Министерство общего и профессионального образования
Российской Федерации
Нижегородский государственный университет
им. Н. И. Лобачевского
Механико-математический факультет
Кафедра геометрии и высшей алгебры

АЛГЕБРАИЧЕСКИЕ СИСТЕМЫ
ЧАСТЬ 2

Методическая разработка

Нижний Новгород, 1998

Typeset by $\mathcal{AMS}$-TEX

УДК 519
Алгебраические системы. Часть 2. Сост. М.И. Кузнецов, С.А. Тюрин.-
Н.Новгород: ННГУ, 1998.

В методической разработке отражены следующие темы курса "Алгебра и теория чисел" для студентов-математиков механико-математического факультета ННГУ: действия групп на множествах, теоремы Силова, разрешимые и простые группы, произведения групп, задание групп образующими и соотношениями, конечно порожденные абелевы группы.
Составители: проф. М.И. Кузнецов, доц. С.А. Тюрин
Рецензент: зав. кафедрой математики
радиофизического факультета ННГУ, проф. Г.А. Уткин

Нижегородский государственный университет им. Н.И. Лобачевского. 1998

4. Действие группы на множестве.

Пусть G – группа, M – множество, $S(M)$ – группа взаимно однозначных отображений множества M на себя. Говорят, что *группа G действует на множестве M*, если задан гомоморфизм Φ группы G в группу $S(M)$. То есть каждому $g \in G$ поставлено в соответствие взаимно однозначное отображение Φ_g множества M на себя, причем:

$$\Phi_{g_1 g_2} = \Phi_{g_1} \circ \Phi_{g_2}. \tag{1}$$

Если $x \in M$, то принято обозначать $\Phi_g(x)$ через gx. В этих обозначениях $(g_1 g_2)x = g_1(g_2 x)$. По свойству гомоморфизмов $\Phi_e = e_M$, где e_M – тождественное отображение M на M (т.е. единица в группе $S(M)$), или $ex = e_M(x) = x$ для любого $x \in M$. Таким образом, если задано действие Φ группы G на множестве M, то отображение $G \times M \longrightarrow M$, определенное по правилу $(g, x) \mapsto gx = \Phi_g(x)$, обладает свойствами

$$(g_1 g_2)x = g_1(g_2 x) \text{ для любых } g_1, g_2 \in G,\ x \in M, \tag{2}$$

$$ex = x \text{ для любого } x \in M. \tag{3}$$

Обратно, если задано отображение $G \times M \longrightarrow M$, $(g, x) \mapsto gx \in M$, удовлетворяющее условиям (2)–(3), то соответствие $\Phi : G \longrightarrow S(M)$, $g \mapsto \Phi_g$, где $\Phi_g(x) = gx$ для любого $x \in M$, является гомоморфизмом групп и, следовательно, задает действие группы G на множестве M. Поэтому часто действие группы G на множестве M определяют как отображение $\varphi : G \times M \longrightarrow M$, $(g, x) \mapsto \varphi(g, x) = gx \in M$, удовлетворяющее условиям (2)–(3). Отметим, что в этом определении gx – просто краткое обозначение для $\varphi(g, x)$.

4.1. Пусть $M = \{1, 2, 3, 4\}$ – множество из четырех элементов, $S(M) = S_4$, $G = \{e, a, b, ab\}$ – четверная группа Клейна (см. пример 1.10). Зададим действие группы G на M. Для этого построим отображение $\Phi : G \longrightarrow S_4$. Положим

$$\Phi_e = e,\ \Phi_a = (12)(34),\ \Phi_b = (13)(24),\ \Phi_{ab} = (14)(23).$$

Легко проверить (проверьте !), что $\Phi_u \circ \Phi_v = \Phi_{uv}$ для любых $u, v \in G$. Таким образом, $\Phi : G \longrightarrow S_4$ – гомоморфизм и G действует на M.

4.2. Пусть $M = \{1, \ldots, n\}$, $G = S_n$, $\Phi : G \longrightarrow S_n$ –тождественный гомоморфизм. Тогда S_n, очевидно, действует на M.

4.3.*Действие группы на себе сопряжениями.*
Пусть G –группа, Φ_g – отображение, определенное по правилу $\Phi_g(x) = gxg^{-1}$, $x \in G$. Φ_g – взаимно однозначное отображение множества G на себя. Действительно, если $gxg^{-1} = gyg^{-1}$, то $x = y$, т.е. Φ_g – инъективное отображение; если $z \in G$, тогда $z = gxg^{-1}$, где $x = g^{-1}zg$, т.е. Φ_g – сюръективное отображение.

$$\Phi_{g_1 g_2}(x) = (g_1 g_2)x(g_1 g_2)^{-1} = g_1(g_2 x g_2^{-1})g_1^{-1} = (\Phi_{g_1} \circ \Phi_{g_2})(x).$$

Итак, $\Phi_{g_1 g_2} = \Phi_{g_1} \circ \Phi_{g_2}$, следовательно, Φ определяет действие группы G на себе. Найдем $\ker \Phi$.

$$g \in \ker \Phi \Longleftrightarrow \Phi_g(x) = gxg^{-1} = x \text{ для любого } x \in G$$

$$\Longleftrightarrow gx = xg \text{ для любого } x \in G \Longleftrightarrow g \in Z(G)\text{–центр группы } G.$$

Отображение $\Phi_g : G \longrightarrow G$ называется *сопряжением*.
Если H – нормальная подгруппа в G, то $H = gHg^{-1} = \Phi_g(H)$ и, следовательно, ограничение $\Phi_g|_H$ определяет *действие группы G сопряжениями на нормальной подгруппе H*.
Пусть $P(G)$ – множество подмножеств группы G. Для подмножества $A \in P(G)$, $g \in G$ положим $\Phi_g(A) = gAg^{-1}$. В результате мы получаем *действие группы G сопряжениями на множестве своих подмножеств*. Если вместо $P(G)$ взять множество подгрупп группы G, то мы получим *действие группы G сопряжениями на множестве своих подгрупп*.
Элементы $x, y \in G$ называются *сопряженными*, если $y = gxg^{-1}$ для некотрого $g \in G$. Аналогично, две подгруппы H_1, $H_2 \subset G$ называются *сопряженными*, если $H_2 = gH_1g^{-1}$ для некоторого $g \in G$.

4.4. *Действие группы на себе левыми сдвигами.*
Пусть G – группа $g \in G$. Левым сдвигом в G называется отображение $L_g : G \longrightarrow G$, $L_g(x) = gx$, $x \in G$. L_g – взаимно однозначное отображение множества G на себя: $L_g(x) = L_g(y) \Rightarrow x = y$; если $z \in G$, то $z = L_g(x)$, где $x = g^{-1}z$. Далее, $L : G \longrightarrow S(G)$, $L : g \mapsto L_g$ – гомоморфизм, так как $L_{g_1 g_2}(x) = (g_1 g_2)x = g_1(g_2 x) = L_{g_1} \circ L_{g_2}(x)$. Таким образом, группа G действует на себе *левыми сдвигами*.
Найдем $\ker L$. $gx = x$ для любого $x \in G \Rightarrow g = e$. Следовательно, $\ker L = \{e\}$.

Если G –конечная группа, $|G| = n$, то $L(G)$ – подгруппа в $S(G) = S_n$. Так как $\ker L = \{e\}$, то $L(G) \cong G$ (по теореме о гомоморфизмах). Таким образом, любая конечная группа изоморфна некоторой подгруппе в группе подстановок достаточно высокой степени (*теорема Кэли*). В этом смысле симметрические группы – "самые большие" группы.

Пусть M – векторное пространство над полем K, $GL(M)$ – группа невырожденных линейных операторов на пространстве M. Гомоморфизм $\rho : G \longrightarrow GL(M)$ называется *линейным представлением* (или просто *представлением*) группы G в пространстве M, пространство M называется *пространством представления* ρ, а размерность M – *степенью представления* ρ. Так как $GL(M)$ – погруппа в $S(M)$, то представление группы G в пространстве M соответствует действию группы G на M линейными преобразованиями.

Пусть группа G действует на множестве M. Зафиксируем элемент $m \in M$. Множество элементов вида gm, где g пробегает всю группу G, называется *G-орбитой* (или просто *орбитой*) элемента m.

Две орбиты либо не пересекаются, либо совпадают и, следовательно, образуют разбиение множества M. Этому разбиению соответсвует отношение эквивалентности на M, при котором два элемента $m, n \in M$ эквивалентны тогда и только тогда,

когда существует элемент $g \in G$, такой, что $gm = n$, т.е. орбиты элементов m и n совпадают.

Говорят, что группа G действует на множестве M *транзитивно*, если для любых $x, y \in M$ существует $g \in G$, такой, что $gx = y$. Иначе, есть лишь одна G-орбита в M. В общем случае орбит может быть много, но на каждой орбите G действует транзитивно.

Пусть G действует на множестве M. *Стабилизатором* $St(x)$ элемента $x \in M$ называется множество всех $g \in G$, таких, что $gx = x$. Очевидно, $St(x)$ – подгруппа в G.

Пусть G – конечная группа, действующая на множестве M, $x \in M$. Обозначим через Gx орбиту элемента x. Тогда $|Gx| = (G : St(x))$ – *формула длины орбиты*. Таким образом, $|Gx|$ делит $|G|$. Если $x = gy$, то $St(x) = gSt(y)g^{-1}$.

4.5. Пусть $G = \mathbb{R}^+$ –группа положительных вещественных чисел с операций умножения. На плоскости E^2 задана декартова прямоугольная система координат Oxy. Определим действие $\mathbb{R}^+$ на E^2. Если $m \in E^2$, $m = (x, y)$, $\alpha \in \mathbb{R}^+$, то $\alpha m = (\alpha x, \alpha y)$. Орбитами являются лучи, сходящиеся к началу координат, и одна точка O.

В этом примере $St(m) = \{1\}$, когда $m \neq O$ и $St(O) = G$.

4.6. Пусть G и M как в предыдущем примере. Определим действие G на M по правилу: $\alpha \in \mathbb{R}^+$, $m = (x, y)$, $\alpha m = (\alpha x, \alpha^{-1} y)$. Если $n = (x_0, y_0)$, $x_0 y_0 \neq 0$, то орбитой Gn является та ветвь гиперболы $xy = x_0 y_0$, на которой лежит точка n. Кроме того, орбитами являются четыре полуоси и одна точка O.

4.7. Пусть G – конечная группа. G действует на себе сопряжениями. Орбита состоит из элементов, сопряженных между собой, и называется *классом сопряженных элементов*. Стабилизатор элемента x называется в этом случае *централизатором* x (обозначение – $C_G(x)$) и состоит из элементов, перестановочных с x. По формуле длины орбиты число элементов, сопряженных с элементом x, равно индексу централизатора элемента x. Класс сопряженных элементов состоит из одного элемента x тогда и только тогда, когда x перестановочен со всеми элементами из группы G, т.е. когда x принадлежит центру $Z(G)$ группы G. Так как группа G разбивается на попарно непересекающиеся классы сопряженных элементов, то число элементов в группе равно сумме длин различных классов сопряженных элементов. Выделяя отдельно классы, состоящие из одного элемента, мы получаем *формулу классов*:

$$|G| = |Z(G)| + \sum_{\alpha=1}^{s} (G : C_G(x_\alpha)), \tag{4}$$

где x_α, $\alpha = 1, \ldots, s$, – представители различных классов сопряженных элементов, число элементов в которых больше единицы.

4.8. Две подгруппы сопряжены (см. 4.3) тогда и только тогда, когда они принадлежат одной орбите при действии группы G сопряжениями на множестве своих подгрупп. В этом случае стабилизатор подгруппы H называется *нормализатором* подгруппы

H и обозначается через $N(H)$ или $N_G(H)$, когда надо подчеркнуть рассматриваемую группу G. Таким образом, $N(H) = \{g \in G |\ gHg^{-1} = H\}$. Очевидно, $H \subset N(H)$ и $N(H)$ – максимальная подгруппа в G, содержащая H, в которой H является нормальной подгруппой. По формуле длины орбиты число различных подгрупп в G, сопряженных с подгруппой H равно $(G : N(H))$.

4.9. Пусть $G = S_3$. Найдем классы сопряженных элементов в G. В любой группе S_n циклы одной длины сопряжены. Действительно, если $C_1 = (i_1, \dots, i_k)$, $C_2 = (j_1, \dots, j_k)$ – два цикла длины k, тогда $C_2 = TC_1T^{-1}$, где T – любая подстановка, переводящая i_1 в $j_1, \dots$, i_k в j_k. Так как $(gxg^{-1})^m = gx^mg^{-1}$, то все элементы, сопряженные между собой имеют один и тот же порядок. Так как порядок цикла равен его длине, то циклы разных порядков не сопряжены. Каждый элемент из S_3, отличный от e, является либо циклом длины 2, либо циклом длины 3. Следовательно, группа S_3 имеет 3 класса сопряженных элементов:

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

Найдем централизаторы элементов (12) и (123). Так как индекс централизатора $C((12))$ элемента (12) равен числу элементов, сопряженных с (12), т.е. 3, а число элементов в $G = S_3$ равно 6, то по теореме Лагранжа получаем, что $|C((12))| = 2$. Мы сразу можем предъявить два элемента из $C((12))$ – e и (12). Поэтому $C((12)) = \{e,\ (12)\}$. Аналогично, $C((123)) = \{e,\ (123),\ (123)^2 = (132)$.

4.10. Пусть G – конечноя группа, H – нормальная подгруппа в G, $|H| = n$. Тогда множество $H\backslash\{e\}$ инвариантно относительно сопряжений элементами из G. Действительно, $ghg^{-1} \in H$ для любого $h \in H$, так как H – нормальный делитель. При этом, если $h \neq e$, то и $ghg^{-1} \neq e$.Таким образом, группа G действует сопряжениями на множестве $H\backslash\{e\}$. Так как $|H\backslash\{e\}| = n-1$, то действие G сопряжениями на $H\backslash\{e\}$ задает гомоморфизм $\Phi : G \longrightarrow S_{n-1}$. Ядром этого гомоморфизма является *централизатор* подгруппы H в G, т.е. подгруппа $C_G(H)$ всех элементов из G, перестановочных с любым элементом из H.

4.11. Пусть M – фигура на плоскости. Множество всех движений плоскости, отображающих фигуру M на себя образует группу. Эта группа называется *группой симметрий фигуры* M, а ее элементы – *симметриями* M. Аналогично определяются симметрии фигуры M в пространстве.

Пусть M – правильный треугольник. Всякое движение на плоскости однозначно определяется образами трех фиксированных точек, не лежащих на одной прямой (доказать!). Поэтому существует взаимно однозначное соответствие между симметриями треугольника и подстановками множества его вершин. Поэтому группа D_3 симметрий правильного треугольника изоморфна подгруппе группы S_3. Покажем, что на самом деле $D_3 \cong S_3$. Действительно, симметриями треугольника являются вращения вокруг его центра на углы $\frac{2}{3}\pi k$ $(k = 0, 1, 2)$ (они образуют подгруппу в D_3, изоморфную A_3) и отражения относительно осей симметрии треугольника (они соответствуют транспозициям в S_3).

5. Теоремы Силова. Пусть p – простое число. Группа порядка p^n называется *p-группой*. Пусть G – конечная группа, p – простое число, делящее порядок G. Подгруппа H в G называется *p-подгруппой*, если порядок H равен p^s. Если порядок H равен p^n и p^n – наибольшая степень p, делящая порядок G, то H называется *силовской* p-подгруппой в G.

Теорема Коши. *Если порядок n конечной группы G делится на простое число p, то G содержит элемент порядка p.*

Доказательство.

(a) Сначала докажем теорему для абелевой группы G.
Пусть m – *показатель* группы G, т.е. такое натуральное число, что $g^m = e$ для любого $g \in G$. Очевидно, одним из показателей конечной группы G является ее порядок. Покажем индукцией по порядку G , что порядок группы делит некоторую степень показателя. Пусть $h \in G$, $h \neq e$, $H =< h >$ – циклическая подгруппа, порожденная h. Так как G – абелева группа, то H – нормальная подгруппа в G и можно рассмотреть факторгруппу G/H. Отметим, что так как $h^m = e$, то порядок элемента h делит m. Так как порядок H равен порядку элемента h, то можно сказать, что порядок H делит m. Кроме того, m является показателем и для G/H ($\bar{g}^n = \overline{g^n} = \bar{e}$). Так как $|G/H| < |G|$, то по индуктивному предположению порядок G/H делит m^k для некоторого k. По теореме Лагранжа $|G| = |G/H||H|$, следовательно, $|G|$ делит m^{k+1}.

Пусть теперь p делит $n = |G|$. В качестве показателя m группы G возьмем произведение порядков всех элементов группы G. Так как n делит некоторую степень m, то p делит порядок некоторого элемента $x \in G$. Пусть порядок x равен ps. Тогда элемент x^s имеет порядок p. Таким образом, теорема доказана для абелевых групп.
(b) Для доказательства в общем случае также используем индукцию по порядку G. Для действия группы G на себе сопряжениями справедлива формула классов (см. (4)):

$$n = |G| = |Z(G)| + \sum_{\alpha=1}^{s} (G : C(x_\alpha)).$$

Здесь $Z(G)$ – центр группы G, x_α – представители различных классов сопряженных элементов, в которых больше одного элемента. Если p делит порядок $Z(G)$, то согласно (a) в $Z(G)$ есть элемент порядка p. Если p не делит $|Z(G)|$, то хотя бы одно из чисел $(G : C(x_\alpha))$ тоже не делится на p. Если $(G : C(x_\alpha))$ не делится на p, то из теоремы Лагранжа получаем, что порядок подгруппы $C(x_\alpha)$ делится на p. Так как $(G : C(x_\alpha)) > 1$, то $|C(x_\alpha)| < |G|$. Следовательно, к подгруппе $C(x_\alpha)$ можно применить предположение индукции. Таким образом, подгруппа $C(x_\alpha)$ а, следовательно, и группа G содержит элемент порядка p.■

Первая теорема Силова. *Если простое число p делит порядок конечной группы G, тогда G содержит силовскую p-подгруппу.*

Доказательство.

(индукция по порядку G). Если порядок G равен p, то G совпадает со своей силовской p-подгруппой и теорема справедлива. Предположим, что теорема справедлива для всех групп, порядок которых меньше порядка G. В частности, если H – собственная подгруппа в G, индекс которой не делится на p, то порядок H по теореме Лагранжа делится на ту же степень p, что и порядок G. Поэтому силовская p-подгруппа в H (которая существует по предположению индукции) является силовской p-подгруппой в G, и, следовательно, в этом случае утверждение теоремы справедливо для группы G. Предположим теперь, что индексы всех собственных погрупп в G делятся на p. Из формулы классов (см. (4)) получаем, что порядок $Z(G)$ также делится на p. Так как $e \in Z(G)$, и, следовательно, $|Z(G)| > 0$, то $|Z(G)|$ – ненулевое кратное p. По теореме Коши $Z(G)$ содержит подгруппу H порядка p. Очевидно, всякая подгруппа в $Z(G)$ является нормальной подгруппой в G. Пусть $\pi : G \longrightarrow G/H$ – каноническая проекция. Если p^s – максимальная степень p, делящая порядок G, то p^{s-1} – максимальная степень p, делящая порядок G/H. По предположению индукции G/H содержит силовскую p-подгруппу $\bar{M}$. Пусть $M = \pi^{-1}(\bar{M})$. Тогда $H \subset M$ и $\bar{M} = M/H$. Так как $|H| = p$, $|\bar{M}| = p^{s-1}$, то по теореме Лагранжа получаем, что $|M| = p^s$. Т.е. M – силовская p-подгруппа в G. Таким образом, утверждение теоремы справедливо для группы G.■

Лемма. *Пусть H – силовская p-подгруппа в G, $N(H)$ – нормализатор H в G и Q – p-подгруппа в $N(H)$. Тогда $Q \subset H$.*

Доказательство.

Так как H – нормальная подгруппа в $N(H)$, то по второй теореме о гомоморфизмах QH – подгруппа в $N(H)$ и $QH/H \cong H/H \cap Q$. Порядок факторгруппы $H/H \cap Q$ равен индексу $[H : (H \cap Q)]$ и по теореме Лагранжа делит порядок H. Так как H – p-группа, то и $H/H \cap Q$ – p-группа. Поэтому порядок подгруппы QH, равный произведению порядков $|H|$ и $|H/H \cap Q|$, есть степень p. Таким образом, силовская p-подгруппа H содержится в p-подгруппе QH. Так как силовская p-подгруппа имеет максимальный порядок среди всех p-подгрупп группы G, то $QH = H$. Поскольку $Q \subset QH$, то $Q \subset H$. ■

Вторая теорема Силова. *В конечной группе каждая p-подгруппа содержится в некоторой силовской p-подгруппе и все силовские p-подгруппы сопряжены.*

Доказательство.

Пусть T – множество силовских p-подгрупп в конечной группе G. Так как две сопряженные подгруппы имеют одинаковые порядки, то группа G действует сопряжениями на множестве T. Зафиксируем силовскую p-подгруппу H и рассмотрим ее G-орбиту T_0 в T. Стабилизатором H является подгруппа $N(H)$ – нормализатор H в G (см. 4.8). Длина орбиты T_0 равна индексу стабилизатора, т.е. $[G : N(H)]$. По определению силовской p-подгруппы $|H|$ равен максимальной степени простого числа p, делящей $|G|$. Так как $|H|$ делит $|N(H)|$ (теорема Лагранжа) и $[G : N(H)] = |G|/|N(H)|$ (теорема Лагранжа), то $|T_0| = [G : N(H)]$ не делится на p, $(|T_0|, p) = 1$.

Пусть Q – p-подгруппа в G, $|Q| > 1$. Рассмотрим теперь действие Q сопряжениями на T_0. Множество T_0 распадается на Q-орбиты. Длина каждой Q-орбиты равна

индексу стабилизатора какого-либо элемента орбиты (см. формулу длины орбиты). Стабилизатор – подгруппа в Q. Так как $|Q|$ является степенью простого числа p, то индекс любой подгруппы в Q (а значит и длина любой Q-орбиты !) также является степенью p. Так как $|T_0|$ равна сумме длин Q-орбит и $(|T_0|, p) = 1$, то в T_0 должны существовать Q-орбиты, длины которых равны $1 = p^0$. Т.е. среди силовских p-подгрупп, сопряженных относительно G подгруппе H, – это определение множества T_0, – имеется хотя бы одна подгруппа H', такая, что $qH'q^{-1} = H'$ для любого $q \in Q$. Следовательно, $Q \subset N(H')$. Применяя лемму к силовской p-подгруппе H' и p-подгруппе Q получаем $Q \subset H'$, что доказывет первое утверждение теоремы.

На самом деле мы доказали чуть больше: всякая p-подгруппа содержится в силовской p-подгруппе, сопряженной фиксированной силовской p-подгруппе H. В частности, если Q – силовская p-подгруппат, то $Q \subset H'$, где $H' = gHg^{-1}$ для некоторого $g \in G$. Так как порядки силовских p-подгрупп в G совпадают, то $Q = H'$. Т.е. любая силовская p-подгруппа Q сопряжена фиксированной силовской p-подгруппе G. ■

Третья теорема Силова. *Пусть p – простое число, делящее порядок конечной группы G. Число силовских p-подгрупп в G сравнимо с 1 по модулю p и делит порядок группы G.*

Доказательство.

В обозначениях доказательства второй теоремы Силова в качестве p-подгруппы Q рассмотрим зафиксированную силовскую p-подгруппу H и ее действие сопряжениями на $T_0 = T$ (последнее равенство составляет содержание второй теоремы Силова). Пусть $H' \in T$. Если $hH'h^{-1} = H'$ для любого $h \in H$, то по лемме, примененной к $Q = H$, получаем $H \subset H'$, и так как H, H' – силовские p-подгруппы, то $H = H'$. Таким образом, множество T имеет только один неподвижный элемент при действии H на T сопряжениями – подгруппу H. Все остальные орбиты имеют больше одного элемента и, как показано при доказательстве второй теоремы Силова, длины этих орбит являются степенями p. Так как T распадается на непересекающиеся H-орбиты, то $|T| \equiv 1(modp)$. Согласно второй теореме Силова T – множество всех силовских p-подгрупп в G. С другой стороны T – одна G-орбита при действии группы G сопряжениями на множестве своих подгрупп. Длина любой G-орбиты является делителем порядка G и, следовательно, $|T|$ делит $|G|$.■

6. Группы порядка pq. Теоремы Силова являются важным инструментом исследования структуры конечных групп. В качестве примера с их помощью мы найдем с точностью до изоморфизма все группы порядка pq, где p и q – различные простые числа, $p < q$. Пусть $|G| = pq$. Силовские p-подгруппы в G имеют порядок p и, следовательно, являются циклическими. Аналогично, силовские q-подгруппы в G – циклические.

По третьей теореме Силова число силовских q-подгрупп равно $1 + tq$ и делит $|G| = pq$. Так как $(1+tq, q) = 1$ и $p < q$, то это возможно, только когда $t = 0$. Следовательно, группа G имеет только одну силовскую q-подгруппу. Обозначим ее через Q, $Q =< b >$. Так как для любого $g \in G$ gQg^{-1} – тоже силовская q-подгруппа, то $Q = gQg^{-1}$, т.е. Q – нормальная подгруппа в G.

Число силовских p-подгрупп в G равно $1+sp$ и делит $|G|=pq$. Так как $(1+sp,p)=1$, то $1+sp$ делит q. Поэтому возможны два случая:
1) p не делит $q-1$. Тогда $1+sp$ делит q только при $s=0$ и, следовательно, группа G имеет единственную силовскую q-подгруппу P, $P=<a>$, которая является нормальной подгруппой в G. Так как $aba^{-1}\in Q$ (Q – нормальная подгруппа), то $aba^{-1}b^{-1}\in Q$. Аналогично, $ba^{-1}b^{-1}\in P$ и $aba^{-1}b^{-1}\in P$. Таким образом, $aba^{-1}b^{-1}\in P\cap Q$. $P\cap Q$ – подгруппа в P и, следовательно, $|P\cap Q|$ делит $|P|=p$. Аналогично, $P\cap Q$ – подгруппа в Q и, следовательно, $|P\cap Q|$ делит $|Q|=q$. Так как p и q – различные простые числа, то $|P\cap Q|=1$ и, значит, $P\cap Q=\{e\}$. Следовательно, $aba^{-1}b^{-1}=e$ и $ab=ba$. Поэтому $(ab)^{pq}=a^{pq}b^{pq}=e$. Если $(ab)^r=e$, то $a^r=b^{-r}\in P\cap Q=\{e\}$. Так как элементы a и b имеют порядки p и q соответственно, то p делит r и q делит r. Следовательно, pq делит r и элемент ab имеет порядок $pq=|G|$, т.е. $G=<ab>$ – циклическая группа.
2) p делит $q-1$. Если в G имеется только одна силовская p-подгруппа, то рассуждения из п.1) показывают, что $G=<ab>$ – циклическая группа.

Пусть число $1+sp$ силовских p-подгрупп в G больше 1. Так как $1+sp$ делит q (q – простое число), то число силовских p-подгрупп в G равно q. Пусть $P=<a>$ – одна из силовских p-подгрупп. Так как $Q=<b>$ – нормальная подгруппа в G и $P\cap Q=\{e\}$, то P отображается изоморфно на свой образ при канонической проекции G на G/Q. Порядок P равен $|G/Q|$, следовательно, G/Q состоит из смежных классов элементов из $P=<a>$. Таким образом, $G=\{a^ib^j,\ i=0,\dots,p-1,\ j=0,\dots,q-1\}$ и для задания умножения в G достаточно знать, как переставляются элементы a и b. Так как Q – нормальная подгруппа в G, то $a^{-1}ba=b^k$ (целое число k определено однозначно по $mod\ q$) и класс вычетов числа k по $mod\ q$ однозначно задает умножение в G. Далее,

$$b=e^{-1}be=(a^p)^{-1}b(a^p)=a^{-1}(a^{-1}(\dots(a^{-1}ba)a)\dots)a=b^{k^p}.$$

Отсюда $k^p\equiv 1(mod\ q)$. В поле $\mathbb{Z}_q$ уравнение $x^p-1=0$ имеет p решений, которые образуют циклическую подгруппу в мультипликативной группе поля $\mathbb{Z}_q$. (Позднее будет показано, что $\mathbb{Z}_q^*$ – циклическая группа порядка $q-1$. Так как p делит $q-1$, то в $\mathbb{Z}_q^*$ имеется в точности одна циклическая подгруппа порядка p. Ее элементы и являются решениями нашего уравнения.) Если k – одно из решений сравнения $x^p\equiv 1(mod\ q)$, $k\not\equiv 1$, то все другие решения, не сравнимые с 1, имеют вид $k,\ k^2,\dots,k^{p-1}$. Однако все эти решения определяют одну и ту же группу, поскольку замена образующего a подгруппы P на a^l приводит к замене k на k^l.

Итак, в случае, когда p делит $q-1$, существует две с точностью до изоморфизма группы порядка pq: одна – циклическая, другая – неабелева. В неабелевом случае

$$G=\{a^ib^j,\ i=0,\dots,p-1,\ j=0,\dots,q-1\},\ (\mathrm{a}^ib^j)(a^mb^n)=a^ia^m(a^{-m}b^ja^m)b^n=$$

$$=a^{i+m}b^{k^mj+n}.$$

Здесь k – любое решение сравнения $x^p\equiv 1(mod\ q)$, $k\not\equiv 1(mod\ q)$.

6.1. Пусть $|G|=15=3\cdot 5$. В этом случае $p=3$, $q=5$, p не делит $q-1$. Следовательно,

согласно 1) G – циклическая группа порядка 15. (Докажите этот факт, не используя теорию групп порядка pq.)

6.2. Найдем все группы порядка 6. Так как $|G| = 2\cdot 3,\ p = 2 \mid q-1 = 2$, то согласно 2) существуют только две с точностью до изоморфизма группы порядка 6: одна абелева (и, следовательно, циклическая) группа, и одна неабелева группа. Неабелева группа порядка 6 уже встречалась – это симметрическая группа S_3. Таким образом, любая неабелева группа порядка 6 изоморфна группе S_3.

7. Разрешимые группы.

Пусть G – группа, $G^{(1)}$ – коммутант группы G. Напомним, что $G^{(1)}$ – подгруппа в G, состоящая из всевозможных произведений коммутаторов $(a,b) = aba^{-1}b^{-1},\ a, b \in G$. Определим по индукции подгруппы $G^{(i)} = (G^{(i-1)})^{(1)}$, т.е. $G^{(i)}$ – коммутант подгруппы $G^{(i-1)}$. Все эти подгруппы являются нормальными делителями в G, более того, они инвариантны относительно любых автоморфизмов группы G. (Подгруппы в G, инвариантные относительно любых автоморфизмов G называются *характеристическими.*) Это следует из более общего свойства коммутантов (доказать !):
если $\varphi G_1 \longrightarrow G_2$ *– эпиморфизм, то* $\varphi(G_1^{(i)}) = G_2^{(i)}$.
Группа G называется *разрешимой*, если $G^{(n)} = \{e\}$ для некоторого n.

7.1. Всякая абелева группа G разрешима, так как уже $G^{(1)} = \{e\}$.

7.2. Пусть G – группа, H – нормальная подгруппа в G. G разрешима тогда и только тогда, когда группы H и G/H разрешимы. (Доказать !)

7.3. Пусть $G = T_2(P)$ – группа всех невырожденных верхних треугольных матриц порядка 2 над полем P. Найдем ее коммутант $G^{(1)}$. Пусть

$$A = \begin{pmatrix} a_1 & a_2 \\ 0 & a_3 \end{pmatrix},\ B = \begin{pmatrix} b_1 & b_2 \\ 0 & b_3 \end{pmatrix} \in G,$$

где $a_1 a_3,\ b_1 b_3 \neq 0$. Тогда

$$ABA^{-1}B^{-1} = \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}, \qquad \text{где } c = \frac{a_1 b_2 - a_2 b_1 + a_2 b_3 - a_3 b_2}{a_3 b_3}.$$

Выбирая подходящим образом элементы матриц A и B, мы можем получить в качестве c любой наперед заданный элемент поля P. Таким образом, $G^{(1)}$ состоит из всех матриц вида $\left(\begin{smallmatrix} 1 & c \\ 0 & 1 \end{smallmatrix}\right)$. Заметим, что любые две матрицы такого вида перестановочны, т.е. $G^{(1)}$ – абелева группа. Слеовательно, $G^{(2)} = \{e\}$ и G – разрешимая группа.

7.4. Если $G = S_3$, то $G^{(1)} = A_3,\ G^{(2)} = \{e\}$.

7.5. Если $G = S_4$, то $G^{(1)} = A_4$. Пусть $B_4 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}$ – подгруппа, состоящая из всех четных подстановок, имеющих порядок 2. Так как

порядок и четность не меняются при сопряжении, то B_4 – нормальная подгруппа в S_4. Непосредственно проверяется, что $B_4 \subset G^{(2)}$. Например, (13)(24) является коммутатором элементов (123) и (12)(34). С другой стороны, факторгруппа A_4/B_3 абелева, так как имеет порядок 3. Следовательно, B_4 содержит $A_4 = G^{(1)}$. Отсюда, $G^{(2)} = B_4$. Так как B_4 абелева, то $G^{(3)} = \{e\}$.

7.6. Пусть G – p-группа, $|G| = p^n$. Индукцией по n покажем, что G – разрешимая группа. Если $n = 1$, то G – циклическая группа и, следовательно, $G^{(1)} = \{e\}$. Пусть $n > 1$. Покажем, что G имеет нетривиальный центр. Действительно, так как индексы собственных подгрупп в G делятся на p, то из формулы классов (4) следует, что число элементов в $Z(G)$ также делится на p, т.е. $|Z(G)| = p^k > 1$. Если $Z(G) = G$, то G абелева и $G^{(1)} = \{e\}$. Если $G \neq Z(G)$, то $k < n$ и $|G/Z(G)| = p^{n-k} < |G|$. По предположению индукции $G/Z(G)$ – разрешимая группа. Теперь из 7.2 получаем, что G разрешима.

7.7. В 1963 г. Фейт и Томпсон доказали, что любая конечная группа нечетного порядка разрешима.

8. Простые группы.

Группа G называется *простой*, если она не имеет нормальных подгрупп, отличных от $\{e\}$ и G.

8.1.

Теорема Галуа. *Знакопеременная группа A_n, $n \geqq 5$, проста.*

Доказательство.

Покажем, что A_n порождается циклами длины 3, т.е. любая четная подстановка является произведением циклов вида (i, j, k). Как известно, четная подстановка раскладывается в произведение четного числа транспозиций. Поэтому достаточно показать, что произведение двух транспозиций можно представить в виде произведения циклов длины 3. Согласно 4.9 достаточно показать это для произведений (12)(13) и (12)(34), т.е. когда транспозиции зависимы и когда независимы. В первом случае получаем цикл (132). Второе произведение равно (12)(34) = (12)(13)(13)(34) = (132)(134).

Найдем централизатор элемента (123) в A_n. Так как $T(123)T^{-1} = (i_1, i_2, i_3)$, где $T(1) = i_1$, $T(2) = i_2$, $T(3) = i_3$, то $T \in C_{A_n}(123)$ тогда и только тогда, когда $T = UV$, где $U(i) = T(i)$ для $i \in \{1, 2, 3\}$ и $U(j) = j$ для $j \in \{4, \ldots, n\}$; $V(i) = i$ для $i \in \{1, 2, 3\}$, $V(j) = T(j)$ для $j \in \{4, \ldots, n\}$. Так как U перестановочно с $(1, 2, 3)$, то $U \in \{e, (123), (1, 3, 2) = (123)^2\}$. В частности, U – четная подстановка, следовательно, $V = U^{-1}T$ – четная подстановка. Очевидно, V может пробегать подгруппу четных постановок, действующих тождественно на множестве $\{1, 2, 3\}$. Эта подгруппа изоморфна A_{n-3}. Итак, $|C_{A_n}(1, 2, 3)| = 3|A_{n-3}| = 3(n-3)!/2$.

Из формулы длины орбиты получаем, что количество циклов длины 3, сопряжен-

ных в A_n циклу $(1,2,3)$, равно

$$|A_n|/|C_{A_n}(1,2,3)| = \frac{n!}{3(n-3)!} = \frac{n(n-1)(n-2)}{3}.$$

Подсчитаем число циклов длины 3 в A_n. Каждое подмножество из трех элементов $\{i_1, i_2, i_3\}$ во множестве $\{1, \dots, n\}$ определяет два цикла длины 3: (i_1, i_2, i_3), (i_1, i_3, i_2). Поэтому общее число циклов длины 3 в A_n равно $2\binom{n}{3} = \frac{n(n-1)(n-2)}{3}$. Таким образом все циклы длины 3 сопряжены в A_n циклу $(1,2,3)$.

Пусть H – произвольная нормальная подгруппа в A_n $(n \geqq 5)$, $H \neq \{e\}$. Если мы покажем, что H содержит цикл длины 3, то H будет содержать все циклы длины 3, и, следовательно, $H = G$. Таким образом, для доказательства теоремы достаточно доказать, что H содержит цикл длины 3. Пусть $t \in H$, $t \neq e$. Разложим t в произведение независимых циклов. Так как t – четная подстановка, то t не может быть транспозицией и мы имеем следующие возможности для разложения t:
1) $t = (i_1, i_2, \dots, i_k)(\dots)\dots$ – в разложении имеется цикл длины $k \geqq 4$;
2) $t = (i_1, i_2, i_3)(i_4, i_5, \dots)(\dots)\dots$ – имеется цикл длины 3 и другие циклы;
3) $t = (i_1 i_2)(i_3 i_4)(\dots)\dots$ – произведение четного числа независимых транспозиций;
4) $t = (i_1, i_2, i_3)$ – цикл длины 3.

Как отмечено выше, в случае 4) утверждение уже доказано. Поэтому рассмотрим случаи 1)-3). Так как H – нормальная подгруппа, то для любой четной подстановки w $wtw^{-1} \in H$ и, следовательно, $wtw^{-1}t^{-1} \in H$. Рассмотрим отдельно случаи 1)-3).
1). Выберем $w = (i_2, i_3, i_4)$, тогда $wtw^{-1}t^{-1} = (i_1, i_2, i_3) \in H$ и теорема доказана.
2) Выберем $w = (i_2, i_3, i_5)$, тогда $wtw^{-1}t^{-1} = (i_1, i_3, i_2, i_3, i_5) \in H$ и мы пришли к случаю 1).
3). Выберем $w = (i_2, i_3, i_4)$, тогда $wtw^{-1}t^{-1} = (i_1 i_3)(i_2 i_4) \in H$. Для простоты обозначений можно считать, что $(12)(34) \in H$. Тогда

$$(1,2,5)(12)(34)(1,2,5)^{-1}[(12)(34)]^{-1} = (1,2,5)(12)(34)(1,5,2)(12)(34) =$$

$$(1,2,5)(12)(1,5,2)(12) = (1,2,5)(1,2,5) = (1,5,2) \in H,$$

откуда следует утверждение теоремы.■

8.2. Пусть P – поле. Группа $SL_n(P)$, состоящая из матриц порядка n с элементами из поля P и с определителем 1, называется специальной линейнй группой. Факторгруппа группы $SL_n(P)$ по центру называется *проективной специальной линейной группой* и обозначается через $PSL_n(P)$ (или $L_n(q)$ в случае, когда P – конечное поле из q элементов). Справедлива следующая теорема.

Теорема Жордана - Диксона. *Для всякого конечного поля P, кроме $\mathbb{Z}_2$ и $\mathbb{Z}_3$, группа $PSL_n(P)$ проста.*

(Доказательство см. [2], стр.101-105.)

8.3. Группа $SO(3)$, состоящая из собственно ортогональных операторов трехмерного

евклидова пространства, является (бесконечной) простой группой. (См. [1], стр.320-321.)

9. Произведения групп.

9.1. Пусть G и H – две группы. Рассмотрим декартово произведение $G \times H$ множеств G и H, т.е. множество пар (g,h), $g \in G$, $h \in H$. Введем на $G \times H$ бинарную операцию

$$(g_1,h_1) \circ (g_2,h_2) = (g_1g_2, h_1h_2).$$

Легко проверить, что относительно этой операции $G \times H$ является группой. Роль единицы играет пара (e_G, e_H). Обратным к элементу (g,h) является (g^{-1},h^{-1}). Группа $G \times H$ называется *прямым произведением групп* G и H. Аналогично можно определить прямое произведение любого конечного числа групп $G_1, \ldots, G_n$. Это "внешнее" произведение групп, поскольку перемножаются, вообще говоря, различные группы.

Группа G называется *прямым произведением своих нормальных подгрупп* $H_1, \ldots, H_n$, если любой элемент $g \in G$ *однозначно* представляется в виде $g = h_1 \cdots h_n$, где $h_i \in H_i$, $i = 1, \ldots, n$. Это "внутреннее" прямое произведение, так как заданная группа G раскладывается в произведение своих подгрупп.

Теорема. *Для того, чтобы группа G являлась произведением своих нормальных подгрупп $H_1, \ldots, H_n$ необходимо и достаточно, чтобы*
1) $G = H_1 \cdot \ldots \cdot H_n$ и
2) $H_i \cap (\prod_{j \neq i} H_j) = \{e\}$ для любого $i = 1, \ldots, n$.

Доказательство.

a) Необходимость. Пусть G – прямое произведение нормальных подгрупп H_i, $i = 1, \ldots, n$. Очевидно, условие 1) выполняется. Если для некоторого i $h_i \in H_i \cap (\prod_{j \neq i} H_j)$, то h_i можно представить в виде произведения

$$h_i = h_1 \ldots h_{i-1} h_{i+1} \ldots h_n =$$

$$h_1 \ldots h_{i-1} e h_{i+1} \ldots h_n, \; h_j \in H_j.$$

Здесь сомножитель e рассматривается как элемент подгруппы H_i. С другой стороны h_i можно записать в виде произведения

$$h_i = e \ldots e h_i e \ldots e,$$

где сомножители равные e рассматриваются как элементы подгрупп H_j, $j \neq i$. В силу единственности такого разложения (G –прямое произведение нормальных подгрупп H_i !) сомножители в обоих разложениях должны быть одинаковые, в частности, для сомножителей из подгуппы H_i получаем, $h_i = e$.
b) Достаточность. Пусть выполнены условия 1)-2). Условие 1) означает, что любой элемент $g \in G$ можно разложить в произведение элементов подгрупп H_i, $i = 1, \ldots, n$. Таким образом, надо лишь доказать единственность такого разложения. Покажем

сначала, что элементы различных подгрупп H_i коммутируют, т.е. $h_ih_j = h_jh_i$, где $h_i \in H_i,\ h_j \in H_j,\ i \neq j$. Действительно, $h_ih_jh_i^{-1} \in H_j,\ h_jh_i^{-1}h_j^{-1} \in H_i$ в силу нормальности подгрупп $H_i,\ H_j$. Следовательно,

$$h_ih_jh_i^{-1}h_j^{-1} \in H_i \cap H_j \subset H_i \cap (\prod_{k\neq i} H_k) = \{e\}.$$

Допустим, что элемент $g \in G$ имеет два разложения в произведение элементов из подгрупп H_i,

$$g = h_1 \dots h_n = h'_1 \dots h'_n,\ h_i, h'_i \in H_i,$$

и для некоторого s $h_s \neq h'_s$. Учитывая перестановочность элементов из различных подгрупп H_i, получаем

$$h_s h_s^{'-1} = h_1^{-1}h'_1 \dots h_{s-1}^{-1}h'_{s-1}h_{s+1}^{-1}h'_{s+1} \dots h_n^{-1}h'_n \in H_s \cap (\prod_{j\neq s} H_j) = \{e\}.$$

Следовательно, $h_s = h'_s$. Получили противоречие. Таким образом, разложение любого элемента из G на множители из подгрупп H_i единственно.■

Отметим, что при доказательстве теоремы мы установили, что если группа G является прямым произведением нормальных подгрупп $H_i,\ i = 1 \dots, n$, то элементы из различных подгрупп H_i перестановочны. Поэтому, если $g_1 = h_1 \dots h_n,\ g_2 = h'_1 \dots h'_n$, то $g_1g_2 = h_1h'_1 \dots h_nh'_n$. Пусть $H_1 \times \dots \times H_n$ – внешнее прямое произведение подгрупп $H_i,\ i = 1, \dots, n$. Из определения внутреннего прямого произведения следует, что отображение $\varphi : H_1 \times \dots \times H_n \longrightarrow G,\ \varphi : (h_1, \dots, h_n) \mapsto g = h_1 \dots h_n \in G$ является биекцией. Приведенное выше выражение для произведения g_1g_2 означает, что φ – изоморфизм. Таким образом, если группа G является прямым произведением своих нормальных подгрупп $H_1, \dots, H_n$, то G изоморфна внешнему произведению групп $H_1 \times \dots \times H_n$. Поэтому часто не делают различия между внешним и внутренним прямыми произведениями групп.

9.2. Четверная группа Клейна B_4 изоморфна произведению двух циклических групп второго порядка. Действительно, пусть $B_4 = \{e, a, b, ab\}, a^2 = b^2 = (ab)^2 = e,\ H_1 = \{e, a\},\ H_2 = \{e, b\}$. Тогда $B_4 = H_1H_2$ и $H_1 \cap H_2 = \{e\}$. По теореме B_4 является прямым произведением своих подгрупп $H_1,\ H_2$. (Т.к. B_4 – абелева группа, то подгруппы $H_1,\ H_2$ автоматически нормальны. Покажите, не используя теорему, что каждый элемент группы B_4 единственным образом раскладывается в произведение элементов из подгрупп H_1 и H_2.)

9.3. Пусть m и n – взаимно простые натуральные числа. Группа классов вычетов $\mathbb{Z}_{mn}$ изоморфна прямому произведению $\mathbb{Z}_m \times \mathbb{Z}_n$. Действительно, классу вычетов $\bar{a}$ целого числа a по модулю mn поставим в соответствие пару $\varphi(\bar{a}) = (a', a'')$, где a' – класс вычетов числа a по модулю m, a'' – класс вычетов числа a по модулю n. Легко проверить (проверьте!), что это соответствие φ корректно, т.е. не зависит от выбора представителя a класса вычетов $\bar{a}$. Пусть (c', b'') – произвольная пара из $\mathbb{Z}_m \times \mathbb{Z}_n,\ c, b \in \mathbb{Z}$.

Согласно китайской теореме об остатках существует единственное по модулю mn целое число a, такое, что $a \equiv c(m)$, $a \equiv b(n)$, т.е. $(c', b'') = \varphi(\bar{a})$ и, следовательно, φ – сюръективное отображение. Теперь, если $\varphi(\bar{a}) = (a', a'') = \varphi(\bar{b}) = (b', b'')$, то $a \equiv b(m)$, $a \equiv b(n)$. Так как $(m, n) = 1$, то из свойств взаимно простых чисел следует, что $a \cong b(mn)$, т.е. $\bar{a} = \bar{b}$ и, значит, отображение φ инъективно. Наконец,

$$\varphi(\bar{a} + \bar{b}) = \varphi(\overline{a+b}) = ((a+b)', (a+b)'') =$$

$$(a' + b', a'' + b'') = (a', a'') + (b', b'') = \varphi(\bar{a}) + \varphi(\bar{b}),$$

т.е. $\varphi : \mathbb{Z}_{mn} \longrightarrow \mathbb{Z}_m \times \mathbb{Z}_n$ – изоморфизм.

9.4. Пусть P^n – арифметическое n-мерное пространство над полем P. По определению P^n аддитивная группа пространства P^n является произведением $\underbrace{P \times \ldots \times P}_{n}$ аддитивных групп поля P.

9.5.

Теорема. *Пусть $G_1, \ldots, G_n$ – группы, $H_1, \ldots, H_n$ – нормальные подгруппы в G_1, $\ldots$, G_n соответственно, $G = G_1 \times \ldots \times G_n$, $H = H_1 \times \ldots \times H_n$. Тогда H – нормальноя подгруппа в G и*

$$G/H \cong (G_1/H_1) \times \ldots \times (G_n/H_n).$$

Доказательство.

Пусть $\Phi : G \longrightarrow (G_1/H_1) \times \ldots \times (G_n/H_n)$ – отображение, определяемое следующим образом: $\Phi(g_1, \ldots, g_n) = (\bar{g}_1, \ldots, \bar{g}_n)$, где $\bar{g}_i = g_i H_i$. Легко проверить, что Φ – гомоморфизм групп и $\ker \Phi = H$. Следовательно, H – нормальная подгруппа в G и нужный изоморфизм следует из теоремы о гомоморфизмах.■

9.6. В аддитивной группе $\mathbb{R}^n$ рассмотрим подгруппу $\mathbb{Z}^n$, состоящую из n-наборов целых чисел. Очевидно, $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n}$. Согласно 9.3 и 9.4

$$\mathbb{R}^n/\mathbb{Z}^n \cong \underbrace{\mathbb{R}/\mathbb{Z} \times \ldots \times \mathbb{R}/\mathbb{Z}}_{n} = \underbrace{T^1 \times \ldots \times T^1}_{n}.$$

Как известно, группа $T^1 = \mathbb{R}/\mathbb{Z}$ изоморфна единичной окружности в комплексной плоскости. Геометрически прямое произведение $T^1 \times T^1$ является (2-мерным) тором. По этой причине группа $T^n = \mathbb{R}^n/\mathbb{Z}^n$ называется *n-мерным тором.*

10. Свободная группа. Задание группы образующими и соотношениями.

Пусть G – группа, S – подмножество в G. Пересечение всех подгрупп в G, содержащих S, является наименьшей подгруппой, содержащей S. Она обозначается через

$< S >$ и называется *подгруппой, порожденной множеством* S, а S называется *множеством образующих* группы $< S >$. Подгруппа $< S >$ состоит из единичного элемента и всевозможных произведений

$$s_1 s_2 \dots s_n \ (n \geq 1), \tag{1}$$

где либо $s_i \in S$, либо $s_i^{-1} \in S$.

Длиной элемента $g \in < S >$ будем называть количество сомножителей из S (или S^{-1}) в самом коротком представлении g в виде (1).

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

10.2. Известно, что любая подстановка n-ой степени является произведением транспозиций. Таким образом, транспозиции составляют множество образующих группы S_n. При доказательстве теоремы 8.1 было показано, что циклы длины 3 составляют множество образующих знакопеременной группы A_n.

Пусть X – множество. Назовем *словом над* X формальное выражение $x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n}$, где $x_i \in X$, $(i = 1, \dots, n)$, $\epsilon_i = \pm 1$. Слово называется *несократимым*, если в нем не встречаются рядом два символа x^{ϵ} и $x^{-\epsilon}$. Пустое слово, т.е. слово, не содержащее ни одного символа, будем обозначать через e. Обозначим через $F(X)$ множество, состоящее из e и всех несократимых слов. Введем умножение в $F(X)$ следующим образом. Если $f \in F(X)$, то $ef = fe = f$, если $f_1,\ f_2 \in F(X)$, то допишем к слову f_1 слово f_2 и произведем сокращения (т.е. будем последовательно вычеркивать стоящие рядом символы x^{ϵ} и $x^{-\epsilon}$, пока не получим либо пустое слово, либо несократимое слово). Полученный в результате элемент множества $F(X)$ назовем произведением $f_1 f_2$. Можно проверить, что умножение на $F(X)$ определено корректно и относительно введенного умножения $F(X)$ является группой с единичным элементом e. Обратным к элементу $f = x_1^{\epsilon_1} \dots x_n^{\epsilon_n}$ является элемент $f^{-1} = x_n^{-\epsilon_n} x_{n-1}^{-\epsilon_{n-1}} \dots x_1^{-\epsilon_1}$. Группа $F(X)$ называется *свободной группой*, порожденной множеством X.

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

10.4.

Теорема. *(Универсальное свойство свободной группы)*
Пусть G – группа, порожденная множеством образующих $\tilde{S}$, S – некоторое множество, $F(S)$ – свободная группа над S, $\varphi : S \longrightarrow \tilde{S}$ – отображение. Существует единственный гомоморфизм Φ группы $F(S)$ в G, такой, что $\Phi(s) = \varphi(s)$ для любого $s \in S$. Если φ сюръективно, то и Φ сюръективно.

Если φ сюръективно, то элементы ядра H гомоморфизма Φ называются *соотношениями* группы G над S. Любая система образующих L подгруппы H в $F(S)$ называется *определяющей системой соотношений* группы G над S. По основной теореме о гомоморфизмах $F(S)/H \cong G$. Поэтому задание множества S и множества

слов L определяет группу G с точностью до изоморфизма. Такое описание группы G называется *заданием группы образующими и соотношениями.* Обозначение: $G = (S\|L)$.

10.5. Пусть $G = B_4 = \{e,\ a,\ b,\ ab\}$ – четверная группа Клейна, $S = \{a, b\}$. Очевидно, $G =< S >$. Канонический гомоморфизм $\Phi : F(S) \longrightarrow G =< S >$ (см. 10.4.) ставит в соответствие формальным словам в алфавите $\{a, b\}$ их значения в группе G, например, $\Phi(aaababbbbab^{-1}a^{-1}bba) = \Phi(a^3bab^4ab^{-1}a^{-1}b^2a) = a^3bab^4ab^{-1}a^{-1}b^2a = a$. Последнее равенство получено в результате вычисления формального слова из $F(S)$ в группе G.

Пусть $H = \ker\Phi$. Покажем, что H порождается словами $a^2,\ b^2,\ (ab)^2$. Действительно, в группе G соответствующие этим словам элементы равны e, следовательно, эти слова лежат в H. Пусть H_1 наименьшая нормальная подгруппа в $F(S)$, содержащая $a^2,\ b^2,\ (ab)^2$. Тогда $a \equiv a^{-1}(H_1),\ b \equiv b^{-1}(H_1),\ ab \equiv ba(H_1)$. Отсюда следует, что любое слово $f \in F(S)$ сравнимо по $\mod H_1$ с одним из слов $e,\ a,\ b,\ ab$, т.е. $|F(S)/H_1| \leqq 4$. Так как $H_1 \subset H$, то по теореме о соответствии

$$G \cong F(S)/H \cong (F(S)/H_1)/(H/H_1).$$

Следовательно, $4 = |G| = |F(S)/H| = |F(S)/H_1| : |H/H_1| \leq 4 : |H/H_1|$. Отсюда получаем, что $|F(S)/H_1| = 4$ и $|H/H_1| = 1$, т.е. $H = H_1$.

10.6. Покажем, что симметрическую группу S_3 можно задать образующими $a,\ b$ и соотношениями $a^2,\ b^2,\ (ab)^3$. Обозначим через a и b транспозиции $(1\ 2),\ (1\ 3)$ соответственно. Покажем, что a и b порождают группу S_3. Так как всякая подстановка раскладывается в произведение транспозиций (в S_3 это – $(1\ 2),\ (1\ 3),\ (2\ 3)$), а $(2\ 3) = bab$, то $S_3 =< a,\ b >$. Легко проверить, что в S_3 выполняются соотношения $a^2 = e,\ b^2 = e,\ (ab)^3 = e$. Пусть $F(S)$ – свободная группа над $S = \{a,\ b\}$, $G =< a,\ b\|\ a^2,\ b^2,\ (ab)^3 >= F(S)/H$, где H – наименьший нормальный делитель в $F(S)$, содержащий $\{a^2,\ b^2,\ (ab)^3\}$.

По универсальному свойству свободной группы существует гомоморфизм φ группы $F(S)$ на S_3, при котором $\varphi(a) = (1\,2),\ \varphi(b) = (1\,3)$. Пусть $H_1 = \ker\varphi,\ \varphi^* : F(S)/H_1 \longrightarrow S_3$ – индуцированный изоморфизм. Очевидно $a^2,\ b^2,\ (ab)^3 \in H_1$ и, следовательно, $H \subset H_1$. По теореме о соответствии существует сюръективный гомоморфизм $\Phi : F(S)/H \longrightarrow F(S)/H_1$. Тогда $\Phi^* = \varphi^* \circ \Phi : G \longrightarrow S_3$ – сюръективный гомоморфизм.

Покажем, что $|G| \leq 6$. Отсюда будет следовать, что Φ^* – изоморфизм, так как $|S_3| = 6$. Группа G имеет две образующие $a,\ b$, поэтому любой элемент $g \in G$ имеет вид $g = a^{n_1}b^{m_1}\dots a^{n_k}b^{m_k}$, где $n_i, m_i \in \mathbb{Z}$. Так как $a = a^{-1},\ b = b^{-1}$, то можно считать, что $0 \leq n_i, m_i \leq 1,\ i = 1, \dots, k$. Пользуясь соотношениями в группе G, выясним сколько различных произведений элементов a и b указанного вида можно составить в группе G. Произведение, содержащее 0 сомножителей, только одно – это e. Можно составить два произведения ab и ba, $ab \neq ba$ в G, поскольку в противном случае $\Phi^*(ab) = (12)(13)$ равнялось бы $\Phi^*(ba) = (13)(12)$ в S_3, а это не так. Произведений

$$a^{n_1}b^{m_1}\dots a^{n_k}b^{m_k},\ n_i,\ m_i \in \{0, 1\}, \tag{5}$$

в которых 3 сомножителя, – два: aba и bab. Однако эти произведения в группе G равны:

$$aba = ab^{-1}a^{-1} = a(ab)^{-1} = a(ab)^2 = a(ab)(ab) = bab.$$

Произведений вида (5), содержащих 4 сомножителя, можно построить два – $abab$ и $baba$, но $abab = (ab)^2 = (ab)^{-1} = b^{-1}a^{-1} = ba$, аналогично, $baba = ab$. Таким образом, длины элементов $abab$ и $baba$ не превосходят 2. Это значит, что в группе G нет элементов длины 4, а, тем более, элементов большей длины. Мы получили, что все элементы группы G содержатся среди произведений $e,\ a,\ b,\ ab,\ ba,\ aba$. Следовательно, $|G| \leq 6$.

10.7. *Группой диэдра* называется группа $D_k =< a, b || a^2,\ b^2,\ (ab)^k >$. Покажем, что $|D_k| = 2k$.

Пусть $H =< g >$ – циклическая группа в D_k, $g = ab$. Так как $(ab)^k = e$, то $|H| \leq k$. Покажем, что aga^{-1} и $bgb^{-1} \in H$. Отсюда будет следовать, что H – нормальный делитель в D_k.

$$aga^{-1} = a(ab)a = ba = (ab)^{-1} = g^{-1} \in H,$$

$$bgb^{-1} = b(ab)b = ba = g^{-1} \in H.$$

Так как $ab^{-1} = ab = g \in H$, то $a \equiv b(\mod H)$. Отсюда следует, что D_k/H порождается одним элементом $\bar{a} = aH$ порядка 2. Следовательно, $|D_k| \leq 2k$. Чтобы доказать равенство, достаточно построить группу G порядка $2k$, порожденную двумя элементами $a,\ b$, такими, что $a^2 = b^2 = (ab)^k = e$. В качестве группы G можно взять группу симметрий правильного n-угольника, которая состоит из поворотов плоскости вокруг центра симметрии правильного n-угольника на углы $2\pi l/k,\ l = 0, \ldots, k-1$, и отражений относительно осей симметрии n-угольника. Группа G порождается двумя отражениями a и b относительно осей симметрии, угол между которыми минимальный (доказать!). Произведение ab является поворотом на угол $2\pi/k$, следовательно, $(ab)^k = e$. Порядок группы G равен $2k$. Поэтому порядок D_k также равен $2k$.

В качестве группы G можно было взять *полупрямое произведение* циклической группы $\mathbb{Z}_2 = \{0,\ 1\}$ и циклической группы $\mathbb{Z}_k = \{0, 1 \ldots, k-1\}$. По определению группа G состоит из всех пар $(u, v),\ u \in \mathbb{Z}_2,\ v \in \mathbb{Z}_k$, с операцией умножения

$$(u_1, v_1)(u_2, v_2) = (u_1 + u_2,\ (-1)^{u_2}v_1 + v_2).$$

Единицей в G является пара $(0,\ 0)$, элементом, обратным к (u, v), является пара $(u,\ -(-1)^u v)$. Положим $a = (1, 0),\ b = (1, 1)$. Тогда $a^2 = b^2 = e,\ ab = (0, 1),\ (ab)^s = (0, s),\ a(ab)^s = (1, s)$. Следовательно, G порождается элементами $a,\ b$ и $a^2 = b^2 = (ab)^k = e$. Из определения G следует, что $|G| = 2k$.

Во всех рассмотренных примерах для определения порядка группы $G =< S||L >$, заданной образующими S и определяющими соотношениями L, применялся один и тот же прием:
1) порядок группы оценивался сверху числом n с помощью преобразований слов от образующих с учетом определяющих соотношений, и
2) находилась конкретная группа G_1 порядка n, имеющая систему образующих S,

для которых выполняются все определяющие соотношения L.
Из универсального свойства свободной группы и теоремы о гомоморфизмах следует существование сюръективного гомоморфизма $\Phi^* : G \longrightarrow G_1$. Из 1) получаем, что Φ^* – изоморфизм и, значит, $|G| = n$. Этот метод применяется и для решения вопроса о конечности группы G: если известна бесконечная группа с множеством образующих S, для которых выполняются соотношеня L, то и группа $G =< S||L >$ бесконечна.

В связи с заданием групп образующими и определяющими соотношениями имеется целый ряд алгоритмических проблем. Среди них центральное место занимают следующие три проблемы разрешимости, сформулированные в 1911 г. М. Дэном. Пусть $G =< S||L >$.
1. *Проблема слов*: существует ли алгоритм, позволяющий за конечное число шагов выяснить для произвольного слова U в алфавите S, выполняется ли в группе G равенство $U = e$. Если такой алгоритм для группы G существует, то говорят, что в группе G *разрешима проблема слов*. (Эту проблему называют также проблемой тождества или проблемой равенства.)
2. *Проблема сопряженности*: существует ли алгоритм, позволяющий для двух произвольных слов U и V в алфавите S за конечное число шагов выяснить, сопряжены ли элементы U и V в группе G.
3. *Проблема изоморфизма*: существует ли алгоритм, позволяющий для произвольной группы $G_1 =< S_1||L_1 >$ за конечное число шагов выяснить, изоморфны ли группы G и G_1.

П. С. Новиков в 1952 г. доказал, что существуют конечно определенная группа (т.е. группа $G =< S||L >$ с конечным множеством образующих S и конечным множеством определяющих соотношений L), для которой проблема равенства неразрешима. С другой стороны проблема равенства всегда разрешима для групп с одним определяющим соотношением (теорема Магнуса). Для групп с двумя соотношениями проблема слов не решена.

Проблема сопряженности также неразрешима. Действительно, из разрешимости проблемы сопряженности для группы G следует разрешимость проблемы слов, так как проверить для слова U равенство $U = e$ – это то же, что проверить сопряженность слова U пустому слову.

Проблема изоморфизма неразрешима даже для случая, когда группа G тривиальна, например, когда $G =< a||a >$ (теорема Адяна, 1957).

11. Конечно порожденные абелевы группы.

Пусть G – абелева группа, записываемая аддитивно. Подмножество S в G называется *линейно независимым*, если для любой конечной системы элементов $s_1, \ldots, s_n \in S$ из равенства

$$m_1 s_1 + m_2 s_2 + \ldots + m_n s_n = 0 \ (m_i \in \mathbb{Z},\ i = 1, \ldots, n)$$

следует, что все $m_i = 0$.
Множество S называется *базисом* группы G, если оно линейно независимо и $< S >= G$, т.е. любой элемент $g \in G$ можно записать в виде линейной комбинации элементов из S с целыми коэффициентами.

Группа G называется *свободной абелевой группой*, если она обладает базисом. Любая абелева группа изоморфна факторгруппе некоторой свободной абелевой группы.

11.1. Пусть $\mathbb{Z}^n$ – множество векторов пространства $\mathbb{R}^n$ с целочисленными компонентами. $\mathbb{Z}^n$ является свободной абелевой группой с базисом

$$S = \{(1, 0, \ldots, 0),\ (0, 1, \ldots, 0), \ldots, (0, 0, \ldots, 1)\}.$$

В случае абелевых групп прямое произведение групп $G_1, \ldots, G_n$ называется прямой суммой и обозначается через $G_1 \oplus \ldots \oplus G_n$.
Абелева группа G называется конечно порожденной, если она обладает конечной системой образующих $S = \{s_1, \ldots, s_n\}$. В этом случае каждый элемент $g \in G$ можно записать в виде $g = m_1 s_1 + m_2 s_2 + \ldots + m_n s_n$ $(m_i \in \mathbb{Z},\ i = 1, \ldots, n)$. Если такое представление единственно, то S является бозисом в G и, следовательно, G – свободная абелева группа. В этом случае $G \cong \mathbb{Z}^n$.

Теорема. *Пусть $\varphi : A \longrightarrow B$ – гомоморфизм абелевой группы A на свободную абелеву группу B, $A' = \ker\varphi$. Существует подгруппа B' в A, такая, что $A = A' \oplus B'$.*

Доказательство.

Пусть $\{b_i\}_{i \in I}$ – базис свободной группы B. Выберем элементы $a_i \in A$, такие что $\varphi(a_i) = b_i$. В качестве подгруппы B' можно взять подгруппу, порожденную элементами $a_i,\ i \in I$. Действительно, если $m_1 a_{i_1} + \ldots + m_k a_{i_k} = 0$, то, применяя φ, получаем $m_1 b_{i_1} + \ldots + m_k b_{i_k} = 0$ и, следовательно, $m_1 = \ldots = m_k = 0$, т.е. B' – свободная подгруппа в A с базисом $\{a_i,\ i \in I\}$. Аналогично получаем, что $B' \cap A' = \{0\}$. Если $a \in A$, $\varphi(a) = m_1 b_{i_1} + \ldots + m_k b_{i_k}$, то $a - (m_1 a_{i_1} + \ldots + m_k a_{i_k}) = a' \in A'$. Следовательно, $A = A' \oplus B'$.■

Теорема. *Пусть G – свободная абелева группа, H – подгруппа в G. Тогда H – свободная абелева группа и мощность базиса в H на превосходит мощности базиса в G.*

Доказательство.

Рассмотрим случай, когда группа G имеет конечный базис $\{s_1, \ldots, s_n\}$. Доказательство проведем индукцией по n. При $n = 1$, отождествляя произвольный элемент $ms_1 \in G$ с $m \in \mathbb{Z}$, можно считать, что $G = \mathbb{Z}$. Как известно, любая подгруппа в $\mathbb{Z}$, отличная от $\{0\}$, изоморфна $\mathbb{Z}$, т.е. свободна. Отметим, что нулевая группа также считается свободной. Допустим, что теорема верна для свободных групп с базисом из $n-1$ элементов, и рассмотрим группу G с базисом $\{s_1, \ldots, s_n\}$. Если подгруппа $H \subset G$ содержится в свободной подгруппе $G' =< s_1, \ldots, s_{n-1} >$, то по предположению индукции утверждения теоремы верны для H. Пусть теперь $H \not\subset G.'$ Множество всех коэффициентов при s_n из разложений всевозможных элементов из H по базису $\{s_1, \ldots, s_n\}$ образует ненулевую подгруппу в $\mathbb{Z}$. Такая подгруппа имеет вид (m), т.е. состоит из всех целых чисел, делящихся на m, $m > 0$. Обозначим через $\hat{h}$ элемент из H, для которого коэффициент при s_n в разложении по базису $\{s_1, \ldots, s_n\}$ равен m.

Тогда для лубого $h \in H$ найдется целое k, такое, что $h - k\hat{h} \in H' = H \cap G'$. По предположению индукции H' – свободная подгруппа в G' с базисом $\{h_1, \dots, h_t\}$, $t \leq n-1$. Теперь легко убедиться, что $\{h_1, \dots, h_t, \hat{h}\}$ – базис подгруппы H, содержащий $t+1$ элемент, $t+1 \leq n$.■

Из теоремы следует, в частности, что все базисы конечно порожденной свободной абелевой группы G содержат одинаковое число элементов. Число элементов в базисе свободной абелевой группы G называется *рангом* G и обозначается $rank G$.

Теорема. *Пусть G – конечно порожденная абелева группа ранга n, H – подгруппа в G, $H \neq \{0\}$. Существует базис $\{y_1, \dots, y_n\}$ в G и натуральные числа $\tau_1, \dots, \tau_m$, такие, что*
1) $\tau_i | \tau_{i+1}$ и
2) $\{x_i = \tau_i y_i\ ,\ i = 1, \dots, m\}$ составляют базис в H.
Числа $\tau_1, \dots, \tau_m$, удовлетворяющие условиям 1) – 2), определены однозначно.

Доказательство теоремы аналогично доказательству теоремы о приведении λ-матрицы к каноническому виду. По аналогии с теорией λ-матриц определим элементарные преобразования целочисленных матриц $A = (a_{ij})$. Преобразование первого типа заключается в умножении какой-либо строки (столбца) на ± 1, преобразование второго типа – в прибавлении к i-ой строке j-ой строки, умноженной на целое число $(i \neq j)$ (аналогично для столбцов). Матрица $A = (a_{ij})$, $a_{ij} \in \mathbb{Z}$, имеет *канонический* вид, если все элементы вне главной диагонали равны нулю, а элементы a_{ii} обладают свойствами $a_{ii} \geq 0$, $a_{ii} | a_{i+1,i+1}$. Здесь предполагается, что если $a_{ii} = 0$, то $a_{jj} = 0$ для $j > i$. В теории λ-матриц доказывается, что любая λ-матрица элементарными преобразованиями может быть приведена к каноническоиу виду. При доказательстве используется теория делимости многочленов от одного неизвестного, аналогичная теории делимости целых чисел. Поэтому доказательство теоремы о приведении λ-матрицы к каноническому виду с помощью элементарных преобразований почти дословно переносится на целочисленные матрицы (повторите это доказательство для случая целочисленных матриц). Напомним, что единственность каноническаго вида λ-матрицы доказывалось с помощью наибольших общих делителей миноров k-го порядка D_k : так как D_k не меняется при элементарных преобразованиях, то элементы e_i, стоящие на главной диагонали (инвариантные множители) можно найти по формулам

$$e_1 = D_1,\ e_i = D_i / D_{i-1},\ i = 2, \dots, r;\ e_j = 0,\ j = r+1, \dots, n. \qquad (1)$$

Здесь r – наибольший порядок, отличных от нуля миноров. Это рассуждение дословно переносится на случай целочисленных матриц, в результате, канонический вид целочисленной матрицы можно также найти по формулам (1). Итак, с помощью элементарных преобразований целочисленную матрицу можно привести к каноническому виду, который определяется однозначно. Отметим, что определение канонического вида и все приведенные выше рассуждения имеют смысл и для прямоугольных матриц. Поэтому утверждение о приведении целочисленной матрицы элементарными преобразованиями к каноническому виду справедливо и для прямоугольных матриц.

Далее, как и для λ-матриц, определяются элементарные целочисленные матрицы первого типа, у которых вне главной диагонали стоят нули, а на главной диагонали

все элементы равны 1, кроме одного, равного -1, и второго типа, которые отличаются от единичной матрицы одним элементом $a_{ij},\ i \neq j$. Выполнение элементарного преобразования над строками (столбцами) матрицы A равносильно умножению матрицы A слева (справа) на соответствующую элементарную матрицу. Каждая элементарная матрица имеет определитель ± 1. Поэтому произведение элементарных матриц также имеет определитель ± 1. Как и для λ-матриц, целочисленые квадратные матрицы с определителем ± 1 называются унимодулярными. Матрица унимодулярна тогда и только тогда, когда ее можно представить в виде произведения элементарных матриц. Доказательство такое же, как для λ-матриц: матрица унимодулярна тогда и только тогда, когда ее каноническим видом является единичная матрица (это следует из того, что единственный минор n-го порядка – определитель матрицы – равен ± 1, а, значит, все наибольшие общие делители миноров D_k также равны 1, см. (1)). Назовем две целочисленные матрицы эквивалентными, если одна из них получается из другой с помощью конечного числа элементарных преобразований. Как и для λ-матриц, получаем критерий эквивалентности для целочисленнных матриц: две целочисленные $n \times m$-матрицы A и B эквивалентны тогда и только тогда, когда существуют унимодулярные целочисленные матрицы U и V, такие, что $B = UAV$.

Пусть теперь $S = \{s_1, \ldots, s_n\}$ – базис группы G, $T = \{w_1, \ldots, w_m\}$ – базис подгруппы $H,\ m \leq n$. Если $S' = \{s'_1, \ldots, s'_n\}$ –другой базис в G, то матрица перехода $T = (t_{ij})$ от S к S' авляется матрицей с целыми коэффициентами, для которой существует обратная матрица с целыми коэффициентами (матрица перехода от S' к S). Таким образом, $|T|$ и $|T^{-1}| = |T|^{-1}$ – целые числа. Следовательно, $|T| = \pm 1$. и матрица T – унимодулярная. Разложм w_i по базису $s_j,\ j = 1, \ldots, n, w_k = \sum_{i=1}^{n} a_{ik}s_i, a_{ik} \in \mathbb{Z}$. В матричном виде можно записать $(w) = (s)A$, где (w) – строка $(w_1, \ldots, w_m)$, (s) – строка $(s_1, \ldots, s_n),\ A = (a_{ij})$ – $n \times m$-матрица. Переход к новым базисам в H и G в матричном виде записывается так: $(w') = (w)T_1,\ (s') = (s)T_2$, где $T_1,\ T_2$ –соответствующие матрицы перехода. Таким образом, $(w') = (w)T_1 = (s)AT_1 = (s')T_2^{-1}AT_1$, следовательно, матрица A', составленная из "координат" базисных векторов w'_i в базисе (s'), связана с матрицей A соотношением $A' = T_2^{-1}AT_1$. Так как $T_1,\ T_2^{-1}$ – унимодулярные матрицы то матрицы A и A' эквивалентны. Кроме того, $T_1,\ T_2$ можно выбрать так, чтобы матрица A' имела канонический вид. Следовательно, можно выбрать базисы (x) и (y) в H и G соответственно, так что $x_i = \tau_i y_i,\ i = 1, \ldots, m$. Единственность натуральных чисел τ_i следует из единственности канонического вида матрицы A.■

Множество $Tor(G)$ элементов конечного порядка в абелевой группе G образует подгруппу, которая называется *подгруппой кручения*. Если $Tor(G) = \{e\}$, то говорят, что G – *группа без кручения*. В общем случае $G/Tor(G)$ – группа без кручения. Действительно, если $n\overline{g} = \overline{ng} = 0$ в $G/Tor(G)$, то $ng \in Tor(G)$ и, следовательно, $m(ng) = (mn)g = 0$ для некоторого m, т.е. $g \in Tor(G)$ и, значит, $\overline{g} = 0$.

Пусть A – свободная абелева группа с базисом $\{y_1, \ldots, y_n\}$, H – подгруппа в A с базисом $\{x_1 = \tau_1 y_1, \ldots, x_m = \tau_m y_m\}$. Соответствие $c_1y_1 + \ldots + c_ny_n \mapsto (c_1, \ldots, c_n)$ является изоморфизмом групп A и $\mathbb{Z}^n$, этот изоморфизм переводит подгруппу H в подгруппу $(\tau_1)\oplus(\tau_2)\oplus\ldots\oplus(\tau_m)\oplus(0)\ldots\oplus(0)$. Поэтому, согласно теореме о факторгруппе прямого произведения групп по прямому произведению нормальных подгрупп,

$$A/H \cong \mathbb{Z}_{\tau_1} \oplus \ldots \oplus \mathbb{Z}_{\tau_m} \oplus \mathbb{Z}^{n-m}, \tag{2}$$

следовательно,

$$Tor(A/H) \cong \mathbb{Z}_{\tau_1} \oplus \ldots \mathbb{Z}_{\tau_m}. \qquad (3)$$

Теорема. *Конечно порожденная абелева группа без кручения свободна.*

Доказательство.

Пусть $\{s_1, \ldots, s_n\}$ – образующие группы G. Рассмотрим свободную абелеву группы A с базисом $\{s'_1, \ldots, s'_n\}$. Соответствие $\varphi : c_1 s'_1 + \ldots + c_n s'_n \mapsto c_1 s_1 + \ldots + c_n s_n$ является эпиморфизмом группы A на G. Пусть $H = \ker \varphi$. Тогда $G \cong A/H$. Как известно (см. выше), можно выбрать базисы $\{y_1, \ldots, y_n\}$, $\{x_1, \ldots, x_m\}$, $(m \leq n)$, в A и H соответственно, так, что $x_i = \tau_i y_i$, $i = 1, \ldots, m$. Однако $0 = Tor(G) \cong Tor(A/H) \cong \mathbb{Z}_{\tau_1} \oplus \ldots \oplus \mathbb{Z}_{\tau_m}$ (см. (3)). Поэтому $\tau_1 = \ldots = \tau_m = 1$ и $G \cong A/H \cong \mathbb{Z}^{n-m}$ (см. (2)). Следовательно, G – свободная группа. ■

Конечная абелева группа G называется *p-примарной,* если ее порядок является степенью простого числа p.

Теорема. *Конечная примарная группа G является прямой суммой циклических примарных подгрупп $H_1, \ldots, H_n$: $G = H_1 \oplus \ldots \oplus H_n$. Если $G = K_1 \oplus \ldots \oplus K_l$ – другое представление G в виде прямой суммы циклических примарных подгрупп, то $l = n$ и с точностью до порядка слагаемых $K_i \cong H_i$.*

Доказательство.

Очевидно, конечная группа является конечно порожденной. Представим конечно-порожденную группу G в виде факторгруппы свободной группы A конечного ранга по подгруппе H, т.е. $G \cong A/H$. Группа A/H имеет вид (2). Так как в нашем случае A/H – конечная группа, то в формуле (2) $n = m$ и $G \cong A/H \cong \mathbb{Z}_{\tau_1} \oplus \ldots \oplus \mathbb{Z}_{\tau_n}$. Группа G – примарная, $|G| = p^s$, поэтому все числа τ_i являются степенями простого числа p. Мы получили представление группы G в виде прямой суммы примарных циклических групп. Так как $\tau_i | \tau_{i+1}$, то $(\tau_1, \ldots, \tau_n) = (p^{m_1}, \ldots, p^{m_n})$, $m_i \leq m_{i+1}$, $s = m_1 + \ldots + m_s$, и

$$G \cong \mathbb{Z}_{p^{m_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{m_n}}.$$

Такое раздожение p-примарной группы G в прямую сумму циклических подрупп будем называть представлением типа $(p^{m_1}, \ldots, p^{m_n})$.

Докажем, что любые разложения p-примарной группы G в прямую сумму циклических подгрупп имеют один тип. Множество $pG = \{pg \mid g \in G\}$ является подгруппой в G и на факторгруппе G/pG естественным образом определяется умножение на элементы поля $\mathbb{F}_p$ классов вычетов по модулю p : $\bar{a}\bar{g} = \overline{ag}$. В результате, абелева группа G/pG становится векторным пространством над $\mathbb{F}_p$. Так как $\mathbb{Z}_{p^k}/p\mathbb{Z}_{p^k} \cong \mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$, то для любого разложения G впрямую сумму примарных циклических подгрупп, $G \cong \mathbb{Z}_{p^{k_1}} \oplus \ldots \oplus \mathbb{Z}_{p^{k_l}}$, $G/pG \cong \mathbb{F}_p \oplus \ldots \oplus \mathbb{F}_p = \mathbb{F}_p^l$, т.е. $l = \dim_{\mathbb{F}_p} G/pG$. Значит, для любого разложения G в прямую сумму циклических p-примарных подгрупп число слагаемых в разложении равно размерности G/pG как векторного пространства над F_p и не зависит от выбора разложения. Единственность типа разложения докажем индукцией по порядку группы G. Группа порядка p является циклической и не имеет собственных ненулевых подгрупп, поэтому $G \cong \mathbb{Z}_p$ – единственное разложение G в

прямую сумму циклических подгрупп. Допустим, единственность типа разложения доказана для p-примарных групп, порядок которых меньше порядка группы G. Допустим, что p-примарная группа G имеет два представления в виде прямой суммы циклических подгрупп: одно разложение типа $(p,\dots,p,p^{m_t},\dots,p^{m_n})$, другое – типа $(p,\dots,p,p^{k_r},\dots,p^{k_n})$. Здесь в записи типов разложений мы выделили слагаемые, изоморфные $\mathbb{Z}_p$. Для первого разложения число таких слагаемых $t-1$, для второго – $r-1$. Легко убедиться, что подгруппа $p\mathbb{Z}_{p^m}$ изоморфна $\mathbb{Z}_{p^{m-1}}$. В частности, $p\mathbb{Z}_p=\{0\}$. Для подгруппы pG получаем два разложения: одно – типа $(p^{m_t-1},\dots,p^{m_n-1})$, другое – типа $(p^{k_r-1},\dots,p^{k_n-1})$. Так как $|pG|<|G|$, то по предположению индукции типы разложений для группы pG совпадают. Таким образом, $t=r,\ m_t=k_t,\ \dots,m_n=k_n$, но это означает, что типы двух разложений группы G совпадают.■

p-примарную группу, которую можно разложить в прямую сумму циклических подгрупп, порядков $p^{m_1},\dots,p^{m_n},\ m_i\le m_{i+1}$, называют *абелевой p-группой типа* $(m_1,\dots,m_n)$. Абелева p-группа типа $(1,\dots,1)$ называется *элементарной абелевой p-группой*. Число циклических слагаемых в разложении элементарной абелевой p-группы называется рангом. (Не путать ранг свободной группы и ранг элементарной абелевой p-группы!)

Теорема. *Пусть G – конечная абелева группа порядка $n=p_1^{k_1}\dots p_m^{k_m}$ $(p_1,\dots,p_m$ – различные простые числа). Множество G_i элементов, порядок которых является степенью числа p_i, образует примарную абелеву подгруппу в G порядка $p_i^{k_i}$ и $G=G_1\oplus\dots\oplus G_m$.*

Доказательство.

Циклическая подгруппа, порожденная элементом порядка p^k, содержится в силовской p-подгруппе. Так как все силовские p-подгруппы сопряжены, то силовская p-подгруппа в абелевой конечной группе единственна и состоит из элементов, порядок которых есть степень p.

Пусть $g\in G$ имеет порядок $m=kl,\ (k,l)=1,\ u,v\in\mathbb{Z}$, такие, что $ku+lv=1$.g можно записать в виде $g=1g=(uk+vl)g=u(kg)+v(lg)$. Элемент kg имеет порядок l, а lg – порядок k. Так как $(l,u)=1$, элемент $u(kg)$ также имеет порядок l. Аналогично, $v(lg)$ имеет порядок k. Таким образом, $g=g_1+g_2$, где $g_1=u(kg),\ g_2=v(lg)$ – элементы взаимно простых порядков k и l. Следовательно, если порядок m элемента g равен $p_1^{s_1}p_2^{s_2}\dots p_r^{s_r}$, где $p_1,\dots,p_r$ – различные простые числа, то $g=g_1+g_2+\dots+g_r$, где элемент g_i имеет порядок $p_i^{m_i}$ и поэтому содержится в силовской p_i-подгруппе G_i. Таким образом, $G=G_1+G_2+\dots+G_m$.

Осталось доказать, что эта сумма – прямая. Пусть $0\ne g\in G_i\cap(\oplus_{j\ne i}G_j)$. Следовательно, g имеет порядок $p_i^l,\ l>0$. С другой стороны, $g=\sum_{j\ne i}g_j,\ g_j\in G_j$. Так как $p_j^{k_j}g_j=0$, то $tg=0$, где $t=\prod_{j\ne i}p_j^{k_j}$. Поэтому $p_i^l|t$, противоречие. ■

Подгруппы $G_1,\dots,G_m$ называются *примарными компонентами* группы G.

Теорема. *Пусть G – конечно порожденная абелева группа. Тогда $G\cong\mathbb{Z}^r\oplus\mathbb{Z}_{\tau_1}\oplus\mathbb{Z}_{\tau_2}\oplus\dots\oplus\mathbb{Z}_{\tau_m}$, где $\tau_i|\tau_{i+1},\ i=1,\dots,m-1$. Числа $r,\ \tau_1,\dots,\tau_m,\ \tau_i|\tau_{i+1}$, определены для группы G однозначно.*

Доказательство.

Представим конечно порожденную группу G в виде A/H (т.е. $G \cong A/H$), где A – свободная абелева группа конечного ранга, H – подгруппа в A. Формула (2) дает нужное разложение группы G, $r = n - m$. Мы можем считать, что все числа τ_i в формуле (2) больше 1 (слагаемые в (2), соответствующие $\tau_i = 1$ – нулевые). Формула (3) дает разложение подгруппы $Tor(A/H) \cong Tor(G)$. Отсюда получаем, что $G/Tor(G) \cong \mathbb{Z}^{n-m} = \mathbb{Z}^r$ – сободная абелева группа ранга r. Поэтому число r определено однозначно. Мы видим также, что $Tor(G) \cong Tor(A/H)$ – конечная абелева группа. Обозначим $Tor(G)$ через $\hat{G}$. Отметим, что из любого разложения группы G,

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}_{\tau_1} \ldots \oplus \mathbb{Z}_{\tau_q},$$

$$\tau_i | \tau_{i+1},\ i = 1, \ldots q-1,\ \tau_1 > 1,$$

мы получаем разложение для подгруппы $\hat{G}$,

$$\hat{G} \cong \Sigma = \mathbb{Z}_{\tau_1} \oplus \ldots \oplus \mathbb{Z}_{\tau_q},$$

$$\tau_i | \tau_{i+1},\ i = 1, \ldots, q-1,\ \tau_1 > 1. \tag{4}$$

Покажем, что числа $\tau_1, \ldots, \tau_q$ определены однозначно.

Конечная абелева группа $\hat{G}$ единственным образом раскладывается в прямую сумму своих силовских p-подгрупп. Силовские p-подгруппы в $\hat{G}$ изоморфны силовским p-подгруппам в Σ. Найдем силовские p-подгруппы в Σ. Пусть $|\hat{G}| = |\Sigma| = \tau_1 \tau_2 \ldots \tau_q = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}$, $p_1, \ldots, p_s$ – различные простые числа. Разложим τ_i на простые множители,

$$\tau_i = p_1^{l_{i1}} p_2^{l_{i2}} \ldots p_s^{l_{is}},\ i = 1, \ldots, q,\ l_{ij} \leq l_{i+1,j}. \tag{5}$$

Здесь некоторые l_{ij} могут быть равны 0. Группа $\mathbb{Z}_{\tau_i}$ раскладывается в прямую сумму своих силовских p-подгрупп, которые являются циклическими группами порядков $p_1^{l_{i1}}, p_2^{l_{i2}}, \ldots, p_s^{lis}$,

$$\mathbb{Z}_{\tau_i} \cong \mathbb{Z}_{p_1^{l_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{l_{is}}}. \tag{6}$$

В результате, из (4) и (6) получаем разложение $\hat{G}$,

$$\hat{G} \cong \Sigma = \oplus_{i=1}^{q} \mathbb{Z}_{\tau_i} =$$

$$= \oplus_{i=1}^{q} [\mathbb{Z}_{p_1^{l_{i1}}} \oplus \ldots \oplus Z_{p_s^{l_{is}}}]. \tag{7}$$

Объединяя слагаемые в двойной сумме (7), соответствующие простому числу p_j, мы получим разложение силовской подгруппы $\hat{G}(p_j)$ в прямую сумму примарных циклических подгрупп,

$$\hat{G}(p_j) \cong \mathbb{Z}_{p_j^{l_{1j}}} \oplus \ldots \oplus \mathbb{Z}_{p_j^{l_{qj}}}. \tag{8}$$

Таким образом, силовская p_j-подгруппа $\hat{G}(p_j)$ имеет тип $(l_{1j}, \ldots, l_{mj}), l_{ij} \leq l_{i+1,j}$. Следовательно, для любого $j = 1, \ldots, s$ тип силовской p_j-подгруппы в $\hat{G}$ определяется однозначно из разложений чисел τ_i в произведение простых чисел (см.(5)).

Обратно, зная типы силовских p_j-подгрупп $\hat{G}(p_j)$, т.е. имея разложения (8) для любого простого p_j, делящего порядок группы $\hat{G}$, мы получим представление $\hat{G}$ в виде (4):

$$\hat{G} = \hat{G}(p_1) \oplus \ldots \oplus \hat{G}(p_s) \cong$$

$$\oplus_{j=1}^{s} [\mathbb{Z}_{p_j^{l_{1j}}} \oplus \ldots \oplus \mathbb{Z}_{p_j^{l_{qj}}}] =$$

$$= \oplus_{i=1}^{q} [\mathbb{Z}_{p_1^{l_{i1}}} \oplus \ldots \oplus \mathbb{Z}_{p_s^{l_{is}}}] =$$

$$= \mathbb{Z}_{\tau_1} \oplus \ldots \oplus \mathbb{Z}_{\tau_q},$$

где $\tau_i = p_1^{l_{i1}} p_2^{l_{i2}} \ldots p_s^{l_{is}}$. Так как $l_{ij} \leq l_{i+1,j}$, то $\tau_i | \tau_{i+1}$, $i = 1, \ldots, q-1$. Таким образом, зная типы силовских p_j-подгрупп в $\hat{G}$ $(l_{1j}, \ldots, l_{qj})$ (эти типы определены однозначно!), мы однозначно находим числа τ_i. ■

Число n называется *рангом* группы G (не путать с рангом свободной абелевой группы и рангом элементарной абелевой группы!). Числа $\tau_1, \ldots, \tau_k$ называются *коэффициентами кручения* группы G.

Пусть G – конечная абелева группа и $|G| = p_1^{s_1} \ldots p_n^{s_n}$. Покажем еще раз, как найти коэффициенты кручения, зная примарные компоненты $G_1, \ldots, G_n$ группы G, $G_i = \oplus_{j=1}^{q_i} \mathbb{Z}_{p_i^{k_{ij}}}$. Будем считать, что $k_{i1} \geq k_{i2} \geq \ldots \geq k_{iq_i}$. Пусть $q = \max\{q_i,\ i = 1, \ldots, n\}$. Составим $n \times q$ - матрицу, в i-ой строке и j-ом столбце которой стоит число $p_i^{k_{ij}}$. Свободные места заполним единицами. Тогда коэффициенты кручения выражаются следующим образом:

$$\tau_{q-j+1} = \prod_{i=1}^{n} p_i^{k_{ij}},\ j = 1, \ldots, q,$$

т.е. τ_{q-i+1} является произведением элементов j-го столбца построенной матрицы.

Доказательство.

$$G = \oplus_{i=1}^{n} G_i \cong \oplus_{i=1}^{n} (\oplus_{j=1}^{q_i} \mathbb{Z}_{p_i^{k_{ij}}}) \cong$$

меняем порядок суммирования

$$\cong \oplus_{j=1}^{q} (\oplus_{i=1}^{n} \mathbb{Z}_{p_i^{k_{ij}}}) \cong \oplus_{j=1}^{q} \mathbb{Z}_{\tau_{q-j+1}}.$$■

11.2. Пусть G – абелева группа порядка $324 = 2^2 \cdot 3^4$. Тогда $G = G_1 \oplus G_2$, где $|G_1| = 2^2$, $|G_2| = 3^4$. Если, например, $G_1 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$, а $G_2 = \mathbb{Z}_9 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$, то $q_1 = 2$, $q_2 = q = 3$, $k_{11} = k_{12} = 1$, $k_{21} = 2$, $k_{32} = k_{23} = 1$. Соответствующая матрица имеет вид

$$\begin{pmatrix} 2 & 2 & 1 \\ 3^2 & 3 & 3 \end{pmatrix}.$$

Тогда $\tau_1 = 3$, $\tau_2 = 6$, $\tau_3 = 18$ и $G = \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{18}$.

Рекомендуемая литература

1. Кострикин А. И. Введение в алгебру. М.: Наука, 1977.
2. Каргаполов М. И., Мерзляков Ю. И. Основы теории групп. М.: Наука, 1977.
3. Ленг С. Алгебра. М.: Мир, 1968.
4. Холл М. Теория групп. М.: ИЛ, 1962.
5. Магнус В., Каррас А., Солитэр Д. Комбинаторная теория групп. М.: Наука, 1974.