Часть 1. Действия групп

Определение 1.1. Действие группы G на множестве X — это отображение $a : G \times X \to X$, такое что

$$(i) \quad \forall g,h \in G,\ x \in X \quad a(g, a(h,x)) = a(gh, x); \qquad (ii) \quad \forall x \in X \quad a(e,x) = x.$$

Для упрощения обозначений действие группы G на множестве X часто записывается как $(g,x) \mapsto gx$.

Примеры 1.2. 1. Тривиальное действие: $(g,x) \mapsto x$.

2. Действие групп μ_n, μ, $\mathbf{S}^1$, $\mathbb{R}^+$, $\mathbb{C}^*$ на $\mathbb{C}$ умножением.
3. Действие группы перестановок $\mathfrak{S}_n$ на множестве $\{1, \ldots, n\}$.
4. Действие группы $\mathrm{Aut}(X)$ на X, где X — любая алгебраическая структура.
5. Пусть G — группа. Легко видеть, что отображение $G \times G \to G$, $\quad (g,x) \mapsto g \circ x$ — это действие группы G на себе. Оно называется действием левыми сдвигами.
6. Пусть G — группа, а $H \subset G$ — подгруппа. Тогда отображение $G \times G/H \to G/H$, $\quad (g, xH) \mapsto gxH$ — это действие группы G на множестве левых классов смежности G по H.
7. Пусть G — группа. Легко видеть, что отображение $G \times G \to G$, $\quad (g,x) \mapsto gxg^{-1}$ — это действие группы G на себе. Оно называется действием сопряжениями.
8. Пусть $(g,x) \mapsto gx$ — действие группы G на множестве X, а $f : H \to G$ — гомоморфизм групп. Тогда $(h,x) \mapsto f(h)x$ — действие группы H на X.
9. Пусть $(g,x) \mapsto gx$ — действие группы G на множестве X, а $Y \subset X$ — подмножество, такое что $GY \subset Y$. Тогда $(g,y) \mapsto gy$ является действием группы G на Y.
10. Пусть $(g,x) \mapsto gx$ и $(g,y) \mapsto gy$ — действия группы G на множествах X и Y. Тогда возникают действия группы G на множествах $X \times Y$, $(g,x,y) \mapsto (gx, gy)$, и $\mathrm{Map}(Y,X)$, $(g,f) \mapsto f^g$, где $f^g(y) := gf(g^{-1}y)$.
11. Пусть $(g,x) \mapsto gx$ — действие группы G на множестве X. Тогда возникает действие группы G на множестве всех подмножеств множества X: $(g,Y) \mapsto gY$, где $Y \subset X$.

Лемма 1.3. *Действия группы G на множестве X находятся в биекции с гомоморфизмами $G \to \mathrm{Aut}(X)$.*

Доказательство: пусть $a : G \times X \to X$ — действие G на X. Всякому элементу $g \in G$ сопоставим отображение $a_g : X \to X$, $x \mapsto a(g,x)$. Легко видеть, что $a_{gh}(x) = a(gh,x) = a(g, a(h,x)) = a_g(a_h(x)) = (a_g \circ a_h)(x)$, и $a_e(x) = a(e,x) = x = \mathrm{Id}_X(x)$, следовательно отображение $a : G \to \mathrm{Map}(X,X)$, $g \mapsto a_g$ является гомоморфизмом моноидов. Следовательно, $\forall g \in G$ $a(g) \in \mathrm{Aut}(X)$ и $a : G \to \mathrm{Aut}(X)$ — гомоморфизм групп. Обратно, если $a : G \to \mathrm{Aut}(X)$, $g \mapsto a_g$ — гомоморфизм групп, то $(g,x) \mapsto a_g(x)$ — действие группы G на X. $\square$

Замечание 1.4. В примере 1.2.7 отображения $S_g : G \to G$, $x \mapsto gxg^{-1}$, являются не только автоморфизмами G как множества, но и как группы (то есть согласованы с групповым законом и переводят e в e). Таким образом возникает гомоморфизм $S : G \to \mathrm{Aut}(G)$ из группы G в группу ее автоморфизмов. Автоморфизмы S_g называются внутренними автоморфизмами группы G. Легко видеть, что они образуют подгруппу в группе $\mathrm{Aut}(G)$; она обозначается $\mathrm{Inn}(G)$. Можно показать, что $\mathrm{Inn}(G) \triangleleft \mathrm{Aut}(G)$. Соответствующая факторгруппа $\mathrm{Out}(G) = \mathrm{Aut}(G)/\mathrm{Inn}(G)$ называется группой внешних автоморфизмов группы G.

Замечание 1.5. В примере 1.2.5 сдвиги $T_g : G \to G$, $x \mapsto gx$ не являются автоморфизмами группы G.

Действия групп еще называют левыми действиями. Кроме того, можно также рассматривать правые действия, то есть отображения $a' : X \times G \to X$, такие что $a'(a'(x,g),h) = a'(x,gh)$ и $a'(x,e) = x$ для любых $g,h \in G$ и $x \in X$. Примером правого действия является действие группы на себе правыми сдвигами.

Если группа G коммутативна, то всякое левое действие G является правым, и наоборот. В общем же случае это неверно. Однако, левое действие превращается в правое при обращении элемента группы.

Лемма 1.6. *Если $a : G \times X \to X$ — левое действие, то $a'(x,g) := a(g^{-1},x)$ — правое действие. Аналогично, если $a' : X \times G \to X$ — правое действие, то $a(g,x) := a'(x,g^{-1})$ — левое действие.*

Доказательство: $a'(a'(x,g),h) = a(h^{-1}, a(g^{-1},x)) = a(h^{-1}g^{-1},x) = a((gh)^{-1},x) = a'(x,gh)$ и так далее. $\square$

Часть 2. Орбиты и стабилизаторы

Пусть группа G действует на множестве X и $x \in X$. Множество $Gx = \{\, gx \mid g \in G \,\} \subset X$ называется орбитой точки x относительно действия группы G. Множество $G_x = \{\, g \in G \mid gx = x \,\} \subset G$ очевидно является подгруппой. Подгруппа G_x называется стабилизатором (стационарной подгруппой) точки x.

Пример 2.1. Пусть X — множество всех подмножеств множества $\{\,1,\dots,n\,\}$. При действии группы $\mathfrak{S}_n$ на множестве X всякая орбита имеет вид $X \supset X_k = \{$ все k-элементные подмножества в $\{\,1,\dots,n\,\}\,\}$. Стабилизатор точки $\{\,i_1,\dots,i_k\,\} \in X_k \subset X$ — это все перестановки $\sigma \in \mathfrak{S}_n$, такие что $\sigma(\{\,i_1,\dots,i_k\,\}) = \{\,i_1,\dots,i_k\,\}$.

Лемма 2.2. *Любые две орбиты либо не пересекаются, либо совпадают.*

Доказательство: предположим, что $Gx \cap Gy \neq \emptyset$. Пусть $z \in Gx \cap Gy$. Тогда $z = gx$ для некоторого $g \in G$, следовательно $x = g^{-1}z$ и, значит, $Gx = Gg^{-1}z = Gz$. Аналогично $Gy = Gz$. Значит $Gy = Gx$. $\square$

Замечание 2.3. Легко видеть, что отношение $x \sim y \iff \exists g \in G\ y = gx$ является отношением эквивалентности на множестве X. Действительно, рефлексивность отношения $\sim$ следует из наличия единицы в группе, симметричность — из существования обратного элемента, а транзитивность — из «ассоциативности» действия. Кроме того, ясно, что классы эквивалентности — это орбиты действия группы.

Если на множестве X задано действие группы G, то говорят, что X — G-множество. Морфизмом G-множеств $X \to Y$ (G-морфизмом, G-эквивариантным отображением) называется отображение $f : X \to Y$, которое коммутирует с действием группы, то есть $\forall g \in G,\ x \in X\ f(gx) = gf(x)$.

Лемма 2.4. *Пусть группа G действует на множестве X и $x \in X$ — произвольная точка. Тогда G-множества Gx и G/G_x канонически изоморфны.*

Доказательство: легко видеть, что отображение $G/G_x \to Gx$, $gG_x \mapsto gG_x x = gx$, корректно определено. Кроме того, оно очевидно является морфизмом G-множеств. Далее, оно сюръективно по определению орбиты, так что остается проверить его инъективность. Предположим, что gG_x и $g'G_x$ переходят в одну и ту же точку орбиты Gx. Тогда $gx = g'x$, следовательно $(g^{-1}g')x = g^{-1}(g'x) = g^{-1}(gx) = (g^{-1}g)x = ex = x$, значит $g^{-1}g' \in G_x$, следовательно $gG_x = g(g^{-1}g'G_x) = g'G_x$. $\square$

Следствие 2.5. *Длина орбиты Gx равна $(G : G_x)$.*

Лемма 2.6. *Если $y \in Gx$, то подгруппы G_y и G_x сопряжены.*

Доказательство: если $y = gx$, то ясно, что $G_y = gG_xg^{-1}$. $\square$

Следствие 2.7. *Индексы сопряженных подгрупп равны.*

Следствие 2.8. *Пусть группа G действует на конечном множестве X. Пусть $x_1,\dots,x_k$ — представители орбит. Тогда $|X| = \sum_{i=1}^{k}(G : G_{x_i})$.*

Важным примером действия является действие группы на себе сопряжениями. Элементы группы, лежащие в одной орбите этого действия называются сопряженными. Иначе говоря, $x, y \in G$ сопряжены $\iff \exists g \in G$ так что $x = gyg^{-1}$. Сами орбиты называются классами сопряженности. Легко видеть, что стабилизатором элемента $x \in G$ является его централизатор. Следствие 2.8 в данном случае дает формулу классов:

$$(G:1) = \sum_x (G : Z_x) \qquad \text{(сумма по представителям классов сопряженности)} \tag{2.9}$$

Дадим, наконец, еще несколько определений. Действие группы называется транзитивным, если все множество X состоит из одной орбиты. Действие группы называется свободным, если стабилизатор любой точки тривиален. Действие группы называется точным, если пересечение всех стабилизаторов (т.е. ядро соответствующего гомоморфизма $G \to \operatorname{Aut}(X)$) тривиально.

Часть 3. Группа перестановок

Пусть $i_1, \dots, i_k$ — попарно различные элементы множества $\{ 1, \dots, n \}$. Перестановка, переводящая $i_1 \mapsto i_2 \mapsto i_3 \mapsto \dots \mapsto i_k \mapsto i_1$ и оставляющая все остальные элементы множества $\{ 1, \dots, n \}$ на месте, называется **циклом** длины n и обозначается $(i_1 i_2 \dots i_k)$. Заметим, что $(i_1 i_2 i_3 \dots i_{k-1} i_k) = (i_2 i_3 \dots i_{k-1} i_k i_1)$. Циклы $(i_1 i_2 \dots i_k)$ и $(j_1 j_2 \dots j_l)$ называются **независимыми**, если $\{ i_1, \dots, i_k \} \cap \{ j_1, \dots, j_l \} = \emptyset$.

Лемма 3.1. *Независимые циклы коммутируют. Любая перестановка раскладывается в произведение попарно независимых циклов. Такое разложение единственно с точностью до перестановки сомножителей и отбрасывания циклов длины 1.*

Доказательство: первая часть очевидна. Докажем теперь вторую. Пусть $\sigma \in \mathfrak{S}_n$. Рассмотрим действие подгруппы $\mathbb{Z}/m\mathbb{Z} \cong \langle\sigma\rangle \subset \mathfrak{S}_n$ на множестве $\{ 1 \dots, n \}$. Пусть $\{ i_1^1, \dots, i_1^s \}$ — представители всех орбит. Для всякого $1 \leqslant t \leqslant s$ положим $i_p^t = \sigma(i_{p-1}^t)$ и пусть k_t — длина орбиты точки i_1^t. Тогда $\langle\sigma\rangle i_1^t \cong \mathbb{Z}/k_t\mathbb{Z}$, поэтому все точки i_p^t при $1 \leqslant p \leqslant k_t$ попарно различны, а $i_{k_t+1}^t = i_1^t$. Более того, легко видеть, что σ раскладывается в произведение циклов $(i_1^1 \dots i_{k_1}^1) \cdot \dots \cdot (i_1^s \dots i_{k_s}^s)$ причем циклы — попарно независимы.

Остается доказать единственность такого разложения. Действительно, пусть $\sigma = (j_1^1 \dots j_{l_1}^1) \cdot \dots \cdot (j_1^r \dots i_{l_r}^r)$ другое разложение. Добавляя циклы длины 1, мы можем считать, что среди чисел j_p^q содержатся все элементы множества $\{ 1, \dots, n \}$. Тогда ясно, что орбиты действия группы $\langle\sigma\rangle$ — это в точности подмножества $\{ j_1^1 \dots j_{l_1}^1 \}, \dots, \{ j_1^r \dots i_{l_r}^r \}$. Поэтому $r = s$ и, переставляя циклы и меняя в них первый элемент, мы можем считать, что $j_1^t = i_1^t$ при всех $1 \leqslant t \leqslant s$. Но тогда ясно, что $l_t = k_t$ и $j_p^t = i_p^t$ при всех p. □

Пусть $\sigma = (i_1^1 \dots i_{k_1}^1) \cdot \dots \cdot (i_1^s \dots i_{k_s}^s)$ — разложение перестановки σ в произведение независимых циклов. Ясно, что добавляя циклы длины 1 и переставляя сомножители, можно считать, что $k_1 \geqslant k_2 \dots \geqslant k_s$ и $k_1 + \dots + k_s = n$. Другими словами $(k_1, \dots, k_s)$ — разбиение числа n. Из леммы 3.1 следует, что такое разбиение однозначно определяется перестановкой σ.

Теорема 3.2. *Перестановки σ и σ' — сопряжены, тогда и только тогда когда соответствующие им разбиения числа n совпадают.*

Доказательство: пусть $\sigma = (i_1^1 \dots i_{k_1}^1) \cdot \dots \cdot (i_1^s \dots i_{k_s}^s)$, $k_1 \geqslant \dots \geqslant k_s$ и $k_1 + \dots + k_s = n$. Предположим, что $\sigma' = g\sigma g^{-1}$. Тогда ясно, что $\sigma' = (g(i_1^1) \dots g(i_{k_1}^1)) \cdot \dots \cdot (g(i_1^s) \dots g(i_{k_s}^s))$, значит разбиение, соответствующее σ' совпадает с $(k_1, \dots, k_s)$. Обратно, предположим, что $\sigma' = (j_1^1 \dots j_{k_1}^1) \cdot \dots \cdot (j_1^s \dots j_{k_s}^s)$. Определим перестановку g правилом $g(i_p^t) = j_p^t$. Тогда ясно, что $\sigma' = g\sigma g^{-1}$. □

Цикл длины 2 называется **транспозицией**.

Лемма 3.3. *Любая перестановка раскладывается в произведение транспозиций.*

Доказательство: заметим, что $(i_1 i_2 i_3 \dots i_{k-1} i_k) = (i_1 i_2) \cdot (i_2 i_3) \cdot \dots \cdot (i_{k-1} i_k)$ и применим лемму 3.1. □

Лемма 3.4. *Пусть $\sigma = \tau_1 \cdot \dots \cdot \tau_N$ — разложение перестановки σ в произведение транспозиций. Тогда четность числа N не зависит от выбора разложения.*

Доказательство: определим число беспорядков перестановки σ как $\text{ЧБ}(\sigma) = |\{ (i,j) \mid i < j \text{ и } \sigma(i) > \sigma(j) \}|$. Достаточно проверить, что $N \equiv \text{ЧБ}(\sigma) \bmod 2$. Пусть σ — любая перестановка σ, а $\tau = (ij)$, $i < j$. Тогда,

$$\text{если } \sigma(i) < \sigma(j), \text{ то } \text{ЧБ}(\sigma \cdot \tau) = \text{ЧБ}(\sigma) + 2|\{ k \mid i < k < j \text{ и } \sigma(i) < \sigma(k) < \sigma(j) \}| + 1;$$
$$\text{если } \sigma(i) > \sigma(j), \text{ то } \text{ЧБ}(\sigma \cdot \tau) = \text{ЧБ}(\sigma) - 2|\{ k \mid i < k < j \text{ и } \sigma(i) < \sigma(k) < \sigma(j) \}| - 1;$$

так что в любом случае $\text{ЧБ}(\sigma \cdot \tau) \equiv \text{ЧБ}(\sigma) + 1 \bmod 2$, и остается применить индукцию по N. □

Перестановка называется **четной**, если она представляется в виде произведения четного числа транспозиций, и **нечетной** в противном случае. Из леммы 3.4 немедленно следует

Теорема 3.5. *Отображение $\varepsilon : \mathfrak{S}_n \to \mu_2 = \{ \pm 1 \}$, переводящее четные перестановки в 1, а нечетные в -1, является гомоморфизмом групп.*

Число $\varepsilon(\sigma) \in \{ \pm 1 \}$ называется **знаком** перестановки σ. Группа четных перестановок $\mathrm{A}_n = \operatorname{Ker} \varepsilon \subset \mathfrak{S}_n$ называется **знакопеременной** группой. Заметим, что $\mathrm{A}_n \triangleleft \mathfrak{S}_n$, $\mathfrak{S}_n/\mathrm{A}_n \cong \mu_2$.