

§11. Композиционные факторы, произведения и силовские подгруппы

11.1. Простые группы. Группа G называется *простой*, если она не содержит нормальных подгрупп, отличных от $\{e\}$ и G . Например, любая группа простого порядка проста, поскольку по теореме Лагранжа¹ вообще не содержит никаких подгрупп кроме $\{e\}$ и G . Согласно сл. 10.1 на стр. 174 простота группы G равносильна тому, что всякий гомоморфизм $G \rightarrow H$ либо инъективен, либо отображает всю группу G в единицу. Одним из выдающихся достижений математики XX века является перечисление всех конечных простых групп. Этот список состоит из нескольких бесконечных серий и 26 так называемых *спорадических групп*, не входящих в серии. Бесконечные серии делятся на три семейства: циклические группы $\mathbb{Z}/(p)$ простого порядка, знакопеременные группы A_n с $n \neq 4$ и простые линейные алгебраические группы над конечными полями², такие как $\text{PSL}_n(\mathbb{F}_q)$, $\text{PSO}_n(\mathbb{F}_q)$, $\text{PSp}_n(\mathbb{F}_q)$ и т. п. Описание конечных простых групп стало итогом сотен работ десятков авторов по различным, напрямую не связанным друг с другом направлениям математики. Никакой универсальной концепции, позволяющей единообразно классифицировать все конечные простые группы не известно.

11.1.1. Простота знакопеременных групп. Покажем, что знакопеременная группа A_5 проста. Так как перестановки сопряжены если и только если у них одинаковый цикловой тип³, классы сопряжённости чётных перестановок в S_5 состоят из перестановок цикловых типов

$$\begin{array}{ccccccc}
 \square & \square & \square & \square & & & \\
 & \square & \square & & & & \\
 & & \square & \square & & & \\
 & & & \square & & & \\
 & & & & \square & & \\
 & & & & & \square & \\
 & & & & & & \square
 \end{array}
 \quad \text{и} \quad
 \begin{array}{c}
 \square \\
 \square \\
 \square \\
 \square \\
 \square
 \end{array}
 \quad (11-1)$$

(5-циклы, 3-циклы, пары независимых транспозиций и тождественное преобразование), коих имеется⁴ соответственно $24 = 5!/5$, $20 = 5!/(3 \cdot 2)$, $15 = 5!/(2^2 \cdot 2)$ и 1.

Упражнение 11.1. Покажите, что класс сопряжённости чётной перестановки g в S_n либо совпадает с её классом сопряжённости в A_n , либо является объединением двух классов сопряжённости в A_n , причём второе происходит если и только если все циклы перестановки g имеют разные нечётные длины.

Мы заключаем, что 3-циклы, пары независимых транспозиций и тождественная перестановка являются классами сопряжённости в A_5 , а 5-циклы разбиваются на два класса сопряжённости в A_5 , состоящие из 12 циклов, сопряжённых $|1, 2, 3, 4, 5\rangle$, и 12 циклов, сопряжённых $|2, 1, 3, 4, 5\rangle$. Поскольку нормальная подгруппа $H \trianglelefteq A_5$ вместе с каждой перестановкой содержит и все ей сопряжённые, её порядок $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, где каждый ε_i равен либо 1, либо 0, при этом по теореме Лагранжа $|H|$ делит $|A_5| = 60 = 3 \cdot 4 \cdot 5$.

Упражнение 11.2. Убедитесь, что такое возможно ровно в двух случаях: когда все $\varepsilon_i = 1$ или когда все $\varepsilon_i = 0$.

Тем самым, в A_5 нет нетривиальных собственных нормальных подгрупп.

ТЕОРЕМА 11.1

Все знакопеременные группы A_n с $n \geq 5$ просты.

¹См. теор. 10.3 на стр. 183.

²Описанию таких групп посвящены спецкурсы по линейным алгебраическим и арифметическим группам, например, см. книгу Дж. Хамфри. *Линейные алгебраические группы*. М., «Наука», 1980.

³См. прим. 10.15 на стр. 180.

⁴См. упр. 10.8 на стр. 169.

Доказательство. Индукция по n . Случай $n = 5$ был разобран выше. Рассмотрим нормальную подгруппу $N \trianglelefteq A_n$. Так как стабилизатор элемента 1 в группе A_n изоморфен A_{n-1} , его пересечение с N , будучи нормальной подгруппой в A_{n-1} , либо совпадает с A_{n-1} , либо тривиально. Поскольку стабилизаторы всех элементов сопряжены, подгруппа N либо содержит стабилизаторы всех элементов, либо действует свободно¹. В первом случае N содержит все 3-циклы и по [упр. 10.31](#) на стр. 186 совпадает с A_n . Рассмотрим второй случай и допустим, что N содержит не тождественную перестановку g . Так как она действует без неподвижных точек, при $n \geq 6$ найдутся такие различные элементы $\{1, i, j, k, \ell, m\}$, что $g(1) = i$ и $g(j) = k$. Сопрягая g циклом $|k, \ell, m\rangle \in A_n$, получаем перестановку $h \in N$ с $h(1) = i$ и $h(j) = \ell \neq k$. Перестановка $gh^{-1} \in N$ не тождественна и оставляет 1 на месте. Противоречие. \square

11.1.2. Простота групп $\mathrm{PSL}_n(\mathbb{k})$. Фактор полной линейной группы координатного векторного пространства \mathbb{k}^n по её центру, состоящему из скалярных матриц λE , где $\lambda \in \mathbb{k}^\times$, называется *проективной линейной группой* и обозначается $\mathrm{PGL}_n(\mathbb{k}) \stackrel{\text{def}}{=} \mathrm{GL}_n(\mathbb{k}) / \mathbb{k}^\times \cdot E$. Эта группа естественным образом действует на множестве одномерных векторных подпространств в \mathbb{k}^n , которое обозначается $\mathbb{P}_{n-1}(\mathbb{k})$ и называется $(n-1)$ -мерным *проективным пространством*² над полем \mathbb{k} . Состоящая из классов пропорциональных матриц определителя 1 подгруппа

$$\mathrm{PSL}_n(\mathbb{k}) = \mathrm{SL}_n(\mathbb{k}) / \mu_n(\mathbb{k}) \cdot E \subset \mathrm{PGL}_n(\mathbb{k}),$$

где $\mu_n(\mathbb{k}) \subset \mathbb{k}^\times$ — мультипликативная группа корней n -той степени из 1 в поле \mathbb{k} , называется *специальной проективной линейной группой*.

УПРАЖНЕНИЕ 11.3. Убедитесь, что PSL_n действует 2-транзитивно³ на \mathbb{P}_{n-1} .

Если $\mathbb{k} = \mathbb{F}_q$ состоит из q элементов, то мультипликативная группа \mathbb{F}_q^\times циклическая порядка $q-1$ и корни уравнения $x^n = 1$ образуют в ней циклическую подгруппу порядка $\mathrm{nod}(q-1, n)$.

УПРАЖНЕНИЕ 11.4. Убедитесь, корни уравнения $nx = 0$ в $\mathbb{Z}/(m)$ составляют циклическую подгруппу порядка $\mathrm{nod}(m, n)$.

Таким образом, $|\mathrm{PSL}_n(\mathbb{F}_q)| = |\mathrm{SL}_n(\mathbb{F}_q)| / \mathrm{nod}(q-1, n) = \prod_{k=0}^{n-1} (q^n - q^k) / ((q-1) \mathrm{nod}(q-1, n))$.

ТЕОРЕМА 11.2

Все группы $\mathrm{PSL}_n(\mathbb{k})$ просты, за исключением⁴ $\mathrm{PSL}_2(\mathbb{F}_2) = \mathrm{GL}_2(\mathbb{F}_2) \simeq S_3$ и $\mathrm{PSL}_2(\mathbb{F}_3) \simeq A_4$.

Доказательство. Обозначим через $P \subset \mathrm{PSL}_n$ стабилизатор одномерного подпространства, порождённого первым вектором стандартного базиса e_1, \dots, e_n в \mathbb{k}^n . Группа P состоит из классов пропорциональных матриц вида

$$\left(\begin{array}{c|ccc} * & * & \cdots & * \\ \hline 0 & & & \\ \vdots & & * & \\ 0 & & & \end{array} \right) \quad (11-2)$$

¹Т. е. никакой отличный от единицы элемент не имеет неподвижных точек, см. н° 10.4 на стр. 177.

²См. стр. 204 и 222 курса http://gorod.bogomolov-lab.ru/ps/stud/geom_ru/2122/list.html.

³Т. е. транзитивно действует на упорядоченных парах точек, см. н° 10.4 на стр. 177.

⁴См. [упр. 10.33](#) на стр. 186.

с определителем 1 и содержит нормальную абелеву подгруппу $A \triangleleft P$ матриц, пропорциональных

$$\left(\begin{array}{c|ccc} 1 & \alpha_2 & \cdots & \alpha_n \\ \hline 0 & 1 & & 0 \\ \vdots & & \ddots & \\ 0 & 0 & & 1 \end{array} \right) = E + \alpha_2 E_{12} + \dots + \alpha_n E_{1n},$$

которая является ядром гомоморфизма $P \rightarrow \text{PGL}_{n-1}$, переводящего матрицу (11-2) в её правую нижнюю угловую подматрицу размера $(n-1) \times (n-1)$.

УПРАЖНЕНИЕ 11.5. Убедитесь, что это и в самом деле гомоморфизм групп.

Так как подгруппа A содержит все трансвекции вида $T_{1j}(\alpha)$, сопряжённые ей подгруппы gAg^{-1} , где $g \in \text{PSL}_n$, содержат вообще все трансвекции и порождают¹ PSL_n .

УПРАЖНЕНИЕ 11.6. Убедитесь, что $T_{ij}(\alpha) = gT_{1j}(-\alpha)g^{-1}$, где $g \in \text{SL}_n$ переводит e_1 в e_i , а e_i в $-e_1$, оставляя все остальные базисные векторы на месте.

Мы заключаем, что произведения элементов вида gag^{-1} , $a \in A$, $g \in \text{PSL}_n$ исчерпывают PSL_n .

Рассмотрим теперь отличную от единичной нормальную подгруппу $N \trianglelefteq \text{PSL}_n$. Пространство \mathbb{P}_{n-1} является дизъюнктивным объединением орбит подгруппы N , и в силу нормальности N каждый элемент $g \in \text{PSL}_n$ переводит N -орбиту точки x в N -орбиту точки gx , ибо

$$y = hx \iff gy = (ghg^{-1})gx.$$

Таким образом, группа PSL_n , с одной стороны, не может перевести пару точек, лежащих в одной N -орбите, в пару точек, лежащих в разных N -орбитах, а с другой стороны, действует 2-транзитивно по упр. 11.3 на стр. 188. Такое возможно, только если N -орбита всего одна, т. е. для любого $g \in \text{PSL}_n$ существует такое $h \in N$, что $ge_1 = he_1$, откуда $h^{-1}g \in P$ и $g \in hP$. Мы заключаем, что $\text{PSL}_n = NP = PN$. Поскольку сопряжение элементами из P оставляет подгруппу $A \triangleleft P$ на месте, каждый элемент из PSL_n является произведением элементов вида hah^{-1} с $a \in A$, $h \in N$ и в силу равенства $AN = NA$ лежит в AN . В прим. 10.23 на стр. 186 мы видели, что все группы SL_n за исключением двух, указанных в условии теоремы, совпадают со своими коммутантами. Но коммутатор элементов вида ah с $a \in A$, $h \in N$ в силу абелевости A и нормальности N лежит в N .

УПРАЖНЕНИЕ 11.7. Убедитесь в этом.

Поэтому $\text{PSL}_n = \text{PSL}'_n = N$ во всех случаях, кроме двух исключительных. □

11.2. Композиционные факторы. Конечная строго убывающая последовательность подгрупп

$$G = G_0 \supsetneq G_1 \supsetneq G_2 \supsetneq \dots \supsetneq G_{n-1} \supsetneq G_n = \{e\} \quad (11-3)$$

называется *композиционным рядом* или *рядом Жордана – Гёльдера* группы G , если при каждом i подгруппа G_{i+1} нормальна в G_i и фактор G_i/G_{i+1} прост. В этой ситуации неупорядоченный набор простых групп G_i/G_{i+1} (в котором возможны повторения) называется набором *композиционных факторов* (или *факторов Жордана – Гёльдера*) группы G , а число n называется *длиной* композиционного ряда (11-3).

¹См. упр. 10.34 на стр. 186.

ПРИМЕР 11.1 (КОМПОЗИЦИОННЫЕ ФАКТОРЫ S_4)

Выше мы видели, что симметрическая группа S_4 имеет композиционный ряд

$$S_4 \triangleright A_4 \triangleright V_4 \triangleright \mathbb{Z}/(2) \triangleright \{e\},$$

в котором $A_4 \triangleleft S_4$ — подгруппа чётных перестановок, $V_4 \triangleleft A_4$ — подгруппа Клейна, состоящая из тождественной перестановки и трёх перестановок циклового типа $\begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, а

$$\mathbb{Z}/(2) \triangleleft V_4 \simeq \mathbb{Z}/(2) \oplus \mathbb{Z}/(2)$$

любая из трёх циклических подгрупп второго порядка, порождённых неединичными элементами. Таким образом, симметрическая группа S_4 имеет композиционные факторы $\mathbb{Z}/(2) = S_4/A_4$, $\mathbb{Z}/(3) = A_4/V_4$, $\mathbb{Z}/(2) = V_4/(\mathbb{Z}/(2))$ и $\mathbb{Z}/(2) = \mathbb{Z}/(2)/\{e\}$.

УПРАЖНЕНИЕ 11.8. Убедитесь, что $A_4/V_4 \simeq \mathbb{Z}/(3)$.

ТЕОРЕМА 11.3 (ТЕОРЕМА ЖОРДАНА – ГЁЛЬДЕРА)

Если группа G имеет конечный композиционный ряд, то неупорядоченный набор его факторов не зависит от выбора композиционного ряда. В частности, все ряды Жордана – Гёльдера имеют одинаковую длину.

Доказательство. Пусть у группы G есть два композиционных ряда

$$G = P_0 \supseteq P_1 \supseteq P_2 \supseteq \dots \supseteq P_{n-1} \supseteq P_n = \{e\} \quad (11-4)$$

$$G = Q_0 \supseteq Q_1 \supseteq Q_2 \supseteq \dots \supseteq Q_{m-1} \supseteq Q_m = \{e\}. \quad (11-5)$$

Мы собираемся вставить между последовательными членами этих рядов дополнительные цепочки нестрого убывающих подгрупп так, чтобы получившиеся удлинённые ряды стали равной длины, и установить между их последовательными факторами биекцию, при которой соответствующие друг другу факторы будут изоморфны. Для этого заменим каждое звено $P_i \supseteq P_{i+1}$ верхней цепочки (11-4) цепочкой

$$P_i \supseteq (Q_1 \cap P_i)P_{i+1} \supseteq (Q_2 \cap P_i)P_{i+1} \supseteq \dots \supseteq (Q_{m-1} \cap P_i)P_{i+1} \supseteq P_{i+1}, \quad (11-6)$$

которая получается пересечением нижней цепочки (11-5) с подгруппой P_i и умножением всех полученных групп на нормальную в P_i подгруппу P_{i+1} . В [предл. 10.5](#) на стр. 185 мы видели, что если подгруппа H нормализует подгруппу N , то $NH = HN$ тоже является подгруппой, причём $NH \triangleright N$, $H \triangleright (H \cap N)$ и $NH/N \simeq H/(H \cap N)$. Применяя это к подгруппам

$$H = Q_k \cap P_i \quad \text{и} \quad N = (Q_{k+1} \cap P_i)P_{i+1},$$

мы получаем $NH = (Q_k \cap P_i)P_{i+1}$ и $H \cap N = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})$.

УПРАЖНЕНИЕ 11.9. Убедитесь, что H нормализует N , и проверьте последние два равенства.

Таким образом, $(Q_k \cap P_i)P_{i+1} \supseteq (Q_{k+1} \cap P_i)P_{i+1}$ и

$$\frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}. \quad (11-7)$$

Группа P_{i+1} является нормальной подгруппой во всех группах цепочки (11-6). Факторизуя по ней, получаем цепочку фактор групп

$$\frac{P_i}{P_{i+1}} \supseteq \frac{(Q_1 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \frac{(Q_2 \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \dots \supseteq \frac{(Q_{m-1} \cap P_i)P_{i+1}}{P_{i+1}} \supseteq \{e\}, \quad (11-8)$$

в которой каждая подгруппа нормальна в предыдущей, а последовательные факторы

$$\frac{(Q_k \cap P_i)P_{i+1}/P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}/P_{i+1}} \simeq \frac{(Q_k \cap P_i)P_{i+1}}{(Q_{k+1} \cap P_i)P_{i+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})}$$

совпадают с (11-7). Так как группа P_i/P_{i+1} проста, мы заключаем, что в цепочке (11-8) имеется ровно одно нестрогое включение, а все остальные включения — равенства. Тем самым, ровно один из факторов (11-7) отличен от единицы и изоморфен P_i/P_{i+1} .

Те же самые рассуждения с заменой P на Q позволяют вставить между последовательными группами $Q_k \triangleright Q_{k+1}$ композиционного ряда (11-5) убывающую цепочку подгрупп

$$Q_k \supseteq (P_1 \cap Q_k)Q_{k+1} \supseteq (P_2 \cap Q_k)Q_{k+1} \supseteq \dots \supseteq (P_{n-1} \cap Q_k)Q_{k+1} \supseteq Q_{k+1}, \quad (11-9)$$

каждая из которых нормальна в предыдущей, а последовательные факторы имеют вид

$$\frac{(P_i \cap Q_k)Q_{k+1}}{(P_{i+1} \cap Q_k)Q_{k+1}} \simeq \frac{(Q_k \cap P_i)}{(Q_{k+1} \cap P_i)(Q_k \cap P_{i+1})} \quad (11-10)$$

и изоморфны соответствующим факторам (11-7). Таким образом, вставляя между последовательными элементами композиционного ряда (11-4) цепочки (11-6), а между последовательными элементами ряда (11-5) — цепочки (11-9), мы получим ряды одинаковой длины, в которых не все включения строгие, но факторы находятся в биективном соответствии, сопоставляющем друг другу изоморфные факторы (11-10) и (11-7). Поскольку Q_{k+1} является нормальной подгруппой всех групп цепочки (11-9), те же аргументы, что применялись выше к подгруппе P_{i+1} и цепочке (11-6), показывают, что при фиксированном k среди факторов (11-10) имеется ровно один отличный от единицы, и он изоморфен Q_k/Q_{k+1} . \square

Замечание 11.1. Непростая группа может иметь несколько разных композиционных рядов с одинаковым набором факторов, а группы с одинаковыми наборами факторов Жордана-Гёльдера не обязательно изоморфны.

11.3. Полупрямые произведения. Для пары подгрупп N, H группы G отображение

$$N \times H \rightarrow NH, \quad (x, h) \mapsto xh,$$

биективно если и только если $N \cap H = \{e\}$. В самом деле, при $x_1 h_1 = x_2 h_2$ элемент $x_2^{-1} x_1 = h_2 h_1^{-1} \in N \cap H$, и если $N \cap H = \{e\}$, то $x_2 = x_1$ и $h_2 = h_1$, а если в $N \cap H$ есть элемент $z \neq e$, то разные пары $(e, e), (z, z^{-1}) \in N \times H$ перейдут в один и тот же элемент $e \in NH$. Будем называть подгруппы $N, H \subset G$ *дополнительными*, если $N \cap H = \{e\}$ и $NH = G$. В этом случае группа G как множество находится в биекции с прямым произведением $N \times H$. Если подгруппа $N \triangleleft G$ при этом нормальна, то композиция элементов $g_1 = x_1 h_1$ и $g_2 = x_2 h_2$ может быть выражена в терминах пар $(x_1, h_1), (x_2, h_2) \in N \times H$. А именно, так как

$$g_1 g_2 = x_1 h_1 x_2 h_2 = x_1 (h_1 x_2 h_1^{-1}) \cdot h_1 h_2 \quad \text{и} \quad h_1 x_2 h_1^{-1} \in N,$$

группу G можно описать как множество $N \times H$ с операцией

$$(x_1, h_1) \cdot (x_2, h_2) = (x_1 \operatorname{Ad}_{h_1}(x_2), h_1 h_2), \quad (11-11)$$

где через $\operatorname{Ad}_h : N \rightarrow N, x \mapsto hxh^{-1}$, обозначено присоединённое действие элемента h на нормальной подгруппе N . В этой ситуации говорят, что группа G является *полупрямым произведением* нормальной подгруппы $N \triangleleft G$ и дополнительной к ней подгруппы $H \subset G$ и пишут $G = N \rtimes H$. Если сопряжение элементами из подгруппы H действует на подгруппе N тривиально, что равносильно перестановочности $xh = hx$ любых двух элементов $x \in N$ и $h \in H$, то полупрямое произведение называется *прямым*. В этом случае $(x_1, h_1) \cdot (x_2, h_2) = (x_1 x_2, h_1 h_2)$ для всех пар $(x_1, h_1), (x_2, h_2) \in N \times H$.

ПРИМЕР 11.2 ($D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$)

Группа диэдра D_n содержит нормальную подгруппу поворотов, изоморфную аддитивной группе $\mathbb{Z}/(n)$. Подгруппа второго порядка, порождённая любым отражением, дополнительная к группе поворотов и изоморфна аддитивной группе $\mathbb{Z}/(2)$. Присоединённое действие отражения на группе поворотов меняет знак у угла поворота. При отождествлении группы поворотов с $\mathbb{Z}/(n)$ это действие превращается в умножение на -1 . Таким образом, $D_n = \mathbb{Z}/(n) \rtimes \mathbb{Z}/(2)$ и в терминах пар $(x, y) \in \mathbb{Z}/(n) \times \mathbb{Z}/(2)$ композиция на группе диэдра задаётся правилом

$$(x_1, y_1) \cdot (x_2, y_2) = (x_1 + (-1)^{y_1} x_2, y_1 + y_2), \quad x_1, x_2 \in \mathbb{Z}/(n), \quad y_1, y_2 \in \mathbb{Z}/(2).$$

ПРИМЕР 11.3 ($\operatorname{Aff}(V) = V \rtimes \operatorname{GL}(V)$, продолжение ПРИМ. 10.20 на стр. 183)

Аффинная группа¹ $\operatorname{Aff}(V)$ содержит нормальную подгруппу параллельных переносов, которая изоморфна аддитивной группе векторного пространства V и является ядром сюръективного гомоморфизма групп

$$D : \operatorname{Aff}(V) \rightarrow \operatorname{GL}(V), \quad \varphi \mapsto D_\varphi, \quad (11-12)$$

сопоставляющего аффинному преобразованию $\varphi : \mathbb{A}(V) \rightarrow \mathbb{A}(V)$ его дифференциал

$$D_\varphi : V \rightarrow V, \quad \overline{pq} \mapsto \overline{\varphi(p)\varphi(q)}.$$

Если зафиксировать в $\mathbb{A}(V)$ какую-нибудь точку p , то ограничение гомоморфизма (11-12) на стабилизатор $\operatorname{Stab}_p \subset \operatorname{Aff}(V)$ задаст изоморфизм $D_p : \operatorname{Stab}_p \xrightarrow{\simeq} \operatorname{GL}(V)$. Обратный изоморфизм сопоставляет линейному оператору $f : V \rightarrow V$ аффинное преобразование

$$\varphi_f : \mathbb{A}(V) \rightarrow \mathbb{A}(V), \quad x \mapsto p + f(\overline{px}),$$

оставляющее на месте точку p . Поскольку каждое преобразование $\varphi \in \operatorname{Aff}(V)$ раскладывается в композицию $\varphi = \tau_v \circ (\tau_{-v} \circ \varphi)$ параллельного переноса τ_v на вектор $v = \overline{p\varphi(p)}$ и преобразования $\tau_{-v} \circ \varphi \in \operatorname{Stab}(p)$, группа $\operatorname{Aff}(V) = V \rtimes \operatorname{Stab}_p \simeq V \rtimes \operatorname{GL}(V)$. Согласно ПРИМ. 10.20 на стр. 183, композиция в группе $V \rtimes \operatorname{GL}(V)$ задаётся правилом $(u, f) \cdot (w, g) = (u + f(w), fg)$.

¹См. ПРИМ. 10.20 на стр. 183.

11.3.1. Полупрямое произведение групп. Предыдущую конструкцию можно применить к двум абстрактным группам N и H как только задано действие группы H на группе N , т. е. гомоморфизм группы H в группу автоморфизмов группы N :

$$\psi : H \rightarrow \text{Aut } N, \quad h \mapsto \psi_h : N \simeq N, \quad (11-13)$$

По аналогии с форм. (11-11) на стр. 192 зададим на множестве $N \times H$ операцию правилом

$$(x_1, h_1) \cdot (x_2, h_2) \stackrel{\text{def}}{=} (x_1 \psi_{h_1}(x_2), h_1 h_2). \quad (11-14)$$

УПРАЖНЕНИЕ 11.10. Проверьте, что формула (11-14) задаёт на $N \times H$ структуру группы с единицей (e, e) и обращением $(x, h)^{-1} = (\psi_h^{-1}(x^{-1}), h^{-1})$, где $\psi_h^{-1} = \psi_{h^{-1}}$ — автоморфизм, обратный к $\psi_h : N \simeq N$.

Полученная таким образом группа называется *полупрямым произведением* групп N и H по действию $\psi : N \rightarrow \text{Aut } N$ и обозначается $N \rtimes_{\psi} H$. Подчеркнём, что результат зависит от выбора действия ψ . Если действие тривиально, т. е. $\psi_h = \text{Id}_N$ для всех $h \in H$, мы получаем прямое произведение $N \times H$ с покомпонентными операциями.

УПРАЖНЕНИЕ 11.11. Убедитесь, что подмножество $N' \stackrel{\text{def}}{=} \{(x, e) \mid x \in N\}$ является изоморфной группе N нормальной подгруппой в $G = N \rtimes_{\psi} H$ и фактор $G/N' \simeq H$, а подмножество $H' \stackrel{\text{def}}{=} \{(e, h) \mid h \in H\}$ (e, h) является изоморфной H и дополнительной к N' подгруппой в G , причём $G = N' \rtimes H'$ является полупрямым произведением своих подгрупп N' и H' .

ПРЕДЛОЖЕНИЕ 11.1

Для любых гомоморфизма $\psi : H \rightarrow \text{Aut}(N)$, $h \mapsto \psi_h$, и автоморфизмов $\alpha : H \simeq H$ и $\beta : N \simeq N$ отображения $(n, h) \mapsto (n, \alpha^{-1}h)$ и $(n, h) \mapsto (\beta n, h)$ задают изоморфизмы полупрямых произведений $N \rtimes_{\psi} H \simeq N \rtimes_{\psi \circ \alpha} H$ и $N \rtimes_{\psi} H \simeq N \rtimes_{\text{Ad}_{\beta}(\psi)} H$, где $\text{Ad}_{\beta}(\psi) : H \rightarrow \text{Aut}(N)$, $h \mapsto \beta \psi_h \beta^{-1}$.

Доказательство. Отображение $(n, h) \mapsto (n, \alpha^{-1}h)$ переводит сомножители из левой части равенства $(n_1, h_1)(n_2, h_2) = (n_1 \psi_{h_1} n_2, h_1 h_2)$ в $(n_1, \alpha^{-1}h_1)$ и $(n_2, \alpha^{-1}h_2)$, произведение которых в $N \rtimes_{\psi \circ \alpha} H$ равно $(n_1 \psi_{\alpha^{-1}h_1} n_2, \alpha^{-1}(h_1 h_2))$. Отображение $(n, h) \mapsto (\beta n, h)$ переводит те же самые сомножители в $(\beta n_1, h_1)$ и $(\beta n_2, h_2)$. Их произведение в $N \rtimes_{\text{Ad}_{\beta}(\psi)} H$ равно $(\beta(n_1 \psi_{h_1} n_2), h_1 h_2)$. \square

ПРИМЕР 11.4 (ГОЛОМОРФ)

Группа автоморфизмов $\text{Aut } G$ произвольной группы G тавтологически действует на G . Полупрямое произведение $\text{Hol } G \stackrel{\text{def}}{=} G \rtimes \text{Aut } G$ по этому действию называется *голоморфом* группы G . Вложение $G \hookrightarrow \text{Hol } G$ замечательно тем, что любой автоморфизм группы G является сужением на G внутреннего автоморфизма объемлющей группы $\text{Hol } G$.

ПРИМЕР 11.5 (СПЛЕТЕНИЕ)

Для любых двух групп H, N множество N^H всех функций $f : H \rightarrow N$ имеет естественную структуру группы, в которой $f_1 f_2 : H \rightarrow N$, $x \mapsto f_1(x) f_2(x)$. Эту группу можно воспринимать как прямое произведение одинаковых копий группы N , занумерованных элементами¹ $x \in H$. Группа H действует на N^H по следующему правилу: элемент $h \in H$ переводит функцию $f : H \rightarrow N$ в функцию $hf : x \mapsto f(xh)$.

УПРАЖНЕНИЕ 11.12. Убедитесь, что $h(f_1 f_2) = (hf_1)(hf_2)$ и $(h_1 h_2)f = h_1(h_2 f)$.

¹Ср. с н° 1.6 на стр. 35.

Полупрямое произведение $N \wr H \stackrel{\text{def}}{=} N^H \rtimes H$ по этому действию называется *сплетением*¹ группы N с группой H . Сплетение замечательно тем, что любая группа G с нормальной подгруппой $N \triangleleft G$ и фактор группой $H = G/N$ допускает гомоморфное вложение Фробениуса $\varphi : G \hookrightarrow N \wr H$. Чтобы задать его, зафиксируем какое-нибудь теоретико-множественное сечение $\sigma : H \hookrightarrow G$ гомоморфизма факторизации $\pi : G \twoheadrightarrow H = G/N$, выбирающее в каждом классе $h \in G/N$ некоторый представитель $\sigma(h) \in G$. Тогда для любых $g \in G$ и $h \in H$ элемент $\sigma(h)g\sigma(h\pi(g))^{-1} \in N$, поскольку $\pi(\sigma(h)g\sigma(h\pi(g))^{-1}) = h\pi(g)(h\pi(g))^{-1} = e$. Рассмотрим функцию

$$\sigma_g : H \rightarrow N, \quad h \mapsto \sigma(h)g\sigma(h\pi(g))^{-1},$$

как элемент группы N^H и положим $\varphi_\sigma(g) = (\sigma_g, \pi(g)) \in N^H \rtimes H$.

УПРАЖНЕНИЕ 11.13. Убедитесь, что $\varphi_\sigma(g_1g_2) = \varphi_\sigma(g_1)\varphi_\sigma(g_2)$ в $N^H \rtimes H$ и что образы двух вложений $\varphi_\sigma, \varphi_\tau : G \hookrightarrow N \wr H$, построенных при помощи разных сечений $\sigma, \tau : H \hookrightarrow G$, сопряжены в группе $N \wr H$.

11.4. p -группы и теоремы Силова. Группа порядка p^n , где $p \in \mathbb{N}$ — простое, называется p -группой. Поскольку все нетривиальные подгруппы p -группы также являются p -группами, длина любой орбиты p -группы при любом её действии на любом множестве либо делится на p , либо равна единице. Мы получаем простое, но полезное

Предложение 11.2

Пусть p -группа G действует на конечном множестве X , число элементов в котором не делится на p . Тогда G имеет на X неподвижную точку. \square

Предложение 11.3

Любая p -группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы является множеством одноточечных орбит этого действия. Так как число элементов в группе и длины всех неодноточечных орбит делятся на p , одноточечные орбиты не могут исчерпываться одной орбитой элемента e . \square

УПРАЖНЕНИЕ 11.14. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

ОПРЕДЕЛЕНИЕ 11.1 (силовские подгруппы)

Пусть G — произвольная конечная группа. Запишем её порядок в виде $|G| = p^n m$, где p — простое, $n \geq 1$, и m взаимно просто с p . Всякая подгруппа $S \subset G$ порядка $|S| = p^n$ называется *силовской p -подгруппой* в G . Количество силовских p -подгрупп в G обозначается через $N_p(G)$.

ТЕОРЕМА 11.4 (ТЕОРЕМА СИЛОВА)

Для любого простого $p \mid |G|$ силовские p -подгруппы в G существуют. Все они сопряжены друг другу, и любая p -подгруппа в G содержится в некоторой силовской p -подгруппе.

Доказательство. Пусть $|G| = p^n m$, где m взаимно просто с p . Обозначим через \mathcal{E} множество p^n -элементных подмножеств в G и рассмотрим действие G на \mathcal{E} , индуцированное левым регулярным действием G на себе. Стабилизатор точки $F \in \mathcal{E}$ состоит из всех элементов $g \in G$, левое

¹По английски *wreath product*.

умножение на которые переводит множество $F \subset G$ в себя: $\text{Stab}(F) = \{g \in G \mid gF \subset F\}$. Так как $g_1x \neq g_2x$ при $g_1 \neq g_2$ в группе G , группа $\text{Stab}(F)$ свободно действует на множестве F и все орбиты этого действия состоят из $|\text{Stab}(F)|$ точек. Поэтому $|F| = p^n$ делится на $|\text{Stab}(F)|$ и имеется следующая альтернатива: либо длина G -орбиты элемента $F \in \mathcal{E}$ делится на p , либо G -орбита элемента $F \in \mathcal{E}$ состоит из m элементов и $|\text{Stab}(F)| = p^n$, т. е. подгруппа $\text{Stab}(F) \subset G$ силовская. Во втором случае согласно [предл. 11.2](#) каждая p -подгруппа $H \subset G$ (в частности, каждая силовская подгруппа), имеет на G -орбите элемента F неподвижную точку gF , а значит, содержится в силовской подгруппе $\text{Stab}(gF) = g \text{Stab}(F) g^{-1}$, сопряжённой к $\text{Stab}(F)$ (и совпадает с ней, если H силовская). Таким образом, для доказательства теоремы остаётся убедиться, что в множестве \mathcal{E} есть G -орбита, длина которой не делится на p . Это следует из [лем. 11.1](#) ниже. \square

ЛЕММА 11.1

$|\mathcal{E}| = \binom{p^nm}{p^n} \equiv m \pmod{p}$ не делится на p .

Доказательство. Класс вычетов $\binom{p^nm}{p^n} \pmod{p}$ равен коэффициенту при x^{p^n} , возникающему при раскрытии бинома $(1+x)^{p^nm}$ над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Так как над \mathbb{F}_p возведение в p -тую степень является аддитивным гомоморфизмом, $(1+x)^{p^n} = 1+x^{p^n}$, откуда $(1+x)^{p^nm} = (1+x^{p^n})^m = 1+mx^{p^n} + \text{старшие степени}$. \square

Следствие 11.1 (дополнение к теореме Силова)

В условиях теоремы Силова число N_p силовских p -подгрупп в G делит m и сравнимо с единицей по модулю p .

Доказательство. Обозначим множество силовских p -подгрупп в G через \mathcal{S} и рассмотрим действие G на \mathcal{S} , индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathcal{S}| = |G|/|\text{Stab}(P)|$, где $P \in \mathcal{S}$ — произвольно взятая силовская p -подгруппа. Поскольку $P \subset \text{Stab}(P)$, порядок $|\text{Stab}(P)|$ делится на $|P| = p^n$, а значит $|\mathcal{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что P , действуя сопряжениями на \mathcal{S} , имеет там ровно одну неподвижную точку, а именно, саму себя. Тогда порядки всех остальных P -орбит будут делиться на p , и мы получим $|\mathcal{S}| \equiv 1 \pmod{p}$.

Пусть силовская подгруппа $H \in \mathcal{S}$ неподвижна при сопряжении подгруппой P . Это означает, что $P \subset \text{Stab}(H) = \{g \in G \mid gHg^{-1} \subset H\}$. Поскольку $H \subset \text{Stab}(H) \subset G$, порядок $|\text{Stab}(H)| = p^nm'$, где $m' | m$ взаимно просто с p . Таким образом, и P , и H являются силовскими p -подгруппами в $\text{Stab}(H)$, причём H нормальна в $\text{Stab}(H)$. Так как все силовские подгруппы сопряжены, мы заключаем, что $H = P$, что и требовалось. \square

Пример 11.6 (группы порядка pq с простыми $p > q$)

Пусть $|G| = pq$, где $p > q$ простые. Тогда в G есть ровно одна, автоматически нормальная силовская p -подгруппа $H_p \simeq \mathbb{Z}/(p)$. Рассмотрим любую силовскую q -подгруппу $H_q \simeq \mathbb{Z}/(q)$. Поскольку H_p и H_q просты, $H_p \cap H_q = e$ и $G = H_p H_q$. Согласно [н° 11.3](#) $G = \mathbb{Z}/(p) \rtimes_{\psi} \mathbb{Z}/(q)$ для некоторого гомоморфизма $\psi : \mathbb{Z}/(q) \rightarrow \text{Aut}(\mathbb{Z}/(p))$.

УПРАЖНЕНИЕ 11.15. Убедитесь, что $\text{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^{\times} \simeq \mathbb{Z}/(p-1)$.

Гомоморфизм $\psi : \mathbb{Z}/(q) \rightarrow \text{Aut}(\mathbb{Z}/(p)) \simeq \mathbb{F}_p^{\times}$ однозначно задаётся своим значением на образующей $[1]_q$, которая является элементом порядка q . Поэтому элемент $\eta = \psi([1]_q) \in \mu_q(\mathbb{F}_p) \subset \mathbb{F}_p^{\times}$

является корнем q -й степени из 1 в поле \mathbb{F}_p . По [упр. 11.4](#) на стр. 188 группа $\mu_q(\mathbb{F}_p)$ циклическая порядка $\text{nod}(q, p-1)$. Мы заключаем, что если $q \nmid (p-1)$, то всякий гомоморфизм $\mathbb{Z}/(q) \rightarrow \text{Aut}(\mathbb{Z}/(p))$ тривиален и, стало быть, единственной группой порядка pq в этом случае является $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$. Если же $q \mid (p-1)$, то существует нетривиальный гомоморфизм

$$\psi: \rightarrow \text{Aut}(\mathbb{Z}/(p)), \quad [1]_q \mapsto \eta, \quad (11-15)$$

где $\eta \in \mathbb{F}_p^\times$ порождает мультипликативную группу $\mu_q(\mathbb{F}_p)$. Гомоморфизм (11-15) сопоставляет каждому элементу $[y]_q \in \mathbb{Z}/(q)$ автоморфизм $\psi_y: \mathbb{Z}/(p) \simeq \mathbb{Z}/(p)$, $[x]_p \mapsto [\eta^y x]_p$, и задаёт полупрямое произведение $\mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$ с операцией

$$([x_1]_p, [y_1]_q) \cdot ([x_2]_p, [y_2]_q) = ([x_1 + \eta^{y_1} x_2]_p, [y_1 + y_2]_q). \quad (11-16)$$

Любой другой нетривиальный гомоморфизм $\mathbb{Z}/(q) \rightarrow \text{Aut}(\mathbb{Z}/(p))$ имеет вид $\psi^m: [1]_q \mapsto \eta^m$, где $1 \leq m \leq q-1$, и является композицией гомоморфизма (11-15) с автоморфизмом умножения на $m: \mathbb{Z}/(q) \simeq \mathbb{Z}/(q)$, $[y]_q \mapsto [my]_q$. По [предл. 11.1](#) на стр. 193 задаваемое им полупрямое произведение $\mathbb{Z}/(p) \rtimes_{\psi \circ m} \mathbb{Z}/(q) \simeq \mathbb{Z}/(p) \rtimes_\psi \mathbb{Z}/(q)$. Мы заключаем, что при $q \mid (p-1)$ кроме абелевой группы $\mathbb{Z}/(p) \times \mathbb{Z}/(q)$ существует единственная с точностью до изоморфизма неабелева группа порядка pq . Она изоморфна $\mathbb{Z}/(p) \rtimes \mathbb{Z}/(q)$ с операцией (11-16). В частности, для простого $p > 2$ единственной с точностью до изоморфизма неабелевой группой порядка $2p$ является группа диэдра¹ D_p .

¹См. [прим. 11.2](#) на стр. 192.

Ответы и указания к некоторым упражнениям

Упр. II.1. Пусть $g \in A_n$, $h \in S_n \setminus A_n$. Всякая перестановка, сопряжённая g в S_n , сопряжена в A_n либо g , либо $\text{Ad}_h g$. Равенство $\text{Ad}_p g = \text{Ad}_h g$ равносильно равенству $\text{Ad}_{p^{-1}h} g = g$. Поэтому существование чётной перестановки p удовлетворяющей первому равенству равносильно существованию нечётной перестановки $p^{-1}h$, коммутирующей с g , т. е. класс сопряжённости перестановки g в S_n не распадается на два класса сопряжённости в A_n если и только если централизатор $Z(g)$ содержит нечётную перестановку. Когда в цикловом типе g есть строка чётной длины или две строки одинаковой нечётной длины, то такая перестановка есть, а если g является произведением попарно разных циклов нечётной длины, то — нет.

Упр. II.2. Правая часть равенства $|H| = 12\varepsilon_1 + 12\varepsilon_2 + 20\varepsilon_3 + 15\varepsilon_4 + 1$, приведённая по модулям 3, 4 и 5, равна, соответственно, $1 - \varepsilon_3$, $1 - \varepsilon_4$ и $1 + 2(\varepsilon_1 + \varepsilon_2)$. Она может делиться на 3 или на 4 только если $\varepsilon_3 = 1$ или $\varepsilon_4 = 1$. В обоих случаях $|H| \geq 16$, так что $|H|$ не может быть ни 3, ни 4, ни $3 \cdot 4$, ни $3 \cdot 5$. Если $|H|$ делится на 5, то $\varepsilon_1 = \varepsilon_2 = 1$ и $|H| \geq 25$, так что $|H|$ не может быть ни 5, ни $4 \cdot 5$. Остаются ровно две возможности: $|H| = 1$ и $|H| = 3 \cdot 4 \cdot 5$.

Упр. II.3. Чтобы перевести одномерные подпространства, порождённые непропорциональными векторами e_1, e_2 , в одномерные подпространства, порождённые непропорциональными векторами v_1, v_2 , дополним эти пары векторов до базисов $e = (e_1, \dots, e_n)$ и $v = (v_1, \dots, v_n)$. Матрица перехода C_{ee} имеет ненулевой определитель δ . Умножая её первый столбец на δ^{-1} получаем матрицу $F \in \text{SL}_n$. Оператор $x \mapsto Fx$ переводит e_1 в $\delta^{-1}v_1$, а e_2 в v_2 .

Упр. II.4. Пусть $1 \leq k \leq m$. Класс $[k] \in \mathbb{Z}/(m)$ удовлетворяет уравнению $n[k] = 0$ если и только если $m \mid kn$. Полагая $m = \mu \text{нод}(m, n)$, $n = \nu \text{нод}(m, n)$, где $\text{нод}(\mu, \nu) = 1$, заключаем, что $m \mid kn$ если и только если $\mu \mid k$, откуда $k = i\mu$, где $i = 1, \dots, \text{нод}(m, n)$.

Упр. II.7. $a_1 n_1 a_2 n_2 n_1^{-1} a_1^{-1} n_2^{-1} a_2^{-1} = (a_1 n_1 a_1^{-1})(a_1 a_2 n_2 n_1^{-1} a_1^{-1} a_2^{-1})(a_2 n_2^{-1} a_2^{-1})$. Так как N нормальна, а A абелева, заключённые в скобки слагаемые лежат в N .

Упр. II.8. При эпиморфизме S_4 на группу треугольника из [прим. 10.9](#) подгруппа чётных перестановок $A_4 \subset S_4$ переходит в группу вращений треугольника.

Упр. II.9. Не вполне очевидно, разве что последнее равенство

$$(Q_k \cap P_i) \cap ((Q_{k+1} \cap P_i)P_{i+1}) = (Q_{k+1} \cap P_i)(Q_k \cap P_{i+1}).$$

Левая часть содержит правую, поскольку $Q_{k+1}Q_k \subset Q_k$ и $P_iP_{i+1} \subset P_i$. Правая часть содержит левую, так как если элемент $c \in Q_k \cap P_i$ имеет вид $c = ab$, где $a \in Q_{k+1} \cap P_i$, $b \in P_{i+1}$, то $b = a^{-1}c$ лежит в Q_k , а значит, и в $Q_k \cap P_{i+1}$.

Упр. II.10. Проверка ассоциативности:

$$\begin{aligned} ((x_1, h_1) \cdot (x_2, h_2)) \cdot (x_3, h_3) &= (x_1 \psi_{h_1}(x_2), h_1 h_2) \cdot (x_3, h_3) = (x_1 \psi_{h_1}(x_2) \psi_{h_1 h_2}(x_3), h_1 h_2 h_3) \\ (x_1, h_1) \cdot ((x_2, h_2) \cdot (x_3, h_3)) &= (x_1, h_1) \cdot (x_2 \psi_{h_2}(x_3), h_2 h_3) = (x_1 \psi_{h_1}(x_2 \psi_{h_2}(x_3)), h_1 h_2 h_3). \end{aligned}$$

Но $\psi_{h_1}(x_2 \psi_{h_2}(x_3)) = \psi_{h_1}(x_2) \psi_{h_1} \circ \psi_{h_2}(x_3) = \psi_{h_1}(x_2) \psi_{h_1 h_2}(x_3)$. Существование единицы:

$$(x, h) \cdot (e, e) = (x, \psi_h(e), he) = (x, h),$$

поскольку $\psi_h(e) = e$ в силу того, что ψ_h гомоморфизм. Существование обратного:

$$(\psi_h^{-1}(x^{-1}), h^{-1}) \cdot (x, h) = (\psi_h^{-1}(x^{-1}) \psi_h^{-1}(x^{-1}), h^{-1} h) = (e, e).$$

Упр. 11.11. Так как $\psi : H \rightarrow \text{Aut } N$ — гомоморфизм, $\psi_e = \text{Id}_N$ и

$$(x_1, e) \cdot (x_2, e) = (x_1 \psi_e(x_2), e) = (x_1 x_2, e),$$

т. е. элементы (x, e) образуют подгруппу, изоморфную N . Она нормальна, поскольку

$$(y, h) \cdot (x, e) \cdot (\psi_h^{-1}(y^{-1}), h^{-1}) = (y \psi_h(x), h) \cdot (\psi_h^{-1}(y^{-1}), h^{-1}) = (y \psi_h(x) y^{-1}, e).$$

Элементы (e, h) очевидно образуют дополнительную подгруппу, изоморфную H , и

$$\text{Ad}_{(e,h)}(x, e) = (\psi_h(x), e).$$

Упр. 11.14. Пусть центр $Z(G) = C$. Если $|C| = p$, то $C \simeq \mathbb{Z}/(p) \simeq G/C$. Пусть $a \in C$ — образующая центра, а $b \in G$ — такой элемент, что смежный класс bC является образующей в G/C . Тогда любой элемент группы имеет вид $b^k a^m$. Так как a централен, любые два таких элемента коммутируют.

Упр. 11.15. Аддитивные автоморфизмы группы $\mathbb{Z}/(p)$ суть линейные автоморфизмы одномерного векторного пространства над полем \mathbb{F}_p . Они образуют группу $\text{GL}_1(\mathbb{F}_p) \simeq \mathbb{F}_p^\times$ ненулевых элементов поля \mathbb{F}_p по умножению. Как и всякая конечная мультипликативная подгруппа поля, она циклическая¹.

¹См. сл. 2.3 на стр. 53.