi_{g_2} \in \operatorname{Inn} G$.

Композиция $\varphi_{g_1} \circ \varphi_{g_2} = \varphi_{g_1 g_2}$ является внутренним автоморфизмом по определению, т.е. для всех $x \in G$:

$(\varphi_{g_1} \circ \varphi_{g_2})(x) = \varphi_{g_1}\big(\varphi_{g_2}(x)\big) = \varphi_{g_1}(g_2^{-1}xg_2) = g_1^{-1}yg_1 = = g_1^{-1}g_2^{-1}xg_2g_1 = (g_2g_1)^{-1}x(g_1g_2) = \varphi_{g_1g_2}(x)\,;\ \varphi_e(x) = e^{-1}xe = = x\varphi_e = \mathrm{id}\,.$

Композиция следующих отображений $\varphi_g \cdot \varphi_{g^{-1}}$ равна тождественному отображению φ_e, следовательно существует $\varphi_g^{-1} = \varphi_{g^{-1}}$.

3. Докажите самостоятельно, что множество внутренних автоморфизмов является нормальной подгруппой $\mathrm{Inn}\,G \lhd \mathrm{Aut}\,G$.

Определение. $\mathrm{Hom}\,\varphi : G \to G$ называется *эндоморфизмом* и обозначается $\mathrm{End}\,G$ — множество всех эндоморфизмов группы G.

Пусть G — абелева группа, и $\varphi, \psi \in \mathrm{End}\,G$, для всех $x \in G$ определим операцию сложения двух гомоморфизмов следующим образом: $(\varphi + \psi)(x) \doteq \varphi(x) + \psi(x)$. Для того, чтобы доказать, что $(\varphi + \psi)$ является гомоморфизмом, необходимо доказать следующее: $(\varphi + \psi)(x + y) = (\varphi + \psi)(x) + (\varphi + \psi)(y)$.

Доказательство.

$(\varphi + \psi)(x + y) = (\varphi)(x + y) + (\psi)(x + y) =$

$= (\varphi)(x) + (\varphi)(y) + \psi(x) + \psi(y) = (\varphi + \psi)(x) + (\varphi + \psi)(y)\,.$

Утверждение. *Пусть G — абелева группа, тогда:*

1) $(\mathrm{End}\,G, +)$ — *абелева группа;*

2) $(\mathrm{End}\,G, *)$ — *полугруппа с* 1.

Докажите данное утверждение самостоятельно.

Следствие. Если G — абелева группа, то $\operatorname{End} G$ — кольцо с 1.

Докажите это самостоятельно.

Пример 11. $Z = \langle 1 \rangle$, пусть $\varphi\colon Z \overset{\text{Hom}}{\to} Z$, и пусть $\varphi(1) = m$, следовательно для всех $a \in Z\colon \varphi(a) = a\varphi(1) = am$.

$\varphi \doteq \varphi_m$, $Z \to \operatorname{End} Z$, тогда $\varphi_m + \varphi_n = \varphi_{m+n}$; $m \to \varphi_m$.

$\varphi_m \circ \varphi_n = \varphi_{m \cdot n}$, $\operatorname{End} G \approx Z$ — кольцо.

Пример 12. V — векторное пространство, $(V, +)$ — абелева группа. $\operatorname{End} V \approx M_n(u)$, где n — размерность пространства V. $\operatorname{Aut} V$ — множество невырожденных линейных операторов.

Упражнение 68. Найти группу автоморфизмов:

а) группы $\mathbb{Z}_5$; б) группы $\mathbb{Z}_6$.

Указание. а) $\operatorname{Aut} G$ — циклическая группа порядка 4, состоящая из автоморфизмов возведения в степень $k = 1, 2, 3, 4$;

б) $\operatorname{Aut} G$ — группа второго порядка, в которую кроме тождественного автоморфизма входит автоморфизм возведения в пятую степень.

Упражнение 69. Доказать, что

а) $\operatorname{Aut} \mathbb{S}_3 \simeq \mathbb{S}_3$, причем все автоморфизмы группы $\mathbb{S}_3$ — внутренние;

б) $\operatorname{Aut} \mathbb{V}_4 \simeq \mathbb{S}_3$, причем внутренним для $\mathbb{V}_4$ является лишь тождественный автоморфизм, где $\mathbb{V}_4$ — группа Клейна, т.е. группа, изоморфная группе перестановок:

$\{e, (12)(34),\ (13)(24),\ (14)(23)\}$.

Указание. а) Каждый автоморфизм группы $\mathbb{S}_4$ определяется своим действием на трех элементах второго порядка;

б) любая перестановка неединичных элементов группы $\mathbb{V}_4$ определяет ее автоморфизм.

Упражнение 70. Является ли циклической группа автоморфизмов:

а) группы $\mathbb{Z}_9$; б) группы $\mathbb{Z}_8$?

Ответ.

а) Да, $\operatorname{Aut}\mathbb{Z}_9$ — циклическая группа порядка 6, порождаемая автоморфизмом возведения в квадрат.

б) Нет, $|\operatorname{Aut}\mathbb{Z}_8| = 4$, но квадрат каждого автоморфизма — тождественное отображение.

Упражнение 71. Найти порядок группы $\operatorname{Aut}\operatorname{Aut}\operatorname{Aut}\mathbb{Z}_9$.

Ответ. $|\operatorname{Aut}\operatorname{Aut}\operatorname{Aut}\mathbb{Z}_9| = 1$.

Определение. Пусть $H \subset G$ — подгруппа группы G. Подгруппа H называется *характеристической подгруппой*, если для всех $\varphi \in \operatorname{Aut} G\colon\ \varphi(H) \subset H$, и *вполне характеристической*, если для всех $\varphi \in \operatorname{End} G\colon\ \varphi(H) \subset H$.

$\varphi(H) = \{\varphi(x) | x \in H\}$.

$H \lhd G$ тогда и только тогда, когда для всех $g \in G$, для всех $h \in H\colon\ g^{-1}hg \in H$.

$g^{-1}hg = \varphi_g(h)$ — сопряженный к элементу h.

$H \lhd G$ тогда и только тогда, когда для всех $g \in G$: $\varphi_g(H) \subset H$ или $H \lhd G$ тогда и только тогда, когда для всех $\varphi \in \operatorname{Inn} G$: $\varphi(H) \subset H$; $\operatorname{End} G \supset \operatorname{Aut} G \supset \operatorname{Inn} G$.

$H \longrightarrow$ вполне характеристическая $\longrightarrow$ характеристическая $\longrightarrow$ нормальная подгруппа.

Учитывая вышесказанное, можно дать еще одно определение *нормальной подгруппы.*

Определение. $H \lhd G$ тогда и только тогда, когда для любого $\varphi \in \operatorname{Inn} G$ $\varphi(H) \subset H$.

11. Центр группы

Определение. $Z(G) = \{g \in G | \forall\ x \in G : gx = xg\}$.

Пример 13. Пусть G — абелева группа, $Z(G) = G$.

Пример 14. $Z(S_3) = \{e\}$.

Пример 15. $G = GL_2(R)$, $Z(G) = \begin{Bmatrix} \lambda & 0 \\ 0 & \lambda \end{Bmatrix}$.

Утверждение. *Центр группы есть абелева характеристическая подгруппа.*

Доказательство. Пусть G — группа, $Z(G)$ — ее центр группы. Пусть $a, b \in Z(G)$, пусть $x \in G$:

$x(ab) = (xa)b = a(xb) = abx$, следовательно $ab \in Z(G)$.

Пусть a принадлежит центру $Z(G)$. Докажем, что обратный элемент тоже принадлежит центру.

$xa^{-1} = (ax^{-1})^{-1} = (x^{-1}a)^{-1} = a^{-1}x$, тогда $a^{-1} \in Z(G)$.

То, что центр является абелевой группой, вытекает из определения. Докажем, что она характеристическая.

Пусть φ — автоморфизм $G \to G$.

Пусть $x \in G$, и пусть $a \in Z(G)$.

Докажем, что $\varphi(a) \in Z(G)$ т. е. $\varphi(a)x = x\varphi(a)$.

Так как φ — сюръекция, то существует $y \in \varphi(y) = x$; $x \cdot \varphi(a) = \varphi(y) \cdot \varphi(a) = \varphi(y \cdot a) = \varphi(a \cdot y) = \varphi(a)\varphi(y) = \varphi(a)x$, следовательно $\varphi(a) \in Z(G)$.

Следствие. Центр группы является нормальной подгруппой.

Упражнение 72. Найти центр группы:

а) $\mathbb{S}_n$; б) $\mathbb{A}_n$; в) $\mathbb{D}_n$, где $\mathbb{D}_n$ — группа диэдра, т.е. группа движений правильного n-угольника.

Ответ.

а) $\mathbb{S}_2$ при $n = 2$ и $\{e\}$ при $n \neq 2$;

б) $\mathbb{A}_3$ при $n = 3$ и $\{e\}$ при $n \neq 3$;

в) центр является единичным при нечетных n, а при четных включает еще поворот на угол π.

Упражнение 73. Найти центр группы:

а) $\mathbb{GL}_n(\mathbb{R})$ — группа невырожденных мариц порядка n над полем $\mathbb{R}$; б) $\mathbb{O}_2(\mathbb{R})$ — группа ортогональных матриц ($A^t = A^{-1}$) порядка 2 над полем $\mathbb{R}$; в) $\mathbb{SO}_2(\mathbb{R})$ — группа ортогональных матриц второго порядка с определителем, равным единице над полем $\mathbb{R}$;

г) $\mathbb{SO}_3(\mathbb{R})$; д) $\mathbb{SU}_2(\mathbb{C})$ — группа унитарных комплексных матриц ($\overline{A}^t = A^{-1}$, $\overline{A}^t$ — матрица, полученная из A^t заменой ее элементов на комплексно сопряженные) второго порядка с определителем, равным единице; е) $\mathbb{SU}_n(\mathbb{C})$.

Ответ.

а) $\{\lambda E\}$; б) $\{\pm E\}$; в) вся группа;

г) $\{E\}$; д) $\{\pm E\}$; е) $\{\alpha E | \alpha^n = 1\}$.

Упражнение 74. Доказать, что если A и B — нормальные делители G и $A \cap B = 1$, то элементы из A коммутируют с элементами из B.

12. Коммутант группы

Определение. Пусть G — группа, $x, y \in G$: $xyx^{-1}y^{-1}$ называется *коммутатором* элементов x, y: $[x, y] = xyx^{-1}y^{-1}$.

Замечание. Если $xy = yx$, то $[x, y] = e$.

Определение. Подгруппа, порожденная всеми коммутаторами группы, называется *коммутантом* группы и обозначается

$$[GG] = \langle [x_1, y_1]; [x_2, y_2]; \ldots \rangle .$$

Система образующих может быть бесконечной.

Пример 16. Пусть G — абелева группа, следовательно $[G\,G] = \{e\}$.

Пример 17. $[S_4\, S_4] = A_4$ — знакопеременная группа.

Пример 18. $[S_n\, S_n] = A_n$

Пример 19. $[A_3\, A_3] = \{e\}$.
$[A_4\, A_4] = \{e, (12)(34), (14)(23)(13)(24)\}$.
Для всех $n \geqslant 5$, $[A_n\, A_n] = A_n$.

Утверждение. *Коммутант группы — вполне характеристическая подгруппа.*

Доказательство. Пусть $\varphi : G \to G$ — произвольный $\operatorname{End} G$. Докажем, что для всех $x, y \in G$, $\varphi\big([x,y]\big) \in [G\, G]$.
$\varphi\big([x,y]\big) = \varphi\left(xyx^{-1}y^{-1}\right) =$
$= \varphi(x)\varphi(y)\big(\varphi(x)\big)^{-1}\big(\varphi(y)\big)^{-1} = \big[\varphi(x), \varphi(y)\big] \in [G\, G]$.

Теорема (основное свойство коммутанта). *Пусть G — группа, $H \lhd G$. Тогда G/H — абелева* тогда и только тогда, когда $[G\, G] \subset H$, *т. е. коммутант группы — это наименьшая подгруппа фактор-группа, по которой абелева.*

Доказательство. Докажем необходимость.

Пусть G/H — абелева. Для того чтобы доказать, что для любых $x, y \in G$, $[x,y] \in H$, достаточно доказать, что $xy \in Hyx$.

Так как $H \lhd G$, $Hyx = yxH = yHxH = xHyH = xyH$, следовательно $Hyx = xyH$. Таким образом, $xy \in Hyx$.

Докажем в обратную сторону.

Так как $[x,y] \in H$, то $xyx^{-1}y^{-1} \in H$, следовательно $xy(y{\cdot}x)^{-1} \in H$, тогда $xyH = yxH$. В то же время $xyH = xHyH$ и $yxH = (yH)(xH)$, следовательно G/H — абелева.

Упражнение 75. Доказать, что коммутатор $[x,y]=xyx^{-1}y^{-1}$ элементов x,y группы G обладает свойствами:

а) $[x,y]^{-1}=[y,x]$;

б) $[xy,z]=x[y,z]x^{-1}[x,z]$;

в) $[z,xy]=[z,x]x[z,y]x^{-1}$.

Упражнение 76. Какие из следующих равенств тождественно выполняются в группе $\mathbb{S}_3$:

а) $x^6=1$; б) $\big[[x,y],z\big]=1$; в) $[x^2,y^2]=1$?

Ответ. а) и в).

Упражнение 77. Доказать, что в группе верхних унитреугольных матриц порядка 3 выполняется тождество

$$(x,y)^n=x^ny^n[x,y]^{-n(n-1)/2},\quad (n\in\mathbb{N}).$$

Упражнение 78. Доказать, что если в группе G выполняется тождество $\big[[x,y],z\big]=1$, то в G выполняются тождества

$$[x,yz]=[x,y][x,z],\quad [xy,z]=[x,z][y,z].$$

Упражнение 79. Доказать, что если в группе G выполняется тождество $x^2=1$, то G коммутативна.

Указание. Рассмотреть элемент $(xy)^2$.

13. Прямое произведение групп

Пусть G_1, G_2 — группы по умножению:

$G_1 \times G_2 = \{(x, y) | x \in G_1, y \in G_2\}$ — декартово произведение.

$(a, b)(x, y) = (ax, by)$ — «покомпонентное» умножение.

Утверждение. $G_1 \times G_2$ — *группа.*

Доказательство. Ассоциативность, очевидно, имеет место, т. к. оно имеет место в компонентах (e_{G_1}, e_{G_2}) — единица. (x_1, x_2) — обратный (x_1^{-1}, x_2^{-1}).

Определение. $G_1 \times G_2$ называется *внешним прямым произведением* групп G_1, G_2.

Упражнение 80. Доказать, что $G_1 \times G_2 \approx G_2 \times G_1$.

Введем новые обозначения и укажем ряд связанных с ними свойств.

1) $\overline{G}_1 = \{(x, e_{G_2}) | x \in G_1\}$ — нормальная подгруппа.

$G_1 \times G_2 \approx G_1$.

Изоморфизм $(x_1, e_{G_2}) \to x_1$.

$(y_1, y_2^{-1})(x_1, e_{G_2})(y_1, y_2) = (y_1^{-1}, y_2^{-1})(x_1, e_{G_2})(y_1, y_2) =$

$= \left(y_1^{-1} x_1 y_1, y_2^{-1} e_{G_2} y_2\right) = \left(y_1^{-1} x_1 y_1, e_{G_2}\right)$, следовательно

$\overline{G}_1 \lhd G_1 \times G_2$.

2) $\overline{G}_2 = \{(e_{G_1}, x) | x \in G_2\} \lhd G_1 \times G_2 \approx G_2$.

3) Элементы из подгрупп $\overline{G}_1$ и $\overline{G}_2$ коммутируют при умножении: $(x_1, e_{G_2})(e_{G_1}, x_2) = (x_1, x_2)$ и $(e_{G_1}, x_2)(x_1, e_{G_2}) = (x_1, x_2)$.

4) $\overline{G}_1 \cap \overline{G}_2 = 1$ — очевидно.

5) $\overline{G}_1 \cdot \overline{G}_2 = G_1 \times G_2$.

Действительно, любой элемент (x_1, x_2) из $G_1 \times G_2$ равен $(x_1, e_{G_2})(e_{G_1}, x_2)$.

Пример 20. $(a, b) + (x, y) = (a + x, b + y) = G_1 \oplus G_2$.

$R^n = \{(x_1, x_2, \ldots, x_n) | x_i \in R\}$.

Определение. Говорят, что G раскладывается в прямое произведение своих подгрупп F и H , если существует изоморфизм: $\varphi : F \times H \to G$, при этом записывают $G = F \times H$.

Замечание. Внешнее прямое произведение может быть сделано внутренним, следующим образом:

Пусть $G_1 \times G_2 = \overline{G}$.

$\overline{G}_1 = \{(x, e_{G_2}) | x \in G_1\}$,

$\overline{G}_2 = \{(e_{G_1}, y) | y \in G_2\}$.

$\overline{G}_i \lhd \overline{G}$, $i = 1, 2, \ldots$, $\overline{G}_1 \times \overline{G}_2 \to \overline{G}$;

$((x, e_2)\,(e_1, y)) \to (x, y)$.

Теорема 6. *Пусть F и H — подгруппы группы G , тогда $G = F \times H$* тогда и только тогда, когда

1. $G = FH$ *(для всех $g \in G$, $g = fh$, $f \in F$, $h \in H$).*
2. $FH = HF$ *— поэлементно, т. е. для всех $f \in F$, $h \in H$:* $fh = hf$.
3 $F \cap H = \{e\}$.

Или 1, 3 или 4, т.е. условия 1 и 3 в теореме можно заменить на условие 4 , которое формулируется следующим образом: для

всех $g \in G$, существует единственное представление $g = fh$, $f \in F$, $h \in H$. Докажем равнозначность этих утверждений.

Доказательство. 1, 3 тогда и только тогда, когда 4.

Пусть $g = fh = f'h'$.

$(f')^{-1}fhh^{-1} = (f')^{-1}f'h'h^{-1}$,

$(f')^{-1}f = h'h^{-1} \in F \cap H = \{e\}$,

$h'h^{-1} = e$ тогда и только тогда, когда $h = h'$.

$(f')^{-1}f = e$ тогда и только тогда, когда $f = f'$.

Из 4 следует 1, 3.

Существование 1 — очевидно.

Пусть $g = fh \in F \cap H$.

$g = e \cdot fh = fh \cdot e$, откуда $fh = e$, следовательно $g = e$, тогда $F \cap H = \{e\}$ ($fh \in F$, $e \in H$).

Перейдем к доказательству теоремы.

Пусть 1, 2, 3 выполняются (для всех $f \in F$, $h \in H$, $\varphi(f, h) = fh$). Определим отображение $F \times H \xrightarrow{\varphi} G$.

Для того, чтобы доказать, что φ является изоморфизмом, докажем следующие факты.

1. φ — Hom.

$\varphi(f, e) = f$;

$\varphi(e, h) = h$;

$(f, h)(x, y) = (fx, hy)$;

$\varphi((f, h)(x, y)) = \varphi(fx, hy) = fxhy \overset{FH=HF}{=} fhxy = \varphi(f, h) \cdot \varphi(x, y)$, откуда φ — Hom.

2. φ — инъективный мономорфизм тогда и только тогда, когда $\operatorname{Ker}\varphi = \{e\} = (e, e)$;

Пусть $\varphi(f, h) = e = fh$, следовательно $fh = e$; $f = e \cdot h^{-1}$, следовательно $f \in H$, откуда $f \in F \cap H = \{e\}$, $f = e$, следовательно $h = e$.

3. По 1, для всех g существует $f, h\colon fh = g \doteq \varphi(f, h)$.

φ — эпиморфизм, сюръекция тогда и только тогда, когда $\operatorname{Im}\varphi = G$ (по свойству 1).

Докажем необходимость.

Пусть $G = F \times H$, тогда существует φ — изоморфизм: $F \times H \to G$.

1) φ — сюръекция, следовательно для всех $g \in G$, существует $(f, h)\colon (\varphi(f, h) = g)$.

Так как φ — Hom , то $\varphi(f, h) = g = \varphi(f, e) \cdot \varphi(e, h) = fh$ — соответственно для всех $g \in G$ существует $f \in F$ и $h \in H$ такие, что $g = fh$.

Но так как $(f, h) = (f, e)(e, h) = (e, h)(f, e)$, то

$\varphi(f, h) = g = hf = fh$.

2) Пусть $g \in F \cap H$. $\varphi(e, g) = g = \varphi(g, e)$, но φ — инъекция, следовательно $(e, g) = (g, e)$, значит $g = e$.

Утверждение. *H_1, H_2 — нормальные подгруппы группы G. $H_1 \cap H_2 = \{e\}$, тогда элементы из H_1 коммутируют с элементами из H_2.*

Доказательство. Пусть $x_1 \in H_1$, $x_2 \in H_2$. Рассмотрим

коммутатор $z = x_1x_2x_1^{-1}x_2^{-1} = x_1(x_2x_1^{-1}x_2^{-1}) \in H_1$, (т.к. $H_1 \lhd G$, $x_2\, x_1^{-1}\, x_2^{-1} \in H$).

Аналогично $z = x_1x_2x_1^{-1}x_2^{-1} = \left(x_1(x_2x_1^{-1})x_2^{-1}\right) \in H_2$, т. к. $H_1 \cap H_2 = \{e\}$, $x_1x_2x_1^{-1}x_2^{-1} = e$, следовательно $x_1x_2 = x_2x_1$.

Следующее утверждение докажите самостоятельно.

Утверждение. *H_1, H_2 — нормальные подгруппы группы G. $H_1 \cap H_2 = \{e\}$ и $H_1H_2 = G$, тогда $G \approx H_1 \times H_2$.*

Понятие прямого произведения естественно обобщается на произвольное конечное множество групп.

Именно (внешним) прямым произведением групп

$$G_1, G_2, \ldots, G_n$$

называется множество строк

$$(x_1, x_2, \ldots, x_n); \quad x_i \in G_i$$

с покомпонентным умножением:

$$(x_1, x_2, \ldots, x_n)(y_1, y_2, \ldots, y_n) = (x_1y_1, x_2y_2, \ldots, x_ny_n).$$

Легко увидеть, что это множество есть группа с единицей $(1, 1, \ldots, 1)$. Прямое произведение обозначается

$$G_1 \times G_2 \times \ldots \times G_n.$$

Свойства:

1. $\overline{G}_i \lhd G_1 \times G_2 \times \ldots \times G_n \approx G_i$;
   $\overline{G}_i = \{1, 1, \ldots, x_i, \ldots, 1 \quad \forall \ x_i \in G_i\}$.

2. $\overline{G}_1 \times \overline{G}_2 \times \ldots \times \overline{G}_n = G_1 \times G_2 \times \ldots \times G_n$.

3. Элементы из $\overline{G}_i, \overline{G}_j$ при $i \neq j$ коммутируют.

4. Пересечение $\overline{G}_i$ для всех i с произведением всех остальных $\overline{G}_j = \{e\}$.

Внутреннее прямое произведение определяется аналогично случаю $n = 2$.

Теорема 7. *Пусть* $H_i \lhd G$ *и* $H_1 H_2 \ldots H_n = G$. *Для любого* i, $\bigcap\limits_{i=1}^{y} H_i = \{e\}$. *Тогда* G *раскладывается в прямое произведение подгруппы* H_i.

Доказательство. Элементы из H_i, H_j коммутируют.

Определим отображение φ:

$$(x_1, x_2, \ldots, x_n) \to x_1 \cdot x_2 \cdot \ldots \cdot x_n.$$

Докажем, что это отображение Hom .

$x_1 \cdot x_2 \cdot \ldots \cdot x_n \cdot y_1 \cdot y_2 \cdot \ldots \cdot y_n = x_1 y_1 \cdot x_2 y_2 \cdot \ldots \cdot x_n y_n$, т. к. x_i, y_j : $i \neq j$ коммутируют.

Докажем, что эпиморфизм. Это вытекает из того, что

$$H_1 H_2 \ldots H_n = G.$$

Докажем, что отображение является мономорфизмом.

Пусть $x_1 \cdot x_2 \cdot \ldots \cdot x_n = y_1 \cdot y_2 \cdot \ldots \cdot y_n$.

В силу того, что элементы коммутируют

$x_i y_i^{-1} = y_1 x_1^{-1} \ldots y_{i-1} x_{i-1}^{-1} \, y_{i+1} x_{i+1}^{-1} \ldots y_n x_n^{-1}$.

Левая часть принадлежит H_i, правая — произведение всех H_j, $i \neq j$, следовательно $x_i y_i^{-1} = \{e\}$, и $x_i = y_i$.

Определение. $H_1, \ldots, H_n$ — подгруппы групп $G_1, \ldots, G_n$.
$H_1 \times H_2 \times \ldots \times H_n$ — подгруппа группы $G_1 \times G_2 \times \ldots \times G_n$.
Если $H_i \lhd G_i$, следовательно

$$H_1 \times H_2 \times \ldots \times H_n \lhd G_1 \times G_2 \times \ldots \times G_n.$$

Утверждение. *Фактор-группа группы* $G_1 \times G_2 \times \ldots \times G_n$ *по* $H_1 \times H_2 \times \ldots \times H_n$ *равна*

$$\left({}^{G_1}\!/_{H_1}\right) \times \left({}^{G_2}\!/_{H_2}\right) \times \ldots \times \left({}^{G_n}\!/_{H_n}\right).$$

Доказательство. Смежные классы группы $G_1 \times \ldots \times G_n$ по $H_1 \times H_2 \times \ldots \times H_n$ образованы последовательностями $(z_1a_1, z_2a_2 \ldots, z_na_n)$, где z_i пробегают H_i, а a_i — фиксированные элементы из G_i.

Эти множества естественно рассматривать как последовательности классов смежности $(H_1a_1, H_2a_2, \ldots, H_na_n)$. Покомпонентное умножение элементов этих множеств сводится к покомпонентному умножению классов смежности, т. е. элементов фактор-группы $\left({}^{G_i}\!/_{H_i}\right)$.

Пример 21. G — абелева. Для любого $x \in V$ существуют $x_1, \ldots, x_n$, $x = x_1e_1 + \ldots + x_ne_n$, $V_i = \langle e_i \rangle$ — подгруппа группы G.

$V = \bigoplus_{i=1}^{n} V_i$; $R^n = \underbrace{R + \ldots + R}_{n}$.

Пример 22. $\left(M_2(x), +\right)$ — абелева группа.

$S = \left\{ \begin{pmatrix} a & \lambda \\ \lambda & b \end{pmatrix} \right\}$ — подгруппа симметричной матрицы.

$K = \left\{ \begin{pmatrix} 0 & -\lambda \\ \lambda & 0 \end{pmatrix} \right\}$ — подгруппа кососимметричной матрицы.

$S \cap K = \{0\}$.

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & \frac{b+c}{2} \\ \frac{b+c}{2} & d \end{pmatrix} + \begin{pmatrix} 0 & \frac{b-c}{2} \\ \frac{c-b}{2} & 0 \end{pmatrix}$, следовательно $M_2(K) = S \oplus K$.

Пример 23. $C^* = R_+ \times T$.

R_+ — подгруппа положительных вещественных чисел по умножению.

$T = \{z \mid |z| = 1\}$. Любое $z \in C^*$ можно представить в виде $z = |z| \cdot (\cos\varphi + i \sin\varphi)$.

Упражнение 81. Доказать, что группы $\mathbb{Z}$ и $\mathbb{Q}$ не разлагаются в прямую сумму ненулевых подгрупп.

Упражнение 82. Разлагаются ли в прямое произведение неединичных подгрупп группы:

а) $\mathbb{S}_3$; б) $\mathbb{A}_4$; в) $\mathbb{S}_4$; г) $\mathbb{Q}_8$?

Упражнение 83. Доказать, что мультипликативная группа комплексных чисел является прямым произведением группы положительных вещественных чисел и группы всех комплексных чисел, по модулю равных 1.

14. Действие группы на множестве

Определение. M — некоторое множество, G — группа, действующая на элементы этого множества, т. е. $G \times M \to M$. Паре элементов из M и элементу из G ставим в соответствие элемент из M.

При этом выполнены следующие условия:

1) для всех $m \in M$, $m \cdot e_G = m$;

2) для всех $m \in M$, $g_1, g_2 \in G$, $m(g_1 g_2) = (mg_1)g_2$.

1), 2) — правая запись действия.

Принята также левая запись действия. $g \in G$, $m \in M$:

1) $e_G \cdot m = m$;

2) $(g_1 g_2)m = g_1(g_2 m)$.

Правая и левая записи равносильны. Но в действии произведения элементов группы на $m \in M$ имеется разница. При правой записи $m(g_1 g_2)$ первым действует g_1, а вторым g_2. При левой записи $(g_1 g_2)m$ первым действует g_2, а вторым g_1. Мы будем использовать правую запись.

Определение. Множество M, на котором определено действие группы G, называется *G-операторным множеством*, или *G-множеством*. Его элементы называются *точками*.

Утверждение. *Пусть $m \in M$, $mG = \{mg | g \in G\}$ — называется орбитой, порожденной точкой m. Точка $m_1 \in mG$ порождает ту же орбиту.*

Доказательство. Пусть $m_1 = mg_1$, тогда

$m_1G = mg_1G = m(g_1G) = mG$.

Следствие. Орбиты могут либо совпадать, либо не иметь общих точек.

Следствие. Таким образом, множество G разбивается на непересекающиеся орбиты.

Замечание. Каждая орбита, в свою очередь, является G-операторным множеством, состоящим из одной орбиты, именно себя самой.

Определение. Если G-множество M состоит из одной орбиты, то говорят, что оно действует транзитивно на M, а M называется однородным пространством по отношению к группе G.

Пример 24. Пусть M — множество точек на плоскости G-группа векторов относительно сложения. Действия вектора на точку определяется как перенос точки на этот вектор. Ясно, что здесь одна орбита (параллельные переносы). Однородное множество.

Пример 25. M — множество точек плоскости G-группы всех движений. Однородное пространство.

Пример 26. M — множество точек на плоскости G-группа вращений вокруг фиксированной точки O. Здесь орбитами будут окружности с центром в точке O и сама точка O.

15. Действие сопряжением

В качестве множества M возьмем саму группу G и действие элемента $z \in G$ на элемент $a \in G$ определим как $z^{-1}az$. Для того чтобы избежать путаницы с обычным умножением, часто обозначают $z^{-1}az = a^z$.

Проверим свойства:

$a^{e_G} = (e_G)^{-1}ae_G = a$;

$a^{z_1 z_2} = z_2^{-1}z_1^{-1}az_1z_2 = z_2^{-1}(z_1^{-1}az_1)z_2 = z_2^{-1}(a^{z_1})z_2 = (a^{z_1})^{z_2}$.

Орбиты в этой ситуации называются классами сопряженных элементов. Среди них имеются состоящие из одного элемента. Например класс, порождающий 1, $z^{-1}e_Gz = z^{-1}ze_G = e_G$ для всех z.

Такими же будут классы, составленные из каждого элемента центра a в $Z(G)$: $a^z = z^{-1}az = z^{-1}za = a$, для всх $z \in G$.

16. Однородное пространство

Пусть G — группа, $H \subset G$ — подгруппа, Ha — множество левых классов смежности. Определим действие группы G как правое умножение на ее элементы $(Ha)z = Haz$, $z \in G$.

Проверьте самостоятельно выполнение аксиом G-оператора.

$Ha_2 = (Ha_1)a_1^{-1}a_2$, следовательно все классы составят одну орбиту, т. е. множество левых классов смежности образует однородное пространство по отношению к правым, умножением на элементы группы G.

Определение. Пусть $M_1 - G_1$ — операторное множество, $M_2 - G_2$ — операторное множество. Они изоморфны, если $G_1 \approx G_2$, т.е. существует взаимнооднозначное соответствие между элементами M_1, M_2, сохраняющее при применении соответствующих друг другу элементов группы G_1 и G_2.

Теорема 8. *Любое однородное G пространство M изоморфно пространству класса смежности по некоторой подгруппе.*

Доказательство. Пусть $m_0 \in M$. Рассмотрим H — множество элементов группы G таких, которые не изменяют m_0, т. е. $z \in G\colon\ m_0 z = m_0$, следовательно $z \in H$.

Они образуют подгруппу, т. к. $m_0 z = m_0$, следовательно $m_0 = m_0 z z^{-1} = m_0 z^{-1}$;

$m_0 z_1 = m_0$ и $m_0 z_2 = m_0$, то $m_0(z_1 z_2) = (m_0 z_1) z_2 = m_0 z_2 = m_0$.

Определение. Подгруппа H называется *стабилизатором* точки m_0.

Рассмотрим $m_1 \neq m_0 \in M$. Так как M — однородно, т. е. состоит из одной орбиты, то существует $x \in G$, $m_0 x = m_1$.

Выясним, какие еще элементы преобразуют m_0 в m_1.

Пусть $m_0 y = m_1$, следовательно $m_0 x y^{-1} = m_1 y^{-1} = m_0$, т. к. $m_0 y y^{-1} = m_1 y^{-1} = m_0$, откуда $xy^{-1} \in H$, следовательно $x \in Hy$.

Таким образом элементы из G, одинаково преобразующие точку m_0, принадлежат одному классу смежности по стабилизатору. Верно и обратное утверждение, если x и y принад-

лежат одному классу по стабилизатору, т. е. $Hx = Hy$. Таким образом $m_0x = m_0y$, следовательно между точками однородного пространства M и левыми классами смежности по стабилизатору существует взаимнооднозначное соответствие. Оно сохраняется при умножении справа на элементы G.

Действительно, $m_1 = m_0x$, следовательно $m_1 \to Hx$.

Пусть $m_2 = m_1y = m_0xy$, тогда $m_2 \to Hxy = (Hx)y$.

Выясним, как связаны стабилизаторы различных точек.

Пусть H — стабилизатор точки m_0.

Для всех m_1, существует $x \in G$: $m_1 = m_0x$.

$$m_1z = m_1 \Leftrightarrow m_0xz = m_0x \Leftrightarrow m_0xzx^{-1} = m_0 \Leftrightarrow$$
$$\Leftrightarrow xzx^{-1} \in H \Leftrightarrow z \in x^{-1}Hx.$$

Таким образом, для точки m_1 стабилизатор имеет вид $x^{-1}Hx$.

Напомним, что $z \to x^{-1}zx$ называется *внутренним автоморфизмом группы*, т. е. подгруппа H переходит в сопряженную подгруппу $x^{-1}Hx$, Ha переходит в множество $x^{-1}Hax = (x^{-1}Hx)x^{-1}ax$, т. е. в левый класс смежности по подгруппе $x^{-1}Hx$, порожденной элементом $x^{-1}ax$.

Таким образом, преобразование левого класса смежности по подгруппе H называется *умножением справа* на $z \in G$ и будет таким же, как преобразование классов смежности по подгруппе $x^{-1}Hx$, вызванное умножением справа на элемент $x^{-1}zx$, следовательно пространство классов смежности по H изоморфно пространству классов смежности по $x^{-1}Hx$.

Наличие такого изоморфизма может служить объяснением того, что в теореме можно было взять точку m_0 и ее стабилизатор произвольно.

17. Централизатор и нормализатор

Рассмотрим G как G-операторное множество.

$a^z = z^{-1}az$, $a \in G$, $z \in G$, т. е. рассмотрим действие элементов G как соответствующий им внутренние автоморфизмы. В этой ситуации орбиты и классы сопряженных элементов совпадают. Каждый класс однородное пространство.

Определение. Пусть C — некоторый класс сопряженных элементов и $a \in C$. Стабилизатором элемента a является множество всех $z \in C$, обладающие свойством $z^{-1}az = a$, т. е. $az = za$, т. е. стабилизатор элемента a — это множество всех элементов, коммутирующих с a.

Это множество образует подгруппу называющуюся централизатором.

По доказанному в § 16, элементы класса, сопряженные с a, находятся во взаимнооднозначном соответствии с левыми классами смежности по централизатору.

Пример 27. Если класс сопряженных элементов конечен, то число его элементов равно $(G : C)$ индексу стабилизатора (централизатора) для любого элемента из этого класса.

Рассмотрим элементы G, действующие на множестве всех подгрупп группы G, в виде внутренних автоморфизмов.

$H \to z^{-1}Hz$, в этом случае орбиты — классы сопряженных подгрупп. Стабилизатор для подгруппы H множество $z \in G$: $z^{-1}Hz = H$.

Определение. Этот стабилизатор называется *нормализатором* группы H, т. е. он является максимальной подгруппой, для которой H нормальна.

Между сопряженными с группой H подгруппами и левым классом смежности группы G по нормализатору H существует взаимнооднозначное соответствие, осуществляющее изоморфизм между однородными пространствами, состоящие из сопряженных с H подгрупп и классами смежности по нормализатору.

Определение. Конечная группа называется *p-группой*, если ее порядок есть степень простого числа p.

Все подгруппы p-группы, являются p-группами, и индекс любой подгруппы в p-группе равен некоторой степени p.

Разобьем p-группу G порядка p^n на класс сопряженных элементов.

Пусть число элементов центра t.

Все элементы, не принадлежащие центру, порождают классы сопряженных, содержащих более одного элемента, и пусть эти классы $C_1, C_2, \ldots, C_k$. Число элементов в каждом таком классе есть индекс централизатора любого элемента класса, и

следовательно является степенью p^m с бóльшим нуля показателем m.

Пусть число элементов в C_i равно $m_i > 0$. Подсчет числа элементов в G:

$$p^n = t + p^{m_1} + p^{m_2} + \ldots + p^{m_k},$$

следовательно, t делится на p, и т. к. $t \geqslant 1$, следовательно $t \geqslant p$. Таким образом, мы доказали, что любая конечная группа имеет нетривиальный центр. Порядок центра равен степени p.

В параграфе 10 мы рассматривали автоморфизмы групп. Напомним основные сведения, для того, чтобы связать их новыми понятиями централизатора и нормализатора.

Определение. Отображение $\varphi : G \to G$ — изоморфизм, называется *автоморфизмом*. Внутренний автоморфизм преобразовывается сопряженным посредством элементов группы.

Теорема 9. *Внутренний автоморфизм образует нормальную подгруппу группы всех автоморфизмов.*

Определение. ${}^{\operatorname{Aut} G}\!/_{\operatorname{Inn} G}$ называется *группой внешних автоморфизмов.*

Теорема 10. ${}^{\operatorname{Inn} G \approx G}\!/_{Z(G)}$.

Доказательство. Рассмотрим G как G-множество по отношению к действию сопряжением $a^z = z^{-1}az$. Индуцированная стабилизатором $a \in G$ в группе G группа преобразований

есть централизатор a. Пересечение всех централизаторов есть центр G, т. к. если элемент принадлежит централизатору всех элементов, то он пересекается со всеми элементами из G, т. е. принадлежит центру, и наоборот.

Любая абелева группа не имеет нетривиальных внутренних автоморфизмов $z^{-1}az = a$.

Внешние автоморфизмы есть даже у циклических групп.

Бесконечная циклическая группа $\langle a \rangle$ имеет один нетождественный автоморфизм $a' \to a^{-1}$. Действительно, образующей бесконечной циклической группы может быть либо a, либо a^{-1}.

Любой автоморфизм должен переводить образующую в образующую $|G| = n$ — конечная циклическая группа, тогда существует $\varphi(n)$ — автоморфизм, $a \to a^m$ если $(m, n) = 1$.

Определение. Группа, центр которой состоит только из нейтрального элемента и все автоморфизмы внутренние, называется *совершенной*.

Пример 28. S_n при $n = 3, 4, 5$ и $n > 6$ совершенны.

Пример 29. Для S_6 фактор-группа группы всех автоморфизмов по группе внутренних автоморфизмов имеет индекс 2.

18. Свободные группы

Пусть $S = \{s_1, s_2, \ldots, s_m\}$, где s_i, s_j — буквы.

Определение. Последовательность букв алфавита называется словами.

Определение. Присоединение к данному слову справа второго слова называется умножением слов. Пустое слово — нейтральный элемент, т. е. играет роль единицы.

Определение. Построенная таким образом полугруппа называется *свободной полугруппой*, порожденной данным алфавитом.

Данная полугруппа группой не является, т. к. у не пустого слова не может быть обратного.

Добавим $\overline{S} = \{\overline{s}_1, \overline{s}_2, \ldots, \overline{s}_m\}$ — алфавит. Будем строить слова в $T = S \cup \overline{S}$ и введем в T отношение эквивалентности.

Определение. *Вставкой* в T назовем присоединение между двумя буквами $s_i\overline{s}_i$ или $\overline{s}_i s_i$.

Определение. *Сокращением* слова назовем исключение из слова его части вида $a_i\overline{a}_i$ или $\overline{a}_i a_i$.

Определение. Два слова назовем *эквивалентными*, если от одного из них можно перейти ко второму посредством конечного числа вставок и сокращений.

Очевидно, что это отношение рефлексивно, симметрично и транзитивно.

Если $A_1 \sim B_1$ и $A_2 \sim B_2$, очевидно, что $A_1A_2 \sim B_1B_2$. Это позволяет ввести естественным образом умножение классов слов, считая произведением класса тот класс, который содержит произведение каких-либо слов из этих классов. Класс, содержащий пустое слово, является единицей при этом умножении.

Ассоциативность следует из ассоциативности умножения слов.

Классы, содержащие s_i и $\overline{s}_i$, взаимно обратные.

Для класса, содержащего любое слово, существует обратное $b_1, b_2, \ldots, b_k$ — слово содержащееся в классе $b_i \in T$, то $\overline{b}_k, \ldots, \overline{b}_2, \overline{b}_1$ — слово, содержащееся в обратном классе. Множество классов эквивалентных слов образуют группу.

Определение. Группа, построенная таким образом, называется *свободной* группой ранга m, ${}^{Fm\approx T}\!/_{\sim}$.

Когда речь идет об обширных классах объектов, всегда приятнее иметь дело с какими-либо стандартными представителями из этих классов. Здесь роль таких представителей играют несократимые слова.

Определение. Слово в алфавите T называется *несократимым*, если в нем не стоят рядом буквы s_i и $\overline{s}_i$.

Теорема 11. *В любом классе эквивалентных слов существует одно и только одно несократимое слово.*

Доказательство. То, что для любого слова найдется эк-

вивалентное ему несократимое слово — факт очевидный, т. е. в исходном слове нужно шаг за шагом сокращать соседними двойки s_i и $\overline{s}_i$. При этом длина слова, т. е. количество букв, будет уменьшатся на две единицы, следовательно процесс сокращения должен закончится на несократимом слове после конечного числа сокращений.

Остается доказать, что различные несократимые слова не могут быть эквивалентны.

Докажем от противного.

Пусть A и B — несократимые слова. $A \sim B$, т. е. существует конечная последовательность слов

$$A = A_0, A_1, A_2, \ldots, A_{m-1}, A_m = B$$

таких, что каждое последующее слово получится из предыдущего вставкой или сокращением.

Так как A и B — несократимые слова, то переход от A_0 к A_1 только вставка, а от A_{m-1} к $A_m = B$ — сокращение.

Определение. *Полной высотой перехода* назовем сумму длин всех промежуточных слов.

Пусть A_i — слово наибольшей длины среди

$$A_0, A_1, A_2, \ldots, A_{m-1}, A_m.$$

Оно не крайнее, ибо длина $A_1 > A_0$ и $A_{m-1} > A_m$, следовательно у A_i имеется сосед слева A_{i-1} и сосед справа A_{i+1}.

Переход от A_{i-1} к A_i — вставка; от A_i к A_{i+1} — сокращение.

Здесь может быть несколько случаев:

1. при переходе от A_{i-1} к A_i вставим $b\overline{b}$ и при переходе от A_i к A_{i+1} эту пару сократим, следовательно $A_{i-1} = A_{i+1}$. Так что мы можем исключить A_i и склеить A_{i-1} и A_{i+1};

2. от A_{i-1} к A_i вставим $b\overline{b}$ и справа от этой вставки находился элемент b. При переходе от A_i к A_{i+1} в тройке соседних букв $b\overline{b}b$ сократили $\overline{b}b$, следовательно A_{i-1} и A_{i+1}. То же самое будет, если вставить $b\overline{b}$ направо от b и в тройке $\overline{b}b\overline{b}$ сократить $\overline{b}b$;

3. при переходе от A_{i-1} к A_i вставим $b\overline{b}$ и при переходе от A_i к A_{i+1} сокращается $c\overline{c}$, и эта пара не имеет общих элементов со вставкой $b\overline{b}$. Тогда переход от A_{i-1} и A_i можно сделать по другому. Буквы c и $\overline{c}$ не были вставлены при переходе от A_{i-1} и A_i, следовательно пара $c\overline{c}$ уже присутствовала в A_{i-1}. Можно было вначале сократить $c\overline{c}$, получив A'_i, затем вставить $b\overline{b}$. Длина промежутка слева A'_i на 4 меньше длины A_i, так что полная высота перехода от A и B уменьшилась на 4.

Во всех случаях полная высота перехода может быть уменьшена. Это невозможно, ибо среди переходов от A и B должен существовать переход с наименьшей полной высотой, следовательно эквивалентные несократимые слова равны, что и требовалось доказать.

Рассмотрим группу $G = \langle g_1, \ldots, g_n \rangle$, заданную системой образующих. Пусть F_n — свободная группа ранга ${}^{T}\!/_{\sim}$. Зададим отображение $\varphi : F_n \to G$ по следующему правилу:

$\varphi(s_i) = g_i$,

$\varphi(\overline{s}_i) = g_i^{-1}$

для всех $i = 1, \ldots, n$.

Докажем, что это отображение является эпиморфизмом.

Доказательство. $\varphi : T \to G$, где T — множество букв. $\omega = \ldots s_i \ldots s_j \ldots$. Вместо буквы s_i пишем g_i.

$\omega_1 \sim \omega_2$, следовательно $\varphi(\omega_1) = \varphi(\omega_2)$. Это очевидно, т.к. вставка $\varphi(s_i\overline{s}_i) = g_i g_i^{-1} = e$, а два слова эквиваленты, если от одного можно перейти к другому за кончное число вставок и сокращений.

Таким образом, φ — отображение из $F_n \approx {}^{T}\!/_{\sim} \to G$. Очевидно, что φ — гомоморфизм.

Если $\omega = \omega_1 \cdot \omega_2$, то $\varphi(\omega) = \varphi(\omega_1) \cdot \varphi(\omega_2)$ по построению φ.

Отображение φ сюръективно, т.к. $\varphi(\omega) = \ldots g_i \ldots g_i^{-1}$, а любой элемент G можно было представить в виде такого произведения g_i.

Теорема 12. *Конечно-порожденная группа есть факторгруппа свободная.*

Доказательство. Пусть $\varphi : Fn \to G$ — эпиморфизм. По первой теореме об изоморфизме ${}^{G \approx Fn}\!/_{\operatorname{Ker}\varphi}$.

1. $\operatorname{Ker}\varphi = \{e\}$, $G \approx Fn$. Можно рассмотреть $Fn = \langle s_1 \ldots s_n \rangle$ и произвести формальную замену $\overline{s} \to s^{-1}$

2. $\operatorname{Ker}\varphi \neq \{e\}$. Рассмотрим, какие элементы переходят в единицу. Существует $\omega = a_1 \dots a_m$, $a_i = \begin{cases} s_i, \\ \overline{s}_i. \end{cases}$

$\varphi(\omega) = l_G = 1$, $g_{i_1}^{e_1} \dots g_{i_m}^{e_m} = 1$, $e_k = \begin{cases} -1, \\ 1. \end{cases}$

Определение. Равенства такого сорта называются *соотношениями* в группе. $(g_{i_1}^{e_1} \dots g_{i_m}^{e_m}) = 1$.

Произведение двух соотношений — соотношение. В группе существует бесконечно много соотношений.

Определение. Система соотношений называется *определяющей* системой соотношений, если из нее можно вывести любое соотношение в группе.

Образующие свободные от соотношений называются свободными образующими.

Если $\operatorname{Ker}\varphi = \{e\}$, то в группе нет никаких отношений.

Порядок группы влияет на размерность отношений.

Пример 30. Пусть $G = \langle x \rangle$ — циклическая. $G \approx Z$, если $|x| = \infty$.

$F_1 \xrightarrow{\varphi} G$, где F_1 — алфавит $s, \overline{s}$.

$\varphi(s) = x$, $\varphi(\overline{s}) = x^{-1}$;

$\operatorname{Ker}\varphi = \{e\}$, т. к. если $\operatorname{Ker}\varphi \neq \{e\}$, то было бы соотношение $x^n = 1$ — противоречие.

Бесконечная циклическая группа есть свободная группа ранга 1, следовательно Z — свободная группа ранга 1.

Пример 31. $G = \langle a, b \rangle$, $a^2 = 1$ тогда и только тогда, когда $a = a^{-1}$, $b^3 = 1$ тогда и только тогда, когда $aba = b^2$.

Очевидным следствием из этих соотношений является $b = ab^2a$. Последние два соотношения можно записать в форме $ba = ab^2$ и $b^2a = ab$. Эти соотношения позволяют переносить образующую a через b или b^2 справа налево, заменяя b на b^2 и b^2 на b. Это позволяет записать элемент группы в форме $a^k b^m$, $k = 0, 1$ и $m = 0, 1, 2$.

Рассмотрим элементы этого вида формально с правилами умножения, вытекающими из правила переноса a справа налево и условии $a^2 = 1$ и $b^3 = 1$. Любые элементы вида $a^k\, b^m$ образуют группу. Она конечна, ее порядок равен b. Легко видеть, что она изоморфна S_3.

Пример 32. Группа задана двумя образующими a, c. Образующая c — свободна, т. к. порождает бесконечную циклическую группу. Очевидное следствие $ac^m a = c^{-m}$ для всех $m \in Z$, т. е. преобразование сопряжения посредством a вызывает в подгруппе, порожденной образующей c единственный нетривиальный автоморфизм. Из соотношения $ac^m a = c^{-m}$ следует правило переноса образующей a справа налево, именно $c^m a = ac^{-m}$.

Это правило позволяет записать любой элемент группы в виде $a^k c^m$, $k = 0, 1, 2, \ldots$, для всех $m \in Z$. Легко проследить, что символы $a^k c^m$ при с правилами, обусловленными соотно-

шениями $a^2 = 1$, $c^m a = ac^m$, действительно образуют группу

$$G = \langle a, |c/a^2 = 1, \quad aca = c^{-1} \rangle.$$

Однако при задании группы образующих соотношений имеет место одна принципиальная неприятность. Если даны 2 элемента группы, записанные через образующие, как узнать, равны они или нет? Вопрос легко решается, если соотношения таковы, что существует каноническая форма записи. Однако такой характер является скорее исключением, чем правилом.

Определение. Проблема распознавания равенства элементов группы, заданной образующими и определяющими соотношениями называется *проблемой тождества* в теории групп.

Для свободной группы она решается благодаря канонической записи элементов виде несократимых слов. Проблема получила положительное решение для групп с одним соотношением.

Однако в 1952 году Новиков П. С. доказал, что не существует алгоритма для решения проблемы тождества в группе, заданной образующей и соотношением. При этом доказательство потребовало точного определения того, что такое алгоритм. Разумеется не существования общего алгоритма для любых двух элементов не означает, что задача не может быть решена индивидуальным приемом для заданной пары элементов. Из того, что алгоритмически неразрешима массовая проблема, не следует не разрешимых индивидуальных проблем.

19. Свободные произведения групп

Определение. Пусть $G_1, G_2, \ldots, G_n$ — группы. Составим слово из произвольных элементов групп $G_1, G_2, \ldots, G_n$ в любом порядке. Для таких слов введем действие удлинения, заключающееся во вставке в любое место единицы любой группы и в замене какого-либо элемента в слове равным ему произведением двух элементов той же группы. Вставку единицы можно рассмотреть как частный случай замены элемента произведение, если отождествить единицы всех групп, т. е. вставка единицы — $a1$. Обратные операции — сокращение.

Определение. Два слова называются *эквивалентными*, если от одного к другому можно перейти за конечное число вставок и сокращений: $\omega_1 \sim \omega_2$, $\omega_3 \sim \omega_4$, следовательно $\omega_1\omega_3 \sim \omega_2\omega_4$.

Определение. Слово называется *несократимым*, если в его составе нет единиц и нет соседних элементов из одной группы.

Определение. Умножение слов *ассоциативно*, роль единицы играет пустое слово, для каждого класса существует обратный. Классы эквивалентных слов образуют группу.

Определение. Эта группа называется свободным произведением групп $G_1, G_2, \ldots, G_n$.

Теорема 13. *В каждом классе эквивалентных слов имеется единственное несократимое слово.*

Доказательство. Для построения этого несократимого слова достаточно выкинуть все единицы и перемножить соседние элементы из одной группы. Остается доказать, что неравные несократимые слова не эквивалентны. Доказательство аналогично доказательству свободных групп.

$A = A_0, A_1, \ldots, A_{M-1}, A_M = B$;

$A \sim B$ — несократимые слова.

$A = A_0$ и A_1 — удлинение, A_{M_1} и $A_M = B$ — сокращение.

Сумма длин слов — полная высота перехода. Пусть A_i — слово наибольшей длины.

$A_i \neq A_0 = A$, $A_i \neq B$;

A_{i-1} (удлинение) A_i (сокращение) A_{i+1}.

1. От A_{i-1} к A_i — b заменили на $b_1 b_2$; от A_i к A_{i+1} — $b_1 b_2$ заменили на b. $A_{i-1} = A_{i+1}$, следовательно A_i можно исключить. Высота перехода уменьшится.

2. От A_{i-1} к A_i — b заменили на $b_1 b_2$; от A_i к A_{i+1} — b_1 соединили с предшествующим элементом a той же группы или со следующим за b_2 элементом d_1, т. е. в A_{i-1} была последовательность $ab(bd_1)$ и в слове A_{i+1} вместо нее появилась последовательность $cb_2c = ab_1$. Переход можно было бы сделать иначе: сократить ab, потом удлинить, вставив вместо $ab = ab_2$. A'_i будет короче A_i на 2, т. к. полная высота уменьшится.

3. При переходе от A_{i-1} к A_i — b заменили на $b_1 b_2$; от A_i

к A_{i+1} — c_1c_2 заменили на c, не затрагивая $b = b_1b_2$. Переход от A_{i-1} к A_{i+1} можно заменить c_1c_2 на c, заменить b на b_1b_2. A'_i будет короче A_i на 2, т. к. полная высота уменьшится.

$A \sim B$ всегда можно уменьшить высоту перехода. Противоречие, ибо безграничное уменьшение высоты невозможно, т. е. любой элемент свободного произведения можно представить в виде произведения несократимых слов.

Предложение. $\langle a\rangle$ и $\langle b\rangle$ — второго порядка. Несократимые слова состоят из чередования букв $abab\ldots$. Пусть $ab = c$, $c^{-1} = ba$, $c^m = abab\ldots ab \neq 1$. C — порождает свободную циклическую группу. a и c — образующие, т. к. $b = ac$, $ca = aba = ac^{-1}$. Таким обрахом, свободное произведение двух циклических групп второго порядка изоморфно группе $\langle a, c|a^2 = 1,\ aca = c^{-1}\rangle$.

В параграфе 18 мы рассматривали группу, любой элемент которой a^kc^m, $k = 0, 1$; $m \in \mathbb{Z}$. Эта группа имеет простую геометрическую интерпретацию.

Рассмотрим на плоскости 2 параллельные прямые: $x = 0$ и $x = c$. Обозначим через a отражение относительно первой прямой, через b — отражение относительно второй прямой. $a^2 = b^2 = 1$.

a переводит x в $-x$, b переводит x в $c - x$, ab переводит x в $c - (-x) = c + x$, т. е. ab есть сдвиг на c. Группа сдвигов на кратные c есть свободная циклическая группа. По-

этому все произведения чередующихся букв a и b различны, т. е. группа, порожденная отображениями от двух параллельных прямых, есть свободное произведение двух циклических групп второго порядка.

20. Группы подстановок

Определение. *Подстановками* называются взаимнооднозначные отображения на себя конечных множеств.

Утверждение. *Число всех перестановок n-элементов равно $n!$.*

Доказательство. Докажем методом математической индукции.

Для $n = 1$ — очевидно. Пусть верно для $n - 1$.

Совокупность перестановок n-элементов разобьем на n частей по положению элемента n на первом, втором, ..., n-ом месте. В каждой части будет $(n-1)!$ перестановок, т. к. их число равно числу элементов $1, 2, \ldots, (n-1)$.

$n(n-1)! = n!$.

Пусть $\alpha_1, \alpha_2, \ldots, \alpha_n$ — некоторая перестановка

Определение. Пара (α_i, α_j), $i < j$, образует инверсию, если $\alpha_j > \alpha_i$.

Определение. Число всех пар элементов перестановки, образующих инверсию, называется *числом инверсий* в перестановке $\mathrm{inv}\,(\alpha_1, \alpha_2, \ldots, \alpha_n)$.

Определение. Перестановка, содержащая четное число инверсий, называется *четной*. Перестановка, содержащая нечетное число инверсий, называется *нечетной*.

Пример 33. $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 1 & 3 & 2 & 4 \end{pmatrix}$.

Определение. Подстановка называется *транспозицией*, если она $n-2$ элемента оставляет на своих местах, а остальные два переставляет местами.

Пусть $\{1, 2, 3, \ldots, n\}$ — множество, на которое действует подстановка. Пусть σ — некоторая подстановка.

$1, \sigma_1, \ldots, \sigma^{m-1}$ — циклическая группа, порожденная этой подстановкой. Множество переставляемых элементов разбивается на орбиты и подстановка вполне определяется тем, как она действует на каждой орбите.

Пусть a_0 — один из переставляемых элементов. a_1 — получается из a_0 подстановкой σ:

$$\sigma(a_0) = a_1 \ldots \sigma^2(a_0) = a_2 \ldots \sigma(a_1) = a_2.$$

При продолжении этого процесса мы в конце концов вернемся к a_0. $(a_0, a_1, \ldots, a_{t-1})$. Таким образом, элементы орбиты, содержащей a_0, естественно располагаются в порядке, в котором σ переставляет элементы по кругу. Таким же образом элементы располагаются на всех орбитах. Подстановка разбивается на циклы

$$\sigma = (a_0, a_1, \ldots, a_{t-1})\,(b_0, b_1, \ldots, b_{m-1}) \ldots (c_0, c_1, \ldots, c_{p-1}).$$

Если каждый цикл рассматривать как подстановку, циклически переставляющую элементы $a_0, a_1, \ldots, a_{t-1}$ и оставляющая остальные на своих местах, то мы можем рассмотреть разложение подстановки в произведение попарно не пересекающихся циклов. Легко видеть, что цикл $(a_0, a_1, \ldots, a_{t-1})$ допускает такое разложение в произведение транспозиций:

$$(a_0, a_1, \ldots, a_{t-1}) = (a_0, a_1)\,(a_0, a_2), \ldots, (a_0, a_{t-1}),$$

следовательно цикл нечетной длины — четная подстановка, а цикл четной длины — нечетная. Поэтому четность или нечетность подстановки совпадает с четностью или нечетностью количества циклов четной длины.

Предложение. σ — подстановка разложенная в произведение попарно непересекающихся циклов. τ — другая подстановка. Тогда, чтобы получить подстановку $\tau^{-1}\sigma\tau$, нужно сделать подстановку τ в каждом цикле подстановки σ.

Доказательство. Пусть

$$\sigma = (a_0, a_1, \ldots, a_{t-1})\,(b_0, b_1, \ldots, b_{m-1}) \ldots (c_0, c_1, \ldots, c_{p-1}), \quad (1)$$

$$\tau = \begin{pmatrix} a_0, a_1, \ldots, a_{t-1}, b_0, b_1, \ldots, b_{m-1}, c_0, c_1, \ldots, c_{p-1} \\ a'_0, a'_1, \ldots, a'_{t-1}, b'_0, b'_1, \ldots, b'_{m-1}, c'_0, c'_1, \ldots, c'_{p-1} \end{pmatrix}, \quad (2)$$

τ^{-1} — строчки наоборот.

Проследим за действием подстановки $\tau^{-1}\sigma\tau$ на элементы $a'_0, a'_1, \ldots, a'_{t-1}$. $\tau^{-1} : a'_0 \to a_0$, $\sigma : a_0 \to a_1$, $\tau : a_1 \to a'_1$, следовательно $\tau^{-1}\sigma\tau : a'_0 \to a'_1$.

Аналогично $a'_1 \to a_1 \to a_2 \to a'_2$.

$a'_{t-1} \to a_{t-1} \to a_1 \to a'_1$ следовательно $(a'_0, a'_1, \ldots, a'_{t-1})$ — замыкается. То же самое происходит с остальными циклами.

Теорема 14. *Для того, чтобы две подстановки были сопряжены, необходимо и достаточно, чтобы они имели разложение на циклы одинаковых порядков.*

Доказательство. Необходимость следует из доказанного предложения. Достаточность из того, что в симметрической группе существуют подстановки, переводящие любое расположение элементов в любое другое.

В силу этой теоремы, число классов сопряженных элементов в группе S_n равно числу разбиения числа u на слагаемые, порядок которых безразличен. Так, число 5 допускает разбиения:

$$5 = 5, \quad 5 = 4 + 1, \quad 5 = 3 + 2, \quad 5 = 3 + 1 + 1, \quad 5 = 2 + 2 + 1,$$
$$5 = 2 + 1 + 1 + 1, \quad 5 = 1 + 1 + 1 + 1 + 1,$$

следовательно в S_4 — 7 классов сопряженных элементов.

Предложение. Пусть в некоторой перестановке σ сделана транспозиция. Она равна произведению нечетного числа транспозиций соседних элементов.

Доказательство. $(a, b, \ldots, c, d, e, \ldots, d, g, h, \ldots, k, l)$ — перестановка. Транспозиция (c, h). Пусть m — число элементов, лежащие между c и h.

Переставляем местами c и d, затем c и e, ..., c и f, c и g. Получится $a, b, \ldots, d, e, \ldots, f, g, c, h, \ldots, k, l$. После m транспозиций, теперь переставим c и h:

$a, b, \ldots, d, e, \ldots, f, g, h, c, \ldots, k, l$.

Перегоним h на место, где стояло c:

$a, b, \ldots, h, d, e, \ldots, f, g, c, \ldots, k, l$. Как будто сделали одну транспозицию. Всего $m + 1 + m = 2m + 1$ транспозиций соседних элементов.

Предложение. При перестановке соседних элементов число инверсий в перестановке меняется на противоположную.

$i_1(a, b, \ldots, c, d, e, f \ldots, k, l)$;

$i'_1(a, b, \ldots, c, d, e, f \ldots, k, l)$.

Сравним число инверсий.

i_1 и i'_1 — число инверсий в парах, не содержащих элементов d и e.

i_2 и i'_2 — число инверсий в парах, содержащих один из элементов d и e.

i_3 и i'_3 — число инверсий в парах d, e.

Через i и i' обозначим полное число инверсий.

$i = i_1 + i_2 + i_3$, $\quad i' = i'_1 + i'_2 + i'_3$.

$i_1 = i'_1$ — очевидно, $i_2 = i'_2$, т. к. расположение d и e относительно остальных элементов одинаково в обоих перестановках.

Пусть $i_3 = 0$, следовательно $i'_3 = 1$, и если $i_3 = 1$, то $i'_3 = 0$.

$i'_1 - i_1 = \pm 1$.

Следствие. Если в перестановке сделать транспозицию соседних элементов, то четность изменится на противоположную.

Следствие. Любая транспозиция меняет четность перестановки.

Утверждение. *Число четных перестановок равно числу нечетных.*

Доказательство. Пусть число четных перестановок — a, нечетных — b.

Рассмотрим множество четных перестановок. Совершив в них одну и туже транспозицию $(1, 2)$, мы получим попарно различные нечетные перестановки, $a \leqslant b$, и наоборот, $b \leqslant a$, следовательно $a = b$.

Следствие. Если во всех четных перестановках сделать одну и туже транспозицию, то мы получим все нечетные перестановки.

Утверждение. *Любая перестановка может быть получена из другой посредством нескольких транспозиций.*

Доказательство. Докажем, используя метод математической индукции.

$n = 2$ — очевидно, для $n = 1$ доказано.

Пусть $n > 2$.

Пусть $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ и $(\beta_1, \beta_2, \ldots, \beta_n)$ — две длинные перестановки.

Если $\alpha_1 = \beta_1$, то от $(\alpha_2, \ldots, \alpha_n)$ и $(\beta_2, \ldots, \beta_n)$ в силу ин-

дукционного предположения можно перейти от $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ к $(\beta_1, \beta_2, \ldots, \beta_n)$ тем же способом.

Пусть $\alpha_1 \neq \beta_1$. Тогда $\beta_1 = \alpha_i$, $i \neq 1$. Сделав в $(\alpha_1, \alpha_2, \ldots, \alpha_n)$ транспозицию (α_1, α_i), мы перейдем к новой перестановке, у которой на первом месте $\alpha_i = \beta_1$.

Утверждение. *Любая подстановка может быть представлена в виде произведений транспозиций.*

21. Группы преобразований

Пусть M — множество точек на плоскости. G — группа всех движений плоскости.

Стабилизатором точки является группа вращений вокруг этой точки. Между точками плоскости и левыми классами смежности группы всех движений по группе вращений вокруг точки имеется изоморфное соответствие. Элементарная геометрия изучает свойства геометрических фигур, остающиеся неизменными при движении. Одно из основных понятий геометрии — расстояние между двумя точками, можно рассмотреть как инвариантную величину, связывающую пару классов смежности полной группы движений плоскости по подгруппе вращений.

Пусть пара групп $H \subset G$ определяет некоторую геометрию, в которой точками являются левые классы смежности G по H, а движениями — правые умножения классов смежности на элементы из G. Взгляд на геометрию с точки зрения тео-

рии групп был развит Клейном в конце 19-го века. Геометрия Лобачевского укладывается в эту схему следующим образом.

Рассмотрим группу дробно-линейных преобразований

$$z \to \frac{\alpha z + \beta}{\gamma z + \delta}$$

комплексных чисел $\alpha, \beta, \gamma, \delta \in R\,,\ \alpha\delta - \beta\gamma = 1\,.$

Верхняя полуплоскость оказывается однородным пространством для этой группы. Действительно, пусть $z = x + yi\,,$ $y > 0\,.$

$$\frac{\alpha z + \beta}{\gamma z + \delta} = \frac{\alpha\gamma(x^2 + y^2) + (\alpha\delta + \beta\gamma)x + \beta\delta + (\alpha\delta - \beta\gamma)yi}{(\gamma x + \delta)^2 + \gamma^2 y^2},$$

так что мнимая часть числа $\dfrac{\alpha z + \beta}{\gamma z + \delta}$ равна

$$\operatorname{Im} \frac{\alpha z + \beta}{\gamma z + \delta} = \frac{y}{(\gamma x + \delta)^2 + x^2 y^2} > 0.$$

Легко проследить, что для любой пары z и $z'\,,$ $\operatorname{Im} > 0\,.$

Существуют $\alpha, \beta, \gamma, \delta \in R\,,\ \alpha\delta - \beta\gamma = 1$ такие, что

$$z' = \frac{\alpha z + \beta}{\gamma z + \delta}.$$

Пусть $z' = x' + y'i\,,\ z = x + yi\,.$

$$(x' + y'i)\big(\gamma(x + yi) + \delta\big) = \alpha(x + yi) + \beta.$$

Пусть $\delta = 0\,,$ тогда

$$\alpha = \gamma\frac{xy' + x'y}{y}, \quad \beta = -\frac{\gamma \cdot y'(x^2 + y^2)}{y},$$

$$\alpha\delta - \beta\gamma = \frac{\gamma^2 y'(x^2 + y^2)}{y}.$$

Пусть $\gamma = \sqrt{\dfrac{y}{y'(x^2+y^2)}}$. Верхняя полуплоскость, в которой движения определены как указанные дробно-линейные преобразования, являются моделью Лобачевского. Она связана с моделью Пуанкаре. Стабилизатором точки i является группа, образованная преобразованием $z \to \dfrac{\alpha z+\beta}{-\beta z+\alpha}$, $\alpha^2+\beta^2=1$. Таким образом, точки плоскости Лобачевского находятся в изоморфном (по отношению к группе движений) соответствии с левыми классами смежности группы дробно-линейных преобразований $z' = \dfrac{\alpha z+\beta}{\gamma z+\delta}$ с $\alpha,\beta,\gamma,\delta \in R$, $\alpha\delta-\beta\gamma=1$ по подгруппе, составленной из преобразований $\dfrac{\alpha z+\beta}{-\beta z+\alpha}$ при $\alpha^2+\beta^2=1$.

22. Разрешимые группы

Определение. Пусть G — группа. Тогда следующая цепочка подгрупп называется *башней подгрупп*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n.$$

Определение. Башня подгрупп называется *нормальной*, если для любого $i = 0, 1, \ldots, n-1$, $G_{i+1} \lhd G_i$.

Определение. Нормальная башня называется *абелевой*, если ${}^{G_i}\!/_{G_{i+1}}$ — абелева.

Определение. Нормальная башня называется *циклической*, если для любого i ${}^{G_i}\!/_{G_{i+1}}$ — циклическая.

Определение. Пусть G — группа. Обозначим

$$G_0 = G_1, \quad G_1 = [G_0, G_0], \quad \ldots, \quad G_i = [G_{i-1}, G_{i-1}],$$
$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n.$$

Группа называется *разрешимой*, если башня обрывается на единичной подгруппе, т.е. существует $n \in N\colon \{e\} = G_n$.

Пример 34. Все абелевы группы разрешимы, т.к. башня в этом случае выглядит следующим образом.

$[G, G] = \{e\}$;
$[G, G] \supset G$.

Рассмотрим другие примеры разрешимости групп.

Пример 35. $S_3 \supset [S_3, S_3] = A_3 \supset [A_3, A_3] = \{e\}$.

Пример 36.
$S_4 \supset [S_4, S_4] = A_4 \supset [A_4, A_4] = K_4 \supset [K_4, K_4] = \{e\}$.

Пример 37. $S_n \supset [S_n, S_n] = A_n \supset [A_n, A_n] \supset \ldots$, при $n \geqslant 5$ — группа неразрешима.

Теорема 15. *Группа G разрешима тогда и только тогда, когда в группе G существует абелева башня подгрупп, образованная на единичной подгруппе*

$$G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}.$$

Доказательство. Докажем необходимость. Пусть G —

разрешима, по определению

$$G = G_0 \supset [G_0, G_0] = G_1 \supset [G_1, G_1] =$$
$$G_2 \supset \ldots \supset [G_{n-1}, G_{n-1}] = G_n = \{e\},$$

т. к. коммутант нормальная группа, то это нормальная и абелева башня (основное свойство коммутанта).

${}^{G_i}\!/_{[G_i,G_i]}$ — абелева.

Докажем необходимость.

Пусть $G = G_0 \supset G_1 \supset G_2 \supset \ldots \supset G_n = \{e\}$ — абелева башня.

$H_0 = G_0$, ${}^{G_0}\!/_{G_1}$ — абелева, следовательно $G_1 \supset H_1$;
$H_1 = [H_0, H_0]$, ${}^{G_1}\!/_{G_2}$ — абелева, следовательно
$G_2 \supset [G_1, G_1] \supset [H_1, H_1] = H_2$, следовательно $G_2 \supset H_2$.
$H_2 = [H_1, H_1]$, $H_n \supset G_n = \{e\}$, следовательно $H_n = \{e\}$.
$H_n = [H_{n-1}, H_{n-1}]$.

Теорема (Основное свойство коммутанта). ${}^{G}\!/_{T}$ — *абелева тогда и только тогда, когда* $[G, G] \subset T$.

Определение. Группа называется *простой*, если она не имеет нетривиальных нормальных делителей.

Пусть G — простая, $G \supset [G, G] = \begin{cases} G, \\ \{e\}. \end{cases}$

Если G — не абелева, следовательно $[G, G] = G$ не разрешима.

Определение. Пусть G — группа $Z(G)$.

$$G_1 = {}^{G}\!/_{Z(G)}, G_2 = {}^{G_1}\!/_{Z(G_1)}, \ldots, G_n = {}^{G_{n-1}}\!/_{Z(G_{n-1})}.$$

Если $G = \{e\}$, следовательно G называется *нильпотентной.*

Теорема 16. *Нильпотентные группы разрешимы.*

23. Конечно-порожденные абелевы группы

Рассмотрим группу $G = \langle g_1, \ldots, g_n \rangle$. Если количество образующих данной группы конечно, то группа называется *конечно-порожденной.*

В дальнейшем будем рассматривать только абелевы группы и пользоваться аддитивной формой записи групповой операции.

Так как группа $G = \langle g_1, \ldots, g_n \rangle$, то для любого $g \in G$ можно представить в следующем виде: $g = x_1 g_1 + x_2 g_2 \ldots + x_n g_n$, где $\forall\ i = 1, \ldots, n$, $x_i \in \mathbb{Z}$.

Если элемент $g \in G$ имеет бесконечный порядок, то равенство $xg = 0$ имеет место только тогда, когда $x = 0$.

Если элемент $g \in G$ имеет конечный порядок $|g| = n$, то $nx = 0$.

Определение. Натуральное число m, для которого $mg = 0$, называется *аннулятором* элемента g.

Докажите следующее утверждение самостоятельно.

Утверждение. *Минимальный аннулятор элемента равен его порядку.*

Утверждение. *Все аннуляторы элемента делятся на его порядок.*

Определение. Система образующих $\{g_1, g_2, \ldots, g_n\}$ конечно-порожденной абелевой группы называется *линейно-независимой* над $\mathbb{Z}$, если равенство

$$x_1 g_1 + x_2 g_2 + \ldots + x_n g_n = 0,$$

где $x_i \in \mathbb{Z}$ возможно только при $x_1 = x_2 = \ldots = x_n$.

Определение. Линейно-независимая система образующих называется *базисом* конечно-порожденной абелевой группы.

Теорема 17. *Если группа G обладает базисом, то любой ее элемент однозначно представляется в виде*

$$g = x_1 g_1 + x_2 g_2 + \ldots + x_n g_n,$$

где $\{g_1, g_2, \ldots, g_n\}$ — базис группы G, а $x_1, x_2, \ldots, x_n \in \mathbb{Z}$.

Доказательство. Существование такого представления вытекает из определения системы образующих. Поэтому необходимо доказать только единственность. Предположим, что элемент $g \in G$ можно представить двумя разными способами

$$g = x_1 g_1 + x_2 g_2 + \ldots + x_n g_n = y_1 g_1 + y_2 g_2 + \ldots + y_n g_n.$$

Получаем следующее равенство:

$$(x_1 - y_1)g_1 + (x_2 - y_2)g_2 + \ldots + (x_n - y_n)g_n = 0.$$

Но так как $\{g_1, g_2, \ldots, g_n\}$ — базис, то для любого i $x_i - y_i = 0$, т.е. $x_i = y_i$, и представление элемента g возможно только единственным способом. Таким образом, теорема доказана.

Следствие. Если группа G обладает базисом, то она раскладывается в прямую сумму бесконечных циклических подгрупп.

Доказательство. Пусть $G = \langle g_1, \ldots, g_n \rangle$, и $\{g_1, \ldots, g_n\}$ — базис группы G. Рассмотрим следующие циклические группы $G_1 = \langle g_1 \rangle, \ldots, G_n = \langle g_n \rangle$. Из доказанной выше теоремы любой элемент $g \in G$ представим в виде $g = x_1 g_1 + \ldots x_n g_n$. Но для любого i, $x_i g_i \in G_i$.

Таким образом, мы доказали, что $G = G_1 \oplus \ldots \oplus G_n$. Осталось доказать, что каждая G_i является бесконечной. Пусть для какого-то i группа G_i конечна. Тогда существует $m_i \in N$: $m_i g_i = 0$. Рассмотрим равенство

$$0 \cdot g_1 + 0 \cdot g_2 + \ldots + m_i \cdot g_i + \ldots + 0 \cdot g_n = 0, \quad m_i \neq 0$$

Но существование такого равенства невозможно, так как $\{g_1, g_2, \ldots, g_n\}$ — базис. Следовательно, все g_i имеют бесконечный порядок. Можно легко доказать, что для любого i, $G_i \approx \mathbb{Z}$, т.е.

$$G \approx \underbrace{\mathbb{Z} \oplus \ldots \oplus \mathbb{Z}}_{m \text{ штук}}$$

Из данного утверждения вытекает, что если конечно-порожденная группа имеет базис, то она является свободной абелевой группой ранга n.

Теорема (основная или структурная теорема конечно-порожденных абелевых групп). *Любая конечно-порожденная абелева группа может быть разложена в прямую сумму циклических групп*

$$G = G_1 \oplus G_2 \oplus \ldots \oplus G_k \oplus G_{k+1} \oplus \ldots \oplus G_t,$$

где $G_1, G_2, \ldots, G_k$ *— конечные циклические группы порядков* $m_1, m_2, \ldots, m_k$ *соответственно, причем* $m_1 | m_2 \ldots | m_k$, *а* $G_{k+1}, \ldots, G_t$ *— бесконечные циклические группы.*

Доказательство. Пусть G — конечно-порожденная абелева группа. Рассмотрим два случая, когда G обладает базисом, и когда G базисом не обладает.

Случай, когда G обладает базисом, вытекает из доказанного выше. Осталось рассмотреть случай, когда G не обладает базисом. Для доказательства будем использовать индукцию по t, где t — количество элементов в минимальной системе образующих группы G.

1) *База индукции.* Пусть $t = 1$. В этом случае группа G является циклической, $G = \langle a_1 \rangle$, и теорема верна.

2) *Индукционная гипотеза.* Пусть теорема верна для любой абелевой группы G, для которой минимальная система образующих состоит из $t - 1$ элементов.

3) *Индукционный переход.* Пусть G — абелева группа, и ее минимальная система образующих содержит t элементов. Так как мы рассматриваем группу G, которая не содержит базиса, следовательно минимальная система образующих $\{a_1, \ldots, a_t\}$ группы G является линейно зависимой. Рассмотрим

$$x_1a_1 + x_2a_2 + \ldots + x_ta_t = 0,$$

в котором существует хотя бы один $x_i \neq 0$. Выполнено также следующее равенство:

$$-x_1a_1 - x_2a_2 - \ldots - x_ta_t = 0.$$

Таким образом, из двух этих комбинаций можно выбрать такую, что $x_i \neq 0$ еще и является положительной.

Существует набор целых чисел $(x_1, x_2, \ldots, x_t)$, в которых какая-то компонента $x_i > 0$.

Определим множество таких наборов, как

$$X = \Big\{(x_1, \ldots, x_t) \mid x_1 \ldots x_t \in \mathbb{Z} \quad \exists\{a_1, \ldots, a_t\}$$

— минимальная система образующих, такая, что

$$x_1a_1 + \ldots x_ta_t = 0\Big\}.$$

Пусть m_1 — минимальное целое положительное число, которое встречается в наборах из множества X. Можно считать, что число m_1 встречается как первая компонента. Таким образом, существует набор $(m_1, x_2, \ldots, x_t) \in X$ такой, что для некоторой системы образующих $\{a_1, a_2, \ldots, a_t\}$

$$m_1a_1 + x_2a_2 + \ldots + x_ta_t = 0.$$

Докажем, что m_1 делит x_i для любого i.

$i = 2, \ldots, m$, $x_i = m_1 \cdot q_i + r_i$, $0 \leqslant r_i \leqslant m_i$.

$$m_1(a_1) + (m_1 q_1 + r_2)a_2 + \ldots + (m_1 q_t + r_t)a_t = 0,$$

$$m_1(a_1 + q_2 a_2 + \ldots + q_t a_t) + r_2 a_2 + \ldots r_t a_t = 0.$$

Обозначим $b = a_1 + q_2 a_2 + \ldots + q_t a_t$.

$$m_1 b + r_2 a_2 + \ldots + r_t a_t = 0.$$

Если бы $b_1 = 0$, то $a_1 = -q_2 a_2 - \ldots - q_t a_t$, т.е. система $\{a_1, a_2, \ldots, a_t\}$ являлась бы не минимальной системой образующих. Следовательно, $b_1 \neq 0$.

Мы получили систему образующих вида $b_1, a_2, \ldots, a_t$ для которой существует набор $(m_1, r_2, \ldots, r_t) \in X$. В силу минимальности m_1, $r_2 = \ldots = r_t = 0$. Так как $m_1 b_1 = 0$ и m_1 — минимальный, то порядок b_1 равен m_1.

Обозначим $G_1 = \langle b_1 \rangle$, а $H = \langle a_2, a_3, \ldots, a_t \rangle$. Докажем, что G раскладывается в прямую сумму этих подгрупп, т.е. $G = G_1 \oplus H$.

1. Любой элемент $g \in G$ действительно можно представить в виде суммы элементов $g_1 \in G$ и $h \in H$, т.е.

$$G = \langle b_1, a_2, \ldots, a_t \rangle = \langle b_1 \rangle + \langle a_2, \ldots, a_t \rangle = G_1 + H.$$

2. Докажем, что пересечение G_1 и H содержит только нейтральный элемент, т.е. $G_1 \cap H = \{0\}$.

Пусть $y \in G_1 \cap H$. Так как $y \in G_1$, а $G_1 = \langle b_1 \rangle$, то $y = x_1 b_1$; причем $0 \leqslant x_1 < m_1$.

Так как $y \in H$, то $y = x_2a_2 + \ldots + x_ta_t$, следовательно $x_1b_1 = x_2a_2 + \ldots + x_ta_t$, откуда $x_1b_1 - x_2a_2 - \ldots - x_ta_t = 0$.

Таким образом, мы получили набор $(x_1, x_2, \ldots, x_t) \in X$, причем $0 < x_1 < m_1$; но в силу минимальности m_1 такого набора в X не существует, следовательно $x_1 = 0$, и $y_1 = 0$.

Таким образом, мы доказали, что $G = G_1 \oplus H$. Рассмотрим подгруппу $H = \langle a_2, \ldots, a_t \rangle$. Ее система образующих состоит из $t-1$ элемента. Заметим, что для этой группы H не существует системы образующих из меньшего числа элементов. К H применим индукционную гипотезу. Следовательно,

$$H = G_2 \oplus \ldots \oplus G_k \oplus G_{k+1} \oplus \ldots \oplus G_t,$$

а группа G в этом случае раскладывается в прямую сумму следующим образом:

$$G = G_1 \oplus H = G_1 \oplus G_2 \oplus \ldots \oplus G_k \oplus G_{k+1} \oplus \ldots \oplus G_t,$$

где G_i, $1 \leqslant i \leqslant k$, имеют конечный порядок $|G_i| = m_i$, а G_j, $k+1 \leqslant j \leqslant t$ имеют бесконечный порядок. Осталось доказать, что $m_i | m_{i+1}$.

Проведем доказательство на примере $i = 1$, т.е. докажем, что $m_1 | m_2$. Рассмотрим набор $(m_1, m_2, 0, \ldots, 0)$. Покажем, что он принадлежит множеству X.

Для любого i, $G_i = \langle b_i \rangle$, $m_1b_1 + m_2b_2 + 0 \cdot b_3 + \ldots + 0 \cdot b_t = 0$, т.к. $m_1b_1 = 0$ и $m_2b_2 = 0$, и т.к. $\{b_1, b_2, b_3, \ldots, b_t\}$ — система образующих для G, то и $(m_1, m_2, 0, \ldots, 0)$ — набор из X.

Разделим m_2 на m_1 с остатком: $m_2 = m_1 q_1 + r_1$. Подставим это в равенство

$$m_1 b_1 + (m_1 q_1 + r_1) b_2 + 0 \cdot b_3 + \ldots + 0 \cdot b_t = 0;$$
$$m_1 (b_1 + q_2 b_2) + r_1 b_2 + 0 \cdot b_3 + \ldots + 0 \cdot b_t = 0.$$

Пусть $\widetilde{b} = b_1 + q_1 b_2 \neq 0$, т.к. $\{b_1, b_2, b_3, \ldots, b_t\}$ — минимальная система образующих. $b_1 = \widetilde{b} - q_1 b_2$. Получили новую систему образующих $\{\widetilde{b}, b_2, b_3, \ldots, b_t\}$ и новый набор $(m_1, r_1, 0, \ldots, 0) \in X$, но в силу минимальности m_1, $r_1 = 0$.

Определение. Абелева группа называется *группой без кручения*, если она не имеет элементов конечного порядка.

24. Конечные абелевы группы

Основные свойства для этих групп выглядят аналогично свойствам из предыдущего параграфа, поэтому приведем их без доказательства.

Теорема 18. *Пусть G — конечная абелева группа. Тогда существует единственный набор целых положительных чисел, больших единицы $m_1, m_2, \ldots, m_k \in \mathbb{Z}_+$ такой, что $G = G_1 \oplus \ldots \oplus G_k$, где для любого i, G_i — циклическая группа порядка m_1 и $m_1 | m_2 | \ldots | m_k$, при этом порядок G равен произведению m_i: $|G| = m_1 m_2 \ldots m_k$.*

Определение. Набор $(m_1, m_2, \ldots, m_k)$, представленный в предыдущей теореме, называется *типом* абелевой группы.

Определение. Пусть $n > 1$ — целое. *Разбиением* числа n называется неубывающая (или невозрастающая) последовательность целых положительных чисел $(n_1, m_n, \ldots, n_k)$, сумма которых равна n.

Рассмотрим пример. Для $n = 4$ разбиения могут быть следующими:

$4 = 1 + 1 + 1 + 1\,, \quad (1, 1, 1, 1)\,;$

$4 = 1 + 1 + 2\,, \quad (1, 1, 2)\,;$

$4 = 1 + 3\,, \quad (1, 3)\,;$

$4 = 2 + 2\,, \quad (2, 2)\,.$

Обозначим $P(n)$ множество всех разбиений числа n.

Для $n = 4$ Это множество имеет вид

$P(4) = \{(1, 1, 1, 1); (1, 1, 2); (1, 3); (2, 2)\}\,.$

Утверждение. *Существует взаимно-однозначное соответствие между всеми неизоморфными абелевыми группами порядка p^n, где p — простое число и множество разбиений числа n.*

Это утверждение можно сформулировать другим образом.

Утверждение. *Число неизоморфных абелевых групп порядка p^n равно числу разбиений числа n.*

Рассмотрим все неизоморфные между собой абелевы группы порядка 2^3. Для этого запишем для каждой из них тип и определим, какой цепочке прямых сумм $\mathbb{Z}_{m_i}$ она соответствует. В первую очередь выпишем все разбиения числа 3:

$3 = 3\,;\quad 3 = 1 + 2\,;\quad 3 = 1 + 1 + 1\,.$

Таким образом, $P(3) = 3$, т.е. существует три неизоморфные абелевы группы порядка 2^3. И три их различных типа разбиения выглядят следующим образом:

$$(2^3) \approx \mathbb{Z}_8\,;\quad (2, 2^2) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4\,;\quad (2, 2, 2) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2\,.$$

Определение. Пусть G — конечная группа $|G| = m \cdot p^n$, $(p, m) = 1$. Если $S \subset G$ — подгруппа группы G и $|S| = p^n$, то S называется *силовской* подгруппой группы G.

Если $H \subset G$ — подгруппа группы G и $|H| = p^\alpha$, то H называется *примарной* подгруппой (или p-подгруппой) группы G.

Теорема 19. *Пусть A — конечная абелева группа и $|A| = p_1^{n_1}\, p_2^{n_2}\, \ldots\, p_k^{n_k}$. Тогда A раскладывается в прямую сумму своих силовских подгрупп, и это разложение единственное.*

Следующая теорема дает ответ на вопрос о количестве неизоморфных абелевых групп порядка m.

Теорема 20. *Пусть $m = p_1^{n_1}\, p_2^{n_2}\, \ldots\, p_k^{n_k}$. Тогда число всех неизоморфных абелевых групп порядка m равно*

$$\prod_{j=1}^{k} |P(n_j)|.$$

Рассмотрим пример, в котором выпишем все неизоморфные абелевы группы порядка $m = 360$. Найдем каноническое разложение числа 360:

$360 = 2^3 \cdot 3^2 \cdot 5$;

$|P(3)| = 3$;

$|P(2)| = 2$;

$|P(1)| = 1$,

Их произведение $3 \cdot 2 \cdot 1 = 6$, т.е. существует шесть неизоморфных абелевых групп порядка 360. Каждой соответствует своя комбинация разложений $2, 3$ и 1. В этом случае вначале рассмотрим цепочки прямых сумм $\mathbb{Z}_{m_i}$, а затем для каждой из них определим тип.

$H_1 \approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$;

$H_2 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$;

$H_3 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5$;

$H_4 \approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$;

$H_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$;

$H_6 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Для того, чтобы каждой H_i определить тип, вспомним, что если $(m_1, m_2, \ldots, m_k)$ — тип группы, то $m_1 | m_2 | \ldots | m_k$.

Для $H_1 \approx \mathbb{Z}_8 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_{360}$, т.к. $(8, 9, 5) = 1$, т.е. тип 360.

Для $H_2 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{180}$, тип $(2, 180)$.

Для $H_3 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{90}$, тип $(2, 2, 90)$.

Для $H_4 \approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_3 \oplus \mathbb{Z}_{120}$, тип $(3, 120)$.

Для $H_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_6 \oplus \mathbb{Z}_{60}$, тип $(2, 2, 90)$.

Для $H_6 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{30}$, тип $(2, 6, 30)$.

Упражнение 84. Выпишите все неизоморфные абелевы группы порядка $m = 250$.

Список литературы

1. Богопольский О. В. Введение в теорию групп. — 94–97. Москва–Ижевск, 2002. — 148 с.

2. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. — М.: Наука, 1982. — 205 с.

3. Тронин С. Н. Введение в теорию групп. Задачи и теоремы. Часть 1. Учебное пособие. — Казань: Казанский государственный университет им. В. И. Ульянова–Ленина, 2006. — 150 с.

4. Кострикин А. И. Введение в алгебру. Часть III. Основные структуры. — 2-е издание, исправл. — М.: Физ-мат. лит., 2001. — 272 с.

5. Белоногов В. А. Задачник по теории групп. — М., Наука, 200. — 239 с.

6. Бахтурин Ю. А. Основные структуры современной алгебры. — М.: Наука, 1990. — 320 с.

7. Фаддеев Д. К. Лекции по алгебре. — Изд. 3-е стер. — СПб.: Лань, 2004. — 415 с.

8. Винберг Э. Б. Курс алгебры. — 3-е изд., перераб. и доп. — М.: Факториал Пресс, 2002. — 544 с.

9. Шубников А. В., Копцик В. А. Симметрия в науке и искусстве. — Изд. 3-е, дополн. — Москва–Ижевск: Ин-т компьютерных исслед., 2004. — 560 с.

10. Алгебра. Учебно-методический комплекс для направления 511200 (бакалавриат) «Математика. Прикладная математика». А. С. Мерзляков, Т. М. Банникова, Н. А. Баранова. УдГУ–Ижевск, 2008. — 50 с.

11. Геометрия и алгебра. Учебно-методический комплекс для специальности 010200 «Прикладная математика и информатика». Т. М. Банникова, Н. А. Баранова. УдГУ–Ижевск, 2008. — 43 с.

Татьяна Михайловна Банникова
Наталья Анатольевна Баранова

Теория групп в задачах и упражнениях

Учебно-методическое пособие

Напечатано в авторской редакции
с оригинал-макета заказчика

Подписано в печать _____ Формат $60\times84\ 1/16$

Печать офсетная. Уч.-изд. л.5,1. Усл. п.л. 5,58
Тираж 100 экз. Заказ № _____.

Издательство «Удмуртский университет»
426034, г. Ижевск, ул. Университетская, 1, корп. 4.