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 будет 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

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[1]

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 поменять 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

[1] 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.

$$\text{ОДА} \to \text{ДОА ОАД АДО}$$
$$\text{ДАО} \to \text{ДОА ОАД АДО}$$
$$\text{АОД} \to \text{ДОА ОАД АДО}$$

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

$$\text{ДОА} \qquad \text{ОАД} \qquad \text{АДО}$$

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:

$$\text{АДО ОАД ДОА} \leftrightarrow \text{ДАО АОД ОДА}$$

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.

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

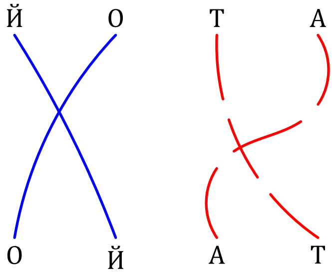
Перестановка σ может быть записана в виде[1]

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

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):

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

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



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

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 $\sigma \circ \tau$.

1.2 Запись перестановки в виде циклов

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

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

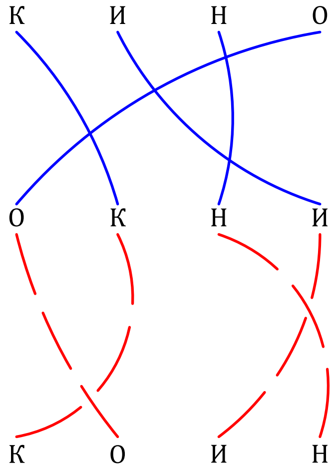
Записывается в виде:

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

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

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

[1] Да! Именно так! Слева-направо!



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

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

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.

1	3	5	2
4	6		

или просто

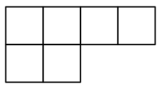


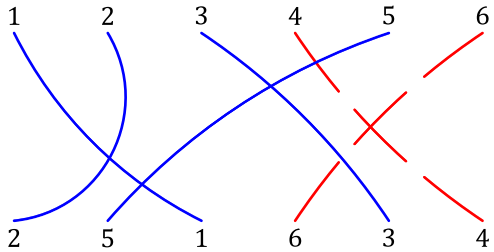
Рис. 3: Цикловой тип перестановки σ.

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.*



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

Рис. 4: Циклическая запись перестановки.

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

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

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 $k_1, k_2, \dots, k_m$. □

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. $(R, \cdot)$ 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):

- 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;
- 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.

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

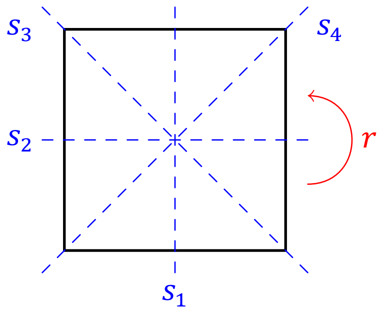


Рис. 5: Группа движений квадрата

Утверждение 2.2. *Правый нейтральный элемент равен левому нейтральному элементу.*

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

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

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

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.

[1]Часто операция опускается и подразумевается, что группа мультипликативна.

Пример 6. Пусть у нас есть группа G, которая содержит в себе, по крайней мере два элемента: $a =$ "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:

(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:

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

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

[2] Такая группа устроена довольно сложно и в нашем курсе рассматриватьсяне будет. Ее название F_2.

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.*

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

4 Гомоморфизм групп

4.1 Ядро и образ гомоморфизма

4.2 Изоморфизм групп

4.3 Теорема о гомоморфизме

5 Действие группы на множестве

5.1 Орбита и стабилизатор

5.1.1 Связь между орбитой и стабилизатором

6 Сопряжение. Классы сопряжённых элементов

6.1 Сопряжение элементов

6.2 Классы сопряжённых элементов

6.3 Нормальные подгруппы

6.4 Центр группы

7 Подсчёт орбит

7.1 Лемма Бернсайда

7.2 Теорема Пойа

8 Кольца

8.1 Определение кольца

8.2 Подкольца

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) $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}$; (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

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

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

10. Пусть даны две перестановки

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

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

11. Пусть даны две перестановки

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

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

ii Группы и теорема Лагранжа

1. Докажите, что A_n – подгруппа группы S_n.
2. Верно ли, что подгруппа абелевой группы всегда абелева? Если да — объясните. Если нет — приведите контрпример.
3. Докажите, что в группе порядка 15 не может быть подгруппы порядка 4.
4. Пусть порядок группы равен 12. Докажите, что порядок любой подгруппы делит 12. Может ли в этой группе существовать элемент порядка 7?
5. Докажите, что все элементы порядка 2 и единица в группе S_n образуют подгруппу.
6. Пусть $H = (\{-1, 1\}, \times)$ в $(\mathbb{R}^*, \times)$.[1] Является ли H подгруппой? Является ли H абелевой?
7. Найдите все подгруппы группы S_3. Укажите их порядок, проверьте, что их порядок делит порядок всей группы. Какие из подгрупп абелевы?
8. Найдите все подгруппы группы $\mathbb{Z}/(6)$. Укажите их порядок, проверьте, что их порядок делит порядок всей группы. Какие из подгрупп абелевы?
9. Летнешкольников заставили выложить плац правильной шестиугольной плиткой. Сколько существует симметрий такого замощения плиткой? Образуют ли они группу? Если да, то какой у нее порядок?
10. 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?

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

11. 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?

iii Гомоморфизмы и действие группы на множестве

1. Пусть $\varphi\colon \mathbb{Z} \to \mathbb{Z}/(6)$ гомоморфизм, который $n \mapsto n \pmod 6$. Является ли он изоморфизмом? Найдите $\ker\varphi$ и опишите, чем являются элементы $\operatorname{im}\varphi$?

2. Пусть $H = \{e, |12\rangle\}$ подгруппа S_3. Постройте гомоморфизм $\psi\colon S_3 \to H$, такой что четные перестановки он переводит в e. А нечетные в $|12\rangle$.
   (a) Проверьте, что гомоморфизм ψ сохраняет композицию.
   (b) Найдите $\ker\psi$.
   (c) Проверьте, что $S_3/\ker\psi \cong H$.

3. Группа D_4 действует на множестве вершин квадрата $\{1, 2, 3, 4\}$.
   (a) Сколько орбит у этого действия?
   (b) Найдите стабилизатор вершины 1. Какой группе он изоморфен?
   (c) Проверьте, что $|D_4| = |\operatorname{Stab}(1)| \cdot |\operatorname{Orb}(1)|$.

4. 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?

5. Пусть задан гомоморфизм $\mu\colon \mathbb{Z}/(12) \to \mathbb{Z}/(12)$, который $z \mapsto 3z$.
   (a) Найдите $\ker\mu$.
   (b) Постройте таблицу Кэли для $\operatorname{im}\mu$.
   (c) Изоморфна ли $\operatorname{im}\mu$ какой-то известной группе?

6. Группа $G = \mathbb{Z}/(4)$ действует на множестве $X = \{1, 2, 3, 4\}$ циклическими сдвигами. Запишите соответствующий гомоморфизм $\varphi\colon G \to S_4$. Чему равно $\ker\varphi$?

7. Группа $\mathbb{Z}/(6)$ действует на множестве $X = \{A, B, C\}$ по правилу

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

   Найдите орбиты и стабилизаторы элементов X.

8. Пусть задан гомоморфизм групп $\varphi\colon G \to M$. Докажите, что для любого элемента $h \in \ker\varphi$ и произвольного $g \in G$ выполняется $ghg^{-1} \in \ker\varphi$.[1]

9. Постройте группу A_n с помощью какого-то эндоморфизма[1] S_n

iv Лемма Бернсайда и теорема Пойа: ожерелья, орнаменты

v Кольца и многочлены

vi Поля. Конечные поля. Факторкольца. Расширение полей

[1]Этим доказательством вы покажете, что ядра гомоморфизмов являются *нормальными* подгруппами.

[1]Эндоморфизм – гомоморфизм в себя, т.е. $\psi\colon G \to G$.