

# Алгебра

Мастера конспектов

22 января 2020 г.

Честно говоря, ненависть к этой вашей топологии просто невообразима.

## Содержание

<b>1 Билеты</b>	<b>4</b>
1.1 Определение кольца. Простейшие следствия из аксиом. Примеры. Области целостности	4
1.2 Евклидовы кольца. Евклидовость $\mathbb{Z}$ . Неприводимые и простые элементы.	5
1.3 Идеалы, главные идеалы. Евклидово кольцо как кольцо главных идеалов	6
1.4 Основная теорема арифметики	7
1.5 Кольцо вычетов $\mathbb{Z}/n\mathbb{Z}$ . Китайская теорема об остатках	10
1.6 Определение поля. $\mathbb{Z}/p\mathbb{Z}$ как поле. Поле частных целостного кольца	10
1.7 Определение гомоморфизма и изоморфизма колец. Фактор-кольцо	10
1.8 Теорема о гомоморфизме	10
1.9 Кольцо многочленов. Целостность и евклидовость кольца многочленов над полем	10
1.10 Лемма Гаусса	10
1.11 Факториальность кольца многочленов	10
1.12 Теорема Безу. Производная многочлена и кратные корни	10
1.13 Интерполяция Лагранжа	10
1.14 Интерполяция Эрмита	10
1.15 Поле разложение многочлена	10
1.16 Комплексные числа. Решение квадратных уравнений в	10
1.17 Основная теорема алгебры	10
1.18 Разложение рациональной функции в простейшие дроби над $\mathbb{C}$ и над $\mathbb{R}$	10
1.19 Определение векторного пространства. Линейная зависимость. Существование базиса	10
1.20 Размерность векторного пространства	10
1.21 Линейные отображения векторных пространств. Подпространство, факторпространство. Ранг линейного отображения	10
1.22 Матрица линейного отображения. Композиция линейных отображений и произведение матриц. Кольцо матриц	10
1.23 Элементарные преобразования. Метод Гаусса. Системы линейных уравнений	10
1.24 Теорема Кронекера-Капелли	10
1.25 Определение группы. Циклическая группа. Порядок элемента	10
1.26 Группа перестановок. Циклы, транспозиции. Знак перестановки	10
1.27 Действие группы на множестве. Орбиты. Классы сопряженности	10
1.28 Группа обратимых элементов кольца. Вычисление обратимых элементов $\mathbb{Z}/n\mathbb{Z}$ . Функция Эйлера	10
1.29 Гомоморфизмы и изоморфизмы групп. Смежные классы, теорема Лагранжа. Теорема Эйлера	10
1.30 Многочлены деления круга	10
1.31 Конечные поля (существование, единственность, цикличность мультипликативной группы)	10
1.32 Фактор-группа, теорема о гомоморфизме	10
1.33 Определитель матрицы. Инвариантность при элементарных преобразованиях, разложение по строчке и столбцу	10

---

1.34	Присоединенная матрица. Формула Крамера. Определитель транспонированной матрицы . . . . .	10
1.35	Вычисление определителя методом Гаусса . . . . .	10
1.36	Принцип продолжения алгебраических тождеств. Определитель произведения матриц . . . . .	10
2	<b>Пофамильный указатель всех мразей</b>	<b>11</b>

# 1 Билеты

## 1.1 Определение кольца. Простейшие следствия из аксиом. Примеры. Области целостности

**Определение 1.** *Кольцом* называется множество  $R$  вместе с бинарными операциями  $+$  и  $\cdot$  (которые называются сложением и умножением соответственно), удовлетворяющим аксиомам:

- операция сложения ассоциативна;
- по отношению к сложению существует нейтральный элемент;
- у каждого элемента есть обратный по сложению
- операция сложения коммутативна;
- умножение ассоциативно;
- умножение дистрибутивно по сложению.

Также можно добавить, что если на множестве выполнены три первые аксиомы, то оно будет называться *группой*, а если выполнены первые четыре, то это уже *абелева группа*. Нейтральный по сложению элемент кольца называют *нулём*.

**Пример(ы) 1.** Кольцо называется:

- *коммутативным*, если оно коммутативно по умножению;
- *кольцом с единицей*, если оно содержит нейтральный элемент по умножению (единица);
- *телом*, если в нём есть 1, и для любых  $a \neq 0 \rightarrow a \cdot a^{-1} = a^{-1} \cdot a = 1$ ;
- *полем*, если это коммутативное тело;
- *полукольцом*, если нет требования противоположного элемента по сложению.

*Следствие 1.* Некоторые следствия из аксиом:

- $0 \cdot a = 0$

*Доказательство.*

$$0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$$

Прибавим к обеим частям  $-0 \cdot a$  и получим требуемое. □

- Нейтральный элемент по сложению единственный

*Доказательство.* Рассмотрим их сумму справа и слева. □

- $a \cdot 0 = 0$

*Доказательство.*

$$a \cdot 1 = a \implies (0 + 1)a = a \implies 0 \cdot a + 1 \cdot a = a \implies 0 \cdot a = 0$$

□

**Определение 2.** Коммутативное кольцо  $R$  с единицей, обладающее свойством

$$xy = 0 \implies x = 0 \vee y = 0 \quad (\forall x, y \in R)$$

называется *областью целостности* или просто *областью*.

**Определение 3.** Число  $d \neq 0$  называется *делителем нуля*, если существует такое  $d' \neq 0$ , что  $dd' = 0$ .

Нетрудно понять, что область целостности - в точности коммутативное кольцо с единицей без делителей нуля.

## 1.2 Евклидовы кольца. Евклидовость $\mathbb{Z}$ . Неприводимые и простые элементы.

Для начала, некоторые связанные понятия, не упомянутые в билетах.

**Определение 4.** Говорят, что  $d$  *делит*  $p$  и пишут  $d|p$ , если  $p = dq$  для некоторого  $q \in R$ .

**Определение 5.** Элемент  $\varepsilon$  называется *обратимым*, если он делит единицу, то есть существует такое  $\varepsilon^{-1} \in R$ , что  $\varepsilon^{-1} \cdot \varepsilon = 1$ .

**Определение 6.** Будем говорить, что элементы  $a$  и  $b$  *ассоциированы* и писать  $a \sim b$ , если выполнено одно из двух эквивалентных условий:

- существует обратимый элемент  $\varepsilon$ , для которого  $a = \varepsilon b$ ;
- $a|b$  и  $b|a$ .

Покажем, что эти условия действительно эквивалентны.

*Доказательство.* Докажем в обе стороны:

$\Rightarrow$  Если  $a = \varepsilon b$ , то  $\varepsilon^{-1}a = b$ . Это и есть второе условие.

$\Leftarrow$  Пусть  $a = bc$  и  $b = ac'$  для каких-то  $c, c'$ . Тогда  $a = (ac')c = a(cc') \leftrightarrow a(1 - cc') = 0$ . Тогда либо  $a = 0$ , либо  $cc' = 1$ , потому что делителей нуля в нашем кольце нет. В любом случае,  $a$  и  $b$  отличаются на обратимый: либо они оба равны нулю, либо  $c$  - обратимый. □

А теперь, что касается самого билета.

**Определение 7.** Область целостности  $R$  называется *евклидовым кольцом*, если существует евклидова норма  $N : R \rightarrow \mathbb{N}_0$  такая, что  $N(0) = 0$  и для любых элементов  $a, b \in R$ , где  $b \neq 0$ , существует меньший чем  $b$  по норме элемент  $r \in R$  такой, что выполнено равенство  $a = bq + r$ .

**Пример(ы) 1.** Кольцо целых чисел  $\mathbb{Z}$  евклидово.

*Доказательство.* Пусть у нас имеются целое число  $a$  и ненулевое целое  $b$ . Тогда существуют такие целые числа  $q$  и  $r$ , что модуль  $r$  меньше модуля  $b$ , а также  $a = bq + r$ . Отметим на оси все кратные  $b$ . Тогда если число  $a$  попало на отрезок  $[kb, (k+1)b]$ ,  $k$  будет частным, а  $a - kb$  - остатком. Дальнейшую формализацию можно провести индукцией. □

Опять несколько небольших новых определений перед тем как перейти к последнему пункту билета (их можно упустить).

**Определение 8.** Пусть  $R$  - область целостности;  $a, b \in R$ . Элемент  $d \in R$  называется *наибольшим общим делителем*  $a$  и  $b$ , если

- $d|a$  и  $d|b$ ;
- для любого  $d' \in R$ , который также делит  $a$  и  $b$ , выполнено также, что он делит  $d$ .

**Теорема 1.** (О линейном представлении НОД в евклидовых кольцах). Пусть  $R$  - евклидово кольцо,  $a, b \in R$ . Тогда существуют  $d := \gcd(a, b)$  и такие  $x, y \in R$ , что  $d = ax + by$ .

Теперь про простые и неприводимые.

**Определение 9.** Пусть  $R$  - область. Необратимый элемент  $p \in R$  - *неприводимый*, если

$$\forall d \in R : d|p \implies d \sim 1 \vee d \sim p$$

**Определение 10.** Пусть  $R$  - область. Ненулевой необратимый элемент  $p \in R \setminus 0$  называется *простым*, если  $\forall a, b \in R : p|ab \implies p|a \vee p|b$ .

**Лемма 1.** (Простые  $\subset$  неприводимые). Если  $p$  - простой элемент произвольного коммутативного кольца с единицей, то  $p$  - неприводим.

*Доказательство.* Пусть  $d$  - какой-то делитель  $p$ , что эквивалентно равенству  $p = da$  для какого-то  $a$ . Проверим, что либо  $d \sim 1$ , либо  $d \sim p$ . Раз  $p$  - простой, то либо он делит  $d$ , либо он делит  $a$ . Если первое, что сразу  $d \sim p$ . Если второе, перепишем в виде  $da = p|a$ . Это то же самое, что  $bda = a$  для некоторого  $b$ . Здесь либо  $a = 0$ , то тогда  $p = 0$ , что невозможно по определению простого, либо мы можем сократить на  $a$  и получим  $bd = 1$ , тогда  $d$  ассоциирован с 1.  $\square$

Смотрите также *немного добавки* про простые и неприводимые после введения ОГИ.

### 1.3 Идеалы, главные идеалы. Евклидово кольцо как кольцо главных идеалов

**Определение 11.** Подмножество

$$(a_1, \dots, a_n) := \{a_1x_1 + \dots + a_nx_n | x_i \in R \text{ для всех } i\}$$

коммутативного кольца  $R$  называется *идеалом*, порождённым  $a_1, \dots, a_n$ .

**Определение 12.** Подкольцо  $I$  кольца  $R$  называется *левым идеалом*, если оно замкнуто относительно домножения слева на элементы кольца:  $RI = I$ . Соответственно, также различают *правые* и *двусторонние идеалы*.

Также идеал можно задать следующими свойствами:

- $\forall x, y \in I \implies x + y \in I$ ;
- $\forall x \in I, \forall r \in R \implies xr \in I$ ;
- $-x \in I$ ;

- $I$  - непустой.

**Определение 13.** Идеал называется *главным*, если он порождён одним элементом.

**Определение 14.** *Область главных идеалов* - область целостности, в которой каждый идеал главный.

**Теорема 2.** (Евклидовы кольца  $\subset$  ОГИ). Пусть  $R$  - евклидово кольцо,  $I \trianglelefteq R$  - идеал. Тогда  $I$  - главный.

*Доказательство.* Найдём элемент, который порождает идеал  $I$ .

Вырожденный случай: если  $I = \{0\}$ , тогда  $I = (0)$ .

Иначе возьмём  $d \in I \setminus 0$  с минимальной нормой (по принципу индукции мы можем это сделать). Хотим показать, что  $I = (d)$ . Покажем это в обе стороны.

$\Rightarrow$  Легко видеть, что  $(d) \subset I$ .

$\Leftarrow$  Пусть  $a \in I$ , тогда поделим  $a$  на  $b$  с остатком:  $a = bd + r$ . Предположим,  $r \neq 0$ ,  $N(r) < N(d)$ . Выразим  $r$  линейной комбинацией  $a \in I$  и  $d \in I$ :  $r = a - bd \in I$  - противоречие с минимальностью нормы  $d$ . Значит,  $r = 0$ , а тогда  $a = bd \in (d)$ .  $\square$

Теперь немного добавки про простые и неприводимые, на всякий случай.

**Лемма 2.** (Неприводимые  $\subset$  простые в ОГИ). Пусть  $p$  - неприводимый в области главных идеалов. Тогда  $p$  - простой.

*Доказательство.* Пусть  $p|ab$ , хотим показать, что  $p|a \vee p|b$ . Воспользуемся тем, что мы в области главных идеалов:  $(p, a) = (d)$ , где  $d := \gcd(a, p)$ , а тогда  $px + ay = d$  для каких-то  $x, y$ .  $d|p$ , воспользуемся неприводимостью  $p$ : либо  $d \sim p$ , либо  $d \sim 1$ .

В первом случае  $p|d$ , тогда  $p|d|a$ .

Во втором случае после домножения на обратимые считать, что  $px + ay = 1$ . Потом домножим на  $b$ :  $pbx + aby = b$ .  $p$  явно делит первое слагаемое, ровно как и второе (по предположению). Значит,  $p|b$ .

В любом случае, приходим к желаемому.  $\square$

## 1.4 Основная теорема арифметики

Сначала опять немного информации, которая к билету не относится, но к нему логично подводит.

**Определение 15.** Коммутативное кольцо с единицей  $R$  удовлетворяет *условию обрыва возрастающих цепей главных идеалов* или, что то же самое, является *нетёровым кольцом*, если не существует бесконечной строго возрастающей цепочки главных идеалов  $(d_1) \subsetneq (d_2) \subsetneq \dots$ . Иначе говоря, бесконечной цепочки  $\dots |d_2|d_1$ , где все  $d_i$  попарно не ассоциированы.

**Теорема 3.** (ОГИ  $\subset$  нетёровы кольца). Область главных идеалов удовлетворяет условию обрыва возрастающих цепей главных идеалов (далее - УОВЦГИ).

*Доказательство.* Предположим, что нашлась такая бесконечная цепочка  $\{d_i\}$ . Объединим  $I := \bigcup_{i=0}^{\infty} (d_i)$ .

Покажем, что  $I$  - идеал.  $0 \in I$ . Пусть  $u \in (d_i)$  и  $v \in (d_j)$ , где  $i \leq j$ , проверяем остальные условия.  $u + v \in (d_j)$ , потому что  $u \in (d_j)$ , с остальными аналогично, не очень сложно.

Вспомним, что мы находимся в ОГИ, то есть, каждый идеал главный. Пусть  $d$  - генератор  $I$  ( $I = (d)$ ). Любой  $(d_i)$  строго содержится в  $(d_{i+1})$ , а этот содержится в  $(d)$  :

$(d_i) \subsetneq (d_{i+1}) \subset (d)$ , значит, любой из  $\{(d_i)\}$  строго содержится в  $(d)$ . Но сам генератор  $d$  тоже должен принадлежать какому-то из  $\{(d_i)\}$ , а значит, на каком-то моменте  $(d) \subset (d_i)$ . Противоречие.  $\square$

**Определение 16.** Кольцо называется *факториальным*, если одновременно выполнено:

- $R$  - область;
- любой неприводимый элемент  $R$  - простой;
- $R$  - нетёрово.

**Пример(ы) 1.** Как мы уже знаем, ОГИ  $\subset$  факториальные кольца.

А теперь, к основному.

**Теорема 4.** (*Основная теорема арифметики*). Пусть  $R$  - факториальное кольцо.

Тогда любой элемент  $x \in R$ , если он не нуль и не обратимый, представляется в виде  $r = p_1 \dots p_n$ , где  $n \geq 1$ , а  $\{p_i\}$  - простые.

При этом, если  $r = q_1 \dots q_m$  - другое такое разложение, то  $m = n$  и существует перестановка индексов  $\pi : n \rightarrow n$ , такая, что  $p_i \sim q_{\pi_i}$  для всех  $i$ .

*Доказательство.* Докажем существование. Зафиксируем  $x$ . Если он неприводимый, то он и простой по определению факториального кольца, поэтому сам будет своим подходящим разложением. Пусть  $x = yz$ , где  $y, z \sim 1$ . Если  $y$  необратим и приводим, разложим и его:  $y = y_1 z_1$ , где  $y_1, z_1 \sim 1$ . Будем раскладывать так иреки, пока можем, и получим строго возрастающую цепочку идеалов  $(y) \subsetneq (y_1) \subsetneq (y_2) \subsetneq \dots$ . Вспомним нетёровость нашего кольца: бесконечно возрастать она не может, значит, на каком-то моменте заработаем для  $x$  один не приводимый делитель  $p : x = pw$  для какого-то  $w$ . Если  $w$  необратим и приводим, разложим и его:  $w = p_1 w_1$ . Продолжим и получим ещё одну возрастающую цепочку идеалов:  $(x) \subsetneq (w) \subsetneq (w_1) \subsetneq \dots$ . К тому времени, когда она оборвётся, у нас будет разложение  $x$  в конечное произведение неприводимых:  $x = p_1 \dots p_n$ . Существование доказано.

Теперь перейдём к доказательству единственности. Разложим двумя способами:  $r = p_1 \dots p_n = q_1 \dots q_m$ . По индукции пожно вывести из определения простого, что

**Лемма 3.** Если  $p$  - простой и  $p|a_1 \dots a_n$ , то  $p|a_i$  для какого-то  $i$ .

Воспользуемся этим фактом: например, мы теперь знаем: что  $q_m|p_i$  для какого-то  $i$ . Но  $p_i$  неприводим, поэтому любой его делитель либо обратим, либо ассоциирован с ним.  $q_m$  не боратим, так как он простой; значит,  $q_m \sim p_i$ . Переставим  $p_i$  и  $p_n$  и считаем, что  $q_m$  теперь  $\sim p_n$ . Осталось вывести следующий факт:

**Лемма 4.** Пусть  $a \sim b$ ,  $ac \sim bd$ ,  $a, b \neq 0$ . Тогда  $c \sim d$ .

*Доказательство.*  $a = \varepsilon b$  и  $ac = \varepsilon bc = \nu bd$  для каких-то обратимых  $\varepsilon$  и  $\nu$ . Последнее равенство можем сократить на  $b \neq 0$ , потому что мы в области.  $\square$

Теперь  $p_1 \dots p_{n-1} \sim q_1 \dots q_{m-1}$ . Можем теперь сказать, что равенство  $p_1 \dots p_{n-1} = q_1 \dots q_{m-1}$  верно по предположению индукции по  $n$ . Так же по индукции  $n = m$ , потому что получим противоречие, если какая-то из серий сомножителей  $\{p_i\}$ ,  $\{q_i\}$  закончится раньше.  $\square$

**Пример(ы) 2.** Обыкновенное кольцо  $\mathbb{Z} \in$  евклидовы кольца  $\subset$  ОГИ  $\subset$  факториальные кольца.





- 1.5 Кольцо вычетов  $\mathbb{Z}/n\mathbb{Z}$ . Китайская теорема об остатках
- 1.6 Определение поля.  $\mathbb{Z}/p\mathbb{Z}$  как поле. Поле частных целостного кольца
- 1.7 Определение гомоморфизма и изоморфизма колец. Фактор-кольцо
- 1.8 Теорема о гомоморфизме
- 1.9 Кольцо многочленов. Целостность и евклидовость кольца многочленов над полем
- 1.10 Лемма Гаусса
- 1.11 Факториальность кольца многочленов
- 1.12 Теорема Безу. Производная многочлена и кратные корни
- 1.13 Интерполяция Лагранжа
- 1.14 Интерполяция Эрмита
- 1.15 Поле разложение многочлена
- 1.16 Комплексные числа. Решение квадратных уравнений в
- 1.17 Основная теорема алгебры
- 1.18 Разложение рациональной функции в простейшие дроби над  $\mathbb{C}$  и над  $\mathbb{R}$
- 1.19 Определение векторного пространства. Линейная зависимость. Существование базиса
- 1.20 Размерность векторного пространства
- 1.21 Линейные отображения векторных пространств. Подпространство, фактор-пространство. Ранг линейного отображения
- 1.22 Матрица линейного отображения. Композиция линейных отображений и произведение матриц. Кольцо матриц
- 1.23 Элементарные преобразования. Метод Гаусса. Системы линейных уравнений
- 1.24 Теорема Кронекера-Капелли
- 1.25 Определение группы. Циклическая группа. Порядок элемента
- 1.26 Группа перестановок. Циклы, транспозиции. Знак перестановки
- 1.27 Действие группы на множестве. Орбиты. Классы сопряженности
- 1.28 Группа обратимых элементов кольца. Вычисление обратимых элементов  $\mathbb{Z}/n\mathbb{Z}$ . Функция Эйлера
- 1.29 Гомоморфизмы и изоморфизмы групп. Смежные классы, теорема Лагранжа. Теорема Эйлера
- 1.30 Многочлены деления круга
- 1.31 Конечные поля (существование, единственность, цикличность мультипликативной группы)
- 1.32 Фактор-группа, теорема о гомоморфизме

И в заключение...

## 2 Пофамильный указатель всех мразей

Быстрый список для особо забывшегося поиска.

[ассоциированность](#)

[делитель нуля](#)

[евклидово кольцо](#)

[идеал](#)

[кольцо, а также его вариации](#)

[неприводимые](#)

[НОД](#)

[ОГИ](#)

[ОТА](#)

[область целостности](#)

[простые](#)

[УОВЦГИ](#)

[факториальность](#)