ГРУППЫ И ИХ ПРОСТЕЙШИЕ СВОЙСТВА

В этой лекции мы вводим понятия группы, подгруппы, порядка групп, подгрупп и элементов, и приводим первые примеры.

§ 1. Группы

Определение. Непустое множество G называется **группой**, если на нем задана бинарная операция $G \times G \longrightarrow G$, $(x, y) \mapsto xy$, обладающая следующими тремя свойствами:
G1. Ассоциативность: $(xy)z = x(yz)$ для любых $x, y, z \in G$;
G2. Существование нейтрального элемента: существует $e \in G$ такой, что $xe = x = ex$ для любого $x \in G$;
G3. Существование обратного элемента: для любого $x \in G$ существует обратный элемент $x^{-1} \in G$ такой, что $xx^{-1} = e = x^{-1}x$.

Бинарная операция на G, превращающая G в группу, называется **групповым законом**. Мощность $|G|$ группы G обычно называется ее **порядком**. Группа G, содержащая конечное число элементов, называется **конечной**. В противном случае группа G называется **бесконечной**.

Определение. Говорят, что элементы x и y группы G **коммутируют**, если $xy = yx$. Группа, в которой любые два элемента коммутируют, называется **коммутативной** или **абелевой**.

Иными словами, в абелевой группе в дополнение к аксиомам G1–G3 выполняется аксиома
G4. Коммутативность: *$xy = yx$ для любых $x, y \in G$.*

Абелевы группы названы так в честь Нильса Абеля, который доказал разрешимость в радикалах уравнений с абелевой группой Галуа. Абелевы группы обычно записываются аддитивно, так что вместо xy пишется $x+y$, 0 вместо e и $-x$ вместо x^{-1}. Термин `абелева группа` в этом смысле был впервые употреблен в 1882 году Генрихом Вебером.

Некоторые свойства групп можно вывести уже непосредственно из определения группы. Например, из свойства G1 несложно вывести следующее утверждение.

Упражнение 1. Пусть G – группа, n – натуральное число и $g_1, \ldots, g_n$ – элементы группы G. Тогда произведение $g_1 g_2 \ldots g_n$ не зависит от расстановки скобок в этом выражении.

Приведем три простейших свойства обратных элементов, которые в дальнейшем постоянно используются без явных ссылок:

Предложение 1. *Пусть G – группа, $x, y \in G$. Тогда*

1. *элемент, обратный к x, существование которого гарантируется свойством G3, является единственным*
2. $(xy)^{-1} = y^{-1}x^{-1}$
3. $(x^{-1})^{-1} = x$.

Доказательство. Действительно, пусть x^{-1} и x' два элемента группы G такие, что $xx^{-1} = x^{-1}x = e = xx' = x'x$. Но тогда

$$x' = x'e = x'(xx^{-1}) = (x'x)x^{-1} = ex^{-1} = x^{-1}.$$

Для доказательства второго утверждения достаточно заметить, что $(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}ey = y^{-1}y = e$. А значит $y^{-1}x^{-1}$ по определению является элементом, обратным к xy. Аналогично, $xx^{-1} = e$, значит также по определению x является элементом, обратным к x^{-1}, а такой элемент, как мы уже знаем, единственный. □

Обратите внимание на порядок множителей во втором утверждении предложения выше. Если две операции не коммутируют, то он весьма существен. Надевают обычно сначала пиджак, а потом пальто, а снимают, соответственно, наоборот, сначала пальто, и только потом пиджак. С другой стороны, если два преобразования коммутируют, как, например, надевание левой и правой перчаток, то коммутируют и обратные к ним преобразования, так что снимать их можно в произвольном порядке.

§ 2. Первые примеры групп

Много примеров групп встречалось уже в школьном курсе математики. Тем не менее, некоторые примеры из приведенных ниже, могут быть непонятны начинающему. Если это произошло с вами, не паникуйте!

Примеры абелевых групп

• **Аддитивные группы чисел.** Числовые множества $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ образуют группы по сложению. Иногда чтобы подчеркнуть, что речь идет именно об аддитивных структурах на этих множествах, пишут $\mathbb{Z}^+$, $\mathbb{Q}^+$ и т. д. Эти группы называются **аддитивными группами** целых, рациональных, вещественных и комплексных чисел, соответственно.
• **Мультипликативные группы чисел.** Множества ненулевых рациональных, вещественных или комплексных чисел $\mathbb{Q}^*$, $\mathbb{R}^*$, $\mathbb{C}^*$ образуют группы по умножению, называемые **мультипликативными группами** рациональных, вещественных и комплексных чисел, соответственно.
• **Мультипликативные группы чисел, cont.** Множества $\mathbb{Q}_{>0} = \mathbb{Q}_+ = \{x \in \mathbb{Q} \mid x > 0\}$ и $\mathbb{R}_{>0} = \mathbb{R}_+ = \{x \in \mathbb{R} \mid x > 0\}$ положительных рациональных и вещественных чисел представляют собой группы по умножению.
• **Группа углов** (`circle group`). Множество $\mathbb{T}$ комплексных чисел модуля 1 также представляет собой группу по умножению. Заметим, впрочем, что операция в этой группе (группе поворотов эвклидовой плоскости или группе углов) обычно записывается **аддитивно**, что согласуется со следующей ее интерпретацией. Группа $\mathbb{T}$ истолковывается как аддитивная группа вещественных чисел $\mathbb{R}^+$ по модулю $2\pi\mathbb{Z}$ (читается `целые кратные` 2π). Иными словами, $\mathbb{T}$ представляется как полуинтервал $[0, 2\pi)$, операция сложения $\oplus$ на котором определяется следующим образом: если $x+y < 2\pi$, то $x \oplus y = x+y$, а если $x+y \geq 2\pi$, то $x \oplus y = x + y - 2\pi$. В действительности, конечно, операция в $\mathbb{T}$ записывается обычным знаком $+$ (`сложение углов`). Подробнее эта конструкция будет обсуждаться в лекции о фактор-группах.
• **Группа корней из 1.** Этот пример будет понятен тем, кто уже знаком с понятием комплексного корня из 1. Мультипликативная группа $\{1\}$ состоит из одного элемента, а $\{\pm 1\}$ — из двух. Вообще, корни n-й степени из 1 в поле $\mathbb{C}$ комплексных чисел образуют группу по умножению, обозначаемую обычно μ_n. Эти группы конечны.
• **Булева группа.** Множество 2^X подмножеств в X является группой относительно **симметрической разности** (aka **булевой суммы**) Δ. При этом нейтральный элемент этой операции равен $\emptyset$, а $Y \Delta Y = \emptyset$, так что каждый элемент является обратным сам себе.
• **Векторные группы.** Пусть снова K обозначает одно из полей $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ — в школьной программе обычно рассматривался случай $K = \mathbb{R}$. Если рассмотреть n-мерное векторное пространство $V = K^n$ и забыть о том, что векторы можно умножать на скаляры, а оставить на V только аддитивную структуру (сложение векторов), то V называется **векторной группой** (`vector group`). Как мы узнаем в одной из последующих лекций, она является прямой суммой n экземпляров аддитивной группы K^+.
• **Группы трансляций.** Группу V можно заставить действовать на себе, а именно, каждому вектору $u \in V$ сопоставляется **аффинное преобразование** $T_u : V \longrightarrow V$, $v \mapsto v + u$, называемое **трансляцией**, или параллельным переносом. Группа $T(V) = \{T_u \mid u \in V\}$ называется **группой трансляций**. В случае, когда $K = \mathbb{R}$, группа $T(V)$ состоит из эвклидовых движений пространства V.

Примеры неабелевых групп

Предшествующие примеры дают совершенно превратное представление о том, что такое группа — группы, фигурирующие во всех этих примерах, абелевы. В действительности, группа гораздо больше похожа не на множество чисел, а на множество взаимно однозначных преобразований чего-то, сохраняющих, быть может, какую-то дополнительную структуру. Следующий пример архетипичен, как мы вскоре увидим, каждая группа **есть** множество преобразований.
• **Симметрическая группа.** Пусть G — множество всех взаимно однозначных отображений множества X на себя. Тогда G является группой относительно композиции, называемой **симметрической группой** множества X и обозначаемой S_X или $S(X)$ (`symmetric group`). В самом деле, как мы знаем, композиция отображений ассоциативна; композиция двух биекций снова является биекцией; тождественное отображение является биекцией и служит нейтральным элементом композиции и, наконец, любая биекция обра-

тима, причем обратное отображение также является биекцией. Мы посвятим изучению симметрической группы конечного множества отдельную лекцию. Заметим, что в случае $|X| \geq 3$ эта группа некоммутативна. В частности, при $n = 3$ получаем **группу симметрий правильного треугольника** S_3 порядка 6 — самую маленькую неабелеву группу.

• **Группы преобразований.** Специализируя этот пример, т. е. рассматривая не все биекции X на себя, а только те, которые сохраняют имеющуюся на X структуру (например, алгебраическую, геометрическую, топологическую, или какую-то их комбинацию), можно получить множество новых примеров групп. Эти примеры будут постоянно возникать далее в нашем курсе.

• **Группа кватернионов.** Рассмотрим группу Q, состоящую из 8 элементов $\{\pm 1, \pm i, \pm j, \pm k\}$; причем $+1 = 1$ действительно действует как единица группы, квадраты всех отличных от ± 1 элементов равны -1, знаки подчиняются обычному правилу (т. е., например, $(-i)(-k) = ik$), а попарно различные i, j, k умножаются как орты $\mathbb{R}^3$ относительно векторного умножения: $ij = -ji = k$, $jk = -kj = i$, $ki = -ik = j$. Так определенное умножение ассоциативно, а все элементы обратимы, например, $i^{-1} = -i$ и, соответственно, $(-i)^{-1} = i$. Группа Q обычно называется **группой кватернионов** (`quaternion group`, `Quaternionengruppe`), хотя правильнее называть ее **группой кватернионных единиц**. Эта группа была использована Гамильтоном в 1842 году при построении тела кватернионов $\mathbb{H}$.

• **Полная линейная группа.** Пусть K — поле, например, $K = \mathbb{Q}, \mathbb{R}, \mathbb{C}$. Тогда множество

$$\mathrm{GL}(n, K) = \{g \in M(n, K) \mid \det(g) \neq 0\}$$

всех невырожденных матриц порядка n над полем K является группой относительно умножения, называемой **полной линейной группой** степени n над K. Обозначение $\mathrm{GL}(n, K)$ является сокращением английского `General Linear group`.

Для читателей, не знакомых с линейной алгеброй, определим полную линейную группу степени 2 явно. Назовем матрицей порядка 2 упорядоченную четверку $A = (a, b, c, d)$ элементов поля K, традиционно записываемую в виде квадратной таблицы $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$. Назовем определителем $\det(A)$ матрицы A элемент поля K, вычисляемый как $ad - bc$. Умножение матриц $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ и $\begin{pmatrix} x & y \\ z & w \end{pmatrix}$ зададим следующей формулой

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x & y \\ z & w \end{pmatrix} = \begin{pmatrix} ax + bz & ay + bw \\ cx + dz & cy + dw \end{pmatrix}.$$

Упражнение 2. Докажите, что множество

$$\mathrm{GL}(2, K) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in K, \det \begin{pmatrix} a & b \\ c & d \end{pmatrix} = ad - bc \neq 0 \right\}$$

образует группу относительно операции умножения, введенной выше. При этом нейтральным элементом этой группы является матрица $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, а обратный элемент вычисляется следующим образом

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \frac{1}{ad - bc} \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

• **Линейные группы, cont.** Мы можем специализировать предыдущий пример, рассмотрев не все матрицы данного порядка, а лишь удовлетворяющие определенному свойству. Несложно видеть, что следующие множества матриц образуют группы относительно матричного умножения и обращения матриц,

введенных в предыдущем пункте:

$$\begin{aligned}
\mathrm{SL}(n,K) &= \{g \in M(n,K) \mid \det(g) = 1\} \\
\mathrm{SL}(2,K) &= \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a,b,c,d \in K, ad-bc = 1 \right\} \\
\mathrm{D}(2,K) &= \left\{ \begin{pmatrix} a & 0 \\ 0 & d \end{pmatrix} \mid a,d \in K \setminus \{0\} \right\} \\
\mathrm{B}(2,K) &= \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \mid a,b,d \in K, ad \neq 0 \right\} \\
\mathrm{U}(2,K) &= \left\{ \begin{pmatrix} 1 & b \\ 0 & 1 \end{pmatrix} \mid b \in K \right\}.
\end{aligned}$$

Группа $\mathrm{SL}(n,K)$ называется **специальной линейной группой порядка** n **над полем** K, группы $\mathrm{D}(2,K), \mathrm{B}(2,K)$ и $\mathrm{U}(2,K)$ – **группами диагональных, верхнетреугольных и верхних унитреугольных матриц**, соответственно.

§ 3. Подгруппы

Определение подгруппы

Определение. Подмножество $H \subseteq G$ называется **подгруппой** в G, если оно само является группой относительно тех же операций. Иными словами, для того, чтобы H было подгруппой, необходимо выполнение следующих трех условий:

i) $h, g \in H \Longrightarrow hg \in H$,

ii) $h \in H \Longrightarrow h^{-1} \in H$,

iii) $e \in H$.

Обычно эти свойства вербализуют следующим образом: подгруппа **замкнута** относительно произведения, перехода к обратному и нейтрального элемента. Чтобы подчеркнуть, что H является подгруппой в G, а не просто подмножеством, в этом случае вместо $H \subseteq G$ обычно пишут $H \leq G$. Запись $G \geq H$ имеет тот же смысл, что и $H \leq G$, любая группа G, содержащая H в качестве подгруппы, называется **надгруппой** H.

Непустое подмножество группы, удовлетворяющее условию i) называется **подполугруппой**, а условию ii) — **симметричным** подмножеством. Условия i) и ii) независимы. Пусть, например, $G = \mathbb{Z}^+$ — аддитивная группа целых чисел. Тогда $\mathbb{N}^+$ является подполугруппой в $\mathbb{Z}^+$, а $\{\pm 1\}$ — симметричным подмножеством, но, очевидно, ни то ни другое множество не является подгруппой. Для конечных групп аналог первого из этих примеров построить не удастся.

Произведение подмножеств группы.

Пусть $X, Y \subseteq G$ — два подмножества группы. Тогда **произведением** XY называется их *произведение по Минковскому*

$$XY = \{xy \mid x \in X, y \in Y\}.$$

Аналогично, множество

$$X^{-1} = \{x^{-1} \mid x \in X\}$$

— это **обратное по Минковскому** к множеству X.

В терминах этих операций определение подгруппы выглядит следующим образом. Условие i) означает, что $HH \subseteq H$, а условие ii) — что $H^{-1} \subseteq H$. Разумеется, если для непустого множества H выполнены *оба эти условия*, то включения здесь можно заменить на равенства, так как тогда $1 \in H$. На самом деле несложно видеть, что достаточно даже требовать лишь выполнения включения $HH^{-1} \subseteq H$.

Первые примеры подгрупп.

Приведем несколько примеров подгрупп.

• **Тривиальная и несобственная подгруппы.** В каждой группе G есть по крайней мере две подгруппы.

А именно, очевидно, что $\{e\} \leq G$. Эта подгруппа называется **тривиальной** и часто обозначается просто e или 1, а в случае аддитивной записи, естественно, 0; обычно это не ведет к недоразумениям. Столь же очевидно, что $G \leq G$. Эта подгруппа называется **несобственной**. Все подгруппы $H < G$, отличные от G, называются **собственными**. Подгруппы 1 и G называются **очевидными** подгруппами группы G. Заметим, что в случае $G = 1$ эти подгруппы совпадают.

• Любая подгруппа в $\mathbb{Z}^+$ имеет вид $m\mathbb{Z}$ для некоторого $n \in \mathbb{Z}$.

• Знакопеременная группа является подгруппой симметрической группы: $A_n \leq S_n$.

• **Транзитивность.** Пусть $F \leq H \leq G$. Тогда $F \leq G$. В частности, $\mathbb{Z}^+ \leq \mathbb{Q}^+ \leq \mathbb{R}^+ \leq \mathbb{C}^+$ являются подгруппами в $\mathbb{C}^+$.

• **Положительные числа.** Произведение двух положительных чисел положительно, обратное к положительному числу положительно, поэтому $\mathbb{R}_+ = \{\lambda \in \mathbb{R} \mid \lambda > 0\}$ — подгруппа в $\mathbb{R}^*$.

• **Подгруппы Q.** Всего в группе кватернионов Q имеется 6 подгрупп, из которых следующие 4 неочевидные:

$$\{\pm 1\}, \quad \{\pm 1, \pm i\}, \quad \{\pm 1, \pm j\}, \quad \{\pm 1, \pm k\}.$$

• **Пересечения подгрупп.** Несложно видеть, что если $H, F \leq G$, то и $F \cap H$ является подгруппой в G. На самом деле, пересечение любого (не обязательно конечного) семейства подгрупп является подгруппой.

§ 4. Центр, централизатор и нормализатор

Центр группы.

Множество элементов, коммутирующих со всеми элементами G, называется **центром** группы G и обозначается $C(G)$ (от английского `centre` или американского `center`):

$$C(G) = \{g \in G \mid \forall x \in G, gx = xg\}.$$

Также употребительно обозначение $Z(G)$ (от немецкого `Zentrum`). Элементы $C(G)$ называются **центральными**. Легко видеть, что $C(G) \leq G$. В действительности, как мы узнаем в лекции о нормальных подгруппах, центр является даже *нормальной* подгруппой, $C(G) \trianglelefteq G$. Любая подгруппа $H \leq C(G)$ называется **центральной подгруппой** в G. Группа G в том и только том случае абелева, когда $G = C(G)$. Группа G, для которой $C(G) = 1$, называется группой **с тривиальным центром**.

Централизатор элемента.

Пусть $x \in G$. Определим **централизатор** элемента x в группе G следующим образом:

$$C_G(x) = \{g \in G \mid gx = xg\}.$$

Легко проверить, что $C_G(x) \leq G$.

Лемма 2. *Для любого $x \in G$ имеем $C_G(x) \leq G$.*

Доказательство. В самом деле, $x1 = x = 1x$, поэтому $C_G(x)$ содержит 1. Если $h, g \in C(G)$, то $(hg)x = h(gx) = h(xg) = (hx)g = (xh)g = x(hg)$, так что $hg \in C(G)$. С другой стороны, если $h \in C(G)$, то умножая равенство $hx = xh$ на h^{-1} справа и слева, получаем $xh^{-1} = h^{-1}x$, так что $h^{-1} \in C(G)$. □

Отсюда, конечно, сразу следует, что $C(G) \leq G$. В самом деле, $C(G) = \bigcap C_G(x)$, где пересечение берется по всем $x \in G$.

Задача 3. Убедитесь, что если $H \leq G$, $x \in H$ и $g \in G$, то i) $C_G(x^g) = C_G(x)^g$, ii) $C_H(x) = G_G(x) \cap H$.

Централизатор подмножества.
Пусть теперь $X \subseteq G$ – любое подмножество в G. Определим **централизатор** X как $C_G(X) = \bigcap C_G(x)$, где пересечение берется по всем $x \in X$. Иными словами, $C_G(X)$ состоит из всех элементов, *поэлементно* коммутирующих с X:

$$C_G(X) = \{g \in G \mid \forall x \in X, gx = xg\}.$$

Так как пересечение любого семейства подгрупп само является подгруппой, $C_G(X)$ — подгруппа в G.

Нормализатор подмножества.
Пусть снова $X \subseteq G$ — любое подмножество в G. Определим **нормализатор** X как множество элементов, которые коммутируют с X *в целом*:

$$N_G(X) = \{g \in G \mid gX = Xg\}.$$

Понятие нормализатора (но не соответствующий термин!) было введено Силовым. Легко убедиться, что $N_G(X)$ подгруппа в G. Совершенно ясно, что для одноэлементных подмножеств нормализатор совпадает с централизатором: если $X = \{x\}$, то $N_G(\{x\}) = C_G(x)$. В общем случае $C_G(X) \leq N_G(X)$.

§ 5. Порядок элемента и экспонента группы

Если G – любая группа, то мы можем определить степень любого элемента $g \in G$ с любым целым показателем. В самом деле, положим $g^0 = e$ и $g^n = g^{n-1}g$, $n \in \mathbb{N}$. Далее для любого $n \in \mathbb{N}$ мы можем дополнительно положить $g^{-n} = (g^{-1})^n = (g^n)^{-1}$. Ясно, что для любых $m, n \in \mathbb{Z}$ имеет место равенство $g^{m+n} = g^m g^n$. Таким образом, множество $\{g^n \mid n \in \mathbb{Z}\}$ всех степеней элемента g в действительности образует подгруппу группы G. Так как любая подгруппа, содержащая g обязана содержать также все степени g, то это *наименьшая* подгруппа, содержащая g. Эта подгруппа обозначается $\langle g \rangle$ и называется **циклической подгруппой** в G, порожденной элементом g.

Порядок $|\langle g \rangle|$ циклической подгруппы $\langle g \rangle$ обозначается через $o(g)$ или $\mathrm{ord}(g)$ (от английского `order`) и называется **порядком** элемента g. Иными словами, $o(g)$ это либо *наименьшее* натуральное число n такое, что $g^n = 1$, либо ∞. Если порожденная g подгруппа бесконечна, то говорят, что g — элемент **бесконечного порядка** и пишут $o(g) = \infty$, в противном случае g называется элементом **конечного порядка**. Группа G называется **периодической**, или **группой кручения**, если все ее элементы имеют конечный порядок. Группа G называется **группой без кручения**, если все ее неединичные элементы имеют бесконечный порядок.

Задача 4. Докажите, что если $g^m = 1$, то $o(g)|m$.

Решение. Деление с остатком в $\mathbb{Z}$. Если $o(g) \nmid m$, то поделив m с остатком на $o(g)$, мы видим, что $m = q \cdot o(g) + r$, где $0 < r < o(g)$. Тогда $1 = g^m = (g^{o(g)})^q g^r = g^r$, что противоречит минимальности $o(g)$.

Теорема 3. *Пусть G — произвольная группа, $g \in G$, $o(g) = n$. Тогда порядок элемента g^m равен $n/\gcd(m, n)$.*

Доказательство. Как мы только что выяснили, порядок элемента g^m — это наименьшее натуральное число k такое, что $(g^m)^k = g^{mk} = e$. Так как $o(g) = n$, это означает, что $n|mk$, или, что то же самое, $nq = mk$ для некоторого $q \in \mathbb{Z}$. Последнее равенство можно сократить на $d = \gcd(m, n)$ и заключить, что $(n/d)q = (m/d)k$, т. е. $(n/d)|(m/d)k$. Так как $\gcd(m/d, n/d) = 1$, отсюда следует, что k делится на n/d. Но наименьшее натуральное число с таким свойством и есть n/d, таким образом, действительно, $o(g^m) = n/\gcd(m, n)$. □

Наименьшее $m \geq 1$ такое, что $g^m = 1$ для всех $g \in G$, называется **экспонентой** или **показателем** группы G. Такого m может не существовать, но если оно существует, то говорят, что группа G имеет **конечную экспоненту** или **конечный показатель**. Для этого необходимо, чтобы порядки всех элементов были ограничены в совокупности. В этом случае экспоненту можно определить также как наименьшее общее кратное порядков элементов группы G.

§ 6. Подгруппа, порожденная подмножеством

В этом параграфе мы изложим важный общий метод построения подгрупп.

Определение. Пусть $X \subseteq G$. Наименьшая подгруппа в G, содержащая X, называется **подгруппой, порожденной** X и обозначается $\langle X \rangle$.

Так как пересечение любого множества подгрупп снова является подгруппой, то $\langle X \rangle$ действительно существует, достаточно взять пересечение *всех* подгрупп в G, содержащих X. Эта подгруппа допускает вполне конкретное описание, подобное тому, которое дано в предыдущем пункте для циклической подгруппы. А именно, для любого подмножества $Y \subseteq G$ обозначим через Y^n множество всех произведений элементов множества Y по n штук:

$$Y^n = \{y_1 \dots y_n \mid y_i \in Y\}.$$

Тем самым $Y^0 = \{e\}$, $Y^1 = Y$, $Y^2 = YY$ и т. д. Обозначим через $M(Y)$ множество **всевозможных** произведений образующих Y, т. е. $M(Y) = \bigcup Y^n$, $n \in \mathbb{N}_0$.

Теорема 4. *Для любого подмножества $X \subseteq G$*

$$\langle X \rangle = M(X \cup X^{-1}) = \{x_1 \dots x_n \mid x_i \in X \cup X^{-1}, n \in \mathbb{N}_0\}.$$

Доказательство. Докажем вначале, что подгруппа $\langle X \rangle$ содержится в $H = M(X \cup X^{-1})$. Для этого заметим, что H — подгруппа, содержащая X. В самом деле, по условию e является пустым произведением и, следовательно, принадлежит H. С другой стороны, если $u = x_1 \dots x_m$ и $v = y_1 \dots y_n$ — два каких-то элемента H, то $uv = x_1 \dots x_m y_1 \dots y_n$ также принадлежит H. Тем самым, $HH \subseteq H$. Далее, для $u = x_1 \dots x_m$ имеем $u^{-1} = {x_m}^{-1} \dots {x_1}^{-1}$. Тем самым, $H^{-1} = H$. Это и значит, что H есть подгруппа. Так как по определению $\langle X \rangle$ — наименьшая среди всех подгрупп, содержащих X, то $\langle X \rangle \leq H$.

Обратно, пусть теперь F — любая подгруппа, содержащая X. Тогда $X^{-1} \subseteq F^{-1} = F$. Тем самым F содержит все слова длины ≤ 1 в образующих $X \cup X^{-1}$. Далее рассуждаем индукцией по длине слова. Любое слово $w \in (X \cup X^{-1})^n$ длины $n \geq 2$ в образующих $X \cup X^{-1}$ имеет вид $w = ux$, где $u \in (X \cup X^{-1})^{n-1}$ — слово длины $n-1$ в тех же образующих, а $x \in X \cup X^{-1}$. По индукционному предположению $u \in F$, а по базе индукции $x \in F$. Тем самым $w = ux \in FF \subseteq F$. Но это значит, что $F \geq H$. Поскольку это верно для любой подгруппы, содержащей X, то $\langle X \rangle \geq H$. □

Задача 5. Пусть X состоит из элементов конечного порядка. Докажите, что тогда

$$\langle X \rangle = M(X) = \{x_1 \dots x_n \mid x_i \in X, n \in \mathbb{N}_0\}.$$

Задача 6. Пусть $H < G$. Покажите, что $\langle G \setminus H \rangle = G$.

§ 7. Циклические группы и их подгруппы

Напомним, что группа G называется **циклической**, если она порождается одним элементом. Иными словами, это означает, что найдется такое $g \in G$, что каждый элемент группы G является степенью g, т. е. $G = \{g^n, n \in \mathbb{Z}\}$. По существу циклические группы изучали де Ферма, Эйлер и Гаусс, в связи с задачами теории чисел. Однако, явным образом класс циклических групп выделил только Кэли в 1891 году, он и придумал название `cyclical group`. Но, конечно, *фактически* следующий результат был известен еще Эйлеру.

Теорема 5. *Каждая подгруппа циклической группы $G = \langle g \rangle$ является циклической.*

Доказательство. Пусть $H \leq G$. Если $H = e$, то она циклическая. Пусть поэтому $H \neq e$ и $g^m \in H$ для некоторого $m \neq 0$. Заменяя, если нужно, m на $-m$, можно считать, что $m \in \mathbb{N}$. Пусть $d \in \mathbb{N}$ — наименьшее натуральное число такое, что $g^d \in H$. Покажем, что тогда $H = \langle g^d \rangle$. В самом деле, пусть $g^m \in H$ для какого-то $m \in \mathbb{Z}$. Поделим m с остатком на d: $m = qd + r$, $0 \leq r < d$. Тогда $g^r = g^m (g^{qd})^{-1} \in H$, что противоречит минимальности d, если $r \neq 0$. Значит, $r = 0$ и все элементы H являются степенями g^d. □

Отметим следующий важнейший частный случай этой теоремы.

Следствие 6. *Каждая подгруппа аддитивной группы $\mathbb{Z}$ имеет вид $n\mathbb{Z}$ для некоторого $n \in \mathbb{N}_0$.*

Если порядок $G = \langle g \rangle$ равен n, то $g^n = e$. Вообще, пусть $g^k = g^l$ для некоторых $k, l \in \mathbb{Z}$. Тогда $e = g^k(g^l)^{-1} = g^{k-l}$, так что $k - l$ делится на n или, что то же самое, $k \equiv l \pmod{n}$. Это значит, что в этом случае $G = \{e = g^0, g, g^2, \ldots, g^{n-1}\}$. Это значит, что **порядок o(g) элемента** $g \in G$ может быть определен как наименьшее натуральное число такое, что $g^n = e$, или $o(g) = \infty$, если такого натурального числа не существует.

Рассмотрим теперь элемент g^m конечной циклической группы $G = \langle g \rangle$ и выясним, какую подгруппу он порождает. Так как $g^0 = e$, можно считать, что $m \neq 0$. Так как образующими циклической группы G порядка n являются те и только те элементы, порядок которых равен n, мы сразу получаем такую характеризацию **функции Эйлера** φ, равную по определению количеству натуральных чисел, меньших n, взаимно-простых с n.

Следствие 7. *Конечная циклическая группа $G = \langle g \rangle$ порядка n содержит $\varphi(n)$ образующих. Образующими G являются те и только степени g^m элемента g, для которых* $\gcd(m, n) = 1$.

Следствие 8. *Пусть $G = \langle g \rangle$ есть конечная циклическая группа порядка n. Тогда для каждого делителя d числа n в группе G существует единственная подгруппа порядка d.*

Доказательство. Пусть $d \mid n$, тогда $g^{n/d}$ порождает подгруппу порядка d. Обратно, пусть H — произвольная подгруппа порядка d. Для $d = 1$ доказывать нечего, поэтому в дальнейшем мы считаем, что $H \neq e$. Согласно теореме 1 мы уже знаем, что H циклическая, значит, $H = \langle g^m \rangle$ для некоторого m. По теореме порядок подгруппы, порожденной g^m, равен $d = n/\gcd(m, n)$. В частности, $(n/d) \mid m$. Это значит, что $H = \langle g^m \rangle$ содержится в подгруппе, порожденной $g^{n/d}$, но, так как их порядки совпадают, $H = \langle g^{n/d} \rangle$. □

§ 8. Смежные классы

Сейчас мы введем одно из ключевых понятий теории групп, которое первым рассматривал Эварист Галуа.

Определение. Левым смежным классом G по подгруппе H называется любое множество вида $Hx = \{hx \mid h \in H\}$, где $x \in G$. При этом x называется **представителем** класса Hx. Аналогично, множество $xH = \{xh \mid h \in H\}$ называется **правым смежным классом** G по H с представителем x.

Через $H\backslash G = \{Hx \mid x \in G\}$ обозначается множество всех *левых* смежных классов G по H, а через $G/H = \{xH \mid x \in G\}$ — множество всех *правых* смежных классов.

Сейчас мы покажем, что смежные классы по подгруппе H задают разбиение группы G. Напомним, что **разбиением** множества X называется его представление в виде объединения попарно непересекающихся непустых подмножеств.

Теорема 9. *Группа G является дизъюнктным объединением всех различных левых (или правых) смежных классов по подгруппе H.*

Доказательство. Так как $x \in Hx$, то $G = \bigcup Hx$, где объединение берется по всем $Hx \in H\backslash G$. Таким образом, нужно лишь показать, что это объединение дизъюнктно. В самом деле, пусть Hx и Hy — два смежных класса G по H. Предположим, что $Hx \cap Hy \neq \emptyset$. Это значит, что найдется $z \in Hx \cap Hy$, т. е. найдутся такие $h, g \in H$, что $z = hx = gy$. Тем самым $y = g^{-1}(hx) = (g^{-1}h)x$, так что $y \in Hx$. Поэтому $Hy \subseteq H(Hx) = (HH)x = Hx$. Точно так же проверяется и включение $Hx \subseteq Hy$. Таким образом, окончательно, $Hx = Hy$. Тем самым, никакие два различных левых смежных класса не пересекаются, что и утверждалось. Доказательство для правых классов совершенно аналогично. □

Эта теорема означает, что

$$G = \bigsqcup Hx, \qquad Hx \in H\backslash G.$$

Разбиение на левые смежные классы G по H называется **разложением группы** G **по подгруппе** H (`Nebenklassenzerlegung`, `coset decomposition`). Одним из смежных классов является сама подгруппа $H = H1 = 1H$. Из наличия сокращения в группе сразу следует, что для каждого $x \in G$ отображение $H \longrightarrow Hx$, $h \mapsto hx$, задает биекцию H на смежный класс Hx, так что, в частности, $|Hx| = |H|$. Из только что доказанной теоремы вытекает, что для любого $x \notin H$ класс Hx не пересекается с H и, значит, не является подгруппой.

Задача 7. Пусть $H \leq G$. Докажите, что если $G \setminus H$ конечно, то либо G конечна, либо $H = G$.

Решение. Пусть G бесконечна, $H \neq G$. Если H конечна, то сравнение мощностей показывает, что $G \setminus H$ бесконечно. С другой стороны, если H бесконечна и $g \notin H$, то $G \setminus H$ содержит бесконечный смежный класс gH и, значит, снова бесконечно.

Задача 8. Пусть $F, H \leq G$. Докажите, что если $Fx = Hy$, то $F = H$.

Сравнение по модулю подгруппы.
Выше мы построили разбиения G на левые/правые классы смежности по H. Мы знаем, что с каждым разбиением связано некоторое отношение эквивалентности. Опишем получающиеся отношения эквивалентности явно.

Будем говорить, что x и y **сравнимы по модулю H слева**, и писать $x \,{}_H\!\equiv\, y$, если $Hx = Hy$. Это означает, что найдутся такие $h, g \in H$, что $hx = gy$. Тем самым, $xy^{-1} = h^{-1}g \in H^{-1}H = H$. С подгруппой H связано и второе отношение эквивалентности, **сравнимость по модулю H справа**: $x \equiv_H y$, если $xH = yH$. Легко видеть, что $xH = yH$ эквивалентно включению $x^{-1}y \in H$. Таким образом, мы можем ввести отношение сравнимости по модулю H и не упоминая смежные классы.

Определение. Говорят, что элементы $x, y \in G$ **сравнимы по модулю H слева** (соответственно, **справа**), если $xy^{-1} \in H$ (соответственно, $x^{-1}y \in H$).

Из теоремы предыдущего пункта вытекает, что это действительно отношение эквивалентности, но это легко усмотреть и непосредственно из определения подгруппы. Посмотрим, скажем на сравнимость по модулю H слева. Это отношение *рефлексивно*, так как $xx^{-1} = e \in H$, *симметрично*, так как $yx^{-1} = (xy^{-1})^{-1} \in H^{-1} = H$, и *транзитивно*, так как $xz^{-1} = (xy^{-1})(yz^{-1}) \in HH = H$.

В случае, когда G коммутативна, $Hx = xH$ так что сравнимости по модулю H слева и справа совпадают. В этом случае обычно говорят просто о сравнимости по модулю H, которая обозначается $x \equiv y \pmod{H}$. В общем случае отношения эквивалентности ${}_H\!\equiv$ и $\equiv_H$ различны.

§ 9. Индекс подгруппы, теорема Лагранжа

Заметим, прежде всего, что между множеством $H\backslash G$ левых смежных классов и множеством G/H правых смежных классов существует естественная биекция. Наивная попытка установить биекцию посредством $Hx \mapsto xH$ не приводит к желаемому результату, так как это соответствие, вообще говоря, не является корректным определением отображения: из $Hx = Hy$ *не следует*, что $xH = yH$. Поэтому приходится поступать чуточку хитрее. Вспомним, прежде всего, определение обратного по Минковскому к множеству X, а именно, $X^{-1} = \{x^{-1} \mid x \in X\}$. Ясно, что $X = Y \iff X^{-1} = Y^{-1}$. В интересующем нас случае $(Hx)^{-1} = x^{-1}H^{-1} = x^{-1}H$, так что $Hx = Hy \iff x^{-1}H = y^{-1}H$. Это значит, что сопоставление $Hx \mapsto x^{-1}H$ корректно определяет биекцию $H\backslash G$ на G/H.

Определение. Пусть $H \leq G$. Мощность $|H\backslash G| = |G/H|$ множества смежных классов G по H называется **индексом** подгруппы H в группе G и обозначается $|G : H|$.

Понятие индекса оказывается особенно полезным в случае, когда множество смежных классов конечно. Если $|G : H| < \infty$, то H называется **подгруппой конечного индекса** в G.

Определение. Трансверсаль X к отношению сравнимости по модулю H слева/справа называется **системой представителей левых/правых смежных классов** G по H или, коротко, **левой/правой трансверсалью** к H в G.

Иными словами, система представителей левых смежных классов G по H — это такое подмножество $X \subseteq G$, что для любого $z \in G$ найдется $x \in X$ такое, что $Hz = Hz$ и из того, что $Hx = Hy$ для некоторых $x, y \in X$ следует, что $x = y$. С учетом этого определения можно заключить, что $G = \bigsqcup Hx$, $x \in X$. Ясно, что $|X| = |G : H|$. Аналогично, если Y — система представителей правых смежных классов, то $G = \bigsqcup yH$, $y \in Y$. Эти понятия особенно полезны для подгрупп конечного индекса. Например, если $X = \{x_1, \ldots, x_n\}$ — система представителей левых смежных классов, то группа G представляется в виде дизъюнктного объединения $G = Hx_1 \sqcup \ldots \sqcup Hx_n$.

Теорема 10 (Лагранж)**.** *Если $H \leq G$, то $|G| = |H||G : H|$.*

Доказательство. Как всегда, правильный способ доказательства равенства двух кардинальных чисел состоит в установлении биекции между некоторыми множествами. В самом деле, пусть X — любая система представителей левых смежных классов. Тогда $|G : H| = |X|$. Мы утверждаем, что отображение $H \times X \longrightarrow G$, $(h, x) \mapsto hx$ представляет собой биекцию. В самом деле, $G = \cup Hx$, $x \in X$, так что это отображение сюръективно. С другой стороны, если для некоторых $h, g \in H$, $x, y \in X$ имеет место равенство $hx = gy$, то $Hx = Hy$, и, значит, по определению трансверсали $x = y$. Сокращая равенство $hx = gx$ на x справа, получаем $h = g$. Но это и значит, что $|G| = |H \times X| = |H||X| = |H||G : H|$. □

Этот результат особенно важен для конечных групп, где из него вытекает важнейшее арифметическое ограничение на подгруппы.

Следствие 11. *Пусть G — конечная группа, $H \leq G$. Тогда порядок G делится на порядок H.*

В частности, применяя это следствие к циклическим подгруппам, мы видим, что порядок $o(g)$ любого элемента конечной группы делит порядок $|G|$ этой группы.

Следствие 12 (теорема Ферма)**.** *Пусть G — конечная группа, $g \in G$. Тогда $g^{|G|} = e$.*

Теорема Лагранжа допускает следующее естественное обобщение, называемое **общей теоремой об индексе** (`allgemeiner Indexsatz`).

Теорема 13. *Если $F \leq H \leq G$, то $|G : F| = |G : H||H : F|$.*

Доказательство. План доказательства этой теоремы точно такой же, как в теореме Лагранжа. А именно, пусть X — система представителей левых смежных классов H по F, а Y — система представителей левых смежных классов G по H. Мы утверждаем, что XY является системой представителей левых смежных классов G F, а отображение $X \times Y \longrightarrow XY$, $(x, y) \mapsto xy$, устанавливает биекцию прямого произведения множеств X и Y с их произведением по Минковскому. Тем самым,

$$|G : F| = |XY| = |X \times Y| = |X||Y| = |H : F||G : H|,$$

что и доказывает теорему.

Проверим теперь высказанные в предыдущем абзаце утверждения. По условию $G = \bigcup Hy$, $y \in Y$, и $H = \bigcup Fx$, $x \in X$. Подставляя выражение для H из второй формулы в первую и пользуясь ассоциативностью, получаем, что $G = \bigcup F(xy)$, $(x, y) \in X \times Y$. Поэтому нам осталось лишь доказать, что если $Fx_1y_1 = Fx_2y_2$ для некоторых $x_1, x_2 \in X$ и $y_1, y_2 \in Y$, то $x_1 = x_2$ и $y_1 = y_2$. В самом деле, пусть $Fx_1y_1 = Fx_2y_2$. Так как $x_1, x_2 \in X \subseteq H$, это означает, что $Hy_1 \cap Hy_2 \neq \emptyset$. По теореме пункта 2 тогда $Hy_1 = Hy_2$, и, значит, $y_1 = y_2 = y$ по определению трансверсали. Сокращая равенство $Fx_1y_1 = Fx_2y_2$ на y справа, получаем $Fx_1 = Fx_2$, так что, снова по определению трансверсали, $x_1 = x_2$, что и требовалось доказать. □

Теорема Лагранжа получается как частный случай этой теоремы в случае $F = 1$.