Алгебра

1 курс, 2 модуль

Фейгин Евгений Борисович

Содержание

1 Группы (29.10.19)

Определение. Группа — это множество G с одной операцией, удовлетворяющей следующим свойствам:

(1) (ab)c = a(bc);

(2) $\exists e \in G : \forall a \in G ea = ae = a$;

(3) $\forall a \in G\ \exists a^{-1} \in G : aa^{-1} = a^{-1}a = e$.

Примеры:
- $\mathbb{R}_+$ — вещественные числа по сложению;
- $\mathbb{R}_+^+$ — вещественные положительные числа по сложению;
- $\mathbb{Z}/_{n\mathbb{Z}}$ — вычеты по модулю n по сложению;
- $\mathbb{F}^* = \mathbb{F}\backslash 0$ — группа обратных элементов поля.

Определение. Абелева (коммутативная) группа: $\forall a, b \in G\ ab = ba$.

Пусть X — множество. Обозначим через S(x) множество всевозможных взаимно-однозначных отображений $X \to X$ с операцией композиции.

Пример. X — конечное множество из n элементов. S(X) обозначим через S_n, n = |X|. Например, X может быть $\{1, ..., n\}$.

Пример. Пусть V — векторное пространство над полем $\mathbb{F}$. Рассмотрим все преобразования V вида $t_a : V \to V,\ t_a(V) = V + a, a \in V$. Тогда $t_a t_b : V \to V,\ t_a t_b(V) = V + a + b = t_a + b$. Таким образом, V образует группу по сложению.

Определение. Подмножество $H \subset G$ называется подгруппой (и также является группой), если

(1) $e \in H$;

(2) $a, b \in H \Rightarrow ab \in H$;

(3) $a \in H \Rightarrow a^{-1} \in H$.

Определение. Гомоморфизм групп: отображение $\varphi : G_1 \to G_2$, где G_1, G_2 — группы, т.ч. $\varphi(g_1, g_2) = \varphi(g_1)\varphi(g_2),\ \varphi(a^{-1}) = \varphi(a)^{-1}$.

Гомоморфизм φ называется изоморфизмом, если φ взаимно-однозначно. Автоморфизм — изоморфизм $\varphi : G \to G$.

Пример. Группа G называется циклической, если $\exists g \in G : \forall g_1 \in G \exists k \in \mathbb{Z} : g_1 = g^k$.

Лемма. Любая циклическая группа изоморфна $\mathbb{Z}/_{n\mathbb{Z}},\ n \geq 1$ или $\mathbb{Z}$ относительно сложения.

Доказательство. Если существует минимальное n т.ч. $g^n = e$ (g — образующая циклической группы), то $G \mapsto \mathbb{Z}/_{n\mathbb{Z}}$ строится по формуле $g^k \mapsto [k], e \mapsto [0]$. Если существует k т.ч. $g^k = e$, то $G = g^k,\ k \in \mathbb{Z},\ g^k \neq g^l$, если $k \neq l$. Тогда G изоморфно $\mathbb{Z},\ g^k \mapsto k$.

Определение. Множество элементов $S = \{g_1, g_2, ..., g_n\}$ называется образующими группы G ($g_i \in G$), если минимальная подгруппа $H \subset G$, содержащая все g_i, совпадает с G. Другими словами, $\forall g \in G, g = g_{i_1}^{\epsilon_1} g_{i_2}^{\epsilon_2} ... g_{i_m}^{\epsilon_m}$, где $\epsilon_k = \pm 1,\ i = 1, ..., k,\ m \geq 0$.

Пример. $g_1 g_1 g_1 g_1$, то есть в записи выше g_{i_k} необязательно различны.

Замечание. Если k = 1, то G циклическая.

Пример. Группа S_3 не является циклической, но порождена двумя элементами. S = (12), (23).

Лирическое отступление. $S_n = S(\{1,...,n\}), (ij) \in S_n, (ij)$ — транспозиция. $i_1 \mapsto i_2, ..., i_k \mapsto i_1, j \mapsto j, j \notin \{i_1, ..., i_k\}$.

Предложение. Группа S_n имеет несколько наборов образующих: $(12), (23), ..., ((n-1)k); (12), (13), ...$

Пример. Свободная группа с двумя образующими g_1, g_2 — группа, состоящая из элементов $g_{i_1}^{\epsilon_1} g_{i_2}^{\epsilon_2} ... g_{i_m}^{\epsilon_m}$, i = 1, 2, $\epsilon = \pm 1, m \geq 0$. Все такие элементы разные с точностью до сокращения $g_1 g_1^{-1} = e, g_2 g_2^{-1} = e, g_1 g_2 \neq g_2 g_1$.

Пример. $S_3 : g_1 = (12), g_2 = (23), g_1 g_2 g_1 = g_2 g_1 g_2$ — соотношение кос, $g_1^2 = e$.

1.1 Ортогональные преобразования плоскости

Определение. Группа O(2) — группа линейных преобразований $\mathbb{R}^{\not{2}}$, сохраняющая расстояние. Любое линейное преобразование $\mathbb{R}^2$ задается матрицей $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ т.ч. $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}$

$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in O(2) \Leftrightarrow (ax + by)^2 + (cx + dy)^2 = x^2 + y^2.$

$a^2 + c^2 = 1, b^2 + d^2 = 1, ab + cd = 0 \Rightarrow a = \cos\alpha, c = \sin\alpha \Rightarrow \left[\begin{array}{l} b = \sin\alpha, d = -\cos\alpha; \\ b = -\sin\alpha, d = \cos\alpha. \end{array}\right.$

$\begin{pmatrix} \cos\alpha & \sin\alpha \\ \sin\alpha & -\cos\alpha \end{pmatrix} \to \det = -1, \begin{pmatrix} \cos\alpha & -\sin\alpha \\ \sin\alpha & \cos\alpha \end{pmatrix} \to \det = 1$

Замечание. Иногда O(2) обозначается $I_{SO}(\mathbb{R}^2)$.

Замечание. Имеется O(3), O(4), ...

Определение. Пусть $x \subset \mathbb{R}^2$. Тогда $I_{SO}(x) = \{g \in O(2) : gx = x\}$.

Утверждение. $I_{SO}(x)$ — подгруппа в O(2).

Доказательство. $l \in I_{SO}(x)$ $(l = \pm d), g_1, g_2 \in I_{SO}(x) \Leftrightarrow g_1 g_2, g_1^{-1} \in I_{SO}(x)$.

Пример. X — правильный n-угольник. $I_{SO}(x) = D_n$ — группа диэдра (группа (конечная) симметрии правильного многоульника, включающая вращения и осевые симметрии, — мое примечание).

1.2 Смежные классы

Обозначается $g \in G$, ord g = min{k: $g^k = 1\} \in \mathbb{Z}_{\geq 0} \cup \infty$.

Пусть H — подгруппа в G. Тогда любое множество вида gH = gh: $h \in H$ называется **правым смежным классом.** Hg = hg: $h \in H$ — **левый смежный класс.**

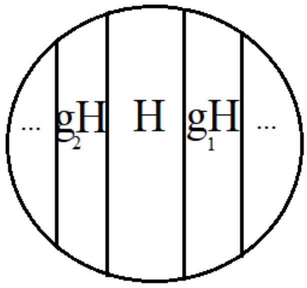
Свойства: • $|gH| = |Hg| = |H|$, так как $gh_1 = gh_2 \Rightarrow h_1 = h_2$;

• H является как левым, так и правым смежным классом;

- 2 левых/правых смежных класса либо совпадают, либо не пересекаются.

Доказательство. $g_1H = g_2H \neq \emptyset \Leftrightarrow \exists h_1, h_2 : g_1h_1 = g_2h_2 \Leftrightarrow g_1h_1h_2^{-1} = g_2 \Leftrightarrow g_1H = g_2H$.

Следствие — теорема Лагранжа. $|H|||G| \Leftrightarrow |G| \vdots |H|$ — порядок группы делится на порядок подгруппы.



Следствие. Пусть H = <g> — подгруппа, порожденная $g \in G$. Тогда если $|G| < \infty, |H| < \infty$, то $|G| \vdots \mathrm{ord}\ \mathrm{g}$.

Следствие. Любые две группы из $p \in \mathbb{P}$ элементов изоморфны.

Доказательство. $\forall g \in G \ \mathrm{ord}\ \mathrm{g} = \begin{cases} 1 \to \mathrm{ord}\ \mathrm{g} = 1 \Leftrightarrow g = l, \\ p \to \forall g \neq l \ \mathrm{ord}\ \mathrm{g} = \mathrm{p} \Rightarrow G \text{ — циклическая.} \end{cases}$

Следствие. Количество правых (левых) смежных классов равно $|G|_{/|H|}$.

Определение. Подгруппа $H \subset G$ называется **нормальной**, если множества правых и левых смежных классов совпадают, то есть $\forall g \in G gH = Hg$.

Замечание. Определение равносильно $gHg^{-1} = H \ \forall g \in G$.

Замечание. $gH = Hg \Leftrightarrow h_1 \in H \ \exists h_2 \in H$ т.ч. $gh_1 = h_2g$.

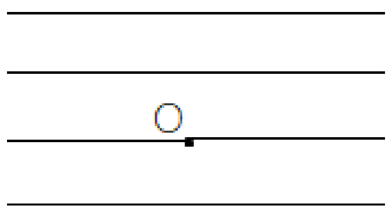
Определение. $\varphi : G_1 \to G_2$ — гомоморфизм групп $\ker\varphi = \{g \in G_1 =: \varphi(g) = e\}$, $\mathrm{Im}\varphi = \{g_2 \in G_2 : \exists g_1 \in G_1 : \varphi(g_1) = g_2\}$.

Лемма. $\ker\varphi$ — нормальная подгруппа в G_1.

Доказательство. • $\ker\varphi$ — подгруппа, так как $e \in \ker\varphi(\varphi(e) = e); g_1g' \in \ker\varphi \Leftrightarrow \varphi(gg') = \varphi(g)\varphi(g') = ee = e$.

- Пусть $x \in G_1$, $g \in \ker\varphi$. Тогда $\varphi(xgx^{-1}) = \varphi(x)\varphi(g)\varphi(x^1) = \varphi(x)\varphi(x)^{-1} = e$. Т.о., $xgx^{-1} \in \ker\varphi$, то есть $\ker\varphi$ нормально.

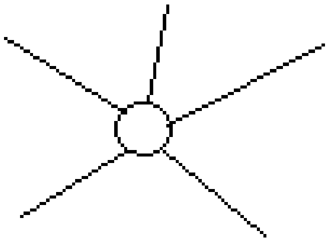
Замечание. Пусть H — нормальная подгруппа, $g \in G$. $gHg^{-1} \subset H$, то есть элемент $g \in G$ задает отображение $adg : H \to H, (adg)(h) = ghg^{-1}$. Что означает, что $(adg)h_1 = (adg)h_2 \Leftrightarrow gh_1g^{-1} \Leftrightarrow h_1 = h_2$. То есть если H конечна, то достаточно требовать, что $gHg^{-1} \subset H$.

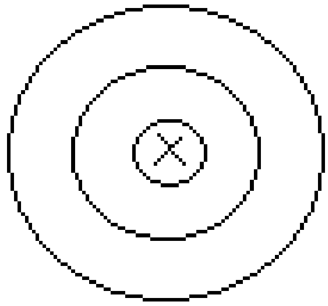


Примеры. • $G = \mathbb{Z}$, $H = h\mathbb{Z}$ (относительно сложения). Смежные классы: $\{a + kn,\ k \in \mathbb{Z}\} = [a]$.

Замечание. Если G — это коммутативная группа, то любая ее подгруппа нормальна ($gHg^1 = gg^{-1}H = H$).

- $G = (\mathbb{C}, +), H = (\mathbb{R}, +) = \{z : Imz = 0\}$, смежные классы: (картинка справа)
- $G = (\mathbb{C}\backslash\{0\}; \times); H = (\mathbb{R}_{>0}, \times)$, смежные классы: (картинка справа)





• $G = (\mathbb{C}\backslash\{0\}, \times), H = S^1 = \{z : |z| = 1\}$, смежные классы: (картинка справа)

• $G = S_n, h = S_{n-1} = \{\sigma \in S_n : \ \sigma(n) = n\}$. Хотим описать левые смежные классы. $\sigma \in S_n,\ H\sigma = \{g \in S_n : g^{-1}(n)\sigma^{-1}(n)\}$. Пусть $g = h\sigma : g^1(n) = (h\sigma)^{-1}(n) = (\sigma^{-1}h^{-1})(n) = \sigma^{-1}(n)$. Пусть $ginS_n, g^{-1}(n) = \sigma^{-1}(n)$. Тогда мы хотим проверить, что g = hG для некоторого $h \in H$, то есть $g\sigma^{-1} \in H \Leftrightarrow (g\sigma^{-1})(n) = n \Leftrightarrow \sigma^{-1}(n) = g^{-1}(n)$.

Правые смежные: $\sigma H = \{\sigma h : h(n) = n\} = \{g \in S_n : g(n) = \sigma(n)\}$.

Вывод. $S_{n-1} \subset S_n$ — ненормальная подгруппа.

Замечание. $\psi : \ G \to G,\ \psi(g) = g^{-1}$ — антиавтоморфизм (умножение не переводится в умножение: $\psi(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = \psi(g_2)\psi(g_1)$. $H \in G, \psi(GH) = H\sigma^{-1}$. То есть ψ осуществляет биекцию между правыми и левыми смежными классами.

$H \subset G, g_1H \cdot g_2H = g_1g_2H \ \Leftrightarrow\ [g_1][g_2] = [g_1g_2],\ [g] = gH$ — смежный класс g.

Предложение. Формула $g_1Hg_2H = g_1g_2H$ определяет корректно заданное умножение на множестве смежных классов $\Leftrightarrow$ H нормальна в G.

Доказательство. Пусть группа нормальна. Хотим проверить, что если $f_1 \in [g_1], f_2 \in [g_2]$, то $[f_1f_2] = [g_1g_2]$. $f_1 = g_1h_1,\ f_2 = g_2h_2 \Leftrightarrow f_1f_2 = g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2(\in H))h_2 = g_1g_2h$(с крышечкой), где h (с волной) $= g_2^{-1}h_1g_2)h_2 \in H \Rightarrow [f_1f_2] = [g_1g_2]$, то есть умножение корректно определено.

Тогда на множестве смежных классов [G:H] возникает структура группы:

$e = [e] = H, [g]^{-1} = [g^{-1}], [g_1(g_2g_3)] = [g_1][g_2g_3] = [g_1]([g_1][g_2])[g_3]$, где $[g_1(g_2g_3)] = [(g_1g_2)g_3] = [g_1g_2][g_3] = ([g_1][g_2])[g_3]$.

$\tau : G \to G_H$ — фактор группа, G фактор по H, $\tau(g) = [g]$ — отображение факторизации, где через G_H обозначается группа, элементами которой являются смежные классы. Тогда τ — гомоморфизм групп, то есть $\tau(g_1g_2) = \tau(g_1)\tau(g_2) \Leftrightarrow [g_1g_2 = [g_1][g_2]].ker\tau = \{g \in G : g \in H\}$.

Таким образом, если на G:H есть структура группы $[g_1][g_2] = [g_1g_2]$, то H $= \ker(\tau : G \to G_H)$, то есть H — нормальна.

Вывод. Фактор группа бывает только по нормальной подгруппе.

Замечание. $H \subset G$ нормальна $\Leftrightarrow \exists$ гомоморфизм $\varphi : G \to G_1$, т.ч. $\ker\varphi = H$.

Доказательство. Если $\varphi :\ G \to G_1$ гомоморфизм, то $\ker\varphi$ нормальна — проверили. Если

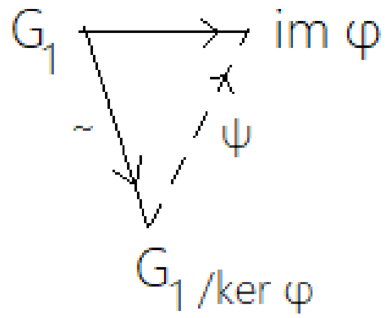
H нормально, то $G \to G_{\backslash H}$ — искомый гомоморфизм.

Пример. $G = (\mathbb{C}, +),\ H = (\mathbb{R}, +),\ G_{\backslash H} \simeq (\mathbb{R}, +), [z] \mapsto \mathrm{Imz}$.

$G = (\mathbb{C}\backslash\{0\}, \times), H = S^1 = \tau : |z| = 1,\ G_{\backslash H} \simeq (\mathbb{R}_+, \times), [z] \mapsto |z|$.

Конструкция. $\varphi : G_1 \to G_2, \mathrm{Im}\varphi \subset G_2$, где $\mathrm{Im}\varphi$ — подгруппа. Имеется отображение факторизации $\tau : G_1 \to G_{1_{\backslash \ker \varphi}},\ g \ \mapsto [g]$.

Лемма. Существует гомоморфизм $\psi : G_{1_{\backslash \ker \varphi}} \to \mathrm{Im}\ \varphi$, т.ч. $\varphi = \psi \cdot \iota$. При этом ψ является изоморфизмом.



2 Гомоморфизм групп

$\varphi :\ G_1 \to G_2$, $\ker\ \varphi = \{g \in G_1 :\ \varphi(g) = e\}$, $\mathrm{Im}\ \varphi = \{h \in G_2 : \exists g \in G_1, \varphi(g) = h\}$.

$\ker\ \varphi$ — нормальная подгруппа, $G\backslash_{ker\varphi}$ — факторгруппа.

$\ker\ \varphi = \varphi^{-1}(e)$. Как устроен прообраз неединичного элемента (слой над произвольным элементом)?

Пусть $h \in G_2,\ g_1\widetilde{g} \in G_1$ т.ч. $\varphi(g) = \varphi(\widetilde{g}) = h$.

$\varphi(g) = \varphi(\widetilde{g}) \Leftrightarrow \varphi(g)\varphi(\widetilde{g})^{-1} = e \Leftrightarrow \varphi(g)\varphi(\widetilde{g}^{-1}) = e \Leftrightarrow \varphi(\widetilde{g}^{-1}) = e \Leftrightarrow gg^{-1} \in ker\varphi$.

$gg^{-1} \in \ker\ \varphi\ \Leftrightarrow g \in (\ker\ \varphi\widetilde{g}$.

Лемма. Все слои гомоморфизма φ могут быть отождествлены с $\ker\ \varphi$ (слой над $e \in G_2$.

Доказательство. Зафиксируем слой как прообраз $h \in G_2$. Зафиксируем $g \in \varphi^{-1}(h)$. Тогда любой другой элемент в слое над h имеет вид $(\ker\ \varphi) \cdot g$.

Следствие. Если $|G_1|,\ |G_2| < \infty$, то все слои содержат одинаковое количество элементов.

Предложение. Любой гомоморфизм $phi : G_1 \to G_2$ может быть разложен в композицию $G_1 \to G_{1_{\backslash ker\varphi}} \to G_2$, где $p : G_1 \to G_{1_{\backslash ker\varphi}},\ g \mapsto [g],\ i : G_{1\backslash ker\varphi} \to G_2,\ [g] \mapsto \varphi(g)$.

Доказательство. i корректно определно, т.к. если $[g_1] = [g_2]$, то $g_1 = g_2h,\ h \in ker\varphi \Rightarrow \varphi(g_1) = \varphi(g_2h) = \varphi(g_2)$. Заметим, что $(ip)(g) = \varphi(g)$ по определению. Осталось проверить, что i — вложение, т.е. $\ker\ i = e$ (или, равносильно, $i(x) = i(y) \Rightarrow x = y$). Действительно, $i([g]) = e \Leftrightarrow \varphi(g) = e \Rightarrow e \in ker\varphi$ — один класс в фактор-группе.

Причем этот класс является единственным элементом в $G_{1\backslash ker\varphi}$.

Замечание. Пусть $|G_1|, |G_2| < \infty$. тогда $|im(\varphi)| = |G_1|_{\backslash |ker\varphi|}$.

Группа преобразований — действия групп на множествах.

Определение. X — множество, Aut(X) — группа всех взаимно-однозначных отображений $X \to X$ с операцией композиции.

Замечание. Если X конечно, то $Aut(X) \simeq S_n$, где $n = |x|$.

Пример. $X = \mathbb{N}, Aut(\mathbb{N}) = \{f : \mathbb{N} \to \mathbb{N} -$ взаимно-однозначные отображения$\}$.

Определения. Любая подгруппа группы Aut(X) называется группой преобразований.

Замечание. Абстрактная группа называется группой преобразований, если ее можно вложить в $Aut(X)$.

Пример. Группа диэдра — линейные преобразования $\mathbb{R}^2$, которые сохраняют правильный многоугольник. В качестве X можно взять сам многоугольник (или множество его вершин).

Пример. Группа преобразований куба.

Бывают собственные и несобственные преобразования.

Пусть $SO_{\text{куб}}$ — собственные преобразования, которые сохраняют куб.

$x \mapsto -x$ — несобственное.

Пусть X — множество, состоящее из четырех диагоналей куба. Если φ — преобразование куба, то φ индуцирует элемент $Aut(X)$.

Утверждение. Мы получаем отображение из группы преобразований куба в $\mathrm{Aut(X)} = S_4$. При это любой элемент S_4 лежит в образе этого отображения. При этом отображение $x \to -x$ (центральная симметрия) индуцирует тождественное преобразование X.

Пусть $G \in Aut(X)$ — группа преобразований.

Пример. Пусть $\sigma \in S_n$ — перестановка. Скажем, что $1 \leq i < j \leq n$ образуют инверсию (беспорядок), если $\sigma(i) > \sigma(j)$. Например, $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}; 13, 12, 23$ — инверсии. Определим значение σ на (-1). σ называется четным, если ее знак 1, иначе нечетным.

• [не расшифровала доску];

• преобразование $\delta \to \{\pm 1\}, \delta \mapsto sgn(\delta)$ — гомоморфизм групп;

• четность перестановки совпадают с четностью количества транспозиций в различных перестановках на транспозиции;

• четные перестановки образуют группу, которая называется **знакопеременная группа** и обозначается A_n. $|A_n| = \dfrac{n!}{2}$, т.к. $S_n = A_n \bigsqcup (12)A_n$.

В частности, A_n — группа преобразований $X = 1, 2, ..., n$.

2.1 Орбита, стабилизатор

Определение. Орбита $x \in X$ под действием g — множество $\{g.x\}$ $g \in G$. Обозначается Gx.

Пример. $G = AutX,\ x \in X, Gx = X,\ G = id$, то $Gx = \{x\}$.

Замечание. Разные орбиты не пересекаются.

Доказательство. Пусть $x, y \in X,\ y \in Gx$. Тогда $\exists g \in G:\ y = g.x \Rightarrow g^{-1}y \Rightarrow Gx = Gy$.

Определение. Стабилизатор точки $x \in X$ — подмножество $Stab_G x \subset G$, состоящее из $g:\ gx = g$.

Замечание. $Stab_G x$ — подгруппа в G, т.к. $(g_1 g_2).x = g_1.(g_2.x)$.

Как связаны стабилизаторы у двух разных точек в одной орбите?

$Stab_G gx = \{g \in G : h.(g.x) = g.x\} = \{h \in G : (hg).x = g.x\} = \{g \in G : g^{-1}.(hg).x = g^{-1}(g.x)\} = \{h \in G : (g^{-1}hg).x = x\} = \{h \in G : g^{-1}hg \in Stab_G x\} = \{h \in G :\ h \in gStab_G(x)g^{-1}\}$.

Следствие. Если G — конечная группа, то стабилизаторы всех точек в одной орбите равномощны.

Доказательство. $a, b \in Stab_G x,\ a \neq b \Rightarrow gag^{-1} \neq gbg^{-1}$.

Следствие. $|G| = |Gx||Stab_G x|$.

Доказательство. $ev_x : G \to X$. Тогда $|ev^{-1}(gx)| = |Stab_G gx| = |Stab_G x|$. (т.к. $kergx \subset G$ отображением ev_x переходит в $gx \in G$). $g \to g.x$.

Следствие. $|G| \vdots |Gx|, |G| \vdots |Stab_G x|$.

X — множество, G — группа, $\mathrm{Aut}(X)$ — взаимно-однозначные отображения $X \to X$.

G — группа преобразований, если G может быть реализована как подгруппа Aut(X). $\varphi : G \to \mathrm{Aut}(X)$, т.ч. φ — гомоморфизм, $\ker \varphi = \{\mathrm{id}\}$.

Определение. $x \in X$, орбита $Gx = \{y \in X : \ \exists g \in G \quad g.x = y\} \quad (gx = g.x = \varphi(g)x)$. Стабилизатор $x \in X$ — подгруппа $Stab_G x = \{g \in G : \ gx = x\}$.

Предложение. Пусть $|G| < \infty$. $|Gx| = |G|_{/|Stab_G x|}$. $ev_x : G \to X,\ g \mapsto gx$.

Определение. G — группа, X — множество. G действует на X, если задан гомоморфизм групп $\varphi : G \to Aut(X)$. Другими словами, имеется отображение $G \times X \to X,\ (g_1 x) \mapsto \varphi(g)x$.

Замечание. Отображение φ может иметь ядро, т.е. могут существовать $g \in \varphi$, т.ч. $\varphi(g) = id,\ g + e$.

Определение. Орбита: $\{y : \exists g \in G \quad gx = y\}$, стабилизатор $Stab_G x = \{g \in G : gx = x\}$.

Замечание. $\varphi : G \to Aut(X)$ — действие, то $\mathrm{Im}\varphi$ — группа преобразований X.

Замечание. Любые две орбиты либо совпадают, либо не пересекаются.

Теорема. Если конечная группа G действует на X, то $|Gx| = |G|_{/|Stab_G x|}$.

Доказательство. Рассмотрим $ev_x : G \to G_x,\ g \mapsto \varphi(g)x$. Тогда легко проверить, что $\forall y \in G_x$. $|ev_x^{-1}(y)| = |Stab_G x| \ni |G| = |G_x||Stab_G x|$.

Замечание. $G \xrightarrow{\varphi} Im\varphi,\ g \mapsto \varphi(g)$. У этого гомоморфизма есть ядро $\ker\varphi$. Пусть $a \in Im\varphi$. Тогда $|\varphi^{-1}(a)| = |ker\varphi|$, т.к. $\varphi(g_1) = \varphi(g_2) = a \Rightarrow \varphi(g_1 g_2^{-1}) = id \Leftrightarrow g_1 g_2^{-1} \in ker\varphi \Leftrightarrow g_1 = \dfrac{ker\varphi}{g_2}$.

$Gx = (Im\varphi)x,\ |G| = |Im\varphi||ker\varphi|, \quad |stab_G x| = |Stab_{Im\varphi} x| \cdot |ker\varphi|$.

2.2 Транзитивность, точность, свободность

Определение. Действие $\varphi : G \to Aut(X)$ называется транзитивным, если $\forall x, y \in X\ \exists g \in G$, т.ч. $gx = y$.

Замечание. У транзитивного действия ровно одна орбита. **Обозначение:** $X_{/G}$ — множество орбит в X при действии G.

Определение. Действие называется **свободным,** если из равенства $gx = x \quad (g \in G,\ x \in X) \Rightarrow g = e$. Т.е. нет неединичных элементов, которые оставляют точку на месте. Иными словами, $Stab_g x = e\ \forall x \in X$.

Определение. Действие называется **точным,** если $\ker\varphi = $ e.

Замечание. Если действие **свободно,** то оно точно. Т.е. ни один элемент группы, кроме единичного, не переходит в тождественное преобразование. В обратную сторону неверно.

Пример. Левое действие группы на себя. $X = G,\ L : G \to Aut(X),\ L(g)x = gx$.

Транзитивно. Берем $x \in G,\ y \in G$. Существует ли $g \in G:\ L(g)x = y \Leftrightarrow gx = y \Rightarrow g = yx^{-1}$? Существует.

Точно. Верно ли, что L — это вложение? ker L $= \{g \in G : L|g| = id\} = \{g \in G:\ gx\ x\ \forall x \in G\}$.

Свободно. $gx = x \Leftrightarrow g = e$.

Пример. Правое действие группы на себя. $x = G,\ R : G \to AutX,\ R(g)x = xg^{-1} \leftarrow$ гомоморфизм. Проверим. $R(g_1g_2) = R(g_1)R(g_2) \Leftrightarrow \forall x:\ R(g_1g_2)x = x(g_1g_2)^{-1} = R(g_1)(R(g_2)x) = xg_2^{-1}g_1^{-1}$.

Пример. Присоединенное действие. Ad: $G \to Aut(X),\ X = G$. $Ad(g)x = gxg^{-1}$.

Не транзитивно. Если G коммутативна, то Ad(g)x = x, т.е. Im Ad = {id}. Возьмем орбиту единичного элемента: $G_e = e$, т.е. e сдвинуть нельзя.

Не точно. Если G коммутативно, то kerφ = G. Вообще говоря, ker $\varphi = \{g \in G:\ gxg^{-1} = x\ \forall x\} = \{g \in G : gx = xg\ \forall x \in G\} = Z(G)$ — центральная группа.

Не свободно.

Пример. $G = S_n$. Хотим описать орбиты присоединенного действия. Пусть σ — перестановка, тогда $(Adg)\sigma = g\sigma g^{-1}$.

Лемма. σ и τ лежат в одной орбите относительно присоединенного действия, если $\forall k = 1, 2, ..., n$ количество циклов длины k в разложении σ и τ на непересекающиеся циклы одинаковое.

Доказательство. $(i_1i_2...i_k)$ — цикл, $g(i_1...i_k)g^{-1} = (g(i_1)...g(i_k))$.

Вопрос. $\sigma \in S_n$, чему равна длина Ad-орбиты элемента σ?

Предложение. $|Stab_{S_n}\sigma| = m_1!m_2!...m_n!1^{m_1}2^{m_2}...n^{m_n} = \Pi_{k=1}^{n}k^{m_k}m_k!$

Пусть σ разложена на непересекающиеся циклы и m_k — количество циклов длины k в этом разложении. В частности, $m_1 + 2m_2 + ... + nm_n = n$.

Доказательство. Мы знаем, что $g(i_1i_2...i_k)g^{-1} = (g(i_1)...g(i_k))$. Поэтому если $g\sigma g^{-1} = \sigma$, то для того, чтобы задать g, нужно задать следующие данные:

• для каждого цикла $(i_1...i_k)$ нужно указать цикл длины k в σ, куда начальный цикл перейдет;

• для каждого цикла $(i_1...i_k)$ нужно задать образ $f(i_1)$ в соответствующем (выбранном) цикле длины k.

Следствие. Орбита перестановок σ относительно присоединенного действия содержит $\dfrac{n!}{\Pi_{k=1}^{n}m_k!k^{m_k}}$ элементов.

Замечание. Орбиты присоединенного действия называются классами сопряженных элементов.

2.3 Диаграммы Юнга

Диаграммы Юнга. Пусть задан класс сопряженных элементов, т.е. $m_1, ..., m_n$.

Пример. $S_{27},\ m_1 = 2, m_3 = 3, m_5 = 2, m_6 = 1$.

Замечание. Диаграмма Юнга из n клеточек находятся во взаимно-однозначном соответствии с цикловыми типами в $S_n \Leftrightarrow$ классы сопряженных элементов.