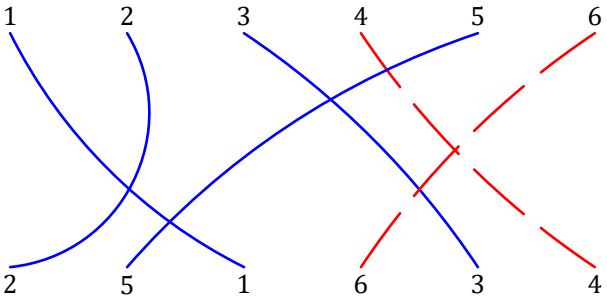
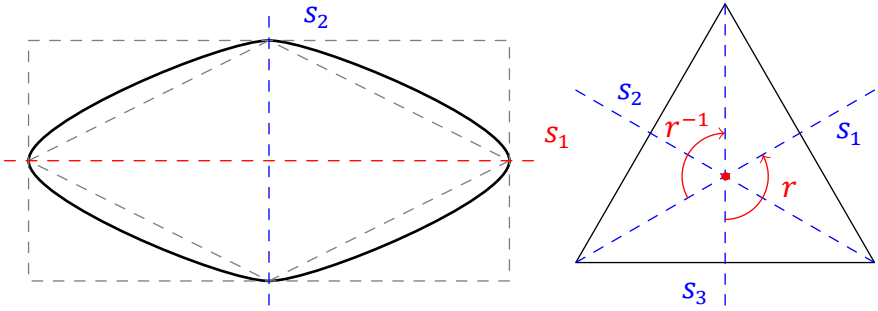
Алгебра-0,5

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 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.

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.

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

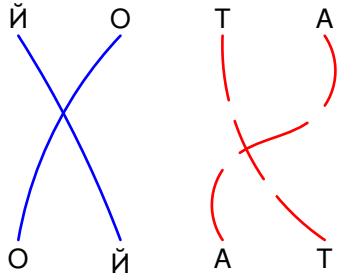
Перестановка σ может быть записана в виде[1]

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

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 $\sigma \circ \tau$.

1.1.1 Запись перестановки в виде циклов

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

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

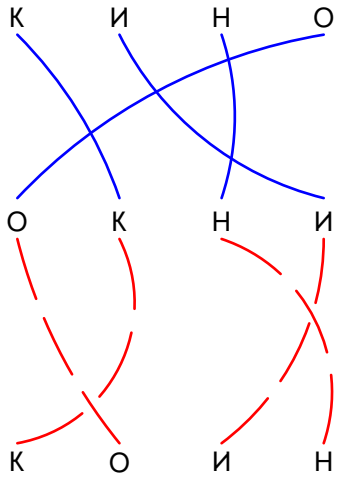
Записывается в виде:

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

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

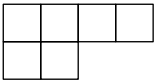


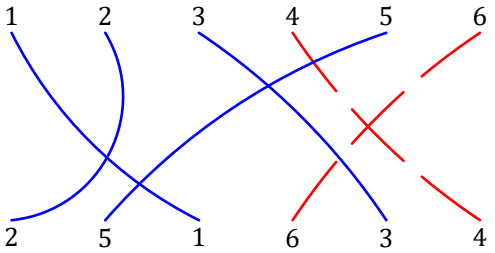
Рис. 3: Цикловой тип перестановки σ.

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.*



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

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

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 $k_1, k_2, \ldots, k_m$. □

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 (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*.

[1] Также такую группу можно было назвать Isom(□).

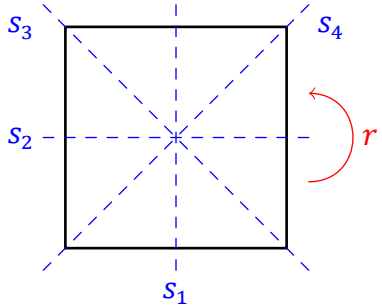


Рис. 5: Группа движений квадрата

Пример 6 (Группа автоморфизмов множества). Все взаимно однозначные отображения множества X в себя (перестановки его элементов) образуют группу. Она обозначается $\mathrm{Aut}\, X$ и называется *группой автоморфизмов* множества X. Если группа X конечна, то $\mathrm{Aut}\, X \cong S_{|X|}$.

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:

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

[1] 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 7. Пусть у нас есть группа G, которая содержит в себе, по крайней мере два элемента: $a =$ „надеть носок“ и $b =$ „надеть ботинок“.[1] 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 8. Четные целые числа с операцией сложения образуют подгруппу группы $(\mathbb{Z}, +)$.

Пример 9. Множество поворотов квадрата образует подгруппу группы D_4.

Пример 10 (Знакопеременная группа). Множество четных перестановок образует подгруппу группы S_n. И такая подгруппа обозначается A_n, а называется *знакопеременной.*

Пример 11 (Группа преобразований). Классическим примером групп являются *группы преобразований*. Любая подгруппа $G \subset \operatorname{Aut} X$ (в примере 6) 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 $g \in \operatorname{Aut} X$, сохраняющую эту структуру, образуют подгруппу в группе $\operatorname{Aut} X$, которая обычно называется группой автоморфизмов этой структуры.

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

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.

Пример 12. Группа $(\mathbb{Z}, +)$ является циклической, так как $G = \langle 1 \rangle$.

Пример 13. Группа $(\mathbb{Z}/(n), +)$ является циклической, так как $G = \langle 1 \rangle$.

3 Группы фигур

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

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.

[1] Мы не будем рассматривать размерности больше 3.

[2] *Диэдр (диэдра)* — это правильный плоский многоугольник.

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.

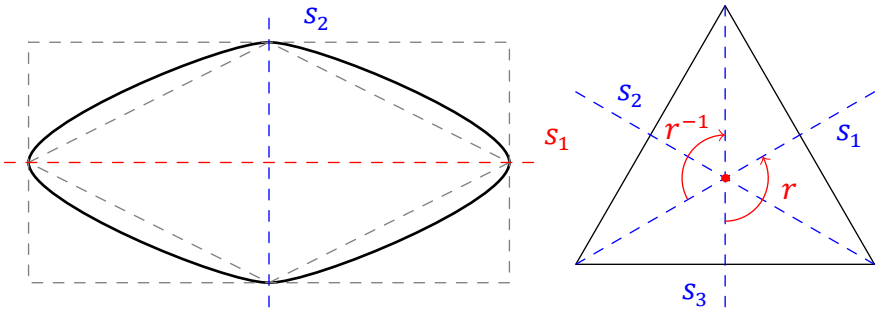


Рис. 6: Двуугольник D_2 и треугольник D_3.

Пример 2. Следующая диэдральная группа — группа треугольника D_3 (на рисунке 6). Она состоит из тождественного движения, двух поворотов r, r^{-1} на $\pm 120°$ 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 одозначно 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 этим 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 пораждает движение плоскости, что в частности является движением треугольника. □

Поскольку движение плоскости, сохращающее правильный n-угольник определяется своим действием на 3 точки (какой-нибудь вершиной, напрмер, и парой соседних сторон). Тогда группа диэдра при $n \geqslant 3$[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 n), а также n симметрий относительно прямых проходяший через пару середин противоположных сторон, в случае четноугольника, а в случае нечетноугольника — прямые проходящие через вершину, и середину противолежащей стороны.

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

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

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, сохранющее 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 содержется 6 отражений s_{ij} в плокостях, проходящих через серидну ребра ij и ребро kl. В

[1] На самом деле, даже при $n \geqslant 2$.

группе S_4 таким отражениям соотвествуют 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 вращение на 180°, представляющие собой одновременную тразсопозицию пары вершин, т.е. $s_{ij}s_{kl}$ перехоят 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 соотвествуют 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 лемой, 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 $\frac{2\pi}{n}$, $\quad n = 1, 2, 3, 4$, 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, соотвественно состоят из 48 и 24, 48 и 24, и 120 и 60 движений.

4 Действие группы на множестве

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

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 $\varphi : G_1 \to G_2$ называется его *образом* и обозначается $\operatorname{im}\varphi$ 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* $f : X \to Y$ над точкой $y \in Y$.

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

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

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

Слои отображения φ выглядят так:

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

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

[1] Формально, здесь разные операции сложения...

равенство получаем то, что надо. Отсюда следует, что образ гомоморфизма — подгруппа.

$$\operatorname{im}\varphi \overset{def}{=} \varphi(G_1) \subset G_2.$$

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

Определение 4.4 (Действие группы на множестве). Гомоморфизм $\varphi : G \to \mathrm{Aut}(X)$ называется *Действием* группы G на множестве X или *представлением* группа G автоморфизмами множества X.

Отображение $\varphi(g) : X \to X$, отвечающее элементу g при действии φ удобно будет обозначать $\varphi_g : X \to X$. 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 $G : X$.

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 *эффектиным*, 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 дейсвтиям* называется гомоморфизм $\lambda_g : x \mapsto gx$, для выбраного 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]

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

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 $\mathbb{R}^times = \mathbb{R} \setminus \{0\}$.

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

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

называется *присоединённым* действием G на себе.

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

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

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:* $x = ex \implies x \sim x$;

(ii) *симметричность:* $y = gx \implies x = g^{-1}y$;

(iii) *транзитивность:* $y = gx, \quad z = hy \implies z = ghy$.

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

Определение 4.5 (Орбита). Классом эквивалентности отношения $x \sim y \iff gx = y$ 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 правльного 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 4.6. *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:

$$g_1 x = z, \quad g_2 y = z.$$

В таком случае, устанавливаем, что

$$g_1 x = g_2 y \implies x = g_1^{-1} g_2 y \implies y \in G_x.$$

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 $\mathrm{ev}_x : G \twoheadrightarrow Gx,\ g \mapsto gx$, слой которого над точкой $y \in Gx$ состоит из всех преобразований группы G, переводящих x в y.

Определение 4.7 (Транспортёр). Слой отображения $\mathrm{ev}_x : G \twoheadrightarrow Gx$ над точкой y называется *трансортёром* x в y и обозначается

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

Определение 4.8 (Стабилизатор). Слоем отображения $\mathrm{ev}_x \colon G \twoheadrightarrow Gx$ над самой точкой x называется *стабилизатором* точки $x \in X$ и обозначается

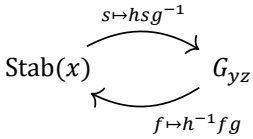
$$\mathrm{Stab}(x) = \{g \in G \mid gx = x\} = G_{xx}.$$

Пример 6. Пусть $X = \{1, 2, 3, 4\}$ — множество вершни квадрата. Тогда $D_4 \colon X$. 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);
- $s_{\overline{d}}(1) = 3$ (диагональ через 2 и 4).

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

Лемма 4.9. *Для любых x, y, z из одной орбиты имеются взаимнообратные биекции:*



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

$$sg^{-1}y = \underbrace{sx}_{x} = h^{-1}z \implies hsg^{-1} \in G_{yz},$$

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

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

□

Утверждение 4.10. *Стабилизаторы всех точек из одной орбиты равномощны и сопряжены:*

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

Доказательство. По теореме 4.9, если $z = y$, а $h = g$, следует это утверждение. □

4.1.1 Связь между орбитой и стабилизатором

Утверждение 4.11 (Формула для длины орбиты). *Длина орбиты произвольной точки $x \in X$ при действии на неё конечной группы преобразований G равна*

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

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 4.9 все эти множества состоят из $|\operatorname{Stab}(x)|$ элементов. Получаем, что $|Gx| \cdot |\operatorname{Stab}(x)| = |G|$. □

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 $w\colon \{1, 2, \dots, n\} \to \mathcal{A}$, 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 множетсве 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 $\operatorname{Stab}(w)$ 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 $|\operatorname{Stab}(w) = m_1!m_2! \dots m_k!$. Тем самым, длина орбиты такого слова равна *мультиномиальному коэффициенту*

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

[1] То 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.

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

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

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

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

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

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 поймают 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 правильно 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 $\pm 60°$;
- двух поворотов $r^{\pm 2}$ на $\pm 120°$;
- 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 Взяв на этих рисунках все допустимые сочетания цветов, получаем, соотвественно, n, n^2, n^3, n^4 и n^3 раскрасок. Тогда по теореме 4.12 число 6-бусинок равно

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

5 Кольцо многочленов

5.1 Определние кольца

5.1.1 Кольцо вычетов

5.2 Присоединение корней

6 Комплексные числа

6.1 Первообразные корни и круговые многочлены

6.2 Гауссовы числа

6.2.1 Пифогоровы тройки

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

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 $360°/n$, 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 плиткой[2]. Сколько существует симметрий такого замощения плиткой? Образуют ли они группу? Если да, то какой у нее порядок?

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

[2] Причем 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 $gH = \{gh \mid h \in H\}$.

    (a) Докажите, что два смежных класса либо совпадают, либо не пересекаются.

    (b)* Докажите, что все смежные классы находятся в биекции друг с другом.

    (c) В каком соотношении находится порядок группы H, число смежных классов и порядок группы G?

    (d) 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 $\{1, 2, 3, 4\}$.

    (a) Сколько орбит у этого действия?

    (b) Найдите стабилизатор вершины 1. Какой группе он изоморфен?

    (c) Проверьте, что $|D_4| = |\operatorname{Stab}(1)| \cdot |\operatorname{Orb}(1)|$.

2. Группа S_3 действует на многочлене $P(x_1, x_2, x_3) = x_1^2 + x_2 x_3$, 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 $\varphi\colon G \to S_4$. Чему равно $\ker \varphi$?

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

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

    Найдите орбиты и стабилизаторы элементов X.

Контрольная работа