

## Содержание

<b>1</b>	<b>Теоретические вопросы</b>	<b>1</b>
1.1	Определение группы. Пример группы . . . . .	1
1.2	Примеры групп по сложению . . . . .	2
1.3	Примеры групп по умножению . . . . .	2
1.4	Группа кватернионов . . . . .	2
1.5	Порядок элемента, порядок группы . . . . .	2
1.6	Группа подстановок. Теорема Кэли . . . . .	2
1.7	Определение циклической группы. Определение образующего элемента циклической группы . . . . .	2
1.8	Теорема Лагранжа. Следствия из теоремы Лагранжа . . . . .	3
1.9	Определение нормальной подгруппы. Определение фактор-группы . . . . .	3
1.10	Определение гомоморфизма групп . . . . .	4
1.11	Основная теорема о гомоморфизмах . . . . .	4
1.12	Определение кольца. Примеры колец . . . . .	4
1.13	Определение гомоморфизма колец . . . . .	4
1.14	Определение идеала. Определение главного идеала. . . . .	4
1.15	Построение факторкольца по идеалу $K/I$ . . . . .	5
1.16	Функция Эйлера. Теорема Эйлера . . . . .	5
1.17	Малая теорема Ферма . . . . .	5
1.18	Определение поля. Пример . . . . .	5
1.19	Простое поле. Пример . . . . .	5
1.20	Теорема о простом подполе . . . . .	5
1.21	Характеристика поля. Пример . . . . .	6
1.22	Алгебраические и трансцендентные элементы поля. . . . .	6
1.23	Определение простого элемента поля. Определение неприводимого многочлена над полем $P$ . . . . .	6
1.24	Построение конечного поля из $p^n$ элементов . . . . .	6
1.25	Мультипликативная группа конечного поля . . . . .	6
1.26	Пример конечного поля . . . . .	6
<b>2</b>	<b>Задачи</b>	<b>7</b>
2.1	1.4 . . . . .	7

## 1 Теоретические вопросы

### 1.1 Определение группы. Пример группы

Пусть  $M$  - некоторое множество

Бинарная операция на  $M$  - это отображение  $\circ : M \times M \rightarrow M, (a, b) \rightarrow a \circ b$

Если на  $M$  задана бинарная операция, то множество  $(M, \circ)$  называют множеством с бинарной операцией.

$(M, \circ)$  называется группой, если выполнены следующие три условия:

$$\begin{cases} a \circ (b \circ c) = (a \circ b) \circ c, \forall a, b, c \in M (\text{ассоциативность}) \\ \text{существует нейтральный элемент } e \in M, e \circ a = a \circ e = a, \forall a \in M \\ \forall a \in M \exists b \in M : a \circ b = b \circ a = e \end{cases}$$

Группы матриц (с операцией умножения):

$$GL_n(\mathbb{R}) = \{A \in Mat_{n \times n} | \det A \neq 0\}$$

$$SL_n(\mathbb{R}) = \{A \in Mat_{n \times n} | \det A = 1\}$$

## 1.2 Примеры групп по сложению

Числовые аддитивные группы:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{Z}_n, +)$ .

## 1.3 Примеры групп по умножению

Числовые мультипликативные группы:  $(\mathbb{Q} \setminus \{0\}, \times)$ ,  $(\mathbb{R} \setminus \{0\}, \times)$ ,  $(\mathbb{C} \setminus \{0\}, \times)$ ,  $(\mathbb{Z}_p \setminus \{0\}, \times)$ ,  $p$  - простое.

## 1.4 Группа кватернионов

$$Q_8 = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} -1 & 0 \\ 0 & -1 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \begin{bmatrix} 0 & -i \\ -i & 0 \end{bmatrix}, \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}, \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix} \right\}.$$

## 1.5 Порядок элемента, порядок группы

Порядок элемента  $g$  — это величина

$$\text{ord}(g) := \begin{cases} \min\{n \in \mathbb{N} : g^n = e\}, & \text{если множество непусто} \\ \infty, & \text{если множество пусто} \end{cases}$$

Порядок группы — мощность носителя группы, то есть, для конечных групп — количество элементов группы

## 1.6 Группа подстановок. Теорема Кэли

симметрическая группа  $S_n$  - все перестановки длины  $n$ ,  $|S_n| = n!$

знакопеременная группа  $A_n$  - все четные перестановки длины  $n$   $|A_n| = n!/2$

**Теорема Кэли:** Всякая конечная группа  $G$ ,  $\text{ord} G = n$ , изоморфна некоторой подгруппе группы перестановок  $S_n$ . При этом каждый элемент группы  $G$  сопоставляется с перестановкой  $\pi_a$ ,  $\pi_a(g) = a \circ g$ , где  $g$  - произвольный элемент группы  $G$ . [пример здесь](#)

## 1.7 Определение циклической группы. Определение образующего элемента циклической группы

$$\langle g \rangle := \{g^n, n \in \mathbb{Z}\}$$

Группа  $G$  называется циклической, если существует такое  $g \in G$ , что  $G = \langle g \rangle$

Элемент  $g$  называется образующим элементом циклической группы  $G$

**Пример:** Группы  $(\mathbb{Z}, +)$ ,  $(\mathbb{Z}_n, +)$  при  $n \geq 1$  являются циклическими.

## 1.8 Теорема Лагранжа. Следствия из теоремы Лагранжа

Множество  $aH := \{ah \mid h \in H\}$  называется левым смежным классом элемента  $a \in G$  по подгруппе  $H$ .

**Индекс подгруппы**  $H$  в группе  $G$  — это число левых смежных классов  $G$  по  $H$ . Обозначение  $[G : H]$

**Теорема Лагранжа:** Пусть  $G$  — конечная группа,  $H \subseteq G$  — подгруппа; тогда  $|G| = |H| \cdot [G : H]$

**Следствие 1:** Пусть  $G$  — конечная группа и  $H \subseteq G$ . Тогда  $|H|$  делит  $|G|$

**Следствие 2:** Пусть  $G$  — конечная группа и  $g \in G$ . Тогда  $\text{ord} g$  делит  $|G|$

**Следствие 3:** Пусть  $G$  — конечная группа и  $|G|$  — простое число. Тогда  $G$  — циклическая группа, порождаемая любым своим неединичным элементом.

## 1.9 Определение нормальной подгруппы. Определение фактор-группы

Подгруппа  $H \subseteq G$  называется нормальной, если  $gH = Hg \forall g \in G$ . Обозначение  $H \triangleleft G$ . Пусть  $H$  — нормальная подгруппа группы  $G$ . Согласно определению, в этой ситуации левые и правые смежные классы  $G$  по  $H$  — это одно и то же, и тогда мы будем называть их просто смежными классами.

Обозначим через  $G/H$  множество всех смежных классов  $G$  по  $H$ . Оказывается, что на  $G/H$  можно ввести структуру группы.

Сначала введём на  $G/H$  бинарную операцию, положив  $(g_1H) \cdot (g_2H) := (g_1g_2)H$  для любых  $g_1, g_2 \in G$ .

Как это понимать? Мы хотим перемножить два смежных класса и получить в результате третий смежный класс. Для этого мы берём какой-нибудь элемент  $g_1$  из первого смежного класса, элемент  $g_2$  из второго смежного класса и объявляем, что результатом перемножения наших двух смежных классов будет смежный класс элемента  $g_1g_2$ . Однако тут возникает потенциальная проблема: а вдруг при другом выборе элементов  $g_1$  и  $g_2$  из тех же смежных классов смежный класс элемента  $g_1g_2$  окажется другим? Оказывается, в нашей ситуации такое невозможно, что доказывается так называемой проверкой корректности.

Корректность: пусть элементы  $g'_1, g'_2 \in G$  таковы, что  $g'_1H = g_1H$  и  $g'_2H = g_2H$  (то есть  $g'_1$  и  $g'_2$  — другие представители наших исходных смежных классов  $g_1H$  и  $g_2H$  соответственно). Тогда  $g'_1 = g_1h_1$  и  $g'_2 = g_2h_2$  для некоторых  $h_1, h_2 \in H$ . В соответствии с тем же определением должно выполняться равенство  $(g'_1H) \cdot (g'_2H) = (g'_1g'_2)H$ , потому нам нужно показать, что  $(g'_1g'_2)H = (g_1g_2)H$ . Имеем

$$g'_1g'_2 = g_1h_1g_2h_2 = g_1g_2g_2^{-1}h_1g_2h_2 \subseteq (g_1g_2)H$$

(в последнем переходе учтено, что  $g_2^{-1}h_1g_2 \in H$  в силу нормальности подгруппы  $H$ ), откуда вытекает  $(g'_1g'_2)H = (g_1g_2)H$ .

Итак, на множестве  $G/H$  корректно определена бинарная операция. Теперь легко проверить, что  $(G/H, \cdot)$  является группой:

ассоциативность:  $((aH)(bH))(cH) = ((ab)H)(cH) = ((ab)c)H = (a(bc))H = (aH)((bc)H) = (aH)((bH)(cH));$

нейтральный элемент — это  $eH$ :  $(eH)(aH) = (ea)H = aH = (ae)H = (aH)(eH);$

обратный к  $gH$  элемент — это  $g^{-1}H$ :  $(g^{-1}H)(gH) = (g^{-1}g)H = eH = (gg^{-1})H = (gH)(g^{-1}H).$

Как видно, все необходимые свойства вытекают из аналогичных свойств для группы  $G$ .

Группа  $(G/H, \cdot)$  называется факторгруппой группы  $G$  по нормальной подгруппе  $H$ .

**Пример.** Пусть  $G = (\mathbb{Z}, +)$  и  $H = n\mathbb{Z}$  для некоторого  $n \in \mathbb{N}$ . Тогда  $G/H$  — это знако-мая нам группа вычетов  $(\mathbb{Z}_n, +)$ . Впрочем, некоторая тонкость тут в том, как именно определять группу  $(\mathbb{Z}_n, +)$ . С теоретической точки зрения наиболее удобно определение данной группы именно как факторгруппы  $\mathbb{Z}/n\mathbb{Z}$ . На практике же наиболее удобным для вычислений является определение «на пальцах», когда рассматривается множество  $\{0, 1, \dots, n-1\}$  с операцией сложения по модулю  $n$ . С формальной точки зрения это будет группа, отличная от  $\mathbb{Z}/n\mathbb{Z}$ , но изоморфная ей (про изоморфизмы см. ниже).

## 1.10 Определение гомоморфизма групп

Пусть  $G, F$  - две группы

Отображение  $\varphi : G \rightarrow F$  называется гомоморфизмом, если  $\varphi(ab) = \varphi(a) \cdot \varphi(b)$  для любых  $a, b \in G$ . В каждой из групп своя бинарная операция (!)

## 1.11 Основная теорема о гомоморфизмах

Ядро гомоморфизма  $\varphi$  - это множество  $\text{Ker} \varphi := \{g \in G | \varphi(g) = e_F\} \subseteq G$

Образ гомоморфизма  $\varphi$  - это множество  $\text{Im} \varphi := \varphi(G) \subseteq F$

**Теорема о гомоморфизме**  $G/\text{ker} \varphi \simeq \text{Im} \varphi$  (изоморфно)

## 1.12 Определение кольца. Примеры колец

Кольцо - это множество  $R$ , на котором заданы две бинарные операции  $(+, \cdot)$ , удовлетворяющие следующим условиям:

1)  $(R, +)$  - абелева группа (аддитивная группа кольца  $R$ )

2)  $\forall a, b, c \in R \begin{cases} a(b+c) = ab+ac \text{ (левая дистрибутивность)} \\ (a+b)c = ac+bc \text{ (правая дистрибутивность)} \end{cases}$

3)  $(ab)c = a(bc) \forall a, b, c \in R$

$R$  (ассоциативность умножения)

4) существует элемент  $1 \in R$  (называемый единицей), такой что  $1 \cdot a = a \cdot 1 = a \forall a \in R$

$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$  - числовые кольца

## 1.13 Определение гомоморфизма колец

Отображение  $\varphi : R \rightarrow Q$  называется гомоморфизмом (колец), если  $\varphi(a+b) = \varphi(a) + \varphi(b)$ ,  $\varphi(ab) = \varphi(a)\varphi(b) \forall a, b \in R$

## 1.14 Определение идеала. Определение главного идеала.

Подмножество  $I$  кольца  $R$  называется (двусторонним) идеалом, если выполнены следующие 2 условия:

1)  $I$  - подгруппа по сложению

2) для всех  $a \in I, r \in R$  выполнено  $ra \in I, ar \in I$

Пусть  $R$  - коммутативное кольцо. С каждым элементом  $a \in R$  связан идеал  $(a) := \{ra | r \in R\}$

Идеал называется **главным**, если существует такое  $a \in R$ , что  $I = (a)$

**Пример.** Для всякого  $\geq 0$  главный идеал  $(k)$  в кольце  $\mathbb{Z}$  есть не что иное, как  $k\mathbb{Z}$

## 1.15 Построение факторкольца по идеалу $K \setminus I$

Пусть  $R$  - произвольное кольцо, а  $I$  - идеал в  $R$

Рассмотрим факторгруппу  $(R/I, +)$ . Её элементами являются смежные классы по идеалу  $I$ , то есть множества вида  $a + I$ , где  $a \in R$ . Мы хотим превратить  $R/I$  в кольцо; для этого введём на  $R/I$  операцию умножения, полагая  $(a + I) \cdot (b + I) := ab + I$  для всех  $a, b \in R$ . Иными словами, чтобы перемножить два смежных класса в  $R/I$ , мы выбираем в каждом из них по представителю, перемножаем их и смежный класс результата объявляем произведением двух исходных смежных классов.

Как и в случае с определением факторгруппы, здесь нужна проверка корректности. Пусть  $a + I = a' + I$ ,  $b + I = b' + I$ , то есть  $a'$  и  $b'$  — другие представители смежных классов  $a + I$  и  $b + I$  соответственно. Тогда  $a' = a + x$ ,  $b' = b + y$  для некоторых  $x, y \in I$ . Тогда то же определение даёт  $(a' + I)(b' + I) = a'b' + I$ , и потому нам нужно показать, что  $a'b' + I = ab + I$ . В самом деле,

$$a'b' + I = (a + x)(b + y) + I = ab + \underbrace{ay + xb + xy}_{\in I} + I = ab + I.$$

Обратим внимание, что в последнем переходе существенно используется то, что  $I$  является идеалом в  $R$ .

## 1.16 Функция Эйлера. Теорема Эйлера

**Функция Эйлера**  $\varphi(n)$  - мультипликативная арифметическая функция, значение которой равно количеству натуральных чисел не превосходящих  $n$  и взаимно простых с ним.

**Теорема Эйлера** - если  $a, m = 1$ , то  $a^{\varphi(m)} \equiv 1 \pmod{m}$ , где  $\varphi(m)$  — функция Эйлера.

$$\begin{aligned}\varphi(p) &= p - 1 \\ \varphi(p^n) &= p^n - p^{n-1}, \text{ где } p - \text{ простое число}\end{aligned}$$

## 1.17 Малая теорема Ферма

Если  $p$  - простое число и  $(a, p) = 1$ , то  $a^{p-1} \equiv 1 \pmod{p}$

## 1.18 Определение поля. Пример

Полем называется коммутативное ассоциативное кольцо с единицей, в котором  $0 \neq 1$  и всякий ненулевой элемент обратим. **Примеры полей:**  $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ .

## 1.19 Простое поле. Пример

Простое поле - это поле, которое не имеет нетривиальных подполей

## 1.20 Теорема о простом подполе

Любое поле имеет ЕДИНСТВЕННОЕ тривиальное подполе, которое изоморфно либо полю рациональных чисел  $\mathbb{Q}$ , либо полю целых чисел по вычету  $p$  ( $\mathbb{Z}_p$ ).

## 1.21 Характеристика поля. Пример

**Определение 1.** *Характеристикой* поля  $K$  называется наименьшее натуральное число  $p$ , для которого  $\underbrace{1 + 1 + \dots + 1}_p = 0$ . Если такого  $p$  не существует, то говорят, что характеристика поля  $K$  равна нулю.

Характеристика поля  $K$  обозначается через  $\text{char } K$ .

**Примеры.**  $\text{char } \mathbb{Q} = \text{char } \mathbb{R} = \text{char } \mathbb{C} = 0$ ,  $\text{char } \mathbb{Z}_p = p$ .

## 1.22 Алгебраические и трансцендентные элементы поля.

Если  $K, F$  - два поля -  $K \subseteq F$ , то поле  $F$  называется расширением поля  $K$

Элемент  $\alpha \in F$  называется **алгебраическим** над  $K$ , если существует ненулевой многочлен  $f \in K[x]$  со свойством  $f(\alpha) = 0$ . В противном случае элемент  $\alpha$  называется **трансцендентным** над  $K$

**Пример:** Рассмотрим расширение полей  $\mathbb{Q} \subseteq \mathbb{R}$ . Элемент  $\sqrt{2}$  является алгебраическим над  $\mathbb{Q}$ , так как он аннулируется многочленом  $x^2 - 2 \in \mathbb{Q}[x]$ . Элементы  $\pi, e$  - трансценденты над  $\mathbb{Q}$

## 1.23 Определение простого элемента поля. Определение неприводимого многочлена над полем $P$

**Простой элемент поля** - элемент, который нельзя представить в виде произведения двух элементов, которые необратимы. **Неприводимый многочлен над полем  $P$**  - нетривиальный многочлен, неразложимый в произведение нетривиальных многочленов. То есть многочлен  $p \in P[x]$  называется неприводимым, если не существует  $q, r \in P[x]$ , таких, что  $p = qr$

## 1.24 Построение конечного поля из $p^n$ элементов

Пусть  $h \in \mathbb{Z}_p[x]$  - неприводимый многочлен степени  $n$ . Тогда мы знаем, что факторкольцо  $F = \mathbb{Z}_p[x]/(h)$  является полем. Также мы знаем, что  $F$  имеет размерность  $n$  как векторное пространство над  $\mathbb{Z}_p$ , а тогда  $|F| = p^n$ , то есть  $F$  - искомое поле из  $p^n$  элементов.

## 1.25 Мультипликативная группа конечного поля

. Пусть  $K$  - произвольное конечное поле из  $p^n$  элементов ( $p$  - простое и  $n \in \mathbb{N}$ ). Имеем  $\text{char } K = p$ , и в частности  $\mathbb{Z}_p \subseteq K$

Рассмотрим группу  $K^\times := (K \setminus \{0\}, \times)$ , она называется мультипликативной группой поля  $K$ .

## 1.26 Пример конечного поля

**Пример.** Построим поле из 4 элементов. В соответствии с описанной выше конструкцией возьмём многочлен

$$h = x^2 + x + 1 \in \mathbb{Z}_2[x].$$

Поскольку  $h(0) = h(1) = 1 \neq 0$ , этот многочлен не имеет корней в  $\mathbb{Z}_2$ . А так как  $\deg h = 2$ , то отсюда следует, что  $h$  неприводим. Значит, факторкольцо

$$F = \mathbb{Z}_2[x]/(h)$$

является искомым полем из 4 элементов. Имеем  $F = \{0, 1, \bar{x}, \bar{x} + 1\}$ , где черта означает класс соответствующего элемента в факторкольце. На этом множестве операция сложения выполняется по модулю 2, а чтобы перемножить два элемента, их нужно сначала умножить как многочлены от  $\bar{x}$ , а затем понизить все степени выше 1 по правилу

$$\bar{x}^2 = \bar{x} + 1.$$

## 2 Задачи

### 2.1 1.4

Найдите остаток от деления  $48^{5n+3}$  на 11

$$48 \equiv 4 \pmod{11} \mapsto 4^{5n+3} \equiv 48^{5n+3} \pmod{11}$$

$$4^{5n+3} \equiv 4^{5n} \cdot 4^3 \equiv 4^{5n} \cdot 9 \equiv 9 \pmod{11}$$

$$4^2 \equiv 5 \pmod{11}$$

$$4^3 \equiv 9 \pmod{11}$$

$$4^4 \equiv 3 \pmod{11}$$

$$4^5 \equiv 1 \pmod{11}$$