Лекция 8

Определение 1. Пусть G – группа, а X – множество. *Действием* группы G на множестве X называется отображение $\alpha\colon G\times X\to X$, удовлетворяющее следующим условиям:

1) для любых $g,h\in G$ и $x\in X$ выполнено $\alpha(g,\alpha(h,x))=\alpha(gh,x)$,
2) для любого $x\in X$ выполнено $\alpha(e,x)=x$.

Если задано действие группы G на множестве X, то говорят, что G *действует* на X и обозначают $G\curvearrowright X$ (в некоторой литературе обозначают $G:X$). При этом $\alpha(g,x)$ называется действием (или применением) элемента g к элементу x, и $\alpha(g,x)$ обозначается $g\cdot x$. В таких обозначениях свойства действия из определения 1 принимают вид:

1) для любых $g,h\in G$ и $x\in X$ выполнено $g\cdot(h\cdot x)=(gh)\cdot x$,
2) для любого $x\in X$ выполнено $e\cdot x=x$.

Заметим, что при фиксированном $g\in G$ отображение $\alpha_g\colon X\to X$, $\alpha_g(x)=\alpha(g,x)$ является биекцией. В самом деле, легко убедиться, что $\alpha_g\circ\alpha_h=\alpha_{gh}$, при этом $\alpha_e=\mathrm{id}$. Это означает, что $\alpha_{g^{-1}}$ – обратное отображение к α_g. Таким образом, мы получаем гомоморфизм φ_α из G в $S(X)$. Напомним, что $S(X)$ – это группа биекций $X\to X$. Гомоморфизм φ_α определяется следующим образом: $\varphi_\alpha(g)=\alpha_g$.

Наоборот, если дан гомоморфизм $\varphi\colon G\to S(X)$, то можно определить действие α_φ группы G на X следующим образом: $g\cdot x=\varphi(g)(x)$.

Лемма 1. *Отображения $\Phi\colon\alpha\mapsto\varphi_\alpha$ и $\Psi\colon\varphi\mapsto\alpha_\varphi$ являются взаимно обратными и, следовательно, устанавливают биекцию между действиями G на X и гомоморфизмами из G в $S(X)$.*

Доказательство. Пусть β – некоторое действие G на X. Имеем $\Psi\circ\Phi(\beta)=\Psi(\varphi_\beta)$. По определению, это действие устроено по правилу $g\cdot x=\varphi_\beta(g)(x)$. С другой стороны по определению $\varphi_\beta(g)=\beta_g$, то есть $\varphi_\beta(g)(x)=\beta_g(x)=\beta(g,x)$. Таким образом $\Psi\circ\Phi(\beta)=\beta$, то есть $\Psi\circ\Phi=\mathrm{id}$.

Пусть теперь $\varphi\colon G\to S(X)$ – гомоморфизм. Тогда $\Phi\circ\Psi(\varphi)=\Phi(\alpha_\varphi)$. По определению Φ имеем $\Phi(\alpha_\varphi)(g)(x)=\alpha_\varphi(g,x)=\varphi(g)(x)$. Так как это верно для любого x и для любого g имеем $\Phi\circ\Psi(\varphi)=\varphi$, то есть $\Phi\circ\Psi=\mathrm{id}$. $\square$

Пример 1. *Пусть $X=\{1,2,\dots,n\}$. Тогда есть естественное действие симметрической группы S_n на X, заданное по формуле $\sigma\cdot i=\sigma(i)$.*

То, что это действие сводится к проверкам
1) $\sigma\cdot(\delta\cdot i)=\sigma(\delta(i))=(\sigma\circ\delta)(i)=(\sigma\circ\delta)\cdot i$,
2) $\mathrm{id}\cdot i=\mathrm{id}(i)=i$.

Пример 2. *Пусть K – поле. Тогда зададим действие $\mathrm{GL}(K)\curvearrowright K^n$ по следующей формуле. Для $A\in\mathrm{GL}(K)$ и $Y=\begin{pmatrix}y_1\\y_2\\\vdots\\y_n\end{pmatrix}\in K^n$ положим $A\cdot Y=AY$. Доказательство того, что это действие сводится к проверкам*
1) $A\cdot(B\cdot Y)=ABY=(AB)\cdot Y$,
2) $E\cdot Y=EY=Y$.

Такое действие называется тавтологическим.

Важный частный случай действий – это действия группы на себе, то есть случай, когда $X = G$. Есть три естественных действия $G \curvearrowright G$.

Пример 3. *1)* **Действие G на себе левыми сдвигами.**
По определению $g \cdot \overline{g} = g\overline{g}$.
Тогда $g_1 \cdot (g_2 \cdot \overline{g}) = g_1 g_2 \overline{g} = (g_1 g_2) \cdot \overline{g}$ и $e \cdot \overline{g} = e\overline{g} = \overline{g}$.
2) **Действие G на себе правыми сдвигами.**
По определению $g \cdot \overline{g} = \overline{g} g^{-1}$. Проверим, что это действие.

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (\overline{g} g_2^{-1}) = (\overline{g} g_2^{-1}) g_1^{-1} = \overline{g}(g_1 g_2)^{-1} = (g_1 g_2) \cdot \overline{g},$$
$$e \cdot \overline{g} = \overline{g} \cdot e = \overline{g}.$$

3) **Действие G на себе сопряжениями.**
По определению $g \cdot \overline{g} = g\overline{g}g^{-1}$. Проверим, что это действие.

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (g_2 \overline{g} g_2^{-1}) = g_1 g_2 \overline{g} g_2^{-1} g_1^{-1} = (g_1 g_2) \overline{g} (g_1 g_2)^{-1} = (g_1 g_2) \cdot \overline{g}.$$
$$e \cdot \overline{g} = e\overline{g}e^{-1} = \overline{g}.$$

Замечание 1. Заметим, что нельзя определить правое действие (действие правыми сдвигами) таким образом $g \cdot \overline{g} = \overline{g} g$, так как при этом

$$g_1 \cdot (g_2 \cdot \overline{g}) = g_1 \cdot (\overline{g} g_2) = \overline{g} g_2 g_1, \qquad (g_1 g_2) \cdot \overline{g} = \overline{g} g_1 g_2.$$

Если группа G не коммутативная, то найдутся два элемента g_1 и g_2 такие, что

$$\overline{g} g_2 g_1 \neq \overline{g} g_1 g_2.$$

Следующие два определения играют центральную роль в теории действий.

Определение 2. Пусть G действует на X и $x \in X$. Орбитой элемента x называется множество $Gx = \{g \cdot x \mid g \in G\} \subset X$.

Определение 3. Пусть G действует на X и $x \in X$. Стабилизатором элемента x называется множество $\mathrm{St}(x) = G_x = \{g \in G \mid g \cdot x = x\}$.

Лемма 2. *Орбиты – это классы эквивалентности, и следовательно, орбиты либо не пересекаются, либо совпадают.*

Доказательство. Докажем, что отношение "$x \sim y$ если x лежит в орбите Gy"является отношением эквивалентности.
1) Рефлексивность. $x \sim x$ так как $e \cdot x = x$, а значит, $x \in Gx$.
2) Симметричность. Если $x \sim y$, то найдется $g \in G$ такое, что $g \cdot y = x$. Значит, $g^{-1} \cdot x = y$, то есть $y \sim x$.
3) Транзитивность. Пусть $x \sim y$ и $y \sim z$. Тогда $x = g \cdot y$, $y = \overline{g} \cdot z$. Тогда $x = (g\overline{g}) \cdot z$. Следовательно, $x \sim z$. □

Лемма 3. *Стабилизатор $\mathrm{St}(x)$ является подгруппой в G.*

Доказательство. Пусть $g, h \in \mathrm{St}(x)$. Тогда $(gh) \cdot x = g \cdot (h \cdot x) = g \cdot x = x$, то есть $gh \in \mathrm{St}(x)$, а значит, множество $\mathrm{St}(x)$ замкнуто относительно умножения.
Если $g \in \mathrm{St}(x)$, то $g \cdot x = x$. Подействуем на обе части этого равенства элементом g^{-1}. Получим $g^{-1} \cdot (g \cdot x) = g^{-1} \cdot x$. Но $g^{-1} \cdot (g \cdot x) = e \cdot x = x$. Значит, $g^{-1} \in \mathrm{St}(x)$, то есть $\mathrm{St}(x)$ замкнут относительно взятия обратного.
Осталось заметить, что единица группы лежит в стабилизаторе любого элемента. □

Пусть G группа и H – ее подгруппа. Пусть $g \in G$. Через gHg^{-1} мы обозначаем множество $\{ghg^{-1} \mid h \in H\}$. Отображение $h \mapsto ghg^{-1}$ устанавливает изоморфизм (биекцию, переводящую умножение в умножение) между H и gHg^{-1}. Следовательно, gHg^{-1} – подгруппа, изоморфная H. Эта подгруппа называется подгруппой, сопряженной к H.

Лемма 4. *Пусть $y = g \cdot x$. Тогда $\mathrm{St}(y) = g\mathrm{St}(x)g^{-1}$. (Стабилизаторы элементов одной орбиты сопряжены.)*

Доказательство. Докажем, что $\mathrm{St}(y) \supseteq g\mathrm{St}(x)g^{-1}$. Пусть $h \in \mathrm{St}(x)$. Тогда

$$(ghg^{-1}) \cdot y = (ghg^{-1}) \cdot (g \cdot x) = g \cdot (h \cdot x) = g \cdot x = y.$$

Но аналогично, так как $x = g^{-1} \cdot y$, имеем $\mathrm{St}(x) \supseteq g^{-1}\mathrm{St}(y)g$. А значит,

$$g\mathrm{St}(x)g^{-1} \supseteq \mathrm{St}(y).$$

Так как доказаны включения в обе стороны, получаем $\mathrm{St}(y) = g\mathrm{St}(x)g^{-1}$. □

Следствие 1. *Если группа G абелева, то стабилизаторы элементов в одной орбите совпадают.*

Теорема 1. *Существует биекция между множеством левых смежных классов группы G по подгруппе $\mathrm{St}(x)$ и элементами орбиты Gx.*

Доказательство. Определим отображение ψ, которое сопоставляет смежному классу $g\mathrm{St}(x)$ элемент орбиты $g \cdot x$. Прежде всего нужно проверить корректность этого отображения, то есть что если $g\mathrm{St}(x) = h\mathrm{St}(x)$, то $g \cdot x = h \cdot x$. В самом деле $g\mathrm{St}(x) = h\mathrm{St}(x)$ тогда и только тогда, когда $h^{-1}g \in \mathrm{St}(x)$, то есть $g = hs$, где $s \in \mathrm{St}(x)$. Получаем $g \cdot x = h \cdot (s \cdot x) = h \cdot x$. Итак, ψ определено корректно.

Пусть $\psi(g\mathrm{St}(x)) = \psi(h\mathrm{St}(x))$, тогда $g \cdot x = h \cdot x$. Подействуем на последнее равенство элементом h^{-1}. Получим $(h^{-1}g) \cdot x = x$, то есть $h^{-1}g \in \mathrm{St}(x)$. Тогда $g\mathrm{St}(x) = h\mathrm{St}(x)$, то есть ψ – инъекция.

То, что ψ сюръективно следует из того, что в элемент орбиты $g \cdot x$ переходит смежный класс $g\mathrm{St}(x)$. □

Следствие 2. *Пусть G – конечная группа. Тогда $|G| = |Gx| \cdot |\mathrm{St}(x)|$.*

С помощью только что доказанной формулы посчитаем количество элементов в группе вращений куба $\mathrm{Sym}_+(K)$. Данная группа состоит из всех движений $\mathbb{R}^3$, сохраняющих ориентацию. (Так как центр куба остается неподвижен, то движение, сохраняющее куб является линейным преобразованием. Ориентацию сохраняют те движения, определитель которых равен 1.)

Предложение 1. *Порядок группы $\mathrm{Sym}_+(K)$ равен 24.*

Доказательство. Рассмотрим куб K с вершинами $ABCDA'B'C'D'$. Есть естественное действие $\mathrm{Sym}_+(K)$ на множестве $\{A, B, C, D, A'B'C'D'\}$. В группе $\mathrm{Sym}_+(K)$ содержится вращение относительно оси, соединяющей две противоположные грани. С помощью композиции таких вращений можно перевести любую вершину в любую другую. Значит, орбита точки A состоит из 8 точек. По следствию 2 получаем

$$|\mathrm{Sym}_+(K)| = |\mathrm{Sym}_+(K)A| \cdot |\mathrm{St}(A)| = 8 \cdot |\mathrm{St}(A)|.$$

Осталось найти $|H|$, где $H = \mathrm{St}(A)$. Пусть вершины, смежные с A – это B, D и A'. Получаем естественное действие H на множестве $\{B, D, A'\}$. Легко видеть, что в группе H лежат вращения относительно диагонали AC' на углы $\frac{2\pi}{3}$ и $\frac{4\pi}{3}$. Они переводят B в D и A' соответственно. Значит, действие H на $\{B, C, D\}$ имеет единственную орбиту $|HB| = 3$. При этом по следствию 2 получаем

$$|H| = |HB| \cdot |\mathrm{St}_H(B)| = 3|\mathrm{St}_H(B)|.$$

(Здесь мы используем индекс в $\mathrm{St}_H(B)$, чтобы подчеркнуть, что это стабилизатор при действии группы H, а не при действии группы G.) Осталось найти $|\mathrm{St}_H(B)|$. Пусть $\xi \in |\mathrm{St}_H(B)$. Тогда $\psi(A) = A$, $\psi(B) = B$. Поскольку смежные с A вершины – это B, D и A', получаем, что либо $\psi(D) = D$ и $\psi(A') = A'$, либо $\psi(D) = A'$ и $\psi(A') = D$. Но если $\psi(D) = A'$ и $\psi(A') = D$, то ψ меняет ориентацию. Следовательно, $\psi(A) = A$, $\psi(B) = B$, $\psi(D) = D$ и $\psi(A') = A'$. То есть ψ сохраняет 4 точки не лежащие в одной плоскости. Значит, $\psi = \mathrm{id}$. Следовательно, $|\mathrm{St}_H(B)| = 1$. Таким образом

$$|\mathrm{Sym}_+(K)| = 8 \cdot |\mathrm{St}(A)| = 24 \cdot |\mathrm{St}_H(B)| = 24.$$

□

Теперь разберемся более подробно с группой $\mathrm{Sym}_+(K)$ вращений куба.

Предложение 2. *Группа вращений куба изоморфна S_4.*

Доказательство. Группа $\mathrm{Sym}_+(K)$ действует на множестве диагоналей куба. (Очевидно, что любой элемент этой группы переводит диагонали в диагонали, то есть производит перестановку диагоналей. При этом композиция элементов дает композицию перестановок.) То есть мы имеем гомоморфизм $\varphi\colon \mathrm{Sym}_+(K) \to S_4$. Поскольку $|\mathrm{Sym}_+(K)| = |S_4| = 24$, для того, чтобы доказать, что φ – изоморфизм достаточно доказать, что φ – сюръекция. Пусть K – середина ребра AA', а L – середина ребра CC'. Рассмотрим ξ вращение на π вокруг KL. Ясно, что $\xi \in \mathrm{Sym}_+(K)$.

$$\xi(A) = A', \xi(A') = A, \xi(C) = C', \xi(C') = C, \xi(B) = D', \xi(D') = B, \xi(B') = D, \xi(D) = B'.$$

Значит, применение ξ меняет местами диагонали AC' и $A'C$ и оставляет на месте диагонали BD' и $B'D$. То есть образ ξ в S_4 – это транспозиция. Но аналогично мы можем доказать, что любая транспозиция лежит в образе φ. Поскольку S_4 порождается транспозициями, φ – сюръекция. □

Аналогично докажем другую геометрическую реализацию группы S_4. Напомним, что группа симметрий фигуры – это группа всех движений пространства (для плоской фигуры – плоскости), сохраняющих данную фигуру. (Группа симметрий не состоит только из симметрий относительно плоскостей/прямых!)

Предложение 3. *Группа симметрий правильного тетраэдра изоморфна S_4.*

Доказательство. Группа симметрий правильного тетраэдра действует на множестве его вершин (их 4). получаем гомоморфизм из этой группы в S_4. Этот гомоморфизм инъективен, так как у него тривиальное ядро. В самом деле, если некое преобразование плоскости лежит в ядре, то оно оставляет на месте вершины тетраэдра (4 точки, не лежащие в одной плоскости), а значит, это тождественное преобразование. Теперь докажем сюръективность данного гомоморфизма. Рассмотрим симметрию относительно плоскости, проходящей через ребро тетраэдра и середину противоположного ребра. Данная симметрия меняет ровно 2 вершины. Значит, в образе нашего гомоморфизма лежат транспозиции. Так как они порождают S_4, гомоморфизм сюръективен. Итак, мы построили гомоморфизм из группы симметрий правильного тетраэдра в S_4, который является биекцией, то есть изоморфизмом. □

Теперь рассмотрим действие группы G на себе сопряжениями. Орбиты и стабилизаторы при этом действии имеют отдельные названия. Орбиты называются *классами сопряженности*, а стабилизаторы – *централизаторами*. Класс сопряженности элемента $g \in G$ обозначается $C(g)$, а централизатор элемента g обозначается $Z(g)$. Следствие 2, примененное к действию G на себе сопряжениями, дает формулу $|C(g)| \cdot |Z(g)| = |G|$.

Замечание 2. Заметим, что и класс сопряженности и централизатор зависят не только от самого элемента g, но и от того, элементом какой группы он рассматривается. Путаница может произойти, например, в случае, когда в группе G есть подгруппа H. Тогда любой элемент $h \in H$ можно рассматривать как элемент G, а можно – как элемент H. Чтобы различать эти ситуации будем там, где это необходимо писать группу в качестве индекса. При этом может так случиться, что $C_G(g) \neq C_H(g)$ и $Z_G(g) \neq Z_H(g)$. Однако легко видеть, что всегда имеются включения в одну сторону: $C_H(g) \subset C_G(g)$, $Z_H(g) \subset Z_G(g)$.

Следующее утверждение следует непосредственно из определений.

Лемма 5. *Подгруппа $H \subset G$ является нормальной тогда и только тогда, когда H состоит из классов сопряженности. (Имеется в виду, что каждый класс сопряженности либо целиком содержится в H, либо целиком содержится в дополнениии к H.)*

Доказательство. Подгруппа H нормальна тогда и только тогда, когда для любых $h \in H$ и $g \in G$ выполнено $ghg^{-1} \in H$. То есть для любого $h \in H$ выполнено $C(h) \subset H$. □

Для того, чтобы описывать нормальные подгруппы (и для других целей) бывает удобно явно описать классы сопряженности в группе. Сделаем это для группы S_n. Назовем *цикловой структурой* перестановки $\sigma \in S_n$ неупорядоченный набор длин независимых циклов этой перестановки.

Лемма 6. *Пусть $\sigma \in S_n$. Тогда $C_{S_n}(\sigma)$ состоит из всех перестановок $\delta \in S_n$ с такой же цикловой структурой.*

Доказательство. Пусть разложение σ в независимые циклы имеет вид

$$\sigma = (a_1, \ldots, a_k)(b_1, \ldots, b_m) \ldots (c_1, \ldots, c_l).$$

Возьмем $\pi \in S_n$. Имеем:

$$\pi\sigma\pi^{-1} = (\pi(a_1), \ldots, \pi(a_k))(\pi(b_1), \ldots, \pi(b_m)) \ldots (\pi(c_1), \ldots, \pi(c_l)). \qquad (*)$$

В самом деле $\pi \colon \{1, 2, , \ldots, n\} \to \{1, 2, \ldots, n\}$ – биекция. А значит, любой элемент $i \in \{1, 2, \ldots, n\}$ равен $\pi(j)$. С другой стороны $\pi\sigma\pi^{-1}(\pi(j)) = \pi(\sigma(j))$. Отсюда следует приведенная выше формула $(*)$. Видно, что перестановка $\pi\sigma\pi^{-1}$ имеет ту же цикловую структуру, что и σ.

Напротив, пусть

$$\delta = (a'_1, \ldots, a'_k)(b'_1, \ldots, b'_m) \ldots (c'_1, \ldots, c'_l)$$

имеет такую же цикловую структуру, что и σ. Положим

$$\pi = \begin{pmatrix} a_1 \ldots a_k b_1 \ldots b_m \ldots c_1 \ldots c_l \\ a'_1 \ldots a'_k b'_1 \ldots b'_m \ldots c'_1 \ldots c'_l \end{pmatrix}.$$

Тогда $\pi\sigma\pi^{-1} = \delta$. □

Задача 1. Найдите все нормальные подгруппы в S_4.

Задача 2. Пусть $\sigma \in A_n$. Докажите, что $C_{S_n}(\sigma)$ либо совпадает с $C_{A_n}(\sigma)$, либо есть объединение двух равномощных классов сопряженности в A_n. А именно, $C_{S_n}(\sigma)$ совпадает с $C_{A_n}(\sigma)$, если в разложении на независимые циклы перестановки из данного класса сопряженности есть цикл четной длины или 2 цикла одинаковой нечетной длины.

Определение 4. Группа G называется p-группой, если $|G| = p^k$ для простого p и некоторого натурального k.

Теорема 2. *Центр p-группы не равен $\{e\}$.*

Доказательство. Заметим, что центр состоит из всех элементов, классы сопряженности которых состоят ровно из одного элемента. Пусть $|G| = p^k$. В пусть $g \in G$. Тогда
$$|C(g)| = \frac{|G|}{|Z(g)|} = p^m, m \in \mathbb{N} \cup \{0\}.$$
Таким образом, порядок любого смежного класса $C(g)$ либо равен 1, либо делится на p. Получаем, что $G \setminus Z(G)$ разбивается на классы сопряженности, порядок которых делится на p, а значит, $|G| - |Z(G)|$ делится на p. Отсюда $|Z(G)|$ делится на p. Следовательно, $Z(G) \neq \{e\}$. □

Следствие 3. *Группа порядка p^2 абелева.*

Доказательство. Пусть $|G| = p^2$. Тогда, так как $|G|$ делится на $|Z(G)|$, есть 3 варианта: $|Z(G)| = 1$, $|Z(G)| = p^2$ и $|Z(G)| = p$. Первый случай не возможен по предыдущей теореме. Второй соответствует абелевой группе. Осталось показать, что не может быть $|Z(G)| = p$. Допустим, что $|Z(G)| = p$, тогда $|G/Z(G)| = p$. Значит, группа $G/Z(G)$ циклическая, но мы доказывали, что такого быть не может. □

Теорема 3 (Теорема Кэли)**.** *Пусть G – конечная группа порядка n. Тогда G изоморфна некоторой подгруппе в S_n.*

Доказательство. Пусть $|G| = n$. Рассмотрим α – действие G на себе левыми сдвигами. Это действие соответствует гомоморфизму $\varphi_\alpha \colon G \to S(G) \cong S_n$. (Явно этот гомоморфизм задается по правилу: элемент g переходит в биекцию $\overline{g} \mapsto g\overline{g}$ из G в G.) При этом ядро φ_α равно $\{e\}$, так как. Значит, φ_α задает вложение G в S_n. □

Определение 5. Пусть G – конечная группа порядка $|G| = p^k m$, где p – простое число, а m – число не делящееся на p. Подгруппа $S \subset G$ называется *силовской p-подгруппой* в G, если $|S| = p^k$.

Теорема 4 (Первая теорема Силова)**.** *Для каждого простого числа p существует силовская p-подгруппа $S \subset G$.*

Доказательство. Докажем данное утверждение индукцией по $|G|$. Базой индукции будет случай, когда $|G|$ не делится на p. Тогда $S = \{e\}$.

Проведем шаг индукции.

Случай 1. $|Z(G)|$ делится на p.

$Z(G)$ – абелева группа. В ней найдется некая подгруппа A такая, что $|A| = p$. Ясно, что A – нормальная подгруппа в G. При этом $|G/A| = \frac{n}{p}$, где $n = |G|$. По предположению индукции в G/A есть силовская p-подгруппа B. Рассмотрим $\pi_A^{-1}(B) \subset G$. Имеем, $|\pi_A^{-1}(B)| = |\mathrm{Ker}\,(\pi_a \,|_{\pi_A^{-1}(B)})| \cdot |\mathrm{Im}\,(\pi_a \,|_{\pi_A^{-1}(B)})| = |A| \cdot |B| = p^k$. Можно взять $S = \pi_A^{-1}(B)$.

Случай 2. $|Z(G)|$ не делится на p.

Расмотрим разложение группы G на классы сопряженных элементов. Классы сопряженности, состоящие из одного элемента – это элементы центра. Так как $|G|$ делится на p (иначе мы в условиях базы индукции), найдется класс сопряженности C такой, что $|C| \neq 1$ не делится на p. Пусть $g \in C$. Рассмотрим $|Z(g)| = \frac{|G|}{|C|} < |G|$. С другой стороны, $|Z(g)|$ делится на p^k. По предположению индукции есть силовская подгруппа $S \subset Z(g) \subset G$, при этом $|S| = p^k$. $\square$

Лемма 7. *Если силовская подгруппа единственна, то она нормальна.*

Доказательство. Рассмотрим gSg^{-1} – это подгруппа G (проверьте это). Но $|gSg^{-1}| = |S|$. В самом деле, очевидно, что $|gSg^{-1}| \leq |S|$, с другой стороны, $S = g^{-1}(gSg^{-1})g$, значит, $S \leq |gSg^{-1}|$. Имеем, gSg^{-1} – силовская подгруппа G, а значит, $gSg^{-1} = S$, то есть S нормальна. $\square$

Теорема 5 (Вторая теорема Силова)**.** *1) Любая p-подгруппа G содержится в некоторой силовской.*

2) Любые две силовские p-подгруппы сопряжены.

Доказательство. Случай $m = 1$ ясен. Пусть $m > 1$.

1) Пусть S – силовская p-подгруппа, $|S| = p^k$. Пусть $H \subset G$ – подгруппа порядка p^l, $l \leq k$. Рассмотрим действие H на множестве левых смежных классов по S:

$$h \cdot gS = (hg)S.$$

Корректность очевидна: если $gS = g'S$, то $g' = gs$ для некоторого $s \in S$. Тогда $hg' = hgs$ и $hgS = hg'S$. Из теоремы Лагранжа количество левых смежных классов по S равно $\frac{|G|}{|S|} = m$. Имеем, $|H| = p^l = |St(gS)| \cdot |Orb(gS)|$, значит, порядок каждой орбиты либо 1, либо степень p. Так как сумма порядков орбит не делится на p, есть орбита из одного элемента. То есть $hgS = gS$. Отсюда $g^{-1}hg \in S$, то есть $h \in gSg^{-1}$. Значит, $H \subset gSg^{-1}$, где $|gSg^{-1}| = p^k$.

2) Если H – силовская подгруппа, то $|H| = p^k$. По доказанному в пункте 1) выполнено $H \subset gSg^{-1}$. Поскольку $|H| = |gSg^{-1}|$, имеем $H = gSg^{-1}$. Значит, любая силовская p-подгруппа H сопряжена фиксированной силовской p-подгруппе S. $\square$