0.1 Группа

1.1.1. Лекция

Определение 0.1.1. Группоид := множество с определенной на нем бинарной операцией.

Определение 0.1.2. Полугруппа := группоид + ассоциативность операции.

Определение 0.1.3. Моноид G := полугруппа + единичный (нейтральный) элемент e, то есть такой, что $\forall g \in G$ выполнено $ge = eg = g$.

Определение 0.1.4. Элемент $b \in G$ называется обратным к элементу $a \in G$, если $ab = ba = e$. Обозначатся a^{-1}. Если к элементу существует обратный, то он называется обратимым.

Определение 0.1.5. Группа := моноид, в котором все элементы обратимы.

Определение 0.1.6. Группа, состоящая из конечного числа элементов, называется конечной группой. Иначе — бесконечной.

Определение 0.1.7. Число элементов в конечной группе называется порядком группы и обозначается $|G|$.

Определение 0.1.8. Пусть g элемент некоторой группы. Наименьшее натуральное число n такое, что $g^n = e$, называют порядком элемента g. Обозначается $|g|$. Если такого n нет, то говорят, что элемент имеет бесконечный порядок: $|g| = \infty$.

Так как с понятием группы мы будем часто встречаться, дадим еще раз определение в удобной форме.

Множество G с определенной на нем бинарной операцией "$\cdot$" называется группой, если
1. операция "$\cdot$" ассоциативна, то есть

$$(a \cdot b) \cdot c = a \cdot (b \cdot c)\, \forall a, b, c \in G$$

2. существует единичный элемент e, то есть такой элемент $e \in G$, что

$$a \cdot e = e \cdot a = a\, \forall a \in G$$

3. к любому элементу существует обратный, то есть

$$\forall a \in G \; \exists a^{-1} \in G : \; a \cdot a^{-1} = a^{-1} \cdot a = e$$

Обозначается $(G, \cdot)$.

Иногда знак операции опускают: вместо $a \cdot b$ пишут ab. Кроме того, благодаря ассоциативности можно опускать скобки: вместо $(ab)c = a(bc)$ пишут abc. Кстати, несложно доказать справедливость ассоциативного закона для n элементов.

Определение 0.1.9. Подмножество элементов H в группе G называется подгруппой, если оно само является группой относительно той же бинарной операции. То, что H подгруппа группы G мы будем обозначать $H \leq G$.

У любой группы G есть как минимум две подгруппы: подгруппа $\{e\}$ и сама G. Их называют тривиальными подгруппами. Если подгруппа H группы G не совпадает со всей группой, то будем писать $H < G$.

Напоминание. Бинарная операция "$\cdot$", определенная на множестве G, называется коммутативной, если $\forall a, b \in G \; ab = ba$.

Определение 0.1.10. Группа с коммутативной операцией называется коммутативной или абелевой.

Определение 0.1.11. Циклической группой (порядка n) называется группа, порожденная одним элементом (порядка n):

$$G = \{e, \; a, \; a^2, \; \ldots, \; a^{n-1}\} = \langle a \rangle = \langle a \rangle_n.$$

Циклической группой бесконечного порядка называется группа, порожденная одним элементом бесконечного порядка:

$$G = \{e, \; a, \; a^{-1}, \; a^2, \; a^{-2}, \; \ldots\} = \{a^n, n \in \mathbb{Z}\} = \langle a \rangle = \langle a \rangle_\infty$$

(здесь $a^{-n} = \left(a^{-1}\right)^n$).

1.1.2. Семинар

В задачах этого семинара требуется доказать сформулированные утверждения.

Задача 0.1.1. Единичный элемент e — единственный.

Доказательство. Пусть e_1, e_2 - две единицы в группе. Тогда $e_1 = e_1 e_2 = e_2$. □

Задача 0.1.2. Для любого $x \in G$ обратный элемент — единственный.

Доказательство. Пусть y, z — суть обратные к x.
Тогда $y = ye = y(xz) = (yx)z = ez = z$. □

Задача 0.1.3. Пусть $x, y \in G$. Тогда, если $xy = e$, то $y = x^{-1}$ (а тогда и $yx = e$).

Доказательство. $y = ey = (x^{-1}x)y = x^{-1}(xy) = x^{-1}e = x^{-1}$ □

Задача 0.1.4. Пусть $x, y \in G$. Тогда $(xy)^{-1} = y^{-1}x^{-1}$.

Доказательство. $(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xex^{-1} = xx^{-1} = e$. □

Задача 0.1.5. Пусть $x \in G$, $n, m \in \mathbb{Z}$. Тогда $x^n x^m = x^{n+m}$.

Доказательство. Рассмотрим несколько случаев:

1. $n > 0, m > 0$, тогда
$$x^n x^m = \underbrace{x \cdot \ldots \cdot x}_{n} \cdot \underbrace{x \cdot \ldots \cdot x}_{m} = \underbrace{x \cdot \ldots \cdot x}_{n+m} = x^{n+m};$$
2. $n < 0, m < 0 \Rightarrow n = -k\ (k > 0), m = -l\ (l > 0)$, тогда $x^n x^m = x^{-k} \cdot x^{-l} = (x^{-1})^k \cdot (x^{-1})^l = (\text{см. случай 1})) = (x^{-1})^{k+l} = x^{-(k+l)} = x^{n+m}$;
3. $n > 0, m < 0, n + m \geq 0$, тогда $x^n x^m = (\text{см. случай 1})) = (x^{n+m} \cdot x^{-m}) \cdot x^{-(-m)} = x^{n+m} \cdot x^{-m} \cdot (x^{-m})^{-1} = x^{n+m}$;
4. $n > 0, m < 0, n + m < 0$, тогда $x^n x^m = (\text{см. случай 2})) = x^n \cdot (x^{-n} \cdot x^{n+m}) = x^n \cdot (x^n)^{-1} \cdot x^{n+m} = x^{n+m}$.

□

Задача 0.1.6. Если $x^2 = e$ для всех элементов группы, то группа G коммутативна.

Доказательство. Если $xx = e$, то $x = x^{-1}$ $\forall x \in G$. Тогда $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$. □

Задача 0.1.7. Если $\exists\, n \neq k \in \mathbb{N} : x^n = x^k$, то $|x| < \infty$.

Доказательство. Пусть для определенности $n > k$. Из $x^n = x^k$ следует, что $x^{-k}x^n = x^{-k}x^k$, то есть $x^{n-k} = e$. □

Задача 0.1.8. Пусть $x, y \in G$. Тогда $|x| = |y^{-1}xy|$.

Доказательство. Пусть $|x| = n \Rightarrow x^n = e$. Тогда

$$(y^{-1}xy)^n = \underbrace{(y^{-1}xy) \cdot (y^{-1}xy) \cdot \ldots \cdot (y^{-1}xy)}_{n} =$$

$$= y^{-1}x(yy^{-1})x \ldots (yy^{-1})xy = y^{-1}x^n y = y^{-1}y = e$$

$\Rightarrow |y^{-1}xy| \leqslant n = |x|$.
Остается заметить, что поскольку
$x = (yy^{-1})x(yy^{-1}) = (y^{-1})^{-1}(y^{-1}xy)y^{-1}$, то $|x| \leqslant |y^{-1}xy|$. □

Задача 0.1.9. Пусть $x, y \in G$. Тогда $|xy| = |yx|$.

Доказательство. Пользуясь предыдущей задачей, получим: $|xy| = |x^{-1}(xy)x| = |yx|$. □

Задача 0.1.10. Пусть $x \in G$ и $|x| = n < \infty$. Тогда, если $x^m = e$, то $n \mid m$.

Доказательство. Пусть $m = nd + r$, где $0 \leqslant r \leqslant n - 1$.
Тогда $x^m = x^{nd+r} = x^{nd}x^r = (x^n)^d x^r = x^r$. Но $x^r = e \Leftrightarrow r = 0$ (так как $x^0 = e$). Отсюда $x^m = e \Leftrightarrow m = nd$. □

Задача 0.1.11. Пусть $H_1 < G, H_2 < G$. Тогда $H_1 \cap H_2 < G$.

Доказательство. Во-первых $H_1 \cap H_2$ содержит единицу, так как $e \in H_1, e \in H_2$. Пусть $x \in H_1 \cap H_2$, то есть $x \in H_1, x \in H_2$. Следовательно, $x^{-1} \in H_1$ и $x^{-1} \in H_2$. Значит, $x^{-1} \in H_1 \cap H_2$. □

Задача 0.1.12. Пусть $H_1 < G, H_2 < G$. Тогда, если $H_1 \cup H_2$ — подгруппа, то либо $H_1 \subseteq H_2$, либо $H_2 \subseteq H_1$.

Доказательство. От противного. Пусть $\exists h_1 \in H_1 \setminus H_2$ и $h_2 \in H_2 \setminus H_1$. Так как по предположению $H_1 \cup H_2$ является подгруппой, $h_1 h_2 = h_3 \in H_1 \cup H_2$. Пусть для определенности $h_3 \in H_1$, тогда $h_2 = h_1^{-1} h_3 \in H_1$, но это противоречит $h_2 \in H_2 \setminus H_1$. □

Задача 0.1.13. Доказать, что группа, имеющая лишь конечное число подгрупп конечна.

Доказательство. Бесконечная циклическая группа изоморфна $\mathbb{Z}$ и, следовательно, имеет бесконечное число подгрупп. Поэтому циклическая подгруппа, порожденная произвольным элементом нашей группы, конечна (в противном случае наша группа содержала бы бесконечное число подгрупп). Поскольку любой элемент содержится в циклической подгруппе порожденной им самим, группа содержится в конечном объединении (так как число всех подгрупп конечно) конечных циклических подгрупп, а значит имеет конечное число элементов. □

Обозначение. $(n, m) = \text{НОД}(m, n)$ — наибольший общий делитель чисел n и m.

Задача 0.1.14. Пусть $x \in G$, $|x| = n$. Тогда $|x^k| = \frac{n}{(k,n)}$.

Доказательство. Пусть $(n, k) = d$. Тогда $(x^k)^{\frac{n}{d}} = x^{\frac{kn}{d}} = (x^n)^{\frac{k}{d}} = e^{\frac{k}{d}} = e$. Поэтому $|x^k| \leq \frac{n}{d}$.
Осталось доказать, что $|x^k| \leq \frac{n}{d}$. Имеем: $n = n_1 d$; $k = k_1 d$, причем $(n_1, k_1) = 1$. Пусть $m \in \mathbb{N}$ такое число, что $(x^k)^m = x^{km} = e$. Следовательно, $mk \vdots n$, то есть $mk_1 d \vdots n_1 d$, откуда $mk_1 \vdots n_1$. Но числа k_1 и $n-1$ взаимно просты, поэтому $m \vdots n_1 = \frac{n}{d}$. Значит, наименьшим m таким, что $(x^k)^m = e$ является $m = \frac{n}{d}$. □

Задача 0.1.15. Пусть $x \in G$. Тогда $|x| = |x^{-1}|$.

Доказательство. Пусть $|x| = n \Rightarrow x^n = e \Rightarrow x^{-n} = (x^{-1})^n = e \Rightarrow |x^{-1}| \leq n = |x|$. Заменив в этом рассуждении x на x^{-1}, получаем $|x| \leq |x^{-1}|$. Следовательно, $|x| = |x^{-1}|$.

Можно рассуждать по-другому. Ясно, что $x^{-1} = x^{n-1}$. Поэтому $|x^{-1}| = |x^{n-1}| = \frac{n}{(n,n-1)} = n$.

Кстати, если $|x| = \infty$, то и $|x^{-1}| = \infty$ (если бы $|x^{-1}| = n$, то предыдущее рассуждение дало бы $|x| = n$. □

Задача 0.1.16. Пусть $x, y \in G$ такие, что $xy = yx$ и $(|x|, |y|) = 1$. Тогда $|xy| = |x||y|$.

Доказательство. Пусть $|x| = n$, $|y| = m$.
Очевидно, что $(xy)^{nm} = (x^n)^m (y^m)^n = e^m e^n = e \Rightarrow |xy| \leq nm$.
Пусть $|xy| = k$. Так как $(xy)^k = x^k y^k = e$, то $y^k = x^{-k}$, откуда $|y^k| = |x^k|$, то есть $\frac{m}{(k,m)} = \frac{n}{(k,n)}$; $m(k,n) = n(k,m)$. Но первый множитель левой части равенства взаимно прост с первым множителем правой части, поэтому (k,n) делится на n, а тогда и k делится на n. Рассуждая аналогично, получаем, что k делится на m. А так как m и n взаимно просты, k делится на их произведение. □

Замечание. Хотелось бы получить обобщение предыдущего результата, отбрасывая то или иное требование. В обоих случаях нас подстерегает неудача. Если не требовать $xy = yx$, контрпример может быть получен уже по результатам следующей лекции о подстановках. Если не требовать $(|x|, |y|) = 1$, то напрашивающееся обобщение вида $|xy| = \text{НОК}(|x|, |y|)$ ложно хотя бы по причине $|xx^{-1}| = |e| = 1$ (почему оно напрашивается: на семинаре, посвященном подстановкам, будет доказано, что порядок произведения независимых циклов равен НОК порядков этих циклов).

Определение 0.1.12. Периодической частью группы G называется множество $T(G) = \{g \in G, |g| < \infty\}$.

Задача 0.1.17. Привести пример группы G, такой что $T(G)$ — не является ее подгруппой.

Доказательство. Пусть G — группа, порожденная отражениями относительно двух параллельных прямых (очевидно, что отражения имеют порядок 2). При этом их произведение является уже параллельным переносом и поэтому имеет бесконечный порядок. □

0.2 Подстановки, теорема Кэли

1.2.1 Лекция

Определение 0.2.1. Перестановкой длины (степени) n называется последовательность чисел $1, 2, \ldots, n$, записанных в произвольном порядке. Всего имеется $n!$ перестановок.

Определение 0.2.2. Подстановкой длины n называется биекция $f : \{1, 2, \ldots, n\} \longrightarrow \{1, 2, \ldots, n\}$. Подстановку принято записывать в виде $\begin{pmatrix} 1 & 2 & \ldots & n \\ f(1) & f(2) & \ldots & f(n) \end{pmatrix}$.

Пример 0.2.1. Подстановка $f = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ действует так: $f(1) = 2$, $f(2) = 1$, $f(3) = 3$. Ясно, что, поменяв местами столбцы, получаем ту же самую подстановку: $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 2 & 1 & 3 \\ 1 & 2 & 3 \end{pmatrix} = \ldots$.

Определение 0.2.3. Пусть есть перестановка $i_1, i_2, \ldots, i_n$. Будем говорить, что пара чисел i_k, i_m, где $k < m$, образует инверсию, если $i_k > i_m$. Другими словами, если большее число встречается раньше меньшего.

Определение 0.2.4. Подстановка $\begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$ называется четной, если сумма количества инверсий в нижней и верхней строчке — четное число, нечетной — если нечетное. Поменяв местами два соседних столбца, меняем число инверсий в каждой строке на 1, при этом сумма инверсий или не поменяется, или изменится на 2, поэтому понятие четной (нечетной) подстановки не зависит от порядка столбцов.

Определение 0.2.5. Пусть подстановка σ имеет k инверсий. Тогда число $(-1)^k$ будем называть знаком подстановки σ и обозначать $\operatorname{sgn}(\sigma)$. Таким образом, если σ — четная подстановка, то $\operatorname{sgn}(\sigma) = 1$, а если нечетная, то $\operatorname{sgn}(\sigma) = -1$.

Пример 0.2.2. Подстановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 3 & 5 & 1 & 2 & 4 \end{pmatrix}$ имеет следующие инверсии: $(3,1), (3,2), (5,1), (5,2), (5,4)$ — 5 штук $\Rightarrow$ подстановка нечетная и, следовательно, имеет знак -1.

Произведение подстановок определяется как суперпозиция двух функций, и, следовательно, осуществляется справа налево.

Пример 0.2.3.

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix} \cdot \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & 1 \end{pmatrix}$$

Рассуждения были следующими. Смотрим на правую подстановку: 1 переходит в 4, смотрим на левую подстановку: 4 переходит в 3, левее подстановок нет, следовательно, 1 переходит в 3. Снова смотрим на правую подстановку: 2 переходит в 1, смотрим на подстановку левее: 1 переходит в 2, следовательно, 2 переходит в 2, то есть остается на месте. Теперь смотрим на 3 в правой подстановке, она переходит в себя же, смотрим на левую подстановку: там 3 переходит в 4, следовательно, 3 переходит в 4. Пока у нас получилось $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 4 & * \end{pmatrix}$. Так как в каждой строчке должны быть все числа от 1 до 4, то вместо $*$ можем дописать 1.

Так как умножение подстановок — суперпозиция функций, то ассоциативность выполняется.

Тождественную подстановку $\begin{pmatrix} 1 & 2 & \dots & n \\ 1 & 2 & \dots & n \end{pmatrix}$, которая все элементы оставляет на месте, будем обозначать id или e.

К любой подстановке $\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix}$ существует обратная $\begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix}$.

Действительно, $\begin{pmatrix} \alpha_1 & \alpha_2 & \dots & \alpha_n \\ \beta_1 & \beta_2 & \dots & \beta_n \end{pmatrix} \cdot \begin{pmatrix} \beta_1 & \beta_2 & \dots & \beta_n \\ \alpha_1 & \alpha_2 & \dots & \alpha_n \end{pmatrix} = id = e.$

Таким образом, мы получили все свойства группы:

1. ассоциативность по умножению;
2. единичный элемент - тождественная подстановка;
3. наличие обратного элемента для каждой подстановки.

Определение 0.2.6. Группу всех подстановок длины n с операцией умножения называют симметрической группой степени n и обозначают S_n.

Какой порядок группы S_n? То есть сколько существует различных подстановок длины n? Располагая числа в первой строке в порядке возрастания, видим, что подстановок столько же, сколько есть перестановок. Поэтому $|S_n| = n!$.

Подстановка может какие-то элементы перемещать, а какие-то оставлять на месте. Например, подстановка $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 2 & 1 & 3 & 7 & 6 & 4 \end{pmatrix}$ оставляет на месте 2 и 6, а остальные элементы двигаются циклически: $1 \longmapsto 5 \longmapsto 7 \longmapsto 4 \longmapsto 3 \longmapsto 1$. Это можно записать в виде цикла длины 5: (15743).

Определение 0.2.7. Подстановки, записанные в виде цикла, так и называются — циклами.

Определение 0.2.8. Два цикла называются независимыми, если у них нет общих элементов.

Легко заметить, что независимые циклы коммутируют.

Определение 0.2.9. Транспозицией называется цикл длины 2.

Пример 0.2.4. Рассмотрим подстановку $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix}$. Здесь есть два независимых цикла: (145) длины 3 и (23) длины 2. Тогда исходная подстановка может быть записана в виде произведения этих двух циклов: $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 2 & 5 & 1 \end{pmatrix} = (145)(23)$. Порядок перемножения этих циклов не важен, так как они независимы.

Таким образом, любую подстановку можно разложить в произведение независимых циклов, причем единственным образом, если не учитывать их порядок и исключить циклы длины 1.

Теорема 0.2.5. (Теорема Кэли) Любая конечная группа порядка n изоморфна некоторой подгруппе S_n.

1.2.2 Семинар

Задача 0.2.6. Как должны быть расположены числа в перестановке, чтобы инверсий было наибольшее количество ?

Решение. В порядке убывания. ◀

Задача 0.2.7. Сколько инверсий образует число 1, стоящее на k-м месте ?

Решение. 1 меньше любого числа в перестановке $\Rightarrow$ 1 будет образовывать инверсии со всеми числами, стоящими левее, а их $k-1$. ◀

Задача 0.2.8. Сколько инверсий образует число n, стоящее на k-м месте, в перестановке из n элементов ?

Решение. Так как n больше любого числа в перестановке, то n будет образовывать инверсии со всеми числами, стоящими правее, а их $n-k$. ◀

Задача 0.2.9. Сколько всего четных (нечетных) перестановок?

Решение. Разобъем все перестановки на пары, включив в одну пару те перестановки, которые отличаются только расположением 1 и 2. В каждой паре одна перестановка четная, одна нечетная. Поэтому всего четных (нечетных) перестановок $\dfrac{n!}{2}$. ◀

Задача 0.2.10. Доказать, что произведение двух четных подстановок является четной подстановкой, произведение двух нечетных — четной, произведение четной и нечетной — нечетной.

Доказательство. Пусть, например, α и β — четные подстановки.

$$\alpha\cdot\beta=\begin{pmatrix}a_1 & \dots & a_n\\ b_1 & \dots & b_n\end{pmatrix}\begin{pmatrix}1 & \dots & n\\ a_1 & \dots & a_n\end{pmatrix}=\begin{pmatrix}1 & \dots & n\\ b_1 & \dots & b_n\end{pmatrix}$$

Перестановка $(1\dots n)$ — четная $\Rightarrow$ $(a_1\dots\ a_n)$ — четная $\Rightarrow$ $(b_1\dots\ b_n)$ — четная. □

Подстановка длины n — элемент конечной группы S_n, следовательно имеет конечный порядок. Порядок цикла длины k равен k.

Задача 0.2.11. Если подстановка разложена в произведение независимых циклов, то ее порядок равен НОК длин этих независимых циклов.

Доказательство. Если $\sigma=\alpha_1\cdot\alpha_2\cdot\ldots\cdot\alpha_k$, то (в силу независимости циклов) $\sigma^m=\alpha_1^m\cdot\alpha_2^m\cdot\ldots\cdot\alpha_k^m$; для того, чтобы $\sigma^m=e$, необходимо и достаточно, чтобы $\alpha_1^m=\alpha_2^m=\ldots=\alpha_k^m=e$. Остается напомнить, что длина цикла совпадает с его порядком, то есть минимальной натуральной степенью, в которой цикл дает e. □

Задача 0.2.12. Пусть $\alpha=(i_1\dots i_k)$ и $\beta\in S_k$.
Тогда $\beta\alpha\beta^{-1}=(\beta(i_1)\beta(i_2)\dots\beta(i_k))$.

Доказательство. $\beta^{-1}(\beta(i_1)) = i_1 \Rightarrow \alpha(\beta^{-1}(\beta(i_1))) = i_2 \Rightarrow$
$\beta(\alpha(\beta^{-1}(\beta(i_1)))) = \beta(i_2)$ $\square$

Задача 0.2.13. Доказать, что любую подстановку можно представить следующими способами:

1. в виде произведения транспозиций;
2. в виде произведения транспозиций $(12), (23), \ldots, (n-1, n)$;
3. в виде произведения транспозиций $(12), (13), \ldots, (1n)$;
4. в виде произведения транспозиции (12) и цикла $(123 \ldots n)$.

Доказательство. 1. $(i_1 i_2 \ldots i_k) = (i_1 i_2)(i_2 i_3) \ldots (i_{k-1} i_k)$.

2. На первом этапе раскладываем циклы в произведение транспозиций (см. первый способ). Далее используем тот факт, что $(ik)(ij)(ik) = (kj)$. (в средней транспозиции i поменялось на k. Пример: $(25) = (23)[(34)(45)(34)](23)$.
3. $(ij) = (1j)(1i)(1j)$.
4. Обозначим $\alpha = (1\,2)$ и $\beta = (1\,2\,\ldots n)$. Воспользуемся предыдущей задачей: $\beta\alpha\beta^{-1} = (\beta(1)\beta(2)) = (23)$; $\beta(23)\beta^{-1} = (\beta(2)\beta(3)) = (34)$, и так далее. Получили все транспозиции из второго способа.

$\square$

Задача 0.2.14. Доказать, что знак цикла длины k равен $(-1)^{k-1}$ (иными словами, цикл четной длины является нечетной подстановкой, а цикл нечетной длины — четной подстановкой.

Доказательство. Указание. Транспозиция - нечетна, а любой цикл раскладывается в произведение транспозиций (см. предыдущую задачу, способ 1). $\square$

Определение 0.2.10. Группа всех четных подстановок называется знакопеременной группой и обозначается A_n.

Задача 0.2.15. Любая четная подстановка из A_n может быть представлена в виде произведения тройных циклов.

Доказательство. Если $n = 3$, то утверждение очевидно.
Покажем, как произведение транспозиций выражается через циклы длины три:
$(i_1 i_2)(i_1 i_3) = (i_1 i_3 i_2), (i_1 i_2)(i_3 i_4) = (i_1 i_4 i_3)(i_1 i_2 i_3)$. □

Задача 0.2.16. Игра в "пятнашки". На поле 4 на 4 расположены плитки с номерами от 1 до 15, причем правый нижний угол свободен:

a_1	a_2	a_3	a_4
a_5	a_6	a_7	a_8
a_9	a_{10}	a_{11}	a_{12}
a_{13}	a_{14}	a_{15}	

Плитки можно передвигать по горизонтали и вертикали. Доказать, что если перестановка $(a_1 a_2 \dots a_{15})$ нечетная, то получить "правильное"распо (на рисунке ниже) невозможно.

1	2	3	4
5	6	7	8
9	10	11	12
13	14	15	

Задача 0.2.17. Выяснить, как изменится разложение подстановки в произведение независимых циклов при умножении ее (с обеих сторон) на произвольную транспозицию.

0.3 Морфизмы

1.3.1 Лекция

Определение 0.3.1. Отображение $\phi : G \longrightarrow H$ называется гомоморфизмом (или морфизмом) группы G в группу H, если $\phi(ab) = \phi(a)\phi(b)$, $\forall a, b \in G$.

Определение 0.3.2. $\operatorname{Ker}\phi = \{g \in G : \phi(g) = e_H\}$ — ядро гомоморфизма ϕ.

Определение 0.3.3. $\operatorname{Im}\phi = \{h \in H : \exists g \in G : \phi(g) = h\}$ — образ гомоморфизма ϕ.

Определение 0.3.4. Гомоморфизм $\phi : G \longrightarrow H$ называется мономорфизмом, если $\forall g_1 \neq g_2 \in G : \Rightarrow \phi(g_1) \neq \phi(g_2)$.

Определение 0.3.5. Гомоморфизм $\phi : G \longrightarrow H$ называется эпиморфизмом, если $\operatorname{Im}\phi = H$.

Определение 0.3.6. Гомоморфизм $\phi : G \longrightarrow H$ называется изоморфизмом, если он является мономорфизмом и эпиморфизмом.

Определение 0.3.7. Если существует изоморфизм $\varphi : G \longrightarrow H$, то группы G и H называются изоморфными. Этот факт обозначается так: $G \cong H$.

Определение 0.3.8. Гомоморфизм $\phi : G \longrightarrow G$ называется эндоморфизмом.

Обозначим множество всех эндоморфизмов через $\operatorname{End} G$. Операция взятия композиции эндоморфизмов вводит структуру моноида, единица – тождественный изоморфизм id_G.

Определение 0.3.9. Изоморфизм $\phi : G \longrightarrow G$ называется автоморфизмом.

Ниже доказывается, что автоморфизмы группы G образуют группу относительно суперпозиции. Эта группа обозначается $\operatorname{Aut} G$.

Свойства гомоморфизма

1. $\phi(e) = e$
   ◀ $\phi(e) = \phi(ee) = \phi(e)\phi(e) \Leftrightarrow \phi(e)(\phi(e))^{-1} = \phi(e)\phi(e)(\phi(e))^{-1} \Leftrightarrow$
   $e = \phi(e)$ ▶

2. $\phi(g^{-1}) = (\phi(g))^{-1}$
   ◀ $e = \phi(e) = \phi(gg^{-1}) = \phi(g)\phi(g^{-1}) \Leftrightarrow (\phi(g))^{-1} = \phi(g^{-1})$ ▶

Ненулевые элементы поля K образуют абелеву группу относительно умножения. Она называется мультипликативной группой поля K и обозначается K^*.
$\mathbb{R}_+$ – множество неотрицательных вещественных чисел.

Пример 0.3.1. $f : \mathbb{C}^* \longrightarrow \mathbb{R}_+^*$, $f(z) = |z|$ — гомоморфизм, не мономорфизм, эпиморфизм, не изоморфизм, не эндоморфизм, не автоморфизм.

Предложение 0.3.2. Пусть $f : G \longrightarrow H$ — гомомоморфизм. Тогда $\operatorname{Ker} f$ — подгруппа группы G.

Доказательство. $g_1, g_2, g \in \operatorname{Ker} f$. Надо доказать две вещи:
(1) $g_1 \cdot g_2 \in \operatorname{Ker} f$
(2) $g^{-1} \in \operatorname{Ker} f$
Если $|G| < \infty$, то достаточно доказать только $g_1 \cdot g_2 \in \operatorname{Ker} f$. То есть не нужно доказывать существование обратного.
Почему так ?
$G = \{g, g^2, g^3, \ldots, g^n = e\}$. Пусть $g^m = g^k, m > k \Rightarrow g^{m-k} = e$. Значит, обратный к g - это g^{m-1}, то есть $gg^{m-1} = e$.
Теперь, наконец, докажем, что $\operatorname{Ker} f < G$.
Пусть $g_1, g_2 \in \operatorname{Ker} f$. Тогда $f(g_1 \cdot g_2) = f(g_1) \cdot f(g_2) = e \cdot e = e \Rightarrow g_1 g_2 \in \operatorname{Ker} f$.
Пусть $g \in \operatorname{Ker} f$. Тогда $f(g^{-1}) = (f(g))^{-1} = e^{-1} = e \Rightarrow g^{-1} \in G$.
Кстати, если $|G| < \infty$, доказательство принадлежности g^{-1} можно модифицировать: в этом случае $g^{-1} = g^{m-1} \in \operatorname{Ker} f$ (здесь m — порядок g). □

Предложение 0.3.3. Пусть $f : G \longrightarrow H$ — гомоморфизм. Тогда $\operatorname{Im} f$ — подгруппа H.

Доказательство. Пусть $h_1, h_2 \in \operatorname{Im} f$, то есть $\exists g_1, g_2 : \ f(g_1) = h_1, \ f(g_2) = h_2$. Тогда $h_1 \cdot h_2 = f(g_1) \cdot f(g_2) = f(g_1 \cdot g_2) \in \operatorname{Im} f$.
Пусть $h \in \operatorname{Im} f$, то есть $\exists g \in G : \ f(g) = h$. Тогда $h^{-1} = (f(g))^{-1} = f(g^{-1}) \in \operatorname{Im} f$. □

Теорема 0.3.4. Гомоморфизм $f : G \longrightarrow H$ является мономорфизмом $\Leftrightarrow \operatorname{Ker} f = \{e\}$.

Доказательство. $\Rightarrow$ Пусть f — мономорфизм, $g \in \operatorname{Ker} f$. Следовательно, $f(g) = e = f(e)$. Значит, $g = e$.
$\Leftarrow$ Пусть $\operatorname{Ker} f = \{e\}$ и $g_1, g_2 \in G$ такие, что $f(g_1) = f(g_2)$. Тогда $f(g_1 \cdot g_2^{-1}) = f(g_1) \cdot f(g_2^{-1}) = f(g_1) \cdot (f(g_2))^{-1} = e$. Отсюда $g_1 \cdot g_2^{-1} = e \Rightarrow g_1 = g_2$, то есть f — мономорфизм. □

Задача 0.3.5. Все автоморфизмы группы G образуют группу относительно суперпозиции, которая обозначается $\operatorname{Aut} G$.

Доказательство. Пусть $f_1, f_2 : G \longrightarrow G$ — автоморфизмы.
Операция есть — $(f_1 f_2)(g) = f_1(f_2(g))$. Нужно проверить, что $f_1 f_2$ - автоморфизм:
$(f_1 f_2)(g_1 g_2) = f_1(f_2(g_1 g_2)) = f_1(f_2(g_1) f_2(g_2)) = f_1(f_2(g_1)) f_1(f_2(g_2)) =$

$(f_1f_2)(g_1)(f_1f_2)(g_2) \Rightarrow f_1f_2$ — гомоморфизм.
Очевидно, что моно и эпи, т. к. f_1, f_2 — автоморфизмы.
Тождественное отображение является автоморфизмом и играет роль единичного элемента.
Обратное отображение к автоморфизму снова является автоморфизмом.
□

Предложение 0.3.6. Зафиксируем элемент $g \in G$. Тогда отображение $i_g : G \longrightarrow G$, $i_g(h) = ghg^{-1}$ является автоморфизмом.

Доказательство. Пусть $h_1, h_2 \in G$. Тогда $i_g(h_1h_2) = g(h_1h_2)g^{-1} = gh_1eh_2g^{-1} = gh_1(g^{-1}g)h_2g^{-1} = (gh_1g^{-1})(gh_2g^{-1}) = i_g(h_1)i_g(h_2) \Rightarrow$ i_g — гомоморфизм. Докажем изо = моно + эпи.
Докажем сначала моно. Пусть $h \in Ker(i_g) \Rightarrow i_g(h) = ghg^{-1} = e \Leftrightarrow h = g^{-1}g = e$.
Докажем теперь эпи. Пусть $a \in G$. Надо найти $h \in G : \ i_g(h) = ghg^{-1} = a$. Ясно, что $h = g^{-1}ag$. □

Определение 0.3.10. Автоморфизм называется внутренним, если он имеет вид $i_g(h) = ghg^{-1}$.

Предложение 0.3.7. Множество всех внутренних автоморфзмов группы G образует группу относительно суперпозиции, которая обозначается $\operatorname{Int} G$. Тем самым, $\operatorname{Int} G < \operatorname{Aut} G$.

Доказательство.

$$(i_{g_1}i_{g_2})(h) = i_{g_1}(i_{g_2})(h)) = i_{g_1}(g_2hg_2^{-1}) = g_1g_2hg_2^{-1}g_1^{-1} = \\ = (g_1g_2)h(g_1g_2)^{-1} = i_{g_1g_2}(h),$$

т.е. $i_{g_1}i_{g_2} = i_{g_1g_2}$. Далее, $i_e(h) = ehe^{-1} = h$, поэтому $i_e = id \in \operatorname{Int} G$ является единичным элементом. Наконец, $i_gi_{g^{-1}} = i_{gg^{-1}} = i_e = id$, т.е. $(i_g)^{-1} = i_{g^{-1}}$. □

Задача 0.3.8. Если G – абелева, то существует единственный внутренний автоморфизм — тождественный.

Доказательство. Используем коммутативность операции: $i_g(h) = ghg^{-1} = gg^{-1}h = h$. □

Предложение 0.3.9. Если $f : G \to H$ — изоморфизм групп (как частный случай $f : G \to G$ — автоморфизм группы G), то для любого элемента g группы G выполнено $|f(g)| = |g|$.

Доказательство. Если $g^k = e$, то $f(g)^k = f(g^k) = f(e) = e \Rightarrow |f(g)| \leq |g|$. Так как к автоморфизму есть обратный, то верно и обратное неравенство. □

Задача 0.3.10. Привести пример группы, у которой $\operatorname{Int} G = \operatorname{Aut} G$.

Доказательство. Докажем, что $\operatorname{Int} S_3 = \operatorname{Aut} S_3 \cong S_3$. Выписывая все внутренние автоморфизмы, убеждаемся, что разные элементы S_3 задают разные автоморфизмы. Поэтому $|\operatorname{Int} S_3| = 6$. Следовательно, $|\operatorname{Aut} S_3| \geq 6$. Далее, вспоминаем, что S_3 порождается транспозициями $a = (12)$ и $b = (13)$ (ну и заодно добавим к ним $c = (23)$, хуже не будет). Каждый автоморфизм каким-то образом перемешивает эти транспозиции. Например, если $f(a) = b$; $f(b) = a$; $f(c) = c$, то естественно сопоставить этому автоморфизму подстановку, состоящую из символов a, b, c: $\begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$

Поэтому функция $\Phi : \operatorname{Aut} S_3 \to S_3$ построена. То, что она является гомоморфизмом, предлагается проверить самостоятельно. Впрочем, можно обойтись и без этого: как известно, есть (с точностью до изоморфизма) только две группы шестого порядка: циклическая и группа подстановок. Так как $\operatorname{Aut} S_3$, очевидно, некоммутативна и состоит из шести элементов, значит, она изоморфна S_3. А тогда и $\operatorname{Aut} S_3$ изоморфна S_3. □

1.3.2 Семинар

Задача 0.3.11. Доказать, что все группы 2-го порядка изоморфны между собой.

Доказательство. $G = \{e,\ g\}$. Тогда $ee = e, eg = ge = g$. Если $g \cdot g = g = ge$, то $g = e$. Противоречие. Значит, $g^2 = e$. Следовательно, существует только одна группа, содержащая 2 элемента. □

Задача 0.3.12. Доказать, что все группы 3-го порядка изоморфны между собой.

Доказательство. $G = \{e,\ g,\ h\}$. Нужно задать таблицу умножения gh, hg, gg, hh. Если $gh = g$, то $h = e$ – противоречие. Аналогично доказываем, что $gh \neq h$. Значит, $gh = e$, а тогда и $hg = e$. Если $gg = g^2 = g$, то $g = e$ – противоречие; если $g^2 = e = gh$, то $g = h$ противоречие. Значит $g^2 = h$ и точно так же $h^2 = g$. Следовательно, существует только одна группа, состоящая из трех элементов. □

Задача 0.3.13. Доказать, что все циклические группы n-го порядка изоморфны.

Доказательство. Пусть $G = \langle a \rangle_n, H = \langle b \rangle_n$ и $f(a = b$ — изоморфизм. Действительно, $f(a^k) = f(aa \cdot \ldots \cdot a) = f(a) \cdot \ldots \cdot f(a) = b \cdot \ldots \cdot b = b^k$. $f(g^l g^m) = l + m$ и $f(g^l g^m) = f(g^{l+m}) = l + m$. □

Задача 0.3.14. Доказать, что все группы простого порядка — циклические.

Доказательство. Если элемент $|g| = p$ – простое число. Тогда если, m – произвольное целое число, то либо $g^m = e$ (m кратно p), либо элемент $|g^m| = p$. Действительно, $(g^m)^p = g^{mp} = (g^p)^m = e^m = e$. Поэтому $|g^m|$ должен быть делителем p, но, p – простое, то либо $|g^m| = p$ либо $m \vdots p$. Теперь вспомним, что порядок элемента равен порядку порожденной им циклической подгруппы. □

$\mathbf{C}_n$ — группа комплексных корней n-й степени из 1.
D_n — группа самосовмещений правильного n-угольника, включающая как вращения, так и осевые симметрии.

Определение 0.3.11. Группа $\mathbb{Z}_n = (\mathbb{Z}_n, +) = \{0, 1, \ldots, n-1\}$ называется группой вычетов по модулю n.

Задача 0.3.15. Доказать, что все группы простого порядка — изоморфны между собой.

Доказательство. Следует из двух предыдущих задач. □

Задача 0.3.16. Найти все (с точностью до изоморфизма) группы 4-го порядка.

Доказательство. Группа вращений квадрата $Rot(\square) = \{e, r_1, r_2, r_3\}$, где $e = R_{0^0}$, $r_1 = R_{90^0}$, $r_2 = R_{180^0}$, $r_3 = R_{270^0}$.

Таблица Кэли для $Rot(\square)$:

	e	r_1	r_2	r_3
e	e	r_1	r_2	r_3
r_1	r_1	r_2	r_3	e
r_2	r_2	r_3	e	r_1
r_3	r_3	e	r_1	r_2

Группа симметрий (самосовмещений) ромба $Sym(\Diamond) = \{e, r, s_1, s_2\}$, где $e = R_{0^0}$, $r = R_{180^0}$, s_1, s_2 - симметрии относительно диагоналей ромба.

Таблица Кэли для $Sym(\Diamond)$:

	e	r	s_1	s_2
e	e	r	s_1	s_2
r	r	e	s_2	s_1
s_1	s_1	s_2	e	r
s_2	s_2	s_1	r	e

Отсюда видно, что $Rot(\square) \ncong Sym(\Diamond)$, т.к. в первой группе есть элемент 4-го порядка, во второй — нет элемента, у которого порядок больше 2. □

Задача 0.3.17. Привести пример неизоморфных групп 6-го порядка.

Доказательство. Например, $D_3 \ncong \mathbf{C}_6$, т.к. $\mathbf{C}_6$ – коммутативна, а D_3 – нет. $\square$

Задача 0.3.18. Доказать, что группы $(\mathbb{Z}, +)$ и $(n\mathbb{Z}, +)$ изоморфны.

Доказательство. Изоморфизм $f(k) = nk \quad \forall k \in \mathbb{Z}$. $\square$

Задача 0.3.19. Доказать, что $(\mathbb{Z}_4, +)$ изоморфна $(\mathbb{Z}_5^*, \cdot)$.

Доказательство. Выпишем изоморфизм поэлементно: $f(0) = 2^0 = 1, f(1) = 2^1 = 2, f(2) = 2^2 = 4, f(3) = 2^3 = 3 \pmod 5$. $\square$

Определение 0.3.12. Группой движений Клейна называется группа самосовмещений ромба. Она обозначается V_4.

Задача 0.3.20. Привести пример плоских геометрических фигур, группы движений которых изоморфны:

1. $\mathbb{Z}_2$ есть группа симметрий фигур: отрезок (тождественное отображение и симметрия относительно центра); две точки (на прямой); равнобедренный, но не равносторонний треугольник (на плоскости);
2. $\mathbb{Z}_3 \cong A_3$
3. $S_3 \cong D_3$

1 | Факторизация и изоморфизмы

1.1 Отношение эквивалентности, факторизация

2.1.1 Лекция

Определение 1.1.1. Мы говорим, что задано отношение на множестве M, если задано подмножество $T \subseteq M \times M = \{(m_1, m_2)\}$.

Определение 1.1.2. Отношением эквивалентности (в этом случае, вместо $(x, y) \in T$ пишут $x \sim y$), называется такое отношение, которое обладает следующими свойствами:
1) Рефлексивность: $x \sim x$.
2) Симметричность: $x \sim y \Rightarrow y \sim x$.
3) Транзитивность: если $x \sim y$ и $y \sim z$, то $x \sim z$.

Обозначим $T_x = \{y : x \sim y\}$ – класс элементов, эквивалентных x.

Предложение 1.1.1. Пусть T – отношение эквивалентности на множестве M. Тогда,

1. $\forall x \in M \Rightarrow x \in T_x$
2. $\bigcup\limits_{x \in G} T_x = M$
3. Если $T_x \cap T_y \neq \varnothing$, то $T_x = T_y$.

Доказательство. Первое утверждение следует из рефлексивности, второе утверждение следует из первого. Докажем 3).
Пусть $z \in T_x \cap T_y \Rightarrow x \sim z$ и $y \sim z$ (а тогда $z \sim y$). Итак, $x \sim z \sim y$, поэтому $x \sim y$, а если $y \sim y_1$, то $x \sim y_1$. Следовательно, $T_y \subseteq T_x$. Аналогично доказываем, что $T_x \subseteq T_y$. В итоге, $T_x = T_y$. $\square$

Таким образом, мы показали, что любое отношение эквивалентности разбивает множество на непересекающиеся классы эквивалентности.

Примеры. Рассмотрим несколько отношений и выясним, являются ли они отношениями эквивалентности.

1. $M = \mathbb{R}$, $T = \{(x, y) : x < y\}$ – не является (выполнена только транзитивность);
2. $M = \mathbb{C}$, $T = \{(z_1, z_2) : z_1$ и z_2 лежат на одном луче, выходящем из нуля$\}$ – выполнено 1) и 2), а 3) не выполнено, так как $(x, 0) \in T, (0, y) \in T \not\Rightarrow (x, y) \in T$;
3. $M = \mathbb{C}^*$, $T = \{(z_1, z_2) : z_1$ и z_2 лежат на одном луче, выходящем из нуля$\}$ – является отношением эквивалентности;
4. $M = M_{2\times 2}$; $T = \{(x, y) : xy = yx\}$ – выполнено 1,2, не выполено 3;
5. $M = M_{2\times 2}$; $T = \{(x, y)$: $\exists z \in M, \det z \neq 0 : x = z^{-1}yz$ – отношение эквивалентности;
6. M – любое непустое множество; $T = \{(x, x)\}$ – отношение эквивалентности;
7. M – любое непустое множество; $T = M \times M$ – отношение эквивалентности.

Задача 1.1.2. На группе G с фиксированной подгруппой H задано отношение $T = \{(x, y) : x^{-1}y \in H\}$. Доказать, что T является отношением эквивалентности.

Доказательство. 1) $x^{-1}x = e \in H \Rightarrow (x, x) \in T$
2) Пусть $(x, y) \in T$, то есть $x^{-1}y \in H \Rightarrow (x^{-1}y)^{-1} = y^{-1}x \in H \Rightarrow (y, x) \in T$.
3) Если $x^{-1}y \in H$, и $y^{-1}z \in H$, то $(x^{-1}y)(y^{-1}z) = x^{-1}(yy^{-1})z = x^{-1}z \in H$. □

В дальнейшем для нас это отношение эквивалентности будет основным. Относительно него $T_x = \{y : x \sim y\} = \{y \mid x^{-1} \cdot y \in H\}$. Группа G оказывается разбитой на непересекающиеся классы эквивалентности. Так как $x \sim y \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists h \in H : x^{-1}y = h \Leftrightarrow y = xh \Rightarrow$ класс эвивалентности T_x — это $xH = \{xh \mid h \in H\}$. Далее, если $h_1 \neq h_2 \Rightarrow xh_1 \neq xh_2$. Отсюда делаем вывод, что если $|H| < \infty$, то во всех классах эквивалентности одинаковое

количество элементов, совпадающее с порядком подгруппы: $|xH| = |H|$.

Определение 1.1.3. $xH = \{xh \mid h \in H\}$ будем называть левым смежным классом элемента x по подгруппе H, а $Hx = \{hx \mid h \in H\}$ – правым смежный классом элемента x по подгруппе H. Правые смежные классы возникают как классы эквивалентности, если задавать эквивалентность по формуле $yx^{-1} \in H$.

Теорема 1.1.3. (Теорема Лагранжа) Порядок подгруппы делит порядок конечной группы.

Доказательство. Утверждение непосредственно следует из доказанного равенства $|xH| = |H|$. □

Задача 1.1.4. Дано: $H < G$; x, $y \in G$. Доказать, что $x^{-1}y \in H \Leftrightarrow \exists g \in G : \ x \in gH, y \in gH$.

Доказательство. Пусть $x^{-1}y = h \in H \Rightarrow y = xh$, то есть $y \in xH$. Кроме того, очевидно, что $x \in xH$, так как $x = xe$. Обратно. Пусть $x = gh_1, y = gh_2$. Следовательно, $x^{-1}y = (gh_1)^{-1}gh_2 = h_1^{-1}g^{-1}gh_2 = {h_1}^{-1}h_2 \in H$. □

Поставим задачу задать структуру группы на множестве левых смежных классов. Естественно, вводимая групповая операция должна быть связана с операцией в исходной группе. Единственным разумным способом добиться этого представляется задание операции по формуле $(xH)(yH) = (xy)H$. Возникает вопрос: если $xH = x_1H$ и $yH = y_1H$, будет ли смежный класс $(xy)H$ совпадать с $(x_1y_1)H$? Оказывается, в общем случае гарантировать совпадение нельзя, хотя, скажем, для коммутативной группы этот факт очевиден.

Пример 1.1.5. $G = S_3 = \{e,\ (12),\ (13),\ (23),\ (123),\ (132)\}$;
$H =< (12) >= \{e,\ (12)\}$;
$eH = (12)H$; $(123)H = (13)H = \{(13),\ (123)\}$;
$e(123)H = (123)H \neq (12)(13)H = \{(132),\ (23)\}$

Итак, у нас есть группа G и ее подгруппа H. Мы умеем строить левые смежные классы, а также правые смежные классы. Вообще

говоря, эти классы не обязаны совпадать. Так, в только что разобранном примере $(13)H = \{(13),\ (123)\} \neq H(13) = \{(13),\ (132)\}$. Но если, например, группа коммутативна, то $xH = Hx$ для любого $x \in G$. Но это не единственный случай их совпадения. А сейчас мы докажем, что их совпадение необходимо и достаточно для того, чтобы в фактормножестве, состоящем, скажем, из левых смежных классов, операция в группе G индуцировала групповую операцию.

Еще раз берем классы $xH = x_1H$ ($\Rightarrow x = x_1a;\ a \in H$), $yH = y_1H$ ($\Rightarrow y = y_1b;\ b \in H$), $(xy)H$ и $(x_1y_1)H$. Тогда $xy = x_1ay_1b$, а для совпадения классов $(xy)H$ и $(x_1y_1)H$ нужно, чтобы $xy = x_1y_1c;\ c \in H$. Приравнивая правые части, получаем $x_1ay_1b = x_1y_1c;\ ay_1 = y_1(cb^{-1});\ y_1^{-1}ay_1 = cb^{-1}$. Меняя x_1 в равенстве $x = x_1a$, мы можем получить любой $a \in H$, поэтому равенство $y_1^{-1}ay_1 = cb^{-1}$ равносильно $y_1^{-1}Hy_1 \subseteq H$. Далее, обратим внимание на то, что y_1 может быть любым элементом группы G. Поэтому лучше переписать это включение в виде

$$g^{-1}Hg \subseteq H;\ g \in G.$$

Умножая его слева на g, а справа на g^{-1}, получаем $H \subseteq gHg^{-1} = (g^{-1})^{-1}Hg^{-1} \subseteq H$. Последнее включение следует из $g^{-1}Hg \subseteq H$, если заменить в нем g на g^{-1}.

Следовательно, включение равносильно равенству

$$g^{-1}Hg = H;\ g \in G,\ \text{ну а оно равносильно равенству}$$

$$Hg = gH;\ g \in G,$$

что и означает совпадение левых и правых смежных классов.

Определение 1.1.4. Подгруппа H группы G называется нормальной подгруппой (будем записывать это в виде $H \lhd G$), если выполнено любое из равносильных условий:

- $g^{-1}Hg \subseteq H\ \forall g \in G$
- $g^{-1}Hg = H\ \forall g \in G$
- $Hg = gH\ \forall g \in G$

2.1.2 Семинар

Задача 1.1.6. Порядок элемента делит порядок группы.

Доказательство. Любой элемент порождает циклическую подгруппу, чей порядок равен порядку этого элемента. По теореме Лагранжа порядок подгруппы делит порядок группы. □

Задача 1.1.7. $D_3 \cong S_3$

Доказательство. D_3 — группа самосовмещений правильного треугольника. Занумеруем вершины треугольника цифрами 1,2,3. Сопоставим каждому элементу $g \in D_3$ подстановку $\phi(g) = \sigma_g \in S_3$, которая задается перестановкой соответствующих вершин треугольника. □

Задача 1.1.8. Если группа коммутативна, то все ее подгруппы нормальны.

Доказательство. Пусть G – коммутативная группа, а H – ее подгруппа. Тогда $g^{-1}hg = g^{-1}gh = h$. □

Задача 1.1.9. Пусть G — группа и $H_1 \lhd G, H_2 \lhd G, \ldots, H_k \lhd G$. Тогда $H_1 \cap H_2 \cap \ldots \cap H_k \lhd G$.

Доказательство. Пусть $h \in H_1 \cap H_2 \cap \ldots \cap H_k$. Тогда $h \in H_1, h \in H_2, \ldots, h \in H_k$. Поэтому если g – произвольный элемент группа G. то $ghg^{-1} \in H_1, ghg^{-1} \in H_2, \ldots, ghg^{-1} \in H_k$. А это значит, что $ghg^{-1} \in H_1 \cap H_2 \cap \ldots \cap H_k$. □

Задача 1.1.10. Пусть $|G| = n, H < G : |H| = \frac{n}{2}$. Тогда $H \lhd G$.

Доказательство. Если $x \in H$, то $xH = Hx = H$. Если $x \notin H$, то $xH \neq H$, $Hx \neq H \Rightarrow xH \cap H = \emptyset$, $Hx \cap H = \emptyset \Rightarrow xH = G \setminus H$, $Hx = G \setminus H$. □

Определение 1.1.5. Подгруппа $H < G : |H| = \frac{|G|}{k}$ называется подгруппой индекса k.

Задача 1.1.11. Найти все подгруппы S_3 и выяснить, какие из них нормальны.

Решение. $|S_3| = 3! = 6$
$H_1 = \{e\}$
$H_2 = \{e, (12)\}$
$H_3 = \{e, (13)\}$
$H_4 = \{e, (23)\}$

$H_5 = \{e, (123), (123)^2 = (132)\} = \langle (123) \rangle_3$
$H_6 = \{e, (12), (23), (13), (123), (132)\} = S_3$
Нормальны H_1, H_5 и H_6. ◀

Задача 1.1.12. Пусть $f : G \longrightarrow F$ — гомоморфизм.Тогда $Ker\, f \lhd G$.

Доказательство. Нам уже известно, что $Ker\, f < G$.
Пусть $h \in Ker\, f, g \in G$. Тогда $f(ghg^{-1}) = f(g)f(h)f(g^{-1}) = f(g)ef(g)^{-1} = e$. Значит, $ghg^{-1} \in Ker\, f$. □

Задача 1.1.13. Привести пример такого гомоморфизма $\phi : G_1 \longrightarrow G_2$, что $\mathrm{Im}\, \phi$ не является нормальной подгруппой G_2.

Определение 1.1.6. Пусть A и B — два подмножества группы G. Их произведением назовем множество $AB = \{ab \mid a \in A, b \in B\}$.

Задача 1.1.14. Пусть G — группа, $H_1 \lhd G, H_2 < G$. Тогда $H_1H_2 < G$.

Доказательство. Пусть $h_1, h_3 \in H_1, h_2, h_4 \in H_2, g \in G$. Из $H_1 \lhd G$ следует, что $gh_1g^{-1} \in H_1$. Тогда $\underbrace{(h_1h_2)}_{\in H_1H_2}\underbrace{(h_3h_4)}_{\in H_1H_2} = h_1h_2h_3h_4 = h_1\underbrace{(h_2h_3h_2^{-1})}_{\in H_1}\underbrace{h_2h_4}_{\in H_2} \in H_1H_2$; $(h_1h_2)^{-1} = h_2^{-1}h_1^{-1} = \underbrace{(h_2^{-1}h_1^{-1}h_2)}_{\in H_1}h_2^{-1} \in H_1H_2$. □

Задача 1.1.15. Пусть G — группа и $H_1 \lhd G, H_2 \lhd G$. Тогда $H_1H_2 \lhd G$.

Доказательство. Пусть $h_1 \in H_1, h_2 \in H_2, g \in G$. Тогда $gh_1g^{-1} \in H_1, gh_2g^{-1} \in H_2$. Следовательно, $g(h_1h_2)g^{-1} = \underbrace{(gh_1g^{-1})}_{\in H_1}\underbrace{(gh_2g^{-1})}_{\in H_2} \in H_1H_2$. □

1.2 Теорема о гомоморфизме

2.2.1 Лекция

Определение 1.2.1. Факторизацией называется переход от множества к классам эквивалентности этого множества.

Мы видели, что операция $xH \cdot yH = xyH$, которую мы ввели на классах эквивалентности, корректна только в случае нормальной подгруппы H. Теперь, удостоверимся, что , если $H \lhd G$, то G/H,

то есть множество смежных классов, является группой (будем называть ее факторгруппой).
Ассоциативность операции следует из ассоциативности в самой группе G, а именно $((xH)\cdot(yH))\cdot(zH) = (xyH)\cdot(zH) = (xyz)H = (xH)\cdot((yz)H) = (xH)\cdot((yH)\cdot(zH))$.
Единичный элемент — это сама подгруппа $H = eH$, так как $(gH)\cdot(eH) = (eH)\cdot(gH) = gH$.
Обратным классом к классу gH будет $g^{-1}H$, так как $(gH)\cdot(g^{-1}H) = (gg^{-1})H = eH = H$ и $(g^{-1}H)\cdot(gH) = (g^{-1}g)H = eH = H$.
Если $|G| < \infty$, то $|G/H| = \frac{|G|}{|H|}$.

Пример 1.2.1. $G/\{e\} = G$ и $G/G = \{e\}$;

$$\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}.$$

Теорема 1.2.2. (Теорема о гомоморфизме)
Пусть $f : G \longrightarrow F$ – гомоморфизм. Тогда имеется естественный изоморфизм $\phi\colon G/\operatorname{Ker} f \cong \operatorname{Im} f$, определенный формулой $\phi(g \operatorname{Ker} f) := f(g)$.

Доказательство. Построим гомоморфизм $\phi : G/\operatorname{Ker} f \longrightarrow \operatorname{Im} f$: $\phi(g \cdot \operatorname{Ker} f) = f(g)$, где $g \in G$.
Проверим корректность (то есть что на эквивалентных элементах получается одинаковый результат). Пусть $g \sim \tilde{g}$, то есть $\exists h \in \operatorname{Ker} f :\ g = \tilde{g}h$. Тогда $f(g) = f(\tilde{g}h) = f(\tilde{g})f(h) = f(\tilde{g})$. Следовательно, $\phi : G/\operatorname{Ker} f \longrightarrow \operatorname{Im} f$ определено корректно.
Пусть $x, y \in G$. Докажем, что $\phi(xy \operatorname{Ker} f) = \phi(x \operatorname{Ker} f)\phi(y \operatorname{Ker} f)$.
Действительно,

$$\phi(xy \operatorname{Ker} f) = f(xy) = f(x)f(y) = \phi(x \operatorname{Ker} f)\phi(y \operatorname{Ker} f).$$

Значит ϕ — гомоморфизм.
С другой стороны, $\phi(x \operatorname{Ker} f) = f(x) = e \Leftrightarrow x \in \operatorname{Ker} f$. Следовательно, $\operatorname{Ker}\phi = \{\operatorname{Ker} f\} = \{e\}$. Значит ϕ — мономорфизм.
Очевидно, что $\operatorname{Im} f = \operatorname{Im}\phi$, то есть ϕ — эпиморфизм. В итоге, ϕ — изоморфизм. □

Следствие 1.2.3. Пусть $f : G \longrightarrow F$ — мономорфизм. Тогда $G \cong \operatorname{Im} f$.

Замечание. Для каждой нормальной подгруппы H группы G найдется гомоморфизм f этой группы (более того, эпиморфизм) такой, что $\operatorname{Ker} f = H$. Это — гомоморфизм, сопоставляющий каждому элементу смежный класс, которому этот элемент принадлежит.

Задача 1.2.4. $S_n/A_n \cong U_2\ (= \{-1,\ 1\} \cong C_2)$

Доказательство. Так как $|S_n| = n!, |A_n| = \frac{n!}{2} \Rightarrow |S_n| = |A_n| \cdot 2 \Rightarrow A_n$ индекса 2, поэтому $A_n \lhd S_n$. Построим гомоморфизм $f : S_n \longrightarrow U_2$: $f(\sigma) = \operatorname{sgn}\sigma$. Тогда $\operatorname{Im} f = U_2$ и $\operatorname{Ker} f = \{\sigma : \operatorname{sgn}\sigma = 1\} = A_n$. По теореме о гомоморфизме, $S_n/\operatorname{Ker} f \cong \operatorname{Im} f$, то есть $S_n/A_n \cong U_2$. Кстати, нормальность A_n можно было не проверять: ядро гомоморфизма автоматически является нормальной подгруппой. □

Предложение 1.2.5. $S_4/V_4 \cong S_3$

Доказательство. Сперва докажем, что $V_4 \lhd S_4$, непосредственно проверив совпадение левых и правых смежных классов:
$V_4 = \{e,\ (12)(34),\ (13)(24),\ (14)(23)\}$;
$(12)V_4 = (34)V_4 = (1324)V_4 = (1423)V_4 = V_4(12) = \ldots$
$\ldots = \{(12),\ (34),\ (1324),\ (1423)\}$ (конечно, все эти вычисления делать не надо: найдя $(12)V_4$ и $V_4(12)$ и убедившись, что они совпадают, делаем вывод, что остальные элементы найденного смежного класса порождают его же);
$(13)V_4 = \{(13),\ (1234),\ (24),\ (1432)\} = V_4(13)$
$(14)V_4 = \{(14),\ (1243),\ (1342),\ (23)\} = V_4(24)$
$(123)V_4 = \{(123),\ (134),\ (243),\ (142)\} = V_4(123)$
$(132)V_4 = \{(132),\ (234),\ (124),\ (143),\} = V_4(132)$
Замечаем следующую закономерность: в каждом смежном классе ровно одна подстановка оставляет на месте цифру 4. Поэтому представляется совершенно естественным при построении изоморфизма $S_4/V_4 \simeq S_3$ поставить в соответствие каждому смежному классу именно эту подстановку (рассматривая ее как элемент S_3). Сохранение операции (то есть гомоморфность этого отображения) очевидна. □

Теорема 1.2.6. (Теорема об изоморфизмах)

1. Пусть G – группа, K и H – ее нормальные подгруппы, причем

K – содержится в H. Тогда H/K – подгруппа в G/K и

$$(G/K)/(H/K) \cong G/H.$$

[Кратко: Пусть $K \leq H \leq G$ и $K \trianglelefteq G$, $H \trianglelefteq G$. Тогда $H/K \trianglelefteq G/K$ и $(G/K)/(H/K) \cong G/H$.]

2. Пусть G – группа, K и H – ее подгруппы, причем K нормальна в G. Тогда HK – подгруппа в G, K – нормальная подгруппа в HK, $H \cap K$ – нормальная подгруппа в H и

$$HK/K \cong H/H \cap K.$$

[Кратко: Пусть $H \leq G$ и $K \trianglelefteq G$. Тогда $HK \leq G$ и $K \trianglelefteq HK$, $H \cap K \trianglelefteq H$ и $HK/K \cong H/H \cap K$.]

Доказательство.

1. Первое утверждение вытекает из теоремы о гомоморфизме, если определить $\varphi\colon G/K \to G/H$ формулой $\varphi(gK) := gH$.

2. Для доказательства второго утверждения снова применяем теорему о гомоморфизме к гомоморфизму

$$\psi\colon HK/K \to H/H \cap K, \;\; \psi(hkK) := h(H \cap K),$$

и проверяем, что ψ на самом деле является изоморфизмом.

□

Отметим, что первое утверждение теоремы дает следующее соотношение между индексами подгрупп:

$$|G : H| = \frac{|G : K|}{|H : K|}.$$

Пример 1.2.7. В S_4 имеется нормальная подгруппа – четверная группа Клейна
$V_4 := \{e, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. Обозначим через T подгруппу в S_4, состоящую из подстановок оставляющих 4 на месте. Ясно, что $T \cong S_3$. Кроме того, $S_4 = TV_4$ и $T \cap V_4 = \{e\}$. Второе утверждение теоремы об изоморфизмах дает

$$S_4/V_4 \cong TV_4/V_4 \cong T/T \cap V_4 = T/\{e\} \cong T \cong S_3.$$

Ниже мы дадим описание этого гомоморфизма используя группу вращений трехмерного куба, которая, как будет показано, изоморфна S_4.

Пример 1.2.8. Дуальная группа. У дуальной группы G^{o} те же элементы и та же единица, что и у самой группы G, но другое умножение, которое определяется фомулой: $g{*}h := hg$. Аксиомы легко проверяются.

Рассмотрим биекцию $\varphi\colon G \to G^{\mathrm{o}}$, $\varphi(g) := g^{-1}$. Имеем $\varphi(g_1g_2) = (g_1g_2)^{-1} = g_2^{-1}g_1^{-1} = g_1^{-1}{*}g_2^{-1} = \varphi(g_1){*}\varphi(g_2)$, поэтому φ – изоморфизм. Обратный изоморфизм $\psi\colon G^{\mathrm{o}} \to G$ дается той же формулой $\psi(g) := g^{-1}$.

Для группы $G = GL(n, \mathbb{K})$, где $\mathbb{K}$ – поле, биекция $G \to G^{\mathrm{o}}$, переводящая матрицу в транспонированную является изоморфизмом. Обратный изоморфизм определяется тем же правилом $A \mapsto A^T$, поскольку $(A^T)^T = A$ для любой матрицы $A \in GL(n, \mathbb{K})$.

Экспонента группы

Определение 1.2.2. Экспонентой группы (обозначается $\exp G$) называется наименьшее натуральное m такое, что $g^m = e \ \ \forall\, g \in G$. Если такое число не существует, то полагаем $\exp(G) = \infty$.

Если группа G конечна, то $g^{|G|} = e$ для любого $g \in G$, поэтому $\exp G \leq |G|$, т. е. экспонента конечной группы не превосходит ее порядка.

Пример 1.2.9. $\exp(\mathbb{Z}_k \oplus \mathbb{Z}_n) = \mathrm{HOK}(k, n)$;
$\exp(\mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_s}) = \mathrm{HOK}(k_1, \ldots, k_s)$;
$\exp(\mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^3} \oplus \cdots \oplus \mathbb{Z}_{p^s} \oplus \ldots) = \infty$.

2.2.2 Семинар

Введем несколько обозначений.

- $\mathrm{GL}(n, \mathbb{C}) = \{A \in M_{n\times n}(\mathbb{C}) \mid \det A \neq 0\}$ — множество невырожденных матриц размера n с элементами из поля $\mathbb{C}$;
- $\mathrm{SL}(n, \mathbb{C}) = \{A \in M_{n\times n}(\mathbb{C}) \mid \det A = 1\}$ — множество матриц размера n с элементами из поля $\mathbb{C}$ с определителем 1;
- $\mathbf{U} = \{z \in \mathbb{C} \mid |z| = 1\}$
- $\mathbf{H}_n = \{z \in \mathbb{C} \mid \arg(z) = \frac{2\pi k}{n},\ k \in \mathbb{Z}\}$

- $\mathbf{C}_n = \mathbf{U}_n = \{z \in \mathbb{C} \mid z = \sqrt[n]{1}\}$

Задача 1.2.10. $\mathrm{SL}(n, \mathbb{C}) \lhd \mathrm{GL}(n, \mathbb{C})$

Доказательство. Надо доказать, что $A \cdot B \cdot A^{-1} \in \mathrm{SL}(n, \mathbb{C}) \quad \forall A \in \mathrm{GL}(n, \mathbb{C}), B \in \mathrm{SL}(n, \mathbb{C})$.
Воспользуемся свойствами определителя:
$\det(ABA^{-1}) = \det A \det B \det A^{-1} = \det A \det B (\det A)^{-1} = \det B = 1$.
Второй способ доказательства сводится к ссылке на то, что $\mathrm{SL}(n, \mathbb{C})$ является ядром гомоморфизма, который строится в следующей задаче. □

Задача 1.2.11. $\mathrm{GL}(n, \mathbb{C})/\mathrm{SL}(n, \mathbb{C}) \cong \mathbb{C}^* = \mathbb{C} \setminus \{0\}$

Доказательство. Зададим $f : \mathrm{GL}(n, \mathbb{C}) \longrightarrow \mathbb{C}^* : \quad f(A) = \det A$.
Ясно, что f — гомоморфизм: $f(AB) = \det AB = \det A \det B = f(A)f(B)$.
Очевидно, что $\forall z \in \mathbb{C}^* \; \exists A \in \mathrm{GL}(n, \mathbb{C}) : \det A = z$.
К тому же $\mathrm{Ker}\, f = \{A : \det A = 1\} = \mathrm{SL}(n, \mathbb{C})$.
По теореме о гомоморфизме $\mathrm{GL}(n, \mathbb{C})/\mathrm{SL}(n, \mathbb{C}) \cong \mathbb{C}^*$. □

Задача 1.2.12. $\mathbb{R}^*/\mathbb{R}_{>0} \cong \mathbb{Z}_2$

Доказательство. Зададим $f : \mathbb{R}^* \longrightarrow \mathbb{Z}_2 : \quad f(x) = \mathrm{sgn}(x) = \begin{cases} 1, & \text{если } x > 0; \\ -1, & \text{если } x < 0; \end{cases} \forall x \in \mathbb{R}^*$.
Так как $f(xy) = \mathrm{sgn}(xy) = \mathrm{sgn}(x)\,\mathrm{sgn}(y) = f(x)f(y) \quad \forall x, y \in \mathbb{R}^*$, то f — гомоморфизм; $\mathrm{Ker}\, f = \mathbb{R}_{>0}$. □

Задача 1.2.13. $\mathbb{C}^*/\mathbb{R}_{>0} \cong \mathbf{U}$

Доказательство. Зададим $f : \mathbb{C}^* \longrightarrow \mathbf{U} : \quad z \longmapsto \frac{z}{|z|}$.
Пусть $z_1, z_2 \in \mathbb{C}^*$. Тогда $f(z_1 z_2) = \frac{z_1 z_2}{|z_1 z_2|} = \frac{z_1}{|z_1|}\frac{z_2}{|z_2|} = f(z_1)f(z_2) \Rightarrow f$ — гомоморфизм. $\mathrm{Ker}\, f = \{\frac{z}{|z|} = 1\} = \mathbb{R}_{>0}$. □

Задача 1.2.14. $\mathbb{C}^*/\mathbf{U} \cong \mathbb{R}_{>0}$

Доказательство. $f : \mathbb{C}^* \longrightarrow \mathbb{R}_{>0} : \quad f(z) = |z|$. □

Задача 1.2.15. $\mathbf{U}/\mathbf{U}_n \cong \mathbf{U}$

Доказательство. $f : \mathbf{U} \longrightarrow \mathbf{U} : \quad z \longmapsto z^n$. □

Задача 1.2.16. $\mathbb{R}/\mathbb{Z} \cong \mathbf{U}$

Доказательство. Зададим $f : \mathbb{R} \longrightarrow \mathbf{U} : \quad f(x) = e^{i2\pi x} = \cos 2\pi x + i \sin 2\pi x,\ x \in \mathbb{R}$.
В группе $\mathbb{R}$ операция — сложение. Тогда $f(x+y) = e^{i2\pi(x+y)} = e^{i2\pi x + i2\pi y} = e^{i2\pi x} e^{i2\pi y} = f(x)f(y) \Rightarrow$ f — гомоморфизм. Найдем ядро: $e^{i2\pi x} = 1 \Leftrightarrow x \in \mathbb{Z}$. То есть $\operatorname{Ker} f = \mathbb{Z}$. □

Задача 1.2.17. $\mathbb{C}^*/\mathbf{U}_n \cong \mathbb{C}^*$

Доказательство. $f : \mathbb{C}^* \longrightarrow \mathbb{C}^* : \quad z \longmapsto z^n$. □

Задача 1.2.18. $\mathbb{C}^*/\mathbf{H}_n \cong \mathbf{U}$

Доказательство. $f : \mathbb{C}^* \longrightarrow \mathbf{U} : \quad z \longmapsto (\frac{z}{|z|})^n$. □

Задача 1.2.19. $\mathbf{H}_n/\mathbb{R}_{>0} \cong \mathbf{U}_n$

Доказательство. $f : \mathbf{H}_n \longrightarrow \mathbf{U}_n : \quad f(z) = \frac{z}{|z|}$. □

Задача 1.2.20. $\mathbf{H}_n/\mathbf{U}_n \cong \mathbb{R}_{>0}$

Доказательство. $f : \mathbf{H}_n \longrightarrow \mathbb{R}_{>0} : \quad z \longmapsto |z| \in \mathbb{R}_{>0}$. □

Задача 1.2.21. $\mathrm{GL}(n,\mathbb{R})/\{X \in \mathrm{GL}(n,\mathbb{R}) \mid \det X > 0\} \cong \mathbf{U}_2$

Доказательство. $f : \mathrm{GL}(n,\mathbb{C}) \longrightarrow \mathbf{U}_2 : \quad X \longmapsto \operatorname{sgn}(\det X)$. □

1.3 Действие группы на множестве

Пусть X – множество. Множество $S(X)$ биекций X на себя превращается в группу если в качестве умножения взять операцию композиции отображений. Единицей группы служит тождественное отображение $\mathrm{id}\colon X \to X$.

Если множества X и Y эквивалентны (имеют одинаковую мощность) и $\phi\colon X \to Y$ – биективное отображение, то $\Phi\colon S(X) \to S(Y)$ заданное формулой

$$\Phi(f) := \phi \circ f \circ \phi^{-1},\ f \in S(X),$$

является изоморфизмом групп. Действительно, ясно, что $\Phi(f) \in S(X)$ и что Φ – биекция, кроме того,

$$\Phi(f\circ g) := \phi\circ(f\circ g)\circ\phi^{-1} = (\phi\circ f\circ\phi^{-1})\circ(\phi\circ g\circ\phi^{-1}) = \Phi(f)\circ\Phi(g),\ f,g \in S(X),$$

так что $\Phi\colon S(X) \to S(Y)$ – изоморфизм.

В частности, если $|X| = n$, то $S(X) \cong S_n$.

1.3.1 Левые и правые действия

Определение 1.3.1. Левое действие группы G на множестве X – это гомоморфизм $G \to S(X)$. Правое действие – гомоморфизм $G \to S(X)^{\mathrm{o}}$ в дуальную группу. Обычно рассматривают левые действия, которые называют просто действиями.

Напомним, что у дуальной группы G^{o} те же элементы и та же единица, что и у самой группы G, но другое умножение, которое определяется фомулой: $g * h := hg$, а отображение $g \mapsto g^{-1}$ дает изоморфизмы $G \to G^{\mathrm{o}}$ и $G^{\mathrm{o}} \to G$.

Если $\alpha\colon G \to S(X)$ – действие (т. е. левое действие), то $\alpha(g)x$ обычно обозначают через $g \cdot x$ или еще проще gx, где $g \in G$ и $x \in X$. Поскольку α – гомоморфизм, имеем $\alpha(e)x = x$ и $\alpha(g_1g_2)x = (\alpha(g_1)\circ\alpha(g_2))(x) = \alpha(g_1)(\alpha(g_2)x)$, что в упрощенных обозначениях приобретает вид:

1. $ex = x$,
2. $(g_1g_2)x = g_1(g_2x)$.

Поэтому можно дать эквивалентное определение: действие (т. е. левое действие) G на X – это отображение $G \times X \to X$, $(g, x) \mapsto gx$, удовлетворющее условиям 1 и 2.

Аналогичные формулы для правого действия таковы:
1. $xe = x$,
2. $x(g_1 g_2) = (xg_1)g_2$.

Имея правое действие на множестве можно определить левое действие и наоборот. Например, имея левое действие мы можем определить правое действие формулой: $xg := g^{-1}x$. Аналогично, по правому действию можно ввести левое: $gx := xg^{-1}$.

Отметим, что действие группы $S(X)$ на X состоит в нахождении образа элемента: $S(X) \times X \to X$, $(f, x) \mapsto f(x)$.

Определение 1.3.2. Действие называется тривиальным, если $gx = x$ для любых $g \in G$ и $x \in X$.

Иными словами, действие $\alpha\colon G \to S(X)$ тривиально, если $\operatorname{Ker}\alpha = G$.

Определение 1.3.3. Действие называется эффективным (или точным), если из того, что $gx = x$ для любого $x \in X$ следует, что $g = e$.

Иными словами, действие G на X эффективно (точно), если $\alpha\colon G \to S(X)$ – мономорфизм.

Примеры 1.3.1. 1. Пусть X и Y – G-множества с действиями, обозначаемыми как $(g, x) \mapsto gx$, $(g, y) \mapsto gy$, где $g \in G$, $x \in X$, $y \in Y$. Обозначим через $M(X, Y) = Y^X$ множество отображений из X в Y. Тогда $M(X, Y)$ становится G-множеством, если определить действие $(g, f) \mapsto g \cdot f$ формулой $(g \cdot f)(x) := gf(g^{-1}x)$.

В частности, если считать, что G действует тривиально на $\mathbb{R}$ и $\mathbb{C}$, то множества вещественно- и комплексно-значных функций $M(X, \mathbb{R})$ и $M(X, \mathbb{C})$ превращаются в G-множества с действием $(g, f) \mapsto gf$, где $(gf)(x) := f(g^{-1}x)$. Эта же формула задает действие на $M(X, Y) = Y^X$, если на Y считать действие группы G тривиальным.

2. Определим отображения $L_g, R_g\colon G \to G$ – левый и правый сдвиги на элемент $g \in G$ формулами $L_g(h) := gh$, $R_g(h) := hg$, $h \in G$. Эти отображения – биекции, поэтому $L_g, R_g \in S(G)$. Отметим также, что левые и правые сдвиги коммутируют между собой, т. е. $L_{g_1} \circ R_{g_2} = R_{g_2} \circ L_{g_1}$ для любых $g_1, g_2 \in G$.

Имеем

$$L_{g_1g_2}(h) = (g_1g_2)h = g_1(g_2h) = g_1L_{g_2}(h) = L_{g_1}(L_{g_2}(h)) = (L_{g_1}\circ L_{g_2})(h).$$

Следовательно, $L_{g_1g_2} = L_{g_1} \circ L_{g_2}$, т. е. отображение $L : G \to S(G)$, определенное формулой $L(g) := L_g,\ g \in G$, является гомоморфизмом. Кроме того, $L_g = \mathrm{id}$ только если $g = e$, поэтому L – мономорфизм или – точное действие. По теореме о гомоморфизме группа G изоморфна образу мономорфизма L, т. е. ее можно считать подгруппой группы $S(G)$. Это утверждение называется теоремой Кэли. Если G конечна и $|G| = n$, то ее можно считать подгруппой симметрической группы S_n.

Аналогично, поскольку $R_{g_1g_2} = R_{g_2} \circ R_{g_1}$, возникает точное правое действие $R\colon G \to S(G)^{\mathrm{o}},\ R(g) := R_g$.

3. Поскольку $g \mapsto R_g$ – правое действие, $g \mapsto R_{g^{-1}}$ – действие (т. е. левое действие). В силу того, что левые и правые сдвиги коммутируют, получаем, что $g \mapsto i_g := L_g \circ R_{g^{-1}}$ – тоже действие. Это действие называется действием сопряжениями. Элементы $h \in G$ и $i_g(h) = (L_g\circ R_{g^{-1}})(h) = ghg^{-1}$ группы G называются сопряженными.

Это действие продолжается до действия на множестве подгрупп группы G. Подгруппа H при действии элемента $g \in G$ переходит в

$$i_g(H) = gHg^{-1} = \{ghg^{-1} \mid h \in H\}.$$

Нетрудно видеть, что gHg^{-1} – подгруппа группы G. Подгруппы H и gHg^{-1} называются сопряженными. Ясно также, что подгруппа $H < G$ нормальна в том и только в том случае, когда $i_g(H) = H$ для дюбого $g \in G$.

Нетрудно показать также, что биекция $i_g\colon G \to G$ для любого $g \in G$ на самом деле является автоморфизмом (обратное отображение – это автоморфизм $i_{g^{-1}}$). Такие автоморфизмы называются внутренними. Множество $\mathrm{Int}\ G$ всех внутренних автоморфизмов является группой, поскольку $i_e = \mathrm{id}_G$, $i_g\circ i_h = i_{gh}$ и $(i_g)^{-1} = i_{g^{-1}}$. Таким образом, $\mathrm{Int}\ G$ – подгруппа группы всех автоморфизмов $\mathrm{Aut}\ G$. Эта подгруппа на самом деле является нормальной подгруппой, т.е. $\mathrm{Int}\ G \trianglelefteq \mathrm{Aut}\ G$. Действительно, пусть $f \in \mathrm{Aut}\ G$, тогда

$$f \circ i_g \circ f^{-1} = i_{f(g)},$$

поскольку для любого $x \in G$ имеем:

$$(f \circ i_g \circ f^{-1})(x) = f(i_g(f^{-1}(x))) = f(gf^{-1}(x)g^{-1}) =$$
$$= f(g)f(f^{-1}(x))f(g^{-1}) = f(g)xf(g)^{-1} = i_{f(g)}(x).$$

Факторгруппу $\mathrm{Int}\ G/\mathrm{Aut}\ G$ называют группой внешних автоморфизмов.

Подробнее действие сопряжениями будет изучаться ниже.

1.3.2 Орбиты и стационарные подгруппы

Определение 1.3.4. Множество $Gx = \{gx \,|\, g \in G\}$ называется орбитой точки $x \in X$. Если орбита – конечное множество, то число ее элементов $|Gx|$ называют длиной орбиты Gx.

Орбиты либо не пересекаются, либо полностью совпадают.

Определение 1.3.5. Множество орбит обозначается X/G и называется фактормножеством множества X по действию группы G.

Определение 1.3.6. Действие называется транзитивным, если имеется ровно одна орбита, т. е. $|X/G| = 1$. Иными словами $X = Gx \ \forall\, x \in X$.

Определение 1.3.7. Пусть X и Y – G-множества. Отображение $f\colon X \to Y$ называется эквивариантным (или G-отображением), если $f(gx) = gf(x)\ \forall\, x \in X,\ \forall\, g \in G$.

Если G-отображение является биекцией, то легко видеть, что обратное отображение также является эквивариантной биекцией. В этом случае мы будем называть G-множества X и Y G-эквивалентными (G-изоморфными), а само отображение f G-эквивалентностью или G-изоморфизмом. Ясно, что в этом случае множества эквивалентны (имеют одинаковую мощность), а само понятие эквивалентности множеств для единичной группы $G = \{e\}$ совпадает с понятием G-эквивалентности.

Определение 1.3.8. Стабилизатором точки x (стационарной подгруппой точки) называется подгруппа $G_x = \mathrm{St}_x := \{g \in G \,|\, gx = x\}$.

Легко видеть, что G_x действительно является подгруппой.

Предложение 1.3.2. Отображение $f\colon Gx \to G/G_x$ переводящее gx в gG_x корректно определено и является G-эквивалентностью.

Предложение 1.3.3. Если группа G конечна, то $|Gx| = |G : G_x| = \frac{|G|}{|G_x|}$.

Предложение 1.3.4. Имеем $G_{gx} = gG_xg^{-1} = i_g(G_x)$. Таким образом, стабилизаторы точек из одной и той же орбиты являются сопряженными подгруппами.

1.3.3 Действия сопряжением

Положим $i_g(h) := ghg^{-1} = (L_g \circ R_{g^{-1}})(h)$, где $h, g \in G$. Отображение $i_g \colon G \to G$ является биекцией как композиция биекций $L_g \circ R_{g^{-1}}$. Это легко проверить и непосредственно – поскольку $h = i_g(g^{-1}hg)$, отображение i_g сюръективно, а из равенства $i_g(h) = i_g(h')$ следует, что $h = h'$, т. е. i_g инъективно.

Далее

$$i_g(h_1h_2) := gh_1h_2g^{-1} = gh_1g^{-1} \cdot gh_2g^{-1} = i_g(h_1)i_g(h_2).$$

Следовательно, i_g является автоморфизмом, т. е. изоморфизмом группы G на себя. Автоморфизмы вида i_g называются внутренними. Определим отображение $i \colon G \to \mathrm{Aut}(G)$ в группу автоморфизмов $\mathrm{Aut}(G)$ группы G формулой $i(g) := i_g$. Поскольку

$$i_{gg'}(h) = gg'h(gg')^{-1} = gg'hg'^{-1}g^{-1} = gi_{g'}(h)g^{-1} = i_g(i_{g'}(h)) = (i_g \circ i_{g'})(h),$$

$i \colon G \to \mathrm{Aut}(G)$ – гомоморфизм. Ядро $\mathrm{Ker}\, i$ состоит из элементов перестановочных со всеми элементами группы. Следовательно, $\mathrm{Ker}\, i$ совпадает с центром группы $Z(G) := \{z \in G \mid zg = gz \ \ \forall g \in G\}$.

Положим $\mathrm{Int}\, G := \{i_g \mid g \in G\}$. Поскольку $\mathrm{Inn}\, G = \mathrm{Im}\, i = i(G)$, а образ гомоморфизма является подгруппой, $\mathrm{Int}\, G$ – подгруппа в $\mathrm{Aut}(G)$. Она называется подгруппой внутренних автоморфизмов. Покажем, что $\mathrm{Int}\, G$ – нормальная подгруппа в $\mathrm{Aut}(G)$.

Пусть $\varphi \colon G \to G$ – автоморфизм. Покажем, что $\varphi \circ i_g \circ \varphi^{-1}$ – внутренний автоморфизм. Имеем

$$(\varphi \circ i_g \circ \varphi^{-1})(h) = \varphi(i_g(\varphi^{-1}(h))) = \varphi(g(\varphi^{-1}(h))g^{-1}) =$$
$$= \varphi(g)\varphi(\varphi^{-1}(h))\varphi(g^{-1}) = \varphi(g)h\varphi(g)^{-1} = i_{\varphi(g)}(h),$$

т. е. $\varphi \circ i_g \circ \varphi^{-1} = i_{\varphi(g)} \in \mathrm{Inn}\, G$.

Факторгруппа $\mathrm{Aut}(G)/\mathrm{Int}\, G$ называется группой внешних автоморфизмо

Поскольку $\mathrm{Aut}(G) \subset S(G)$, можно рассматривать i как гомоморфизм $G \to S(G)$, т. е. как действие G на себе, действие сопряжением. Орбиты этого действия называются классами сопряженных элементов. Орбиту элемента $x \in G$ обозначим как $C(x) := \{gxg^{-1} \mid g \in G\}$.

Если $H < G$ – подгруппа, то gHg^{-1} – подгруппа в G. Эти подгруппы называются сопряженными. Таким образом, G действует сопряжениями на множестве подгрупп. Орбиты – классы сопряженных подгрупп. Орбитой подгруппы H является множество подгрупп $\{gHg^{-1} \mid g \in G\}$.

Определение 1.3.9. $Z(x) := \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$ называется централизатором элемента $x \in G$. Легко видеть, что централизаторы элементов являются подгруппами в G.

Определение 1.3.10. Нормализатором подгруппы H в G называется

$$N(H) := \{g \in G \mid gH = Hg\} = \{g \in G \mid gHg^{-1} = H\}.$$

Нормализатор – подгруппа в G и H – нормальная подгруппа в $N(H)$.

Теорема 1.3.5. Мощность множества элементов группы G, сопряженных с элементом $x \in G$ равна $|G : Z(x)|$ – индексу централизатора элемента x. Мощность множества подгрупп группы G, сопряженных с подгруппой H группы G, равна $|G : N(H)|$ – индексу нормализатора подгруппы H в G.

Доказательство. При действии сопряжением орбитой точки $x \in G$ является класс сопряженных элементов $C(x) = \{gxg^{-1} \mid g \in G\}$. Покольку стабилизатором точки x является как раз централизатор $Z(x)$ элемента x, мощность множества элементов группы G, сопряженных с $x \in G$ равна $|G : Z(x)| = |G|/|Z(x)|$.

Аналогично, G действует сопряжениями на множестве подгрупп группы G, причем орбитой подгруппы H является множество подгрупп вида $\{gHg^{-1} \mid g \in G\}$ – класс подгрупп сопряженных с H. Стабилизатором точки H является нормализатор $N(H)$. Поэтому мощность множества подгрупп группы G, сопряженных с подгруппой H, равна индексу нормализатора $|G : N(H)| = |G|/|N(H)|$. □