А. Ю. Воловиков • Ю. О. Головин • К. В. Цыганов

Лекции и семинары по теории групп

2014

Оглавление

1 | Начало

1.1 Группа, порядок элемента, порядок группы, подгруппа

1.1.1 Лекция

Определение 1.1.1. *Группоид* := множество с определенной на нем бинарной операцией.

Определение 1.1.2. *Полугруппа* := группоид + ассоциативность операции.

Определение 1.1.3. *Моноид* G := полугруппа + единичный (нейтральный) элемент e, то есть такой, что $\forall g \in G$ выполнено $ge = eg = g$.

Определение 1.1.4. 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 1.1.5. *Группа* := моноид, в котором все элементы обратимы.

Определение 1.1.6. Группа, состоящая из конечного числа элементов, называется *конечной* группой. Иначе — *бесконечной*.

Определение 1.1.7. Число элементов в конечной группе называется *порядком группы* и обозначается $|G|$.

Определение 1.1.8. 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 1.1.9. 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 будем обозначать $H < G$.

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

Определение 1.1.10. Группа с коммутативной операцией называется *коммутативной* или *абелевой*.

Определение 1.1.11. *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 1.1.1. Единичный элемент e — единственный.

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

Задача 1.1.2. 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 1.1.3. 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 1.1.4. 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 1.1.5. 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 $x^n x^m = x^{-k} \cdot x^{-l} = (x^{-1})^k \cdot (x^{-1})^l =$ (см. случай 1)) $= (x^{-1})^{k+l} = x^{-(k+l)} = x^{n+m}$; 3) $n > 0, m < 0, n+m \geq 0$, тогда $x^n x^m =$ (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 $x^n x^m =$ (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 1.1.6. 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 1.1.7. 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 1.1.8. 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 $x = (yy^{-1})x(yy^{-1}) = (y^{-1})^{-1}(y^{-1}xy)y^{-1}$, $|x| \leqslant |y^{-1}xy|$. □

Задача 1.1.9. Пусть $x, y \in G$. Тогда $|xy| = |yx|$.

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

Задача 1.1.10. 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 1.1.11. 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 1.1.12. 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 1.1.13. 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 1.1.14. 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 1.1.15. 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 1.1.16. 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 $\dfrac{m}{(k,m)} = \dfrac{n}{(k,n)}$; $m(k, n) = n(k, m)$. 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 1.1.12. *Периодической частью группы* G называется множество $T(G) = \{g \in G, |g| < \infty\}$.

Задача 1.1.17. 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. □

1.2 Подстановки, теорема Кэли

1.2.1 Лекция

Определение 1.2.1. *Перестановкой* длины (степени) n называется последовательность чисел $1, 2, \ldots, n$, записанных в произвольном порядке. Всего имеется $n!$ перестановок.

Определение 1.2.2. *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 1.2.1. 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 1.2.3. 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 1.2.4. 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 1.2.5. Пусть подстановка σ имеет k инверсий. Тогда число $(-1)^k$ будем называть *знаком подстановки* σ и обозначать $\mathrm{sgn}(\sigma)$. Таким образом, если σ — четная подстановка, то $\mathrm{sgn}(\sigma) = 1$, а если нечетная, то $\mathrm{sgn}(\sigma) = -1$.

Пример 1.2.2. 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 1.2.3.

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

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

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

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

Таким образом, мы получили все свойства группы:

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

Определение 1.2.6. 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 1.2.7. Подстановки, записанные в виде цикла, так и называются — *циклами*.

Определение 1.2.8. Два цикла называются *независимыми*, если у них нет общих элементов.

Легко заметить, что независимые циклы коммутируют.

Определение 1.2.9. *Транспозицией* называется цикл длины 2.

Пример 1.2.4. 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 1.2.5. ***(Теорема Кэли)*** *Любая конечная группа порядка n изоморфна некоторой подгруппе S_n.*

1.2.2 Семинар

Задача 1.2.6. Как должны быть расположены числа в перестановке, чтобы инверсий было наибольшее количество ?

Решение. В порядке убывания. ◀

Задача 1.2.7. 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 1.2.8. 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 1.2.9. 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 1.2.10. 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 1.2.11. 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 1.2.12. Пусть $\alpha=(i_1\dots i_k)$. Тогда $\beta\alpha\beta^{-1}=(\beta(i_1)\beta(i_2)\dots\beta(i_k))$.

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

Задача 1.2.13. Доказать, что любую подстановку можно представить следующими способами:

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

Доказательство.

1. $(i_1i_2\dots i_k)=(i_1i_2)(i_2i_3)\dots(i_{k-1}i_k)$

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. Для простоты восприятия рассмотрим 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.

□

Задача 1.2.14. 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). □

Определение 1.2.10. Группа всех четных подстановок называется знакопеременной группой и обозначается A_n.

Задача 1.2.15. 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:
$(i_1i_2)(i_1i_3) = (i_1i_3i_2), (i_1i_2)(i_3i_4) = (i_1i_4i_3)(i_1i_2i_3)$. □

Задача 1.2.16. 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 $(a_1a_2\ldots a_{15})$ нечетная, то получить "правильное"расположение (на рисунке ниже) невозможно.

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

Задача 1.2.17. Выяснить, как изменится разложение подстановки в произведение независимых циклов при умножении ее (с обеих сторон) на произвольную транспозицию.

1.3 Морфизмы.

1.3.1 Лекция

Определение 1.3.1. 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 1.3.2. $\operatorname{Ker}\phi = \{g \in G : \phi(g) = e_H\}$ — *ядро* гомоморфизма ϕ.

Определение 1.3.3. $\operatorname{Im}\phi = \{h \in H : \exists g \in G : \phi(g) = h\}$ — *образ* гомоморфизма ϕ.

Определение 1.3.4. 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 1.3.5. Гомоморфизм $\phi : G \longrightarrow H$ называется *эпиморфизмом*, если $\operatorname{Im}\phi = H$.

Определение 1.3.6. Гомоморфизм $\phi : G \longrightarrow H$ называется *изоморфизмом*, если он является мономорфизмом и эпиморфизмом.

Определение 1.3.7. Если существует изоморфизм $\varphi : G \longrightarrow H$, то группы G и H называются изоморфными. Этот факт обозначается так: $G \cong H$.

Определение 1.3.8. Гомоморфизм $\phi : G \longrightarrow G$ называется *эндоморфизмом*.

Определение 1.3.9. Изоморфизм $\phi : G \longrightarrow G$ называется *автоморфизмом*.

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

Предложение 1.3.2. *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 1.3.3. *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 1.3.4. *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 1.3.5. 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:
$(f_1 f_2)(g_1 g_2) = f_1(f_2(g_1 g_2)) = f_1(f_2(g_1) f_2(g_2)) = f_1(f_2(g_1)) f_1(f_2(g_2)) = (f_1 f_2)(g_1)(f_1 f_2)(g_2) \Rightarrow f_1 f_2$ — 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 1.3.6. *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 $i_g(h_1 h_2) = g(h_1 h_2)g^{-1} = gh_1 e h_2 g^{-1} = gh_1(g^{-1}g)h_2 g^{-1} = (gh_1 g^{-1})(gh_2 g^{-1}) = i_g(h_1) i_g(h_2) \Rightarrow i_g$ — 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 1.3.10. Автоморфизм называется *внутренним*, если он имеет вид $i_g(h) = ghg^{-1}$.

Предложение 1.3.7. *Множество всех внутренних автоморфзмов группы G образует группу относительно суперпозиции, которая обозначается* $\operatorname{Int} G$. *Тем самым,* $\operatorname{Int} G < \operatorname{Aut} G$.

Доказательство. $(i_{g_1} i_{g_2})(h) = i_{g_1}(i_{g_2}(h)) = i_{g_1}(g_2 h g_2^{-1}) == g_1 g_2 h g_2^{-1} g_1^{-1} = (g_1 g_2) h (g_1 g_2)^{-1} = i_{g_1 g_2}(h) \Rightarrow i_{g_1} i_{g_2} = i_{g_1 g_2}$.
$i_e(h) = ehe^{-1} = h \Rightarrow i_e = id \in \operatorname{Int} G$ — единичный элемент.
$i_g i_{g^{-1}} = i_{gg^{-1}} = i_e = id$,то есть $(i_g)^{-1} = i_{g^{-1}}$ □

Задача 1.3.8. Если G – абелева, то существует единственный внутренний автоморфизм — тождественный.

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

Предложение 1.3.9. *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 1.3.10. 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 1.3.11. Доказать, что все группы 2-го порядка изоморфны между собой.

Доказательство. $|G| = 2$. Пусть g элемент группы и e единичный элемент. Тогда $ee = e, eg = ge = g$ и остается задать только $g \cdot g$. Если $g \cdot g = g = ge$,то $g = e$. Получили противоречие (т.к. группа второго порядка). Значит, $g^2 = e$. Следовательно, существует только одна группа, содержащая 2 элемента. □

Задача 1.3.12. Доказать, что все группы 3-го порядка изоморфны между собой.

Доказательство. Пусть e, g, h элементы группы. Нужно задать таблицу умножения gh, hg, gg, hh. Если $gh = g$, то $h = e$ противоречие (в группе должно быть 3 различных элемента). Аналогично, если $gh = h$, то $g = e$ противоречие. Значит, $gh = e$ и точно так же $hg = e$. 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 , содержащая три элемента . □

Задача 1.3.13. 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 1.3.14. 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 n-угольного диэдра (многоугольника), включающая как вращения, так и осевые симметрии.

Определение 1.3.11. Группа $\mathbb{Z}_n = (\mathbb{Z}_n, +) = \{0, 1, \ldots, n-1\}$ называется *группой вычетов по модулю* n.

Задача 1.3.15. Доказать, что все группы простого порядка — изоморфны между собой.

Доказательство. Следует из двух предыдущих задач. □

Задача 1.3.16. 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 1.3.17. 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. □

Задача 1.3.18. Доказать, что группы $(\mathbb{Z}, +)$ и $(n\mathbb{Z}, +)$ изоморфны.

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

Задача 1.3.19. Доказать, что $(\mathbb{Z}_4, +)$ изоморфна $(\mathbb{Z}_5^*, \cdot)$.

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

Определение 1.3.12. *Группой движений Клейна* называется группа самосовмещений ромба. Она обозначается V_4.

Задача 1.3.20. Привести пример плоских геометрических фигур, группы движений которых изоморфны :

1. $\mathbb{Z}_2$ — отрезок (тождественный и симметрия относительно центр); две точки (на прямой); равнобедренный, но не равносторонний треугольник (на плоскости);
2. $\mathbb{Z}_3 \cong A_3$
3. $S_3 \cong D_3$

2 | Факторизация и изоморфизмы

2.1 Отношение эквивалентности, факторизация

2.1.1 Лекция

Определение 2.1.1. Мы говорим, что задано *отношение* на множестве M, если задано подмножество $T \subseteq M \times M = \{(m_1, m_2)\}$.

Определение 2.1.2. *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 2.1.1. *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, $T_x = T_y$. □

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 2.1.2. 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 2.1.3. $xH = \{xh \mid h \in H\}$ 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 2.1.3. ***(Теорема Лагранжа)*** *Порядок подгруппы делит порядок конечной группы.*

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

Задача 2.1.4. 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 2.1.5. $G = S_3 = \{e,\ (12),\ (13), (23),\ (123),\ (132)\}$; $H =< (12) >= \{e,\ (12)\}$.
$eH = (12)H$; $(123)H = (13)H = \{(13),\ (123)\}$; $e(123)H = (123)H \neq (12)(13)H = \{(132),\ (23)\}$

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 факторможестве, 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

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

Ну а оно равносильно равенству

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

Что и означает совпадение левых и правых смежных классов.

Определение 2.1.4. 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 2.1.6. 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 2.1.7. $D_3 \cong S_3$

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 2.1.8. 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 2.1.9. 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 2.1.10. 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 2.1.5. Подгруппа $H < G : |H| = \frac{|G|}{k}$ называется *подгруппой индекса* k.

Задача 2.1.11. 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 2.1.12. 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 2.1.13. Привести пример такого гомоморфизма $\phi : G_1 \longrightarrow G_2$, что $\mathrm{Im}\,\phi$ не является нормальной подгруппой G_2.

Определение 2.1.6. Пусть A и B — два подмножества группы G. Их произведением назовем множество $AB = \{ab \mid a \in A, b \in B\}$.

Задача 2.1.14. 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 2.1.15. 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, $g(h_1h_2)g^{-1} = \underbrace{(gh_1g^{-1})}_{\in H_1}\underbrace{(gh_2g^{-1})}_{\in H_2} \in H_1H_2$. □

2.2 Теорема о гомоморфизме

2.2.1 Лекция

Определение 2.2.1. *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 2.2.1. $G/\{e\} = G$ и $G/G = \{e\}$; $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n = \{0, 1, \ldots, n-1\}$

Теорема 2.2.2. ***(Теорема о гомоморфизме)***
Пусть $f : G \longrightarrow F$ — гомоморфизм. Тогда $G/\operatorname{Ker} f \cong \operatorname{Im} f$.

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 2.2.3. *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 2.2.4. $S_n/A_n \cong U_2 \ (= \{-1, \ 1\} \cong C_2)$

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 2.2.5. $S_4/V_4 \cong S_3$

Доказательство. Сперва докажем, что $V_4 \lhd S_4$, непосредственно проверив совпадение левых и правых смежных классов:
$V_4 = \{e, \ (12)(34), \ (13)(24), \ (14)(23)\}$;
$(12)V_4 = (34)V_4 = (1324)V_4 = (1423)V_4 = V_4(12) = \ldots = \{(12), \ (34), \ (1324), \ (1423), \}$ (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 2.2.6. ***(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.

□

Пример 2.2.7. 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
$$S_4/V_4 \cong TV_4/V_4 \cong T/T \cap V_4 = T/\{e\} \cong T \cong S_3.$$

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

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

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

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

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

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

Задача 2.2.13. $\mathbf{U}/\mathbf{U}_n \cong \mathbf{U}$

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

Задача 2.2.14. $\mathbb{R}/\mathbb{Z} \cong \mathbf{U}$

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 $\mathrm{Ker}\, f = \mathbb{Z}$. □

Задача 2.2.15. $\mathbb{C}^*/\mathbf{U}_n \cong \mathbb{C}^*$

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

Задача 2.2.16. $\mathbb{C}^*/\mathbf{H}_n \cong \mathbf{U}$

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

Задача 2.2.17. $\mathbf{H}_n/\mathbb{R}_{>0} \cong \mathbf{U}_n$

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

Задача 2.2.18. $\mathbf{H}_n/\mathbf{U}_n \cong \mathbb{R}_{>0}$

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

Задача 2.2.19. $\mathrm{GL}(n,\mathbb{R})/\{X \in \mathrm{GL}(n,\mathbb{R}) \mid \det X > 0\} \cong \mathbf{U}_2$

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

2.3 Коммутант и центр

2.3.1 Лекция

Определение 2.3.1. *Коммутатором* элементов a, b называют $[a, b] = aba^{-1}b^{-1}$.

Определение 2.3.2. *Коммутантом* G' (или $K(G)$) группы G называется множество всевозможных произведений коммутаторов группы G.

Предложение 2.3.1. $G' \lhd G$

Доказательство. Сначала докажем, что $G' < G$.
Произведение двух коммутаторов, по определению, лежит в G'.
$[a, b]^{-1} = [b, a]$, так как $[a, b][b, a] = (aba^{-1}b^{-1})(bab^{-1}a^{-1}) = e$. Если $a \in G'$, то $a = k_1k_2 \cdot \ldots \cdot k_m$, где все k_i — коммутаторы. Тогда $a^{-1} = (k_1k_2 \cdot \ldots \cdot k_m)^{-1} = k_m^{-1} \cdot \ldots \cdot k_2^{-1}k_1^{-1}$, и так как k_i^{-1} — коммутаторы, то $a^{-1} \in K(G)$. Вообще, раз произведение двух элементов из G' лежит в G', и для любого элемента обратный тоже лежит в G', то единичный автоматически лежит в G'. Но можно и явно проверить: $[e, e] = eee^{-1}e^{-1} = e$.
Теперь докажем нормальность G'.
Пусть $g \in G, k = [a, b] = aba^{-1}b^{-1}$. Тогда $gkg^{-1} = gaba^{-1}b^{-1}g^{-1} = (gag^{-1})(gbg^{-1})(ga^{-1}g^{-1})(gb^{-1}g^{-1}) = (gag^{-1})(gbg^{-1})(gag^{-1})^{-1}(gbg^{-1})^{-1}$ — тоже коммутатор. Пусть $a \in G', a = k_1k_2 \cdot \ldots \cdot k_m$, где все k_i — коммутаторы. Тогда $gag^{-1} = g(k_1k_2 \cdot \ldots \cdot k_n)g^{-1} = (gk_1g^{-1})(gk_2g^{-1}) \cdot \ldots \cdot (gk_ng^{-1})$ является произведением коммутаторов и, следовательно, содержится в коммутанте G'. □

Предложение 2.3.2. *Пусть G — группа. Тогда $G' = \{e\} \Leftrightarrow G$ — коммутативна.*

Доказательство. $[a, b] = aba^{-1}b^{-1} = e \Leftrightarrow ab = ba$ □

Предложение 2.3.3. *Если $\varphi : G \longrightarrow H$ — гомоморфизм, то $\varphi(G') \subseteq H'$ и $\varphi^{-1}(H') \supseteq G'$.*

Доказательство. Если g_1 и g_2 – произвольные элементы группы G и $\varphi(g_1) = h_1, \varphi(g_2) = h_2$, то $\varphi(g_1^{-1}) = h_1^{-1}, \varphi(g_2^{-1}) = h_2^{-1}$. Отсюда $\varphi(g_1g_2g_1^{-1}g_2^{-1}) = \varphi(g_1)\varphi(g_2)\varphi(g_1^{-1})\varphi(g_2^{-1}) = h_1h_2h_1^{-1}h_2^{-1}$, т.е образ любого коммутатора в группе G является коммутатором в группе H. Любой элемент коммутанта G' представим в виде $g_1'g_2' \ldots g_n'$, где g_i' – коммутаторы. Элемент $\varphi(g_1'g_2' \ldots g_n') = \varphi(g_1')\varphi(g_2') \ldots \varphi(g_n')$ является произведением коммутаторов в группе H и, следовательно, содержится в коммутанте H'. Значит, $\varphi(G') \subseteq H'$. Отсюда вытекает также, что $\varphi^{-1}(H') \supseteq G'$. Если $\varphi(G) = H$, то $\varphi(G') = H'$. □

Теорема 2.3.4.

1. *Любая подгруппа $H < G$, содержащая коммутант G' группы G, нормальна.*
2. *Факторгруппа G/G' — коммутативна.*
3. *Факторгруппа G/H коммутативна тогда и только тогда, когда G' содержится в H.*

Доказательство.

1. Если $x \in H, g \in G$ и $H \supseteq G'$, то $gxg^{-1} = (gxg^{-1}x^{-1})x = [g, x]x \in G'H = H$. Значит, $H \lhd G$.
2. Рассмотрим естественный гомоморфизм $\varphi : G \longrightarrow G/G'$. Тогда $(G/G')' = \varphi(G') = \{e\}$ и, значит, группа G/G' коммутативна.
3. ($\Leftarrow$) Из того, что $H \lhd G$ и $G' \subseteq H$, следует, что $[aH, bH] = (aH) \cdot (bH) \cdot (a^{-1}H) \cdot (b^{-1}H) = (aba^{-1}b^{-1})H = [a, b]H = H \ \forall a, b \in G$, то есть коммутатор любых двух элементов (смежных классов) факторгруппы G/H равен единичному элементу H. Следовательно G/H — коммутативная группа.
   ($\Rightarrow$) Если $H \lhd G$ и факторгруппа G/H — коммутативна, то $[a, b]H = [aH, bH] = H \ \forall a, b \in G$. Значит, $[a, b] \in H$ и $G' \subseteq H$, поскольку G' порождается коммутаторами.

□

Предложение 2.3.5. *G/G' — коммутативна.*

Доказательство. Пусть xG', yG' — классы смежности.
Тогда $(xG')(yG')(xG')^{-1}(yG')^{-1} = G'$, так как $[x, y] = xyx^{-1}y^{-1} \in G'$. Значит, $xG'yG' = yG'xG'$, то есть G/G' — коммутативна. □

Предложение 2.3.6. *Коммутант G' группы G является наименьшей нормальной подгруппой, факторгруппа по которой абелева.*

Доказательство. 1) Пусть $\varphi : G \longrightarrow G/G'$ — естественный гомоморфизм. Тогда $(G/G')' = \varphi(G') = \{e\}$ и, значит, группа G/G' коммутативна.
2) Пусть $N \lhd G$ такая, что G/N — абелева, и пусть $\varphi : G \longrightarrow G/N$ — естественный гомоморфизм. Тогда $\varphi(G') = (G/G')' = \{e\}$ и, значит, $G' \subset N$. □

Теорема 2.3.7. *Любая подгруппа $H < G$, содержащая коммутант G' группы G, нормальна. Факторгруппа G/G' — коммутативна и G' содержится в каждой нормальной подгруппе H такой, что G/H — коммутативна.*

Доказательство. Если $x \in H, g \in G$ и $H \supseteq G'$, то $gxg^{-1} = (gxg^{-1}x^{-1})x = [g, x]x \in G'H = H$. Значит, $H \lhd G$. (⇒) Из того, что $H \lhd G$ и $G' \subseteq H$, следует, что $[aH, bH] = aH \cdot bH \cdot a^{-1}H \cdot b^{-1}H = aba^{-1}b^{-1}H = [a, b]H = H \ \forall a, b \in G$, то есть коммутатор любых двух элементов (смежных классов) факторгруппы G/H равен единичному элементу H. Откуда, G/H — коммутативная группа.
Если $H \lhd G$ и факторгруппа G/H — коммутативна, то $[a, b]H = [aH, bH] = H \ \forall a, b \in G$. Значит, $[a, b] \in H$ и $G' \subseteq H$, поскольку G' порождается коммутаторами. □

Определение 2.3.3. *Центром* группы G называется множество $Z(G) = \{h \in G \mid hg = gh \ \forall g \in G\}$.

Очевидно, что $e \in Z(G)$, а также что центр коммутативной группы совпадает с ней самой.

Предложение 2.3.8. *Пусть G — группа. Тогда $Z(G) \lhd G$.*

Доказательство. Сперва докажем, что $Z(G) < G$.
1. Пусть $x, y \in Z(G)$. Тогда для любого $g \in G$ выполнено $(xy)g = xgy = g(xy)$, то есть $xy \in Z(G)$.
2. Пусть $x \in Z(G)$. Тогда $gx = xg \ \forall g \in G \Leftrightarrow (gx)^{-1} = (xg)^{-1} \ \forall g \in G \Leftrightarrow x^{-1}g^{-1} = g^{-1}x^{-1} \ \forall g \in G$. Но g^{-1} пробегает всю группу G. Поэтому $x^{-1} \in Z(G)$.
Нормальность очевидна, так как левые смежные классы совпадают с правыми. □

Предложение 2.3.9. *Пусть G — группа. Тогда* $\operatorname{Int} G \cong G/Z(G)$.

Доказательство. Докажем, что отображение $f : G \ni g \longmapsto \phi_g \in \operatorname{Int} G$ — гомоморфизм. Напомним, что $\phi_g(x) = gxg^{-1}$. Действительно, пусть $g, h \in G$. Тогда $f(gh)(x) = \phi_{gh}(x) = ghx(gh)^{-1} = g(hxh^{-1})g^{-1} = \phi_g(\phi_h(x))$.
Найдем ядро f: $g \in \operatorname{Ker} f \Leftrightarrow \phi_g = id \Leftrightarrow gxg^{-1} = x; \forall g \in G \Leftrightarrow gx = xg; \forall g \in G$. То есть $\operatorname{Ker} f = Z(G)$.
По построению, $\operatorname{Im} f = \operatorname{Int} G$. Значит, согласно теореме о гомоморфизме, $\operatorname{Int} G \cong G/Z(G)$. □

Предложение 2.3.10. *Факторгруппа некоммутативной группы G по ее центру $Z(G)$ не может быть циклической, то есть $G/Z(G) \neq \langle aZ(G)\rangle$ ни для какого $a \in G$.*

Доказательство. От противного. Допустим, что смежный класс $gZ(G)$ порождает факторгруппу $G/Z(G)$. Рассмотрим произвольные элементы $a, b \in G$. Тогда $aZ(G) = (gZ(G))^n = g^nZ(G)$, $bZ(G) = (gZ(G))^m = g^mZ(G)$, т. е. $a = g^nz_1$, $b = g^mz_2$, где $z_1, z_2 \in Z(G)$. Тогда $ab = g^nz_1g^mz_2 = g^{n+m}z_1z_2 = g^mz_2g^nz_1 = ba$, то есть группа G коммутативна. Противоречие. □

Определение 2.3.4. $Z(x) = \{g \in G \mid gx = xg\}$ — *централизатор* элемента x.

2.3.2 Семинар

Задача 2.3.11. Найти S_n'.

Решение. Пусть $\alpha, \beta \in S_n$. Коммутатор $[\alpha, \beta] = \alpha\beta\alpha^{-1}\beta^{-1}$ является четной подстановкой, так как знаки подстановки и обратной к ней совпадают. Поэтому $S_n' \subseteq A_n$.
Далее, так как $[(ij), (ik)] = (ij)(ik)(ij)^{-1}(ik)^{-1} = (ijk)$, а A_n порождается циклами длины три, то $S_n' \supseteq A_n$. В итоге, $S_n' = A_n$. ◀

Задача 2.3.12. Найти $Z(S_n), n \geqslant 3$.

Решение. Пусть $\alpha \in S_n$, и $\alpha \neq id$, то есть существуют такие $i \neq j$, что $\alpha(i) = j$. Так как $n \geqslant 3$, то существует $k \leq n$, отличное от i и j. Рассмотрим $\beta = (jk)$. Тогда $\beta\alpha\beta^{-1}(i) = \beta\alpha(i) = \beta(j) = k$. Значит, $\beta\alpha\beta^{-1}(i) = k \neq j = \alpha(i)$, то есть подстановки α и β не коммутируют. Таким образом, мы показали, как для данной нам неединичной подстановки найти такую, которая с ней не коммутирует. Поэтому $Z(S_n) = \{e\}$. ◀

Задача 2.3.13. Доказать, что $D_n' = \begin{cases} \langle a^2 \rangle, & \text{если } n = 2m \\ \langle a \rangle, & \text{если } n = 2m+1 \end{cases}$, где a — поворот на $\frac{2\pi}{n}$.

Задача 2.3.14. Доказать, что $Z(D_n) = \begin{cases} \langle a^m \rangle, & \text{если } n = 2m \\ e, & \text{если } n = 2m+1 \end{cases}$, где a — поворот на $\frac{2\pi}{n}$.

Задача 2.3.15. Доказать, что $A_4' = V_4$ и $A_n' = A_n$ при $n \geqslant 5$.

Доказательство. Заметим во-первых, что при любом $n \geq 4$ группа A_n' содержит все произведения пар независимых транспозиций (при $n \leq 4$ таких пар нет): $[(ijk), (ijl)] = (ij)(kl)$.
Пусть $n = 4$. Порядок факторгруппы A_4/V_4 равен $\frac{12}{4} = 3$. Есть только одна группа 3-го порядка — C_3. Она абелева. Значит, A_4/V_4 — абелева. Следовательно, $A_4' \subseteq V_4$, но по доказанному выше $V_4 \subseteq A_4'$.
Пусть $n \geq 5$. Снова воспользуемся тем, что при любом n группа A_n' содержит все произведения пар независимых транспозиций. Кроме того, $[(ij)(kl), (ij)(km)] = (klm)$, поэтому A_n' содержит все тройные циклы, которые порождают A_n. □

Задача 2.3.16. $Z(GL(n, \mathbb{C})) = \{\lambda E\}$, $\lambda \neq 0$

2.4 Кватернионы.

Кватернионы можно определить как множество формальных сумм $a+ib+jc+kd$, где $a, b, c, d \in \mathbb{R}$, а i, j, k определяются следующими соотношениями $i^2 = j^2 = k^2 = ijk = -1$.
Обозначение множества кватернионов — $\mathbb{H}$.

Сложение двух кватернионов покомпонентное, и таким образом, свойства поля $\mathbb{R}$ индуцируются (для операции сложения) на кватернионы, т.е. оно будет ассоциативным и коммутативным.
Умножение должно быть дистрибутивно относительно сложения, так что достаточно уметь умножать базисные кватернионы.
Таблица умножения для кватернионов выглядит следующим образом:

	1	i	j	k
1	1	i	j	k
i	i	-1	k	$-j$
j	j	$-k$	-1	i
k	k	j	$-i$	-1

Из таблицы умножения можно заметить, что разные кватернионные “единицы” не коммутируют, а антикоммутируют: $ij = k$ и $ji = -k$. Таким образом, если знать, что $ij = k$, то остальное выводится из ассоциативности умножения. Например, $ik = iij = -j$, поскольку $i^2 = -1$.
Правило умножения базисных кватернионов получается из формулы $ij = k$ циклическими перестановками: $ij = k \quad jk = i \quad ki = j$.

Сопряженным к $q = a + ib + jc + kd$ называется кватернион $\overline{q} = a - ib - jc - kd$.

Нормой кватерниона называется величина $\|q\| := \sqrt{q \cdot \overline{q}} = \sqrt{a^2 + b^2 + c^2 + d^2}$.
Обозначается: $N(q)$, $\|q\|$.
Если кватернион $q = \overrightarrow{0} \Leftrightarrow \|q\| = 0$, а поэтому всякий ненулевой кватернион обратим: $q^{-1} = \frac{\overline{q}}{\|q\|}$.

Множество $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$ является мультипликативной группой, а $\mathbb{H}$ является примером некоммутативного тела.

Также кватернионы можно определить через **комплексные матрицы**.

$$\begin{pmatrix} \alpha & \beta \\ -\overline{\beta} & \overline{\alpha} \end{pmatrix} = \begin{pmatrix} a + bi & c + di \\ -c + di & a - bi \end{pmatrix}$$

Тогда $i = \begin{pmatrix} i & 0 \\ 0 & -i \end{pmatrix}$, $j = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$, $k = \begin{pmatrix} 0 & i \\ i & 0 \end{pmatrix}$.
Свойства такого представления.

1. Сопряженному кватерниону соответсвует сопряженная матрица;
2. Квадрат нормы кватерниона равен определителю матрицы.

Аналогично комплексным числам, кватернионы можно определить через **вещественные матрицы**.

$$\begin{pmatrix} a & -b & -c & -d \\ b & a & -d & c \\ c & d & a & -b \\ d & -c & b & a \end{pmatrix}$$

При таком определении вытекают следующие свойства.

1. Сопряженному кватерниону соответсвует транспонированная матрица;
2. Норма кватерниона равна корню из определителя матрицы.

Подгруппы и факторгруппы группы Q_8.

Если h — любой элемент Q_8, отличный от 1 и -1, то $h^2 = -1$. Поэтому любая подгруппа (отличная от тривильной $\{1\}$) содержит элемент -1. Первую подгруппу получаем, если ограничимся элементами $\{1, -1\}$.
Так как элемент -1 входит в любую (нетривиальную) подгруппу, то элементы i и $-i$ либо оба входят, либо оба не входят в подгруппу. То же верно для j и $-j$, k и $-k$. Так как (нетривиальная) подгруппа в группе кватернионов может содержать только 2 или 4 элемента (по теореме Лагранжа), то мы получаем еще только 3 подгруппы: $\{1, -1, i, -i\}, \{1, -1, j, -j\}, \{1, -1, k, -k\}$.
Все подгруппы нормальны.
$Q_8/\{1, -1\} = \{\{1, -1\}, \{i, -i\}, \{j, -j\}, \{k, -k\}\}$.
$Q_8/\{1, -1, i, -i\} = \{\{1, -1, i, -i\}, \{j, -j, k, -k\}$. Первая факторгруппа изоморфна V_4, факторгруппы по трем подгруппам 4-го порядка изоморфны C_2.

Коммутант и центр группы Q_8.

Элементы 1 и -1 коммутируют со всеми остальными элементами группы кватернионов. Поэтому если один из элементов g_1, g_2 совпадает с 1 или -1, то $g_1 g_2 g_1^{-1} g_2^{-1} = 1$. Если g - любой элемент, отличный от 1 и -1, то $g \cdot (-g) = -g^2 = -(-1) = 1$, т. е. $g^{-1} = -g$. Поэтому, если g_1 и g_2 - элементы, отличные от 1 и -1, то $g_1 g_2 g_1^{-1} g_2^{-1} = g_1 g_2 (-g_1)(-g_2) = g_1 g_2 g_1 g_2 = (g_1 g_2)^2$. Но квадрат любого элемента в группе кватернионов равен 1 или -1. Поэтому коммутант может содержать только элементы 1 и -1, а так как группа кватернионов не коммутативна, то коммутант отличен от $\{1\}$. Следовательно, коммутант — это $\{1, -1\}$.
Из того, что 1 и -1 (и только они) коммутируют со всеми остальными элементами группы кватернионов следует, что $Z(G) = \{1, -1\}$.

3 | Прямое и полупрямое произведения групп

3.1 Прямое произведение групп

3.1.1 Лекция

Внешнее прямое произведение

Пусть G, H — группы. Рассмотрим множество пар $G \times H = \{(g,h) \mid g \in G, h \in H\}$. Пусть $g_1, g_2 \in G, h_1, h_2 \in H$. Введем операцию на $G \times H$: $(g_1,h_1)\cdot(g_2,h_2) = (g_1g_2, h_1h_2)$.
Тогда $G \times H$ — группа. Действительно,
1) Ассоциативность: $((g_1,h_1)(g_2,h_2))(g_3,h_3) = (g_1g_2,h_1h_2)(g_3,h_3) = (g_1g_2g_3, h_1h_2h_3) = (g_1,h_1)(g_2g_3,h_2h_3) = (g_1,h_1)((g_2,h_2)(g_3,h_3))$.
2) Единичный элемент: $e_{G\times H} = (e_G, e_H)$.
3) Обратный: $(g,h)^{-1} = (g^{-1}, h^{-1})$.
Группа $G \times H$ называется *внешним прямым произведением* групп G и H.

Свойства прямого произведения

1. $G \times \{e_H\} = \{(g, e_H)\} < G \times H$
2. $G \times \{e_H\} \cong G$
3. $G \cap H = \{e\}$
   ◀ $(\{G \times \{e_H\}\} \cap \{\{e_G\} \times H\}) = e_{G\times H}$ ▶
4. Пусть $g \in G, h \in H$. Тогда $gh = hg$ (т.е. $(g,e_H)(e_G,h) = (e_G,h)(g,e_H) = (g,h)$).
5. $\forall z \in G \times H\ \exists! g \in G, \exists! h \in H:\ z = gh = (g,e_H)(e_G,h)$
6. $G \lhd G \times H$, $H \lhd G \times H$
7. Если $|G| = n$, $|H| = m \Rightarrow |G \times H| = n \cdot m$.
8. Пусть $g \in G, h \in H$ и $|g| = m$, $|h| = l \Rightarrow |(g,h)| = \text{НОК}(m,l)$.
   ◀ Если $|(g,h)| = k \Rightarrow\ (g,h)^k = (g^k, h^k) = (e_G, e_H) \Rightarrow \begin{cases} g^k = e_G \\ h^k = e_H \end{cases} \Rightarrow \begin{cases} k \vdots |g| \\ k \vdots |h| \end{cases} \Rightarrow k$ — общее кратное, то есть $k = \text{НОК}(|g|, |h|)$. ▶
9. Частный случай: $\text{НОД}(m,l) = 1 \Rightarrow \text{НОК}(m,l) = ml = |(g,h)|$.
10. Если $G = \langle g\rangle, |g| = m, H = \langle h\rangle, |h| = l, \text{НОД}(m,l) = 1 \Rightarrow G \times H = \langle (g,h)\rangle$.

Пример 3.1.1. $U_5 \times U_7 \cong U_{35}$

Теперь, рассмотрим общий случай. Пусть $G_1, \ldots, G_n$ — группы. Тогда $G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n\}$ их *прямое произведение*.
Операция: $(g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n) = (g_1h_1, g_2h_2, \ldots, g_nh_n)$.
$G = G_1 \times G_2 \times \ldots \times G_n$ — группа. Действительно,

$e_G = (e_{G_1}, \dots, e_{G_n})$.
$(g_1, g_2, \dots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \dots, g_n^{-1})$.
Ассоциативность в G выполняется, потому что выполняется в группах $G_1, G_2, \dots, G_n$.

Свойства прямого произведения (продолжение)

1. $|G| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$
2. G — коммутативная группа $\Leftrightarrow$ G_i — коммутативная $(i = 1, 2, \dots, n)$.
3. $|(g_1, g_2, \dots, g_n)| = \text{НОК}(|g_1|, |g_2|, \dots, |g_n|)$
4. Пусть $G_i = \langle g_i \rangle_{k_i}$ $(k_i, k_j) = 1$ $(\forall i, j = 1, 2, \dots, n$ таких, что $i \neq j) \Rightarrow G_1 \times \ldots \times G_n = \langle (g_1, g_2, \dots, g_n) \rangle_{k_1 k_2 \cdot \ldots \cdot k_n}$.
   ◀ Из 3) $|(g_1, g_2, \dots, g_n)| = \text{НОК}(|g_1|, |g_2|, \dots, |g_n|)$. Так как НОД$(k_i, k_j) = 1 \Rightarrow$ НОК$(k_1, \dots, k_n) = k_1 k_2 \dots k_n$. ▶
5. $\tilde{G_1} = G_1 \times \{e_2\} \times \ldots \times \{e_n\} = (g_1, e_2, \dots, e_n)$ $(\forall g_1 \in G_1)$ — подгруппа G.
6. При $i \neq j$ $\tilde{G_i} \cap \tilde{G_j} = \{e_G\}$.
7. Пусть $g_i \in G_i, g_j \in G_j$ и $i < j$. Тогда $\tilde{g_i}\tilde{g_j} = \tilde{g_j}\tilde{g_i}$, то есть $(e, \dots, g_i, \dots, e)(e, \dots, g_j, \dots, e) = (e, \dots, g_j, \dots, e)(e, \dots, g_i, \dots, e) = (e, \dots, g_i, \dots, g_j, \dots, e)$.
8. $\forall g \in G\, \exists!\, g_1 \in G_1, \dots, g_n \in G_n :\ g = \tilde{g_1}\tilde{g_2} \dots \tilde{g_n}$.
   ◀ $g = (g_1, \dots, g_n) = (g_1, e, \dots, e)(e, g_2, e, \dots, e) \dots (e, \dots, e, g_n)$ ▶
9. $\tilde{G_i} = \{e\} \times \ldots \times G_i \times \ldots \times \{e\} \lhd G$.
   ◀ $(g_1, \dots, g_n)\tilde{g_i}(g_1, \dots, g_n)^{-1} = (g_1, \dots, g_n)(e, \dots, g_i, \dots, e)(g_1, \dots, g_n)^{-1} = \dots$ ▶
10. $(G_1 \times G_2 \times \{e_{G_3}\} \times \ldots \times \{e_{G_n}\}) \cap (\{e_{G_1}\} \times \{e_{G_2}\} \times G_3 \times \{e_{G_3}\} \times \ldots \{e_{G_n}\}) = \{e\}$

Внутреннее прямое произведение

Пусть G — группа, а $G_1, \dots, G_n$ — ее подгруппы.
Возьмем $G_1 \times \ldots \times G_n = \{(g_1, g_2, \dots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \dots, g_n \in G_n\}$ — (внешнее) прямое произведение $G_1, \dots, G_n$.
Что нужно потребовать от $G_1, \dots, G_n$, чтобы существовал изоморфизм $\varphi : G_1 \times \ldots \times G_n \longrightarrow G$?
Естественно, мы хотим, чтобы $\varphi(e, \dots, g_i, \dots, e) = g_i$.
Тогда $\varphi(g_1, g_2, \dots, g_n) = \varphi(g_1, e, \dots, e) \cdot \varphi(e, g_2, e, \dots, e) \dots \cdot \varphi(e, \dots, e, g_n) = g_1 g_2 \dots g_n$.
Проверим, является ли отображение φ гомоморфизмом. $\varphi((g_1, g_2, \dots, g_n)(h_1, h_2, \dots, h_n)) = \varphi(g_1 h_1, g_2 h_2, \dots, g_n h_n) = g_1 h_1 g_2 h_2 \dots g_n h_n \neq g_1 g_2 \dots g_n h_1 h_2 \dots h_n = \varphi(g_1, \dots, g_n)\varphi(h_1, \dots, h_n)$. Следовательно, для гомоморфизма нам требуется перестановочность элементов из разных подгрупп $G_1, \dots, G_n$, то есть $g_i g_j = g_j g_i$ $\forall g_i \in G_i, g_j \in G_j$ $(\forall i, j = 1, 2, \dots, n\ i \neq j)$. Пусть это выполнено.
Является ли φ мономорфизмом ?
Очевидно, что $g_1 \dots g_n = h_1 \dots h_n \Leftrightarrow g_1 = h_1, g_2 = h_2, \dots, g_n = h_n$.
Отсюда, φ мономорфизм, если элемент $g \in G$ можно разложить в произведение $g = g_1 g_2 \cdot \ldots \cdot g_n$, $g_1 \in G_1, \dots, g_n \in G$ единственным образом.
Проверим, является ли φ эпиморфизмом.
$\text{Im}\,\varphi = G$. $\exists\, g_1, \dots, g_n : \varphi(g_1, \dots, g_n) = g_1 \dots g_n = g \in G$.
Изо = Моно + Эпи $\Leftrightarrow \forall g \in G\, \exists!\, (g_1, \dots, g_n) \in G_1 \times \ldots \times G_n :\ g = g_1 \cdot \ldots \cdot g_n$.

Определение 3.1.1. Группа G называется *внутренним прямым произведением* своих подгрупп $G_1, \dots, G_n$, если $\begin{cases} 1.\ g_i g_j = g_j g_i\ \forall g_i \in G_i, g_j \in G_j\ (\forall i, j = 1, 2, \dots, n \\ 2.\ \forall g \in G\, \exists! g_1 \in G_1, \dots, g_n \in G_n :\ g = g_1 \cdot \ldots \cdot g_n \end{cases}$

Задача 3.1.2. Доказать, что если пересечение двух нормальных подгрупп H_1 и H_2 группы G содержит лишь e, то $h_1 h_2 = h_2 h_1$ для любых элементов $h_1 \in H_1, h_2 \in H_2$.

Доказательство. $H_2 \ni \underbrace{(h_1 h_2 h_1^{-1})}_{\in H_2} h_2^{-1} = h_1 \underbrace{(h_2 h_1^{-1} h_2^{-1})}_{\in H_1} \in H_1 \Rightarrow h_1 h_2 h_1^{-1} h_2^{-1} = e \Rightarrow h_1 h_2 = h_2 h_1$ □

Какие существуют эквивалентные определения ?
Пусть G — группа, и $G_1, G_2, \ldots, G_n$ — ее подгруппы.
Тогда $G = G_1 \times G_2 \times \ldots \times G_n \Leftrightarrow$

$$\begin{cases} 1.\ G_1 \cap G_2 \cap \ldots \cap G_n = \{e\} \\ 2.\ G = G_1G_2 \cdot \ldots \cdot G_n = \{g_1g_2 \cdot \ldots \cdot g_n \mid \forall g_1 \in G_1, \forall g_2 \in G_2, \ldots, \forall g_n \in G_n\} \\ 3.\ G_1 \lhd G, G_2 \lhd G, \ldots, G_n \lhd G \end{cases} \Leftrightarrow$$

$$\begin{cases} 1.\ G_1 \cap G_2 \cap \ldots \cap G_n = \{e\} \\ 2.\ G = G_1G_2 \cdot \ldots \cdot G_n \\ 3.\ g_ig_j = g_jg_i\ \forall g_i \in G_i, g_j \in G_j\ (\forall i, j = 1, 2, \ldots, n) \end{cases} \Leftrightarrow$$

(в случае, когда $|G| < \infty$)

$$\begin{cases} 1.\ |G| = |G_1||G_2| \cdot \ldots \cdot |G_n| \\ 2.\ G = G_1G_2 \cdot \ldots \cdot G_n \\ 3.\ g_ig_j = g_jg_i\ \forall g_i \in G_i, g_j \in G_j\ (\forall i, j = 1, 2, \ldots, n) \end{cases}$$

Задача 3.1.3. Доказать, что группу $(\mathbb{Z}, \cdot)$ нельзя представить в виде прямого произведения своих подгрупп.

Доказательство. Подгруппы $k\mathbb{Z}$ и $n\mathbb{Z}$ пересекаются, например, по $kn\mathbb{Z}$. □

Теорема 3.1.4. *A — класс сопряженных элементов в $G_1 \times G_2 \Leftrightarrow A = A_1 \times A_2$, где A_1, A_2 — классы сопряженных элементов в G_1, G_2 соответственно.*

Доказательство. ($\Leftrightarrow$) Пусть $(g_1, g_2) \in A$, где A — класс сопряженных элементов в $G_1 \times G_2$. Тогда $A = \{(h_1, h_2)(g_1, g_2)(h_1, h_2)^{-1}\} = \{(h_1g_1h_1^{-1}, h_2g_2h_2^{-1})\}$.
Отсюда, $A_1 = \{h_1g_1h_1^{-1}\}$ — класс сопряженных элементов G_1, $A_2 = \{h_2g_2h_2^{-1}\}$ — класс сопряженных элементов G_2. □

Следствие 3.1.5. *Если в G_1 — k классов сопряженных элементов, в G_2 — m классов сопряженных элементов, то в $G_1 \times G_2$ — km классов сопряженных элементов.*

Следствие 3.1.6. $N_1 \lhd G_1,\ N_2 \lhd G_2 \Rightarrow N_1 \times N_2 \lhd G_1 \times G_2$

Задача 3.1.7. Пусть $\varphi_1, \varphi 2$ – гомоморфизмы двух групп. Тогда $\operatorname{Ker}(\varphi_1 \cdot \varphi_2) = \operatorname{Ker}\varphi_1 \times \operatorname{Ker}\varphi_2$.

Задача 3.1.8. Пусть $\varphi_1, \varphi 2$ – гомоморфизмы двух групп. Тогда $\operatorname{Im}(\varphi_1 \cdot \varphi_2) = \operatorname{Im}\varphi_1 \times \operatorname{Im}\varphi_2$.

Задача 3.1.9. $N_1 \lhd G_1,\ N_2 \lhd G_2 \Rightarrow (G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.

Доказательство. Пусть $\varphi_1 : G_1 \longrightarrow G_1/N_1$ — естественный эпиморфизм ($g \longmapsto gN_1$). Аналогично $\varphi_2 : G_2 \longrightarrow G_2/N_2$. Имеем $\operatorname{Ker}\varphi_1 \cdot \varphi_2 = \operatorname{Ker}\phi_1 \times \operatorname{Ker}\phi_2 = N_1 \times N_2$. По теореме о гомоморфизме групп — существует изоморфизм. □

3.1.2 Семинар

Задача 3.1.10. $V_4 \cong C_2 \times C_2$

Доказательство. Пусть $V_4 = \{e, s_1, s_2, r\}, H_1 = \{e, s_1\} \cong C_2, H_2 = \{e, s_2\} \cong C_2$ — подгруппы V_4, где s_1, s_2 — отражения относительно диагоналей. Построим изоморфизм $\varphi : V_4 \longrightarrow H_1 \times H_2$ следующим образом: $\varphi(e) = (e_{H_1}, e_{H_2}), \varphi(s_1) = (s_1, e), \varphi(s_2) = (e, s_2), \varphi(r) = (s_1, s_2)$. □

Задача 3.1.11. Если G, F — коммутативные группы, то $G \times F$ также коммутативна.

Доказательство. $G \times F \ni (g_1, f_1)(g_2, f_2) = (g_1 g_2, f_1 f_2) = (g_2 g_1, f_2 f_1) = (g_2, f_2)(g_1, f_1)$ □

Задача 3.1.12. $C_m \times C_n \cong C_{mn} \Leftrightarrow (m, n) = 1$

Доказательство. Пусть $C_m = \langle a \rangle_m$ и $C_n = \langle b \rangle_n$. Рассмотрим элемент $(a, b) \in C_m \times C_n$. И пусть его порядок равен k. Так как $(a, b)^{mn} = (a^{mn}, b^{mn}) = (e, e)$, то $k \leqslant mn$. С другой стороны, $(a, b)^k = (a^k, b^k) = (e, e)$, поэтому k делится на m и n. То есть $k = \text{НОК}(m, n)$. А так как m и n взаимно просты, то $k = mn$. Значит (a, b) — образующий элемент в $C_m \times C_n$. Следовательно, $C_m \times C_n \cong C_{mn}$. Если $(m, n) \neq 1$, то $k = \text{НОК}(m, n) < mn$. Пусть $k = mk_1 = nk_2$. Тогда $(a, b)^k = (a^k, b^k) = ((a^m)^{k_1}, (b^n)^{k_2}) = (e, e)$. Следовательно, в $C_n \times C_m$ нет элемента порядка mn и, значит, она не изоморфна C_{mn}. □

Задача 3.1.13. Разлагаются ли в прямое произведение неединичных подгрупп следующие группы: S_3, A_4, S_4, Q_8 ?

Решение. В каждой из этих групп нет нетривиальных подгрупп пересекающихся только по единице. Поэтому нет, не разлагаются. ◀

Задача 3.1.14. $\mathbb{R}_{>0} \times \mathbf{U} \cong \mathbb{C}^* = \mathbb{C} \setminus \{0\}$

Доказательство. $\mathbb{C}^* \ni z = re^{i\varphi} \in \mathbb{R}_{>0} \times \mathbf{U} \cong \mathbb{C}^*$, то есть $\mathbb{C}^* = \mathbb{R}_{>0}\mathbf{U}$.
Подгруппы $\mathbb{R}_{>0}$ и $\mathbf{U}$ нормальны (так как группа $\mathbb{C}^*$ по умножению — коммутативна) и пересекаются только по 1. □

Задача 3.1.15. $G = \text{GL}^+(n, \mathbb{R}) = \{A \in M_{n\times n} : \det A > 0\}$, $G_1 = \{\lambda E \mid \mathbb{R} \ni \lambda > 0\}, G_2 = \text{SL}(n, \mathbb{R})$. Тогда $G = G_1 \times G_2$.

Доказательство. Подгруппы G_1, G_2 — нормальны и пересекаются только по единичной матрице. К тому же $G = G_1 G_2 : \text{GL}^+(n, \mathbb{R}) \ni A = \lambda A_1 = (\lambda E)A_1$, где $\lambda = \sqrt[n]{\det a}, A_1 = \frac{1}{\lambda} A \in \text{SL}(n, \mathbb{R})$. □

3.2 Полупрямое произведение

Внутреннее полупрямое произведение

Задача 3.2.1. $N \lhd G,\ H < G \Rightarrow NH = \{nh : n \in N, h \in H\}$ — подгруппа G.

Доказательство. С ассоциативностью все в порядке, т.к. G — группа. Пусть $n_1, n_2 \in N, h_1, h_2 \in H, g \in G$. По определению, $N \lhd G \Leftrightarrow gn_1g^{-1} = \tilde{n_1} \in N$, где $\tilde{n_1} \in N$. Тогда $\underbrace{(n_1h_1)}_{\in NH}\underbrace{(n_2h_2)}_{\in NH} = n_1h_1n_2h_2 = n_1\underbrace{(h_1n_2h_1^{-1})}_{\in N}\underbrace{h_1h_2}_{\in H} \in NH$. И $(nh)^{-1} = h^{-1}n^{-1} = (h^{-1}n^{-1}h)h^{-1} \in NH$. □

Определение 3.2.1. Пусть G — группа. Говорят, что G разлагается в *полупрямое (внутреннее) произведение* своих подгрупп N и H, если

$\begin{cases} 1.\ N \lhd G \\ 2.\ \forall g \in G\ \exists! n \in N, h \in H : g = nh \end{cases}$ Обозначение $G = N \leftthreetimes H\ \ (G = H \rtimes N)$.

Эти условия эквивалентны:

$\begin{cases} 1.\ N \lhd G, H < G \\ 2.\ N \cap H = \{e\} \\ 3.\ NH = G \end{cases}$ а также, в случае, когда G имеет конечный порядок, следующим: $\begin{cases} 1.\ N \lhd G, H < G \\ 2.\ N \cap H = \{e\} \\ 3.\ |G| = |N||H| \end{cases}$

Пример 3.2.2. Группу кватернионов Q_8 нельзя разложить ни в прямое, ни в полупрямое произведение своих подгрупп, так как любая подгруппа Q_8 содержит 1 и -1, следовательно пересечение двух подгрупп группы Q_8 доставляет по крайней мере -1, не считая единицы.

Задача 3.2.3. Докажите, что $S_n = A_n \leftthreetimes \langle(12)\rangle_2$.

Доказательство. Проверим равенство порядков групп: $|S_n| = |A_n||\langle(12)\rangle_2|$. Также имеем $A_n \lhd S_n$, $\langle(12)\rangle_2 < S_n$. И $A_n \cap \langle(12)\rangle_2 = \{e\}$. □

Задача 3.2.4. $S_4 = V_4 \leftthreetimes S_3$

Доказательство. Для начала вспомним, что $V_4 \lhd S_4$. Группа S_3 вложена в S_4 в виде подгруппы, оставляющей на месте 4. Для каждого $k \in \{1, 2, 3, 4\}$ в V_4 имеется единственная подстановка, переводящая 4 в k. Значит, каждая подстановка $\sigma \in S_4$ предствляется единственным образом в виде $\sigma = \alpha\beta$, где $\alpha \in V_4, \beta \in S_3$. □

Задача 3.2.5. $\mathrm{GL}(n, \mathbb{R}) = \mathrm{SL}(n, \mathbb{R}) \leftthreetimes \left\{ \begin{pmatrix} \lambda & \dots & 0 \\ 0 & 1 \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 1 \end{pmatrix} \in \mathrm{GL}(n, \mathbb{R}) \mid \lambda \in \mathbb{R}^* \right\}$

Доказательство. Известно, что $\mathrm{SL}(n, \mathbb{R}) \lhd \mathrm{GL}(n, \mathbb{R})$.

Также ясно, что $SL(n, \mathbb{R}) \cap \left\{ \begin{pmatrix} \lambda & \dots & 0 \\ 0 & 1 \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 1 \end{pmatrix} \mid \lambda \neq 0 \right\} = \{E\}$, где E — единичная матрица.

Так как $\mathrm{GL}(n, \mathbb{R})$ имеет бесконечный порядок, то дадим явное соответствие:

$\mathrm{GL}(n, \mathbb{C}) \ni G \longmapsto \frac{G}{\sqrt{\det G}} \cdot \begin{pmatrix} \sqrt{\det G} & \dots & 0 \\ \dots & \dots & \\ 0 & \dots & 1 \end{pmatrix}$. □

Предложение 3.2.6. *Если $G = N \leftthreetimes H$, то $G/N \cong H$.*

Внешнее полупрямое произведение

Пусть N, H — группы. Как задать произведение на парах (n, h), чтобы $NH = G$ была группой, такой что $G = N \leftthreetimes H$? $(n_1, h_1) * (n_2, h_2) = ?$
Пусть $\varphi_{h_1} : n_2 \longmapsto h_1 n_2 h_1^{-1}$ — автоморфизм, причем внутренний. Т.е. существует $\varphi_{h_1}(n_2) = h_1 n_2 h_1^{-1}$. Для разных $h_1 \in H$ существуют разные внутренние автоморфизмы. Например, $\varphi_h(g) = hgh^{-1}$ — внутренний автоморфизм группы G. Но если в качестве $g \in G$ брать только элементы группы N, то $\varphi_{h_1} : N \longrightarrow N$. Получился просто автоморфизм группы N, т.к. h_1 не имеет никакого отношения к N. Тогда $(n_1, h_1)(n_2, h_2) = (n_1(h_1 n_2 h_1^{-1})(h_1 h_2)) = (n_1 \varphi_{h_1}(n_2))(h_1 h_2)$. Вернемся к $N \leftthreetimes H$, где N и H никак не связаны. Если существует гомоморфизм $\varphi : H \longrightarrow \operatorname{Aut} N$, где $\varphi(h) = \varphi_h \in \operatorname{Aut} N$, то говорят, что существует *полупрямое (внешнее) произведение* двух групп N и H. Таким образом $(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)$. Частный случай: если $\varphi = \mathrm{id} \Rightarrow N \leftthreetimes H = N \times H$. Если мы придумаем $(n_1 \varphi_{h_1}(n_2), h_1 h_2)$ — мы сделаем из двух групп полупрямое произведение. Причем, разные гомоморфизмы φ_h дают разные полупрямые произведения. Заметим, что из двух групп мы можем всегда сделать их прямое произведение (его нам доставляет всегда существующий тождественный автоморфизм), а полупрямое - не всегда получится. Если бывают разные гомоморфизмы, то записываем $N \leftthreetimes_\varphi H$, если зафиксировали гомоморфизм, то записываем $N \leftthreetimes H$.

Задача 3.2.7. Доказать, что $N \leftthreetimes H$ — группа.

Доказательство.

1. Операция не выводит из “множества” ? Из определения (внутреннего) полупрямого произведения $(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_1), h_1 h_2) \in N \leftthreetimes H$.
2. Ассоциативность. $[(n_1, h_1)(n_2, h_2)]\,(n_3, h_3) = (n_1 \varphi_{h_1}(n_2), h_1 h_2)(n_3, h_3) = (n_1 \varphi_{h_1}(n_2) \varphi_{h_1 h_2}(n_3), h_1 h_2 h_3)$
$(n_1, h_1)\,[(n_2, h_2)(n_3, h_3)] = (n_1, h_1)(n_2 \varphi_{h_2}(n_3), h_2 h_3) = (n_1 \varphi_{h_1}(n_2 \varphi_{h_1 h_2}(n_3)), h_1 h_2 h_3)$.
$\varphi_{h_1}(n_2 \varphi_{h_2}(n_3))) =$ по определению гомоморфизма $= \varphi_{h_1}(n_2) \varphi_{h_1 h_2}(n_3))\,(= \varphi_{h_1}(n_2) \varphi_{h_1}(\varphi_{h_2}(n_3)))$.
3. Единичный элемент $e_{N \leftthreetimes H} = (e_N, e_H)$.
4. Обратный элемент $(n, h)^{-1} = (?, h^{-1})$. Из определения обратного, $(n, h)(?, h^{-1}) = (n, \varphi_h(?), hh^{-1}) = (e, e)$. Тогда $n \varphi_h(?) = e \Leftrightarrow \varphi_h(?) = n^{-1} \Rightarrow \exists \varphi_h^{-1}(n^{-1}) = e$. Поэтому $(n, h)^{-1} = (\varphi_h^{-1}(n^{-1}), h)$ — обратный.

□

Задача 3.2.8. Пусть $N = A_3$ и $H = C_2$. Найти все полупрямые произведения $N \leftthreetimes H$.

Доказательство. Группа четных подстановок $A_3 = \{e, (123), (132)\} = C_3 = \langle e, a, a^2 \}$ имеет порядок $|A_3| = 3$. Группа $C_2 = \langle e, s \rangle$ — циклическая группа порядка 2. Для того, чтобы найти все полупрямые произведения $C_3 \leftthreetimes C_2$, рассмотрим гомоморфизм $\varphi : C_2 \longrightarrow \mathrm{Aut} C_3$.
Случай 1: $\varphi(e_{C_2}) = \mathrm{id}$, $\varphi(s) = \mathrm{id}$. Тогда $\mathrm{id}(e_{C_3}) = e$, $\mathrm{id}(a) = a$, $\mathrm{id}(a^2) = a^2$ и $C_3 \leftthreetimes_\varphi C_2 = C_3 \times C_2$.
Случай 2: $\varphi(e) = \mathrm{id}$, $\varphi(s) = \varphi_s : \varphi_s(e) = e, \varphi_s(a) = a^2, \varphi_s(a^2) = a$. Значит,
$C_3 \leftthreetimes_\varphi C_2 = \{(e, e), (a, e), (a^2, e), (e, s), (a, s), (a^2, s)\}$. Проверим получившуюся группу на коммутативность: $(a, e)(a^2, s) = (a \varphi_e(a^2), es) = (aa^2, s) = (e, s)$, $(a, s)(a^2, s) = (a \varphi_s(a^2), ss) = (a^2, e)$. Групп 6-го порядка всего две: $C_6 \cong C_2 \times C_3$ и D_3. Но наша группа не коммутативна, следовательно, она изоморфна D_3: $A_3 \leftthreetimes \langle (12) \rangle_2 = S_3 \cong D_3$. □

4 | Теория конечных групп

4.1 Гомоморфизмы

Теорема 4.1.1 (О гомоморфизме)**.** *Пусть $\varphi\colon G \to G_1$ – гомоморфизм и $K = \operatorname{Ker}\varphi$ – его ядро. Тогда имеется естественный изоморфизм $\psi\colon G/\operatorname{Ker}\varphi \cong \operatorname{Im}\varphi$, определенный формулой $\psi(gK) := \varphi(g)$.*

Теорема 4.1.2 (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. Первое утверждение вытекает из теоремы о гомоморфизме, если определить $\varphi\colon G/K \to G/H$ формулой $\varphi(gK) := gH$.

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 4.1.3. В S_4 имеется нормальная подгруппа – четверная группа Кляйна $V_4 := \{e, (12)(34), (13)(24), (14)(23)\} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$. 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 4.1.4. 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 $\psi(g) := g^{-1}$.

4.1.1 Экспонента группы

Определение 4.1.1. 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 4.1.5. $\exp(\mathbb{Z}_k \oplus \mathbb{Z}_n) = \mathrm{HOK}(k, n)$;
$\exp(\mathbb{Z}_{k_1} \oplus \cdots \oplus \mathbb{Z}_{k_s}) = \mathrm{HOK}(k_1, \ldots, k_s)$;
$\exp(\mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \oplus \mathbb{Z}_{p^3} \oplus \cdots \oplus \mathbb{Z}_{p^s} \oplus \ldots) = \infty$.

4.2 Конечно порожденные абелевы группы

Теорема 4.2.1 (Основная теорема (без доказательства))**.** *Конечная абелева группа изоморфна конечной прямой сумме конечных циклических групп.*

Конечно порожденная абелева группа изоморфна прямой сумме свободной абелевой группы конечного ранга и конечной абелевой группы.

Если $(m, n) = 1$, то $\mathbb{Z}_{mn} = \mathbb{Z}_m \oplus \mathbb{Z}_n$.

Задачи 4.2.2. 1. a) $\mathrm{End}(\mathbb{Z}) = \mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$.
b) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}_2$.
2. a) $\mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_n) = 0$, если $(m, n) = 1$.
b) $\mathrm{End}(\mathbb{Z}_m) = \mathrm{Hom}(\mathbb{Z}_m, \mathbb{Z}_m) = \mathbb{Z}_m$
3. $\mathrm{Hom}(A \oplus B, C) \cong \mathrm{Hom}(A, C) \oplus \mathrm{Hom}(B, C)$.
4. $\mathrm{Hom}(A, B \oplus C) \cong \mathrm{Hom}(A, B) \oplus \mathrm{Hom}(A, C)$.

4.3 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 $S(X) \cong S_n$.

4.3.1 Левые и правые действия

Определение 4.3.1. 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.

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 $\alpha(g_1 g_2)x = (\alpha(g_1) \circ \alpha(g_2))(x) = \alpha(g_1)(\alpha(g_2)x)$, что в упрощенных обозначениях приобретает вид:

1. $ex = x$,
2. $(g_1 g_2)x = g_1(g_2 x)$.

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. $x(g_1g_2) = (xg_1)g_2$.

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 определить левое: $gx := xg^{-1}$.

Определение 4.3.2. 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 4.3.3. 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 4.3.1. 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 $M(X,Y)$ 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 годится и для Y с тривиальным действием.

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. Такие автоморфизмы называются *внутренними*.

Подробнее действие сопряжениями будет изучаться ниже.

4. Пусть $X = V$ – конечномерное векторное пространство (над некоторым, полем). Тогда группа $GL(V)$ обратимых линейных операторов является подгруппой в $S(V)$. Важен случай, когда действие $G \to S(V)$ разлагается в композицию гомоморфизмов $G \to GL(V) \to S(V)$. В этом случае действие

называется линейным, а гомоморфизм $G \to GL(V)$ называется *линейным представлением* группы G в пространстве V. Если V векторное пространство над полем $\mathbb{C}$ (соответственно над $\mathbb{R}$), то представление называется комплексным (соответственно вещественным). Представление G в $\mathbb{C}^n$, т.е. гомоморфизм $G \to GL(n,\mathbb{C})$ называется *унитарным*, если образ этого гомоморфизма содержится в унитарной группе $U(n,\mathbb{C})$. Аналогично, вещественное представление $G \to GL(n,\mathbb{R})$, т. е. представление G в $\mathbb{R}^n$, называется *ортогональным*, если этот гомоморфизм пропускается через ортогональную группу $O(n,\mathbb{R})$.

Теория представлений групп – обширная, имеющая многочисленные применения (например, в физике), область математики.

Мы ограничимся здесь лишь несколькими простыми примерами, поскольку элементы теории представлений будут более подробно рассматриваться позже.

Если G – подгруппа в $GL(V)$, то имеется очевидное представление G в V, а именно – гомоморфизм вложения подгруппы $G \to GL(V)$.

a) Циклическая группа $< a >_n \cong \mathbb{Z}_n$ порядка n линейно над полем $\mathbb{C}$ действует на комплексном одномерном пространстве $\mathbb{C}$ по формуле $a^k z := e^{2\pi k i/n} z,\ z \in \mathbb{C}$. Получается комплексное одномерное линейное представление $\mathbb{Z}_n \to GL(\mathbb{C})$. Это есть вложение $\mathbb{Z}_n$ в $GL(\mathbb{C}) = \mathbb{C} \setminus 0$. На самом деле, ясно, что $\mathbb{Z}_n$ вложена в унитарную группу $U(1) = \{z \in \mathbb{C} \,|\, |z| = 1\} \subset GL(\mathbb{C})$, т. е. представление является *унитарным*.

b) Пусть $b\colon \mathbb{C} \to \mathbb{C}$ – комплексное сопряжение: $bz = \bar{z}$. Это отображение не является $\mathbb{C}$-линейным, но является $\mathbb{R}$-линейным $b\colon \mathbb{R}^2 \to \mathbb{R}^2$, где $\mathbb{R}^2 \cong \mathbb{C}$, $x + ib \leftrightarrow (x,y)$, – $\mathbb{R}$-линейный изоморфизм. Ясно также, что $a \in GL(2,\mathbb{R}) = GL(\mathbb{R}^2)$.

Имеем $a(bz) = a\bar{z} = e^{2\pi i/n}\bar{z} = \overline{e^{-2\pi i/n} z} = \overline{e^{2\pi(n-1)i/n} z} = b(a^{n-1}z)$, т. е. $ab = ba^{n-1}$. Подгруппа в $GL(2,\mathbb{R})$, порожденная a и b изоморфна диэдральной группе D_n (любое соотношение в группе D_n проверяется описанным выше способом). Построенное двумерное вещественное представление группы D_n пропускается через ортогональную группу $O(2,\mathbb{R})$, т.е. является *ортогональным*, поскольку матрицы операторов a и b являются ортогональными (a – вращение против часовой стрелки на угол $\frac{2\pi}{n}$, а b – отражение относительно оси Ox).

c) В качестве еще одного примера рассмотрим следующее, называемое *мономиальным*, представление симметрической группы S_n на n-мерном векторном пространстве V. Зафиксируем некоторый базис в V. Сопоставим подстановке перестановку базисных векторов. Такая престановка определяет линейный оператор. Матрица его (в выбранном базисе) содержит n единиц, по одной в каждой строке и в каждом столбце, остальные элементы равны нулю. Тем самым определен гомоморфизм $S_n \to GL(V)$. Он является мономорфизмом, поскольку разным подстановкам соответствуют разные матрицы.

4.3.2 Орбиты и стационарные подгруппы

Определение 4.3.4. 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 4.3.5. Множество орбит обозначается X/G и называется *фактор-множеством* множества X по действию группы G.

Определение 4.3.6. Действие называется транзитивным, если имеется ровно одна орбита, т. е. $|X/G| = 1$. Иными словами $X = Gx\ \ \forall\, x \in X$.

Определение 4.3.7. 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 4.3.8. 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 4.3.2. *Отображение $f\colon Gx \to G/G_x$ переводящее gx в gG_x корректно определено и является G-эквивалентностью.*

Предложение 4.3.3. *Если группа G конечна, то $|Gx| = |G : G_x| = \frac{|G|}{|G_x|}$.*

Предложение 4.3.4. *Имеем $G_{gx} = gG_xg^{-1} = i_g(G_x)$. Таким образом, стабилизаторы точек из одной и той же орбиты являются сопряженными подгруппами.*

Пример 4.3.5. Пусть G – группа вращений трехмерного куба и X – множество его вершин. Ясно, что G дейсвует транзитивно на X, поэтому $X = G/G_x$, где x – любая вершина куба. Элементы подгруппы G_x оставляют неподвижной как вершину x так и противоположную по большой диагонали куба вершину x', поэтому G_x – циклическая группа порядка 3 (подгруппа вращений, оставляющая диагональ xx' и ее концы на месте). Таким образом, $8 = |X| = |G/G_x| = \frac{|G|}{|G_x|} = \frac{|G|}{3}$, откуда $|G| = 24$.

Группа G переставляет четыре диагонали куба, причем каждому элементу соответствует ровно одна перестановка, поэтому G можно реализовать как подгруппу симметрической группы S_4 (для этого нужно как нибудь занумеровать диагонали числами 1, 2, 3, 4). Поскольку порядки одинаковы ($|G| = 24 = |S_4|$), мы видим, что эти группы изоморфны: $G \cong S_4$.

Задача 4.3.6. Найти порядок группы вращений трехмерного куба, используя транзитивность ее действия на множестве

a) больших диагоналей куба,
b) диагоналей граней,
c) ребер,
d) граней,
e) пар противоположных граней.

Задача 4.3.7. Найти порядок группы вращений правильного тетраэдра, используя транзитивность ее действия на множестве

a) вершин,
b) ребер,
c) граней.

Задача 4.3.8. Найти порядок диэдральной группы D_n, используя транзитивность ее действия на множестве

a) вершин правильного n-угольника,
b) ребер правильного n-угольника.

Задача 4.3.9. Найти порядок группы вращений правильного

a) додекаэдра,
b) икосаэдра.

Предложение 4.3.10. *Пусть p – наименьший простой делитель порядка $|G|$ группы G. Тогда всякая подгруппа H группы G индекса $p = |G : H|$ нормальна.*

Доказательство. Рассмотрим действие группы H на G/H левыми умножениями. Длина любой орбиты делит $|H|$, а, значит, и $|G|$, поэтому она либо равна 1, либо не меньше p, так как p – наименьший простой делитель $|G|$. Поскольку $|G/H| = p$ и имеется по меньшей мере одна неподвижная точка – смежный класс eH, действие тривиально. Поэтому для любых $h \in H$ и $g \in G$ имеем $hgH = gH$, т. е. $hg = gh'$ где $h' \in H$, откуда получаем $g^{-1}hg \in H$. Это означает, что H нормальна. □

В частности, подгруппа индекса 2 нормальна.

4.3.3 Лемма (не) Бернсайда

Пусть G – конечная группа и X – конечное G-множество. Положим $\mathrm{Fix}\,(g) = \{x \in X \mid gx = x\}$ – множество неподвижных точек отображения $g\colon X \to X$, при котором x переходит в gx.

Следующее утверждение называют леммой Бернсайда, а также леммой не Бернсайда, поскольку Бернсайд, доказавший много лемм и теорем, именно к этой лемме отношения не имеет.

Лемма 4.3.11 (Лемма (не) Бернсайда)**.** $|X/G| = \frac{1}{|G|}\sum\limits_{g\in G}|\mathrm{Fix}\,(g)|$.

Доказательство.

$$|\{(g,x)\in G\times X \mid gx=x\}| = \sum_{g\in G}|\mathrm{Fix}\,(g)| = \sum_{x\in X}|G_x| = \sum_{x\in X}\frac{|G|}{|Gx|} = |X/G|\cdot|G|,$$

поскольку элементы из одной и той же орбиты дают одинаковый вклад в сумму $\sum_{x\in X}\frac{|G|}{|Gx|}$. □

Прежде, чем привести пример применения леммы Бернсайда опишем элементы группы вращений трехмерного куба.

Группа вращений трехмерного куба. Пусть G – группа вращений трехмерного куба. Мы знаем, что $|G| = 24$. Имеются вращения следующих типов:

a) вращения вокруг диагоналей куба,

b) вращения вокруг осей, проходящих через центры противоположных граней,

c) вращения вокруг осей, проходящих через центры противоположных ребер.

Группа вращений вокруг фиксированной диагонали куба (вращения сохраняют вершины диагонали) является циклической группой порядка 3. Среди этих вращений два нетривиальных и, следовательно, имеется $4\cdot 2 = 8$ нетривиальных вращений типа a), поскольку у куба 4 диагонали.

Группа вращений вокруг оси, проходящей через центры фиксированной пары противоположных граней является циклической группой порядка 4. Нетривиальных вращений три, и поскольку мы имеем три пары противоположных граней получается $3\cdot 3 = 9$ нетривиальных вращений типа b).

Наконец нетривиальное вращение вокруг оси, проходящей через центры фиксированной пары противоположных ребер, ровно одно, и поскольку таких пар ребер 6, имеем $6\cdot 1 = 6$ нетривиальных вращений типа c).

Всего получаем $8 + 9 + 6 = 23$ нетривиальных вращений. Вместе с тривиальным вращением получаем все элементы группы вращений трехмерного куба.

Опишем геометрически построенный выше эпиморфизм $S_4 \to S_3$ с ядром V_4.

Каждое вращение куба дает единственную перестановку пар противоположных граней куба. Это и дает эпиморфизм $S_4 \to S_3$. Эпиморфность легко устанавливается – достаточно показать, что любая транспозиция содержится в образе этого гомоморфизма, поскольку S_3 порождается транспозициями. Пусть пары противоположных граней помечены числами 1,2,3 и i, j, k – перестановка этих чисел. Рассмотрим вращение на 90° (в любую сторону) вокруг оси, проходящей через центры противоположных граней, помеченных числом k. Образ этого вращения в группе S_3 является транспозицией (ij).

Задача 4.3.12. Дать (в том же духе) описание элементов группы вращений правильного тетраэдра.

Решение. Обозначим эту группу через T. Имеются вращения двух типов:

a) вращения вокруг осей, проходящих через вершину и центр противоположной грани; таких осей четыре и для фиксированной оси все такие вращения образуют циклическую подгруппу порядка 3, поэтому имеется $4\cdot 2 = 8$ нетривиальных вращений этого типа.

b) вращения вокруг осей, проходящих через центры противоположных ребер; таких осей три и для фиксированной оси все такие вращения образуют циклическую подгруппу порядка 2, т. е. всего имеем $3\cdot 1 = 3$ нетривиальных вращений этого типа.

Вместе с единичным элементом получается 12 элементов группы. Других элементов нет, поскольку $|T| = 12$. Действительно, T действует транзитивно на множестве из четырех вершин, а стабилизатор вершины имеет порядок 3, поэтому в группе $4\cdot 3 = 12$ элементов. Кроме того, рассматривая T как подгруппу в S_4 мы видим, что ее индекс равен двум, и, следовательно, T изоморфна группе четных подстановок A_4. □

Пример 4.3.13. Найдем число различных вершинных раскрасок трехмерного куба в d цветов. Две раскраски вершин считаем одинаковыми, если одну из другой можно получить некоторым вращением куба. Всего раскрасок d^8: для одной вершины имеется d возможностей, а для занумерованных восьми вершин – d^8. Обозначим множество таких раскрасок через X. Элементы этого множества можно представлять себе как матрицы с двумя строками и восемью столбцами – в первой стоят числа от 1 до 8, а во второй цвета (или их номера). Поскольку группа вращений куба отождествляется

с симметрической группой S_4, мы можем описать ее действие на элементе $x \in X$ так: σx, где $\sigma \in S_4 = G$, получается из x следующим образом: заменяем первую строчку матрицы x на вторую строчку подстановки σ, а затем в полученной матрице переставляем столбцы так, чтобы числа в первой строке шли в правильном порядке, т. е. возрастали от 1 до 8. Таким образом, нам нужно найти $|X/G|$, что мы и сделаем ниже с помощью леммы Бернсайда.

Ясно, что $\mathrm{Fix}(e) = X$, поэтому $|\mathrm{Fix}(e)| = d^8$.

Пусть $g \in G = S_4$ – нетривиальный элемент группы вращений куба. Чтобы найти $|\mathrm{Fix}(g)|$ нужно найти орбиты действия циклической группы $< g >$ на множестве вершин куба. Поскольу при действии элемента g на орбите $< g > a$ вершины a куба точки этой орбиты циклически переставляются, их надо покрасить в один и тот же цвет. Поэтому $|\mathrm{Fix}(g)| = d^{q_g}$, где q_g – число обит действия подгруппы $< g >$ на множестве вершин куба.

Пусть g – нетривиальное вращение типа a), т. е. вращение вокруг диагонали куба, соединяющей противоположные вершины a и a'. Как мы знаем, циклическая группа порожденная элементом g является подгруппой порядка 3. Имеется 4 орбиты действия этой подгруппы на множестве вершин куба – две одноэлементные и две трехэлементные. Одноэлементные – это вершины a и a', в трехэлементные входят по три вершины, которые ребрами соединяются с a и соответственно с a'. Выбирая для каждой орбиты по цвету получаем d^4 раскрасок. Поскольку у нас 8 нетривиальных элементов типа a), сумма чисел $|\mathrm{Fix}(g)|$ взятая по всем нетривиальным g типа a) равна $8d^4$.

Рассмотрим теперь нетривиальный g типа b). Здесь два случая: либо $< g >= \mathbb{Z}_4$ (таких элементов 6), либо $< g >= \mathbb{Z}_2$ (3 элемента). В первом случае орбит действия подгруппы $< g >$ на множестве вершин куба две (по 4 вершины от каждой из противоположных граней, через центры которых проходит ось вращения), во втором – четыре (каждую четверку вершин граней надо представить объединением пар вершин противоположных по диагонали квадрата). Таким образом, $|\mathrm{Fix}(g)| = d^4$ в первом случае и $|\mathrm{Fix}(g)| = d^2$ во втором случае, а сумма чисел $|\mathrm{Fix}(g)|$ взятая по всем нетривиальным g типа b) равна $6d^2 + 3d^4$.

Наконец, орбиты действия (на множестве вершин куба) нетривиального элемента g типа c) такие же как в ситуации второго случая для элементов типа b), т.е. их четыре. Всего таких элементов шесть, поэтому сумма чисел $|\mathrm{Fix}(g)|$ взятая по всем нетривиальным g типа c) равна $6d^4$.

Таким образом, $\sum\limits_{g\in G} |\mathrm{Fix}(g)| = d^8 + 8d^4 + 6d^2 + 3d^4 + 6d^4 = d^8 + 17d^4 + 6d^2$ и по лемме Бернсайда получаем:

$$|X/G| = \frac{d^8 + 17d^4 + 6d^2}{24}.$$

В частности, при покраске в три цвета ($d = 3$) получаем

$$\frac{1}{24}(3^8 + 17 \cdot 3^4 + 6 \cdot 3^2) = 333$$

различных вершинных раскрасок куба.

Задача 4.3.14. Найти число различных реберных раскрасок трехмерного куба в d цветов.

Задача 4.3.15. Найти число различных раскрасок граней трехмерного куба в d цветов.

Решение. Поскольку граней шесть, число различных раскрасок с учетом фиксированной нумерации граней равно d^6, и это есть

вклад единичного элемента в сумму $\sum_{g\in G} |\mathrm{Fix}(g)|$.

Рассматривая действие нетривиального элемента g типа a) мы видим, что три грани куба, сходящиеся в вершине диагонали куба, вокруг которой происходит вращение, должны иметь одинаковый цвет, и оставшиеся 3 грани, сходящиеся в противоположной вершине, также должны быть покрашены одинаково. Только в этом случае раскраска принадлежит $\mathrm{Fix}\, g$. Таким образом, g дает вклад d^2 в сумму, а все элементы этого типа – вклад $8d^2$.

Элемент типа a) порядка 4 дает вклад d^3, а все такие элементы – вклад $6d^3$. Действительно, потивоположные грани (через центры которых проходит ось вращения) красятся произвольно, а оставшиеся 4 грани надо покрасить одним и тем же цветом. Элемент типа a) порядка 2 дает вклад d^4, а все такие элементы – вклад $3d^4$. Всего нетривиальные элементы типа a) дают влад $6d^3 + 3d^4$.

Для элементов типа c) каждая из следующих пар граней должна быть покрашена в свой цвет: пары граней, примыкающие к противоположным ребрам, через центры которых проходит вращение, оставшаяся пара противоположных граней. Вклад элемента в сумму равен d^3, а всех элементов этого типа – $6d^3$.

Таким образом, $\sum_{g\in G}|\mathrm{Fix}(g)| = d^6+8d^2+(6d^3+3d^4)+6d^3 = d^6+3d^4+12d^3+8d^2$ и, следовательно, по лемме Бернсайда число существенно различных раскрасок равно

$$\frac{1}{24}\sum_{g\in G}|\mathrm{Fix}(g)| = \frac{1}{24}(d^6+3d^4+12d^3+8d^2).$$

В частности, при покраске в три цвета ($d=3$) получаем

$$\frac{1}{24}(3^6+3\cdot 3^4+12\cdot 3^3+8\cdot 3^2) = 57$$

существенно различных граневых раскрасок куба. □

Задача 4.3.16. Найти число различных вершинных раскрасок правильного тетраэдра в d цветов.

Задача 4.3.17. Найти число различных реберных раскрасок правильного тетраэдра в d цветов.

Задача 4.3.18. Найти число различных раскрасок граней правильного тетраэдра в d цветов.

Задача 4.3.19. Найти число различных раскрасок ожерелья из p бусин, где p простое, в d цветов. Равносильно: Найти число различных вершинных раскрасок правильного p-угольника в d цветов.
[Указание: Использовать диэдральную группу D_p.]

Задача 4.3.20. Найти число различных реберных раскрасок правильного p-угольника, где p простое, в d цветов.
[Указание: Использовать диэдральную группу D_p.]

4.4 Теоремы Силова

4.4.1 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 $Z(G) := \{z\in G\,|\,zg = gz\ \ \forall g\in G\}$.

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

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

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

Фактор-группа $\mathrm{Aut}(G)/\mathrm{Inn}\, G$ называется группой *внешних автоморфизмов*.

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 $C(x) := \{gxg^{-1}\,|\,g\in G\}$.

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 $\{gHg^{-1}\,|\,g\in G\}$.

Определение 4.4.1. $Z(x) := \{g \in G \,|\, gx = xg\} = \{g \in G \,|\, gxg^{-1} = x\}$ называется централизатором элемента $x \in G$. Легко видеть, что централизаторы элементов являются подгруппами в G.

Определение 4.4.2. Нормализатором подгруппы H в G называется

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

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

Теорема 4.4.1. *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 $C(x) = \{gxg^{-1} \,|\, g \in G\}$. Поскольку 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 $\{gHg^{-1} \,|\, g \in G\}$ – класс подгрупп сопряженных с H. Стабилизатором точки H является нормализатор $N(H)$. Поэтому мощность множества подгрупп группы G, сопряженных с подгруппой H, равна $|G : N(H)| = |G|/|N(H)|$. □

4.4.2 Силовские подгруппы

Определение 4.4.3. Конечная группа G называется p-группой, где p – простое число, если ее порядок является степенью числа p, т. е. $|G| = p^n$.

В частности, тривиальная группа (содержащая только единичный элемент) является p-группой для любого простого p. Поскольку по теореме Лагранжа порядок подгруппы делит порядок группы, мы видим, что любая подгруппа p-группы сама является p-группой.

Теорема 4.4.2. *Центр нетривиальной p-группы нетривиален.*

Доказательство. Пусть Z – центр группы. Так как $e \in Z$, имеем $|Z| \geq 1$. Нам нужно показать, что центр содержит более одного элемента.

Пусть $K \subset G$ – такой класс сопряженных элементов, что $|K| = 1$. Тогда $K = \{a\}$, $a \in G$, и $gag^{-1} = a$ для любого $g \in G$. Поэтому $a \in Z$. Пусть $C(x)$ – класс сопряженных элементов элемента $x \in G$ такой, что $|C(x)| > 1$. Тогда $|C(x)|$ делится на p, поскольку $|C(x)| = \frac{|G|}{|Z(x)|} > 1$ и $|G|$ – степень простого числа p. Группа G представляется в виде дизъюнктного объединения $G = Z \coprod K_1 \coprod \cdots \coprod K_s$, где K_j – нетривиальные классы сопряженных элементов. Поскольку p делит каждое из чисел $|G|, |K_1|, \ldots, |K_s|$ и $|G| = |Z| + |K_1| + \cdots + |K_s|$, порядок центра $|Z|$ делится на p, а поскольку $|Z| \geq 1$, получаем что центр нетривиален, т. е. является нетривиальной p-группой. □

Предложение 4.4.3. *Всякая группа порядка p^2, где p - простое число, является абелевой.*

Доказательство. По предыдущей теореме центр Z группы нетривиален, поэтому либо $|Z| = p$, либо $|Z| = p^2$. Во втором случае $Z = G$ и значит G абелева.

Покажем, первое предположение ведет к противоречию. Итак, пусть $|Z| = p$. Тогда и $|G/Z| = p$, откуда следует что обе эти группы изоморфны $\mathbb{Z}_p$. Если aZ – образующий группы $G/Z \cong \mathbb{Z}_p$, то любой $g \in G$ представляется в виде $g = a^k z = za^k$, $z \in Z$. Поскольку любые два элемента такого вида коммутируют, группа G коммутативна и значит $Z = G$ – противоречие. □

Абелевых групп порядка p^2 с точностью до изоморфизма всего две – циклическая $\mathbb{Z}_{p^2}$ и $\mathbb{Z}_p \oplus \mathbb{Z}_p$.

Определение 4.4.4. Силовской p-подгруппой группы G называется всякая ее подгруппа, индекс которой не делится на p, т.е. любая подгруппа порядка p^n, где $|G| = p^n m$ и $(m, p) = 1$.

Теорема 4.4.4. *Силовская p-подгруппа существует.*

Доказательство. Проведем индукцию по порядку группы. Для $|G|$ доказывать нечего. Пусть $|G| > 1$, $|G| = p^n m$, где $(m,p) = 1$ и $n > 0$. Рассмотрим разбиение группы G на классы сопряженных элементов. Возможны два случая:

1) Существует нетривиальный, содержащий более одного элемента, класс сопряженных элементов, количество элементов в котором не делится на p.

2) Число элементов любого нетривиального класса сопряженных элементов делится на p.

В первом случае имеется элемент $x \in G$ такой, что $|C(x)| > 1$ и $|C(x)|$ не делится на p. Из равенства $|C(x)| = \frac{|G|}{|Z(x)|}$ следует, что $|Z(x)|$ делится на p^n. Кроме того, $|Z(x)| < |G|$, поскольку $|C(x)| > 1$. Следовательно, по предположению индукции $Z(x)$ содержит силовскую p-подгруппу, которая и будет силовской p-подгруппой в G.

Во втором случае рассмотрим представление группы в виде дизъюнктного объединения $G = Z \coprod K_1 \coprod \cdots \coprod K_s$, где K_j – нетривиальные классы сопряженных элементов. Поскольку p делит каждое из чисел $|G|, |K_1|, \ldots, |K_s|$ и $|G| = |Z| + |K_1| + \cdots + |K_s|$, порядок центра $|Z|$ делится на p, поэтому $|Z| = d\,p^\alpha$, где d не делится на p и $\alpha > 0$. Если $\alpha = n$, то Z является p-силовской подгруппой в G. Поэтому предположим, что $\alpha < n$. По предположению индукции в Z существует силовская p-подгруппа Z_1 порядка p^α. Тогда $|G/Z_1| = |G : Z_1| = |G|/|Z_1| = m\,p^{n-\alpha}$. По предположению индукции в группе G/Z_1 существует подгруппа H порядка $p^{n-\alpha}$ – ее силовская p-подгруппа. Полный прообраз подгруппы H при гомоморфизме $G \to G/Z_1$ (обозначим его через G_1) и есть p-силовская подгруппа в G. Действительно, $|G_1| = |G_1/Z_1|\,|Z_1| = |H|\,|Z_1| = p^{n-\alpha}p^\alpha = p^n$. □

Теорема 4.4.5. *Всякая p-подгруппа группы G содержится в некоторой силовской p-подгруппе. Все силовские p-подгруппы сопряжены.*

Доказательство. Пусть S – силовская p-подгруппа группы G и пусть H – p-погруппа. Рассмотрим действие H на G/S левыми умножениями. Так как число элементов любой нетривиальной H-орбиты делится на p, а $|G/S|$ не делится на p, то имеются неподвижные точки H-действия, т. е. существует $g \in G$ такой, что $HgS = gS$. Отсюда следует, что $g^{-1}HgS = S$, поэтому $g^{-1}Hg \subset S$, откуда получаем включение $H \subset gSg^{-1}$.

Если H силовская p-подгруппа, то из сравнения порядков $|gSg^{-1}| = |S| = |H|$ получаем $H = gSg^{-1}$. □

Теорема 4.4.6. *Число силовских p-подгрупп делит индекс силовской p-подгруппы и сравнимо с 1 по модулю p, т. е. если $|G| = mp^n$, где m не делится на p, то число силовских p-подгрупп делит m и сравнимо с 1 по модулю p.*

Доказательство. Из доказательства предыдущей теоремы видно, что множество всех силовских p-подгрупп совпадает с классом $C(S)$ подгрупп сопряженных с S, где S – какая-нибудь силовская p-подгруппа. Таким образом, число N_p силовских p-подгрупп равно $|C(S)|$. Имеем $N_p = |C(S)| = |G : N(S)| = \frac{|G|}{|N(S)|}$. Поскольку S является подгруппой нормализатора $N(S)$ подгруппы S, порядок $|N(S)|$ делится на $|S| = p^n$. Поэтому $N_p = |C(S)|$ делит m.

Рассмотрим действие группы S на $C(S)$ сопряжениями: подгруппа gSg^{-1} переходит при действии элемента $h \in S$ в $hgSg^{-1}h^{-1}$. Тогда $C(S)$ разбивается на S-орбиты. Среди орбит могут быть неподвижные точки и нетривиальные S-орбиты, причем длина нетривиальных орбит делится на p. Докажем что неподвижная точка ровно одна – сама подгруппа S, отсюда будет следовать, что $N_p = |C(S)| \equiv 1 \pmod p$.

Пусть $H \in C(S)$ – неподвижная точка S-действия. Это означает, что $sHs^{-1} = H$ для любого $s \in S$ и, следовательно, S является подгруппой нормализатора $N(H)$ подгруппы H. Тогда H и S – силовские p-подгруппы группы $N(H)$ и по предыдущей теореме они сопряжены в $N(H)$. Но поскольку H нормальна в $N(H)$, получаем, что $H = S$. □

Пример 4.4.7. Положим $GL(n,q) := GL(n,\mathbb{F}_q)$, где $q = p^d$, p – простое число. Обозначим через $UT(n,q)$ подгруппу в $GL(n,q)$ верхне-треугольных матриц с 1-ми на главной диагонали. Покажем, что $UT(n,q)$ является силовской p-подгрупой в $GL(n,q)$.

Имеем $|GL(n,q)| = (q^n-1)(q^n-q)(q^n-q^2)\ldots(q^n-q^{n-1}) = \prod_{i=0}^{n-1}(q^n-q^i)$. Действительно, столбцы матрицы должны быть линейно независимы, поэтому первый столбец матрицы может быть любым ненулевым вектором из $\mathbb{F}_q^n$, т. е. имеем q^n-1 возможностей, второй столбец – любым вектором не коллинеарным первому столбцу (дает q^n-q вариантов), третий – любым вектором, не лежащим в

двумерном подпространстве, натянутом на первые два столбца (дает $q^n - q^2$ вариантов), и т. д. Далее, имеем

$$|GL(n,q)| = \prod_{i=0}^{n-1}(q^n - q^i) = m\prod_{i=1}^{n-1} q^i = m\, q^{\sum_{i=1}^{n-1} i} = mq^{\frac{n(n-1)}{2}} = p^{\frac{dn(n-1)}{2}} m,$$

где $m = \prod_{i=0}^{n-1}(q^{n-i} - 1)$ и, следовательно, $(m, p) = 1$.

Число над диагональных элементов в матрицах из $UT(n,q)$, которые могут быть произвольными элементами поля $\mathbb{F}_q$, равно $(n^2 - n)/2 = \frac{n(n-1)}{2}$. Поэтому $|UT(n,q)| = q^{\frac{n(n-1)}{2}} = p^{\frac{dn(n-1)}{2}}$, откуда и следует, что $UT(n,q)$ – силовская p-подгруппа группы $GL(n,q)$.

Задача 4.4.8. Если p – простой делитель порядка группы, то в группе существует элемент порядка p.

Решение. Возьмем какую-нибудь силовскую p-подгруппу. Из условия следует, что она нетривиальна, поэтому в ней имеется нетривиальный элемент a. Его порядок делит порядок силовской p-подгруппы и, следовательно, равен p^k с $k \geq 1$. Тогда $a^{p^{k-1}}$ – искомый элемент порядка p. □

Пример 4.4.9. Покажем, что всякая группа G порядка 45 абелева.

Обозначим через N_p, число силовских p-подгупп группы G, $p = 3, 5$. Имеем $N_3 \equiv 1 \pmod 3$ и $N_3 \,|\, 5$ (число силовских p-подгрупп делит индекс силовской p-подгруппы). Отсюда следует, что $N_3 = 1$. Следовательно, силовская 3-подгруппа единственна и значит нормальна. Обозначим ее через G_3. Поскольку порядок группы G_3 равен квадрату простого числа – $|G_3| = 3^2$, она абелева.

Аналогично получаем $N_5 \equiv 1 \pmod 5$ и $N_5 \,|\, 9$, откуда $N_5 = 1$, и следовательно, силовская 5-подгруппа единственна, а значит нормальна. Обозначим ее через G_5. Поскольку $|G_5| = 5$, группа G_5 изоморфна $\mathbb{Z}_5$, и поэтому абелева.

Из того, что $G_3 \cap G_5 = \{e\}$ и нормальности подгрупп G_3 и G_5, следует, что группа G является прямым произведением $G = G_3 \times G_5$. Из абелевости сомножителей вытекает абелевость группы G.

Поскольку G абелева имеются только две возможности – либо G изоморфна $\mathbb{Z}_9 \oplus \mathbb{Z}_5$, либо – $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

4.5 Разрешимые группы

Элемент $[a,b] = aba^{-1}b^{-1}$, называется *коммутатором* элементов $a, b \in G$. Коммутатор равен единице группы в том и только том случае, когда a и b коммутируют, т. е. $ab = ba$, поскольку равенства $aba^{-1}b^{-1} = e$ и $ab = ba$, очевидно, эквивалентны. Элемент обратный к коммутатору является коммутатором: $[a,b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b,a]$. Кроме того, $[a,a] = e$ для дюбого $a \in G$.

Определение 4.5.1. Подгруппа в G порожденная всеми коммутаторами называется коммутантом и обозначается G'.

По определению G' состоит из элементов, которые равны произведениям коммутаторов и элементов обратных коммутаторам, но поскольку обратный к коммутатору сам является коммутатором, G' состоит из элементов, равных произведениям коммутаторов, т. е.

$$G' = \{[a_1,b_1]\cdot\dots\cdot[a_k,b_k] \mid a_j, b_j \in H, j = 1,\dots,k;\ k \in \mathbb{N}\}.$$

Предложение 4.5.1. *Коммутант – нормальная подгруппа. Фактор-группа по коммутанту абелева.*

Доказательство. Пусть $g \in G$. Поскольку i_g – автоморфизм,

$$i_g([a,b]) = i_g(aba^{-1}b^{-1}) = i_g(a)i_g(b)i_g(a)^{-1}i_g(b)^{-1} = [i_g(a), i_g(b)],$$

откуда получаем, что

$$\begin{aligned} i_g([a_1,b_1]\cdot\dots\cdot[a_k,b_k]) &= i_g([a_1,b_1])\cdot\dots\cdot i_g([a_k,b_k]) = \\ &= [i_g(a_1), i_g(b_1)]\cdot\dots\cdot[i_g(a_k), i_g(b_k)] \in G', \end{aligned}$$

т. е. G' – нормальная подгруппа в G.

Абелевость фактор-группы G/G' вытекает из следующего вычисления:

$$g_1G' \cdot g_2G' = g_1g_2G' = g_2g_1g_1^{-1}g_2^{-1}g_1g_2G' = g_2g_1[g_1^{-1}, g_2^{-1}]G' = g_2g_1G' = g_2G' \cdot g_1G'.$$

□

Ясно также, что $G' = \{e\}$ в том и только в том случае, когда G абелева.

Если $\varphi\colon G_1 \to G_2$ – гомоморфизм групп, то образ коммутатора равен коммутатору образов: $\varphi([a,b]) = [\varphi(a), \varphi(b)]$, $a, b \in G_1$. Поэтому $\varphi(G_1') \subset G_2'$ и если $\varphi(G_1) = G_2$, то $\varphi(G_1') = G_2'$. Пользуясь этим можно дать другое доказательство абелевости группы G/G'.

Теорема 4.5.2. *Коммутант G' группы G является наименьшей нормальной подгруппой, факторгруппа по которой абелева.*

Доказательство. Пусть $\varphi\colon G \to G/G'$ – канонический эпиморфизм. Тогда $(G/G')' = \varphi(G') = \{eG'\}$ – единичная подгруппа в G/G'. Следовательно, G/G' абелева.

Пусть подгруппа N нормальна в G и G/N абелева. Пусть $\pi\colon G \to G/N$ – канонический эпиморфизм. Тогда $\pi(G') = (G/N)' = \{eN\}$ – единичная подгруппа в G/N. Следовательно, $G' \subset N$. □

Определение 4.5.2. Кратные коммутанты определяются индуктивно: $G^{(k+1)} := (G^{(k)})'$, где $G^{(1)} := G'$.

Предложение 4.5.3. *Пусть $\varphi\colon G_1 \to G_2$ – гомоморфизм групп. Тогда при любом $k \geq 1$ имеет мето включение $\varphi(G_1^{(k)}) \subset G_2^{(k)}$ и если $\varphi\colon G_1 \to G_2$ – эпиморфизм, то $\varphi(G_1^{(k)}) = G_2^{(k)}$.*

Доказательство. Индукция по k. Для $k = 1$ это было доказано выше. Пусть верно для $k = n-1$, докажем для $k = n$. Положим $H_1 = G_1^{(n-1)}$, $H_2 = G_2^{(n-1)}$. Тогда $H_1' = G_1^{(n)}$, $H_2' = G_2^{(n)}$ и по предположению индукции $\varphi(H_1) \subset H_2$. Обозначая ограничение φ на подгруппу H_1 по прежнему через $\varphi\colon H_1 \to H_2$, имеем $\varphi(H_1') \subset H_2'$, т. е. $\varphi(G_1^{(n)}) \subset G_2^{(n)}$.

Если $\varphi\colon G_1 \to G_2$ – эпиморфизм, то по предположению индукции $\varphi(H_1) = H_2$, т. е. $\varphi\colon H_1 \to H_2$ – эпиморфизм. Поэтому $\varphi(H_1') = H_2'$, т. е. $\varphi(G_1^{(k)}) = G_2^{(k)}$.

□

В частности, если H – подгруппа в G, то $H^{(k)} \subset G^{(k)}$ при любом $k \geq 1$.

Задача 4.5.4. Доказать, что подгруппа $G^{(k)}$ нормальна в G при любом k.

Решение. Индукция по k. При $k = 1$ верно. Пусть верно для $k = n-1$, докажем для $k = n$. Положим $H = G^{(n-1)}$. Тогда $H' = G^{(n)}$. Любой элемент из H' имеет вид

$$[a_1, b_1] \cdot \dots \cdot [a_k, b_k],$$

где $a_j, b_j \in H$, $j = 1, \dots, k$.

По предположению индукции H является нормальной подгруппой в G, поэтому для любого $g \in G$ и $a_j, b_j \in H$, $j = 1, \dots, k$, имеем $i_g(a_j), i_g(b_j) \in H$. Следовательно,

$$i_g([a_1, b_1] \cdot \dots \cdot [a_k, b_k]) = [i_g(a_1), i_g(b_1)] \cdot \dots \cdot [i_g(a_k), i_g(b_k)] \in H' = G^{(n)},$$

что и означает нормальность подгруппы $G^{(n)}$ в G. □

Определение 4.5.3. Группа G называется разрешимой, если существует натуральное число $m \in \mathbb{N}$ такое, что $G^{(m)} = \{e\}$.

Задачи 4.5.5. *1.* Всякая подгруппа и всякая фактор-группа разрешимой группы разрешима.

2. Если подгруппа N нормальна в G и N и G/N разрешимы, то G разрешима.

Решение. 1. Пусть H – подгруппа в G. Поскольку $H^{(k)} \subset G^{(k)}$ при любом k, из равенства $G^{(m)} = \{e\}$ следует, что $H^{(m)} = \{e\}$, т. е. H разрешима.

Пусть N – нормальная подгруппа в G. Поскольку $G \to G/N$ – эпиморфизм, образ подгруппы $G^{(k)}$ совпадает с $(G/N)^{(k)}$ при любом k. Поэтому из равенства $G^{(m)} = \{e\}$ следует, что $(G/N)^{(m)} = \{eN\}$, т. е. что G/N разрешима.

2. Пусть $N^{(n)} = \{e\}$ и $(G/N)^{(m)} = \{eN\}$. Поскольку $G \to G/N$ – эпиморфизм, образ подгруппы $G^{(m)}$ совпадает с $(G/N)^{(m)} = \{eN\}$, откуда следует, что $G^{(m)} \subset N$. Поэтому $(G^{(m)})^{(n)} \subset N^{(n)} = \{e\}$. Поскольку $(G^{(m)})^{(n)} = G^{(m+n)}$, имеем $G^{(m+n)} = \{e\}$, т. е. G разрешима. □

В следующем предложении p – произвольное простое число.

Предложение 4.5.6. *Всякая p-группа разрешима.*

Доказательство. Индукция по n, где p^n – порядок p-группы. При $n \leq 2$ группа абелева, и, значит, разрешима. Предположим, что утверждение верно для p-групп порядка не превосходящего p^{n-1}. Докажем для группы порядка p^n.

Центр p-группы – нетривиальная абелева нормальная подгруппа. Она разрешима в силу абелевости. Фактор-группа по центру имеет порядок строго меньший, чем p^n, в силу нетривиальности центра, и поэтому по предположению индукции разрешима. Из разрешимости нормальной подгруппы и фактор-группы следует разрешимость самой группы.

□

Пример 4.5.7. Группа $T(n, \mathbb{K})$ верхне треугольных невырожденных матриц с элементами из поля $\mathbb{K}$ разрешима.

Доказательство. Доказательство проведем индукцией по n. Поскольку $T(1, \mathbb{K}) \cong \mathbb{K}^*$ – абелева, она разрешима.

Вычеркивая последнюю строку и последний столбец из верхне треугольной матрицы размера $n \times n$ получаем верхне треугольную матрицу размера $(n-1) \times (n-1)$. Легко видеть, что построенное отображение $\varphi\colon T(n, \mathbb{K}) \to T(n-1, \mathbb{K})$ на самом деле является гомоморфизмом. Ядро $\operatorname{Ker}\varphi$ состоит из матриц вида

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & c_{n-1} \\ 0 & 0 & 0 & \dots & 0 & c_n \end{pmatrix}.$$

Ставя в соответствие такой матрице число c_n получаем гомоморфизм $\psi : \operatorname{Ker}\varphi \to \mathbb{K}^*$, ядро которого $\operatorname{Ker}\psi$ состоит из матриц вида

$$\begin{pmatrix} 1 & 0 & 0 & \dots & 0 & c_1 \\ 0 & 1 & 0 & \dots & 0 & c_2 \\ \vdots & \vdots & \ddots & & \vdots & \vdots \\ 0 & 0 & 0 & \dots & 1 & c_{n-1} \\ 0 & 0 & 0 & \dots & 0 & 1 \end{pmatrix},$$

которые, как нетрудно видеть, коммутируют между собой. Поскольку $\operatorname{Ker}\psi$ и $\mathbb{K}^*$ абелевы, получаем, что $\operatorname{Ker}\varphi$ разрешима. Предположив, что $T(n-1, \mathbb{K})$ разрешима и используя только что доказанный факт разрешимости группы $\operatorname{Ker}\varphi$, получаем, что $T(n, \mathbb{K})$ разрешима. □

Лемма 4.5.8. *Группа четных подстановок A_n порождается тройными циклами, а при $n \geq 5$ порождается произведениями пар независимых транспозиций.*

Доказательство. Симметрическая группа S_n порождается транспозициями, поэтому A_n порождается произведениями пар транспозиций. Для попарно различных i, j, k, l, m справедливы соотношения

$$\begin{aligned} (ij)(jk) &= (ijk), \\ (ij)(kl) &= (ijk)(jkl), \\ (ij)(jk) &= (ij)(lm)(jk)(lm), \end{aligned}$$

откуда и вытекает лемма. □

Предложение 4.5.9. *Пусть $\sigma = (i_1 \dots i_p)$ – цикл и π – подстановка. Тогда внутренний автоморфизм, соответствующий подстановке π, действует на σ по формуле*

$$i_\pi(\sigma) = \pi\sigma\pi^{-1} = (\pi(i_1) \dots \pi(i_p)).$$

Более общо, если $\sigma = (i_1 \dots i_p)(j_1 \dots i_q) \dots (k_1 \dots k_r)$, то

$$i_\pi(\sigma) = (\pi(i_1) \dots \pi(i_p))(\pi(j_1) \dots \pi(j_q)) \dots (\pi(k_1) \dots \pi(k_r)).$$

Следствие 4.5.10. *Классы сопряженных элементов в S_n состоят из подстановок одинаковой цикловой структуры. Число классов сопряженных элементов в симметрической группе S_n равно числу представлений числа n в (неупорядоченную) сумму натуральных чисел.*

Примеры 4.5.11. *1.* Покажем, что $S_n' = A_n$ при $n \geq 3$.

Поскольку $S_n/A_n \cong \mathbb{Z}_2$ абелева, имеем $S_n' \subset A_n$. Так как $|A_3| = |S_3|/2 = 3$, группа A_3 абелева ($A_3 \cong \mathbb{Z}_3$). Поэтому S_3' либо совпадает с A_3, либо тривиальна. Второй случай отпадает, поскольку S_3 не является абелевой. Таким образом, $S_3' = A_3$. Отсюда, из предложения 4.5.9 и нормальности коммутанта получаем, что S_n' содержит все тройные циклы и, следовательно, S_n' совпадает с A_n (в силу леммы 4.5.8).

2. Покажем, что $A_4' = V_4$, где V_4 – четверная группа Кляйна ($V_4 \cong \mathbb{Z}_2 \oplus \mathbb{Z}_2$).

Имеем $|A_4| = |S_4|/2 = 12$, V_4 нормальна в S_4 и $|A_4/V_4| = 12/4 = 3$. Поэтому $A_4/V_4 \cong \mathbb{Z}_3$ абелева. Следовательно, $A_4' \subset V_4$. Так как A_4 не абелева, то $|A_4'| > 1$. Поэтому либо $A_4 = V_4$, либо $|A_2'| = 2$. Последний случай исключается, что легко понять с помощью предложения 4.5.9.

3. Покажем, что $A_n' = A_n$ при $n \geq 5$.

Действительно, поскольку $A_4' = V_4$, группа A_n' содержит все произведения пар независимых транспозиций и, следовательно, в силу последнего утверждения леммы 4.5.8 совпадает с A_n.

4. Из 1, 2, 3 следует, что S_n разрешима при $n \leq 4$ и не разрешима при $n \geq 5$.

4.6 Простые группы

Определение 4.6.1. Группа называется простой, если в ней нет других нормальных подгрупп, кроме единичной подгруппы и самой группы.

Примером простой группы, очевидно, является группа $\mathbb{Z}_p$ вычетов по модулю p, где p – любое простое число.

4.6.1 Простота группы A_n, при $n \geq 5$

Группы A_n просты при $n \leq 3$ (так как $|A_1| = |A_2| = 1$ и $A_3 \cong \mathbb{Z}_3$), в то время как A_4 не является простой, поскольку содержит нормальную подгруппу $A_4' = V_4$. Таким образом, из следующей теоремы мы видим, что группы A_n просты при всех n кроме $n = 4$.

Теорема 4.6.1. *Группа A_n проста при $n \geq 5$.*

Доказательство. 1. Покажем сначала, что A_n при $n \geq 5$ не содержит нормальных подгрупп группы S_n, отличных от $\{e\}$ и A_n.

Пусть N – нормальная подгруппа группы S_n и $\sigma \in N$, $\sigma \neq e$.

a) Предположим, что в разложении σ в произведение независимых циклов имеется цикл $\gamma = (i_1 \dots i_p)$ длины $p \geq 3$. Пусть $\sigma = \gamma\tau$, где τ – произведение остальных циклов. Возьмем $\delta = (i_1 i_2)$ и рассмотрим элемент

$$\sigma' = i_\delta(\sigma) = \delta\sigma\delta^{-1} \in N.$$

Поскольку символы i_1, i_2 не входят в циклы из которых состоит τ, получаем с помощью предложения 4.5.9

$$\begin{aligned}\sigma' = i_\delta(\sigma) = i_\delta(\gamma) i_\delta(\tau) = i_\delta(\gamma)\tau = \delta\gamma\delta^{-1}\tau = \\ = (\delta(i_1)\delta(i_2)\delta(i_3)\dots\delta(i_p))\tau = (i_2 i_1 i_3 \dots i_p)\tau \in N.\end{aligned}$$

Поэтому

$$\sigma'\sigma^{-1} = (i_2 i_1 i_3 \dots i_p)\tau\tau^{-1}(i_1 i_2 i_3 \dots i_p)^{-1} = (i_2 i_1 i_3 \dots i_p)(i_1 i_2 i_3 \dots i_p)^{-1} = (i_1 i_2 i_3) \in N.$$

Так как все тройные циклы сопряжены в S_n и A_n ими порождается, получаем, что $N = A_n$.

b) Если в σ нет циклов длины $p \geq 3$, то σ – произведение четного числа независимых транспозиций. Запишем σ в виде $\sigma = (i_1 i_2)(i_3 i_4)\tau$, где в τ не входят символы i_1, i_2, i_3, i_4. Положим $\delta = (i_2 i_3)$. Тогда

$$\sigma' := i_\delta(\sigma) = i_\delta((i_1 i_2)) i_\delta((i_3 i_4)) i_\delta(\tau) = (\delta(i_1)\delta(i_2))(\delta(i_3)\delta(i_4))\tau = (i_1 i_3)(i_2 i_4)\tau \in N.$$

Следовательно,

$$\sigma'\sigma^{-1} = (i_1 i_3)(i_2 i_4)\tau\tau^{-1}(i_3 i_4)^{-1}(i_1 i_2)^{-1} = (i_1 i_3)(i_2 i_4)(i_3 i_4)(i_1 i_2) = (i_1 i_4)(i_2 i_3) \in N.$$

Так как все произведения пар независимых транспозиций сопряжены в S_n и A_n ими порождается, получаем, что $N = A_n$.

2. Пусть N – нормальная подгруппа в A_n, $|N| > 1$ и N не является нормальной подгруппой в S_n. Тогда в S_n имеется ровно две подгруппы сопряженные с N, а именно $N_1 = N$ и $N_2 = (12)N(12)^{-1} = (12)N(12)$. Отметим, что N_2 – нормальная подгруппа в A_n. Пересечение $N_1 \cap N_2$ и произведение N_1N_2 – нормальные подгруппы в S_n. Следовательно, из доказанного выше получаем, что $N_1 \cap N_2 = \{e\}$ и $N_1N_2 = A_n$. Поэтому $A_n = N_1 \times N_2$ и, в частности, $|A_n| = |N_1| \cdot |N_2| = |N|^2$. Поскольку $|A_5| = 60$ не является квадратом, получаем, что A_5 проста.

Далее будем доказывать по индукции. Предположим, что A_{n-1} проста, $n \geq 6$. Будем рассматривать A_{n-1} как подгруппу $A_{n-1} \subset A_n$, состоящую из четных подстановок, оставляющих символ n на месте. Так как $N_2 \cap A_{n-1}$ нормальна в A_{n-1}, то либо $A_{n-1} \subset N_2$, либо $N_2 \cap A_{n-1} = \{e\}$. В первом случае $|A_{n-1}| \leq |N_2| = |N|$, во втором A_{n-1} изоморфно проектируется на некоторую подгруппу группы N_1 и, следовательно, $|A_{n-1}| \leq |N_1| = |N|$. Таким образом, в любом случае $|N| \geq |A_{n-1}|$ и, значит, $|A_n| \geq |A_{n-1}|^2$, что очевидно неверно. □

4.6.2 Теорема Жордана – Диксона

Группа матриц размера $n \times n$ с определителем 1 и элементами из поля $\mathbb{K}$ обозначается через $SL(n, \mathbb{K})$ и называется специальной линейной группой. Если поле $\mathbb{K}$ конечно, $\mathbb{K} = \mathbb{F}_q$, будем обозначать эту группу через $SL(n, q)$. Проективная специальная линейная группа $PSL(n, \mathbb{K})$ – это факторгруппа группы $SL(n, \mathbb{K})$ по ее центру, который состоит из скалярных матриц, т.е. матриц вида λE, где E – единичная матрица. Определитель такой матрицы равен λ^n, а с другой равен 1. Таким образом, λ – корень n-й степени из 1 (в поле $\mathbb{K}$).

В случае $\mathbb{K} = \mathbb{F}_q$ обозначаем $PSL(n, \mathbb{F}_q)$ через $PSL(n, q)$.

Задача 4.6.2. Доказать, что группа $PSL(2, 2) := PSL(2, \mathbb{F}_2)$ изоморфна S_3.

Решение. Ясно, что $GL(2, 2) = SL(2, 2) = PSL(2, 2)$. Элемент $x \in GL(2, 2)$ действует умножением слева на вектор-столбцы $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, которым мы сопоставим числа 1, 2, 3 соответственно. Поэтому каждому элементу x соответствует единственная подстановка – элемент группы S_3. Тем самым получаем инъективное отображение $\varphi\colon GL_2(2) \to S_3$, которое и является искомым изоморфизмом. Действительно, гомоморфность следует из построения φ, а поскольку порядки групп одинаковы и φ инъективно, получаем, что φ – биективный гомоморфизм, т. е. изоморфизм.

Укажем явно описанное соответствие. Имеем $GL(2, 2) = \{e, a, b, c, d, f\}$, где

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},$$
$$c = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix},\ d = \begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix},\ f = \begin{pmatrix} 0 & 1 \\ 1 & 1 \end{pmatrix}.$$

Поскольку

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix},\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix},\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},$$

получаем $\varphi(a) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23)$ и аналогичное вычисление для других элементов дает:

$$\varphi(b) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = (13), \qquad \varphi(c) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (12),$$
$$\varphi(d) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = (132), \qquad \varphi(f) = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (123).$$

□

Задача 4.6.3. Доказать, что группа $PSL(2, 3) := PSL(2, \mathbb{F}_3)$ изоморфна A_4.

Решение. $PSL(2,3) = \{e, a, b, c, d, f, g, h, m, n, p, r\}$, где элементы группы можно представить матрицами (точнее классами этих матриц)

$$e = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix},\ a = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix},\ b = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix},\ c = \begin{pmatrix} 0 & 1 \\ 2 & 0 \end{pmatrix},$$
$$d = \begin{pmatrix} 1 & 1 \\ 2 & 0 \end{pmatrix},\ f = \begin{pmatrix} 0 & 1 \\ 2 & 1 \end{pmatrix},\ g = \begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix},\ h = \begin{pmatrix} 1 & 0 \\ 2 & 1 \end{pmatrix},$$
$$m = \begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix},\ n = \begin{pmatrix} 0 & 2 \\ 1 & 1 \end{pmatrix},\ p = \begin{pmatrix} 2 & 1 \\ 1 & 1 \end{pmatrix},\ r = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}.$$

Элементы группы – это преобразования множества прямых, проходящих через начал координат, двумерного пространства $\mathbb{F}_3^2$. Всего имеется 4 прямые, которые порождены векторами $\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \begin{pmatrix} 1 \\ 2 \end{pmatrix}$, и мы занумеруем эти прямые числами 1, 2, 3, 4. Элементы группы соответствуют действию указанных матриц на прямых, т. е. соответствуют перестановкам чисел 1, 2, 3, 4. Например, действие a на двух первых векторах такое же как в предыдущей задаче, т. е. 1-я прямая остается на месте, а 2-я переходит в 3-ю. Поскольку

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 2 \\ 1 \end{pmatrix},\ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 2 \end{pmatrix} = \begin{pmatrix} 0 \\ 2 \end{pmatrix},$$

а векторы $\begin{pmatrix} 2 \\ 1 \end{pmatrix} = 2\begin{pmatrix} 1 \\ 2 \end{pmatrix}$ и $\begin{pmatrix} 0 \\ 2 \end{pmatrix} = 2\begin{pmatrix} 0 \\ 1 \end{pmatrix}$ порождают 4-ю и 2-ю прямую соответственно, мы видим что a соответсвует подстановке $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix} = (234)$. Таким образом, возникает мономорфизм $\varphi\colon PSL(2,3) \to S_4$, при котором, как показывает прямое вычисление, имеем

$$\varphi(a) = (234),\ \varphi(b) = (134),\ \varphi(c) = (12)(34),\ \varphi(d) = (142),\ \varphi(f) = (123),\ \varphi(g) = (243),$$
$$\varphi(h) = (143),\ \varphi(m) = (132),\ \varphi(n) = (124),\ \varphi(p) = (14)(23),\ \varphi(r) = (13)(24).$$

откуда видно, что $\operatorname{Im}\varphi = A_4$ и, следовательно, $PSL(2,3) \cong A_4$. □

Из двух предыдущих задач следует, что группы $PSL(2,2)$ и $PSL(2,3)$ не просты.

Теорема 4.6.4 (Теорема Жордана – Диксона)**.** *Пусть* $\mathbb{K}$ *– поле и* $n \geq 2$. *Группа* $PSL_n(\mathbb{K})$ *является простой, кроме случаев* $PSL(2,2)$ *и* $PSL(2,3)$.

Определение 4.6.2. Действие называется k-транзитивным, если для любых двух наборов $(x_1, \ldots, x_k)$ и $(y_1, \ldots, y_k)$ элементов из X таких, что $x_i \neq x_j$ и $y_i \neq y_j$ для всех $i \neq j$, найдется элемент $g \in G$ такой, что $gx_i = gy_i$, $i = 1, \ldots, n$.

Пример 4.6.5. Очевидно, что симметрическая группа S_n действует n-транзитивно на $\{1, \ldots, n\}$. Группа A_n действует $(n-2)$-транзитивно на $\{1, \ldots, n\}$. Действительно, перевести набор $(i_1, \ldots, i_{n-2})$ в $(j_1, \ldots, j_{n-2})$ можно любой из двух подстановок

$$\begin{pmatrix} i_1 \ldots i_{n-2} i_{n-1} i_n \\ j_1 \ldots j_{n-2} j_{n-1} j_n \end{pmatrix} \qquad \text{и} \qquad \begin{pmatrix} i_1 \ldots i_{n-2} i_{n-1} i_n \\ j_1 \ldots j_{n-2} j_n j_{n-1} \end{pmatrix},$$

одна из которых четна.

Гипотеза 1 (Гипотеза Жордана)**.** *Если* G *действует точно и* k*-транзитивно, где* $k > 5$, *на* $\{1, 2, \ldots, n\}$, *то* G *изоморфна* S_n *или* A_n.

Гипотеза доказана в середине 80-х. Матье исследовал 4- и 5-транзитвные группы и открыл 5 спорадических групп.

Предложение 4.6.6. *Если* G *действует на* X *точно и 2-транзитивно, то любая ее неединичная нормальная подгруппа* N *действует на* X *транзитивно.*

Доказательство. Доказательство проведем от противного. Предположим, что $X = Nx_1 \coprod Nx_2 \coprod \dots$ – дизъюнктное объединение орбит действия N на X. В этом объединении есть по крайней мере две орбиты и по крайней мере одна из орбит содержит более одного элемента, поскольку действие G на X предполагалось точным. Без ограничения общности можно считать, что $|Nx_1| > 1$. Тогда $hx_1 \neq x_1$ для некоторого $h \in N$. Так как G действует 2-транзитивно на X, то найдется элемент $g \in G$ такой, что $gx_1 = x_2$ и $ghx_1 = x_1$. Тогда с одной стороны $ghg^{-1}x_2 \in Nx_2$, а с другой $ghg^{-1}x_2 = ghx_1 = x_1 \in Nx_1$, что невозможно, поскольку $Nx_1 \cap Nx_2 = \emptyset$. □

Предложение 4.6.7 (Критерий простоты)**.** *Пусть G действует на X точно и 2-транзитивно. Тогда G проста, если выполнены условия:*

1) $G = G'$,

2) существует точка $x \in X$, в стабилизаторе G_x которой содержится подгруппа A такая, что

a) A абелева,

b) A нормальна в стабилизаторе G_x,

c) $G = < gAg^{-1} \mid g \in G >$.

Доказательство. Пусть N – неединичная нормальная подгруппа в G. Простота группы G будет доказана, если показать, что N совпадает с G.

По предложению 4.6.6 N действует транзитивно на X и, значит, $X = Gx = Nx$. Поэтому $G = NG_x$, где G_x – стабилизатор точки x. Действительно, для любого $g \in G$ существует $h \in N$ такой, что $gx = hx$. Поэтому $h^{-1}gx = x$ и, значит, $h^{-1}g \in G_x$ откуда следует, что $g = h(h^{-1}g) \in NG_x$.

Покажем, что $G = NA$. В силу условия c) любой $g \in G$ можно представить в виде $g = g_1 a_1 g_1^{-1} \cdot \dots \cdot g_k a_k g_k^{-1}$, где $a_i \in A$, $g_i \in G$. Далее запишем g_i в виде $g_i = h_i s_i$, где $h_i \in N$, $s_i \in G_x$, тогда $g = h_1 s_1 a_1 s_1^{-1} h_1^{-1} \cdot \dots \cdot h_k s_k a_k s_k^{-1} h_k^{-1}$. При каноническом гомоморфизме $G \to G/N$ образы элементов g и $a := s_1 a_1 s_1^{-1} \cdot \dots \cdot s_k a_k s_k^{-1}$ одинаковы. Так как A нормальна в стабилизаторе G_x в силу условия b), элемент a принадлежит A, поэтому $g \in Na \subset NA$. Поскольку $g \in G$ был произвольным элементом, получаем, что $G = NA$.

Далее заметим, что любой коммутатор вида $[h_1 a_1, h_2 a_2]$, где $h_1, h_2 \in N$ и $a_1, a_2 \in A$, лежит в ядре канонического гомоморфизма $G \to G/N$, поскольку образ в G/N такого коммутатора равен образу коммутатора $[a_1, a_2] = e$ (последний равен единице в силу абелевости A). Таким образом, $[h_1 a_1, h_2 a_2] \in N$, и мы получаем $G = G' = (NA)' \subset N$. Следовательно, $G = N$, что и нужно было установить. □

Трансвекции. Матрицы размера $n \times n$ с элементами из поля $\mathbb{K}$ вида

$$t_{ij}(\alpha) := E + \alpha E_{ij}, \quad i \neq j, \ \alpha \in \mathbb{K},$$

где E – единичная матрица, а E_{ij} – матрица, у которой на месте (i, j) стоит 1, а остальные элементы нулевые, называются *трансвекциями*.

Ясно, что определитель любой трансвекции равен 1, поэтому $t_{ij}(\alpha) \in SL(n, \mathbb{K})$.

Умножение матрицы слева на $t_{ij}(\alpha)$ сводится к тому, что в матрице к i-й строке прибавляется j-я строка умноженная на α, а остальные строки не меняются. В частности, $t_{ij}^{-1}(\alpha) = t_{ij}(-\alpha)$.

Таким образом, трансвекции дают элементарные преобразования над строками 1-го типа.

Предложение 4.6.8. *1) $SL(n, \mathbb{K})$ порождается трансвекциями;*

2) $[t_{ik}(\alpha), t_{kj}(\beta)] = t_{ij}(\alpha\beta)$, где i, j, k попарно различны;

3) $[t_{ij}(\alpha), \operatorname{diag}(\alpha_1, \dots, \alpha_n)] = t_{ij}(\alpha(1 - \frac{d_i}{d_j}))$;

4) $M_\sigma t_{ij}(\alpha) M_\sigma^{-1} = t_{\sigma(i)\sigma(j)}(\alpha)$, где $\sigma \in S_n$ и M_σ – матрица, у которой на местах $(\sigma(i), i)$, $i = 1, \dots, n$, стоит 1, а на остальных местах 0.

Доказательство. 1) Следует из того, что любую матрицу из $SL(n, \mathbb{K})$ можно элементарными преобразованиями 1-го типа привести к единичной.

Формулы 2), 3), 4) проверяются вычислением. □

Предложение 4.6.9. *Если $|\mathbb{K}| > 3$, то $SL(n, \mathbb{K})' = GL(n, \mathbb{K})' = SL(n, \mathbb{K})$.*

Доказательство. Так как $GL(n,\mathbb{K})/SL(n,\mathbb{K}) = \mathbb{K}^*$ абелева, имеем включение $GL(n,\mathbb{K})' \subset SL(n,\mathbb{K})$. Вычисление показывает, что

$$\left[\begin{pmatrix} \lambda & 0 \\ 0 & \frac{1}{\lambda} \end{pmatrix}, \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}\right] = \begin{pmatrix} 1 & (\lambda^2-1)c \\ 0 & 1 \end{pmatrix}.$$

Поскольку в $\mathbb{K}$ имеется $\lambda \neq 0, \pm 1$, коммутант $SL(n,\mathbb{K})'$ содержит все трансвекции и, следовательно, совпадает с $SL(n,\mathbb{K})$. □

Замечание 4.6.10. На самом деле $GL(n,\mathbb{K})' = SL(n,\mathbb{K})$ во всех случаях, кроме $n = 2,\ \mathbb{K} = \mathbb{F}_2$.

Следствие 4.6.11. $PSL(n,\mathbb{K})' = PSL(n,\mathbb{K})$, *кроме случаев* $PSL(2,2),\ PSL(2,3)$.

Доказательство. Если $G' = G$ и N нормальна в G, то $(G/N)' = G/N$. Действительно, так как $G \to G/N$ – эпиморфизм, образ G' в G/N при этом эпиморфизме совпадает с $(G/N)'$, но поскольку $G' = G$, этот образ совпадает с G/N, т.е. $(G/N)' = G/N$.

Остается в качестве G взять $SL(n,\mathbb{K})$, а в качестве N ее центр. □

Доказательство теоремы Жордана – Диксона. Положим $V := \mathbb{K}^n$ и пусть $e_1, \ldots, e_n$ – стандартный базис. Обозначим через X множество прямых, проходящих через начало координат (т. е. $X = \mathbb{K}P^{n-1}$ – проективное пространство). Для ненулевого вектора v обозначим через $\bar{v}$ прямую с направляющим вектором v. Образ матрицы $A \in SL(n,\mathbb{K})$ в $G := PSL(n,\mathbb{K})$ обозначим через $\bar{A}$. Тогда действие G на X определяется как $\bar{A}\bar{v} = \overline{Av}$. Покажем, что это действие удовлетворяет критерию простоты.

1) Проверим точность действия. Пусть $\bar{A}$ действует на X как тождественное преобразование. Тогда $Ae_i = \lambda e_i$, $i = 1, \ldots, n$, и $A(e_1 + \cdots + e_n) = \lambda(e_1 + \cdots + e_n)$, поэтому $\lambda(e_1 + \cdots + e_n) = Ae_1 + \cdots + Ae_n = \lambda_1 e_1 + \cdots + \lambda_n e_n$, откуда следует, что $\lambda = \lambda_1 = \cdots = \lambda_n$. Значит A – скалярная матрица и, следовательно, $\bar{A}$ – единица группы G.

2) 2-транзитивность действия следует из того, что прямые $\bar{e}_1, \bar{e}_2$ можно перевести в любые две прямые элементом $\bar{v}_1, \bar{v}_2$ элементом $\bar{A}$, где $A \in SL(n,\mathbb{K})$ – такая матрица, у которой 1-й и 2-й столбцы пропорциональны v_1 и v_2 соответственно.

3) Равенство $G = G'$ было длказано выше.

4) Пусть $x = \bar{e}_n$. Тогда

$$G_x = \{\bar{B} \mid B = (b_{ij}),\ b_{1n} = \cdots = b_{n-1,n} = 0\},$$

т.е. G_x состоит из всех таких $\bar{B}$, что Be_n пропорционален e_n. Пусть $A < G_x$ – подгруппа, состоящая из $\bar{B}$ таких, что

$$B = \begin{pmatrix} 1 & 0 & \ldots & 0 \\ \vdots & \ddots & & \vdots \\ 0 & \ldots & 1 & 0 \\ * & \ldots & * & 1 \end{pmatrix}.$$

Легко видеть, что A абелева и нормальна в G_x.

5) Равенство $G = \{gAg^{-1} \mid g \in G\}$ следует из того, что в A лежат образы трансвекций вида $t_{ni}(\alpha)$ и из пунктов 1) и 4) предложения 4.6.8.

□

4.7 Мультипликативные группы конечного поля и кольца $\mathbb{Z}_n$ и немного элементарной теории чисел

Пусть K – кольцо с единицей. Скажем, что элемент $u \in K$ обратим, если найдется $v \in K$ такой, что $uv = vu = 1$.

Определение 4.7.1. Пусть K – кольцо с единицей и K^* – множество обратимых элементов кольца K, рассматриваемое с операцией умножения (в кольце K). Это множество является группой (ее единица – единица кольца K) и называется гуппой обратимых элементов кольца K или мультипликативной группой кольца K.

Задача 4.7.1. Показать, что
a) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}^* \cong \mathbb{Z}_2$,
b) $\mathrm{Aut}(\mathbb{Z}_\mathrm{n}) \cong \mathbb{Z}_n^*$.

Если $K = \mathbb{K}$ – поле, то любой ненулевой элемент обратим, поэтому $\mathbb{K}^* := \mathbb{K} \setminus 0$.

Определение 4.7.2. Группу $\mathbb{K}^*$ называют мультипликативной группой поля.

Таким образом, в случае конечного поля получаем $|\mathbb{K}^*| = |\mathbb{K}| - 1$. Если p – характеристика конечного поля, то $\mathbb{K}$ содержит простое поле $\mathbb{F}_p$ из p элементов и само является векторным пространством размерности n (для некоторого натурального n) над полем $\mathbb{F}_p$. Поэтому $|\mathbb{K}| = p^n$. С точностью до изоморфизма такое поле единственно и его обычно обозначают $\mathbb{F}_q$, $q = p^n$.

В частности, $|\mathbb{F}_p^*| = p - 1$ и, поскольку порядок любого элемента делит порядок группы, получаем $a^{p-1} = 1$ для любого $a \in \mathbb{F}_p^*$, и умножая это равенство на a получаем также, что $a^p = a$ (здесь операция в группе $\mathbb{F}_p^*$ – это операция умножения элементов в поле $\mathbb{F}_p$).

Теорема 4.7.2 (Малая теорема Ферма)**.** *Если $k \in \mathbb{Z}$ не делится на простое число p, то* $k^{p-1} \equiv 1 \pmod p$. *Для любого $k \in \mathbb{Z}$ имеем* $k^p \equiv k \pmod p$.

Доказательство. Первое утверждение, а также второе утверждение для k не делящегося на p, прямо следует из рассуждения, приведенного непосредственно перед теоремой. Второе утверждение для k делящегося на p очевидно. □

Теорема 4.7.3 (Теорема Вильсона)**.** *Если p – простое число, то* $(p-1)! \equiv -1 \pmod p$.

Доказательство. Элементы группы $\mathbb{F}_p^*$ будем представлять целыми числами k такими, что $1 \leq k \leq p-1$. Если $k \in \mathbb{F}_p^*$ и $k^2 = 1$ в $\mathbb{F}_p^*$ (т. е. $k^2 \equiv 1 \pmod p$), то $k^2 - 1 = (k-1)(k+1)$ делится на p. Так как $1 \leq k \leq p-1$ и p – простое число, то либо $k = 1$, либо $k = p-1$. Следовательно, для k таких, что $2 \leq k \leq p-2$, нет чисел обратных самим себе в $\mathbb{F}_p^*$. Поэтому множество чисел $\{2, \ldots, p-2\}$ разбивается на пары взаимно обратных и значит $2 \cdot 3 \cdot \cdots \cdot (p-2) = 1$ в $\mathbb{F}_p^*$, откуда следует, что $1 \cdot 2 \cdot \cdots \cdot (p-1) = p-1$ в $\mathbb{F}_p^*$, т. е. $(p-1)! = p-1$ в $\mathbb{F}_p^*$. Последнее равенство можно понимать и как равенство в поле $\mathbb{F}_p$. Оно эквивалентно сравнению $(p-1)! \equiv p-1 \equiv -1 \pmod p$. □

На самом деле, $\mathbb{F}_p^*$ – циклическая группа порядка $p-1$. Аналогичное верно и в общем случае, т. е. группа ненулевых элементов конечного поля (с операцией умножения элементов поля) является циклической:

Теорема 4.7.4. *Мультипликативная группа конечного поля циклическая, т. е. если $\mathbb{K}$ – конечное поле, то группа K^* изоморфна $\mathbb{Z}_{q-1}$, где $q = |\mathbb{K}|$.*

Доказательство. Пусть $\mathbb{K}$ – конечное поле, $\mathbb{K}^* = \mathbb{K} \setminus 0$ – его мультипликативная группа (группа обратимых элементов с операцией умножения) и $|\mathbb{K}^*| = p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}$, где p_j простые и $p_i \neq p_j$ при $i \neq j$. Пусть P_i – силовская p_i-подгруппа в $\mathbb{K}^*$, $|P_i| = p_i^{k_i}$, $i = 1, \ldots, s$. Из теоремы Лагранжа следует, что порядки элементов из P_i делят $p_i^{k_i}$ и поэтому являются степенями простого числа p_i. Если бы в P_i не существовало элемента максимального порядка $p_i^{k_i}$, то для любого $g \in P_i$ было бы выполнено равенство $g^{p_i^{k_i-1}} = 1$. Однако в поле $\mathbb{K}$ уравнение $x^{p_i^{k_i-1}} = 1$ может иметь не более $p_i^{k_i-1}$ корней (для доказательства можно использовать теорему Безу). Полученное противоречие показывает что существует элемент порядка $p_i^{k_i}$ в $\mathbb{K}^*$, т. е. P_i является циклической группой порядка $p_i^{k_i}$.

Из доказанного получаем, что существуют $g_1, \ldots, g_s \in \mathbb{K}^*$ такие, что $\mathrm{ord}(g_i) = p_i^{k_i}$, откуда следует, что $\mathrm{ord}(g_1 \cdot \cdots \cdot g_s) = p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}$ и, значит, $\mathbb{K}^*$ – циклическая группа (порядка $p_1^{k_1} \cdot \cdots \cdot p_s^{k_s}$). Отметим, что соотношение с порядками вытекает из следующего общего простого утверждения: если элементы a, b группы G коммутируют, т. е. $ab = ba$, и их порядки взаимно просты, т. е. $(\mathrm{ord}(a), \mathrm{ord}(b)) = 1$, то порядок произведения этих эдементов равен произведению их порядков, т. е. $\mathrm{ord}(ab) = \mathrm{ord}(a) \cdot \mathrm{ord}(b)$.

2-е доказательство. Положим $d := \exp(\mathbb{K}^*)$. Экспонента d не превосходит порядка группы $\mathbb{K}^*$, т. е. $d \leq |\mathbb{K}^*|$. Все элементы из $\mathbb{K}^*$ являются корнями многочлена $x^d - 1$, тем самым этот многочлен делится на произведение $|\mathbb{K}^*|$ линейных множителей $\prod\limits_{\alpha \in \mathbb{K}^*} (x - \alpha)$, т. е. $d \geq |\mathbb{K}^*|$). Таким образом, получаем $d = |\mathbb{K}^*|$. Следовательно, в $\mathbb{K}^*$ имеется элемент, попядок которого равен порядку группы $\mathbb{K}^*$, что означает, что группа циклическая. □

4.7.1 Прямая сумма колец

Пусть K_1, K_2 – кольца. Определим прямую сумму колец $K_1 \oplus K_2$ как прямую сумму абелевых групп K_1 и K_2 с умножением $(k_1, k_2) \cdot (k_1', k_2') = (k_1 k_1', k_2 k_2')$, где $k_1, k_1' \in K_1$, $k_2, k_2' \in K_2$.

Пусть m, n – взаимно простые натуральные числа. Тогда кольца $\mathbb{Z}_{mn}$ и $\mathbb{Z}_m \oplus \mathbb{Z}_n$ изоморфны. Действительно, рассмотрим следующую коммутативную диаграмму, в которой верхняя стрелка – диагональное вложение $k \mapsto (k, k)$, а остальные стрелки – канонические отображения факторизации

$$\begin{array}{ccc} \mathbb{Z} & \to & \mathbb{Z} \oplus \mathbb{Z} \\ \downarrow & & \downarrow \\ \mathbb{Z}_{mn} & \to & \mathbb{Z}_m \oplus \mathbb{Z}_n \end{array}$$

Нижняя горизонтальная стрелка – мономорфизм, поскольку если целое число делится на m и одновременно на n, которые взаимно просты, то оно делится на mn. Поскольку порядки групп в нижней строчке диаграммы одинаковы, нижняя стрелка – изоморфизм.

Далее по индукции легко доказывается, что кольца $\mathbb{Z}_m$ и $\mathbb{Z}_{m_1} \oplus \cdots \oplus \mathbb{Z}_{m_r}$ изоморфны, если $m_1, \ldots, m_r$ – попарно взаимно простые натуральные числа и $m = m_1 \cdot \cdots \cdot m_r$. Отсюда вытекает следующая теорема.

Теорема 4.7.5 (Китайская теорема об остатках)**.** *Пусть $m_1, \ldots, m_r$ попарно взаимно простые натуральные числа и пусть $b_1, \ldots, b_r \in \mathbb{Z}$. Тогда найдется $a \in \mathbb{Z}$ такое, что $a \equiv b_i \pmod{m}$, $i = 1, \ldots, r$ где $m = m_1 \cdot \cdots \cdot m_r$.*

Теорема означает, что следующая система сравнений разрешима (для любых целых b_i)

$$x \equiv b_i \pmod{m_i}, \quad i = 1, \ldots, r.$$

Поясним как практически найти ее решение. Положим

$$M_i := m_1 \cdot \cdots \cdot m_{i-1} m_{i+1} \cdot \cdots \cdot m_r = \frac{m}{m_i}, \ \ i = 1, \ldots, r.$$

Поскольку $(m_i, M_i) = 1$, найдется $\widetilde{M_i}$, что $M_i \widetilde{M_i} \equiv 1 \pmod{m_i}$, $\quad i = 1, \ldots, r$. Тогда

$$x_0 := \sum_{i=1}^{r} b_i M_i \widetilde{M_i}$$

является решением системы. Действительно, так как m_j делит M_i при $i \neq j$, получаем $x_0 \equiv b_j M_j \widetilde{M_j} \equiv b_j \pmod{m_j}$, $\quad j = 1, \ldots, r$. Остальные решения имеют вид $x = x_0 + k m_1 \cdot \cdots \cdot m_r$, $k \in \mathbb{Z}$.

4.7.2 Функция Эйлера

Пусть K – прямая сумма колец K_1 и K_2. Тогда $K^* \cong K_1^* \times K_2^*$. В частности, если m и n взаимно просты (т.е. $(m, n) = 1$), то $\mathbb{Z}_{mn} \cong \mathbb{Z}_m \oplus \mathbb{Z}_n$, поэтому $\mathbb{Z}_{mn}^* \cong \mathbb{Z}_m^* \times \mathbb{Z}_n^*$.

Пусть $n = p_1^{d_1} \cdot \cdots \cdot p_k^{d_k}$, где p_i – попарно различные простые числа. Тогда

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{d_1}}^* \times \cdots \times \mathbb{Z}_{p_k^{d_k}}^*.$$

Определение 4.7.3. Функция $\varphi(n) = |\mathbb{Z}_n^*|$ натурального аргумента $n \in \mathbb{N}$ называется функцией Эйлера.

Из определения обратимых элементов следует, что $\varphi(n)$ равно числу натуральных чисел не превосходящих n и взаимнопростых с n. Обычно так функцию Эйлера и определяют.

Кроме того, $\varphi(p^s) = p^s - p^{s-1} = p^s(1 - \frac{1}{p})$, где p – простое число. Действительно, число взаимно простое с p^s взаимно просто с p. Таким образом, достаточно подсчитать число натуральных чисел не превосходящих p^s и делящихся на p и вычесть его из p^s. Такие числа имеют вид pm, где $1 \leq m \leq p^{s-1}$, поэтому их число равно p^{s-1}.

Функция φ мультипликативна, т. е. $\varphi(mn) = \varphi(m)\varphi(n)$, если m и n взаимно просты (это равенство – прямое следствие указанного выше соотношения между мультипликативными группами колец). Следовательно, если $n = p_1^{d_1} \cdot \cdots \cdot p_k^{d_k}$, где p_i – попарно различные простые числа, то

$$\varphi(n) = \varphi(p_1^{d_1}) \cdot \cdots \cdot \varphi(p_k^{d_k}) = (p_1^{d_1} - p_1^{d_1 - 1}) \cdot \cdots \cdot (p_k^{d_k} - p_k^{d_k - 1}) = n \left(1 - \frac{1}{p_1}\right) \cdot \cdots \cdot \left(1 - \frac{1}{p_k}\right).$$

Приведем без доказательства еще одно полезное соотношение:

$$\sum_{d \mid n} \varphi(d) = n.$$

Из того, что порядок элемента делит порядок группы получаем, что $a^{\varphi(n)} = 1$ для любого $a \in \mathbb{Z}_n^*$. Поэтому справедливо следующее обобщение малой теоремы Ферма ($\varphi(p) = p - 1$ для простого p), принадлежащее Эйлеру.

Теорема 4.7.6 (Теорема Эйлера)**.** *Пусть $n, k \in \mathbb{N}$, $n > 1$ и k взаимно просто с n. Тогда $k^{\varphi(n)} \equiv 1 \pmod{n}$*

Теорема 4.7.7. *Пусть p – нечетное простое число. Тогда $\mathbb{Z}_{p^m}^*$ является циклической группой порядка $\varphi(p^m) = p^m - p^{m-1} = p^m(1 - \frac{1}{p})$.*

Группа $\mathbb{Z}_{2^m}^*$ является циклической для $m = 1, 2$, причем $|\mathbb{Z}_2^*| = 1$, $|\mathbb{Z}_4^*| = 2$. При $m \geq 3$ группа $\mathbb{Z}_{2^m}^*$ имеет порядок $\varphi(2^m) = 2^{m-1}$ и является произведением циклических групп порядков 2^{m-2} и 2, т. е. $\mathbb{Z}_{2^m}^* \cong \mathbb{Z}_{2^{m-2}} \times \mathbb{Z}_2$.

Следствие 4.7.8. *Группа $\mathbb{Z}_m^*$ является циклической только при $m = 2, 4, p^k, 2p^k$, где p – нечетное простое число.*

Отметим, что порядки груп $\mathbb{Z}_{p^k}^*$ и $\mathbb{Z}_{2p^k}^*$ одинаковы и равны $p^k(1 - \frac{1}{p})$, p – нечетное простое число.

По другому это следствие можно сформулировать так: примитивный корень по модулю m существует тогда и только тогда, когда $m = 2, 4, p^k, 2p^k$, где p – нечетное простое число.

4.8 Шифрование с открытым ключом RSA

В этом параграфе мы очень кратко опишем алгоритм шифрования с открытым ключом RSA, названный так по первым буквам фамилий авторов – Ривест, Шамир и Адлеман. Алгоритм основан на вычислительной сложности задачи факторизации больших натуральных чисел (факторизация – нахождение разложения натурального числа в произведение простых чисел). Если простые числа p и q состоят из нескольких сотен цифр, то зная $n = pq$ за обозримое время не удастся найти сомножители p и q.

Итак пусть задано $n = pq$, где p и q – простые числа. В качестве сообщения Отправителем будет передаваться Получателю целое число $a \in \{0, 1, \ldots, n-1\}$, которое Отправитель предварительно зашифрует.

Выберем натуральные числа e и d большие 1 и меньшие $\varphi(n) = (p-1)(q-1)$, где $\varphi(n)$ – функция Эйлера, так, чтобы

$$ed \equiv 1 \pmod{\varphi(n)}.$$

Таким образом, e и d взаимно обратны в кольце $\mathbb{Z}_{\varphi(n)}$ (если каким-нибудь способом выбрать e взаимно простым с $\varphi(n)$, то d можно, например, найти с помощью алгортма Евклида). Пару чисел n и e, называемую открытым ключом, Получатель передает Отправителю, число d держит в секрете (закрытый ключ). Шифрование состоит в том, что Отправитель вычисляет $b := a^e \pmod{n}$. Затем он отправляет b по каналу связи Получателю, который дешифрует сообщение вычислив $b^d \pmod{n}$. Остается показать, что a и $b^d = a^{ed}$ равны по модулю n. Заметим, что если постороннее лицо перехватит сообщение, то для дешифрования ему нужно будет знать $\varphi(n)$, а для этого придется решить задачу факторизации числа n.

Итак, покажем, что $a = a^{ed} \pmod{n}$. Мы ограничимся случаем, когда a взаимно просто с n и, следовательно, по теореме Эйлера $a^{\varphi(n)} \equiv 1 \pmod{n}$. [Случай когда a делится на p или на q оставляется читателю в качестве упражнения.] Поскольку e и d положительны и $ed \equiv 1 \pmod{\varphi(n)}$, найдется неотрицательное целое число m такое, что $ed = 1 + m\varphi(n)$. Поэтому

$$a^{ed} = a^{1+m\varphi(n)} = a(a^{\varphi(n)})^m \equiv a \cdot 1^m \equiv a \pmod{\varphi(n)}.$$

5 | Доклады студентов

5.1 Кольца и поля

Опр. *Кольцом* называется множество A с бинарными операциями сложения "+" и умножения "·", удовлетворяющие следующим аксиомам.
(AA) $\forall a, b, c \in A : a + (b + c) = (a + b) + c$ (ассоциативность сложения)
(AZ) $\exists 0 \in A\ \forall a \in A : a + 0 = 0 + a = a$ (существование *нуля*)
(AI) $\forall a \in A\ \exists(-a) \in A$(*противоположный*): $a + (-a) = (-a) + a = 0$
(AC) $\forall a, b \in A : a + b = b + a$ (коммутативность сложения)
(MA) $\forall a, b, c \in A : a \cdot (b \cdot c) = (a \cdot b) \cdot c$ (ассоциативность умножения)
(D) $\forall a, b, c \in A : (a + b) \cdot c = a \cdot c + b \cdot c$ (дистрибутивность)

Полукольцо := (AA) + (D) + (MA)

Кольцо с единицей := Кольцо + (MId)
(MId) $\forall a \in A \exists 1 \in A : a \cdot 1 = 1 \cdot a = a$ (существование *единицы*)

Коммутативное кольцо := Кольцо + (MC)
(MC) $\forall a, b \in A : a \cdot b = b \cdot a$ (коммутативность умножения)

Кольцо с делением (тело) := Кольцо с единицей + (MI)
(MI) $\forall a \in A \setminus \{0\}\ \exists a^{-1} \in A$(*обратный*): $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Опр. *Поле* := Коммутативное кольцо с единицей + (MI)

Свойства аксиом
1^0. $\exists! 0 \in A$
2^0. $\forall a \in A \exists!(-a) \in A$
3^0. $\exists! 1 \in A$
4^0. $\forall a \in A\ 0 \cdot a = 0$
5^0. $\forall a \in A\ (-1) \cdot a = (-a)$

Примеры
$\mathbb{N}$ - полукольцо.
$M_{n \times n}$ - кольцо с единицей.
$\{0\}$ - единственное кольцо, где 0 = 1.
$\mathbb{Z}, \mathbb{Z}_n$, $\mathbb{Z}[i] = \{a + i \cdot b \mid \forall a, b \in \mathbb{Z}\}$ - коммутативные кольца с единицей (а $\mathbb{Z}_p$ при простом p - поле).
$A[x] = \{a_0 + a_1 x + \cdots + a_n x^n \mid a_i \in A\}$, где A - коммутативное кольцо - коммутативное кольцо.
$\mathbb{H}$ - тело.
$\mathbb{Q}, \mathbb{R}, \mathbb{C}$ - поля.

Опр. Коммутативное кольцо с единицей и без делителей нуля называется *целостным кольцом* (областью целостности).

Лемма. Поле является целостным кольцом.
◀ Надо доказать, что в поле F нет делителей нуля.

Пусть a содержится в поле F. Тогда a - обратим, т.е. $\exists a^{-1} \in F : a^{-1}a = 1$. И пусть a - делитель нуля, т.е. $\exists b : ab = 0$. Тогда $0 = a^{-1}0 = a^{-1}(ab) = (a^{-1}a)b = 1b = b$. ►

Утв. Кольцо $\mathbb{Z}_m$ - поле $\Leftrightarrow$ m - простое.
◄ Пусть m - не простое, т.е. $m = k \cdot l$, где $1 < k, l < n$. Тогда $[k]_m \neq 0, [l]_m \neq 0$, но $[k]_m \cdot [l]_m = [m]_m = [0]_m$. Получили противоречие с тем, что в поле нет делителей нуля.
Пусть m - простое. Найдем обратный элемент для произвольного $a \in \mathbb{Z}_m$.
НОД(a, m)=1, т.к. a и m взаимно просты. Тогда $\exists x, y : ax + my = 1$. $[a]_m \cdot [x]_m + [m]_m \cdot [y]_m = [1]_m \Leftrightarrow [a]_m \cdot [x]_m = [1]_m$. ►

Опр. *Гомоморфизм* полей/колец/групп $\varphi : A \longrightarrow B$ - отображение множеств, такое что $\forall a, b \in A$ $\varphi(a + b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\varphi(b)$

Свойста гомоморфизма колец
Пусть $\varphi : A \longrightarrow B$ - гомомрфизм.
1^0. $\varphi(0_A) = 0_B$.
◄ $\varphi(a_A) = \varphi(a_A + 0_A) = \varphi(a_A) + \varphi(0_A)$
$-\varphi(a_A) + \varphi(a_A) = -\varphi(a_A) + \varphi(a_A) + \varphi(0_A)$
$0_B = \varphi(0_A)$ ►
2^0. $\varphi(-a) = -\varphi(a)$
◄ $0 = \varphi(0) = \varphi(a - a) = \varphi(a) + \varphi(-a)$
$-\varphi(a) = -\varphi(a) + \varphi(a) + \varphi(-a)$
$-\varphi(a) = \varphi(-a)$ ►

Опр. *Мономорфизм/эпиморфизм/изоморфизм* полей/колец/групп - гомоморфизм полей/колец/групп, такой что на уровне множеств соответсвенно инъекция/сюръекция/биекция.

Пример
$\varphi : \mathbb{Z} \longrightarrow \mathbb{Z}_m$, т.е. $a \longmapsto [a]_m$. φ - эпиморфизм. При этом отображении $Ker(\varphi) = m\mathbb{Z}$.

5.2 Поиск групп данного порядка

Дано число N — порядок.
Найти все попарно неизоморфные группы порядка N.

Будем пользоваться тремя фактами.
Утв1. Если порядок группы простое число, то она изоморфна C_p.
◄ 1. Порядок любого элемента равен порядку порожденной им циклической подгруппы.
2. Порядок подгруппы делит порядок группы. (Теорема Лагранжа)
(1,2) ⇒ если порядок группы p — простое число, то порядок любого элемента, отличного от единичного, равен p.
3. Любые циклические группы одного порядка изоморфны между собой (естественный изоморфизм $\phi : a^k \longrightarrow b^k$). ((1,2),3) ⇒ само утверждение ►

Утв2. Если порядок группы G имеет вид $2p$, где p — простое и $p > 2$, то эта группа либо D_p, либо C_{2p}.
◄ Если в G есть элемент порядка $2p$, то она циклическая, и, следовательно изоморфна C_{2p}.
В дальнейшем мы будем предполагать, что такого элемента нет, и будем пытаться доказать, что она изоморфна D_p.
Первый шаг: есть элемент порядка p. По теореме Лагранжа, каждый неединичный элемент имеет порядок p или 2. Предположим, что каждый элемент порядка 2. Тогда она коммутативна. Тогда $\forall a, b \in G^*$, $\{e, a, b, ab\}$ — подгруппа порядка 4, что противоречит теореме Лагранжа, т.к. не делит $2p$ ($p > 2$). Значит, в группе G есть элемент порядка p.
Пусть есть элемент a порядка p.
Второй шаг: каждый элемент, не принадлежащий $\langle a\rangle_p$, имеет порядок 2.
Пусть $b \notin \langle a\rangle_p$. Тогда $G = \langle a\rangle_p \cup \langle a\rangle_p b$. Так как $\langle a\rangle_p$ и $\langle a\rangle_p b$ единственные смежные классы в разложении G по нормальной (индекса 2) подгруппе $\langle a\rangle_p$, то $\langle a\rangle_p b^2 = \langle a\rangle_p b$ или $\langle a\rangle_p$. Если $\langle a\rangle_p b^2 = \langle a\rangle_p b$, то $\langle a\rangle_p b = \langle a\rangle_p$, что противоречит тому, что $b \notin \langle a\rangle_p$. Значит $\langle a\rangle_p b^2 = \langle a\rangle_p$, следоваетельно $b^2 \in \langle a\rangle_p$. Из того что $|\langle a\rangle_p| = p$ следует, что $b^2 = e$ или $|b^2| = p$. Если $|b^2| = p$, то, т.к. мы изначально предположили, что в G нет элемента порядка $2p$, $|b| = p$. Но это противоречит тому, что $b \notin \langle a\rangle_p \Rightarrow |b| = 2$. Посмотрим теперь на элемент ab. $ab \notin \langle a\rangle_p \Rightarrow |ab| = 2 \Rightarrow ab = (ab)^{-1} = b^{-1}a^{-1} = ba^{-1}$, последнее равенство, т.к. $|b| = 2$. В итоге, получаем $a = ba^{-1}b^{-1}$ — недостающее соотношение для D_p. ►

Лемма1. Фактор-группа некоммутативной группы G по ее центру $Z(G)$ не может быть циклической.
◄ От противного. Допустим, что смежный класс $gZ(G)$ — порождающий элемент фактор-группы $G/Z(G)$. Рассмотрим произвольные элементы $a, b \in G$. Тогда $aZ(G) = (gZ(G))^n = g^nZ(G)$, $bZ(G) = (gZ(G))^m = g^mZ(G)$, т.е. $a = g^n z_1$, $b = g^m z_2$, где $z_1, z_2 \in Z(G)$. Теперь посмотрим: $ab = g^n z_1 g^m z_2 = g^{n+m} z_1 z_2 = g^m z_2 g^n z_1 = ba$, т.е. группа G коммутативна. Противоречие. ►

Лемма2. Пусть G — группа, $|G| = p^n$, p — простое. Тогда $Z(G) \neq \{e\}$.
◄ без док-ва ►

Утв3. Если $|G| = p^2$, где p — простое, то эта группа либо $C_p \times C_p$, либо C_{p^2}. (без доказательства)
◄ Хотим доказать, что наша группа G может быть только коммутативной, тогда утверждение будет верным (по ранее доказанной теореме). Для того, чтобы это сделать, будем сравнивать центр группы и ее саму. Так как центр любой группы является ее подгруппой (и к тому же нормальной), а подгруппы групп G имеют порядки $1, p, p^2$, то соответственно, $|Z(G)|$ может быть равен $1, p^2$ или p.
Если $|Z(G)| = p^2 = |G|$, то группа G коммутативна и утверждение верно.
Если $|Z(G)| = p$, то $|G/Z(G)| = |G|/|Z(G)| = \frac{p^2}{p} = p$, из чего можно ошибочно подумать, что $G/Z(G)$ — циклическая группа порядка p, но мы этого не сделаем, т.к. у нас есть лемма. Значит, группа G коммутативна.
Теперь докажем, что $Z(G) \neq \{e\}$ или, что то же самое, $|Z(G)| \neq 1$. ... ►

Если число N не подошло ни под одно из этих условий:
1) Сперва найдем все коммутативные группы порядка N следующим образом:

разложим наше число $N = p_1^{k_1} p_2^{k_2} \dots p_s^{k_s}$, и тогда каждое разложение в сумму каждой степени $p_i (i = 1, ..., s)$ будет давать нам разложение в прямое произведение циклических групп, неизоморфное другим разложениям.
Например, для $N = 12$: $12 = 2^2 3 \Rightarrow C_2 \times C_2 \times C_3 \cong C_2 \times C_6$ и $C_4 \times C_3 \cong C_{12}$.
2) Теперь, для поиска некоммутативных групп, будем пользоваться теоремой Кэли (любая группа порядка N изоморфна некоторой подгруппе S_N). Это имеет смысл, т.к. на ассоциативность проверка отпадает.
Сначала выберем только те подстановки из S_N, чей порядок делит N, т.к. только они могут быть элементами группы порядка N (по теореме Лагранжа). Из них возьмем подстановки, чей порядок h_1 равен наименьшему делителю числа N, и будем порождать для них циклические группы порядка N (для которых возможно) с двумя образующими подстановками, проверяя в процессе эти группы на коммутативность (так как все коммутативные группы данного порядка мы нашли в пункте 1). Потом берем подстановки, чей порядок h_2 — второй по величине делитель числа N, и порождаем циклические группы порядка N (за этим следим по ходу выполнения) с двумя образующими, где на одном месте стоит подстановка порядка h_2, а на втором либо подстановка порядка h_1, либо подстановка порядка h_1. Далее берем подстановки с порядком равным третьему по величине делителю числа N и повторяем все. Так как число N конечно, то это когда-нибудь прекратится. При этом каждый раз, когда мы находим новую группу, мы проверяем: не изоморфна ли она уже какой-то найденой группе. Опытным путем было выявлено, что очень ускоряет проверку на изоморфизм простая проверка на совпадение порядков элементов этих групп (тем более, что порядки уже посчитаны, т.к. были нужны в самом начале для отбора подстановок-кандидатов на элементы). Но, если и мультимножества порядков совпали, то проверяем по таблицам Кэли этих групп до первого несовпадения.

Результаты приведены в таблице ниже.

Порядок	Группы
1	C_1
2	C_2
3	C_3
4	$C_4, V_4 \cong C_2 \times C_2$
5	C_2
6	C_6, S_3
7	C_7
8	$C_8, C_4 \times C_2, C_2 \times C_2 \times C_2, D_4, Q_8$
9	$C_9, C_3 \times C_3$
10	C_{10}, D_5
11	C_{11}
12	$C_{12}, C_6 \times C_2, D_6, A_4, C_3 \leftthreetimes C_4$

6 | Типовой расчет

Задача 1

Найти все целочисленные решения уравнения $ax^k - by^k = 1$, или доказать, что их нет.

N	a	b	k	N	a	b	k	N	a	b	k
1	3	14	2	9	10	11	2	17	13	10	2
2	13	5	1	10	19	14	1	18	24	13	1
3	13	5	2	11	11	14	2	19	13	14	2
4	16	9	1	12	19	15	1	20	24	17	1
5	5	17	2	13	10	7	2	21	13	16	2
6	17	12	1	14	23	17	1	22	24	19	1
7	6	17	2	15	13	7	2	23	19	7	2
8	17	14	1	16	23	19	1	24	27	16	1
								25	2	13	2

Задача 2

Найти в Z_n все решения уравнения $ax^k + b = c$, или доказать, что их нет.

N	a	b	c	n	k	N	a	b	c	n	k
1	9	15	4	19	1	13	8	13	3	17	1
2	1	9	3	19	2	14	1	8	6	16	2
3	8	5	2	19	1	15	9	10	7	16	1
4	1	8	6	19	2	16	1	14	3	16	2
5	5	16	2	18	1	17	13	8	7	16	1
6	1	11	3	18	2	18	1	10	5	15	2
7	13	16	8	18	1	19	11	14	2	15	1
8	1	12	1	18	2	20	1	13	4	15	2
9	6	9	5	17	1	21	3	10	4	14	1
10	1	10	8	17	2	22	1	9	6	14	2
11	7	9	4	17	1	23	9	6	2	14	1
12	1	7	3	17	2	24	1	8	2	14	2
						25	8	7	3	13	1

Задача 3

Доказать, что данное подмножество $H \subset \mathbb{Z}_n$ является группой по умножению. Найти ее порядок. Представить ее в виде произведения циклических групп.

N	H	n	N	H	n	N	H	n
1	A	11	9	C	20	17	A	26
2	B	12	10	A	12	18	A	16
3	B	17	11	B	13	19	A	22
4	A	7	12	B	8	20	A	18
5	C	24	13	C	30	21	A	20
6	A	14	14	C	16	22	A	8
7	A	13	15	A	24	23	A	30
8	A	15	16	A	10	24	A	9
			26	B	16	25	B	15

Подмножество H:

A: Все обратимые элементы в кольце $\mathbb{Z}_n$

B: Все решения уравнения $x^4 = 1$ в кольце $\mathbb{Z}_n$

C: Все решения уравнения $x^2 = 1$ в кольце $\mathbb{Z}_n$

Задача 4

Перечислить возможно большее число неизоморфных групп порядка N_1 и N_2. Доказать, что перечисленные группы попарно не изоморфны.

N	N_1	N_2	N	N_1	N_2	N	N_1	N_2
1	5	28	9	13	20	17	21	16
2	6	26	10	14	19	18	22	15
3	7	27	11	15	18	19	23	10
4	8	23	12	16	17	20	24	7
5	9	22	13	17	12	21	25	14
6	10	25	14	18	11	22	26	9
7	11	24	15	19	8	23	27	4
8	12	21	16	20	5	24	28	13
						25	29	6

Задача 5

Доказать, что отображение φ абелевой группы $G = Z_a \times Z_b$ в себя, задаваемое формулой $\varphi(x) = cx$, является гомоморфизмом. Найти его ядро и образ. Найти факторгруппу $G/Ker\varphi$.

N	a	b	c	N	a	b	c	N	a	b	c
1	4	6	3	9	3	15	5	17	4	14	2
2	5	35	7	10	25	10	5	18	4	10	2
3	9	6	2	11	4	14	14	19	4	14	4
4	2	14	7	12	9	15	15	20	25	10	10
5	2	10	5	13	3	6	2	21	9	15	5
6	25	10	2	14	9	6	3	22	25	10	25
7	4	10	5	15	4	6	2	23	3	15	3
8	4	14	7	16	2	6	3	24	5	35	5
								25	9	15	3

Задача 6

1) Пусть $G \subseteq S_n$ подгруппа, порожденная перестановками α и β. Найти $|G|$. Коммутативна ли она? Какой из известных вам групп она изоморфна?

2) Является ли подгруппа группы G, порожденная элементом α, нормальной подгруппой? Если да, найти фактор-группу по ней.

3) То же задание для подгруппы, порожденной элементом β.

N	n	α	β	N	n	α	β
1	8	(1326)(4578)	(1427)(3865)	13	6	(132)	(645)
2	7	(134)	(567)	14	5	(25)(34)	(12)(35)
3	5	(12345)	(25)(34)	15	6	(162)(345)	(62)(34)
4	9	(12345)	(67)	16	6	(123456)	(14)(25)(36)
5	5	(12345)	(14253)	17	8	(1234)(57)	(68)
6	6	(1234)(56)	(13)	18	7	(64125)	(65)(24)(37)
7	8	(123)(456)	(78)	19	8	(12345678)	(14)(58)(23)(67)
8	5	(12345)	(13524)	20	9	(12345)	(67)(89)
9	6	(1243)	(14)(56)	21	5	(453)	(45)(12)
10	5	(15)	(53)(24)	22	6	(1234)	(13)(24)(65)
11	9	(4753)(2196)	(4259)(7631)	23	6	(12356)	(32)(15)
12	7	(1234)(567)	(1432)	24	8	(14)(7865)	(5687)
26	6	(123)(56)	(23)(56)	25	9	(123)(456)	(798)

Задача 7

Пусть G множество матриц $A \in GL(n, \mathbb{Z}_p)$, удовлетворяющих указанным условиям. Доказать, что G является группой относительно операции умножения матриц. Найти $|G|$. Коммутативна ли она? Какой из известных Вам групп она изоморфна?

N	n	p	Условие на матрицы A
1	2	3	Верхнетреугольные матрицы $A \in SL(2, \mathbb{Z}_3)$, т.е. $= \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$, удовлетворяющие условию det(A)=1.
2	2	5	Верхнетреугольные матрицы $A \in GL(2, \mathbb{Z}_5)$ вида $= \begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix}$.
3	2	3	Матрицы $A \in GL(2, \mathbb{Z}_3)$ вида $= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$.
4	2	3	$O(2, \mathbb{Z}_3)$ — ортогональные матрицы $A \in GL(2, \mathbb{Z}_3)$, т.е. $^t =$.
5	2	3	Верхнетреугольные матрицы $A \in GL(2, \mathbb{Z}_3)$, т.е. $= \begin{pmatrix} a & b \\ 0 & c \end{pmatrix}$.
6	2	7	Матрицы $A \in GL(2, \mathbb{Z}_7)$ вида $= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ или $= \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}$.
7	3	2	Верхнетреугольные матрицы $A \in GL(3, \mathbb{Z}_2)$, т.е. $= \begin{pmatrix} a & b & c \\ 0 & d & e \\ 0 & 0 & f \end{pmatrix}$.
8	2	5	Матрицы $A \in SL(2, \mathbb{Z}_5)$ вида $= \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ или $= \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$, т.е. $ab = 1$ и $cd = -1$.
9	3	3	Верхнетреугольные матрицы $A \in GL(3, \mathbb{Z}_3)$ вида $= \begin{pmatrix} 1 & a & b \\ 0 & 1 & a \\ 0 & 0 & 1 \end{pmatrix}$.
10	2	5	Матрицы $A \in GL(2, \mathbb{Z}_5)$ вида $= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, удовлетворяющие условию det(A)= ± 1.
11	2	7	Матрицы $A \in SL(2, \mathbb{Z}_7)$ вида $= \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, т.е удовлетворяющие условию det(A)=1.
12	3	2	$O(3, \mathbb{Z}_2)$ — ортогональные матрицы $A \in GL(3, \mathbb{Z}_2)$, т.е. $^t =$.
13	2	5	$O(2, \mathbb{Z}_5)$ — ортогональные матрицы $A \in GL(2, \mathbb{Z}_5)$, т.е. $^t =$.
14	2	5	Матрицы $A \in GL(2, \mathbb{Z}_5)$ вида $= \begin{pmatrix} a & 0 \\ 0 & a \end{pmatrix}$ или $= \begin{pmatrix} 0 & b \\ b & 0 \end{pmatrix}$.
15	2	11	Матрицы $A \in SL(2, \mathbb{Z}_{11})$ вида $= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, т.е удовлетворяющие условию det(A)=1.
16	2	11	Верхнетреугольные матрицы $A \in GL(2, \mathbb{Z}_{11})$ вида $= \begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix}$.
17	2	3	Матрицы $A \in GL(2, \mathbb{Z}_3)$ вида $= \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}$ или $= \begin{pmatrix} 0 & c \\ d & 0 \end{pmatrix}$ т.е. $ab = 1$ и $cd = 1$.

18	2	7	Матрицы $A \in SL(2,\mathbb{Z}_7)$ вида $= \begin{pmatrix} a & b \\ -b & a \end{pmatrix}$, т.е удовлетворяющие условию det(A)=1.
19	2	3	Верхнетреугольные матрицы $A \in GL(2,\mathbb{Z}_3)$ вида $= \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$.
20	2	7	Верхнетреугольные матрицы $A \in GL(2,\mathbb{Z}_7)$ вида $= \begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix}$
21	2	11	Матрицы $A \in SL(2,\mathbb{Z}_{11})$ вида $= \begin{pmatrix} a & b \\ b & a \end{pmatrix}$, т.е удовлетворяющие условию det(A)=1.
22	4	2	Верхнетреугольные матрицы $A \in GL(4,\mathbb{Z}_2)$ вида $= \begin{pmatrix} 1 & a & b & c \\ 0 & 1 & a & b \\ 0 & 0 & 1 & a \\ 0 & 0 & 0 & 1 \end{pmatrix}$.
23	2	7	Матрицы $A \in SL(2,\mathbb{Z}_7)$ вида $= \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, т.е удовлетворяющие условию det(A)=1.
24	2	7	Верхнетреугольные матрицы $A \in GL(2,\mathbb{Z}_7)$ вида $= \begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix}$
25	2	5	Верхнетреугольные матрицы $A \in GL(2,\mathbb{Z}_5)$ вида $= \begin{pmatrix} \pm 1 & a \\ 0 & 1 \end{pmatrix}$.
26	2	5	Матрицы $A \in SL(2,\mathbb{Z}_5)$ вида $= \begin{pmatrix} a & b \\ 2b & a \end{pmatrix}$, т.е удовлетворяющие условию det(A)=1.

Задача 8

1) Какой цикленный тип могут иметь элементы порядка k в S_n? Какие из них четные, а какие нечетные? Выпишите по одной подстановке каждого типа и найдите количество подстановок каждого типа.

2) Для одной из выписанных подстановок α найти множество подстановок β, перестеновочных с α (т.е. $\alpha\beta = \beta\alpha$). Доказать, что это группа, найти ее порядок и определить, какой из известных групп она изоморфна.

N	n	k	N	n	k	N	n	k
1	18	7	9	8	6	17	19	7
2	8	4	10	17	7	18	11	8
3	12	8	11	6	6	19	6	4
4	7	3	12	6	3	20	13	5
5	9	10	13	10	5	21	10	8
6	11	5	14	13	8	22	15	7
7	7	6	15	7	4	23	5	2
8	9	4	16	8	3	24	10	10
			26	10	12	25	9	12

Литература

1. Винберг Э. Б. Курс алгебры. М.: МЦНМО, 2011.
2. Головина Л. И. Линейная алгебра и некоторые её приложения. М.: Наука, 1985.
3. Кострикин А. И. Введение в алгебру. Часть I: Основы алгебры. М.: МЦНМО, 2009.
4. Кострикин А. И. Введение в алгебру. Часть II: Линейная алгебра. М.: МЦНМО, 2009.
5. Кострикин А. И. Введение в алгебру. Часть III: Основные структуры. М.: МЦНМО, 2009.
6. Кострикин А. И. Сборник задач по алгебре. М.: МЦНМО, 2009.