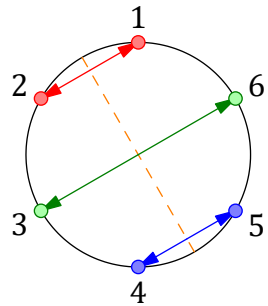
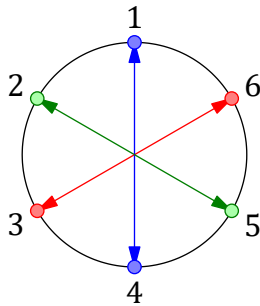
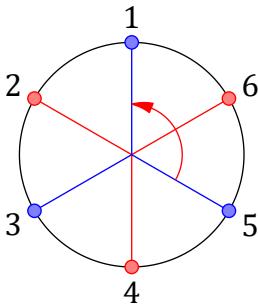
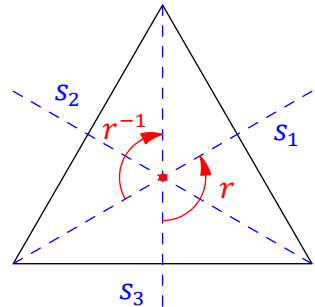
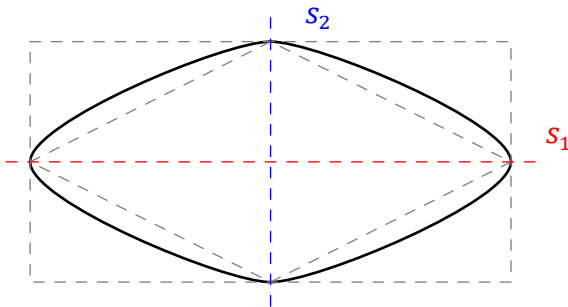
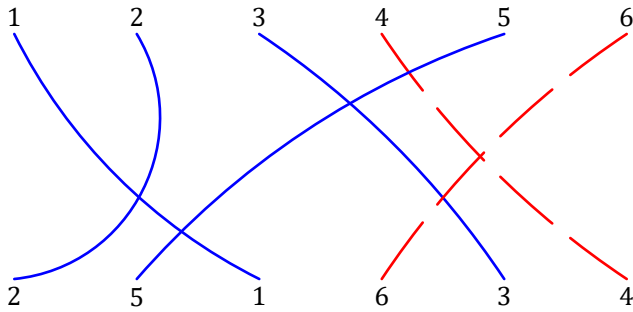


Алгебра-0,5

Направление точных наук

Егор Лунёв (@egorrshuk)



Место под соснами
Лето, 2025

Аннотация

А помните алгебру? Числа там, дроби всякие, уравнения, неравенства. На самом деле, это все ерунда. Алгебра – про структуры, про симметрии. Этот курс именно про это, мы будем изучать, что называют „абстрактной“ алгеброй. Может вы слышали, как учитель на уроке случайно сказал, о поле действительных чисел, а не о множестве. А про целые числа, так он почему-то не говорил. Мы подвигаем разные фигурки, повертим бусы в руках.

Чтобы понять каждую тему, нужно иметь базовые знания про числа, операции с ними и многочлены. Также он подойдет для тех, кто не боится непонятных слов (например, группа преобразований, гомоморфизм и поле) и хочет разобраться в том, что они значат.

Содержание

0	Множества и отображения	1
0.1	Множества	1
0.2	Отображения	2
0.2.1	Слои отображения	3
0.3	Классы эквивалентности	4
1	Перестановки	5
1.1	Нотация перестановок	7
1.1.1	Запись перестановки в виде циклов	8
1.2	Чётность и порядок	9
2	Введение в группы	10
2.1	Определение группы	10
2.1.1	Абелевы группы	14
2.2	Подгруппы	14
2.2.1	Циклические подгруппы	15
2.3	О классификации конечных групп	16
3	Группы фигур	17
3.1	Группы диэдров D_n	17
3.2	Группа тетраэдра	19
3.3	Группа додекаэдра	20
4	Действие группы на множестве	21
4.1	Орбита и стабилизатор	24
4.1.1	Связь между орбитой и стабилизатором	26
4.2	Подсчёт орбит	27
Задачи		29
0	Отображения и множества	29
1	Перестановки	29
2	Группы	31
3	Группы фигур	32
4	Действие группы	32
5	Формула Пойа-Бернсайда: ожерелья, орнаменты	32
Контрольная работа		33

Алгебра – наука о структурах, которые описываются с помощью операций и законов. Возможно, то что мы будем называть „алгебра“ – это не совсем то, что вы привыкли называть „алгебра“ Потому что в школьном курсе алгебры, особенно в старших классах, почему-то изучается анализ, а не сама алгебра.

0 Множества и отображения

Этот параграф носит вспомогательный характер. В нём собраны некоторые факты о множествах и отображениях, используемые в этой книге.

0.1 Множества

В конце 19 века Георг Кантор создал теорию множеств, пытаясь строго обосновать математику. Его идеи казались парадоксальными (множество всех множеств!), но стали фундаментом. Мы используем „наивную“ версию, избегая парадоксов. Для понимания этого курса достаточно интуитивного школьного представления о множестве как „абстрактной совокупности элементов произвольной природы“. Элементы множеств мы часто будем называть точками. Все точки в любом множестве, по определению, различны.

Множество X задано, как только про любой объект можно сказать, является он элементом множества X или нет. Принадлежность точки x множеству X записывается как $x \in X$. Два множества равны, если они состоят из одних и тех же элементов. Существует единственное множество, не содержащее ни одного элемента. Оно называется пустым и обозначается \emptyset . Если множество X конечно, то мы обозначаем через $|X|$ количество точек в нём.

Множество X называется подмножеством множества Y , если каждый его элемент $x \in X$ лежит также и в $y \in Y$. В этом случае пишут $X \subset Y$ или $X \subseteq Y$. Отметим, что пустое множество является подмножеством любого множества и всякое множество является подмножеством самого себя. Подмножества, отличные от всего множества, называются собственными. В частности, пустое подмножество непустого множества собственное. Если надо указать, что X является собственным подмножеством в Y , используется обозначение $X \subsetneq Y$.

Упражнение 1. Сколько всего подмножеств (включая пустое и несобственное) имеется у множества, состоящего из n элементов.

Для заданных множеств X, Y их *объединение* $X \cup Y$ состоит из всех элементов, принадлежащих хотя бы одному из множеств X, Y ; *пересечение* $X \cap Y$

состоит из всех элементов, принадлежащих одновременно каждому из множеств X, Y ; *разность* $X \setminus Y$ состоит из всех элементов множества X , которые не содержатся в Y .

Определение 0.1 (Дизъюнктное объединение). Множество X , являющееся объединением двух непересекающихся множеств Y и Z , называется *дизъюнктным объединением* $Y \sqcup Z$.

Пример 1. Множество натуральных чисел является дизъюнктным объединением четных и нечетных чисел.

Множество натуральных чисел является дизъюнктным объединением чисел с одним делителем (только 1), чисел с двумя делителями (простые) и чисел с большим количеством делителей (составные).

Пример 2. Множество человеческих рук является дизъюнктным объединением правых и левых рук.

Определение 0.2 (Декартово произведение). Множество $X \times Y$, элементами которого являются всевозможные пары (x, y) с $x \in X$, $y \in Y$, называется *декартовым произведением* множеств X и Y .

Пример 3. Координатная плоскость, которую не зря также называются декартовой, является декартовым произведением $\mathbb{R} \times \mathbb{R}$, такие произведения как и числа, удобно записывать в виде степени \mathbb{R}^2 .

Также как и на числовой прямой \mathbb{R} можно выделить целые числа \mathbb{Z} , а говоря формально $\mathbb{Z} \subset \mathbb{R}$, то и $\mathbb{Z}^2 := \mathbb{Z} \times \mathbb{Z} \subset \mathbb{R}^2$, что является целочисленной решеткой на координатной плоскости.

0.2 Отображения

Отображения $f: X \rightarrow Y$ из множества X в множество Y есть правило, однозначно сопоставляющее каждой точке $x \in X$ некоторую точку $y = f(x) \in Y$, которая называется образом точки x при отображении f .

Определение 0.3 (Полный прообраз). Множество всех таких точек $x \in X$, образ которых равен заданной точке $y \in Y$, называется *полным прообразом* точки y или *слоем* отображения f над y и обозначается

$$f^{-1}(y) \stackrel{\text{def}}{=} \{x \in X \mid f(x) = y\}.$$

Замечание. Полные прообразы различных точек не пересекаются и могут быть как пустыми, так и состоять из многих точек.

Определение 0.4 (Образ отображения). Множество $y \in Y$, имеющих непустой прообраз, называется образом отображения f и обозначается

$$f(X) = \text{im}(f) \stackrel{\text{def}}{=} \{y \in Y \mid \exists x \in X: f(x) = y\}.$$

Пример 4. Отображение $f: \{1, 2, 3, 4\} \rightarrow \{A, B, C\}$, где $f(1) = A, f(2) = B, f(3) = A, f(4) = A$. Тогда, например, $f^{-1}(C) = \emptyset$, а $\text{im}(f) = \{A, B\} \subset \{A, B, C\}$.

Два отображения $f, g: X \rightarrow Y$ равны, если $f(x) = g(x)$ для всех $x \in X$.

Определение 0.5 (Сюръекция). Отображение $f: X \rightarrow Y$ называется *наложением* (а также *сюръекцией* или *эпиморфизмом*), если $\text{im}(f) = Y$. Мы будем отображать сюръективные отображения стрелками $f: X \twoheadrightarrow Y$.

Определение 0.6 (Инъекция). Отображение $f: X \rightarrow Y$ называется *вложением* (а также *инъекцией* или *мономорфизмом*), если $f(x_1) \neq f(x_2)$ при $x_1 \neq x_2$. Мы будем отображать инъективные отображения стрелками $f: X \hookrightarrow Y$.

Упражнение 2. Перечислите все отображения $\{0, 1, 2\} \rightarrow \{0, 1\}$ и $\{0, 1\} \rightarrow \{0, 1, 2\}$. Сколько среди них сюръекций и инъекций?

Определение 0.7 (Биекция). Отображение $f: X \rightarrow Y$, которое является и вложением, и наложением называется *взаимно однозначным* (а также *биекцией* или *изоморфизмом*). Мы будем обозначать биекцию стрелками $X \xrightarrow{\sim} Y$.

Упражнение 3. Из отображений: (a) $\mathbb{N} \rightarrow \mathbb{N}: x \mapsto x^2$; (b) $\mathbb{Z} \rightarrow \mathbb{Z}: x \mapsto x^2$, и (c) $\mathbb{Z} \rightarrow \mathbb{Z}: x \mapsto 7x$ выделите все вложения, наложения и биекции.

0.2.1 Слои отображения

Задание отображения $f: X \rightarrow Y$ равносильно указанию подмножества $\text{im}(f) \subset Y$ и разбиению множества X в дизъюнктное объединение занумерованных точками $y \in \text{im}(f)$ непустых подмножества $f^{-1}(y)$:

$$\bigsqcup_{y \in \text{im}(f)} f^{-1}(y).$$

Такой взгляд на отображения часто оказывается полезным при подсчёте количества элементов в том, или ином множестве. Например, когда все непустые слои отображения $f: X \rightarrow Y$ состоят из одного и того же числа точек $a = |f^{-1}(y)|$, число элементов в образе отображения f связано с числом элементов в множестве X соотношением

$$|X| = a \cdot |\text{im}(f)|.$$

Которое при всей своей простоте имеет много различных применений.

0.3 Классы эквивалентности

Альтернативным способом разбить множество X в дизъюнктное объединение подмножеств состоит в том, чтобы объявить элементы, входящие в одно подмножество такого разбиения „эквивалентными“. Формализуем это так.

Определение 0.8 (Бинарное отношение). Назовём *отношением* на множестве X любое подмножество

$$R \subset X \times X = \{(a, b) \mid a, b \in X\}.$$

Принадлежность какой-то пары (a, b) отношению R обычно записывают как $a \sim_R b$, а еще чаще опускают до $a \sim b$.

Пример 5. На множестве целых чисел \mathbb{Z} имеются отношения

$$\begin{array}{ll} \text{равенство} & a \sim b \Leftrightarrow a = b; \\ \text{неравенство} & a \sim b \Leftrightarrow a \leq b \\ \text{делимость} & a \sim b \Leftrightarrow a \text{ делится на } b \\ \text{сравнимость по модулю } n & a \sim b \Leftrightarrow a \equiv b \pmod{n}^1. \end{array}$$

Пример 6 (Отношение эквивалентности). Отношение $R \subset X \times X$ называется *эквивалентностью*, если оно обладает тремя свойствами:

- (i) рефлексивность: $a \sim a, \quad \forall a \in X$;
- (ii) транзитивность: для любых $a, b, c \in X$ из $a \sim b$ и $b \sim c$ вытекает $a \sim c$;
- (iii) симметричность: $a \sim b \Leftrightarrow b \sim a, \quad \forall a, b \in X$.

Если множество X разбито в объединение непересекающихся подмножеств, то отношение $a \sim b$ означающее, что a и b лежат в одном и том же подмножестве этого разбиения, оче видно, является эквивалентностью.

Наоборот, пусть на множестве X задано отношение эквивалентности R . Рассмотрим для каждого $x \in X$ подмножество в X , состоящее из всех элементов, эквивалентных x . Оно называется классом эквивалентности элемента x и обозначается

$$[x]_R \stackrel{\text{def}}{=} \{z \in X \mid x \sim z\}.$$

Любые два класса $[x]_R$ и $[y]_R$ либо вообще не пересекаются, либо полностью совпадают. В самом деле, если существует элемент z , эквивалентный и x и y , то в силу симметричности и транзитивности отношения R элементы

x и y будут эквивалентны между собой, а значит, любой элемент, эквивалентный x , будет эквивалентен также и y , и наоборот. Таким образом, множество X распадается в дизъюнктное объединение различных классов эквивалентности.

Определение 0.9 (Факторизация). Множество классов эквивалентности по отношению $R \subset X \times X$ называется *фактором* множества X по отношению R и обозначается X/R . Наложение

$$f: X \rightarrow X/R, \quad x \mapsto [x]_R,$$

сопоставляющее каждому элементу $x \in X$ его класс эквивалентности называется *отображением факторизации*.

Пример 7 (Классы вычетов). Зафиксируем натуральное $n \in \mathbb{N}$. Фактор множества \mathbb{Z} по отношению сравнимости по модулю n обозначается $\mathbb{Z}/(n)$. Мы будем записывать его элементы символами $[z]_n$, где $z \in \mathbb{Z}$, и часто опускать индекс n . Класс эквивалентности

$$[z]_n := \{x \in \mathbb{Z} \mid (z - x) \text{ делится на } n\}$$

называется *классом вычетов* по модулю n . Отображении факторизации

$$f: \mathbb{Z} \rightarrow \mathbb{Z}/(n), \quad z \mapsto [z]_n$$

называется *приведением* по модулю n . Множество $\mathbb{Z}/(n)$ состоит из n различных классов

$$[0]_n, [1]_n, \dots, [n-1]_n.$$

При желании их можно воспринимать как остатки от деления на n , однако в практических вычислениях удобно работать именно с *подмножествами*. Например, остаток от деления 12^{100} на 13 можно искать как

$$[12^{100}]_{13} = [12]_{13}^{100} = [-1]_{13}^{100} = [(-1)^{100}]_{13} = [1]_{13}.$$

1 Перестановки

Первая структура, с которой мы с вами познакомимся – это группы. Это одно из самых „базовых понятий“, но оно же и является центральным.

Самая интерпретируемая группа — это группа перестановок. Вероятно, вы уже слышали о том, что такое перестановка, не задумываясь о её групповой структуре. Для начала, „нестрого“ разберемся с перестановками.

Упражнение 1. Сколько есть способов переставить n человек в очереди?

Пример 1. Напишем, какое-нибудь слово, например:

УШКА¹

За один шаг разрешается поменять местами любые две буквы. Например, можно поменяв буквы А и К, получить слово

УШАК

Упражнение 2. Можно ли получить слово КАШУ из слова УШКА за один шаг? Если нет, то за какое минимальное число шагов можно это сделать?

Упражнение 3. Можно ли, начав, со слова ТАПОК, вернуться в исходное слово после 10 шагов? После 11 шагов?

В упражнении 3, вы заметили, что за 10 шагов все получилось. А вот за 11 — никак. На самом деле это не случайность, и верен более общий факт.

Утверждение 1.1. Если на каждом шаге разрешено менять только две буквы, то за нечетное число шагов не получится вернуться в исходное слово.

Теперь возьмём другое слово, допустим, АДО. Есть три пары букв, которые можно поменять. Так что, за один шаг мы можем получить три слова.

ОДА ДАО АОД

На втором шаге мы должны выбрать одно из этих слов и поменять в нём две буквы. Пару для обмена в каждом слове можно выбрать двумя способами, а два другие дадут новые слова.

ОДА → ДОА ОАД АДО

ДАО → ДОА ОАД АДО

АОД → ДОА ОАД АДО

Видно, что в результате получаются одни и те же три слова.

ДОА ОАД АДО

Упражнение 4. Проверьте, что за три шага получается тот же набор слов, что и за 1 шаг.

Видно, что мы разбили все варианты на две группы по три слова и на каждом шаге переходим из одной группы в другую:

АДО ОАД ДОА ↔ ДАО АОД ОДА

А значит, вернуться в исходную группу (в частности, получить слово АДО) можно только за четное число шагов.

¹Это слово осмысленное, но в дальнейшем, мы будем называть „словами“ любые цепочки букв, не заботясь о том, являются ли они словами русского языка.

1.1 Нотация перестановок

Определение 1.2 (Перестановка). Перестановка — это биективное отображение, которое множеству букв сопоставляет себя.

$$\sigma : \{1, 2, \dots, n\} \rightarrow \{1, 2, \dots, n\}.$$

Перестановка σ может быть записана в виде¹

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \dots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \dots & \sigma(n) \end{pmatrix}.$$

Пример 2. При перестановка $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ Первая буква переходит на вторую, вторая — на первую, третья — на четвёртую, четвёртая — на третью. Допустим, со словом **ЙОТА** наша перестановка σ сделает (на рисунке **1**):

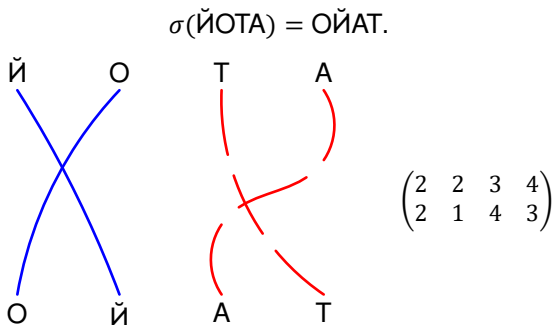


Рис. 1: Перестановка σ .

Применяя одну перестановку за другой, мы можем получить новую перестановку. Для этого тоже есть запись. Пусть у нас есть две перестановки σ и τ . Тогда их произведение $\sigma \circ \tau$ — это перестановка, которая получается из τ , после чего к ней применяют σ ¹.

Пример 3. Пусть $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$ и $\tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 4 & 3 & 1 \end{pmatrix}$. Тогда их произведение будет равно:

$$\sigma \circ \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ \sigma(\tau(1)) & \sigma(\tau(2)) & \sigma(\tau(3)) & \sigma(\tau(4)) \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 4 & 2 \end{pmatrix}.$$

¹Существуют и другая запись: $(\sigma(1) \sigma(2) \sigma(3) \dots \sigma(n))$.

¹Да! Именно так! Слева-направо!

Давайте рассмотрим, что у нас происходит на примере слова КИНО (на рисунке 2).

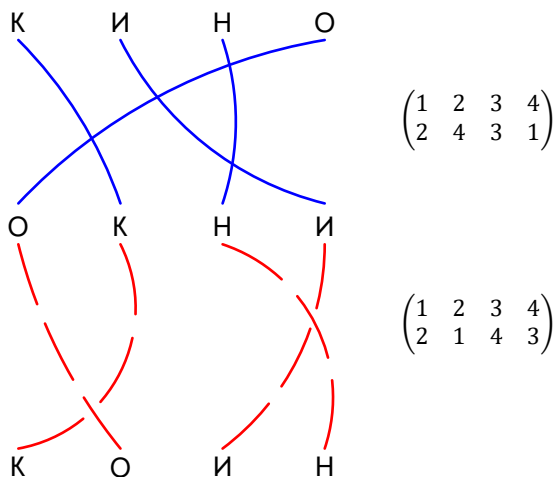


Рис. 2: Перестановка $\sigma \circ \tau$.

Упражнение 5. Найдите композицию $\tau \circ \sigma$. Проверьте, что это не то же самое, что $\sigma \circ \tau$.

1.1.1 Запись перестановки в виде циклов

Определение 1.3 (Циклическая запись). Любую перестановку можно записать в виде композиции циклов. Например, перестановка σ (на рисунке 4)

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 1 & 5 & 6 & 2 & 4 \end{pmatrix}.$$

Записывается в виде:

$$\sigma = |1 \ 3 \ 5 \ 2|4 \ 6\rangle.$$

У такой записи есть „свобода выбора“. Один и тот же цикл можно записать по-разному. Например,

$$|1 \ 3 \ 5 \ 2\rangle = |3 \ 5 \ 2 \ 1\rangle = |5 \ 2 \ 1 \ 3\rangle = |2 \ 1 \ 3 \ 5\rangle.$$

Мы будем говорить, что у перестановки σ цикловой тип $(4, 2)$ (в данном случае, это значит, что у нас есть один 4-цикл и один 2-цикл). А иногда еще будем рисовать диаграмму Юнга (на рисунке 3), данного циклового типа.

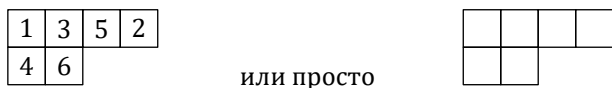
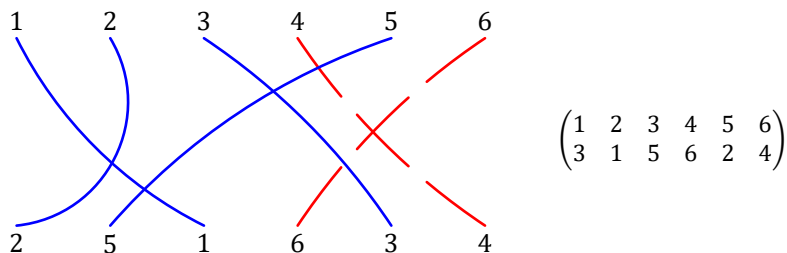
Рис. 3: Цикловой тип перестановки σ .

Рис. 4: Циклическая запись перестановки.

1.2 Чётность и порядок

Есть одно важное понятие, которое может таким не показаться. Возможно, мы не сможем в полном объеме раскрыть его в этом курсе, но что же поделать. Перед этим, скажем, что *транспозиция* — это перестановка, которая меняет местами только две буквы.

Определение 1.4 (Четность перестановки). Перестановка называется *четной*, если она может быть записана в виде произведения четного числа транспозиций. Иначе, она называется *нечетной*.

Следствие 1.4.1. *Перестановка является чётной, если в ней чётное число циклов чётной длины.*

Утверждение 1.5. *Перестановка является четной, если на рисунке „ниточек“ нечётное число пересечений.*

Определение 1.6 (Порядок перестановки). Порядок перестановки σ — это наименьшее число n , такое что $\sigma^n = \text{id}$.

Теорема 1.7. *Порядок перестановки σ равен наименьшему общему кратному длин всех циклов в её циклической записи.*

Доказательство. Цикл длины k_i возвращает элементы на место после k_i применений. Поскольку циклы не пересекаются, порядок всей перестановки — минимальное число k , при котором k делится на каждое k_i . Это и есть наименьшее общее кратное k_1, k_2, \dots, k_m . \square

2 Введение в группы

Симметрия, как бы широко или узко мы не понимали это слово, есть идея, с помощью которой человек веками пытался объяснить и создать порядок, красоту и совершенство.

Герман Вейль.

«Теория групп» расширяет и формализует понятие *симметрии*. Например, когда мы говорим, что у человека симметричное лицо, мы подразумеваем, что мы можем отразить его лицо относительно *оси симметрии*, и оно будет выглядеть абсолютно также. Это утверждение о действии. Или, например, снежинка тоже симметрична, но во много большем порядке: мы можем поворачивать ее на 60° или на 120° , можно отражать ее относительно множества осей симметрии или не делать ничего; и все эти преобразования оставят ее вид прежним. Вот такое вот собрание действий и называется группой.

Вернее, если бы более честным, то группа это более формальное и абстрактное понятие. Например, как и число 3. Обращаясь к нему мы не задумываемся о каком именном числе объектов идет речь: не важно головки сыра это или миллиарды лет. Но с числом работать намного удобнее: складывая два числа, мы совсем-совсем уже забываем о изначальной „природе“.

2.1 Определение группы

Определение 2.1 (Группа). Это множество G с операцией \star , которое обладает следующими свойствами:

(i) *Замкнутость*:

$$\forall a, b \in G : a \star b \in G.$$

(ii) *Ассоциативность*:

$$\forall a, b, c \in G : (a \star b) \star c = a \star (b \star c).$$

(iii) *Наличие нейтрального элемента*:

$$\exists e \in G : \forall a \in G : e \star a = a.$$

(iv) *Наличие обратного элемента:*

$$\forall a \in G : \exists a^{-1} \in G : a \star a^{-1} = e.$$

Для группы также существует обозначение: (G, \star) . Если группа G конечна, то ее порядок $|G|$ – это количество элементов в ней.

Стоит еще обратить свое внимание на то, насколько общеупотребимое слово выбрано для этого понятия, для казалось бы, такого специфического объекта симметрий. Это показатель фундаментальности и общности этого понятия. Группа фиксирует суть симметрии объекта — не сами движения, а то, как они сочетаются друг с другом. Операция в группе (композиция) кодирует вопрос: 'Если я сделаю преобразование А, а потом преобразование В, какое одно преобразование С даст тот же итоговый эффект?' Именно эта структура (замкнутость, ассоциативность, наличие 'ничего' и 'отмены') делает группы универсальным инструментом для описания симметрий любой природы.

Существуют различные классификации групп. Например, классификация по типу операции. Бывают группы по сложению (аддитивные), то есть с операцией сложения. А также бывают группы по умножению (мультипликативные) – с операцией умножения.

Пример 1. Группа отражений лица по вертикали называется группой $\mathbb{Z}/(2)$ и состоит ровно из двух элементов: ничего не делать и сделать что-то.

Пример 2. $(\mathbb{Z}, +)$ множество целых чисел с операцией сложения.

Пример 3. $(\mathbb{Z}/(5), +)$ множество остатков по модулю 5 с операцией сложения.

Пример 4. (\mathbb{R}, \cdot) множество действительных чисел с операцией умножения.

Пример 5. Как множество – движения правильной фигуры, а операция тут – композиция этих движений. Например, у нас есть квадрат. Мы можем его поворачивать на 90 градусов, а также можем его отражать относительно осей симметрии. Тогда у нас получится группа, которая называется D_4 ¹, она состоит из 8 элементов (на рисунке 5):

- | | |
|---------------------------------|---------------------------------|
| • e — ничего не делать; | сов; |
| • r — поворот на 90 градусов; | • r^3 — поворот на 270 граду- |
| • r^2 — поворот на 180 граду- | сов; |

¹Также такую группу можно было назвать $\text{Isom}(\square)$.

- s_1 — отражение относительно оси симметрии по оси x ;
- s_2 — отражение относительно оси симметрии по оси y ;
- s_3 — отражение относительно диагонали, которая идет

из левого верхнего угла в правый нижний;

- s_4 — отражение относительно диагонали, которая идет из правого верхнего угла в левый нижний.

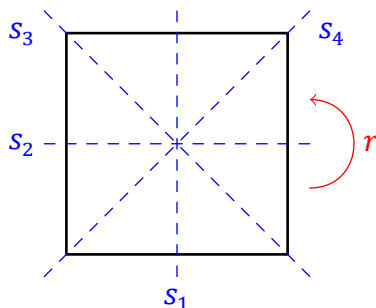


Рис. 5: Группа движений квадрата

Пример 6 (Симметрическая группа). До этого мы рассматривали с вами перестановки букв в словах. Такие перестановки тоже образуют группу. Она обозначается S_n , где n — количество букв в слове, а называется *симметрической*.

Пример 7 (Группа кубика Рубика). Примером группы огромного порядка ($\sim 4,3 \cdot 10^{19}$) может быть группа кубика Рубика. Повороты граней кубика Рубика образуют группу. Композиция поворотов — это наша операция. 'Ничего не делать' — нейтральный элемент. Обратный элемент — поворот в обратную сторону или последовательность ходов, отменяющая действие. Эта группа не коммутативна: повернуть верхнюю грань, а потом правую — не то же самое, что повернуть правую, а потом верхнюю!

Пример 8 (Группа автоморфизмов множества). Все взаимно однозначные отображения множества X в себя (перестановки его элементов) образуют группу. Она обозначается $\text{Aut } X$ и называется *группой автоморфизмов* множества X . Если группа X конечна, то $\text{Aut } X \cong S_{|X|}$.

Заострим свое внимание на том, насколько важна структура, которую мы хотим сохранить в группах. Допустим у нас есть 6 точек и мы хотим рассмотреть все-все преобразования, которые оставляют их на месте. Мы

уже познакомились с таким понятием — это все перестановки 6 элементов, а таких 720 штук. Если же в точках была дополнительная структура, допустим, они бы образовывали вершины правильного шестиугольника, то движений которые оставляют такой шестиугольник на месте ровно 12 штук. Столько же, сколько и симметрий у снежинки.

Утверждение 2.2. Правый нейтральный элемент равен левому нейтральному элементу.

Доказательство. Пусть e_l — левый нейтральный элемент, а e_r — правый нейтральный элемент. Тогда: $e_l = e_l * e_r = e_r$. \square

Утверждение 2.3. Если e — нейтральный элемент группы, то он единственный.

Доказательство. Пусть e_1 и e_2 — нейтральные элементы группы. Тогда: $e_1 = e_1 * e_2 = e_2$. \square

Упражнение 1. Докажите, что правый обратный элемент равен левому обратному элементу.

Упражнение 2. Докажите, что обратный элемент единственный.

Да, все эти движения могут показаться интересными, но может возникнуть вопрос зачем это все нужно... Одно из применений групп возникло, когда математики прошлого столкнулись с проблемой решений уравнений различных степеней. Вы уже знакомы с тем, как находить корни квадратного уравнения: для этого есть довольно удобная формула дискриминанта. Возможно, вы знаете, что есть формула для кубического уравнения, а также для уравнения 4-степени, правда они уже довольно ужасны. В поисках формулы для уравнений пятой степени люди были безуспешны, как оказалось, за этим стоит группа, которая переставляет корни уравнения пятой степени, а именно S_5 и её подгруппа A_5 , вот что-то в их природе такое есть, что не делает разрешимым в радикалах уравнения выше пятой степени. Теория о автоморфизмах корней уравнений называется «теорией Эвариста Галуа»

Молодой французский математик Эварист Галуа (1811–1832), буквально за ночь перед дуэлью, записал идеи, связавшие разрешимость уравнений в радикалах со структурой групп перестановок их корней. Он ввел само понятие группы (хотя и не использовал этот термин) и показал, почему для уравнений степени 5 и выше общей формулы быть не может. Его работы легли в основу теории Галуа.

Один из самых глубоких результатов, связывающих симметрии и реальный мир — теорема Эмми Нётер (1918). Грубо говоря, она гласит: Каждой

непрерывной симметрии физической системы соответствует закон сохранения. Симметрия относительно сдвигов во времени? Сохранение энергии! Симметрия относительно сдвигов в пространстве? Сохранение импульса! Симметрия относительно поворотов? Сохранение момента импульса! Группы лежат в основе формулировки этих симметрий.

2.1.1 Абелевы группы

Среди всех групп, абелевы группы, пожалуй самые „родные“ и понятные, для большинства людей в мире. Идея о том, что операция коммутативна — очень приятна, поэтому давайте познакомимся с ними.

Определение 2.4 (Абелева группа). Группа G ¹ называется абелевой, если она коммутативна, то есть:

$$\forall a, b \in G : ab = ba..$$

В этом моменте нужно себя спросить: „А что, бывает по-другому?“ И вот оказывается, что бывает. Для этого, можно рассмотреть один яркий пример.

Пример 9. В группе S_3 если взять, например $|1, 2\rangle$ и $|1, 3\rangle$, То $|1, 2\rangle|1, 3\rangle = |1, 3, 2\rangle$, а если взять в обратном порядке, т.е. $|1, 3\rangle|1, 2\rangle = |1, 2, 3\rangle$. Поэтому группа S_3 не абелева!

Пример 10. Пусть у нас есть группа G , которая содержит в себе, по крайней мере два элемента: $a =$ „надеть носок“ и $b =$ „надеть ботинок“.² Тогда одна последовательность действий не приведет к *странным взглядам окружающих*, а другая да.

Упражнение 3. Какой из этих случаев „нормален“, а какой нет?

Упражнение 4. Является ли группа D_4 абелевой?

Упражнение 5. Приведите свои примеры *абелевых* и *неабелевых* групп.

2.2 Подгруппы

Определение 2.5 (Подгруппа). Пусть G – группа. Тогда $H \subset G$ называется подгруппой, если:

¹Часто операция опускается и подразумевается, что группа мультипликативна.

²Такая группа устроена довольно сложно и в нашем курсе рассматриваться не будет. Ее название F_2 .

- (i) $e \in H$;
- (ii) $\forall a, b \in H : a \star b \in H$;
- (iii) $\forall a \in H : a^{-1} \in H$.

Пример 11. Четные целые числа с операцией сложения образуют подгруппу группы $(\mathbb{Z}, +)$.

Пример 12. Множество поворотов квадрата образует подгруппу группы D_4 .

Пример 13 (Знакопеременная группа). Множество четных перестановок образует подгруппу группы S_n . И такая подгруппа обозначается A_n , а называется *знакопеременной*.

Пример 14 (Группа преобразований). Классическим примером групп являются *группы преобразований*. Любая подгруппа $G \subset \text{Aut } X$ (в примере 8) называется *группой преобразований* множества X . Как правило мы будем сокращать запись $g(x)$, где $g \in G, x \in X$, до gx . Если X наделено дополнительной структурой, то биекции $g \in \text{Aut } X$, сохраняющую эту структуру, образуют подгруппу в группе $\text{Aut } X$, которая обычно называется группой автоморфизмов этой структуры.

Упражнение 6. Придумайте свои примеры подгрупп.

Упражнение 7. Являются ли четные целые числа подгруппой группы (\mathbb{Z}, \cdot) ?

2.2.1 Циклические подгруппы

Определение 2.6 (Циклическая подгруппа). Наименьшая по включению подгруппа $H \subset G$, содержащая данный элемент $g \in G$, состоит из всевозможных целых степеней g , и называется *циклической*, а обозначается $\langle g \rangle$. Она является абелевой.

Наименьшая степень $n \in \mathbb{N}$, для которого $g^n = e$, называется *порядком элемента g* .

Замечание. Порядок элемента — это не то же самое, что и порядок группы. Например, в группе $\{e, g, g^2, g^3\}$, где $g^4 = e$, порядок элемента g равен 4 и совпадает с порядком группы. А порядок элемента g^2 равен 2.

Циклическая подгруппа, порожденная элементом g , похожа на циферблат часов с n делениями (где n — порядок g). Умножение на g — это поворот стрелки на одно деление. Умножение на g^k — поворот на k делений. „Обнуление“ ($g^n = e$) происходит, когда стрелка делает полный круг.

Пример 15. Группа $(\mathbb{Z}, +)$ является циклической, так как $G = \langle 1 \rangle$.

Пример 16. Группа $(\mathbb{Z}/(n), +)$ является циклической, так как $G = \langle 1 \rangle$.

2.3 О классификации конечных групп

Вопросом о классификации всех возможных конечных групп, вы наверняка задались, но я постараюсь немного на него ответить.

Во-первых, мы всегда задаемся вопросом насколько сильно классифицировать группы, будем ли мы считать группу преобразований черного листа A4 отличной от группы преобразований синего листа A4? И конечно, хочется сказать нет, и мы так и сделаем, ответив более формально.

Мы считаем группы с точностью до их изоморфизма. Это означает, что если мы сможем сопоставить взаимно однозначное соответствие между элементами двух групп, при этом также между тем, как эти элементу умножаются, то такие группы будут одинаковыми.

Пример 17. Например, как мы скоро узнаем, группа движений правильного треугольника изоморфна перестановкам из трех элементов. А группа перестановок из 4 элементов изоморфна группе вращений куба (изоморфизм строится по диагоналям.)

Кажется, теперь пора сказать, что этот вопрос оказался чрезвычайно сложным. И был решен лишь в 2004 году. Математики нашли все *простые* группы, „периодическую таблицу групп“. Эта таблица состоит из 18 бесконечных семейств групп, а также 26 отдельных «*спорадических групп*». Одним из семейств являются все простые циклические группы: $\mathbb{Z}/(2)$, $\mathbb{Z}/(3)$, $\mathbb{Z}/(5)$, $\mathbb{Z}/(7)$, ..., еще одним семейством являются четные перестановки A_5 , A_6 , A_7 , Остальные 16 групп являются *группами Ли*, которые намного сложнее.

Но самыми интересными и непонятными являются те самые 26 спорадических групп, которые так странно выглядят, в таком фундаментальном месте, как теория групп. Наибольшей из них является известная *группа Монстра* Джона Конвея. Ее порядок равен 808, 017, 424, 794, 512, 875, 886, 459, 904, 961, 710, 757, 005, 754, 368, 000, 000, 000. Следующая по порядку, и это совсем не шутка, называется *маленький Монстр* (*baby monster group*). На самом деле 20 из 26 относятся к семье „монстров“, а остальные 6 называется *изгоями*. Как и прошлые группы, группа Монстра описывает симметрии какого-то объекта, но не как мы привыкли в 2- или 3-мерном пространстве, и даже не 4 — 196883-мерном пространстве. Один элемент такой группы занимает без сжатия 4 гигабайта памяти в компьютере.

В 70-х годах прошлого столетия математик Джон Маккей перестает заниматься конечными группами и начинает заниматься смежной с теорией групп теорией Галуа. И удивительным образом находит число очень похожее на 196883, выплывшее в совершенно не связанном месте. Число на

1 больше данного возникло в разложении в ряд одной из фундаментальнейших функций теории модулярных форм и эллиптических функций. Эту проблему назвали «Monstrosus moonshine» (гипотеза чудовищного вздора). Позже в 1992 Ричард Боршердс доказал эту связь, кстати, спустя 6 лет он выиграл Филдовскую медаль. Это достижение позволило установить связь между группой Монстра и теорией струн.

3 Группы фигур

Рассмотрим фигуру Φ в „обычном“ n -мерном пространстве.¹ Группа преобразований $\Phi \rightarrow \Phi$, переводящих фигуру в себя называется *полной группой фигуры* Φ . Подгруппа, сохраняющая „ориентацию“ фигуры, называется *собственной группой фигуры* Φ .

3.1 Группы диэдров D_n

Определение 3.1 (Группа диэдра). Группа преобразований правильно плоского n -угольника, лежащего в трёхмерном пространстве, называется *группой диэдра*².

Пример 1. Простейший диэдр, пусть нам и непривычный, называется *двуугольник*. Его можно представлять себе, как выпуклую линзу или глаз (на рисунке 6). Группа D_2 такой линзы совпадает с группами описанного вокруг неё прямоугольника, и вписанного в него ромба. Она состоит из трех поворотов, вокруг каждой из координатных осей, а также из тождественного движения, которое еще обозначается id .

Упражнение 1. Убедитесь, что $D_2 \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2)$.

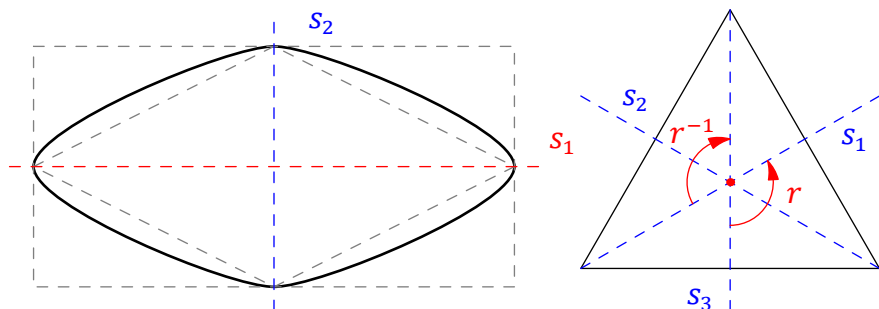
Группа D_2 настолько часто возникала в математике, что для нее придумали даже специальное название. А именно, *Группа Клейна или четверная группа Клейна* V_4 .

Вообще, имя Феликса Клейна не возникает в школьной программе, что и понятно. Его знаменитый доклад на *Эрлангенской конференции* призывал изучать геометрию именно с помощью групп, как это делаем и мы сейчас: изучать то, какие движения оставляют на месте разные объекты.

Пример 2. Следующая диэдральная группа — группа треугольника D_3 (на рисунке 6). Она состоит из тождественного движения, двух поворотов r, r^{-1}

¹Мы не будем рассматривать размерности больше 3.

²Диэдр (диэдра) — это правильный плоский многоугольник.

Рис. 6: Двуугольник D_2 и треугольник D_3 .

на $\pm 120^\circ$ вокруг центра треугольника, а также из трёх осевых симметрий s_1, s_2, s_3 . Воспользуемся следующей леммой, что доказать изоморфизм S_3 и D_3 .

Лемма 3.2. *Движение плоскости однозначно задается своим действием на вершины треугольника.*

В этом курсе мы ее строго не докажем, но я приведу некоторые факты, которые помогут ее понять. Понятно, что действия на две вершины не хватит, ведь можно сделать осевую симметрию относительно прямой, проходящей, через эти точки. А трёх вершин уже будет достаточно, ведь мы будем знать расположение третьей, а вернее в какой полуплоскости она лежит.

Доказательство изоморфизма. Теперь можем доказать изоморфизм групп. Понятно, что $D_3 \subset S_3$. Осталось показать, что $S_3 \subset D_3$. Любой элемент из S_3 действует на вершины треугольника, а тем самым порождает движение плоскости, что в частности является движением треугольника. \square

Поскольку движение плоскости, сохраняющее правильный n -угольник определяется своим действием на 3 точки (какой-нибудь вершиной, например, и парой соседних сторон). Тогда группа диэдра при $n \geq 3$ ¹ состоит из $2n$ движений. Выбранную вершину можно перевести в любую из n вершин диэдра, а потом двумя способами совместить оставшиеся ребра. Этим $2n$ движений состоят из n поворотов на $\frac{2\pi}{n}$ (циклическая группа порядка

¹На самом деле, даже при $n \geq 2$.

n), а также n симметрий относительно прямых проходящих через пару середин противоположных сторон, в случае четногоугольника, а в случае нечетногоугольника — прямые проходящие через вершину, и середину противоположащей стороны.

Упражнение 2. Порисовать диэдры, их оси симметрий и повороты.

Упражнение 3. Написать таблицы Кэли (умножения) для групп D_3 , D_4 , D_5 .



Рис. 7: Другие объекты, обладающие группами D_3 , D_4 , D_5 и D_6 .

3.2 Группа тетраэдра

Как и в случае с треугольником воспользуемся схожей леммой. Тогда любое движение пространства, сохраняющее на месте тетраэдр однозначно определяется своим действием на вершины. Тем самым, полная группа тетраэдра изоморфна S_4 .

Собственная же группа состоит из $4 \cdot 3 = 12$ движений: поворот тетраэдра однозначно задаётся своим действием на вершину, и три ребра которые через нее проходят, и может переводить эту вершину в любую из четырёх вершин, после чего, остается ровно три возможности для совмещения рёбер, сохраняющее ориентацию пространства. Полный список всех собственных движений тетраэдра:

1. тождественное преобразование;

2. $4 \cdot 2 = 8$ поворотов на углы $\pm 120^\circ$ вокруг прямых, проходящих через вершину и центр противоположной грани;
3. 3 поворота на 180° вокруг прямых, проходящих через середины противоположных рёбер.

В несобственной группе, помимо этих движений, еще содержится 6 отражений s_{ij} в плоскостях, проходящих через середину ребра ij и ребро kl . В группе S_4 таким отражениям соответствуют транспозиции букв i и j ; повороты на $\pm 120^\circ$ переходят в 3-циклы переставляющие буквы i, j, k по циклу, они представляют собой композиции $s_{ij}s_{jk}$; три вращения на 180° , представляющие собой одновременную транспозицию пары вершин, т.е. $s_{ij}s_{kl}$ переходят в перестановки: $|12\rangle|34\rangle$, $|13\rangle|24\rangle$, $|14\rangle|23\rangle$.

Упражнение 4. Убедитесь, что вместе в тождественным преобразованием, эти три поворота образуют группу изоморфную V_4 .

Оставшиеся 6 несобственных преобразований тетраэдра соответствуют 4-циклам $|1234\rangle$, $|1243\rangle$, $|1324\rangle$, $|1342\rangle$, $|1423\rangle$, $|1432\rangle$. Они реализуются с помощью поворота на $\pm 90^\circ$ вокруг оси, проходящей через середины противоположных рёбер, с последующим отражением относительно „сер-перной“ плоскости этого отрезка.

3.3 Группа додекаэдра

Воспользуемся той же самой леммой, что и в случае тетраэдра, для определения порядка собственной группы додекаэдра. Движение додекаэдра однозначно определяется действием на вершину и три ребра, тем самым может переводить вершину в любую из 20, а затем тремя способами совмещать рёбра с сохранением ориентации. Поэтому собственная группа додекаэдра состоит из $20 \cdot 3 = 60$ движений. А именно:

1. тождественное преобразование;
2. $6 \cdot 4 = 24$ поворота на углы $\frac{2\pi}{n}$, $n = 1, 2, 3, 4$, вокруг осей, проходящих через середины противоположных граней;
3. 15 поворотов на 180° вокруг осей, проходящих через середины противоположных рёбер.

Полная же группа додекаэдра состоит из $20 \cdot 6 = 120$ движений. Помимо перечисленных, туда входят их композиции с центральной симметрией относительно центра додекаэдра.

Упражнение 5. Проверьте, что полные и собственные группа куба, октаэдра и икосаэдра, соответственно состоят из 48 и 24, 48 и 24, и 120 и 60 движений.

4 Действие группы на множестве

Определение 4.1 (Гомоморфизм групп). Отображение $\varphi: G_1 \rightarrow G_2$ называется *гомоморфизмом*, если переводит композицию в композицию, иначе говоря для любых $a, b \in G_1$ в группе G_2 выполняется соотношение $\varphi(ab) = \varphi(a)\varphi(b)$.

Эпиморфизмом называют сюръективный гомоморфизм, *мономорфизмом* называют инъективный гомоморфизм, а *изоморфизмом*, на самом деле, называют биективный гомоморфизм.

Упражнение 1. Докажите, что композиция двух гомоморфизмов — тоже гомоморфизм.

Определение 4.2 (Образ гомоморфизма). Множество всех значений гомоморфизма $\varphi: G_1 \rightarrow G_2$ называется его *образом* и обозначается $\text{im } \varphi$ или

$$\varphi(G_1) = \{\varphi(g_1) \mid g_1 \in G_1\}.$$

Определение 4.3 (Слой отображения). Подмножество $f^{-1}(y) \subset X$ называется *слоем отображения* $f: X \rightarrow Y$ над точкой $y \in Y$.

Пример 1. Отображение $\varphi: (\mathbb{Z}, +) \rightarrow (\mathbb{Z}/(n), +), a \mapsto a \pmod{n}$ является гомоморфизмом групп. Проверка, что это гомоморфизм ($\varphi(a+b) = \varphi(a) + \varphi(b)$)¹, т.е. $(a \pmod{n}) + (b \pmod{n}) = (a+b \pmod{n})$. Но это и является основным правилом сложения в циклической группе.

Образом гомоморфизма является вся группа $\mathbb{Z}/(n)$, это так, просто потому что

$$\begin{aligned} 0 &\mapsto 0, \\ 1 &\mapsto 1, \\ &\vdots \\ n-1 &\mapsto n-1. \end{aligned}$$

Слои отображения φ выглядят так:

$$k + (n) \stackrel{\text{def}}{=} \{k + nz \mid z \in \mathbb{Z}\}, \quad k = 1, 2, \dots, n-1.$$

Пример 2. Отображение $f: S_n \rightarrow (\pm 1, \cdot), \sigma \mapsto \text{sign}(\sigma)$ является гомоморфизмом, где $\text{sign}(\sigma)$ равен 1, если перестановка четная и -1 , если нечетная. Для проверки, что это гомоморфизм, нужно проверить, что $\text{sign}(\sigma \circ \tau) = \text{sign}(\sigma) \cdot \text{sign}(\tau)$. Если σ осуществима за k транспозиций, а τ за m , то $\sigma \circ \tau$ за

¹Формально, здесь разные операции сложения...

$k + m$. А четности из соответственно $(-1)^k, (-1)^m, (-1)^{k+m}$. Образом опять является вся группа. А разбиение на слои такое: слой над точкой 1 — группа A_n , она так и определяется. А слой над точкой -1 — все нечетные перестановки, но они группу не образуют.

Гомоморфизм переводит единицу в единицу, а обратный в обратный. Докажем только первое. $\varphi(e_1)\varphi(e_1) = \varphi(e_1 e_1) = \varphi(e_1)$, домножая на единицу равенство получаем то, что надо. Отсюда следует, что образ гомоморфизма — подгруппа.

$$\text{im } \varphi \stackrel{\text{def}}{=} \varphi(G_1) \subset G_2.$$

Определение 4.4 (Ядро гомоморфизма). Полный прообраз единицы $e_2 \in G_2$ при гомоморфизме групп $\varphi: G_1 \rightarrow G_2$ называется *ядром* гомоморфизма φ , обозначается

$$\ker \varphi \stackrel{\text{def}}{=} \{g_1 \in G_1 \mid \varphi(g_1) = e_2\}.$$

Он является подгруппой в G_1 , ибо из равенства $\varphi(g) = e_2, \varphi(h) = e_2$ вытекает равенство $\varphi(gh) = e_2 e_2 = e_2$, а из равенства $\varphi(g) = e_2$ равенство $\varphi(g^{-1}) = \varphi(g)^{-1} = e_2^{-1} = e_2$.

Следующую теорему в этом курсе мы не докажем, но она является мощнейшим инструментом в алгебре.

Теорема 4.5 (Первая теорема об изоморфизме). Для гомоморфизма конечных групп $\varphi: G_1 \rightarrow G_2$ верен изоморфизм групп:

$$\text{im } \varphi \cong G / \ker \varphi^1$$

В частности: $|\text{im } \varphi| = |G| : |\ker \varphi|$.

Напомню, что $\text{Aut}(X)$, где X — множество, называется множество взаимнооднозначных отображений X в себя, т.е. его перестановки.

Определение 4.6 (Действие группы на множестве). Гомоморфизм $\varphi: G \rightarrow \text{Aut}(X)$ называется *действием* группы G на множестве X или *представлением* группа G автоморфизмами множества X .

Отображение $\varphi(g): X \rightarrow X$, отвечающее элементу g при действии φ удобно будет обозначать $\varphi_g: X \rightarrow X$. Тот факт, что $g \mapsto \varphi_g$ является гомоморфизмом групп означает, что $\varphi_{ab} = \varphi_a \circ \varphi_b$. Если хочется указать, что группа действует на множестве, то пишут $G: X$.

¹Мы и не определили, что такое факторизация по ядру гомоморфизма, и почему так можно делать..

Мы по-сути и определяли группу D_n как группу автоморфизмов диэдра, она же и действует на множестве вершин его.

Упражнение 2. Посмотрите, как группа D_n действует на сторонах диэдра.

Можно классифицировать действия по разному, приведу в пример классическую. Действие называется *транзитивным*, если любую точку множества X можно перевести в любую другую элементов из G . Действие называется *свободным*, если каждое преобразование из G действует на X без неподвижных точек, т.е. $gx = x$ возможно лишь если $g = e$. Действие называется *точным* или *эффективным*, если любое нетождественное преобразование из G действует не тождественно, т.е. двигает что-то куда-то.

Разберём конкретные примеры действий группы, в первую очередь на себе.

Пример 3 (Регулярное действие). Пусть X — множество элементов группы G . Тогда *левым регулярным действиям* называется гомоморфизм $\lambda_g : x \mapsto gx$, для выбранного элемента $g \in G$. Это действительно гомоморфизм групп:

$$\lambda_{ab}(x) = abx = \lambda_a(bx) = \lambda_a \lambda_b(x).$$

Так как равенство $gx = x$ в группе выполняется только при $g = e$, то такое действие свободно и в частности, эффективно.

Правым регулярным действием называется гомоморфизм $\rho_g : x \mapsto xg^{-1}$ правого умножения на обратный.¹

Упражнение 3. Убедитесь, что ρ_g свободное действие.

Тем самым, любая абстрактная группа G может быть реализована как группа преобразований некоторого множества. Например, левые регулярные представления числовых групп реализуют аддитивную группу \mathbb{R} группой сдвигов $\lambda_v : x \mapsto x + v$ числовой прямой, а мультипликативную группу \mathbb{R}^\times — группой гомотетий $\lambda_c : x \mapsto cx$ проколотой прямой $\mathbb{R}^t \text{imes} = \mathbb{R} \setminus \{0\}$.

Пример 4 (Присоединённое действие). Отображение $Ad : G \rightarrow \text{Aut}(G)$, сопоставляющее элементу $g \in G$ автоморфизм сопряжения этим элементом

$$Ad_g : G \rightarrow G, \quad h \mapsto ghg^{-1},$$

называется *присоединённым действием* G на себе.

Образ присоединённого действия $\text{im } Ad$ называется группой *внутренних* автоморфизмов группы G и обозначается $\text{Int}(G)$. Автоморфизмы, которые не лежат в $\text{Int}(G)$, называются, логично, *внешними* автоморфизмами

¹Тут g^{-1} , конечно, не с проста. Проверьте, что если бы было просто g , то преобразование было бы антигомоморфизмом.

группы G . В отличие от левого и правого регулярных действий присоединённое действие, вообще говоря, не свободно и не точно. Заметим также, что если выполняется равенство $h = ghg^{-1}$, то выполняется и равенство $gh = hg$. Подгруппа элементов, которая удовлетворяет такому равенству называется *центром* группы и обозначается

$$Z(G) = \{g \in G \mid \forall h \in G \ gh = hg\}.$$

Упражнение 4. Убедитесь, что Ad_g является гомоморфизмом, а также и Ad .

4.1 Орбита и стабилизатор

Со всякой группой преобразований G множества X связано отношение $x \sim y$ на X , означающее, что $y = gx$ для некоторого преобразование $g \in G$. Проверим некоторые важные свойства этого отношения:

- (i) *рефлексивность*: $x = ex \Rightarrow x \sim x$;
- (ii) *симметричность*: $y = gx \Rightarrow x = g^{-1}y$;
- (iii) *транзитивность*: $y = gx, \quad z = hy \Rightarrow z = ghy$.

Такие отношения называются отношениями *эквивалентности*, действительно, логично считать, что точки которые, совмещаются преобразованием из G в каком-то смысле эквиваленты. *Классом эквивалентности* точки X называются все точки, которые ей эквиваленты.

Определение 4.7 (Орбита). Классом эквивалентности отношения $x \sim y \Leftrightarrow gx = y$ называется *орбитой* точки x под действием G и обозначается

$$Gx = \{gx \mid g \in G\}.$$

Множеством всех орбит называется *фактором* множества X под действием G и обозначается X/G .

Пример 5. Циклическая группа порядка 3 действует на рёбрах правильного треугольника $\mathbb{Z}/(3) : \{a, b, c\}$. $\mathbb{Z}/(3) = \{e, r, -r\}$, тогда

- $ea = a, eb = b, ec = c$;
- $ra = b, rb = c, rc = a$;
- $-ra = c, -rb = a, -rc = b$.

Орбита $\mathbb{Z}/(3)a = \{a, b, c\}$, аналогично и $\mathbb{Z}/(3)b = \mathbb{Z}/(3)c = \mathbb{Z}/(3)a$. Фактором $\frac{\{a,b,c\}}{\mathbb{Z}/(3)}$ является само $\{a, b, c\}$.

$$(\forall x \in X)(\exists! y \in Y) \quad x = y.$$

Утверждение 4.8. *Множество X распадается в объединение орбит, в том смысле, что две орбиты либо полностью совпадают, либо вообще не пересекаются.*

Доказательство. В самом деле, возьмём две орбиты Gx и Gy , а также z , который принадлежит и первой и второй орбите:

$$g_1x = z, \quad g_2y = z.$$

В таком случае, устанавливаем, что

$$g_1x = g_2y \Rightarrow x = g_1^{-1}g_2y \Rightarrow y \in G_x.$$

Тем самым $G_y \subset G_x$, аналогично $G_x \subset G_y$. □

С каждой точкой $x \in X$ и его орбитой Gx связано сюръективное отображение $\text{ev}_x: G \rightarrow Gx$, $g \mapsto gx$, слой которого над точкой $y \in Gx$ состоит из всех преобразований группы G , переводящих x в y .

Определение 4.9 (Транспортёр). Слой отображения $\text{ev}_x: G \rightarrow Gx$ над точкой y называется *транспортёром* x в y и обозначается

$$G_{xy} = \{g \in G \mid gx = y\}.$$

Определение 4.10 (Стабилизатор). Слоем отображения $\text{ev}_x: G \rightarrow Gx$ над самой точкой x называется *стабилизатором* точки $x \in X$ и обозначается

$$\text{Stab}(x) = \{g \in G \mid gx = x\} = G_{xx}.$$

Пример 6. Пусть $X = \{1, 2, 3, 4\}$ — множество верши квадрата. Тогда $D_4: X$. Найдём стабилизатор элемента 1:

- $e(1) = 1$;
- $r(1) = 2$;
- $r^2(1) = 3$;
- $r^3(1) = 4$;
- $s_v(1) = 2$;

- $s_h(1) = 4$;
- $s_d(1) = 1$ (диагональ через 1 и 3);
- $s_{\bar{d}}(1) = 3$ (диагональ через 2 и 4).

Таким образом, $\text{Stab}(1) = \{e, s_d\}$. Найдем также транспортер $D_{4_{12}}$ по прошлой записи, т.е. это $\{r, s_v\}$.

Лемма 4.11. *Для любых x, y, z из одной орбиты имеются взаимнообратные биекции:*

$$\begin{array}{ccc} & s \mapsto hsg^{-1} & \\ \text{Stab}(x) & \xrightarrow{\quad} & G_{yz} \\ & f \mapsto h^{-1}fg & \end{array}$$

Доказательство. Если $y = gx$ и $z = hx$, то

$$sg^{-1}y = \underbrace{sx}_x = h^{-1}z \Rightarrow hsg^{-1} \in G_{yz},$$

для всех $s \in \text{Stab}(x)$. Наоборот, если $fy = z$, то

$$(h^{-1}fg)x = (h^{-1}f)y = h^{-1}z = x \Rightarrow h^{-1}fg \in \text{Stab}(x).$$

□

Утверждение 4.12. *Стабилизаторы всех точек из одной орбиты равномощны и сопряжены:*

$$y = gx \Rightarrow \text{Stab}(y) = g \text{Stab}(x) g^{-1} = \{ghg^{-1} \mid h \in \text{Stab}(y)\}.$$

Доказательство. По теореме 4.11, если $z = y$, а $h = g$, следует это утверждение. □

4.1.1 Связь между орбитой и стабилизатором

Утверждение 4.13 (Формула для длины орбиты). *Длина орбиты произвольной точки $x \in X$ при действии на неё конечной группы преобразований G равна*

$$|Gx| = \frac{|G|}{|\text{Stab}(x)|}.$$

В частности, длины всех орбит и порядки стабилизаторов всех точек являются делителем порядка группы.

Доказательство. Группа G является объединением непересекающихся множеств G_{yx} по всем $y \in Gx$. Тогда по теореме 4.11 все эти множества состоят из $|\text{Stab}(x)|$ элементов. Получаем, что $|Gx| \cdot |\text{Stab}(x)| = |G|$. \square

Пример 7 (Действие перестановок букв на словах). Зафиксируем алфавит из k букв $\mathcal{A} = \{a_1, a_2, \dots, a_k\}$. И рассмотрим множество X , которое состоит из всех n буквенных слов w . Также о каждом слове можно думать как о отображении $w: \{1, 2, \dots, n\} \rightarrow \mathcal{A}$, где каждому номеру приписывается буква из алфавита \mathcal{A} . Сопоставим каждой перестановке $\sigma \in S_n$ преобразование $w \mapsto w\sigma^{-1}$, которое переставляет буквы в словах, как предписывает σ ¹. Таким образом, мы получили действие симметрической группы S_n на множестве слов X . Орбита слова $w \in X$ под действием этой группы состоит из всех слов, где каждая буква алфавита встречается столько же раз, сколько в слове w . Стабилизатор $\text{Stab}(w)$ слова w , в котором буква a_i встречается m_i раз (для каждого $i = 1, \dots, k$), состоит из перестановок между собою одинаковых букв и имеет порядок $|\text{Stab}(w)| = m_1!m_2! \dots m_k!$. Тем самым, длина орбиты такого слова равна *мультиномиальному коэффициенту*

$$|S_n w| = \frac{|S_n|}{|\text{Stab}(w)|} = \frac{n!}{m_1!m_2! \dots m_k!} = \binom{n}{m_1, \dots, m_k}.$$

Этот пример показывает, что длины орбит и порядки стабилизаторов разных точек могут быть разными.

4.2 Подсчёт орбит

Подсчёт числа элементов в факторе X/G (числа орбит) конечного множества X под действием конечной группы G наталкивается на очевидную трудность: поскольку длины орбит бывают разными, количество орбит „разных типов“ придётся считать по отдельности, по ходу дела уточняя, что такое „тип орбиты“. С этим нам поможет следующее утверждение.

Теорема 4.14 (Формула Пойа-Бернсайда). *Пусть конечная группа G действует на конечном множестве X . Для каждого $g \in G$ обозначим, через $X^g = \{x \in X \mid gx = x\} = \{x \in X \mid g \in \text{Stab}(x)\}$ множество неподвижных точек преобразования g . Тогда верная следующая формула*

$$|X/G| = \frac{1}{|G|} \cdot \sum_{g \in G} |X^g|.$$

¹То есть слово $a_{\lambda_1} \dots a_{\lambda_n}$ переходит в слово $a_{\lambda_{\sigma^{-1}(1)}} \dots a_{\lambda_{\sigma^{-1}(n)}}$, на i -м месте стоит та буква, номер которой в исходном слове w переводится перестановкой σ в номер i .

Доказательство. Обозначим через $F \subset G \times X$ таких пар, что $gx = x$. Такое множество можно описать двумя способами:

$$F = \bigsqcup_{g \in G} X^g = \bigsqcup_{x \in X} \text{Stab}(x).$$

Первое получается рассмотрением проекции $F \rightarrow G, (g, x) \mapsto g$: слой над точкой g и есть X^g . Второе получается проекцией $F \rightarrow X, (g, x) \mapsto x$: слой над точкой x суть $\text{Stab}(x)$. Согласно первому описанию $|F| = \sum_{g \in G} |X^g|$, а по второму $|F| = \sum_{x \in X} |\text{Stab}(x)| = |G| \cdot |X/G|$. \square

Пример 8 (Ожерелья). Задача „ожерелья“ является одной из классических задач теории групп, действия группы на множестве. На её примере рассмотрим применение формулы *Пойа-Бернсайда*. Эта проблема формулируется обычно как-то так: «У одного очень хитрого мужчины, мистера А. Л. Г., есть неограниченный запас бусинок из n цветов. Он хочет подарить как можно большему числу дам подарки-ожерелья из 6 бусин. Дамы заподозрят обман, если поймут мужчину на одинаковых ожерельях. Скольким дамам сможет сделать подарок мистер А. Л. Г.?»

Ответом на данный вопрос, конечно же, является количество орбит группы диэдра D_6 на множестве всех раскрасок вершин правильного шестиугольника в n цветов. А вы как думали?!

Группа диэдра D_6 состоит из 12 элементов:

- тождественного преобразования e ;
- двух поворотов $r^{\pm 1}$ на $\pm 60^\circ$;
- двух поворотов $r^{\pm 2}$ на $\pm 120^\circ$;
- центральной симметрии r^3 ;
- трёх отражений s_{14}, s_{25}, s_{36} относительно больших диагоналей;
- и трёх отражений $\overline{s}_{14}, \overline{s}_{25}, \overline{s}_{36}$ относительно серединных перпендикуляров к сторонам.

Единица оставляет на месте все n^6 раскрасок. Раскраски, симметричные относительно других преобразований, показанных на рисунке. Взяв на этих рисунках все допустимые сочетания цветов, получаем, соответственно, n, n^2, n^3, n^4 и n^3 раскрасок. Тогда по теореме 4.14 число 6-бусинок равно

$$\frac{n^6 + 3n^4 + 4n^3 + 2n^2 + 2n}{12}.$$

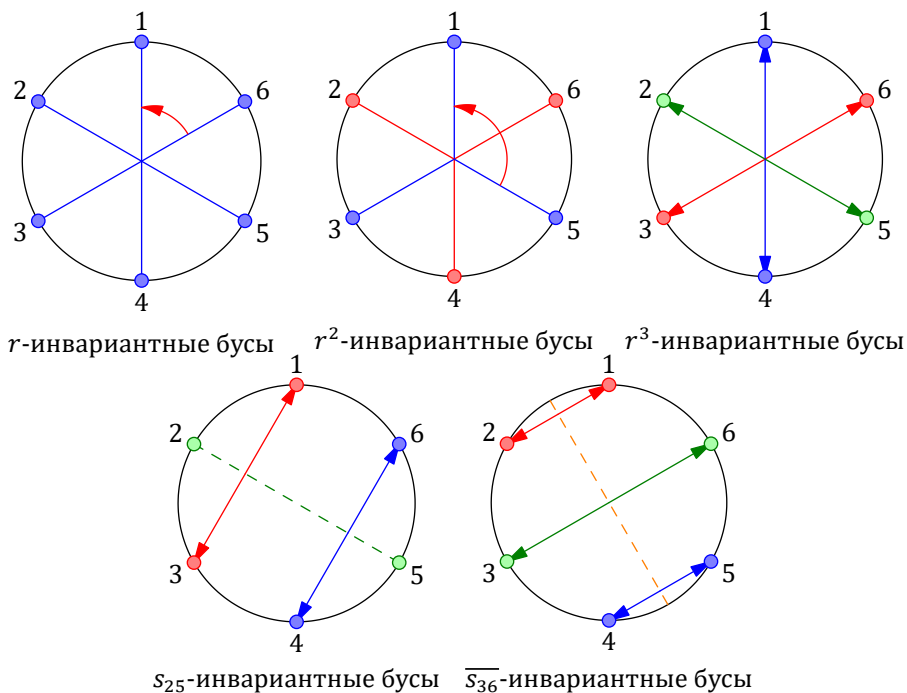


Рис. 8: Симметричные ожерелья из 6 бусин.

Задачи

0 Отображения и множества

1. Перечислите все отображения $\{0, 1, 2\} \rightarrow \{0, 1\}$ и $\{0, 1\} \rightarrow \{0, 1, 2\}$. Сколько среди них сюръекций и инъекций?

1 Перестановки

1. Возьмите какое-нибудь четырёхбуквенное слово, скажем, прошлое слово УШКА. Покажите, что все варианты (А сколько, кстати, их?) тоже разбиваются на две группы, и обмен двух букв местами переводит нас из одной группы в другую.
2. Вова сказал своей подруге, что подарит ей доширак, если она в слове КОМАНДА сделает семь попарных обменов и получит исходное слово.

В чём просчитался Вова?

3. Найти цикловой тип, порядок и четность перестановки

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 \\ 5 & 9 & 1 & 3 & 2 & 11 & 10 & 8 & 4 & 7 & 6 \end{pmatrix}.$$

4. Найдите все перестановки трехэлементного множества.
5. Сколько существует перестановок слова РЫБА, состоящих ровно из двух циклов? Найдите эти слова.
6. Докажите, что любая перестановка имеет обратную.
7. Найдите обратную перестановку для:

$$(a) \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \quad (b) \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 1 & 4 & 5 & 3 \end{pmatrix}.$$

8. Верно ли, что композиция двух циклов длины 2 является перестановкой порядка 1 или 2?
9. Пусть дана перестановка в виде композиции циклов

$$\sigma = |1, 4, 7|2, 5\rangle.$$

Напишите ее „матричный вид“, ее порядок и обратную ей.

10. Пусть даны две перестановки

$$\sigma = |1, 4, 2\rangle, \quad \tau = |1, 3|2, 5\rangle.$$

Найдите композиции $\tau \circ \sigma$ и $\sigma \circ \tau$, четность и порядок этих композиций. А также их „матричный вид“.

11. Пусть даны две перестановки

$$\sigma = |1, 8, 5, 2|3, 7\rangle, \quad \tau = |1, 4|2, 3, 6|5, 8\rangle.$$

Найдите композиции $\tau \circ \sigma$ и $\sigma \circ \tau$, четность и порядок этих композиций.

2 Группы

1. Сколько элементов в группе D_5 ? А сколько элементов порядка 2?
2. Докажите, что A_n — подгруппа группы S_n .
3. Верно ли, что подгруппа абелевой группы всегда абелева? Если да — объясните. Если нет — приведите контрпример.
4. В группе D_6 найдите композицию $r \circ s_1$, где r — поворот на 60° , а s_1 — отражение относительно вертикальной оси.
5. Напишите таблицу Кэли для группы S_3 . Какие из элементов коммутируют между собой?
6. Докажите, что в группе D_n выполняется равенство:

$$s \circ r = r^{-1} \circ s.$$

Где r — поворот на $360^\circ/n$, а s — отражение относительно любой оси.

7. Пусть $H = (\{-1, 1\}, \times)$ в (\mathbb{R}^*, \times) .¹ Является ли H подгруппой? Является ли H абелевой?
8. Изоморфны ли группы: (a) S_2 и $\mathbb{Z}/(2)$; (b) S_3 и $\mathbb{Z}/(3)$; (c) D_4 и S_4 ; (d) S_4 и D_{12} , и (f*) S_5 и D_{10} .
9. Найдите все подгруппы в: (a) $\mathbb{Z}/(6)$; (b) S_3 ; (c) D_4 ; (d) D_6 ; (e*) D_{12} , и (f*) A_4 . Для каждой подгруппы проверьте, что ее порядок делит порядок всей группы. Подумайте над тем, каким группам изоморфны каждая из них.
10. Летнешкольников заставили выложить плац правильной шестиугольной плиткой². Сколько существует симметрий такого замощения плиткой? Образуют ли они группу? Если да, то какой у нее порядок?
11. Пусть H — множество всех перестановок из S_3 , которые оставляют тройку на месте. Является ли H подгруппой группы S_3 ? Если да, то какой у нее порядок и является ли она абелевой?
12. Является ли множество $G = \{2^n \mid n \in \mathbb{Z}\}$ с операцией умножения группой? Если да, то является ли она абелевой? Какие в ней подгруппы?

¹Здесь “звёздочка” обозначает то, что нет нуля.

²Причем плитка самая обычная, на ней даже узоров никаких нет.

13. Придумайте свой объект, например, букву “Ж”. Опишите его группу симметрий. Подумайте, какой группе она изоморфна.
14. Пусть H подгруппа группы G . Тогда *левым смежным классом* называется $gH = \{gh \mid h \in H\}$.
 - (а) Докажите, что два смежных класса либо совпадают, либо не пересекаются.
 - (б)* Докажите, что все смежные классы находятся в биекции друг с другом.
 - (с) В каком соотношении находится порядок группы H , число смежных классов и порядок группы G ?
 - (д) Почему в группе порядка 15 не может быть подгруппы порядка 4?

3 Группы фигур

1. Группа D_4 действует на множестве вершин квадрата $\{1, 2, 3, 4\}$.
 - (а) Сколько орбит у этого действия?
 - (б) Найдите стабилизатор вершины 1. Какой группе он изоморфен?
 - (с) Проверьте, что $|D_4| = |\text{Stab}(1)| \cdot |\text{Orb}(1)|$.
2. Группа S_3 действует на многочлене $P(x_1, x_2, x_3) = x_1^2 + x_2x_3$, переставляя переменные. Найдите орбиты этого действия. Какой стабилизатор у P ?
3. Группа $G = \mathbb{Z}/(4)$ действует на множестве $X = \{1, 2, 3, 4\}$ циклическими сдвигами. Запишите соответствующий гомоморфизм $\varphi: G \rightarrow S_4$. Чему равно $\ker \varphi$?
4. Группа $\mathbb{Z}/(6)$ действует на множестве $X = \{A, B, C\}$ по правилу

$$k \cdot A = A, \quad k \cdot B = C, \quad k \cdot C = B, \quad \forall k \in \mathbb{Z}/(6).$$

Найдите орбиты и стабилизаторы элементов X .

4 Действие группы

5 Формула Пойа-Бернсайда: ожерелья, орнаменты

Контрольная работа