

# Алгебра. Экзамен

Бобень Вячеслав  
[@darkkeks](#), [GitHub](#)

2020

“Какой-то ты слишком идеальный, редуцируем его!”.

---

— Bottom text

## Содержание

1	Бинарные операции. Полугруппы, моноиды и группы. Коммутативные группы. Примеры групп. Порядок группы. Подгруппы. Описание всех подгрупп в группе $(\mathbb{Z}, +)$	3
2	Подгруппы. Циклические подгруппы. Циклические группы. Порядок элемента. Связь между порядком элемента и порядком порождаемой им циклической подгруппы	4
3	Смежные классы. Индекс подгруппы. Теорема Лагранжа	5
4	Пять следствий из теоремы Лагранжа	6
5	Нормальные подгруппы и факторгруппы	7
6	Гомоморфизмы групп. Простейшие свойства гомоморфизмов. Изоморфизмы групп. Ядро и образ гомоморфизма групп, их свойства	8
7	Теорема о гомоморфизме для групп	9
8	Классификация циклических групп	10
9	Прямое произведение групп. Разложение конечной циклической группы. Теорема о строении конечных абелевых групп	11
10	Экспонента конечной абелевой группы и критерий цикличности	12
11	Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи Хеллмана обмена ключами. Криптосистема Эль-Гамала	13
12	Кольца. Коммутативные кольца. Обратимые элементы, делители нуля и нильпотенты. Примеры колец. Поля. Критерий того, что кольцо вычетов является полем	14
13	Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец	15
14	Кольцо многочленов от одной переменной над полем: деление с остатком, наибольший общий делитель двух многочленов, теорема о его существовании и линейном выражении	16
15	Теорема о том, что кольцо многочленов от одной переменной над полем является кольцом главных идеалов	17
16	Неприводимые многочлены. Факториальность кольца многочленов от одной переменной над полем	18

17	Критерий того, что факторкольцо $\mathbb{K}[x]/(h)$ является полем. Базис и размерность факторкольца $\mathbb{K}[x]/(h)$ как векторного пространства над полем $\mathbb{K}$	19
18	Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов	20
19	Старший член многочлена от нескольких переменных. Элементарная редукция многочлена относительно другого многочлена. Лемма о конечности цепочек элементарных редукций относительно системы многочленов	21
20	Остаток многочлена относительно заданной системы многочленов. Системы Грёбнера. Характеризация систем Грёбнера в терминах цепочек элементарных редукций	22
21	$S$ -многочлены. Критерий Бухбергера	23
22	Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трёх эквивалентных условиях. Решение задачи вхождения многочлена в идеал	24
23	Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Грёбнера идеала	25
24	Теорема Гильберта о базисе идеала	26
25	Редуцируемость к нулю $S$ -многочлена двух многочленов с взаимно простыми старшими членами	27
26	Характеристика поля. Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений	28
27	Присоединение корня неприводимого многочлена. Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители	29
28	Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства	30
29	Подполе в расширении полей, порождённое алгебраическим элементом	31
30	Порядок конечного поля. Автоморфизм Фробениуса	32
31	Теорема существования для конечных полей	33
32	Цикличность мультипликативной группы конечного поля и неприводимые многочлены над $\mathbb{Z}_p$	34

- 1 Бинарные операции. Полугруппы, моноиды и группы. Коммутативные группы. Примеры групп. Порядок группы. Подгруппы. Описание всех подгрупп в группе  $(\mathbb{Z}, +)$

## 2 Подгруппы. Циклические подгруппы. Циклические группы. Порядок элемента. Связь между порядком элемента и порядком порождаемой им циклической подгруппы

### 3 Смежные классы. Индекс подгруппы. Теорема Лагранжа

## 4 Пять следствий из теоремы Лагранжа

## 5 Нормальные подгруппы и факторгруппы

**6 Гомоморфизмы групп. Простейшие свойства гомоморфизмов. Изоморфизмы групп. Ядро и образ гомоморфизма групп, их свойства**



## 7 Теорема о гомоморфизме для групп

## 8 Классификация циклических групп

**9 Прямое произведение групп. Разложение конечной циклической группы. Теорема о строении конечных абелевых групп**

## 10 Экспонента конечной абелевой группы и критерий цикличности

- 11 Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи Хеллмана обмена ключами. Криптосистема Эль-Гамала

**12 Кольца. Коммутативные кольца. Обратимые элементы, делители нуля и нильпотенты. Примеры колец. Поля. Критерий того, что кольцо вычетов является полем**

- 13 Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме для колец

- 14 Кольцо многочленов от одной переменной над полем: деление с остатком, наибольший общий делитель двух многочленов, теорема о его существовании и линейном выражении



- 15 Теорема о том, что кольцо многочленов от одной переменной над полем является кольцом главных идеалов

## 16 Неприводимые многочлены. Факториальность кольца многочленов от одной переменной над полем

- 17 Критерий того, что факторкольцо  $\mathbb{K}[x]/(h)$  является полем. Базис и размерность факторкольца  $\mathbb{K}[x]/(h)$  как векторного пространства над полем  $\mathbb{K}$

**18    Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов**

- 19 Старший член многочлена от нескольких переменных. Элементарная редукция многочлена относительно другого многочлена. Лемма о конечности цепочек элементарных редукций относительно системы многочленов

**20    Остаток многочлена относительно заданной системы многочленов. Системы Грёбнера. Характеризация систем Грёбнера в терминах цепочек элементарных редукций**



- 22** Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трёх эквивалентных условиях. Решение задачи вхождения многочлена в идеал



- 23 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Грёбнера идеала



**25** Редуцируемость к нулю  $S$ -многочлена двух многочленов с взаимно простыми старшими членами

**26 Характеристика поля. Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений**

- 27 Присоединение корня неприводимого многочлена. Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители

**28 Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства**

## 29 Подполе в расширении полей, порождённое алгебраическим элементом





## 31 Теорема существования для конечных полей

## 32 Цикличность мультипликативной группы конечного поля и неприводимые многочлены над $\mathbb{Z}_p$