НОРМАЛЬНЫЕ ПОДГРУППЫ И ФАКТОР-ГРУППЫ

Здесь мы обсуждаем два ключевых понятия теории групп: нормальные делители и фактор-группы. Переход от уровня абстракции, который ассоциируется со школьной алгеброй, к тому уровню абстракции, который ассоциируется с алгеброй университетской, связан ровно с одной конструкцией — рассмотрением фактор-объектов. Тот, кто в состоянии понять, что такое фактор-группа, в состоянии полностью овладеть всем содержанием настоящего курса.

§ 1. Нормальные подгруппы, простые группы

1. Нормальные подгруппы. Сейчас мы введем *важнейший* класс подгрупп, а именно, нормальные подгруппы, впервые определенные в 1830 году Эваристом Галуа (сам Галуа называл их `инвариантными`). Собственно говоря, с этого момента предсуществование теории групп и переходит в существование. Как выяснится в дальнейшем, нормальные подгруппы — это *в точности* такие подгруппы в G, отношение сравнимости по модулю которых является конгруэнцией на G. Иными словами — это *в точности* такие подгруппы в G, что на множестве G/H смежных классов по H можно *естественным образом* ввести структуру группы!

Определение. Подгруппа H группы G называется **нормальной** в G, если для любого $x \in G$ левый смежный класс элемента x по H совпадает с правым:

$$Hx = xH.$$

Чтобы обозначить, что H нормальна в G, пишут $H \trianglelefteq G$ или $G \trianglerighteq H$.

Таким образом, подгруппа H в том и только том случае нормальна в G, когда для любых двух элементов $x, y \in G$, включение $xy^{-1} \in H$ эквивалентно включению $x^{-1}y \in H$. В старинных книгах нормальные подгруппы чаще назывались **нормальными делителями** (от немецкого `Normalteiler`) или **инвариантными подгруппами** (от французского `sous-groupe invariant`, `sous-groupe distingué`, также и по-немецки иногда использовалось выражение `invariante Untergruppe` и, совсем редко, `ausgezeichnete Untergruppe`).

Следующая задача дает весьма выразительную переформулировку того, что подгруппа H нормальна в G.

Задача 1. Докажите, что подгруппа $H \leq G$ в том и только том случае нормальна в G, когда для любых $x, y \in G$ из $xy \in H$ следует, что $yx \in H$.

2. Очевидные нормальные подгруппы. Во всякой группе есть два **очевидных** нормальных делителя. А именно, **тривиальный** нормальный делитель $1 \trianglelefteq G$ и **несобственный** нормальный делитель $G \trianglelefteq G$. Будем писать $H \triangleleft G$, чтобы подчеркнуть, что H **собственная** нормальная подгруппа.

Основной интерес в теории групп представляют группы, в которых нет никаких неочевидных нормальных делителей. Группа G называется **простой**, если $G \neq 1$ и из того, что $H \trianglelefteq G$ вытекает, что $H = 1$ или $H = G$. Простые группы являются блоками, из которых собраны все остальные группы и сами не могут быть разобраны на меньшие составные части. При этом, в отличие от (бессмысленной!) задачи классификации всех групп, классификация простых групп различных классов, хотя и очень сложна, но возможна. В частности, центральными достижениями математики XX века были классификация простых алгебраических групп и классификация простых конечных групп. В действительности, в соответствии с нашим сегодняшним уровнем понимания, именно классификация простых групп и изучение их строения является основной задачей теории групп.

§ 2. Примеры нормальных подгрупп

Укажем несколько очевидных примеров нормальных делителей. В дальнейшем, когда мы научимся строить нормальные делители из гомоморфизмов и сопряженных классов, возникнет много других, более интересных примеров.

• **Подгруппы абелевой группы.** В абелевой группе $Hx = xH$ для любой подгруппы H и любого элемента $x \in G$. Тем самым, в абелевой группе *все* подгруппы нормальны.

• **Центральные подгруппы.** Предыдущий пример допускает следующее очевидное обобщение: если $H \leq C(G)$, то $H \trianglelefteq G$.

• **Гамильтоновы группы.** Следующее понятие ввел в 1896 году Рихард Дедекинд Группа G называется **гамильтоновой**, если все ее подгруппы нормальны — иногда при этом еще требуется, чтобы сама G не была абелевой. Важнейшим примером гамильтоновой группы является группа Q кватернионных единиц. Напомним ее определение. Q есть группа из 8 элементов $\{\pm 1, \pm i, \pm j, \pm k\}$ с таблицей умножения (первый аргумент записан в первом столбце, второй – в первой строке)

$\cdot$	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	-1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

Гораздо проще запомнить таблицу умножения следующим образом: 1 является нейтральным элементом, квадрат любого элемента отличного от ± 1 равен -1, знаки выносятся из произведения и скоращаются также, как в целых числах, а умножение элементов i, j и k легче всего описать при помощи следующей диаграммы.

$$\begin{tikzcd} & i \arrow[dr, bend left] & \\ k \arrow[ur, bend left] & & j \arrow[ll, bend left] \end{tikzcd}$$

Читать ее следует так. Допустим, мы хотим умножить элемент x на y, где $x \neq y \in \{i, j, k\}$. Их произведением будет третий элемент на диаграмме со знаком плюс, если стрелочка идет от x к y и со знаком минус, если стрелочка идет от y к x. Например, произведение ij равняется k, а произведение $ji = -k$.

В Q имеется ровно 6 подгрупп, 1, $\{\pm 1\}$, G и три подгруппы вида $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$. Подгруппы 1 и G являются очевидными нормальными делителями, подгруппа $\{\pm 1\}$ совпадает с центром Q и, значит, нормальна, а все остальные подгруппы имеют индекс 2 в Q и, тем самым, как мы убедимся в следующем пункте, тоже нормальны.

Пока же, из чистого любопытства приведем полное описание гамильтоновых групп. Оказывается, группа кватернионов является *по существу* единственным примером неабелевой гамильтоновой группы. Для конечных групп следующий результат был доказан Дедекиндом, а в общем случае Рейнольдом Бэром в 1933 году.

Теорема 1. *Любая (неабелева) гамильтонова группа представлима в виде прямого произведения $Q \times A \times B$, где A абелева группа, все элементы которой имеют конечный нечетный порядок, а B — (абелева) группа, все элементы которой имеют период 2.*

• **Подгруппы индекса 2.** Каждая подгруппа индекса 2 является нормальным делителем. В самом деле, в этом случае $G = H \sqcup (G \setminus H)$ является разбиением G как на левые, так и на правые смежные классы по H. Если $x \in H$, то $Hx = H = xH$. Если же $x \neq H$, то $Hx \neq H$ и $xH \neq H$, и, значит, $Hx = G \setminus H = xH$. Важнейший пример — **знакопеременная группа** A_n, состоящая их всех четных перестановок степени n. Эта подгруппа имеет индекс 2 в симметрической группе S_n и, следовательно, согласно только что сделанному наблюдению, $A_n \trianglelefteq S_n$.

Упражнение 2. Если $|G : H| = 2$, то для любого $g \in G$ имеем $g^2 \in H$.

• **Централизатор и нормализатор** Рассмотрим подмножество $X \subseteq G$. Ранее мы определили централизатор $C_G(X)$ и нормализатор $N_G(X)$ множества X.

Задача 3. Докажите, что

$$C_G(gXg^{-1}) = gC_G(X)g^{-1}, \qquad N_G(gXg^{-1}) = gN_G(X)g^{-1}.$$

Задача 4. Докажите, что $C_G(X) \trianglelefteq N_G(X)$.

Следствие 2. $N_G(X) \leq N_G(C_G(X))$.

• **Нормальная подгруппа, порожденная подмножеством.** Пусть $X \subseteq G$. Существует ли наименьшая *нормальная* подгруппа в G, содержащая X, и как ее описать?

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

Заметим, что некоторые авторы обозначают нормальную подгруппу, порожденную X через $\langle\langle X \rangle\rangle$, однако это обозначение подразумевает, что группа G фиксирована. Наше обозначение представляется мне более удобным, так как, во-первых, оно является комбинацией двух общепринятых обозначений $\langle X \rangle$ и H^G и, во-вторых, в нем явно указана группа G. Существование такой подгруппы гарантируется тем, что пересечение *любого* множества нормальных подгрупп снова является нормальной подгруппой. Эта подгруппа допускает вполне конкретное описание, проверку которого мы оставляем читателю. В следующей теореме X^G имеет обычный смысл: $X^G = \{gxg^{-1} \mid x \in X, g \in G\}$.

Теорема 3. *Для любого подмножества* $X \subseteq G$

$$\langle X \rangle^G = \langle X^G \rangle = \{y_1 x_1 y_1^{-1} \dots y_n x_n y_n^{-1} \mid x_i \in X \cup X^{-1}, y_i \in G, n \in \mathbb{N}_0\}.$$

§ 3. Не каждая подгруппа нормальна

Сейчас мы приведем два примера подгрупп, весьма далеких от нормальных.

1. Минимальный контрпример. Все подгруппы абелевой группы нормальны. Самая маленькая неабелева группа — это группа $G = D_3 \cong S_3$ симметрий правильного треугольника. Несложно убедиться, что подгруппа в D_3, состоящая из тождественного преобразвания и одной осевой симметрии не является нормальной, так как левый и правый смежный классы по *другой* симметрии не совпадают.

2. Диагональные матрицы над целыми числами. Еще один пример не нормальной подгруппы можно построить следующим образом. Рассмотрим группу $G = \mathrm{GL}(2, \mathbb{Z})$ обратимых матриц порядка 2 с целыми записями. Пусть $D = \left\{ \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \right\}$. Ясно, что это двухэлементное множество является подгруппой в G. Рассмотрим элемент $x = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \in G$. Ясно, что

$$xD = \left\{ x, \begin{pmatrix} 1 & -1 \\ 0 & -1 \end{pmatrix} \right\} \qquad \text{и} \qquad Dx = \left\{ x, \begin{pmatrix} 1 & 1 \\ 0 & -1 \end{pmatrix} \right\}.$$

Таким образом, D не нормальна.

§ 4. Субнормальные подгруппы, теорема Виландта

Верно ли, что отношение нормальности транзитивно? Иными словами, верно ли, что нормальная подгруппа нормальной подгруппы сама нормальна? Легко видеть, что это не так. Следующий пример станет понятнее после прослушивании лекции о группах перестановок. Пусть $G = A_4$ — знакопеременная группа степени 4, $H = V$ — четверная группа, то есть группа $\{e, (12)(34), (13)(24), (14)(23)\}$, а F — любая подгруппа порядка 2 в V, скажем, $F = \langle (12)(34) \rangle$. Несложно видеть, что $V \trianglelefteq A_4$, а так как V абелева, то и $F \trianglelefteq V$. В то же время очевидно, что F не может быть нормальным делителем в A_4, в самом деле, F не коммутирует, например с элементом (123). Таким образом, $F \trianglelefteq H \trianglelefteq G$, но $F \ntrianglelefteq G$.

Вышесказанное объясняет, почему Виландт в 1939 году начал рассматривать следующий класс подгрупп.

Определение. Говорят, что подгруппа $F \trianglelefteq G$ **субнормальна** в G и пишут $F \trianglelefteq\trianglelefteq G$, если существует ряд подгрупп
$$F = G_0 \trianglelefteq G_1 \trianglelefteq G_2 \trianglelefteq \ldots \trianglelefteq G_d = G$$
в котором каждая подгруппа нормальна в следующей. Наименьшее такое d называется **глубиной** субнормальной подгруппы.

Таким образом,
• субнормальная подгруппа глубины 1 — это в точности нормальная подгруппа;
• субнормальная подгруппа глубины 2 — это подгруппа, для которой существует H, $F \trianglelefteq H \trianglelefteq G$;
и т. д. Ясно, что отношение субнормальности уже транзитивно: если $F \trianglelefteq\trianglelefteq H \trianglelefteq\trianglelefteq G$, то $F \trianglelefteq\trianglelefteq G$.

Упражнение 5. Убедитесь, что если $H \trianglelefteq\trianglelefteq G$ и $F \leq G$, то $H \cap F \trianglelefteq\trianglelefteq F$.

Упражнение 6. Убедитесь, что если $H \trianglelefteq\trianglelefteq G$ и $H \leq F \leq G$, то $H \trianglelefteq\trianglelefteq F$.

В частности, если $H \trianglelefteq\trianglelefteq G$ и $H \leq F \leq G$, то $H \trianglelefteq\trianglelefteq F$. Естественно спросить, верно ли, что если $F \trianglelefteq\trianglelefteq G$ и $H \trianglelefteq\trianglelefteq G$, то $F \cap H \trianglelefteq\trianglelefteq G$ и $\langle F, H\rangle \trianglelefteq\trianglelefteq G$? Для пересечения это действительно всегда так, для порождения ситуация значительно сложнее.

Задача 7 (Виландт)**.** Докажите, что пересечение двух субнормальных подгрупп $F, H \trianglelefteq\trianglelefteq G$ является субнормальной подгруппой. При этом глубина подгруппы $F \cap H$ не превосходит сумму глубины F и глубины H.

Решение. Пусть глубина F равна r,
$$F = F_0 \trianglelefteq F_1 \trianglelefteq F_2 \trianglelefteq \ldots \trianglelefteq F_r = G,$$
а глубина H равна s,
$$H = H_0 \trianglelefteq H_1 \trianglelefteq H_2 \trianglelefteq \ldots \trianglelefteq H_s = G.$$
Тогда
$$F \cap H = F \cap H_0 \trianglelefteq F \cap H_1 \trianglelefteq F \cap H_2 \trianglelefteq \ldots \trianglelefteq F \cap H_r = F$$
показывает, что $F \cap H$ является субнормальной подгруппой в F, глубина которой не превосходит s.

Следующая теорема приводится без доказательства.

Теорема 4 (Виландт)**.** *Пусть G конечная группа, $F, H \trianglelefteq\trianglelefteq G$. Тогда $\langle F, H\rangle \trianglelefteq\trianglelefteq G$.*

§ 5. Фактор-группы

Теперь мы в состоянии определить, когда на множестве G/H смежных классов G по H можно естественным образом ввести структуру группы.

1. Умножение смежных классов по нормальной подгруппе. Для нормальной подгруппы $H \trianglelefteq G$ отношения сравнимости слева и справа совпадают, тем самым вместо левых и правых смежных классов можно говорить просто о смежных классах G по H.

Лемма 5. *Отношение сравнимости $\equiv$ alias $\equiv_H$ по нормальной подгруппе H является конгруэнцией в G. Иными словами,*
• *если $x \equiv y$ и $u \equiv v$, то $xu \equiv yv$;*
• *если $x \equiv y$, то $x^{-1} \equiv y^{-1}$.*

Доказательство. По условию, $xH = yH$ и $uH = vH$. Нам нужно показать, что $xuH = yvH$. В самом деле,
$$xuH = (xu)(HH) = x(uH)H = x(Hu)H = (xH)(uH) =$$
$$= (yH)(vH) = y(Hv)H = y(vH)H = (yv)(HH) = yvH.$$

Кроме ассоциативности и определения подгруппы мы здесь воспользовались тем, что $uH = Hu$ и $Hv = vH$, т. е. тем, что H нормальна. Второе утверждение леммы вытекает из первого (и поэтому обычно не включается в определение конгруэнции). Перемножая сравнения $x^{-1} \equiv x^{-1}$, $x \equiv y$, $y^{-1} \equiv y^{-1}$, по только что доказанному получаем $y^{-1} = x^{-1}xy^{-1} \equiv x^{-1}yy^{-1} = x^{-1}$. □

Утверждение леммы можно сформулировать и чуть иначе. А именно, мы доказали два следующих утверждения. Если $H \trianglelefteq G$, то:

• результат произведения по Минковскому двух смежных классов снова является смежным классом,

• обратный по Минковскому к смежному классу является смежным классом.

Первое из этих утверждений неверно, если H не является нормальной подгруппой. Что касается второго, то, как мы уже знаем, $(xH)^{-1} = Hx^{-1}$, но для нормальной подгруппы $Hx^{-1} = x^{-1}H$.

2. Фактор-группа. Как мы только что показали, если $H \trianglelefteq G$, то на множестве смежных классов G/H можно корректно определить умножение. Впервые эту конструкцию начали систематически рассматривать Жордан и Гельдер, причем сам термин `Faktorgruppe` впервые использовал Отто Гельдер в 1889 году.

Определение. Пусть $H \trianglelefteq G$. Тогда множество смежных классов G по H с умножением $xH \cdot yH = xyH$ называется **фактор-группой** G по H и обозначается G/H.

По только что доказанной лемме умножение, которое мы определили на G/H, действительно **корректно**. Иными словами, результат *не зависит* от выбора представителей $u \in xH$ и $v \in yH$. Корректность вытекает также из того, что определенное выше умножение классов совпадает с умножением по Минковскому:

$$(xH)(yH) = x(Hy)H = x(yH)H = (xy)(HH) = xyH = xH \cdot yH.$$

Убедимся в том, что оно действительно определяет на G/H структуру группы.

Теорема 6. *Пусть $H \trianglelefteq G$. Тогда множество G/H относительно операции умножения классов образует группу.*

Доказательство. Так как умножение классов определяется в терминах умножения представителей, то ассоциативность вытекает из ассоциативности умножения в G. Нейтральным элементом в G/H является $H = e_{G/H}$. Наконец, классом, обратным к классу xH, является $x^{-1}H$. □

Отображение $\pi : G \longrightarrow G/H$, $x \mapsto xH$, сопоставляющее каждому элементу его класс, называется **канонической проекцией** G на G/H. При этом

$$\pi(xy) = xyH = xHyH = \pi(x)\pi(y).$$

§ 6. Первые примеры фактор-групп

Приведем несколько очевидных примеров фактор-групп. Забегая вперед, введем понятие изоморфизма.

Определение. Пусть G, F – группы. Биективное (взаимно-однозначное) отображение $\varphi : G \longrightarrow F$ называется, **изоморфизмом группы** G **на группу** F, если для любых двух элементов $x, y \in G$ выполняется равенство $\varphi(xy) = \varphi(x)\varphi(y)$. В случае, если существует изоморфизм $\varphi : G \longrightarrow F$, группы G и F называются **изоморфными**; при этом пишут $G \cong F$.

Изоморфные группы являются разными *воплощениями* одной и той же группы. Подробнее понятие изоморфизма будет изучено далее в нашем курсе.

• **Группа классов вычетов.** Пусть $G = \mathbb{Z}$, $H = m\mathbb{Z}$. Тогда $G/H = \mathbb{Z}/m\mathbb{Z}$ есть уже знакомая нам аддитивная группа классов вычетов по модулю m.

• **Фактор-группы группы** $\mathbb{R}^*$. Пусть $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ — мультипликативная группа ненулевых вещественных чисел, а $H = \mathbb{R}_+ = \{\lambda \in \mathbb{R} \mid \lambda > 0\}$ — подгруппа положительных вещественных чисел. Тогда $G/H = \{\mathbb{R}_+, -\mathbb{R}_+\} \cong \{\pm 1\}$. С другой стороны, если $H = \{\pm 1\}$, то $G/H = \{\{\pm\lambda\}, \lambda \in \mathbb{R}_+\} \cong \mathbb{R}_+$. Конечно, это связано с тем, что $\mathbb{R}^* = \mathbb{R}_+ \times \{\pm 1\}$.

• **Группа дробных частей.** Пусть $G = \mathbb{R}^+$ — аддитивная группа вещественных чисел, $H = \mathbb{Z}$. Тогда

$G/H = \{\lambda + \mathbb{Z}, \lambda \in [0, 1)\}$ состоит из дробных частей вещественных чисел, при этом сумма двух дробных частей $x, y \in [0, 1)$ — это их обычная сумма $x + y$, как вещественных чисел, если $x + y < 1$ и $x + y - 1$, если $x + y \geq 1$. Легко видеть, что $x \mapsto \cos(2\pi x) + i \sin(2\pi x)$ определяет изоморфизм G/H на мультипликативную группу $\mathbb{T}$ комплексных чисел по модулю равных 1.
• **Фактор-группы $\mathbb{C}^*$.** Пусть $G = \mathbb{R}^* = \mathbb{R} \setminus \{0\}$ — мультипликативная группа ненулевых вещественных чисел, а $H = \mathbb{R}_{>0}$ — подгруппа положительных вещественных чисел. Тогда $G/H = \{\{\varphi\mathbb{R}_{>0}\}, \varphi \in \mathbb{T}\} \cong \mathbb{T}$. С другой стороны, если $H = \mathbb{T}$, то $G/H = \{\{\lambda\mathbb{T}\}, \lambda \in \mathbb{R}_{>0}\} \cong \mathbb{R}_{>0}$. В действительности, это связано с тем, что $\mathbb{C}^* = \mathbb{R}_{>0} \times \mathbb{T}$.
• **Перестановки по модулю четных перестановок.** Пусть $G = S_n$ — симметрическая группа, а $H = A_n$ — знакопеременная группа степени n. Тогда $G/H \cong \{\pm 1\}$. Этот и следующий примеры будут подробно рассмотрены в лекции о группе перестановок.
• Группа $S_3 \cong S_4/V$ является фактор-группой S_4 по модулю четверной группы V.

§ 7. Теорема о соответствии

Пусть $H \trianglelefteq G$. Сейчас мы построим изоморфизм между решетками $L(G, H)$ и $L(G/H) = L(1, G/H)$.

Теорема 7. *Пусть $H \trianglelefteq G$ и $\pi : G \longrightarrow G/H$. Тогда сопоставление $\varphi : F \mapsto \pi(F) = F/H$ устанавливает биекцию между множеством всех подгрупп в G, содержащих H, и множеством всех подгрупп в G/H. Эта биекция сохраняет включения, пересечения и порождения, а также свойство нормальности. Иными словами, для любых $H \leq F, K \leq G$ имеем:*
i) $F \leq K \iff F/H \leq K/H$;
ii) $\varphi(F \cap K) = \varphi(F) \cap \varphi(K)$;
iii) $\varphi(\langle F, K\rangle) = \langle\varphi(F), \varphi(K)\rangle$;
iv) $F \trianglelefteq G \iff F/H \trianglelefteq G/H$.

Доказательство. Так как $H \leq F \leq G$, $H \trianglelefteq G$ влечет $H \trianglelefteq F$, мы можем рассматривать F/H как подгруппу в G/H. Предположим, что $H \leq F, K \leq G$ — две подгруппы в G такие, что $F/H = K/H$. Тогда для любого $f \in F$ найдется такое $k \in K$, что $fH = kH$ и, тем самым, $f \in KH = K$. Обратное включение проверяется аналогично. Тем самым, $\varphi : L(G, H) \longrightarrow L(G/H, 1)$ инъективно. С другой стороны, если $L \leq G/H$ — подгруппа в G/H, то $F = \pi^{-1}(L) \geq H$ и, так как π сюръекция, то $\pi(F) = \pi(\pi^{-1}(L)) = L$. Тем самым, φ сюръекктивно, как и утверждалось. Проверка свойств i–iv совершенно элементарна и оставляется читателю в качестве упражнения. □