Действие групп

prerequisite knowledge: Теория групп.

Мотивация

Применим теорию групп на реальном примере (сколько имеется различных ожерелий из n бусин, окрашенных в k цветов?) и докажем легендарную теорему о гомоморфизме.

Определение и примеры

G - группа, X - множество.

Говорят, что задано **действие G на X**, если задано отображение точка (действие):

- $\cdot : G \times X \to X$, и выполнено два условия:

1. $\forall g, h \in G : g(h \cdot x) = (gh) \cdot x$
2. $\forall x \in X : 1_G \cdot x = x$, где 1_G - нейтральный G.

Обычно знак умножения (действия) опускается.

Примеры действия групп:

1. $G = S_n$ - группа перестановок, $X = \{1, \dots, n\}$
   Действие будет таким: $\sigma \cdot i = \sigma(i),\ \sigma \in S_n,\ i \in X$.

Оно ассоциативно: $(\sigma\tau) \cdot i = \sigma\big(\tau(i)\big)$
Нейтральный: $1_{S_n} = id$, и для каджого
$i \in X: \; id \cdot i = id(i) = i$, т.е. выполняются оба свойства действия.

2. K - поле. $G = GL_n(K)$ - множество всех обратимых матриц размера $n \times n = \{g \in M_n(K) \mid \det g \neq 0\}$.
   $X = K^n$ - вектор-столбцы.
   Действие обратимой матрицы на столбец:
   $mv \mapsto m \cdot v, \; m \in G; \; v \in X$. (просто умножаем матрицу на столбец)
   Первое свойство действия следует из ассоциативности матричного умножения. Второе свойство: нейтральный G - I - единичная матрица.
   $I \cdot v = v \quad \forall v \in X$.
3. Группа симметрий куба действует на множестве вершин, или на множестве рёбер, или на множестве граней куба.
4. $G, \; X = G$. (действие на себе)
   $* : G \times X \to G$
   $g * h \mapsto ghg^{-1}$ - **сопряжение** G на себе.
   1. $(g_1 g_2) * h = g_1 g_2 h (g_1 g_2)^{-1} = g_1 g_2 h g_2^{-1} g_1^{-1}$
      $= g_1 (g_2 * h) g_1^{-1} = g1 * (g_2 * h)$.
   2. $1_G * h = 1_G h 1_G^{-1} = h$.
5. $G = GL_n(K) = \{g \in M_n(K) \mid \deg g \neq 0\}$.
   $X = M_n(K)$
   $G \times X \to X$
   $(g, m) \mapsto gmg^{-1}$
6. G - группа, $X = G$.
   $G \times G \to G$

$gx \mapsto gx$

7. $G,\ H \leq G.$
   $x = \{wH\}$ - множество левых смежных классов.
   $G \times X \to X$
   $(g, wH) \mapsto gwH.$
   А если $H = \{1\}$, по получится пример 6.

2. Орбиты и стабилизаторы

#todo картинки

G - группа, X - множество.
Задано действие $G \times X \to X,\ x \in X.$
$St_x = \{g \in G : gx = x\}$ - **стабилизатор** x - такие элементы группы, которые оставляют x на месте.
x - **неподвижная точка**.

Предложение. $St_x \leq G.$

D:

$1 \cdot x = x \implies 1 \in St_x \implies St_x \neq \varnothing.$
$g, h \in St_x.$
$(gh) \cdot x = g(h \cdot x) = g \cdot x = x \implies gh \in St_x$ (замкнутость относительно действия группы).
$g \in St_x,\ g^{-1} \in G.$
$g \cdot x = x = (g^{-1}g) \cdot x = g^{-1} \cdot x \implies g^{-1} \in St_x$ (замкнутость относительно взятия обратного).
$\implies$ по критерию подгруппы $St_x \leq G.$

Введём отношение $\sim$ на X:

$x \sim y \iff \exists g \in G : gx = y$

Предложение. Отношение выше - отношение эквивалентности.

D:

$1x = x \implies x \sim x$ - рефлексивность.
$x \sim y$.
$x = 1x = g^{-1}gx = g^{-1}(gx) = g^{-1}y$.
$g^{-1}y = x \implies y \sim x$ - симметричность.
$\exists g, h \in G : gx = y,\ hy = z$.
$(hg)x = h(gx) = hy = z \implies x \sim z$ - транзитивность.
$\implies \sim$ - отношение эквивалентности.

Каждый класс эквивалентности по отношению $\sim$, введённого выше, называется <u>**орбитой**</u>. *(один элемент может быть получен действием на другой элемент орбиты)*

Примеры орбит:

1. $x = \mathbb{R}^2$, G - группа поворотов плоскости вокруг начала координат. Орбиты - окружности с центром в начале координат. Два элемента лежат на одной орбите, если они одинаково удалены от центра.
   $x \in X$, орбита $x = \{gx : g \in G\}$

2. K - алгебраически замкнутое поле.
   $G = GL_n(K)$ - обратимые матрицы.
   $X = M_n(K)$.
   $G \times X \to X$
   $(g, m) \mapsto gmg^{-1}$
   Инвариант орбиты - ЖНФ матриц. Если две ЖНФ сопряжены, то они могут отличаться только порядком клеток.
3. $G = S_n,\ X = G, G$ действует на себе с сопряжением.
   Орбиты для этого действия - классы сопряжённости:
   $x \sim y \iff \exists y \in S_n : gxg^{-1} = y$.
   $x \sim y \iff$ цикловые типы совпадают.

Транзитивное действие

$G \times X \to X,\ A$ - орбита.
$G \times A \to A$ - **сужение действия** G на X, на $G \times A$ оно задаёт действие G на A.

У суженного на A действия одна орбита - сама A.

Действие **транзитивно**, если у него одна орбита:
$\forall x, y \in X\ \ \exists g \in G : gx = y$.

Предложение. G действует на $X,\ x \in X,\ A$ - орбита, содержащая x. Тогда имеется естественная биекция между A и множеством левых классов смежности по St_x - подгруппе G

D:

Сначала докажем, что $gx = hx \iff g^{-1}h \in St_x,\ h, g \in G$.

$\boxed{\Rightarrow}$ $gx = hx$. $x = 1x = g^{-1}gx = g^{-1}hx \implies g^{-1}h \in St_x$

$\boxed{\Leftarrow}$ $g^{-1}h \in St_x \implies g^{-1}hx = x \quad | \, g \cdot$

$gg^{-1}hx = gx \implies hx = gx$.

Теперь доказываем предложение. Фиксируем $x \in A$, а $y \in A$ - пробегаем.

$B_y = \{g \in G : gx = y\},\ g, h \in B_y \Rightarrow y = gx = hx$.

Так как $g^-1h \in St_x$, то по [построению левого класса смежности](#) $g \sim h \implies gSt_x = hSt_x$).

Докажем $B_y = gSt_x$:

$w \in St_x : \quad gwx = g(wx) = gx = y \implies gw \in B_y$

Так как $gx = hx$, то $g^{-1}h \in St_x$.

$h \in B_y : \quad (g^{-1}h)x = g^{-1}hx = g^{-1}y = x =$

$g^{-1}y = wx \implies y = gwx \implies hx = gwx \implies h = gw \in gSt_x$.

Это справедливо для всех элементов из обоих множеств, значит равенство выполняется.

Мы доказали, что отображение задано корректно - оно не зависит от выбора g :

$y = gx \implies y \in A$.

$A \to \{gSt_x\}$

$gx \mapsto gSt_x$ - биекция.

Теорема об орбитах и стабилизаторах. G действует на X, $|G| < \infty$. $x \in X,\ A$ - орбита X.

Тогда

$$|G| = |St_x| \cdot |A|$$

D:

По последнему предложению есть биекция между A и $\{gSt_x\}_{g\in G}$.
Значит, они равномощны $|A| = |\{gSt_x\}| = [G : St_x]$ - индекс A в G.
По теореме Лагранжа $|G| = |St_x| \cdot [G : St_x] = |St_x| \cdot |A|$

Пример:

G - группа самосовмещений куба. H - группа самосовмещений куба, сохраняющих ориентацию.
Две смежные вершины должны переходить в две смежные вершины. G и H действуют на множестве вершин транзитивно
1 поворотом вокруг вертикальной оси
1 поворотом на $\pi/2$. Далее аналогично.
Одна орбита длины 8 $|G| = St_1^G = 8 \quad |H| = St_1^H = 8$
Если #TODO (не записал нормально плюс щас не могу понять)

3. Лемма Бернсайда

G действует на X.
θ - множество всех орбит.
$x \in X \quad St_x = \{g \in G : gx = x\}$ - стабилизатор x.
$g \in G \quad X^g = \{x \in X : gx = x\}$ - неподвижные под действием g элементы X.

Теорема (лемма Бернсайда) $|G| < \infty$, $|X| < \infty$. Тогда

$$|\theta| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

D:

$\boxed{\sum\limits_{g \in G} |X^g|} = \sum_{g \in G} \left|\{x \in X : gx = x\}\right| = \sum_{g \in G} \sum_{x \in X : gx = x} 1 =$
$\sum_{(g,x) : gx = x} 1 = \sum_{x \in X} \sum_{g \in G : gx = x} 1 = \sum_{x \in X} |St_x| = \sum_{x \in X} \frac{|G|}{|Gx|}$
$Gx = \{gx : g \in G\}$ - орбита x.
$\sum_{x \in X} \frac{|G|}{|Gx|} = |G| \sum_{x \in X} \frac{1}{|G|} = |G| \sum_{A \in \theta} \sum_{x \in A} \frac{1}{|Gx|} =$
$|G| \sum_{A \in \theta} \sum_{x \in A} \frac{1}{|A|} = |G| \sum_{A \in \theta} 1 = \boxed{|G| \cdot |\theta|}$
$\implies |\theta| = \frac{1}{|G|} \sum_{g \in G} |X^g|$

4. Пример применения леммы Бернсайда

Сколько имеется различных ожерелий из n бусин, окрашенных в k цветов?

Для решения этой задачи построим следующую математическую модель:

Пронумеруем бусинки от 1 до n.
X - множество всех раскрасок n вершин в k цветов.
$|X| = k^n$ (каждая бусинка окрашивается независимо от других, всего вариантов $\underbrace{k \cdot k \cdot \ldots \cdot k}_{n}$)

G - группа самосовмещений правильного n-угольника.
$G = D_n$ - диэдральная группа.
$|G| = 2n$ - n поворотов и n отражений. Проверим это утверждение:

> По лемме Бернсайда:
> $\theta = \{1, \ldots, n\}$ - множество всех орбит
> $|St_i| = 2 \; \forall i \in \theta \implies \quad |G| = 2n$

> Интуитивно:
> Повороты на $2\pi l/n, \; l = 0, \ldots, n-1$
> Получили n штук поворотов.
> Отражения: если n чётно, то отражаем по противоположным сторонам и вершинам: $n/2 + n/2 = n$.
> Если n нечётно, то отражаем через вершину и противолежащую сторону - n отражений.
> Итого $2n$ действий, сохраняющих n-угольник.

D_n действует на X. Каждое ожерелье отождествляем с орбитами действия диэдральной группы на X.

Разберём наглядно для $n = 8, \; k = 4$:

g	$\|Fixg\|$	кол-во g
id	4^8	1
поворот на 45°	4	2
поворот на 135°	4	2
поворот на 90°	4^2	2
поворот на 180°	$4^4=256$	1
отражение через середины	$4^4=256$	4
отражение по противоположным вершинам	$4^5=1024$	4

$|Fixg|$ - количество ожерелий, не меняющих раскраску под действием g.
Итого число ожерелий по лемме Бернсайда:
$\sum_{g \in G} |X^g|/|G| = (4^8 + 4*2 + 4*2 + 4^2*2 + 4^4 + 4^5 + 4^6)/16 = 4435$

5. Нормальные подгруппы

G - группа, $H \leq G$ - подгруппа.
Рассмотрим множества левых и правых классов смежности: $\{xH\}$, $\{Hx\}$.
Всегда ли они совпадают?

> Для $G = S_3,\ H = \langle(1,2)\rangle$ левые не совпадают с правыми.
> $S_3 = \{id,\ (1,2),\ (1,3),\ (2,3),\ (1,2,3), (1,3,2)\}$

> $\{(2,3)\cdot H\} = \{(2,3),\ (1,3,2)\}$
> $\{H\cdot(2,3)\} = \{(2,3),\ (1,2,3)\}$

А когда они совпадают? Оказывается, есть специальный класс подгрупп - **нормальные подгруппы**. Мы определяем её как подгруппу, удовлетворяющая хотя бы одному (а значит и всем) из пяти условий теоремы:

Теорема. $H \leq G$. Следующие условия равносильны:

1. $\forall g \in G,\ \forall h \in H : gh^{-1}h \in H$.
2. $\forall g \in G : gHg^{-1} \subseteq H$.
3. $\forall g \in G : gHg^{-1} = H$.
4. $\forall g \in G : gH = Hg$.
5. Всякий левый класс смежности по H есть правый класс смежности по H.
   $H \trianglelefteq G$ - пишут так.

D:

$\underline{2}$ - переформулировка $\underline{1}$: $gHg^{-1} = \{ghg^{-1} \mid h \in H\}$.

$\underline{3} \implies \underline{2}$ очевидно.

$\underline{2} \implies \underline{3}$: $g \in G,\ gHg^{-1} \subseteq H$. Можем переписать так:
$\forall g^{-1} \in G,\ g^{-1}Hg \subseteq H$.
$H = g(g^{-1}Hg)g^{-1} \subseteq gHg^{-1} \implies H = gHg^{-1}$.
Чтобы понять последний переход, представьте, что $g^{-1}Hg = H$. Тогда $g(g^{-1}Hg)g^{-1} = gHg^{-1}$. Но у нас не равенство, а включение, значит тут тоже включение.

$\underline{2} \implies 4: gHg^{-1} = H \quad | \cdot g$
$gH = Hg$

$4 \implies 3: gH = Hg$
$gHg^{-1} = Hgg^{-1} = H$

$4 \implies 5$ очевидно. 4 условие более сильное.

$5 \implies 4: gH = Hf$
$g = g \cdot 1 \in gH$ (т.к. $1 \in H$)
$g \in Hf$ (т.к. $gH = Hf$).
$g = 1 \cdot g \in Hg$.
g лежит в двух классах смежности: Hf, Hg.
$g \in Hg \cap Hf \neq \varnothing \implies Hg = Hf$ так как классы смежности как классы эквивалентности либо не пересекаются, либо совпадают. (тут совпали)
Получили $gH = Hf = Hg$.

Примеры нормальных подгрупп:

1. $G \trianglelefteq G$
2. $\{1\} \trianglelefteq G \quad g1g^{-1} = 1$

G - **<u>простая группа</u>**, если у неё нет нормальных подгрупп, кроме G и $\{1\}$.

(продолжение примеров)

3. G абелева. Всякая её подгруппа нормальна.
   $ghg^{-1} = hgg^{-1} = h$
4. $A_n \trianglelefteq S_n$ - множество чётных перестановок - нормальная подгруппа группы перестановок.
   Если τ чётная, то $\sigma\tau\sigma^{-1}$ - чётная. (обратная к чётной - чётна, обратная к нечётной - нечётна.)
   Факт: $A_n,\ n \geq 5$ - простая.
   A_4 - не простая: $\{id, (12)(34), (1324), (14)(23)\} \trianglelefteq A_4$
5. $H \leq G,\ [G:H] = 2$ - индекс подгруппы. $H \trianglelefteq G$.
   Левых класса смежности два. Классы смежности, как классы эквивалентности, либо совпадают, либо не пересекаются. Совпадать они не могут, значит не пересекаются и разбивают изначальное множество G на два равномощных множества. (т. Лагранжа)
   Положим $g \in H$, тогда $gH = H = Hg$ и всё доказано.
   Положим $g \notin H$, тогда есть два непересекающихся левых класса: H, gH. Мощности gH и H совпадают и равны $|G|/2$. Отсюда $gH = G \setminus H$. Но два правых класса H, Hg тоже не пересекаются. Значит $Hg = G \setminus H$.
   Отсюда $Hg = gH$.

6. Нормальные подгруппы и гомоморфизмы

G, K - группы.
Вспомним определение гомоморфизма групп:
$f: G \to K$ **гомоморфизм групп**, если $\forall a, b \in G: f(ab) = f(a)f(b)$.

f - **изоморфизм**, если f гомоморфно и биективно.

Факты

1. композиция гомоморфизмов - гомоморфизм
2. композиция изоморфизм - изоморфизм
3. обратный к изоморфизму - изоморфизм
4. f - гомоморфизм. $f(1_G) = 1_K, \; f(a^{-1}) = f(a)^{-1}$

$f^{-1}(\ldots)$ - полный прообраз.
$f(\ldots)^{-1}$ - обратный.

$f^{-1}\big(\{1_K\}\big) = \{a \in G : f(a) = 1_K\} = \ker f$ - **ядро гомоморфизма** - все элементы G, которые под действием гомоморфизма отправляются в нейтральный K.

Теорема. $\ker f \trianglelefteq G$ - ядро гомоморфизма - нормальная подгруппа.

D:

Сначала докажем, что ядро - подгруппа.
$1_G \in \ker f \implies \ker f \neq \varnothing$.
$a, b \in \ker f$.
$f(ab) = f(a)f(b) = 1_K$.
$ab \in \ker f$ - замкнутость относительно операции.
$f(a^{-1}) = f(a)^{-1} = 1_K^{-1} = 1_K$.
$a^{-1} \in \ker f$ - замкнутость относительно взятия обратного.
По критерию подгруппы $\ker f \leq G$.
Теперь покажем нормальность.
$a \in \ker f, \; b \in G$.

Хотим доказать $bab^{-1} \in \ker f$.
$f(bab^{-1} = f(b)f(a)f(b^{-1}) = f(b)f(b^{-1}) = f(bb^{-1}) = f(1_G) = 1_K$.
$bab^{-1} \in \ker f \quad \forall b \in G \implies \ker f \trianglelefteq G$.

7. Факторгруппа по нормальной подгруппе

G - группа, $N \trianglelefteq G$ - нормальная подгруппа.
$\{gN\} = \{Ng\},\ g \in G$.
$G/N = \{gN \mid g \in G\}$ - множество всех левых классов по N.
Введём на G/N структуру группы.
Определим умножение двух множеств:
$A,\ B \subseteq G$.
$A \cdot B = \{ab \mid a \in A,\ b \in B\}$ - **произведение по Минковскому**.
Теперь рассмотрим произвдение двух элементов G/N:
$gN \cdot hN = \{gn_1 \cdot hn_2 \mid n_1, n_2 \in N\} =$
$(g(n_1h)n_2 \mid n_1, n_2 \in N\} = g(Nh)N \overset{N \trianglelefteq G}{=} g(hN)N = \{ghn_1n_2 \mid n_1, n_2 \in N\}$
ghN.
Получили, что произведение классов смежности - класс смежности:
$G/N \times G/N \to G/N$.

$(G/n, \cdot)$ - группа?
Предложение. Да, $(G/N, \cdot)$ - группа.

D:

$g, h, w \in G.$
$(gNhN)wN = ghNwN = ghwN$
$gN(hNwN) = gNhwN = ghwN$ - умножение по Минковскому ассоциативно.
$N = 1_G \cdot N$
$N \cdot hN = 1 \cdot hN = hN$
$1_{G/N} = N$ - нейтральный.
$gNg^{-1}N = gg^{-1}N = N = 1_{G/N}$
$g^{-1}NgN = g^{-1}gN = N = 1_{G/N}$ - обратные есть.
$\implies (G/N, \cdot)$ - группа.

Эта группа - **факторгруппа G по нормальной подгруппе N**.

Рассмотрим отображение $\varphi : G \to G/N,\ g \mapsto gN$.
$\varphi(g) = gN$.
$\varphi(g)\varphi(h) = gNhN = ghN = \varphi(gh)$.
Отображение из группы в левый класс по её нормальной подгруппе - гомоморфизм.

$\ker \varphi = \{g \in G : gN = N = 1 \cdot N\}$
$gN = 1 \cdot N$
$g \sim 1 \iff g \in N$
$\ker \varphi = \{g \mid g \in N\}$.

Обобщим полученный результат:
Множество нормальных подгрупп G - в точности множество ядер гомоморфизмов из G (в какие-то группы).
Мы ранее доказали что ядро всякого гомоморфизма в любую группу - нормальная подгруппа. Значит, множество ядер всяких гомоморфизмов - подмножество множества всех

нормальных групп.
Сейчас мы доказали, что ядра отображений во все нормальные подгруппы - нормальные подгруппы. Значит, множество всех нормальных подгрупп - подмножество ядер всяких гомоморфизмов.
Включение в обе стороны, значит равенство.

8. Теорема о гомоморфизме

Докажем легендарную теорему.
$\psi : G \to H$ - гомоморфизм групп.
$\psi(G) \leq H$ - гомоморфный образ группы. Интересно узнать, как устроена эта подгруппа.
$N = \ker \psi,\ N \trianglelefteq G$ - доказали в конце прошлого параграфа.

Теорема. $\psi : G \to H$ - гомоморфизм. $N = \ker \psi$.
Тогда $\psi(G) \cong G/N$,

$$\begin{tikzcd} G \arrow[r, "\psi"] \arrow[dr, "\varphi"'] & H \\ & G/N \arrow[u, dashed, "\theta"'] \end{tikzcd}$$

и существует изоморфизм $\theta : G/N \to H$ между G/N и $\psi(G)$ такой, что $\psi = \theta \circ \varphi$.
(гомоморфный образ группы изоморфен факторгруппе по ядру гомоморфизма)

D:

Определим и построим $\theta : G/N \to H$.

$\forall g \in G : \quad \theta(gN) = \psi(g)$.

Проверим независимость от выбора $g \in G$:

$g_1N = g_2N$. Будут ли равны $\theta(g_1N),\ \theta(g_2N)$?

$g_2^{-1}g_1N = N \implies g_2^{-1}g_1 \in N = \ker\psi$.

$\psi(g_2^{-1}g_1) = 1_H$.

$\underline{\psi(g_1)} = \psi(g_2g_2^{-1}g_1) = \psi(g_2)\psi(g_2^{-1}g_1) = \underline{\psi(g_2)}$

Проверим гомоморфность θ :

$\theta(gNhN) = \theta(ghN) = \psi(gh) = \psi(g)\psi(h) = \theta(gN)\theta(gH)$.

Проверим инъективность θ(т.е. $\ker\theta = 1_{G/N}$):

$\theta(gN) = 1_H \implies$

$\psi(g) = 1_H$.

$g \in \ker\psi = N$

$\implies gN = N = 1_{G/N} \implies \ker\theta = N$.

Из инъективности θ :

$\theta(G/N) \subseteq \psi(G)$.

Докажем обратное включение:

$\theta(gN) = \psi(g)$.

Рассмотрим $h \in \psi(G)$. Для каждого h

$\exists g \in G : h = \psi(g)$. Это равносильно $h = \theta(gN) \quad \forall h \in \psi(G)$. То есть у каджого h есть прообраз в $\theta(G/N)$. Отсюда

$\psi(G) \subseteq \theta(G/N)$.

Включение в обе стороны $\implies \psi(G) = \theta(G/N)$.

Таким образом θ - изоморфизм между G/N и $\psi(G)$.

(неточность т.к. мы строили отображение в H, а не $\psi(G)$, но мы их отождествим.)

$\forall g \in G : (\theta \circ \varphi)(g) = \theta(gN) = \psi(g)$.

Пример:

1. $\mathbb{R}, +$
   $(\mathbb{Z}, +),\ \mathbb{Z} \trianglelefteq \mathbb{R}.$
   $\mathbb{R}/\mathbb{Z}$ - дробные части.
   $S = \big(\{z \in \mathbb{C} : |z| = 1\},\ \ \cdot\ \big)$
   $\mathbb{R}/\mathbb{Z} \cong S$
   Строим гомоморфизм $\varphi : \mathbb{R} \to S$.
   $\ker \varphi = \mathbb{Z}$.
   $S = \varphi(\mathbb{R}) \cong \mathbb{R}/\mathbb{Z}$ по т. о гомоморфизме.
   $\varphi(x) = \cos 2\pi x + i \sin 2\pi x = e^{2\pi i x}$.
   $\varphi(x+y) = \varphi(x)\varphi(y)$ (при перемножении комплексных чисел аргументы складываются).
   φ - гомоморфизм.
   $1 = \varphi(x) \iff \begin{cases} cos 2\pi x = 1 \\ \sin 2\pi x = 0 \end{cases} \quad x \in \mathbb{Z},\ \ \ker\varphi = \mathbb{Z}.$

9. Действие группы на множестве и гомоморфизмы

Как связано действие группы и гомоморфизмы? Оказывается, что всякое действие задаёт гомоморфизм, и наоборот.

G - группа, X - множество. Задано действие на $G \times X \to X$.
Зафиксируем $g \in G$.
Придумаем отображение $\varphi_g : X \to X$, которое бы сопостовляло элементу из X его образ под действием элемента g:

$\varphi_g(x) = g \cdot x$.
По свойству действия:
$\varphi_{gh}(x) = gh \cdot x = g\varphi_h(x) = \varphi_g\big(\varphi_h(x)\big) \implies$
$\varphi_{gh} = \varphi_g \circ \varphi_h$.
$\varphi_1 = id_x$ - по свойству действия нейтрального. Комбинируем два свойства:
$\varphi_g \circ \varphi_{g^{-1}} = \varphi_1 = id_x$
$\varphi_{g^{-1}} \circ \varphi_g = \varphi_1 = id_x$
φ_g и $\varphi_{g^{-1}}$ - пара взаимно обратных отображений. В частности, φ_g - биекция на X.

Действие G на X задало биекции на X.

Теперь рассмотрим $S(X)$ - множество всех биекций на X.
$(S(x), \circ)$ - симметрическая группа.
Зададим на G отображение $\Phi : G \to S(x),\ g \mapsto \varphi_g$.
$\Phi(g) = \varphi_g$
$\Phi(gh) = \varphi_{gh} = \Phi(g) \circ \Phi(h)$
Φ - гомоморфизм групп G и $S(x)$.
Получили, что всякое действие задаёт гомоморфизм $\Phi : G \to S(x)$.

Покажем, что верно и обратное.
$\Phi : G \to S(x)$. Зададим действие на $G \times X \to X : gx = \Phi(g)(x)$.
Проверим аксиомы действия:

1. $(gh)x = \Phi(gx)(x) = \big(\Phi(g) \circ \Phi(h)\big)(x) = \Phi(g)\big(\Phi(h)(x)\big) = g(hx)$.
2. $1_G \cdot x = \Phi(1_G)x = id_x(x) = x$.

Итого, действие группы на множестве и гомоморфизм в биекции на множестве - одно и тоже.

Точное действие

G действует на X. Действие называется **точным**, если
$\forall x \in X \;\; gx = x \implies g = 1_G$.
По доказанному выше факту, действие точно, если
$\Phi(g) = 1_{S(x)} \implies g = 1_G \iff \ker \Phi = \{1_G\}$.
Если $\ker \Phi = \{1\}$, то по теореме о гомоморфизме
$\Phi(G) \cong G/\ker \Phi = G/\{1\} = G$. (группа изоморфна своему гомоморфному образу)

Теорема (Кэли). Всякая конечная группа изоморфна некой подгруппе перестановок.

D:

Зададим действие на себе: $G \times G \to G,\; |G| = n$.
$(g, h) \mapsto gh$ (действие на себе умножением слева)
Это действие точно: $\forall h \in G \; gh = h \implies g = 1$.
Рассмотрим $\Phi : G \to S(X)$. Так как действие точно, то
$\ker \Phi = \{1\} \implies G \cong \Phi(G)$. (каждому элементу сопоставляем какую-то перестановку)
Занумеруем элементы G.
$G = \{g_1, \dots, g_n\}$, $S(G) \cong S_n$.
$\sigma(g_i) = g_{\sigma(i)}$
$G \xrightarrow{\Phi} S(G) \cong S_n$.

Пример:

Теорема Кэли даёт изоморфное вложение S_m в $S_{m!}$.

10. Центр группы. Центр p -группы.

G - группа.
$Z(G) = \{x \in G : \forall g \in G \; gx = xg\}$ - **центр группы**. (множество элементов, коммутирующих со всеми элементами группы)
$1 \in Z(G)$.

Лемма. $Z(G) \trianglelefteq G$.

D:

$1 \in Z(G) \neq \varnothing$.
Рассмотрим $x, y \in Z(G)$.
$xyg = xgy = gxy \implies xy \in Z(G)$.
$x^{-1} \cdot \mid \quad xg = gx \quad \mid \cdot x^{-1}$
$gx^{-1} = x^{-1}g \implies x^{-1} \in Z(G)$.
По критерию подгруппы $Z(G) \leq G$.
$x \in Z(G), \; g \in G$.
$gxg^{-1} = xgg^{-1} = x \in Z(G) \implies Z(G) \trianglelefteq G$.

Группа абелева, если она совпадает со своим центром.

Примеры:

1. $n \geq 3, \; Z(S_n) = \{1\}$.

2. $G = GL_n(K) = \{g \in M_n(K) : \det g \neq 0\}$.
   $Z(G) = \{\lambda I : \lambda \in K^*\}$

p-группа

p - простое число.
G - p-группа, если её порядок $= p^n$.

Примеры:

1. $|D_4| = 8 = 2^3$ - 2-группа.
2. $i, j, k \quad i^2 = j^2 = k^2 = -1$
   $ij = k,\ ji = -k,\ ki = j,\ ij = -j, jk = i,\ kj = -i$
   $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ - группа из 8 элементов - 2 -группа.
3. p - простое. $G = \left\{ \begin{pmatrix} 1 & * & * \\ 0 & 1 & * \\ 0 & 0 & 1 \end{pmatrix} \in M_n(\mathbb{Z}/p\mathbb{Z}) \right\}$. $|G| = p^3$.

Теорема. G - p-группа. $|Z(G)| > 1$.

D:

G действует на себе с сопряжением.
Орбиты - классы сопряжённости:
$\{gxg^{-1} \mid g \in G\}$
Z_x - стабилизатор x в этом действии.
$Z_x = \{g : gxg^{-1} = x\} = \{g \in G : gx = xg\}$
$Z_x = G \iff x \in Z(G) \iff$ класс сопряжённости x одноэлементен.

Если $x \notin Z(G)$, то мощность его класса сопряжённости делится на p.
$|\{gxg^{-1}\}| = |G|/|Z_x|$ - теорема об орбитах и стабилизаторах.
$|G| = p^n$.
$\{Z_x\}$ - подгруппа $G \implies$ по т. Лагранжа делит $|G| \implies |Z_x| = p^k$.
Так как x не из центра, то $k < n \implies |\{gxg^{-1}\}| = p^{n-k}$ делится на p.
G - объединение классов сопряжённости

$$|G| = \sum_{x \in Z(G)} 1 + \sum_{x \notin Z(G)} \text{порядки неодноэлементных классов сопр.}$$

Порядок G делится на p, сумма справа делится на p.
Отсюда количество элементов в центре делится на $p \implies |Z(G)| \geq p > 1$.

Конец алгебры.