

### **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. Погуляем в полях, примерим кольца.

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 и хочет разобраться в том, что они значат.

# Содержание

<b>1</b>	<b>Перестановки</b>	<b>1</b>
1.1	Нотация перестановок	2
1.2	Запись перестановки в виде циклов	3
	Задачи	5
<b>2</b>	<b>Введение в группы</b>	<b>6</b>
2.1	Определение группы	6
2.1.1	Абелевы группы	8
2.2	Подгруппы	9
2.2.1	Циклические группы	9
	Задачи	10
<b>3</b>	<b>Левые и правые смежные классы</b>	<b>12</b>
3.1	Левый смежный класс	12
3.2	Правый смежный класс	12
3.3	Индекс подгруппы	12
3.3.1	Теорема Лагранжа	12
	Задачи	12
<b>4</b>	<b>Гомоморфизм групп</b>	<b>12</b>
4.1	Ядро и образ гомоморфизма	12
4.2	Изоморфизм групп	12
4.3	Теорема о гомоморфизме	12
	Задачи	12
<b>5</b>	<b>Действие группы на множестве</b>	<b>12</b>
5.1	Орбита и стабилизатор	12
5.1.1	Связь между орбитой и стабилизатором	12
	Задачи	12
<b>6</b>	<b>Сопряжение. Классы сопряжённых элементов</b>	<b>12</b>
6.1	Сопряжение элементов	12
6.2	Классы сопряжённых элементов	12
6.3	Центр группы	12
	Задачи	12

<b>7</b>	<b>Подсчёт орбит</b>	<b>12</b>
7.1	Лемма Бернсайда . . . . .	12
7.2	Теорема Пойа . . . . .	12
	Задачи . . . . .	12
<b>8</b>	<b>Кольца</b>	<b>12</b>
8.1	Определение кольца . . . . .	12
8.2	Подкольца . . . . .	12
8.3	Кольца вычетов . . . . .	12
	Задачи . . . . .	12
<b>9</b>	<b>Кольцо многочленов</b>	<b>12</b>
9.1	Деление с остатком . . . . .	12
9.2	Неприводимые многочлены . . . . .	12
9.3	Теорема Безу . . . . .	12
9.4	Факториальность кольца . . . . .	12
	Задачи . . . . .	12
<b>10</b>	<b>Поля и расширения</b>	<b>12</b>
10.1	Определение поля . . . . .	12
10.2	Расширение поля . . . . .	12
10.3	Конечные поля . . . . .	12
	Задачи . . . . .	12

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.

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

## 1 Перестановки

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:

УШКА<sup>1</sup>

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 менять. Так что, за один шаг мы можем получить три слова.

ОДА      ДАО      АОД

---

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

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 группу 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.

## 1.1 Нотация перестановок

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

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

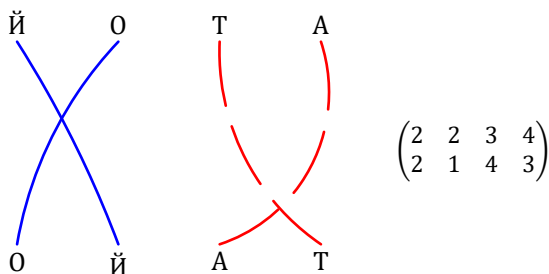
Перестановка  $\sigma$  может быть записана в виде<sup>1</sup>

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

*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  $\sigma$  сделает (на рисунке 1):

$$\sigma(\text{ЙОТА}) = \text{ЙОТА}.$$

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

Рис. 1: Перестановка  $\sigma$ .

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

*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:

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

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

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

## 1.2 Запись перестановки в виде циклов

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

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

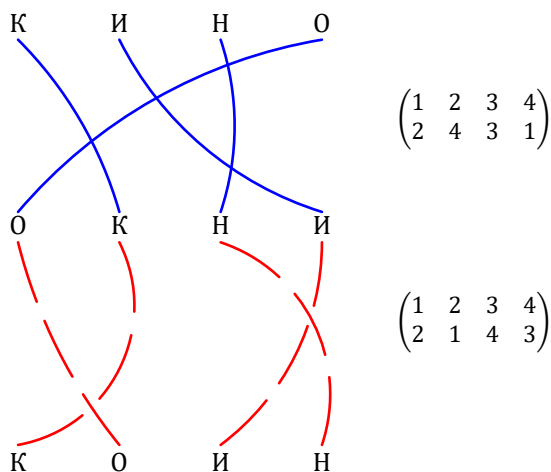
Записывается в виде:

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

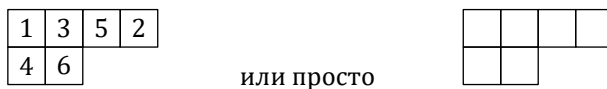
У такой записи есть “свобода выбора”. Один и тот же цикл можно записать по-разному. Например,

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

<sup>1</sup>Да! Именно так! Слева-направо!

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

Мы будем говорить, что у перестановки  $\sigma$  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  $\sigma$ .

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 “ниточки” нечётное число пересечений.

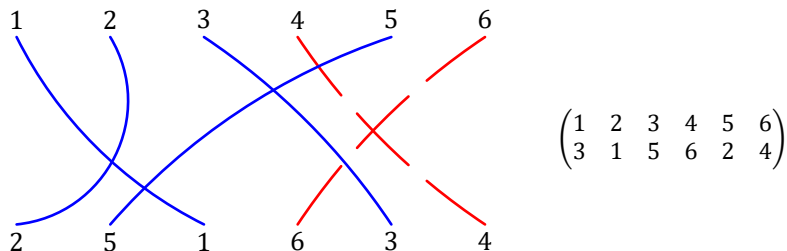


Рис. 4: Циклическая запись перестановки.

**Определение 1.6** (Порядок перестановки). Порядок перестановки  $\sigma$  – это наименьшее число  $n$ , такое что

$$\sigma^n = \text{id}.$$

**Теорема 1.7.** Порядок перестановки  $\sigma$  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  $k_1, k_2, \dots, k_m$ .  $\square$

## Задачи

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. Докажите, что любая перестановка имеет обратную.

6. Найдите обратную перестановку для:

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

7. Верно ли, что композиция двух циклов длины 2 является перестановкой порядка 1 или 2?

8. Пусть дана перестановка в виде композиции циклов

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

Напишите ее "матричный вид", ее порядок и обратную ей.

9. 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.

10. 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 Введение в группы

### 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.

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

*Пример 2.*  $(\mathbb{Z}/(5), +)$  множество остатков по модулю 5 с операцией сложения.

*Пример 3.*  $(\mathbb{R}, \cdot)$  множество действительных чисел с операцией умножения.

*Пример 4.* 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  $D_4$ <sup>1</sup>, она состоит из 8 элементов (на рисунке 5):

- |  |  |
|--|--|
| <ul style="list-style-type: none"> <li>• <math>e</math> – ничего не делать;</li> <li>• <math>r</math> – поворот на 90 градусов;</li> <li>• <math>r^2</math> – поворот на 180 градусов;</li> <li>• <math>r^3</math> – поворот на 270 градусов;</li> <li>• <math>s_1</math> – отражение относительно оси симметрии по оси <math>x</math>;</li> </ul> | <ul style="list-style-type: none"> <li>• <math>s_2</math> – отражение относительно оси симметрии по оси <math>y</math>;</li> <li>• <math>s_3</math> – отражение относительно диагонали, которая идет из левого верхнего угла в правый нижний;</li> <li>• <math>s_4</math> – отражение относительно диагонали, которая идет из правого верхнего угла в левый нижний.</li> </ul> |
|--|--|

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

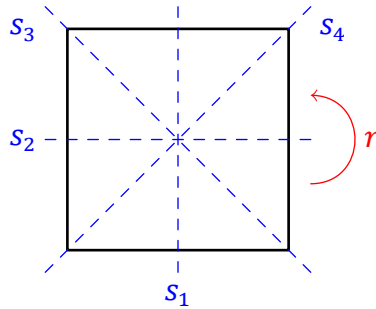


Рис. 5: Группа движений квадрата

*Пример 5.* 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.

**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.

### 2.1.1 Абелевы группы

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

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

<sup>1</sup>Часто операция опускается и подразумевается, что группа мультипликативна.

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

**Пример 6.** Пусть у нас есть группа  $G$ , которая содержит в себе, по крайней мере два элемента:  $a$  = “надеть носок” и  $b$  = “надеть ботинок”.<sup>1</sup> 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:

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

**Пример 8.** Множество поворотов квадрата образует подгруппу группы  $D_4$ .

**Пример 9.** Множество четных перестановок образует подгруппу группы  $S_n$ . И такая подгруппа обозначается  $A_n$ .

**Упражнение 6.** Придумайте свои примеры подгрупп.

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

### 2.2.1 Циклические группы

**Определение 2.6** (Циклическая группа). Группа  $G$  называется циклической, если существует элемент  $g \in G$ , такой что:

$$G = \{g^n \mid n \in \mathbb{Z}\}.$$

<sup>1</sup>Такая группа устроена довольно сложно и в нашем курсе рассматриваться не будет. Ее название  $F_2$ .

Элемент  $g$  называется генератором группы  $G$ . Если  $g$  – генератор группы  $G$ , то  $G$  обозначается как  $\langle g \rangle$ .

*Пример 10.* Группа  $(\mathbb{Z}, +)$  является циклической, так как  $G = \langle 1 \rangle$ .

*Пример 11.* Группа  $(\mathbb{Z}/(n), +)$  является циклической, так как  $G = \langle 1 \rangle$ .

**Теорема 2.7** (Циклическая группа). Пусть  $G$  – циклическая группа, тогда  $G$  является абелевой группой.

## Задачи

1. Докажите, что  $A_n$  – подгруппа группы  $S_n$ .
2. Верно ли что любая подгруппа абелевой группы является абелевой? Если да, то почему? Если нет, то приведите контрпример.
3. Докажите, что все элементы порядка 2 и единица в группе  $S_n$  образуют подгруппу.
4. Пусть  $H = (\{-1, 1\}, \cdot)$  в  $(\mathbb{R}^*, \cdot)$ .<sup>1</sup> Является ли  $H$  подгруппой? Является ли  $H$  абелевой группой?
5. Найдите все подгруппы группы  $S_3$ . Укажите их порядок. Какие из них абелевы?
6. Найдите все подгруппы группы  $\mathbb{Z}/(6)$ . Укажите их порядок. Какие из них абелевы?
7. Летнешкольников заставили выложить плац правильной шестиугольной плиткой. Сколько существует симметрий такого замощения плиткой? Образуют ли они группу? Если да, то какой у нее порядок?
8. 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?
9. Множество  $G = \{2^n \mid n \in \mathbb{Z}\}$  с операцией умножения является ли группой? Если да, то является ли она абелевой? Какие в ней подгруппы?

---

<sup>1</sup>Здесь “звёздочка” обозначает то, что нет нуля.



## **3 Левые и правые смежные классы**

### **3.1 Левый смежный класс**

### **3.2 Правый смежный класс**

### **3.3 Индекс подгруппы**

#### **3.3.1 Теорема Лагранжа**

#### **Задачи**

## **4 Гомоморфизм групп**

### **4.1 Ядро и образ гомоморфизма**

### **4.2 Изоморфизм групп**

### **4.3 Теорема о гомоморфизме**

#### **Задачи**

## **5 Действие группы на множестве**

### **5.1 Орбита и стабилизатор**

#### **5.1.1 Связь между орбитой и стабилизатором**

#### **Задачи**

## **6 Сопряжение. Классы сопряжённых элементов**

### **6.1 Сопряжение элементов**

### **6.2 Классы сопряжённых элементов**

### **6.3 Центр группы**

#### **Задачи**

## **7 Подсчёт орбит**

### **7.1 Лемма Бернсайда**

### **7.2 Теорема Пойа**

#### **Задачи**