§7. Группы в действии

7.1. Действие группы на множестве. Пусть G — группа, а X — множество. Обозначим через $\mathrm{Aut}\,(X)$ группу всех взаимно однозначных отображений из X в себя.

Определение 7.1
Гомоморфизм $G \xrightarrow{\varphi} \mathrm{Aut}\,(X)$ называется *действием* группы G на множестве X или *представлением* группы G автоморфизмами множества X. Если понятно, о каком действии идёт речь, результат применения отображения $\varphi(g) : X \longrightarrow X$ к точке $x \in X$ обозначается через gx.

Действие называется *точным* (или *эффективным*), если $\ker\varphi = 0$, т. е. если каждый отличный от единицы элемент группы действует на X нетождественным образом.

Действие называется *свободным*, если каждый отличный от единицы элемент группы действует на X без неподвижных точек.

Действие называется *транзитивным*, если любую точку множества X можно перевести в любую другую точку каким-нибудь преобразованием из группы G.

7.1.1. Стабилизатор. С каждой точкой $x \in X$ связана подгруппа в G, состоящая из всех преобразований, оставляющих точку x на месте. Она называется *стабилизатором* точки x в группе G и обозначается

$$\mathrm{Stab}_G(x) = \{g \in G \mid gx = x\} \tag{7-1}$$

Таким образом, действие свободно, если стабилизатор каждой точки тривиален (состоит только из единицы группы).

Более общим образом, с каждым подмножеством $F \subset X$ (или, поэтичнее, с каждой фигурой F в пространстве X) связаны две подгруппы в G:

$$\textit{нормализатор} \quad N_G(F) = \{g \in G \mid gF \subset F\} \quad \text{и} \tag{7-2}$$

$$\textit{централизатор} \quad C_G(F) = \{g \in G \mid gx = x \ \forall\, x \in F\} = \bigcap_{x\in F} \mathrm{Stab}_G(x) \tag{7-3}$$

Когда $F = \{x\}$ — одна точка, $\mathrm{Stab}(x) = N(x) = C(x)$ (тут и дальше мы опускаем в обозначениях указание на группу G, если оно не очень существенно). Иначе можно сказать, что $N(F) = \mathrm{Stab}(F)$ является стабилизатором фигуры F при действии G на множестве фигур в X, вызванным действием G на X, а $C(F) \subset N(F)$ является ядром действия группы $N(F)$ на фигуре F. В частности, $C(F)$ является нормальной подгруппой в $N(F)$.

7.1.2. Геометрический смысл нормальности. Подгруппа $H \subset G$ нормальна тогда и только тогда, когда существует гомоморфизм $\varphi : G \longrightarrow G'$ из группы G в какую-нибудь группу G', такой что $H = \ker\varphi$. В самом деле, легко проверить, что ядро любого гомоморфизма групп нормально, и наоборот, если $H \subset G$ нормальна, то в качестве G' можно взять фактор группу $G' = G/H$, а в качестве φ — эпиморфизм факторизации $G \longrightarrow\!\!\!\!\!\rightarrow G/H$, переводящий g в gH.

Если реализовать группу G' группой преобразований некоторого множества X (например, при помощи левого регулярного действия на себе, см. n° 7.2 ниже), то сказанному можно придать более наглядную форму: подгруппа $H \subset G$ нормальна тогда и только тогда, когда имеется действие группы G на некотором множестве X, такое что H — это совокупность всех преобразований из G, которые действуют на X тождественно (оставляют на месте каждую точку).

Например, собственная группа куба $\mathrm{SO}_{\text{куб}}$ действует на трёх отрезках, соединяющих центры противоположных граней куба. Ядро этого действия — диэдральная группа D_2, состоящая из тождественного преобразования и трёх поворотов на 180° вокруг проходящих через эти отрезки осей. Тем самым, $D_2 \subset \mathrm{SO}_{\text{куб}}$ нормальна, и $\mathrm{SO}_{\text{куб}}/D_2 \simeq S_3$.

Упражнение 7.1. Отождествите собственную группу куба с симметрической группой S_4 и переговорите предыдущий абзац на языке перестановок.

7.1.3. Орбиты. С действием группы G на множества X связано бинарное отношение $x \underset{G}{\sim} y$ на X, означающее, что $y = gx$ для некоторого $g \in G$. Из определений группы и действия вытекает, что это отношение является эквивалентностью: оно рефлексивно, поскольку $x = ex$, симметрично, поскольку $y = gx \iff x = g^{-1}y$, и транзитивно, поскольку из $y = gx$ и $z = hy$ вытекает, что $z = (hg)x$.

Класс эквивалентности точки $x \in X$ по отношению $\underset{G}{\sim}$ обозначается Gx и называется *орбитой* x под действием G. Он состоит из всех точек, которые можно получить из x, применяя всевозможные преобразования из группы G. Из общих свойств классов эквивалентности вытекает, что орбиты двух различных точек или не пересекаются или совпадают[1]. Множество всех орбит называется *фактором* множества X по действию группы G и обозначается X/G.

7.2. Левое регулярное действие. Обозначим через X множество элементов группы G. Отображение

$$L : G \longrightarrow \mathrm{Aut}\,(X)\,, \tag{7-4}$$

сопоставляющее элементу $g \in G$ преобразование L_g левого умножения на g:

$$L_g : X \xrightarrow{x \mapsto gx} X\,, \tag{7-5}$$

называется *левым регулярным действием* группы G на себе. Это действие свободно и транзитивно. Первое означает, что равенство $gx = x$ возможно только при $g = e$, второе — что для любых $x, y \in G$ уравнение $y = gx$ разрешимо относительно g (оба факта устанавливаются умножением обеих частей соответствующего равенства справа на x^{-1}).

Будучи свободным, левое регулярное действие точно. Тем самым, любая абстрактная группа может быть реализована как некоторая группа преобразований подходящего множества.

Обозначим через $\mathscr{E}_q$ множество q-элементных подмножеств в G и рассмотрим действие G на $\mathscr{E}_q$, вызванное левым регулярным действием G на себе. Стабилизатор произвольной точки $F \in \mathscr{E}$ состоит из всех элементов $g \in G$, левое умножение на которые переводит F в себя

$$\mathrm{Stab}(F) = \{g \in G \,|\, gF \subset F\}$$

Лемма 7.1
$|\mathrm{Stab}(F)|$ делит $|F|$, и равенство $|\mathrm{Stab}(F)| = |F|$ равносильно тому, что F является правым смежным классом подгруппы $\mathrm{Stab}(F) \subset G$.

Доказательство. $\mathrm{Stab}(F)$ свободно действует на F, и каждая орбита этого действия состоит из $|\mathrm{Stab}(F)|$ точек, т. к. $g_1 x \neq g_2 x$ при $g_1 \neq g_2$. Поскольку F является дизъюнктным объединением орбит, $|F|$ делится на $|\mathrm{Stab}(F)|$. Равенство $|\mathrm{Stab}(F)| = |F|$ означает, что все точки F составляют одну орбиту, т. е. $F = \{gx \,|\, g \in \mathrm{Stab}(F)\} = \mathrm{Stab}(F) \cdot x$ есть правый сдвиг подгруппы $\mathrm{Stab}(F)$ на элемент $x \in F$. □

Упражнение 7.2 (правое регулярное действие). Покажите, что сопоставление элементу $g \in G$ отображения $R_g : X_G \xrightarrow{x \mapsto xg^{-1}} X_G$ правого умножения на g^{-1} задаёт свободное транзитивное действие[2] группы G на себе. Сформулируйте и докажите для него аналог лем. 7.1

7.3. Присоединённое действие. Отображение

$$\mathrm{Ad} : G \longrightarrow \mathrm{Aut}\,(G)\,, \tag{7-6}$$

сопоставляющее элементу $g \in G$ автоморфизм Ad_g сопряжения элементом g

$$\mathrm{Ad}_g : G \xrightarrow{h \mapsto ghg^{-1}} G\,, \tag{7-7}$$

[1] это легко увидеть и непосредственно: если $gx = hy$ для некоторых $g, h \in G$, то $x = g^{-1}hy$ и $\forall f \in G\ fx = fg^{-1}hy \in Gy$, т. е. $Gx \subset Gy$; противоположное включение $Gx \supset Gy$ следует из равенства $y = h^{-1}gx$

[2] появление g^{-1} не случайно: проверьте, что сопоставление элементу $g \in G$ отображения правого умножения на g является не гомоморфизмом, а антигомоморфизмом (т. е. оборачивает порядок сомножителей в произведениях)

называется *присоединённым действием* группы G на себе. В отличие от левого сдвига L_g из (7-5) преобразование сопряжения Ad_g является *гомоморфизмом* из G в G.

Упражнение 7.3. Проверьте это, а также проверьте, что отображение (7-6) является гомоморфизмом.

Другое важное отличие присоединённого действия от регулярного заключается в том, что присоединённое действие может быть не свободно и не точно. Например, если группа G абелева, все внутренние автоморфизмы (7-7) исчерпываются тождественным отображением, и ядро присоединённого действия в этом случае совпадает со всей группой.

В общем случае $\ker(\mathrm{Ad})$ образовано такими $g \in G$, что $ghg^{-1} = h$ для всех $h \in G$. Последнее равенство равносильно равенству $gh = hg$ и означает, что g *коммутирует* со всеми элементами группы. Подгруппа элементов, перестановочных со всеми элементами группы G называется *центром* группы G и обозначается

$$Z(G) = \{g \in G \mid \ \forall\, h \in G \ \ gh = hg\}\,.$$

Таким образом, ядро присоединённого действия — это центр группы G.

Образ присоединённого действия называется *группой внутренних автоморфизмов* группы G и обозначается $\mathrm{Int}(G) = \mathrm{Ad}_G = \mathrm{im}\,(\mathrm{Ad}) \subset \mathrm{Aut}\,(G)$. Автоморфизмы, не попавшие в образ присоединённого действия, называются *внешними*.

Упражнение 7.4. Покажите, что подгруппа внутренних автоморфизмов нормальна в группе всех автоморфизмов.

7.4. Длины орбит. Количество точек в орбите (если оно конечно) называется её *длиной*. Все орбиты конечной группы имеют конечную длину. Чтобы связать $|Gx|$ с $|G|$ рассмотрим сюръективное *отображение вычисления*

$$\mathrm{ev}_x : G \xrightarrow{\ g \mapsto gx\ } Gx\,. \tag{7-8}$$

Слой этого отображения над точкой x представляет собою стабилизатор $\mathrm{Stab}(x)$ точки x. Слой над произвольной точкой $y = gx$ состоит из всех $h \in G$, переводящих x в y. Такие преобразования образуют левый смежный класс стабилизатора, поскольку

$$hx = gx \quad \Longleftrightarrow \quad g^{-1}h \in \mathrm{Stab}(x) \quad \Longleftrightarrow \quad h \in g \cdot \mathrm{Stab}(x)\,.$$

Таким образом, точки орбиты биективно соответствуют левым смежным классам стабилизатора произвольно выбранной точки этой орбиты. Стабилизаторы точек из одной орбиты сопряжены:

$$\mathrm{Stab}(gy) = g \cdot \mathrm{Stab}(x) \cdot g^{-1}\,.$$

Из вышесказанного вытекает простая, но очень важная

Теорема 7.1 (формула для длины орбиты)
Длина орбиты произвольной точки при действии на неё конечной группы преобразований G равна $|Gx| = |G| : |\mathrm{Stab}_G(x)|$. □

7.4.1. Пример: действие перестановок букв на словах. Зафиксируем какой-нибудь k-буквенный алфавит $A = \{a_1, a_2, \ldots, a_k\}$ и рассмотрим множество X всех n-буквенных слов w, которые можно написать с его помощью.

Иначе X можно воспринимать как множество всех отображений $w : \{1,\ 2,\ \ldots\ ,\ n\} \longrightarrow A$.

Сопоставим каждой перестановке $\sigma \in S_n$ преобразование $w \mapsto w\sigma^{-1}$, которое переставляет буквы в словах так, как предписывает[1] σ. Таким образом мы получаем действие симметрической группы S_n на множестве слов.

[1] т. е. переводит слово $w = a_{\nu_1}a_{\nu_2}\ \ldots\ a_{\nu_n}$ в слово $a_{\nu_{\sigma^{-1}(1)}}a_{\nu_{\sigma^{-1}(2)}}\ \ldots\ a_{\nu_{\sigma^{-1}(n)}}$, на i-том месте которого стоит та буква, номер которой в исходном слове w переводится перестановкой σ в номер i

Орбита слова $w \in X$ под действием этой группы состоит из всех слов, где каждая буква алфавита встречается столько же раз, сколько в слове w. Стабилизатор $\mathrm{Stab}(w)$ слова w, в котором буква a_i встречается m_i раз (для каждого $i = 1, \ldots, k$), состоит из перестановок между собою одинаковых букв и имеет порядок

$$|\mathrm{Stab}(w)| = m_1! \cdot m_2! \cdot \cdots \cdot m_k! \,.$$

Таким образом, длина орбиты такого слова равна мультиномиальному коэффициенту

$$|S_n w| = \frac{|S_n|}{|\mathrm{Stab}(w)|} = \frac{n!}{m_1! \cdot m_2! \cdot \cdots \cdot m_k!} = \binom{n}{m_1 \ldots m_k} .$$

Этот пример показывает, что разные орбиты могут иметь разную длину, и порядки стабилизаторов точек из разных орбит могут быть разными.

7.4.2. Пример: классы сопряжённости в симметрической группе. Перестановка

$$\mathrm{Ad}_g(\sigma) = g\sigma g^{-1} \,,$$

сопряжённая данной перестановке $\sigma = (\sigma_1, \sigma_2, \ldots, \sigma_n) \in S_n$, для каждого $i = 1, 2, \ldots, n$ переводит $g(i)$ в $g(\sigma_i)$. Например, при сопряжении цикла $\tau = |i_1, i_2, \ldots, i_k\rangle \in S_n$ перестановкой $g = (g_1, g_2, \ldots, g_n)$ получится цикл $|g(i_1),\, g(i_2),\, \ldots\,,\, g(i_k)\rangle$.

Предложение 7.1
Орбиты присоединённого действия симметрической группы S_n на себе взаимно однозначно соответствуют диаграммам Юнга веса n. Орбита, отвечающая диаграмме λ, состоит из всех перестановок циклового типа λ. Если диаграмма λ имеет m_1 строк длины 1, m_2 строк длины $2, \ldots, m_n$ строк длины n, то централизатор $C(\lambda)$ любой перестановки циклового типа λ состоит из $z_\lambda = 1^{m_1} \cdot m_1! \cdot 2^{m_2} \cdot m_2! \cdot \cdots \cdot n^{m_n} \cdot m_n! = \prod_{\alpha=1}^{n} m_\alpha! \alpha^{m_\alpha}$ перестановок, и длина присоединённой орбиты такой перестановки равна $n! \cdot z_\lambda^{-1}$.

Доказательство. Сопоставим произвольному заполнению диаграммы λ веса n неповторяющимися числами от 1 до n перестановку $\sigma \in S_n$ циклового типа λ, которая является произведением независимых циклов, слева направо циклически переставляющих элементы каждой строки заполнения. Действие внутреннего автоморфизма Ad_g на такую перестановку σ состоит в применении отображения g ко всем элементам заполнения, т. е. в замене каждого числа i числом g_i. Ясно, что таким образом можно получить любое заполнение диаграммы λ, т. е. присоединённая орбита состоит в точности из перестановок заданного циклового типа. Это доказывает первые два утверждения.

Вторые два утверждения следуют из того, что два заполнения диаграммы λ тогда и только тогда дают одну и ту же перестановку σ, когда они отличаются друг от друга независимыми циклическими перестановками элементов в строках и произвольными перестановками между собою строк одинаковой длины как единого целого. □

7.5. Перечисление орбит. Подсчёт числа элементов в факторе X/G конечного множества X по действию конечной группы G наталкивается на очевидную трудность: поскольку длины у орбит могут быть разные, число орбит «разного типа» придётся подсчитывать по отдельности, заодно уточняя по ходу дела, что именно имеется в виду под «типом орбиты». Разом преодолеть обе эти трудности позволяет

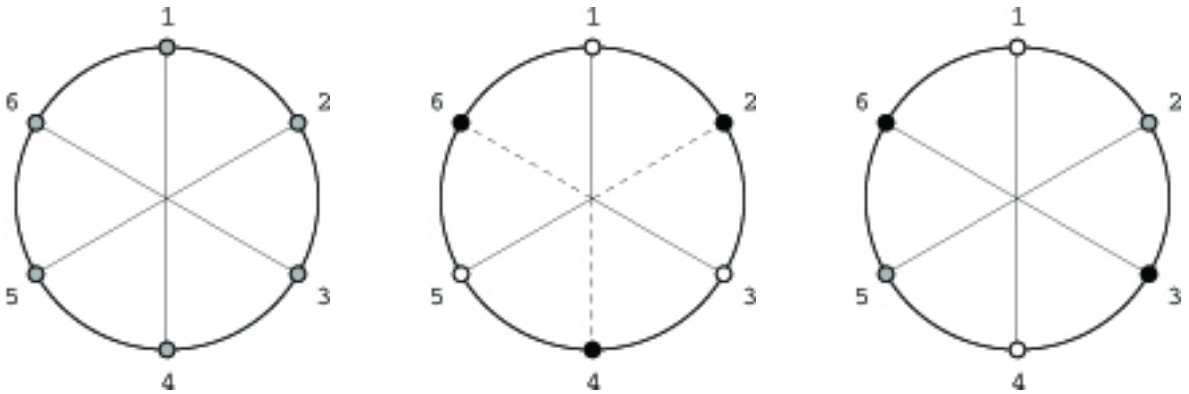
Теорема 7.2 (формула Полиа – Бернсайда)
Пусть конечная группа G действует на конечном множестве X. Для каждого $g \in G$ обозначим через $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \mathrm{Stab}(x)\}$ множество неподвижных точек преобразования g. Тогда $|X/G| = |G|^{-1} \sum\limits_{g \in G} |X^g|$.

Доказательство. Обозначим через $F \subset G \times X$ множество всех пар (g, x), таких что $gx = x$. Иначе F можно описать как $F = \sqcup_{x \in X} \operatorname{Stab}(x) = \sqcup_{g \in G} X^g$. Первое из этих описаний получается из рассмотрения проекции $F \longrightarrow X$, второе — из рассмотрения проекции $F \longrightarrow G$. Согласно второму описанию, $|F| = \sum\limits_{g \in G} |X^g|$. С другой стороны, из первого описания мы заключаем, что $|F| = |G| \cdot |X/G|$. В самом деле, стабилизаторы всех точек, принадлежащих одной орбите, имеют одинаковый порядок, и сумма этих порядков по всем точкам орбиты равна произведению порядка стабилизатора на длину орбиты, т. е. $|G|$. Складывая по всем орбитам, получаем $|F| = |G| \cdot |X/G| = \sum\limits_{g \in G} |X^g|$. □

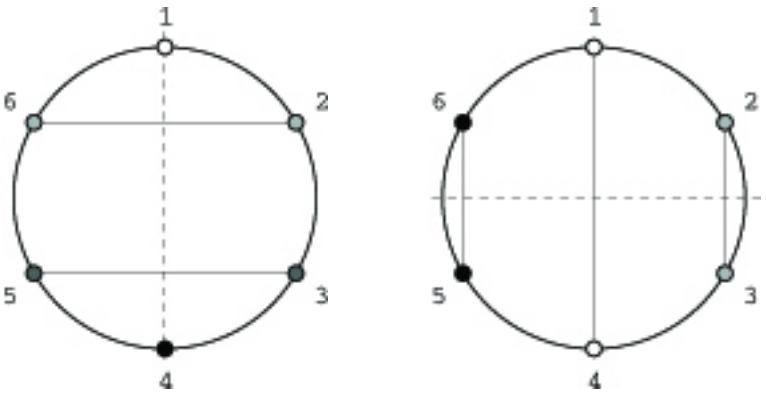
7.5.1. Пример: ожерелья. Предположим у нас имеются одинаковые по форме бусины n различных цветов (количество бусин каждого цвета неограничено). Сколько различных ожерелий одинаковой формы можно сделать из 6 бусин?

Ответом на этот вопрос является количество орбит группы диэдра D_6 на множестве всех раскрасок вершин правильного шестиугольника в n цветов.

Группа D_6 состоит из 12 элементов: тождественного преобразования e, двух поворотов $\tau^{\pm 1}$ на $\pm 60°$, двух поворотов $\tau^{\pm 2}$ на $\pm 120°$, центральной симметрии τ^3, трёх отражений σ_{14}, σ_{23}, σ_{36} относительно больших диагоналей и трёх отражений $\overline{\sigma}_{14}$, $\overline{\sigma}_{23}$, $\overline{\sigma}_{36}$ относительно срединных перпендикуляров к сторонам. Единица оставляет на месте все n^6 раскрасок. Раскраски, симметричные относительно остальных преобразований, показаны на рис. 7◇1 (одинаковым оттенкам серого отвечают одинаковые цвета).



τ-инваринтные бусы τ^2-инваринтные бусы τ^3-инваринтные бусы



σ_{14}-симметричные бусы $\overline{\sigma}_{14}$-симметричные бусы

Рис. 7◇1. Симметричные ожерелья из шести бусин.

Беря все допустимые сочетания цветов, получаем, соответственно, n, n^2, n^3, n^4 и n^3 раскрасок. По теор. 7.2 искомое число 6-бусинных ожерелий равно

$$\frac{1}{12} \cdot \left(n^6 + 3\,n^4 + 4\,n^3 + 2\,n^2 + 2\,n\right)$$

Упражнение 7.5. Подсчитайте количество ожерелий из 7, 8, 9, и 10 бусин.

7.6. Орбиты p-групп. Группа порядка p^n, где $p \in \mathbb{N}$ — простое, называется *p-группой*. Поскольку все подгруппы p-группы также являются p-группами, длина любой орбиты p-группы либо делится на p, либо равна единице. Мы получаем простое, но полезное

Предложение 7.2
Пусть p-группа G действует на конечном множестве X, число элементов в котором не делится на p. Тогда G имеет на X неподвижную точку. □

Следствие 7.1
Любая p-группа имеет нетривиальный центр.

Доказательство. Рассмотрим присоединённое действие группы на себе. Центр группы представляет собой множество неподвижных точек этого действия. Поскольку и число элементов в группе, и длины всех орбит, содержащих более одной точки, делятся на p, кроме одноточечной орбиты e должны быть и другие одноточечные орбиты. □

Упражнение 7.6. Покажите, что любая группа G порядка p^2 (где p простое) абелева.

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

Теорема 7.3 (теорема Силова)
Для любого простого p, делящего $|G|$, 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 $|G| = qm$, где $q = p^n$ и m взаимно просто с p. Обозначим через $\mathscr{E}_q$ множество q-элементных подмножеств в G и рассмотрим действие G на $\mathscr{E}_q$, индуцированное левым регулярным действием G на себе, как в лем. 7.1.

Лемма 7.2
$|\mathscr{E}_q| = \binom{p^n m}{p^n} \equiv m \pmod p$ (в частности, не делится на p).

Доказательство. $\binom{p^n m}{p^n} \pmod p$ равен коэффициенту при x^{p^n} в биноме $(1+x)^{p^n m}$, раскрытом над полем $\mathbb{F}_p = \mathbb{Z}/(p)$. Поскольку $(a+b)^p = a^p + b^p$ над $\mathbb{F}_p$, получаем

$$(1+x)^{p^n m} = \big((1+x)^p\big)^{p^{n-1}m} = (1+x^p)^{p^{n-1}m} =$$
$$= \big((1+x^p)^p\big)^{p^{n-2}m} = \big(1+x^{p^2}\big)^{p^{n-2}m} = \ldots$$
$$\cdots = \big(1+x^{p^n}\big)^m = 1 + mx^{p^n} + \text{ старшие степени}$$

что и требовалось. □

Вернёмся к доказательству теоремы Силова. Согласно лем. 7.1, порядок $|\mathrm{Stab}(F)|$ стабилизатора произвольно взятой точки $F \in \mathscr{E}_q$ является делителем $q = p^n$. Если $|\mathrm{Stab}(F)| < q$, длина орбиты точки F делится на p. Поскольку $|\mathscr{E}_q|$ не делится на p, найдётся $\mathfrak{F} \in \mathscr{E}_q$ со стабилизатором порядка $|\mathrm{Stab}(\mathfrak{F})| = q = |\mathfrak{F}|$. Таким образом, подгруппа $\mathfrak{S} = \mathrm{Stab}(\mathfrak{F}) \subset G$ — силовская.

Для доказательства остальных утверждений заметим, что длина орбиты $G\mathfrak{F}$ рана m, так что стабилизатор любой точки этой орбиты — силовская p-подгруппа. Произвольная p-подгруппа $H \subset G$, действуя на $G\mathfrak{F}$, имеет по предл. 7.2 неподвижную точку $F \in G\mathfrak{F}$ и, тем самым, содержится в силовской p-подгруппе $\mathrm{Stab}(F)$. В частности, если H сама является силовской, мы получим равенство $H = \mathrm{Stab}(F)$, т. е. любая силовская подгруппа является стабилизатором некоторой точки из орбиты $G\mathfrak{F}$. Так как стабилизаторы всех точек одной орбиты сопряжены, все силовские подгруппы сопряжены. □

Следствие 7.2 (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 $\mathscr{S}$ и рассмотрим действие G на $\mathscr{S}$, индуцированное присоединённым действием G на себе. По теореме Силова это действие транзитивно, откуда $|\mathscr{S}| = |G|/|\mathrm{Stab}(\mathfrak{S})|$, где $\mathfrak{S} \in \mathscr{S}$ — произвольно взятая силовская p-подгруппа. Поскольку $\mathfrak{S} \subset \mathrm{Stab}(\mathfrak{S})$, порядок $|\mathrm{Stab}(\mathfrak{S})|$ делится на $|\mathfrak{S}| = p^n$, а значит $|\mathscr{S}|$ делит $|G|/p^n = m$, что доказывает первое утверждение.

Для доказательства второго утверждения достаточно проверить, что $\mathfrak{S}$, действуя на $\mathscr{S}$, имеет там ровно одну неподвижную точку (а именно $\mathfrak{S} \in \mathscr{S}$) — порядки всех остальных $\mathfrak{S}$-орбит делятся на p, и мы получим $|\mathscr{S}| \equiv 1 \pmod p$.

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

7.6.2. Строение небольших групп часто удаётся полностью выяснить при помощи теоремы Силова и дополнения к ней.

Например, пусть $|G| = 15$. Тогда в G есть ровно одна силовская подгруппа $H_3 \simeq \mathbb{Z}/(3)$ порядка 3 и ровно одна силовская подгруппа $H_5 \simeq \mathbb{Z}/(5)$ порядка 5. Следовательно, обе они нормальны. Поскольку H_3 и H_5 к тому же ещё и просты $H_3 \cap H_5 = e$. Поэтому элементы ab с $a \in H_3$, $b \in H_5$ все различны. Наконец, $ab = ba$, т. к. $aba^{-1}b^{-1} \in H_5 \cap H_3 = e$. Следовательно, $G = \mathbb{Z}/(3) \times \mathbb{Z}/(5)$.

Ещё пример: опишем все группы G порядка 10. В G имеется ровно одна силовская подгруппа $H_5 \simeq \mathbb{Z}/(5)$ порядка 5, и она, тем самым, нормальна. Кроме того, в G может быть либо 1, либо 5 силовских подгрупп порядка 2, каждая из которых тривиально пересекается с H_5. Если подгруппа второго порядка одна, то мы, как и выше, получим $G \simeq \mathbb{Z}/(5) \times \mathbb{Z}/(2)$. Если двухэлементных подгрупп 5, обозначим одну из них через H_2 и посмотрим её присоединенное действие на нормальной подгруппе H_5.

Упражнение 7.7. Убедитесь, что группа $\mathrm{Aut}\,(\mathbb{Z}/(5)) \simeq \mathbb{Z}/(4)$ представляет собою циклическую группу, порождённую автоморфизмом, переводящим класс $[1] \in \mathbb{Z}/(5)$ в класс $[2] \in \mathbb{Z}/(5)$.

Присоединённое действие $H_2 \longrightarrow \mathrm{Aut}\,(H_5)$ переводит элемент $b \neq e$ из H_2 либо в тождественный эндоморфизм H_5, либо в автоморфизм второго порядка, каковой имеется ровно один — переводящий образующий элемент $a \in H_5$ в a^{-1}. В первом случае подгруппа H_2 коммутирует с подгруппой H_5, откуда $G = H_2 \times H_5 \simeq \mathbb{Z}/(5) \times \mathbb{Z}/(2)$. Во втором случае $bab^{-1} = a^{-1}$ и группа $G \simeq D_5$ — подгруппа H_5 представляет собой подгруппу поворотов, пять силовских подгрупп второго порядка порождаются пятью отражениями, сопряжёнными между собою посредством поворотов, и сопряжение любым отражением изменяет образующий поворот на обратный.

7.7. Полупрямые произведения. Рассуждение использованное в последнем примере допускает следующее обобщение. Пусть группа Q действует на группе N групповыми автоморфизмами, т. е. задан гомоморфизм групп

$$\varrho : Q \xrightarrow{g \mapsto \varrho_g} \mathrm{Aut}\,(N) \tag{7-9}$$

Тогда на множестве $N \times Q$ можно ввести групповую структуру так, чтобы $N = N \times e$ стала нормальной подгруппой, а сопряжение элементов из N элементами из $e \times Q = Q$ задавалось действием (7-9). А именно, рассмотрим множество формальных произведений ab с $a \in N$, $b \in Q$, которые по-определению считаются различными, и положим $bab^{-1} = \varrho_b(a)$ для любых $a \in N$, $b \in Q$. Это позволяет перемножать формальные произведения ab по естественному правилу

$$(a_1b_1)(a_2b_2) = a_1b_1a_2b_2 = a_1b_1a_2b_1^{-1}b_1b_2 = (a_1\varrho_{b_1}(a_2))(b_1b_2)$$

Упражнение 7.8. Убедитесь, что операция $(a_1, b_1) \cdot (a_2, b_2) \stackrel{\text{def}}{=} (a_1 \varrho_{b_1}(a_2), b_1 b_2)$ наделяет теоретико-множественное произведение $N \times Q$ структурой группы с единичным элементом (e, e). Покажите, что элементы вида (a, e) образуют в этой группе нормальную подгруппу, изоморфную N, а элементы вида (e, b) составляют (не обязательно нормальную) подгруппу, изоморфную Q.

Получающаяся таким образом группа обозначается $N \underset{\varrho}{\rtimes} Q$ и называется *полупрямым произведением* групп N и Q по действию ϱ. Если ϱ тривиален, т. е. отображает все элементы Q в тождественный автоморфизм группы N, эта конструкция даёт прямое произведение групп $N \times G$.

Упражнение 7.9. Постройте изоморфизм группы диэдра D_n с $\mathbb{Z}/(n) \underset{\varrho}{\rtimes} \mathbb{Z}/(2)$, где

$$\varrho : \mathbb{Z}/(2) \longrightarrow \mathrm{Aut}\,(\mathbb{Z}/(n))$$

переводит образующую $\mathbb{Z}/(2)$ в инволюцию $\mathbb{Z}/(n) \xrightarrow{[k] \mapsto [-k]} \mathbb{Z}/(n)$.

Предложение 7.3
Группа G тогда и только тогда является полупрямым произведением нормальной подгруппы $N \lhd G$ на некоторую подгруппу $Q \subset G$, когда $N \cap Q = e$ и $NQ = G$.

Доказательство. Последние два условия означают, что любой элемент группы G единственным образом представляется в виде ab с $a \in N$, $b \in Q$. Поскольку N нормальна, подгруппа Q действует на N сопряжениями. Обозначим это действие через ϱ. Тогда

$$(a_1 b_1)(a_2 b_2) = a_1 b_1 a_2 b_2 = a_1 b_1 a_2 b_1^{-1} b_1 b_2 = (a_1 \varrho_{b_1}(a_2))(b_1 b_2)$$

как это и происходит в полупрямом произведении $N \underset{\varrho}{\rtimes} Q$. □