0.1 Знак перестановки и подстановки

Определение 0.1. *Пусть есть перестановка $i_1, i_2, \ldots, i_n$. Будем говорить, что пара чисел i_k, i_m, где $k < m$, образует инверсию, если $i_k > i_m$. Другими словами, если большее число встречается раньше меньшего.*

Определение 0.2. *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. Перестановка местами двух соседних столбцов, влечет изменение числа инверсий в каждой строке на 1, при этом сумма инверсий либо остается прежней, либо изменяется на 2, поэтому понятие четной (нечетной) подстановки не зависит от порядка столбцов.*

Определение 0.3. *Пусть подстановка σ имеет k инверсий. Тогда число $(-1)^k$ будем называть знаком подстановки σ и обозначать $\operatorname{sgn}(\sigma)$. Таким образом, если σ — четная подстановка, то $\operatorname{sgn}(\sigma) = 1$, а если нечетная, то $\operatorname{sgn}(\sigma) = -1$.*

Определим аналогичным образом и знак перестановки $i_1, i_2, \ldots, i_n$:

$$\operatorname{sgn}(i_1, i_2, \ldots, i_n) = (-1)^d,$$

где d – число инверсий в перестановке.

Тогда для

$$\sigma = \begin{pmatrix} i_1 & i_2 & \ldots & i_n \\ j_1 & j_2 & \ldots & j_n \end{pmatrix}$$

имеем $\operatorname{sgn}\sigma = \operatorname{sgn}(i_1 \ldots, i_n) \cdot \operatorname{sgn}(j_1 \ldots, j_n)$.

Задача 0.4. Показать, что если поменять местами два числа в перестановке, то знак новой перестановки будет противоположен знаку исходной.

Предложение 0.5. *Отображение $\operatorname{sgn} : S_n \to C_2 = \{\pm 1\}$, $\sigma \mapsto \operatorname{sgn}\sigma$, является гомоморфизмом.*

Доказательство. Пусть α и β – подстановки и

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

Тогда $\operatorname{sgn}\alpha \cdot \beta = \operatorname{sgn}(b_1, \ldots, b_n)$ и

$$\operatorname{sgn}\beta = \operatorname{sgn}(a_1 \ldots\ a_n), \quad \operatorname{sgn}\alpha = \operatorname{sgn}(a_1 \ldots\ a_n) \cdot \operatorname{sgn}(b_1, \ldots, b_n),$$

поэтому $\operatorname{sgn}\alpha \cdot \operatorname{sgn}\beta = \operatorname{sgn}^2(a_1 \ldots\ a_n) \cdot \operatorname{sgn}(b_1, \ldots, b_n) = \operatorname{sgn}(b_1, \ldots, b_n) = \operatorname{sgn}\alpha \cdot \beta$. $\square$

Итак, произведение двух четных подстановок является четной подстановкой, произведение двух нечетных – четной, произведение четной и нечетной – нечетной. Ядро гомоморфизма sgn является нормальным делителем в S_n и состоит из четных подстановок, называется *знакопеременной группой* и обозначается A_n. Из теоремы о гомоморфизме следует, что $S_n/A_n \cong \mathbb{Z}_2$, поэтому индекс подгруппы A_n равен двум, т.е. $|S_n : A_n| = 2$, и, следовательно, $|A_n| = |S_n|/2 = n!/2$.

Знак транспозиции, т.е. цикла длины 2, равен -1. Знак цикла длины k равен $(-1)^{k-1}$. Иными словами, цикл четной длины является нечетной подстановкой, а цикл нечетной длины — четной подстановкой. Это вытекает из того, что

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

1 Факторизация и изоморфизмы

1.1 Отношение эквивалентности, факторизация

Определение 1.1. *Мы говорим, что задано отношение на множестве M, если задано подмножество $T \subseteq M \times M = \{(m_1, m_2)\}$.*

Определение 1.2. *Отношением эквивалентности (в этом случае, вместо $(x, y) \in T$ пишут $x \sim y$), называется такое отношение, которое обладает следующими свойствами:*
1) Рефлексивность: $x \sim x$.
2) Симметричность: $x \sim y \Rightarrow y \sim x$.
3) Транзитивность: если $x \sim y$ и $y \sim z$, то $x \sim z$.

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

Предложение 1.3. *Пусть T – отношение эквивалентности на множестве M. Тогда,*

1. $\forall x \in M \Rightarrow x \in T_x$
2. $\bigcup\limits_{x \in M} T_x = M$
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 1.4. *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 одним из основных. Относительно него $T_x = \{y : x \sim y\} = \{y \mid x^{-1} \cdot y \in H\}$. Группа G оказывается разбитой на непересекающиеся классы эквивалентности. Так как $x \sim y \Leftrightarrow x^{-1}y \in H \Leftrightarrow \exists h \in H : x^{-1}y = h \Leftrightarrow y = xh \Rightarrow$ класс эвивалентности T_x — это $xH = \{xh \mid h \in H\}$. Далее, если $h_1 \neq h_2 \Rightarrow xh_1 \neq xh_2$. Отсюда делаем вывод, что если $|H| < \infty$, то во всех классах эквивалентности одинаковое количество элементов, совпадающее с порядком подгруппы: $|xH| = |H|$.

Определение 1.5. *$xH = \{xh \mid h \in H\}$ будем называть левым смежным классом элемента x по подгруппе H, а $Hx = \{hx \mid h \in H\}$ – правым смежный классом элемента x по подгруппе H. Правые смежные классы возникают как классы эквивалентности, если задавать эквивалентность по формуле $yx^{-1} \in H$.*

Теорема 1.6 (Теорема Лагранжа)**.** *Порядок подгруппы делит порядок конечной группы.*

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

Задача 1.7. *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, $x^{-1}y = (gh_1)^{-1}gh_2 = h_1^{-1}g^{-1}gh_2 = {h_1}^{-1}h_2 \in H$. □

Задача 1.8. Как задать посредством понятия отношения эквивалентности орбиты действий (левых и правых), эвивалентность бесконечно малых и бесконечно больших функций и последовательностей?

1.2 Левые и правые действия

Определение 1.9. *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 $\alpha(g)x = \alpha(g)(x)$ обычно обозначают через $g \cdot x$ или еще проще gx, где $g \in G$ и $x \in X$. Поскольку α – гомоморфизм, имеем $\alpha(e)x = x$ и $\alpha(g_1g_2)x = (\alpha(g_1) \circ \alpha(g_2))(x) = \alpha(g_1)(\alpha(g_2)x)$, что в упрощенных обозначениях приобретает вид:

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

Поэтому можно дать эквивалентное определение: действие (т. е. левое действие) G на X – это отображение $G \times X \to X$, $(g, x) \mapsto gx$, удовлетворяющее 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: $gx := xg^{-1}$. Если G абелева, то по можно ввести правое действие по левому и формулой $xg := gx$, и этим же сотношением ввести левое действие при наличии правого.

Примеры 1.10. 1. Группа $GL(n, \mathbb{K})$, где $\mathbb{K} = \mathbb{Q}, \mathbb{R}, \mathbb{C}$ действует на $\mathbb{K}^n$:

$$GL(n, \mathbb{K}) \times \mathbb{K}^n \to \mathbb{K}^n, \ \ (g, v) \mapsto gv,$$

g – матрица, v – вектор-столбец.

2. Правое действие: $\mathbb{K}^n \times GL(n, \mathbb{K}) \to \mathbb{K}^n$, $(v, g) \mapsto vg$, где g – матрица, а v – вектор-строка.

Определение 1.11. *Действие называется тривиальным, если $gx = x$ для любых $g \in G$ и $x \in X$.*

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

Определение 1.12. *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.

Определение 1.13. *Действие называется транзитивным, если имеется ровно одна орбита, т. е. $|X/G| = 1$. Иными словами $X = Gx \ \ \forall\, x \in X$.*

Задачи 1.14. 1. Легко видеть, что имеется ровно две орбиты действия группы $GL(n,\mathbb{R})$ на $\mathbb{R}^n$. Одна орбита состоит из одной точки – начала координат, другая – это $\mathbb{R}^n \setminus 0$. Таким образом, $GL(n,\mathbb{R})$ действует транзитивно на $\mathbb{R}^n \setminus 0$. Доказать, что и $SL(n,\mathbb{R})$ действует транзитивно на $\mathbb{R}^n \setminus 0$.

2. Пусть X – множество точек аффинного пространства, ассоциированного с векторным пространством V. Рассматривая V как абелеву группу, показать, что V действует транзитивно на X "прибавлением вектора к точке": $V \times X \to X$, $(v,p) \mapsto p+v$.

Определение 1.15. *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.

1.3 Орбиты и стационарные подгруппы

Определение 1.16. *Множество $Gx = \{gx \mid g \in G\}$ называется орбитой точки $x \in X$. Если орбита – конечное множество, то число ее элементов $|Gx|$ называют длиной орбиты Gx.*

Орбиты либо не пересекаются, либо полностью совпадают.

Определение 1.17. *Множество орбит обозначается X/G и называется факторомножеством множества X по действию группы G.*

Определение 1.18. *Стабилизатором точки x (стационарной подгруппой точки) называется подгруппа $G_x = \mathrm{St}_x := \{g \in G \mid gx = x\}$.*

Легко видеть, что G_x действительно является подгруппой. Действительно, если $g_1, g_2 \in G_x$, то $(g_1g_2)x = g_1(g_2x) = g_1x = x$), следовательно, $g_1g_2 \in G_x$. Если $g \in G_x$, то $x = ex = (g^{-1}g)x = g^{-1}(gx) = g^{-1}x$, т.е. $g^{-1} \in G_x$.

Предложение 1.19. *Отображение $f\colon Gx \to G/G_x$ переводящее gx в gG_x корректно определено и является G-эквивалентностью.*

Предложение 1.20. *Если группа G конечна, то $|Gx| = |G : G_x| = \frac{|G|}{|G_x|}$.*

Предложение 1.21. *Имеем $G_{gx} = gG_xg^{-1} = i_g(G_x)$. Таким образом, стабилизаторы точек из одной и той же орбиты являются сопряженными подгруппами.*

Доказательство. Если $h \in G_x$, то

$$(ghg^{-1})gx = (ghg^{-1}g)x = (gh)x = g(hx) = gx,$$

поэтому $ghg^{-1} \in G_{gx}$. Далее, если $g_1 \in G_{gx}$, то $g_1(gx) = gx$, откуда находим $(g^{-1}g_1g)x = x$, поэтому $g^{-1}g_1g \in G_x$ и обозначая этот элемент через $h = g^{-1}g_1g$ получаем $g_1 = ghg^{-1} \in i_g(G_x)$. □

Предложение 1.22. *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.

Пример 1.23. 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 1.24. 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 1.25. Найти порядок группы вращений правильного тетраэдра, используя транзитивность ее действия на множестве

a) вершин,

b) ребер,

c) граней.

Задача 1.26. Найти порядок диэдральной группы D_n, используя транзитивность ее действия на множестве

a) вершин правильного n-угольника,

b) ребер правильного n-угольника.

Задача 1.27. Найти порядок группы вращений правильного

a) додекаэдра,

b) икосаэдра.

1.4 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 1.28 (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 $\sum_{x\in X} \frac{|G|}{|Gx|} = |G|\sum_{x\in X}\frac{1}{|Gx|}$. Более подробно: пусть $|X/G| = d$, тогда G является дизъюнктным объединением d орбит $G = Gx_1 \sqcup \cdots \sqcup Gx_d$. Поэтому

$$\sum_{x\in X}\frac{1}{|Gx|} = \sum_{k=1}^{d}\sum_{y\in Gx_k}\frac{1}{|Gy|},$$

но поскольку $Gy = Gx_k$ для любого $y \in Gx_k$, получаем

$$\sum_{y\in Gx_k}\frac{1}{|Gy|} = \sum_{y\in Gx_k}\frac{1}{|Gx_k|} = \frac{|Gx_k|}{|Gx_k|} = 1,$$

и, следовательно, $\sum_{x\in X}\frac{1}{|Gx|} = \sum_{k=1}^{d} 1 = d = |X/G|$. □

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 1.29. 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 1.30. 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, вложенной в S_8 (вращение дает перестановку восьми вершин куба), мы можем описать ее действие на элементе $x \in X$ так: σx, где $\sigma \in S_4 = G < S_8$, 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[1], 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, $|\mathrm{Fix}(g)| = d^2$ в первом случае и $|\mathrm{Fix}(g)| = d^4$ во втором случае, а сумма чисел $|\mathrm{Fix}(g)|$ взятая по всем нетривиальным g типа b) равна $6d^2 + 3d^4$.

Наконец, число орбит действия (на множестве вершин куба) нетривиального элемента g типа c) такое же как в ситуации второго случая для элементов типа b), т.е. орбит 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

[1]Это – правое действие. Действительно, раскраску вершин можно понимать как отображение из множества вершин V куба в множество красок $K = \{1, \ldots, d\}$, а, как мы знаем, левое и правое действия на K^V задаются соответственно формулами $(gf)(v) = f(g^{-1}v)$ и $(fg)(v) = f(gv)$, где $v \in V$, $f \in K^V$, $g \in G$.

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 1.31. Найти число различных реберных раскрасок трехмерного куба в d цветов.

Задача 1.32. 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 b) 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 b) порядка 2 дает вклад d^4, а все такие элементы – вклад $3d^4$. Всего нетривиальные элементы типа b) 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 середины которых проходит ось вращения, и еще 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 1.33. Найти число различных вершинных раскрасок правильного тетраэдра в d цветов.

Задача 1.34. Найти число различных реберных раскрасок правильного тетраэдра в d цветов.

Задача 1.35. Найти число различных раскрасок граней правильного тетраэдра в d цветов.

Задача 1.36. 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 1.37. Найти число различных реберных раскрасок правильного p-угольника, где p простое, в d цветов.

[Указание: Использовать диэдральную группу D_p.]

Диэдральная группа D_n – это группа симметрий правильного n-угольника. Реализуем такой многоугольник на комплексной плоскости, считая, что его вершины – корни n-й степени из единицы, т.е. лежащие на единичной окружности с центром в начале координат числа $e^{2\pi ki/n}$, $k = 0, 1 \ldots, n$. Тогда повороты на углы кратные $2\pi/n$ и симметрия относительно вещественной оси (т.е. сопряжение $z \mapsto \bar{z}$) сохраняют этот правильный n-угольник, и, следовательно, принадлежат D_n. Обозначим поворот комплексной плоскости против часовой стрелки на угол $2\pi/n$ через a, сопряжение – через b. Тогда $a^n = e = b^2$. Поэтому D_n содержит циклические подгруппы $< a >_n$ и $< b >_2$ и произведение элементов этих подгрупп. Легко видеть, что

$$| < a >_n \cdot < b >_2 | = | < b >_2 \cdot < a >_n | = 2n$$

(элементы a^k и $a^m b$ не могут быть равны ни при каких k и m, поскольку первый сохраняет, а второй меняет ориентацию плоскости). С другой стороны, имеем $|D_n| = 2n$. Действительно, группа D_n действует транзитивно на множестве вершин нашего правильного n-угольника, а стационарная подгруппа вершины $1 \in \mathbb{C}$ есть $< b >_2$, откуда и следует сделанное утверждение, поскольку порядок группы, действующей транзитивно на множестве, равен числу элементов этого множества умноженному на порядок стационарной подгруппы любого элемента этого множества. Таким образом,

$$D_n =< a >_n \cdot < b >_2 =< b >_2 \cdot < a >_n = \{a^k,\ a^k b \,|\, k = 0, 1 \ldots, n-1\} = \\ = \{a^k,\ ba^k \,|\, k = 0, 1 \ldots, n-1\}.$$

Остается понять как перемножать элементы группы D_n представленные указанным образом. Это можно сделать используя доказанную ниже формулу $ab = ba^{n-1}$, или $ab = ba^{-1}$, так как $a^n = e$. Поскольку $b^2 = e$, умножая равенство $ab = ba^{-1}$ слева на b, получим легко запоминающееся соотношение $bab = a^{-1}$.

Представления

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.

Пример 1.38. Циклическая группа $< a >_n \cong \mathbb{Z}_n$ порядка n линейно над полем $\mathbb{C}$ действует на комплексном одномерном пространстве $\mathbb{C}$ по формуле $a^k z := e^{2\pi ki/n} z$, $z \in \mathbb{C}$. 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*.

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 $\mathbb{R}^2 \cong \mathbb{C}$, $x + iy \leftrightarrow (x, y)$, – $\mathbb{R}$-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).

2 Прямое произведение

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 $G \times H$:

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2).$$

Докажем, что $G \times H$ — группа.

1. Ассоциативность непосредственно следует из ассоциативности операций в сомножителях.

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.

В случае, когда группы абелевы и используется аддитивная запись, то произведение групп также называется *прямой суммой* и обозначается $G \oplus H$. Элемент $(g,h) = (g,0) + (0,h)$ удобно обозначать как $g + h$.

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 $|(g,h)| = k \Rightarrow\ (g,h)^k = (g^k, h^k) = (e_G, e_H) \Rightarrow \begin{cases} g^k = e_G \\ h^k = e_H \end{cases}$
   $\begin{cases} k \vdots |g| \\ k \vdots |h| \end{cases} \Rightarrow k$ — 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 $G = \langle g \rangle, |g| = m, H = \langle h \rangle, |h| = l, \text{НОД}(m,l) = 1$, то $G \times H = \langle (g,h) \rangle$.

Примеры 2.1. 1. $C_5 \times C_7 \cong C_{35}$.
2. $\mathbb{Z}_{100} \cong \mathbb{Z}_4 \oplus \mathbb{Z}_{25}$.
3. $\mathbb{Z}_{210} \cong \mathbb{Z}_{10} \oplus \mathbb{Z}_{21} \cong \mathbb{Z}_6 \oplus \mathbb{Z}_{35}$.

Теперь, рассмотрим общий случай. Пусть $G_1, \ldots, G_n$ — группы. Тогда

$$G_1 \times G_2 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n\}$$

называется *прямым произведением* групп $G_1, \ldots, G_n$.
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, $e_G = (e_{G_1}, \ldots, e_{G_n})$.
$(g_1, g_2, \ldots, g_n)^{-1} = (g_1^{-1}, g_2^{-1}, \ldots, g_n^{-1})$. Ассоциативность в G выполняется, потому что выполняется в группах $G_1, G_2, \ldots, G_n$.

Для абелевых групп с аддитивной записью бинарной операции прямое произведение также называют прямой суммой и обозначают $G_1 \oplus G_2 \oplus \ldots \oplus G_n$. Элементы этой группы записывают в виде $a_1 + \cdots + a_n$, $a_i \in G_i$, нейтральный элемент – просто как 0.

Пример 2.2. $\mathbb{Z}_{210} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_7$.

Отметим также, что перестановка сомножителей (слагаемых в абелевом случае) дает изоморфную группу, в частности, $G_1 \times G_2 \cong G_2 \times G_1$.

Свойства прямого произведения (продолжение)

1. $|G| = |G_1| \cdot |G_2| \cdot \ldots \cdot |G_n|$.

2. G — коммутативная группа $\Leftrightarrow$ G_i коммутативна $\forall i$.

3. $|(g_1, g_2, \ldots, g_n)| = \text{НОК}(|g_1|, |g_2|, \ldots, |g_n|)$.

4. Пусть $G_i = \langle g_i \rangle_{k_i}$ $(k_i, k_j) = 1$ ($\forall i, j = 1, 2, \ldots, n$ таких, что $i \neq j$) $\Rightarrow G_1 \times \ldots \times G_n = \langle (g_1, g_2, \ldots, g_n) \rangle_{k_1 k_2 \cdot \ldots \cdot k_n}$.
   ◀ Из 3) $|(g_1, g_2, \ldots, g_n)| = \text{НОК}(|g_1|, |g_2|, \ldots, |g_n|)$.
   Так как $\text{НОД}(k_i, k_j) = 1 \Rightarrow \text{НОК}(k_1, \ldots, k_n) = k_1 k_2 \ldots k_n$. ▶

5. $\widetilde{G}_1 = G_1 \times \{e_2\} \times \ldots \times \{e_n\} = \{(g_1, e_2, \ldots, e_n) \mid \forall g_1 \in G_1\} < G$.
   Аналогичным образом определяется $\widetilde{G}_i < G$ для $i = 2, \ldots, n$.

6. $\widetilde{G}_i \cap \widetilde{G}_j = \{e_G\}$ при $i \neq j$.

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
   $(e, \ldots, g_i, \ldots, e)(e, \ldots, g_j, \ldots, e) = (e, \ldots, g_j, \ldots, e) \cdot$
   $\cdot (e, \ldots, g_i, \ldots, e) = (e, \ldots, g_i, \ldots, g_j, \ldots, e)$.

8. $\forall g \in G \; \exists! \; g_1 \in G_1, \ldots, g_n \in G_n : \; g = \tilde{g}_1 \tilde{g}_2 \ldots \tilde{g}_n$, т.к.
   $g = (g_1, \ldots, g_n) = (g_1, e, \ldots, e)(e, g_2, e, \ldots, e) \ldots (e, \ldots, e, g_n)$.

9. $\widetilde{G}_i = \{e\} \times \ldots \times G_i \times \ldots \times \{e\} \lhd G$.
   Действительно, пусть $h_i \in G_i$, тогда

$$\begin{aligned}(g_1, \ldots, g_n)\tilde{h}_i(g_1, \ldots, g_n)^{-1} = \\ = (g_1, \ldots, g_n)(e, \ldots, h_i, \ldots, e)(g_1, \ldots, g_n)^{-1} = \\ = (e, \ldots, g_i h_i g_i^{-1}, \ldots, e) \in \widetilde{G}_i.\end{aligned}$$

10. $(G_1 \times G_2 \times \{e_{G_3}\}) \cap (\{e_{G_1}\} \times \{e_{G_2}\} \times G_3\}) = \{e\}$, и аналогичное верно для любого n и произвольного разбиения множества сомножителей на два непересекающихся подмножества.

Внутреннее прямое произведение

Пусть G – группа, а $G_1, \ldots, G_n$ – ее подгруппы.
Возьмем

$$G_1 \times \ldots \times G_n = \{(g_1, g_2, \ldots, g_n) \mid g_1 \in G_1, g_2 \in G_2, \ldots, g_n \in G_n\}$$

— (внешнее) прямое произведение $G_1, \ldots, G_n$.
Что нужно потребовать от $G_1, \ldots, G_n$, чтобы существовал изоморфизм

$$\varphi : G_1 \times \ldots \times G_n \longrightarrow G\,?$$

Естественно, мы хотим, чтобы $\varphi(e, \ldots, g_i, \ldots, e) = g_i$. Тогда

$$\varphi(g_1, g_2, \ldots, g_n) = \varphi(g_1, e, \ldots, e) \cdot \varphi(e, g_2, e, \ldots, e) \cdot \ldots \cdot \varphi(e, \ldots, e, g_n) = g_1 g_2 \ldots g_n.$$

Проверим, является ли отображение φ гомоморфизмом.

$$\begin{aligned}\varphi((g_1, g_2, \ldots, g_n)(h_1, h_2, \ldots, h_n)) &= \varphi(g_1h_1, g_2h_2, \ldots, g_nh_n) = \\ &= g_1h_1g_2h_2 \ldots g_nh_n \neq g_1g_2 \ldots g_nh_1h_2 \ldots h_n = \\ &= \varphi(g_1, \ldots, g_n)\varphi(h_1, \ldots, h_n).\end{aligned}$$

Следовательно, для гомоморфизма нам требуется перестановочность элементов из разных подгрупп $G_1, \ldots, G_n$, то есть

$$g_ig_j = g_jg_i \;\forall g_i \in G_i, g_j \in G_j \;(\forall i, j = 1, 2, \ldots, n \; i \neq j).$$

Пусть это выполнено. Является ли φ мономорфизмом?
Очевидно, что $g_1 \ldots g_n = h_1 \ldots h_n \Leftrightarrow g_1 = h_1, g_2 = h_2, \ldots, g_n = h_n$.
Отсюда, φ – мономорфизм, если элемент $g \in G$ можно разложить в произведение $g = g_1g_2 \cdot \ldots \cdot g_n$, $g_1 \in G_1, \ldots, g_n \in G$ единственным образом.

Проверим, является ли φ эпиморфизмом.
$\operatorname{Im}\varphi = G$. $\exists\, g_1, \ldots, g_n : \varphi(g_1, \ldots, g_n) = g_1 \ldots g_n = g \in G$.
Изо = Моно + Эпи $\Leftrightarrow \forall g \in G \;\exists!\; (g_1, \ldots, g_n) \in G_1 \times \ldots \times G_n :\; g = g_1 \cdot \ldots \cdot g_n$.

Определение 2.3. *Группа G называется внутренним прямым произведением своих подгрупп $G_1, \ldots, G_n$, если*

$$\begin{cases}1.\; g_ig_j = g_jg_i \;\forall g_i \in G_i, g_j \in G_j \;(\forall i, j = 1, 2, \ldots, n \\ 2.\; \forall g \in G \;\exists! g_1 \in G_1, \ldots, g_n \in G_n :\; g = g_1 \cdot \ldots \cdot g_n\end{cases}$$

Задача 2.4. Доказать, что если пересечение двух нормальных подгрупп H_1 и H_2 группы G содержит лишь e, то $h_1h_2 = h_2h_1$ для любых элементов $h_1 \in H_1, h_2 \in H_2$.

Доказательство. $H_2 \ni \underbrace{(h_1h_2h_1^{-1})}_{\in H_2}h_2^{-1} = h_1\underbrace{(h_2h_1^{-1}h_2^{-1})}_{\in H_1} \in H_1 \Rightarrow h_1h_2h_1^{-1}h_2^{-1} = e \Rightarrow$ $h_1h_2 = h_2h_1$. □

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

$$G \cong G_1 \times G_2 \times \ldots \times G_n \Leftrightarrow \begin{cases} 1.\ G_i \cap G_j = \{e\},\ \ i \neq j \\ 2.\ G = G_1 G_2 \cdot \ldots \cdot G_n = \{g_1 g_2 \cdot \ldots \cdot g_n \mid \forall g_i \in G_i\} \\ 3.\ G_1 \lhd G, G_2 \lhd G, \ldots, G_n \lhd G \end{cases}$$

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

В случае, когда $|G| < \infty$

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

Задача 2.5. 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 $kn\mathbb{Z}$. □

Предложение 2.6. $N_1 \lhd G_1,\ N_2 \lhd G_2 \Rightarrow N_1 \times N_2 \lhd G_1 \times G_2$.

Предложение 2.7. *Пусть $\varphi_i : G_i \to G_i'$ – гомоморфизмы, $i = 1, 2$. Тогда*

$$\operatorname{Ker}(\varphi_1 \times \varphi_2) = \operatorname{Ker}\varphi_1 \times \operatorname{Ker}\varphi_2 \quad и \quad \operatorname{Im}(\varphi_1 \times \varphi_2) = \operatorname{Im}\varphi_1 \times \operatorname{Im}\varphi_2,$$

где $\varphi_1 \times \varphi_2 : G_1 \times G_2 \to G_1' \times G_2'$ определяется следующей формулой $(\varphi_1 \times \varphi_2)(g_1, g_2) = (\varphi(g_1), \varphi(g_2))$.

Теорема 2.8. $N_1 \lhd G_1,\ N_2 \lhd G_2 \Rightarrow (G_1 \times G_2)/(N_1 \times N_2) \cong G_1/N_1 \times G_2/N_2$.

Доказательство. Пусть $\varphi_i : G_i \longrightarrow G_i/N_i$, $g \mapsto gN_i$, – естественный эпиморфизм $i = 1, 2$. Имеем $\operatorname{Ker}\varphi_1 \times \varphi_2 = \operatorname{Ker}\varphi_1 \times \operatorname{Ker}\varphi_2 = N_1 \times N_2$. По теореме о гомоморфизме получаем требуемый изоморфизм. □

Теорема 2.9. *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 поскольку $(h_1, h_2)(g_1, g_2)(h_1, h_2)^{-1} = (h_1 g_1 h_1^{-1}, h_2 g_2 h_2^{-1})$, имеем

$$A = \{(h_1 g_1 h_1^{-1}, h_2 g_2 h_2^{-1}) \mid h_1 \in G_1,\ h_2 \in G_2\} = A_1 \times A_2,$$

где $A_1 = \{h_1 g_1 h_1^{-1} \mid h_1 \in G_1\}$ и $A_2 = \{h_2 g_2 h_2^{-1} \mid h_2 \in G_2\}$ – классы сопряженных элементов в G_1, G_2 соответственно. □

Следствие 2.10. *Если в G_i число классов сопряженных элементов равно k_i, $i = 1, 2$, то число классов сопряженных элементов в $G_1 \times G_2$ равно $k_1 k_2$.*

Задача 2.11. $V_4 \cong C_2 \times C_2$.

Решение. На группу V_4 можно смотреть как на группу симметрий ромба. Нетривиальные элементы — отражения s_1, s_2 относительно диагоналей ромба и их произведение $r = s_1 s_2 = s_2 s_1$, т.е. $V_4 = \{e, s_1, s_2, r\}$. $H_1 = \{e, s_1\} \cong C_2, H_2 = \{e, s_2\} \cong C_2$ — подгруппы V_4, 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 2.12. *Если G, F – коммутативные группы, то $G \times F$ также коммутативна.*

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

Задача 2.13. $C_m \times C_n \cong C_{mn} \Leftrightarrow (m, n) = 1$.

Решение. 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 $k = \text{НОК}(m, n)$. Если 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 $(a, b)^k = (a^k, b^k) = ((a^m)^{k_1}, (b^n)^{k_2}) = (e, e)$. Но из сотношения $a^k = e$ следует равенство $(a^r)^k = a^{rk} = (a^k)^r = e^r = e$ и аналогично получаем, что $(b^s)^k = e$. Следовательно, $(a^r, b^s)^k = (e, e)$ и мы видим, что порядки всех элементов в группе $C_m \times C_n$ не превосходят $k < mn$. Таким образом, в $C_m \times C_n$ нет элемента порядка mn и, значит, она не изоморфна C_{mn}. □

Задача 2.14. *Можно ли разложить в прямое произведение собственных подгрупп следующие группы: S_3, A_4, S_4, Q_8 ?*

Решение. В каждой из этих групп нет двух нетривиальных подгрупп, удовлетворяющих указанным выше свойствам, например, нет нетривиальных нормальных подгрупп, пересекающихся только по единице, и произведение порядков которых равно порядку группы, а, скажем, в Q_8 вообще нет нетривиальных подгрупп, пересекающихся только по единице. Поэтому нет, не разлагаются. □

Задача 2.15. $\mathbb{R}_{>0} \times \mathbf{U} \cong \mathbb{C}^*$, *где $\mathbb{C}^* = \mathbb{C} \setminus \{0\}$ – группа ненулевых комплексных чисел по умножению.*

Решение. Имеем биекцию $\mathbb{R}_{>0} \times \mathbf{U} \to \mathbb{C}^*$, $(r, e^{i\varphi}) \mapsto re^{i\varphi}$. Легко видеть, что эта биекция – гомоморфизм. Следовательно, $\mathbb{C}^* \cong \mathbb{R}_{>0} \times \mathbf{U}$. Отметим также, что подгруппы $\mathbb{R}_{>0}$ и $\mathbf{U}$ нормальны (так как группа $\mathbb{C}^*$ по умножению абелева) и пересекаются только по 1. □

Задача 2.16. *Положим*

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

Тогда $G \cong G_1 \times G_2$.

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 $\lambda = \sqrt[n]{\det A}$, $A_1 = \frac{1}{\lambda} A \in \text{SL}(n, \mathbb{R})$. Действительно, $\det\left(\frac{1}{\lambda} A\right) = \frac{1}{\lambda^n} \det A = \frac{\det A}{\det A} = 1$. □

3 Полупрямое произведение

Внутреннее полупрямое произведение

Задача 3.1. $N \lhd G,\ H < G \Rightarrow NH = \{nh : n \in N, h \in H\}$ — *подгруппа* G.

Доказательство. С ассоциативностью все в порядке, так как 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. *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 $G = N \leftthreetimes H$ $(G = H \rtimes N)$.

Условия из определения эквивалентны следующим:

$$\begin{cases} 1.\ N \lhd G, H < G \\ 2.\ N \cap H = \{e\} \\ 3.\ NH = G \end{cases}$$

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 3.3. 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 3.4. *Докажите, что* $S_n = A_n \leftthreetimes \langle(12)\rangle_2$.

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

В доказанном утверждении вместо транспозиции (12) можно взять любую другую транспозицию.

Задача 3.5. $S_4 = V_4 \leftthreetimes S_3$.

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 3.6. *Показать, что*

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

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. Группа $\mathrm{GL}(n,\mathbb{R})$ представляется в виде произведения указанных подгрупп слеующим образом:

$$\mathrm{GL}(n,\mathbb{R}) \ni A = \widetilde{A} \cdot \begin{pmatrix} \det A & \dots & 0 \\ 0 & 1 \dots & 0 \\ \dots & \dots & \dots \\ 0 & \dots & 1 \end{pmatrix},$$

где первый столбец матрицы $\widetilde{A}$ получается из первого столбца матрицы A делением всех элементов столбца на $\det A$, а остальные столбцы такие же как у A. Действительно, обозначим через C_λ диагональную матрицу из второй подгруппы. Тогда $C_{\lambda_1} C_{\lambda_2} = C_{\lambda_1\lambda_2}$, $C_1 = E$ и $\det C_\lambda = \lambda$. Имеем $A = AC_{\frac{1}{\lambda}} C_\lambda$. Возьмем $\lambda = \det A$ и положим $\widetilde{A} = AC_{\frac{1}{\lambda}}$. Тогда $\det \widetilde{A} = \det\left(AC_{\frac{1}{\lambda}}\right) = \det A \det C_{\frac{1}{\lambda}} = \det A / \det A = 1$ и $A = \widetilde{A} C_\lambda$. Это – требуемое разложение. Кроме того, умножение матрицы A справа на $C_{\frac{1}{\lambda}}$ изменяет только ее первый столбец – он делится на λ, т.е. на $\det A$. □

Предложение 3.7. *Если $G = N \leftthreetimes H$, то $G/N \cong H$.*

Доказательство. Отображение $G \to H$, $g = nh \mapsto h$, корректно определено и является эпиморфизмом. Его ядро, очевидно, равно N, поэтому результат следует из теоремы о гмоморфизме.

□

Внешнее полупрямое произведение

Пусть N, H — группы. Определим новую операцию умножения на декартовом произведении этих групп. Оно будет зависить от выбора гомоморфизма

$$\varphi : H \longrightarrow \mathrm{Aut}\, N.$$

Положим $\varphi_h = \varphi(h) \in \mathrm{Aut}\, N$, и определим умножение формулой:

$$(n_1, h_1)(n_2, h_2) = (n_1 \varphi_{h_1}(n_2), h_1 h_2).$$

Обратный элемент: $(n,h)^{-1} = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$.

Мы проверим, что получается группа, она называется *полупрямым (внешним) произведеним* двух групп N и H.

Таким образом, полупрямое (внешнее) произведение зависит от гомоморфизма φ. Если необходимо подчеркнуть эту зависимость, то пишем $N \leftthreetimes_{\varphi} H$, если зафиксировали гомоморфизм, то пишем просто $N \leftthreetimes H$.

Отметим, что если взять φ таким, что $\operatorname{Im}\varphi = \operatorname{id}_N$, т.е. φ отображает всю подгруппу H в единицу группы $\operatorname{Aut} N$, то получается прямое произведение групп.

Задача 3.8. *Доказать, что $N \leftthreetimes H$ – группа.*

Доказательство. Прежде, чем переходить к доказательству, отметим, что поскольку $\varphi : H \longrightarrow \operatorname{Aut} N$ – гомоморфизм и мы обозначили $\varphi(h)$ через φ_h, то $\varphi_e = \operatorname{id}_N$ и справедливо сотношение $\varphi_{h_1 h_2} = \varphi_{h_1} \circ \varphi_{h_2}$, т.е. $\varphi_{h_1 h_2}(n) = \varphi_{h_1}(\varphi_{h_2}(n))$ для любого $n \in N$. В частности, $\varphi_h \circ \varphi_{h^{-1}} = \varphi_{hh^{-1}} = \varphi_e = \operatorname{id}_N$, поэтому $\varphi_{h^{-1}} = \varphi_h^{-1}$.

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.
   $$\begin{aligned}
   [(n_1, h_1)(n_2, h_2)]\,(n_3, h_3) &= (n_1 \varphi_{h_1}(n_2), h_1 h_2)(n_3, h_3) = \\
   &= (n_1 \varphi_{h_1}(n_2) \varphi_{h_1 h_2}(n_3), h_1 h_2 h_3) = \\
   &= (n_1 \varphi_{h_1}(n_2) \varphi_{h_1}(\varphi_{h_2}(n_3)), h_1 h_2 h_3), \\
   (n_1, h_1)\,[(n_2, h_2)(n_3, h_3)] &= (n_1, h_1)(n_2 \varphi_{h_2}(n_3), h_2 h_3) = \\
   &= (n_1 \varphi_{h_1}(n_2 \varphi_{h_2}(n_3)), h_1 h_2 h_3) = \\
   &= [\text{ так как } \varphi_{h_1} \text{ – гомоморфизм}] = \\
   &= (n_1 \varphi_{h_1}(n_2) \varphi_{h_1}(\varphi_{h_2}(n_3)), h_1 h_2 h_3).
   \end{aligned}$$

3. Единичный элемент $e_{N \leftthreetimes H} = (e_N, e_H)$.

4. Обратный элемент $(n, h)^{-1} = (?, h^{-1})$. Из определения обратного, $(n, h)(?, h^{-1}) = (n, \varphi_h(?), hh^{-1}) = (e, e)$. Пусть $x \in N$ – обозначенный вопросом искомый элемент. Тогда
   $$n \varphi_h(x) = e \Leftrightarrow \varphi_h(x) = n^{-1} \Rightarrow x = \varphi_h^{-1}(n^{-1}).$$

Поэтому $(n, h)^{-1} = (\varphi_h^{-1}(n^{-1}), h^{-1}) = (\varphi_{h^{-1}}(n^{-1}), h^{-1})$ – обратный элемент. □

Пусть G – внутреннее полупрямое произведение подгрупп N и H, где N нормальна. Тогда любой элемент $g \in G$ однозначным образом представляется в виде $g = nh$, $n \in N$, $h \in H$. Пусть $g_1 = n_1 h_1$, $g_2 = n_2 h_2$, тогда

$$g_1 g_2 = n_1 h_1 n_2 h_2 = n_1 h_1 n_2 h_1^{-1} h_1 h_2 = n_1 i_{h_1}(n_2) h_1 h_2,$$

где i_{h_1} – внутренний автоморфизм. Определим $i : G \to \operatorname{Int} G$ следующим образом: $i(g) = i_g$. Тогда i – гомоморфизм, и ограничивая его на H и учитывая нормальность подгруппы N, видим, что i определяет гомоморфизм $\varphi : H \to \operatorname{Aut} N$. Отображение $G \to N \leftthreetimes_\varphi H$, $nh \mapsto (n, h)$, является изоморфизмом, т.е. $G \cong N \leftthreetimes_\varphi H$. Таким образом, если группа G есть внутреннее полупрямое произведение подгрупп N и H, то она изоморфна внешнему полупрямому произведению этих подгрупп.

Задача 3.9. *Пусть $N = A_3$ и $H = C_2$. Найти все полупрямые произведения $N \leftthreetimes H$.*

Решение. Группа четных подстановок $A_3 = \{e, (123), (132)\} = C_3 = \{e, a, a^2\}$ имеет порядок $|A_3| = 3$. Группа $C_2 = \{e, s\}$ – циклическая группа порядка 2. Для того, чтобы найти все полупрямые произведения $C_3 \leftthreetimes C_2$, рассмотрим все возможные гомоморфизмы $\varphi : C_2 \longrightarrow \operatorname{Aut} \mathrm{C}_3$.
Случай 1: $\varphi(e_{C_2}) = \mathrm{id} = \mathrm{id}_{C_3}$, $\varphi(s) = \mathrm{id}$. Тогда $\mathrm{id}\,(e_{C_3}) = e$, $\mathrm{id}\,(a) = a$, $\mathrm{id}(a^2) = a^2$ и $C_3 \leftthreetimes_\varphi C_2 = C_3 \times C_2$ – прямое произведение.
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. Итак,

$$A_3 \leftthreetimes \langle (12) \rangle_2 = S_3 \cong D_3.$$

□

Задача 3.10. Пусть A – абелева группа.

1. Показать, что

$$D(A) = \{(a, \varepsilon) \mid a \in A,\ \varepsilon = \pm 1\}$$

с операцией умножения $(a_1, \varepsilon_1)(a_2, \varepsilon_2) = (a_1 a_2^{\varepsilon_1}, \varepsilon_1\varepsilon_2)$ является группой.

2. Показать, что если $A =< a >_n$, то $D(A)$ изоморфна диэдральной группе D_n.

3. Показать, что $D(A) \cong A \leftthreetimes C_2$. Как определяется φ?

[Подсказки: К задаче 2:
$D(\langle\, a \,\rangle_n) = \{(e, 1), (a, 1), \ldots, (a^{n-1}, 1); (e, -1), (a, -1), \ldots, (a^{n-1}, -1)\}$,
$D_n = \{e, a, \ldots, a^{n-1}; b, ab, \ldots, a^{n-1}b\}$. Изоморфизм $D(\langle\, a \,\rangle_n) \cong D_n$ дается биекцией $a^k \leftrightarrow (a^k, 1)$, $a^k b \leftrightarrow (a^k, -1)$, $k = 0, \ldots, n-1$.
К задаче 3: $\varphi_1 = \mathrm{id}_A$, $\varphi_{-1}(a) = a^{-1}$.]

Задача 3.11. Пусть группа A неабелева. Показать, что в этом случае умножение, введенное на $D(A)$ в предыдущей задаче, неассоциативно (тем самым $D(A)$ в этом случае даже не полугруппа).

Задача 3.12. Изоморфна ли группа $GL(n, \mathbb{R})$ прямому, или полупрямому, произведению групп $GL^+(n, \mathbb{R})$ и $C_2 = \{\pm 1\}$?

Задача 3.13. Пусть группа A неабелева. Показать, что в этом случае умножение, введенное на $D(A)$ в предыдущей задаче, неассоциативно (тем самым $D(A)$ в этом случае даже не полугруппа).

Задача 3.14. Изоморфна ли группа $GL(n, \mathbb{R})$ прямому, или полупрямому, произведению групп $GL^+(n, \mathbb{R})$ и $C_2 = \{\pm 1\}$?

3.1 Образующие

Пусть S – подмножество в группе G. Наименьшая подгруппа группы G, содержащая S, называтся подгуппой порожденной системой порождающих элементов из S и обозначается $< S >$. Ясно, что $< S >$ состоит из всевозможных произведений элементов из S и их обратных. Если $G =< S >$, то говорят, что S – множество порождающих элементов группы G.

В частности, если $a \in G$, то $< a >$ – циклическая подгруппа группы G.

Если $G =< S >$ и S – конечное множество, то группу G называют конечнопорожденной.

Пусть S – некоторое множество. Будем смотреть на его элементы как на буквы алфавита, в который вместе с каждым символом $s \in S$ мы включим (формальный) символ s^{-1}. Рассмотрим множество слов от всех символов s и s^{-1}, $s \in S$ и добавим к нему пустое слово. Введем на этом множестве слов бинарную операцию – соединение слов. Мы получаем моноид в котором роль единицы играет пустое слово (соединение слова слева или справа с пустым словом не меняет слова). Ведем опреацию редуцирования слова, состоящую в стирании в слове рядом стоящих символов вида ss^{-1} или $s^{-1}s$. Например, в результате редуцирования слова $t^{-1}tss^{-1}$ мы получаем пустое слово. Введем на множестве нередуцирумых слов оперцию умножения следующим образом: соединяем слова и редуцируем полученное слово. В результате получаем группу. Эта группа называется свободной группой, а S – множеством ее свободных (образующих). Обозначим свободную группу через $F(S)$.

Для любого отображения $S \to G$ в произвольную группу существует и единственен гомоморфизм $F(S) \to G$, продолжающий это отображение.

Теорема Нильсена–Шраера утверждает, что подгруппа свободной группы свободна.

Любая группа изоморфна факторгруппе свободной.

Первое и третье утверждения тривиальны. Теорема Нильсена–Шраера – глубоко нетривиальное утверждение.

3.2 Конечно порожденные абелевы группы

Пусть A – абелева группа и $a_1, \ldots, a_n \in A$ – произвольные элементы группы. Множество всех линейных комбинаций этих элементов с целыми коэффициентами, т. е. элементов вида $k_1a_1 + \cdots + k_na_n$, где $k_1, \ldots, k_n \in \mathbb{Z}$, образует подгруппу, которую будем обозначать через $< a_1, \ldots, a_n >$ и называть подгруппой порожденной элементами $a_1, \ldots, a_n$.

Определение 3.15. *Абелева группа A называется конечно порожденной, если существуют элементы $a_1, \ldots, a_n \in A$, называемые образующими, такие, что $A =< a_1, \ldots, a_n >$.*

Определение 3.16. *Элементы $a_1, \ldots, a_n \in A$ называются линейно независимыми, если равенство $k_1a_1 + \cdots + k_na_n = 0$ влечет тривиальность всех коэффициентов $k_1, \ldots, k_n \in \mathbb{Z}$.*

Определение 3.17. *Если $A =< a_1, \ldots, a_n >$, где $a_1, \ldots, a_n \in A$ линейно независимы, то A называется свободной абелевой группой ранга n, а множество элементов $\{a_1, \ldots, a_n\} \subset A$ называется базисом.*

Нетрудно видеть, что свободная абелева группа ранга n изоморфна прямой сумме n экземпляров бесконечной циклической группы, т.е. $A \cong \mathbb{Z} \oplus \cdots \oplus \mathbb{Z}$ (n слагаемых).

Кроме того, легко доказать, что любая конечно порожденная абелева группа с n образующими является эпиморфным образом свободной абелевой группа ранга n (базисные элементы свободной абелевой группы нужно отобразить в образующие и продолжить отображение по линейности). Таким образом, любая конечно порожденная абелева группа A с n образующими является факторгруппой свободной абелевой группы F ранга n по некоторой подгруппе H. Можно показать, что любая подгруппа свободной абелевой группы ранга n также свободна и имеет ранг не превосходящий n. Более того, в F существует такой базис $a_1, \ldots, a_n \in F$, что множество элементов $\{m_1a_1, \ldots, m_ka_k\} \subset F$, где $k \leq n$ и $m_1, \ldots, m_k \in \mathbb{N}$, является базисом группы H. Отсюда вытекает следующий результат:

Теорема 3.18 (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.

Определение 3.19. *Циклическая группа называется примарной, если ее порядок равен степени простого числа.*

Если $(m, n) = 1$, то $\mathbb{Z}_{mn} = \mathbb{Z}_m \oplus \mathbb{Z}_n$. Поэтому конечная абелева группа изоморфна конечной прямой сумме примарных циклических групп. Таким образом, конечно порожденная абелева группа изоморфна прямой сумме свободной абелевой группы конечного ранга и конечной сумме примарных циклических групп.

Пример 3.20. $60 = 2^2 \cdot 3 \cdot 5$, $\mathbb{Z}_{60} = \mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Пример 3.21. Перечислим все абелевы группы $|G| = 36$.
$36 = 2^2 \cdot 3^2$
1) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$,
2) $\mathbb{Z}_4 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
3) $\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_9$
4) $\mathbb{Z}_4 \oplus \mathbb{Z}_9$
Все эти группы не изоморфны.

Примеры 3.22. Изоморфны ли группы?
1) $\mathbb{Z}_{24} \oplus \mathbb{Z}_9$ и $\mathbb{Z}_4 \oplus \mathbb{Z}_{54}$

$24 = 2^3 \cdot 3$
$\mathbb{Z}_{24} \oplus \mathbb{Z}_9 = \mathbb{Z}_{2^3} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{3^2}$
$54 = 2 \cdot 3^3$
$\mathbb{Z}_4 \oplus \mathbb{Z}_{54} = \mathbb{Z}_{2^2} \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^3}$
$\mathbb{Z}_{24} \oplus \mathbb{Z}_9 \ncong \mathbb{Z}_4 \oplus \mathbb{Z}_{54}$

2) $\mathbb{Z}_6 \oplus \mathbb{Z}_{36}$ и $\mathbb{Z}_{12} \oplus \mathbb{Z}_{18}$
$6 = 2 \cdot 3$
$36 = 2^2 \cdot 3^2$
$\mathbb{Z}_6 \oplus \mathbb{Z}_{36} = \mathbb{Z}_2 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_{2^2} \oplus \mathbb{Z}_{3^2}$
$12 = 2^2 \cdot 3$
$18 = 2 \cdot 3^2$
$Z_{12} \oplus Z_{18} = Z_{2^2} \oplus Z_3 \oplus Z_2 \oplus Z_{3^2}$
$Z_6 \oplus Z_{36} \cong Z_{12} \oplus Z_{18}$

На множестве гомоморфизмов $\mathrm{Hom}(A, B)$ из абелевой группы A в абелеву группу B, которые рассматриваются в аддитивной записи, естественным образом вводится структура абелевой группы: если $f, g \in \mathrm{Hom}(A, B)$ – два гомоморфизма, то их сумма $f + g \in \mathrm{Hom}(A, B)$ – это гомоморфизм, принимающий на элементе $a \in A$ значение $f(a) + g(a)$, т.е. $(f + g)(a) := f(a) + g(a)$. Проверка того факта, что $f + g$ – гомоморфизм и, что операция сложения коммутативна, не составляет труда:

$$\begin{aligned}(f+g)(a+b) = f(a+b) + g(a+b) = f(a) + f(b) + g(a) + g(b) = \\ = f(a) + g(a) + f(b) + g(b) = (f+g)(a) + (f+g)(b) \;\Rightarrow \\ (f+g)(a+b) = (f+g)(a) + (f+g)(b),\end{aligned}$$

т.е. $f + g$ – гомоморфизм, и коммутативность операции:

$$(f+g)(a) = f(a) + g(a) = g(a) + f(a) = (g+f)(a) \;\Rightarrow\; f + g = g + f.$$

Нейтральный элемент группы $\mathrm{Hom}(A, B)$ (обозначаемый нулем) – это гомоморфизм, отображающий A в $0 \in B$. Обратным к гомомморфизму $f \in \mathrm{Hom}(A, B)$ является гомомморфизм $-f$, переводящмй $a \in A$ в $-f(a)$, т.е.$(-f)(a) := -f(a)$.

Ясно, что $\mathrm{End}(A) = \mathrm{Hom}(A, A)$.

Задачи 3.23. 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. $\mathrm{Hom}(A, B \oplus C) \cong \mathrm{Hom}(A, B) \oplus \mathrm{Hom}(A, C)$.
5. Пусть $f\colon A \to F$ – эпиморфизм и F свободна (свободная абелева группа).
Показать, что тогда $A = \mathrm{Ker}\, f \oplus B$, где $B \cong F$. Таким образом, $\mathrm{Ker}\, f$ *выделяется прямым слагаемым.*

6. Показать, что $\mathbb{Q}$, $\mathbb{R}$ и $\mathbb{C}$ не являются конечно порожденными.

7^*. Можно ли представить $\mathbb{R}$ в качестве прямой суммы подгрупп изоморфных $\mathbb{Q}$, а $\mathbb{C}$ – изоморфных

a) $\mathbb{Q}$,

b) $\mathbb{R}$?

3.3 Действия сопряжением

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

Далее

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

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

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

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

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

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

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

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

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

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

Пример 3.24. Если подстановка $\sigma \in S_n$ представлена в виде произведения независимых циклов $\sigma = (i_1 \ldots, i_p)(j_1, \ldots, j_q) \cdot \ldots \cdot (k_1, \ldots, k_r)$, и $\tau \in S_n$ – еще одна подстановка, то как мы знаем

$\tau\sigma\tau^{-1} = (\tau(i_1) \ldots, \tau(i_p))(\tau(j_1), \ldots, \tau(j_q)) \cdot \ldots \cdot (\tau(k_1), \ldots, \tau(k_r))$.

Поэтому две подстановки сопряжены в том и только том случае, когда совпадают наборы длин циклов (цикленный тип) в их разложениях в произведение независимых циклов, и, следовательно, число классов сопряженных элементов в S_n равно числу неупорядоченных разбиений числа n в сумму натуральных чисел.

Для того, чтобы найти классы сопряженных элементов диэдральной группы нам понадобится ее описание в терминах образующих и соотношений.

Теорема 3.25. *Предположим, что $G = \langle a, b \rangle$ имеет порядок $2n$, порядки элементов a и b равны n и 2 соответственно, и $bab = a^{-1}$. Тогда $G \cong D_n$.*

Решение. Ясно, что $b \notin \langle a \rangle_n$, и легко видеть, что $G = \langle a \rangle_n \cdot \langle b \rangle_2$. Кроме того, подгруппа $\langle a \rangle_n$ нормальна так как ее индекс равен двум и $\langle a \rangle_n \cap \langle b \rangle_2 = \{e\}$. Поэтому наша группа является внутренним полупрямым произведением этих подгрупп, причем точно таким же каким является D_n, если под $a, b \in D_n$ понимать те образующие диэдральной группы, которые были введены нами выше при определении этой группы (a – поворот комплексной плоскости против часовой стрелки на угол $2\pi/n$, b – сопряжение).

Можно дать и другое объяснение – соотношение $ba = a^{-1}b$ дает возможность полностью определить таблицу Кэли, которая будет совпадать с таблицей Кэли группы D_n. □

Пример 3.26. Найдем классы сопряженных элементов в группе D_n. Мы знаем, что D_n порождается элементами $a, b \in D_n$, такими, что $a^n = e = b^2$ и $bab = a^{-1}$. Последнее равенство записывается в виде $i_b(a) = a^{-1}$, поскольку $b = b^{-1}$. Имеем $ba^k b = i_b(a^k) = (i_b(a))^k = (a^{-1})^k = a^{-k}$, т.е. $ba^k = a^{-k}b$. В частности, $ba^{-1} = ab$.

$$i_{a^m b}(a^k) = i_{a^m}(i_b(a^k)) = i_{a^m}(a^{-k}) = a^m a^{-k} a^{-m} = a^{-k} = a^{n-k}.$$

Таким образом, a^k и a^{-k} лежат в одном классе и других элементов там нет. Если n нечетно, получаем классы $\{e\}$, $\{a, a^{n-1}\}$, $\{a^2, a^{n-2}\}, \ldots, \{a^{\frac{n-1}{2}}, a^{\frac{n+1}{2}}\}$. Число этих классов равно $\frac{n+1}{2}$. При четном n имеем классы
$\{e\}, \{a, a^{n-1}\}, \{a^2, a^{n-2}\}, \ldots, \{a^{\frac{n}{2}-1}, a^{\frac{n}{2}+1}\}, \{a^{n/2}\}$, число которых равно $\frac{n}{2} + 1$.

Далее,
$i_b(b) = bbb^{-1} = b$,
$i_a(b) = aba^{-1} = aab = a^2 b$,
$i_a(a^k b) = i_a(a^k) i_a(b) = a^k a^2 b = a^{k+2} b$,
$i_{a^2}(b) = i_a(i_a(b)) = i_a(a^2 b) = i_a(a^2) i_a(b) = a^2 i_a(b) = a^4 b$,
$i_{a^m}(b) = a^{2m} b$.
Из этих равенств видно, что b и $a^{2m}b$ сопряжены, поэтому при нечетном n все элементы вида $a^k b$ принадлежат одному классу сопряженных элементов. При четном n элементы ab и $a^{2m+1}b$ сопряжены, но не сопряжены с b и получается два класса сопряженных элементов. Сказанное следует из вычислений:
$i_b(a^k b) = ba^k = a^{-k} b$,
$i_{a^m}(a^k b) = i_{a^m}(a^k) i_{a^m}(b) = a^k i_{a^m}(b) = a^{2m+k} b$,
$i_{a^m b}(a^k b) = i_{a^m}(i_b(a^k b)) = i_{a^m}(a^{-k} b) = a^{2m-k} b$.

Итак общее число классов сопряженных элементов равно $\frac{n+1}{2} + 1 = \frac{n+3}{2}$ при нечетном n, и равно $\frac{n}{2} + 3 = \frac{n+6}{2}$ при четном n.

Теорема 3.27. *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 поскольку $(h_1, h_2)(g_1, g_2)(h_1, h_2)^{-1} = (h_1 g_1 h_1^{-1}, h_2 g_2 h_2^{-1})$, имеем

$$A = \{(h_1 g_1 h_1^{-1}, h_2 g_2 h_2^{-1}) \mid h_1 \in G_1,\, h_2 \in G_2\} = A_1 \times A_2,$$

где $A_1 = \{h_1 g_1 h_1^{-1} \mid h_1 \in G_1\}$ и $A_2 = \{h_2 g_2 h_2^{-1} \mid h_2 \in G_2\}$ – классы сопряженных элементов в G_1, G_2 соответственно. □

Следствие 3.28. *Если в G_i число классов сопряженных элементов равно k_i, $i = 1, 2$, то число классов сопряженных элементов в $G_1 \times G_2$ равно $k_1 k_2$.*

Если $H < G$ – подгруппа, то gHg^{-1} – подгруппа в G. Эти подгруппы называются *сопряженными*. Таким образом, G действует сопряжениями на множестве подгрупп. Орбиты – классы сопряженных подгрупп. Орбитой подгруппы H является множество подгрупп $\{gHg^{-1} \mid g \in G\}$. Тот факт, что gHg^{-1} – подгруппа в G, легко проверить непосредственно, но можно воспользоваться и общим утверждением об образе гомоморфизма, поскольку $gHg^{-1} = i_g(H)$, т. е. является образом подгруппы H при внутреннем автоморфизме i_g.

Определение 3.29. *$Z(x) := \{g \in G \mid gx = xg\} = \{g \in G \mid gxg^{-1} = x\}$ называется централизатором элемента $x \in G$. Легко видеть, что централизаторы элементов являются подгруппами в G.*

Определение 3.30. *Нормализатором подгруппы H в G называется*

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

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

Теорема 3.31. *Мощность множества элементов группы G, сопряженных с элементом $x \in G$ равна $|G : Z(x)|$ – индексу централизатора элемента x. Мощность множества подгрупп группы G, сопряженных с подгруппой H группы G, равна $|G : N(H)|$ – индексу нормализатора подгруппы H в G.*

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

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

Предложение 3.32. $\operatorname{Int} G \cong G/Z(G)$, *где $Z(G)$ – центр группы G.*

Доказательство. Мы знаем, что $i : G \to \operatorname{Int} G$ – эпиморфизм, $i(g) = i_g$. Его ядро состоит из таких элементов $g \in G$, что $i_g = \mathrm{id}_G$, последнее означает, что $gxg^{-1} = x\ \forall x \in G \Leftrightarrow gx = xg\ \forall x \in G \Leftrightarrow g \in Z(G)$. Таким образом, $\operatorname{Ker} i = Z(G)$, и по теореме о гомоморфизме получаем $\operatorname{Int} G \cong G/Z(G)$. □

Предложение 3.33. *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. □

3.4 Силовские подгруппы

Определение 3.34. *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 3.35. *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 3.36. *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 что 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 $g = a^kz = za^k$, $z \in Z$. 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 3.37. *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 3.38. *Силовская p-подгруппа существует.*

Доказательство. Проведем индукцию по порядку группы. Для $|G| = 1$ 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 3.39. *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 3.40. *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 3.41. 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 $|GL(n,q)| = (q^n-1)(q^n-q)(q^n-q^2)\dots(q^n-q^{n-1}) = \prod_{i=0}^{n-1}(q^n-q^i)$. 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 наддиагональных 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 $GL(n,q)$.

Предложение 3.42. Если p – простой делитель порядка группы, то в группе существует элемент порядка p.

Доказательство. 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 3.43. 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 – $\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_5$.

Предложение 3.44. *Если каждый элемент группы, отличный от единицы, имеет порядок* 2*, то группа абелева. Если она конечна, то ее порядок является степенью двойки, т.е. это –* 2*-группа.*

Доказательство. Пусть $a \neq b$ – два произвольных элемента группы, отличных от единицы. Тогда $a^2 = e = b^2$, откуда $a = a^{-1}$, $b = b^{-1}$, поэтому $ab \neq e$, и, значит, тоже имеет порядок 2, т.е. $(ab)^2 = e$. Следовательно,

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba,$$

т.е. $ab = ba$. □

Например, пользуясь этим утверждением, легко показать, что группа порядка 4 абелева и изоморфна либо $\mathbb{Z}_4$, либо $\mathbb{Z}_2 \oplus \mathbb{Z}_2$. В частности, четверная группа Клейна V_4 изоморфна группе $\mathbb{Z}_2 \oplus \mathbb{Z}_2$, поскольку не является циклической (в ней все три отличных от e элемента имеют порядок 2).

Отметим также, что если использовать аддитивную запись, то в такой группе $2a = 0$ для любого элемента, поэтому группу можно рассматривать как векторное пространство над полем из двух элементов.

Предложение 3.45. *Группа порядка* $2p$*, где* p *– простое число большее* 2*, либо изоморфна циклической группе* $\mathbb{Z}_{2p} \cong \mathbb{Z}_2 \oplus \mathbb{Z}_p$*, либо диэдральной группе* D_p*.*

Доказательство. Поскольку порядок группы делится на простые числа 2 и p, в ней имеется элемент a порядка p и элемент b порядка 2, причем $b \notin \langle\, a \,\rangle = \langle\, a \,\rangle_p$, поскольку в циклической группе $\langle\, a \,\rangle_p$ все элементы, кроме e имеют порядок $p > 2$. Нетрудно видеть, что среди $2p$ элементов

$$e, a, a^2, \ldots, a^{p-1}, b, ab, a^2b, \ldots, a^{p-1}b$$

нет равных, поэтому группа порождается элементами a и b. Индекс подгруппы $\langle\, a \,\rangle_p$ равен двум, поэтому она нормальна. Следовательно, $bab = bab^{-1} = i_b(a) \in \langle\, a \,\rangle_p$ и, значит, $i_b(a) = a^m$ для некоторого $m \in 1, \ldots, p-1$. Если $m = 1$, то $ab = ba$

и этот элемент имеет порядок $2p$, т.е. наша группа изоморфна циклической группе $\mathbb{Z}_{2p}$. Если же $m > 1$, то применив внутренний автоморфизм i_b к равенству $i_b(a) = a^m$ получим

$$i_b(i_b(a)) = i_b(a^m) = (i_b(a))^m = (a^m)^m = a^{m^2}.$$

Но $i_b(i_b(a)) = i_{b^2}(a) = i_e(a) = a$, поэтому $a = a^{m^2}$, откуда $a^{m^2-1} = e$. Следовательно $m^2-1 = (m-1)(m+1)$ делится на p, и поскольку $1 \leq m \leq p-1$, либо $m = 1$, либо $m = p-1$. При $m = 1$ получаем рассмотренный выше случай, а при $m = p-1$ имеем $bab = a^{p-1} = a^{-1}$, и тогда $G \cong D_p$, как было показано выше. □

Теорема 3.46. *Неабелева группа порядка* 8 *изоморфна либо* D_4*, либо* Q_8*.*

4 Разрешимые группы

Элемент $[a, b] = aba^{-1}b^{-1}$, называется *коммутатором* элементов $a, b \in G$. Коммутатор равен единице группы в том и только в 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 4.1. *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.

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

Предложение 4.2. *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

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

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 4.3. *Коммутант G' группы G является наименьшей нормальной подгруппой, фактор-группа по которой абелева.*

Доказательство. Пусть $\varphi : G \to G/G'$ – 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, $G' \subset N$. □

Пример 4.4. Найдем 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 $\{1, -1\}$.
Так как 1 и -1 (и только они) коммутируют со всеми остальными элементами группы кватернионов, то $Z(Q_8) = \{1, -1\}$.

Определение 4.5. *Кратные коммутанты определяются индуктивно: $G^{(k+1)} := (G^{(k)})'$, где $G^{(1)} := G'$.*

Предложение 4.6. *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. $\varphi(G_1^{(n)}) = G_2^{(n)}$.

□

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

Задача 4.7. 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 4.8. *Группа G называется разрешимой, если существует натуральное число $m \in \mathbb{N}$ такое, что $G^{(m)} = \{e\}$.*

Задачи 4.9. *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 4.10. *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 4.11. 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 группа $T(n-1,\mathbb{K})$ разрешима и используя только что доказанный факт разрешимости группы $\operatorname{Ker}\varphi$, получаем, что $T(n,\mathbb{K})$ разрешима. □

Лемма 4.12. *Группа четных подстановок A_n порождается тройными циклами при $n \geq 3$, 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 4.13. *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 $\sigma = (i_1 \dots i_p)(j_1 \dots i_q) \cdot \ \dots \ \cdot (k_1 \dots k_r)$, то

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

Следствие 4.14. *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 4.15. *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 4.13 и нормальности коммутанта получаем, что S_n' содержит все тройные циклы и, следовательно, S_n' совпадает с A_n (в силу леммы 4.12).

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 $|A_4'| = 2$. Последний случай исключается, что легко понять с помощью предложения 4.13.

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 4.12 совпадает с A_n.

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

5 Простые группы

Определение 5.1. *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.

5.1 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 5.2. *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 $\sigma \in N$, $\sigma \neq e$.

а) 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 4.13

$$\sigma' = i_\delta(\sigma) = i_\delta(\gamma)i_\delta(\tau) = i_\delta(\gamma)\tau = \delta\gamma\delta^{-1}\tau = \\ = (\delta(i_1)\delta(i_2)\delta(i_3)\dots\delta(i_p))\tau = (i_2i_1i_3\dots i_p)\tau \in N.$$

Поэтому

$$\sigma'\sigma^{-1} = (i_2i_1i_3\dots i_p)\tau\tau^{-1}(i_1i_2i_3\dots i_p)^{-1} = \\ = (i_2i_1i_3\dots i_p)(i_1i_2i_3\dots i_p)^{-1} = (i_1i_2i_3) \in N.$$

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 $\sigma = (i_1i_2)(i_3i_4)\tau$, где в τ не входят символы i_1, i_2, i_3, i_4. Положим $\delta = (i_2i_3)$. Тогда

$$\sigma' := i_\delta(\sigma) = i_\delta((i_1i_2))i_\delta((i_3i_4))i_\delta(\tau) = \\ = (\delta(i_1)\delta(i_2))(\delta(i_3)\delta(i_4))\tau = (i_1i_3)(i_2i_4)\tau \in N.$$

Следовательно,

$$\sigma'\sigma^{-1} = (i_1i_3)(i_2i_4)\tau\tau^{-1}(i_3i_4)^{-1}(i_1i_2)^{-1} = \\ = (i_1i_3)(i_2i_4)(i_3i_4)(i_1i_2) = (i_1i_4)(i_2i_3) \in N.$$

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 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. □

5.2 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 фактор-группа 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 5.3. *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 $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 0 \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}$, $\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 0 \\ 1 \end{pmatrix} = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$, и

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}\begin{pmatrix} 1 \\ 1 \end{pmatrix} = \begin{pmatrix} 0 \\ 1 \end{pmatrix},\ \text{получаем } \varphi(a) = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = (23),$$

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 5.4. *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

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

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

6 Элементы теории чисел

6.1 Мультипликативная группа конечного поля

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

Определение 6.1. *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 6.2. Показать, что
a) $\mathrm{Aut}(\mathbb{Z}) \cong \mathbb{Z}^* \cong \mathbb{Z}_2$,
b) $\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^*$.

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

Определение 6.3. *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 6.4 (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. □

Задача 6.5. Критерий Эйлера: сравнение $x^2 \equiv a \pmod p$ для a, не делящегося на простое $p > 2$, имеет два решения (отличающихся знаком), если $a^{\frac{p-1}{2}} \equiv 1 \pmod p$, и не имеет решения, если $a^{\frac{p-1}{2}} \equiv -1 \pmod p$. Если решение есть, то a сравнимо по модулю p с одним из чисел

$$1^2, 2^2, 3^2, \ldots, \left(\frac{p-1}{2}\right)^2.$$

[Указание: В силу малой теоремы Ферма $a^{p-1} \equiv 1 \pmod p$ для a, не делящегося на простое $p > 2$, поэтому $a^{\frac{p-1}{2}} \equiv \pm 1 \pmod p$.]

Теорема 6.6 (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 $1 \le k \le p-1$. 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 $1 \le k \le p-1$ и p – простое число, то либо $k = 1$, либо $k = p-1$. Следовательно, для k таких, что $2 \le k \le p-2$, 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 6.7. *Мультипликативная группа конечного поля является циклической, 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 $|\mathbb{K}^*| = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$, где p_j простые и $p_i \neq p_j$ при $i \neq j$. Пусть P_i – силовская p_i-подгруппа в $\mathbb{K}^*$, $|P_i| = p_i^{k_i}$, $i = 1, \dots, s$. 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 $g_1, \dots, g_s \in \mathbb{K}^*$ такие, что $\operatorname{ord}(g_i) = p_i^{k_i}$, откуда следует, что $\operatorname{ord}(g_1 \cdot \dots \cdot g_s) = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$ и, значит, $\mathbb{K}^*$ – циклическая группа (порядка $p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$). 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. $(\operatorname{ord}(a), \operatorname{ord}(b)) = 1$, то порядок произведения этих элементов равен произведению их порядков, т. е. $\operatorname{ord}(ab) = \operatorname{ord}(a) \cdot \operatorname{ord}(b)$.

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, порядок которого равен порядку группы $\mathbb{K}^*$, что означает, что группа циклическая. □

6.2 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 6.8 (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 $M_i \widetilde{M_i} \equiv 1 \pmod{m_i}$, $i = 1, \ldots, r$. 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 $x = x_0 + k m_1 \cdot \cdots \cdot m_r$, $k \in \mathbb{Z}$.

6.3 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 6.9. *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 $n = p_1^{d_1} \cdot \dots \cdot p_k^{d_k}$, где p_i – попарно различные простые числа, то

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

Приведем еще одно полезное соотношение:

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

Доказательство следует из тождества:

$$\sum_{d \mid n} \varphi(d) = (1 + \varphi(p_1) + \varphi(p_1^2) + \dots + \varphi(p_1^{d_1})) \cdot \dots \cdot (1 + \varphi(p_k) + \varphi(p_k^2) + \dots + \varphi(p_k^{d_k})).$$

Раскрыв скобки получаем слагаемые вида $\varphi(p_1^{s_1}) \dots \varphi(p_k^{s_k}) = \varphi(p_1^{s_1} \dots p_k^{s_k})$, где $1 \le s_j \le d_j$, $1 \le j \le k$, причем слагаемые встречаются только по одному разу, а это совпадает с тем, что стоит в левой части. Поскольку

$$1 + \varphi(p_j) + \varphi(p_j^2) + \dots + \varphi(p_j^{d_j}) = 1 + (p_j - 1) + (p_j^2 - p_j) + \dots + (p_j^{d_j} - p_j^{d_j-1}) = p_j^{d_j},$$

получаем требуемое $\sum\limits_{d \mid n} \varphi(d) = p_1^{d_1} \cdot \dots \cdot p_k^{d_k} = n$.

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 6.10 (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 6.11. *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 $m \ge 3$ 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 6.12. *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.

6.4 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 (R. Rivest, A. Shamir, L. Adleman).

Алгоритм служит для передачи конфиденциальной информации по незащищенному каналу связи.

Коротко принцип работы можно описать следующим образом:

Получатель пересылает по открытому каналу связи "открытый ключ", с его помощью отправитель шифрует сообщение и пересылает получателю, который, используя "закрытый ключ", дешифрует сообщение. Открытым ключом в RSA служит пара натуральных чисел (n, e), где $n = pq$ – произведение двух достаточно больших простых чисел p и q. Эти простые числа, а также e выбирает получатель, он же вычисляет натуральное число d – закрытый ключ, необходимый для дешифрования сообщения (о выборе e и d см. ниже).

Отправитель предварительно кодирует текст сообщения и получает целое неотрицательное число не превосходящее n, затем произвдит шифрование – получает новое целое число не превосходящее n, которое и пересылает по открытому каналу связи получателю. Поучатель расшифровывает, а затем декодирует пришедшее сообщение. Схема кодирования известна как отправителю так и получателю и, вообще говоря, секретом не является. В настоящем контексте она не имеет значения (например, можно закодировать буквы алфавита, пробел и знаки пунктуации двузначными числами, а затем получить целое число, записав коды символов текста сообщения подряд). Максимально возможное число символов в пересылаемом сообщении ограничено, оно тем больше, чем больше n (слишком длинный текст сообщения надо разбить на несколько подтекстов).

Практическая применимость алгоритма RSA основана на вычислительной сложности задачи факторизации больших натуральных чисел (факторизация – нахождение разложения натурального числа в произведение простых чисел). Зная n и e, закрытый ключ d можно вычислить только, если найти разложение числа n на множители. Если простые числа p и q состоят из нескольких сотен цифр, то зная $n = pq$ за обозримое время не удастся найти сомножители.

Итак, получатель выбирает простые числа p и q и вычисляет $n = pq$. Затем он выбирает число e такое, что e взаимно просто с $\varphi(n) = (p-1)(q-1)$, где $\varphi(n)$ – функция Эйлера. Пару (n, e), называемую открытым ключом, получатель пересылает отправителю. Наконец, получатель вычисляет закрытый ключ – такое d, что

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

Таким образом, e и d взаимно обратны в кольце $\mathbb{Z}_{\varphi(n)}$. Это число d, которое получатель держит в секрете, можно найти, например, с помощью алгоритма Евклида.

В качестве сообщения отправителем будет передаваться получателю целое число $a \in \{0, 1, \ldots, n-1\}$, которое отправитель предварительно зашифрует. Шифрование состоит в том, что отправитель вычисляет $b := a^e \pmod{n}$. Затем он отправляет b по каналу связи получателю, который дешифрует сообщение вычислив $b^d \pmod{n}$.

Поскольку $b^d = a^{ed}$, остается показать, что a и 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

$$a \equiv a^{ed} \pmod{n}.$$

Пусть сначала a взаимно просто с n. Тогда в силу теоремы Эйлера $a^{\varphi(n)} \equiv 1 \pmod{n}$. 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

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

Далее рассмотрим случай, когда a делится только на один из сомножителей. Например, пусть a делится на p и не делится на q. Тогда a^{ed} делится на p, поэтому $a^{ed} - a \equiv 0 \pmod{p}$. Поскольку a не делится на q, малая теорема Ферма дает сравнение $a^{q-1} \equiv 1 \pmod{q}$, и используя вычисление, приведенное в доказательстве первого случая, получаем:

$$\begin{aligned} a^{ed} &= a(a^{\varphi(n)})^m = a(a^{(p-1)(q-1)})^m = \\ &= a(a^{q-1})^{(p-1)m} \equiv a \cdot 1^{(p-1)m} \equiv a \pmod{q}. \end{aligned}$$

Таким образом, $a^{ed} - a \equiv 0 \pmod{q}$ и получается, что $a^{ed} - a$ делится на p и на q одновременно, откуда в силу простоты чисел p и q получаем, что $a^{ed} - a$ делится и на их произведение, и, следовательно, $a \equiv a^{ed} \pmod{n}$.

Наконец, если a делится и на p и на q, то a делится на n, но тогда и a^{ed} делится на n, поэтому $a^{ed} - a \equiv 0 \pmod{n}$, т. е. $a \equiv a^{ed} \pmod{n}$.