

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 (например, группа преобразований, гомоморфизм и поле) и хочет разобраться в том, что они значат.

Содержание

1	Перестановки	1
1.1	Нотация перестановок	2
1.1.1	Запись перестановки в виде циклов	3
1.2	Чётность и порядок	4
2	Введение в группы	5
2.1	Определение группы	5
2.1.1	Абелевы группы	7
2.2	Подгруппы	8
2.2.1	Циклические группы	8
3	Группы фигур	9
3.1	Группы диэдров D_n	9
3.2	Группа тетраэдра	9
3.3	Группа додекаэдра	9
4	Действие группы на множестве	9
4.1	Орбита и стабилизатор	9
4.1.1	Связь между орбитой и стабилизатором	9
4.2	Группы фигур	9
4.2.1	Собственная группа куба	9
4.2.2	Собственная группа додекаэдра	9
5	Подсчёт орбит	9
5.1	Лемма Бернсайда	9
5.2	Теорема Пойа	9
6	Кольцо многочленов	9
6.1	Определение кольца	9
6.1.1	Кольцо вычетов	9
6.2	Присоединение корней	9
7	Комплексные числа	9
7.1	Первообразные корни и круговые многочлены	9
7.2	Гауссовы числа	9
7.2.1	Пифагоровы тройки	9
7.2.2	Теорема Ферма-Эйлера-Гаусса	9

Задачи	10
i Перестановки	10
ii Группы	11
iii Орбита и стабилизатор. Собственные группы фигур	12
iv Лемма Бернсайда и теорема Пойа: ожерелья, орнаменты	13
v Многочлены	13
vi Комплексные числа	13
vii Гауссовы числа “в хвост и в гриву”	13
Контрольная работа	14

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:

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

ОДА ДАО АОД

¹Это 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 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.

1.1 Нотация перестановок

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

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

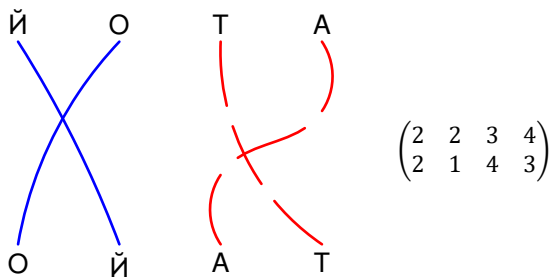
Перестановка σ может быть записана в виде¹

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

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):

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

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

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:

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

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 $\sigma \circ \tau$.

1.1.1 Запись перестановки в виде циклов

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

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

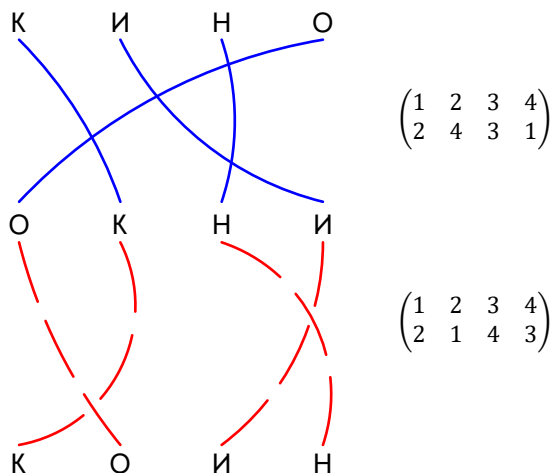
Записывается в виде:

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

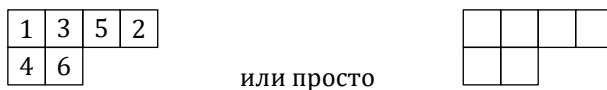
У такой записи есть “свобода выбора”. Один и тот же цикл можно записать по-разному. Например,

$$(1\ 3\ 5\ 2) = (3\ 5\ 2\ 1) = (5\ 2\ 1\ 3) = (2\ 1\ 3\ 5).$$

¹Да! Именно так! Слева-направо!

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

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 .

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 четной, если в ней четное число циклов четной длины.

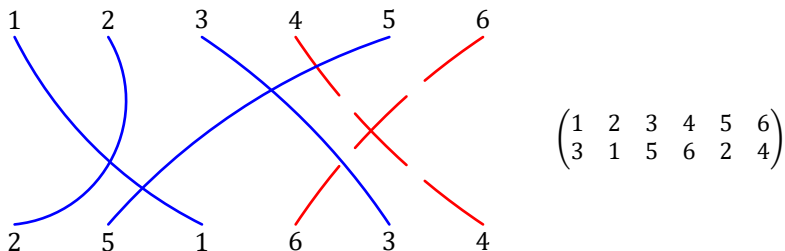


Рис. 4: Циклическая запись перестановки.

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

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:*

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

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. (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 ¹, она состоит из 8 элементов (на рисунке 5):

- | | |
|--|--|
| <ul style="list-style-type: none"> • e — ничего не делать; • r — поворот на 90 градусов; • r^2 — поворот на 180 градусов; • r^3 — поворот на 270 градусов; • s_1 — отражение относительно оси симметрии по оси x; | <ul style="list-style-type: none"> • 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. |
|--|--|

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.

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

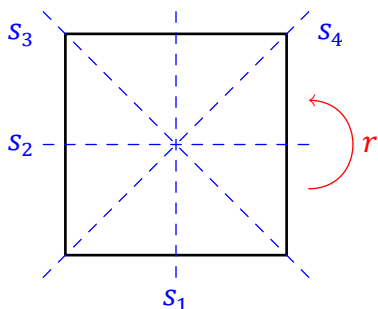


Рис. 5: Группа движений квадрата

Утверждение 2.2. Правый нейтральный элемент равен левому нейтральному элементу.

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

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

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

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

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

¹Часто операция опускается и подразумевается, что группа мультипликативна.

Пример 6. Пусть у нас есть группа G , которая содержит в себе, по крайней мере два элемента: $a = \text{“надеть носок”}$ и $b = \text{“надеть ботинок”}$.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:

- (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:

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

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

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

Лемма 2.7 (Циклическая группа). Пусть G — циклическая группа, тогда G является абелевой группой.

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

3 Группы фигур

3.1 Группы диэдров D_n

3.2 Группа тетраэдра

3.3 Группа додекаэдра

4 Действие группы на множестве

4.1 Орбита и стабилизатор

4.1.1 Связь между орбитой и стабилизатором

4.2 Группы фигур

4.2.1 Собственная группа куба

4.2.2 Собственная группа додекаэдра

5 Подсчёт орбит

5.1 Лемма Бернсайда

5.2 Теорема Пойа

6 Кольцо многочленов

6.1 Определение кольца

6.1.1 Кольцо вычетов

6.2 Присоединение корней

7 Комплексные числа

7.1 Первообразные корни и круговые многочлены

7.2 Гауссовы числа

7.2.1 Пифагоровы тройки

7.2.2 Теорема Ферма-Эйлера-Гаусса

Задачи

i 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

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

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

10. Пусть даны две перестановки

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

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

11. Пусть даны две перестановки

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

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

ii 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?

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

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

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?
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?

iii Орбита и стабилизатор. Собственные 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 .

iv Лемма Бернсайда и теорема Пойа: ожерелья, орнаменты

v Многочлены

vi Комплексные числа

vii Гауссовы числа “в хвост и в гриву”

Контрольная работа