

# Летний экзамен по алгебре

hse-ami-open-exams

## Содержание

<b>1</b>	<b>Бинарные операции. Полугруппы, моноиды и группы. Коммутативные группы. Примеры групп. Порядок группы. Описание всех подгрупп в группе <math>(\mathbb{Z}, +)</math></b>	<b>5</b>
1.1	Бинарные операции. . . . .	5
1.2	Полугруппы, моноиды и группы. . . . .	5
1.3	Коммутативные группы. . . . .	5
1.4	Примеры групп. . . . .	5
1.5	Порядок группы. . . . .	5
1.6	Описание всех подгрупп в группе $(\mathbb{Z}, +)$ . . . . .	5
<b>2</b>	<b>Подгруппы. Циклические подгруппы. Циклические группы. Порядок элемента. Связь между порядком элемента и порядком порождаемой им циклической подгруппы.</b>	<b>6</b>
2.1	Циклические подгруппы. . . . .	6
2.2	Циклические группы. . . . .	6
2.3	Порядок элемента. . . . .	6
2.4	Связь между порядком элемента и порядком порождаемой им циклической подгруппы. . . . .	6
<b>3</b>	<b>Смежные классы. Индекс подгруппы. Теорема Лагранжа.</b>	<b>7</b>
3.1	Смежные классы. . . . .	7
3.2	Индекс подгруппы. . . . .	7
3.3	Теорема Лагранжа. . . . .	7
<b>4</b>	<b>Пять следствий из теоремы Лагранжа.</b>	<b>8</b>
4.1	Следствие 1. . . . .	8
4.2	Следствие 2. . . . .	8
4.3	Следствие 3. . . . .	8
4.4	Следствие 4. . . . .	8
4.5	Следствие 5. . . . .	8
<b>5</b>	<b>Нормальные подгруппы и факторгруппы.</b>	<b>9</b>
5.1	Нормальные подгруппы. . . . .	9
5.1.1	Эквивалентность условий нормальности группы. . . . .	9
5.2	Факторгруппы. . . . .	9
5.2.1	Корректность. . . . .	9
5.2.2	Примеры факторгрупп. . . . .	9
<b>6</b>	<b>Гомоморфизмы групп. Простейшие свойства гомоморфизмов. Изоморфизмы групп. Ядро и образ гомоморфизма групп, их свойства.</b>	<b>10</b>
6.1	Гомоморфизмы групп. . . . .	10
6.2	Простейшие свойства гомоморфизмов. . . . .	10
6.3	Изоморфизмы групп. . . . .	10
6.4	Ядро и образ гомоморфизма групп, их свойства. . . . .	10
<b>7</b>	<b>Теорема о гомоморфизме для групп.</b>	<b>11</b>
<b>8</b>	<b>Классификация циклических групп.</b>	<b>12</b>
<b>9</b>	<b>Прямое произведение групп. Разложение конечной циклической группы.</b>	<b>13</b>
9.1	Прямое произведение групп. . . . .	13
9.2	Разложение конечной циклической группы. . . . .	13

<b>10 Подгруппы <math>p</math>-крючения в абелевых группах. Разложение конечной абелевой группы в прямое произведение подгрупп <math>p</math>-крючения.</b>	<b>14</b>
10.1 Подгруппы $p$ -крючения в абелевых группах. . . . .	14
10.2 Разложение конечной абелевой группы в прямое произведение подгрупп $p$ -крючения. . . . .	14
<b>11 Примарные абелевы группы. Теорема о строении конечных абелевых групп, доказательство единственности.</b>	<b>15</b>
11.1 Примарные абелевы группы. . . . .	15
11.2 Теорема о строении конечных абелевых групп, доказательство единственности. . . . .	15
<b>12 Экспонента конечной абелевой группы и критерий цикличности.</b>	<b>16</b>
<b>13 Криптография с открытым ключом. Задача дискретного логарифмирования. Система Диффи-Хеллмана обмена ключами. Криптосистема Эль-Гамала.</b>	<b>17</b>
13.1 Задача дискретного логарифмирования. . . . .	17
13.2 Система Диффи-Хеллмана обмена ключами. . . . .	17
13.3 Криптосистема Эль-Гамала. . . . .	17
<b>14 Кольца. Коммутативные кольца. Обратимые элементы, делители нуля и нильпотенты. Примеры колец. Поля. Критерий того, что кольцо вычетов является полем.</b>	<b>18</b>
14.1 Кольца. . . . .	18
14.2 Коммутативные кольца. . . . .	18
14.3 Обратимые элементы, делители нуля и нильпотенты. . . . .	18
14.4 Примеры колец. . . . .	18
14.5 Поля. . . . .	18
14.6 Критерий того, что кольцо вычетов является полем. . . . .	19
<b>15 Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме колец.</b>	<b>20</b>
15.1 Идеалы колец. . . . .	20
15.2 Факторкольцо кольца по идеалу. . . . .	20
15.3 Гомоморфизмы и изоморфизмы колец. . . . .	20
15.4 Ядро и образ гомоморфизма колец. . . . .	20
15.5 Теорема о гомоморфизме колец. . . . .	21
<b>16 Делимость и ассоциированные элементы в коммутативных кольцах без делителей нуля. Наибольший общий делитель. Кольца главных идеалов. Существование наибольшего общего делителя и его линейного выражения в кольце главных идеалов.</b>	<b>22</b>
16.1 Делимость и ассоциированные элементы в коммутативных кольцах без делителей нуля. . . . .	22
16.2 Наибольший общий делитель. . . . .	22
16.3 Кольца главных идеалов. . . . .	22
16.4 Существование наибольшего общего делителя и его линейного выражения в кольце главных идеалов. . . . .	22
<b>17 Деление с остатком в кольце многочленов от одной переменной над полем. Теорема о том, что это кольцо является кольцом главных идеалов.</b>	<b>23</b>
17.1 Деление с остатком в кольце многочленов от одной переменной над полем. . . . .	23
17.2 Теорема о том, что это кольцо является кольцом главных идеалов. . . . .	23
<b>18 Простые элементы. Факториальные кольца. Факториальность кольца многочленов от одной переменной над полем. (todo)</b>	<b>24</b>
18.1 Простые элементы. . . . .	24
18.2 Факториальные кольца. . . . .	24
18.3 Факториальность кольца многочленов от одной переменной над полем. . . . .	24

<b>19 Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов. (todo)</b>	<b>25</b>
19.1 Лексикографический порядок на множестве одночленов от нескольких переменных. . . . .	25
19.2 Лемма о конечности убывающих цепочек одночленов. . . . .	25
<b>20 Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов. (todo)</b>	<b>26</b>
20.1 Лексикографический порядок на множестве одночленов от нескольких переменных. . . . .	26
20.2 Лемма о конечности убывающих цепочек одночленов. . . . .	26
<b>21 Остаток многочлена относительно заданной системы многочленов. Системы Гребнера. Характеризация систем Гребнера в терминах цепочек элементарных редукций. (todo)</b>	<b>27</b>
21.1 Остаток многочлена относительно заданной системы многочленов. . . . .	27
21.2 Системы Гребнера. . . . .	27
21.3 Характеризация систем Гребнера в терминах цепочек элементарных редукций. . . . .	27
<b>22 S-многочлены. Критерий Бухбергера. (todo)</b>	<b>28</b>
22.1 S-многочлены. . . . .	28
22.2 Критерий Бухбергера. . . . .	28
<b>23 Базис Гребнера идеала в кольце многочленов от нескольких переменных, теорема о трех эквивалентных условиях. Решение задачи вхождения многочлена в идеал. (todo)</b>	<b>29</b>
23.1 Базис Гребнера идеала в кольце многочленов от нескольких переменных, теорема о трех эквивалентных условиях. . . . .	29
23.2 Решение задачи вхождения многочлена в идеал. . . . .	29
<b>24 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Гребнера идеала. (todo)</b>	<b>30</b>
24.1 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. . . . .	30
24.2 Алгоритм Бухбергера построения базиса Гребнера идеала. . . . .	30
<b>25 Редуцируемость к нулю S-многочлена двух многочленов с взаимно простыми старшими членами. (todo)</b>	<b>31</b>
<b>26 Характеристика поля. Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений. (todo)</b>	<b>32</b>
26.1 Характеристика поля. . . . .	32
26.2 Расширение полей. . . . .	32
26.3 Конечное расширение и его степень. . . . .	32
26.4 Степень композиции двух расширений. . . . .	32
<b>27 Критерий того, что факторкольцо кольца многочленов от одной переменной над полем является полем. Степень расширения этого поля. (todo)</b>	<b>33</b>
27.1 Критерий того, что факторкольцо кольца многочленов от одной переменной над полем является полем. . . . .	33
27.2 Степень расширения этого поля. . . . .	33
<b>28 Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители. Поле разложения многочлена. (todo)</b>	<b>34</b>
28.1 Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители. . . . .	34
28.2 Поле разложения многочлена. . . . .	34

<b>29 Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства. (todo)</b>	<b>35</b>
29.1 Алгебраические и трансцендентные элементы. . . . .	35
29.2 Минимальный многочлен алгебраического элемента и его свойства. . . . .	35
<b>30 Подполе в расширении полей, порожденное алгебраическим элементом. (todo)</b>	<b>36</b>
<b>31 Порядок конечного поля. Автоморфизм Фробениуса. (todo)</b>	<b>37</b>
31.1 Порядок конечного поля. . . . .	37
31.2 Автоморфизм Фробениуса. . . . .	37
<b>32 Теорема существования и единственности для конечных полей. (todo)</b>	<b>38</b>
<b>33 Цикличность мультипликативной группы конечного поля и неприводимые многочлены над <math>\mathbb{Z}_p</math> (todo)</b>	<b>39</b>
<b>34 Подполя конечного поля. (todo)</b>	<b>40</b>
<b>35 Коды над конечным алфавитом. Расстояние Хэмминга. Минимальное расстояние кода. Коды, исправляющие t ошибок: определение и эквивалентные переформулировки. Код с повторением. (todo)</b>	<b>41</b>
35.1 Коды над конечным алфавитом. . . . .	41
35.2 Расстояние Хэмминга. . . . .	41
35.3 Минимальное расстояние кода. . . . .	41
35.4 Коды, исправляющие t ошибок: определение и эквивалентные переформулировки. . . . .	41
35.5 Код с повторением. . . . .	41
<b>36 Линейные коды. Проверочная матрица. Связь минимального расстояния линейного кода с его проверочной матрицей. Бинарный код Хэмминга, его минимальное расстояние и число ошибок, которое он может исправлять. (todo)</b>	<b>42</b>
36.1 Линейные коды. . . . .	42
36.2 Проверочная матрица. . . . .	42
36.3 Связь минимального расстояния линейного кода с его проверочной матрицей. . . . .	42
36.4 Бинарный код Хэмминга, его минимальное расстояние и число ошибок, которое он может исправлять. . . . .	42
<b>37 Коды БЧХ. Теорема о количестве ошибок, исправляемых кодом БЧХ. Оценка на размерность кода БЧХ. (todo)</b>	<b>43</b>
37.1 Коды БЧХ. . . . .	43
37.2 Теорема о количестве ошибок, исправляемых кодом БЧХ. . . . .	43
37.3 Оценка на размерность кода БЧХ. . . . .	43

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

## 1.1 Бинарные операции.

**Определение 1.** Множество с бинарной операцией – это множество  $M$  с заданным отображением

$$M \times M \rightarrow M, \quad (a, b) \mapsto a \circ b.$$

Множество с бинарной операцией обычно обозначают  $(M, \circ)$ .

## 1.2 Полугруппы, моноиды и группы.

**Определение 2.** Множество с бинарной операцией  $(M, \circ)$  называется **полугруппой**, если данная бинарная операция **ассоциативна**, т.е.

$$a \circ (b \circ c) = (a \circ b) \circ c \quad \text{для всех } a, b, c \in M.$$

**Определение 3.** Полугруппа  $(S, \circ)$  называется **моноидом**, если в ней есть нейтральный элемент, т.е. такой элемент  $e \in S$ , что  $e \circ a = a \circ e = a$  для любого  $a \in S$ .

**Определение 4.** Моноид  $(S, \circ)$  называется **группой**, если для каждого элемента  $a \in S$  найдется обратный элемент, т.е. такой  $b \in S$ , что  $a \circ b = b \circ a = e$ .

## 1.3 Коммутативные группы.

**Определение 5.** Группа  $(G, \circ)$  называется **коммутативной** или **абелевой**, если групповая операция коммутативна, т.е.  $a \circ b = b \circ a$  для любых  $a, b \in G$ .

## 1.4 Примеры групп.

1. Числовые аддитивные группы:  $(\mathbb{Z}, +)$ ,  $(\mathbb{Q}, +)$ ,  $(\mathbb{R}, +)$ ,  $(\mathbb{C}, +)$ ,  $(\mathbb{Z}_n, +)$ .
2. 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.
3. Группы матриц:  $GL_n(\mathbb{R}) = \{A \in Mat(n \times n, \mathbb{R}) \mid \det(A) \neq 0\}$ ;  $SL_n(\mathbb{R}) = \{A \in Mat(n \times n, \mathbb{R}) \mid \det(A) = 1\}$ .
4. Группы подстановок: симметрическая группа  $S_n$  – все подстановки длины  $n$ ,  $|S_n| = n!$ ; знакопеременная группа  $A_n$  – четные подстановки длины  $n$ ,  $|A_n| = n!/2$ .

## 1.5 Порядок группы.

**Определение 6.** **Порядок** группы  $G$  – это число элементов в  $G$ . Группа называется **конечной**, если ее порядок конечен, и **бесконечной** иначе.

## 1.6 Описание всех подгрупп в группе $(\mathbb{Z}, +)$

**Определение 7.** Подмножество  $H$  группы  $G$  называется **подгруппой**, если выполнены следующий три условия:

1.  $e \in H$
2.  $ab \in H$  для любых  $a, b \in H$
3.  $a^{-1} \in H$  для любого  $a \in H$

**Утверждение 1.** Всякая подгруппа в  $(\mathbb{Z}, +)$  имеет вид  $k\mathbb{Z} = \{ka \mid a \in \mathbb{Z}\}$  для некоторого целого неотрицательного  $k$ .

**Доказательство.** Пусть  $H$  – подгруппа в  $\mathbb{Z}$ . Если  $H = \{0\}$ , положим  $k = 0$ . Иначе пусть  $k = \min(H \cap \mathbb{N})$  – наименьшее натуральное число, лежащее в  $H$ . Тогда  $k\mathbb{Z} \subseteq H$ . С другой стороны, если  $a \in H$  и  $a = qk + r$  – результат деления  $a$  на  $k$  с остатком, то  $0 \leq r \leq k - 1$  и  $r = a - qk \in H$ . Отсюда  $r = 0$  и  $H = k\mathbb{Z}$ .  $\square$

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

### 2.1 Циклические подгруппы.

**Определение 8.** Пусть  $G$  – группа и  $g \in G$ . **Циклической подгруппой**, порожденной элементом  $g$ , называется подмножество  $\{g^n \mid n \in \mathbb{Z}\}$ . Циклическая подгруппа, порожденная элементом  $g$ , обозначается  $\langle g \rangle$ . Элемент  $g$  называется **порождающим** или **образующим** для подгруппы  $\langle g \rangle$ .

### 2.2 Циклические группы.

**Определение 9.** Группа  $G$  называется **циклической**, если найдется такой элемент  $g \in G$ , что  $G = \langle g \rangle$ .

### 2.3 Порядок элемента.

**Определение 10.** Пусть  $G$  – группа и  $g \in G$ . **Порядком элемента  $g$**  называется такое наименьшее натуральное число  $m$ , что  $g^m = e$ . Если такого натурального числа  $m$  не существует, говорят, что порядок элемента  $g$  равен бесконечности. Порядок элемента обозначается  $\text{ord}(g)$ .

### 2.4 Связь между порядком элемента и порядком порождаемой им циклической подгруппы.

**Утверждение 2.** Пусть  $G$  – группа и  $g \in G$ . Тогда  $\text{ord}(g) = |\langle g \rangle|$ .

*Доказательство.* Заметим, что если  $g^k = g^s$ , то  $g^{k-s} = e$ . Поэтому если элемент  $g$  имеет бесконечный порядок, то все элементы  $g^n, n \in \mathbb{Z}$ , попарно различны и подгруппа  $\langle g \rangle$  содержит бесконечно много элементов. Если же порядок элемента  $g$  равен  $m$ , то из минимальности числа  $m$  следует, что элементы  $e = g^0, g = g^1, g^2, \dots, g^{m-1}$  попарно различны. Далее, для всякого  $n \in \mathbb{Z}$  мы имеем  $n = mq + r$ , где  $0 \leq r \leq m-1$ , и

$$g^n = g^{mq+r} = (g^m)^q g^r = e^q g^r = g^r.$$

Следовательно,  $\langle g \rangle = \{e, g, \dots, g^{m-1}\}$  и  $|\langle g \rangle| = m$ . □

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

#### 3.1 Смежные классы.

**Определение 11.** Пусть  $G$  – группа,  $H \subseteq G$  – подгруппа и  $g \in G$ . **Левым смежным классом** элемента  $g$  группы  $G$  по подгруппе  $H$  называется подмножество

$$gH = \{gh \mid h \in H\}.$$

#### 3.2 Индекс подгруппы.

**Определение 12.** Пусть  $G$  – группа и  $H \subseteq G$  – подгруппа. **Индексом подгруппы  $H$**  в группе  $G$  называется число левых смежных классов  $G$  по  $H$ . Индекс группы  $G$  по подгруппе  $H$  обозначается  $[G : H]$ .

#### 3.3 Теорема Лагранжа.

**Лемма 1.** Пусть  $G$  – группа,  $H \subseteq G$  – ее подгруппа и  $g_1, g_2 \in G$ . Тогда либо  $g_1H = g_2H$ , либо  $g_1H \cap g_2H = \emptyset$ .

*Доказательство.* Предположим, что  $g_1H \cap g_2H \neq \emptyset$ , т.е.  $g_1h_1 = g_2h_2$  для некоторых  $h_1, h_2 \in H$ . Нужно доказать, что  $g_1H = g_2H$ . Заметим, что  $g_1H = g_2h_2h_1^{-1}H \subseteq g_2H$ . Обратное включение доказывается аналогично.  $\square$

**Лемма 2.** Пусть  $G$  – группа и  $H \subseteq G$  – конечная подгруппа. Тогда  $|gH| = |H|$  для любого  $g \in G$ .

*Доказательство.* Поскольку  $gH = \{gh \mid h \in H\}$ , в  $gH$  элементов не больше, чем в  $H$ . Если  $gh_1 = gh_2$ , то домножаем слева на  $g^{-1}$  и получаем  $h_1 = h_2$ . Значит, все элементы вида  $gh$ , где  $h \in H$ , попарно различны, откуда  $|gH| = |H|$ .  $\square$

**Теорема 1.** Пусть  $G$  – конечная группа и  $H \subseteq G$  – подгруппа. Тогда

$$|G| = |H| \cdot [G : H].$$

*Доказательство.* Каждый элемент группы  $G$  лежит в (своем) левом смежном классе по подгруппе  $H$ , разные смежные классы не пересекаются (лемма 1) и каждый из них содержит по  $|H|$  элементов (лемма 2).  $\square$

## 4 Пять следствий из теоремы Лагранжа.

### 4.1 Следствие 1.

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

### 4.2 Следствие 2.

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

*Доказательство.* Это вытекает из следствия 1 и утверждения 2. □

### 4.3 Следствие 3.

**Следствие 3.** Пусть  $G$  – конечная группа и  $g \in G$ . Тогда  $g^{|G|} = e$ .

*Доказательство.* Согласно следствию 2 мы имеем  $|G| = \text{ord}(g) \cdot s$ , откуда  $g^{|G|} = (g^{\text{ord}(g)})^s = e^s = e$ . □

### 4.4 Следствие 4.

**Следствие 4.** Пусть  $G$  – группа. Предположим, что  $|G|$  – простое число. Тогда  $G$  – циклическая группа, порождаемая любым своим неединичным элементом.

*Доказательство.* Пусть  $g \in G$  – произвольный неединичный элемент. Тогда циклическая подгруппа  $\langle g \rangle$  содержит более одного элемента и  $|\langle g \rangle|$  делит  $|G|$  по следствию 1. Значит,  $|\langle g \rangle| = |G|$ , откуда  $G = \langle g \rangle$ . □

### 4.5 Следствие 5.

**Следствие 5** (малая теорема Ферма). Пусть  $p$  – простое число и  $\text{НОД}(a, p) = 1$ . Тогда  $a^{p-1} \equiv 1 \pmod{p}$ .

*Доказательство.* Применим следствие 3 к группе  $(\mathbb{Z}_p \setminus \{0\}, \times)$ . □



## 5 Нормальные подгруппы и факторгруппы.

### 5.1 Нормальные подгруппы.

**Определение 13.** Подгруппа  $H$  группы  $G$  называется **нормальной**, если  $gH = Hg$  для любого  $g \in G$ .

5.1.1 Эквивалентность условий нормальности группы.

**Утверждение 3.** Для подгруппы  $H \subseteq G$  следующие условия эквивалентны:

1.  $H$  нормальна
2.  $gHg^{-1} \subseteq H$  для любого  $g \in G$
3.  $gHg^{-1} = H$  для любого  $g \in G$

*Доказательство.* (1)  $\Rightarrow$  (2) Пусть  $h \in H$  и  $g \in G$ . Поскольку  $gH = Hg$ , имеем  $gh = h'g$  для некоторого  $h' \in H$ . Тогда  $ghg^{-1} = h'gg^{-1} = h' \in H$ .

(2)  $\Rightarrow$  (3) Так как  $gHg^{-1} \subseteq H$ , остается проверить обратное включение. Для  $h \in H$  имеем  $h = gg^{-1}hgg^{-1} = g(g^{-1}hg)g^{-1} \in gHg^{-1}$ , поскольку  $g^{-1}hg \in H$  в силу пункта (2), где вместо  $g$  взято  $g^{-1}$ .

(3)  $\Rightarrow$  (1) Для произвольного  $g \in G$  в силу (3) имеем  $gH = gHg^{-1}g \subseteq Hg$ , так что  $gH \subseteq Hg$ . Аналогично проверяется обратное включение. □

### 5.2 Факторгруппы.

5.2.1 Корректность.

Обозначим через  $G/H$  множество смежных классов группы  $G$  по нормальной подгруппе  $H$ . На  $G/H$  можно определить бинарную операцию следующим образом:

$$(g_1H)(g_2H) := g_1g_2H.$$

**Утверждение 4.** Указанная выше операция корректна.

*Доказательство.* Заменим  $g_1$  и  $g_2$  другими представителями  $g_1h_1$  и  $g_2h_2$  тех же смежных классов. Нужно проверить, что  $g_1g_2H = g_1h_1g_2h_2H$ . Это следует из того, что  $g_1h_1g_2h_2 = g_1g_2(g_2^{-1}h_1g_2)h_2$  и  $g_2^{-1}h_1g_2$  лежит в  $H$ . Ясно, что указанная операция на множестве  $G/H$  ассоциативна, обладает нейтральным элементом  $eH$  и для каждого элемента  $gH$  есть обратный элемент  $g^{-1}H$ . □

**Определение 14.** Множество  $G/H$  с указанной операцией называется **факторгруппой** группы  $G$  по нормальной подгруппе  $H$ .

5.2.2 Примеры факторгрупп.

1. Если  $G = (\mathbb{Z}, +)$  и  $H = n\mathbb{Z}$ , то  $G/H$  – это в точности группа вычетов  $(\mathbb{Z}_n, +)$ .

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

### 6.1 Гомоморфизмы групп.

**Определение 15.** Пусть  $G$  и  $F$  – группы. Отображение  $\varphi : G \rightarrow F$  называется **гомоморфизмом**, если  $\varphi(ab) = \varphi(a)\varphi(b)$  для любых  $a, b \in G$ .

### 6.2 Простейшие свойства гомоморфизмов.

**Лемма 3.** Пусть  $\varphi : G \rightarrow F$  – гомоморфизм групп и пусть  $e_G$  и  $e_F$  – нейтральные элементы групп  $G$  и  $F$  соответственно. Тогда

$$(a) \quad \varphi(e_G) = e_F$$

$$(б) \quad \varphi(a^{-1}) = \varphi(a)^{-1} \text{ для любого } a \in G.$$

*Доказательство.* (а) Имеем  $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$ . Теперь умножая крайние части этого равенства на  $\varphi(e_G)^{-1}$  (например, слева) получим  $e_F = \varphi(e_G)$ .

(б) Имеем  $\varphi(a^{-1})\varphi(a) = \varphi(a^{-1}a) = \varphi(e_G) = e_F$ , откуда  $\varphi(a^{-1}) = \varphi(a)^{-1}$ .  $\square$

### 6.3 Изоморфизмы групп.

**Определение 16.** Гомоморфизм групп  $\varphi : G \rightarrow F$  называется **изоморфизмом**, если отображение  $\varphi$  биективно.

### 6.4 Ядро и образ гомоморфизма групп, их свойства.

**Определение 17.** С каждым гомоморфизмом групп  $\varphi : G \rightarrow F$  связаны его ядро

$$\text{Ker}(\varphi) = \{g \in G \mid \varphi(g) = e_F\}$$

и образ

$$\text{Im}(\varphi) = \{a \in F \mid \exists g \in G : \varphi(g) = a\}.$$

Ясно, что  $\text{Ker}(\varphi) \subseteq G$  и  $\text{Im}(\varphi) \subseteq F$  – подгруппы.

**Лемма 4.** Гомоморфизм групп  $\varphi : G \rightarrow F$  инъективен тогда и только тогда, когда  $\text{Ker}(\varphi) = \{e_G\}$ .

*Доказательство.* Ясно, что если  $\varphi$  инъективен, то  $\text{Ker}(\varphi) = \{e_G\}$ . Обратно, пусть  $g_1, g_2 \in G$  и  $\varphi(g_1) = \varphi(g_2)$ . Тогда  $g_1^{-1}g_2 \in \text{Ker}(\varphi)$ , поскольку  $\varphi(g_1^{-1}g_2) = \varphi(g_1^{-1})\varphi(g_2) = \varphi(g_1)^{-1}\varphi(g_2) = e_F$ . Отсюда  $g_1^{-1}g_2 = e_G$  и  $g_1 = g_2$ .  $\square$

**Следствие 6.** Гомоморфизм групп  $\varphi : G \rightarrow F$  является изоморфизмом тогда и только тогда, когда  $\text{Ker}(\varphi) = \{e_G\}$  и  $\text{Im}(\varphi) = F$ .

**Утверждение 5.** Пусть  $\varphi : G \rightarrow F$  – гомоморфизм групп. Тогда подгруппа  $\text{Ker}(\varphi)$  нормальна в  $G$ .

*Доказательство.* Достаточно проверить, что  $g^{-1}hg \in \text{Ker}(\varphi)$  для любых  $g \in G$  и  $h \in \text{Ker}(\varphi)$ . Это следует из цепочки равенств

$$\varphi(g^{-1}hg) = \varphi(g^{-1})\varphi(h)\varphi(g) = \varphi(g^{-1})e_F\varphi(g) = \varphi(g^{-1})\varphi(g) = e_F.$$

$\square$

## 7 Теорема о гомоморфизме для групп.

**Теорема 2.** Пусть  $\varphi : G \rightarrow F$  – гомоморфизм групп. Тогда группа  $\text{Im}(\varphi)$  изоморфна факторгруппе  $G/\text{Ker}(\varphi)$ .

*Доказательство.* Рассмотрим отображение  $\psi : G/\text{Ker}(\varphi) \rightarrow F$ , заданное формулой  $\psi(g \text{Ker}(\varphi)) = \varphi(g)$ . Проверка корректности: равенство  $\varphi(gh_1) = \varphi(gh_2)$  для любых  $h_1, h_2 \in \text{Ker}(\varphi)$  следует из цепочки равенств

$$\varphi(gh_1) = \varphi(g)\varphi(h_1) = \varphi(g) = \varphi(g)\varphi(h_2) = \varphi(gh_2).$$

Отображение  $\psi$  сюръективно по построению и инъективно в силу того, что  $\varphi(g) = e_F$  тогда и только тогда, когда  $g \in \text{Ker}(\varphi)$  (т.е.  $g \text{Ker}(\varphi) = \text{Ker}(\varphi)$ ). Остается проверить, что  $\psi$  – гомоморфизм:

$$\psi((g \text{Ker}(\varphi))(g' \text{Ker}(\varphi))) = \psi(gg' \text{Ker}(\varphi)) = \varphi(gg') = \varphi(g)\varphi(g') = \psi(g \text{Ker}(\varphi))\psi(g' \text{Ker}(\varphi)).$$

□

## 8 Классификация циклических групп.

**Утверждение 6.** Пусть  $G$  – циклическая группа. Тогда:

1. Если  $|G| = \infty$ , то  $G \simeq (\mathbb{Z}, +)$
2. Если  $|G| < \infty$ , то  $G \simeq (\mathbb{Z}_n, +)$

*Доказательство.* По определению, если  $G$  – циклическая, то  $G = \langle g \rangle$  для некоторого  $g \in G$ .

1.  $\varphi : \mathbb{Z} \rightarrow G, \varphi : k \mapsto g^k$   
Это гомоморфизм и биекция  $\Rightarrow$  изоморфизм.
2.  $\varphi : \mathbb{Z} \rightarrow G, \varphi : k \mapsto g^k$   
Рассмотрим, куда переходит  $k + ns$ , где  $0 \leq k \leq n - 1$   
 $k + ns \mapsto g^{k+ns} = g^k g^{ns} = g^k (g^n)^s = g^k$ .

□


## 9 Прямое произведение групп. Разложение конечной циклической группы.

### 9.1 Прямое произведение групп.

**Определение 18.** *Прямым произведением групп  $G_1, \dots, G_m$  называется множество*


$$G_1 \times \dots \times G_m = \{(g_1, \dots, g_m) \mid g_1 \in G_1, \dots, g_m \in G_m\}$$

*с операцией  $(g_1, \dots, g_m)(g'_1, \dots, g'_m) = (g_1g'_1, \dots, g_mg'_m)$ . Ясно, что эта операция ассоциативна, обладает нейтральным элементом  $(e_{G_1}, \dots, e_{G_m})$  и для каждого элемента  $(g_1, \dots, g_m)$  есть обратный элемент  $(g_1^{-1}, \dots, g_m^{-1})$ .*

 <https://youtu.be/1oceAPu3b8o>

### 9.2 Разложение конечной циклической группы.

**Определение 19.** *Группа  $G$  раскладывается в прямое произведение своих подгрупп  $H_1, \dots, H_m$ , если отображение  $H_1 \times \dots \times H_m \rightarrow G, (h_1, \dots, h_m) \mapsto h_1 \cdot \dots \cdot h_m$  является изоморфизмом.*

 <https://youtu.be/1oceAPu3b8o?t=293>

**Теорема 3.** *Пусть  $n = ml$  – разложение натурального числа  $n$  на два взаимно простых множителя. Тогда имеет место изоморфизм групп*


$$\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l.$$

*Доказательство.* Рассмотрим отображение

$$\varphi: \mathbb{Z}_n \rightarrow \mathbb{Z}_m \times \mathbb{Z}_l, \quad (k \bmod n) \mapsto (k \bmod m, k \bmod l).$$


Поскольку  $m$  и  $l$  делят  $n$ , отображение  $\varphi$  определено корректно. Ясно, что  $\varphi$  – гомоморфизм.

Далее,  $a \bmod n \in \text{Ker}(\varphi) \Rightarrow a \bmod m = 0, a \bmod l = 0 \Rightarrow a$  делится на  $m$ ,  $a$  делится на  $l$ . Так как  $\text{НОД}(m, l) = 1$ , то  $a$  делится на  $n = ml \Rightarrow a \bmod n = 0 \Rightarrow \text{Ker}(\varphi) = \{0\}$ . Следовательно, гомоморфизм  $\varphi$  инъективен. Поскольку множества  $\mathbb{Z}_n$  и  $\mathbb{Z}_m \times \mathbb{Z}_l$  содержат одинаковое число элементов, отображение  $\varphi$  биективно.  $\square$

 <https://youtu.be/1oceAPu3b8o?t=585>

**Следствие 7.** *Пусть  $n \geq 2$  – натуральное число и  $n = p_1^{k_1} \dots p_s^{k_s}$  – его разложение в произведение простых множителей (где  $p_i \neq p_j$  при  $i \neq j$ ). Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}.$$

 <https://youtu.be/1oceAPu3b8o?t=1061>


## 10 Подгруппы $p$ -крючения в абелевых группах. Разложение конечной абелевой группы в прямое произведение подгрупп $p$ -крючения.

### 10.1 Подгруппы $p$ -крючения в абелевых группах.

**Определение 20.** Пусть  $(A, +)$  – абелева группа,  $p$  – простое число. Положим


$$T_p(A) := \{a \in A \mid \exists k \geq 0 : p^k \cdot a = 0\} = \{a \in A \mid \exists m \geq 0 : \text{ord}(a) = p^m\}$$

– подгруппа в  $A$ . Тогда  $T_p(A)$  называется **подгруппой  $p$ -крючения**.

 <https://youtu.be/1oceAPu3b8o?t=1260>


### 10.2 Разложение конечной абелевой группы в прямое произведение подгрупп $p$ -крючения.

**Утверждение 7** (без доказательства). Пусть  $|A| < \infty$  и  $T_p(A) = A$  для некоторого простого  $p$ . Тогда  $A \simeq \mathbb{Z}_{p^{k_1}} \times \dots \times \mathbb{Z}_{p^{k_s}}, k_i \geq 1$ , причем число множителей и их порядки определены однозначно (с точностью до перестановки).

 <https://youtu.be/1oceAPu3b8o?t=1474>

**Утверждение 8.** Пусть  $|A| < \infty, |A| = p_1^{k_1} \times \dots \times p_s^{k_s}$  – разложение на простые множители. Тогда  $A = T_{p_1}(A) \times \dots \times T_{p_s}(A)$ .


*Доказательство.* Нужно доказать, что отображение  $\varphi : T_{p_1}(A) \times \dots \times T_{p_s}(A) \rightarrow A, (a_1, \dots, a_s) \mapsto a_1 + \dots + a_s$  является изоморфизмом. Ясно, что  $\varphi$  – гомоморфизм. Докажем инъективность. Пусть  $(a_1, \dots, a_s) \in T_{p_1}(A) \times \dots \times T_{p_s}(A)$ , такое что  $a_1 + \dots + a_s = 0$ . Для любого  $i, 1 \leq i \leq s$   $\text{ord}(a_i) = p_i^{m_i}, m_i \geq 0$ . При фиксированном  $i$  умножим  $a_1 + \dots + a_s = 0$  на  $n_i = p_1^{m_1} \cdot \dots \cdot p_{i-1}^{m_{i-1}} \cdot p_{i+1}^{m_{i+1}} \cdot \dots \cdot p_s^{m_s}$  и получим  $n_i \cdot a_i = 0$ . Следовательно,  $n_i$  делится на  $p_i^{m_i} \Rightarrow m_i = 0 \Rightarrow \text{ord}(a_i) = 1 \Rightarrow a_i = 0 \Rightarrow \text{Ker}(\varphi) = 0$ . Докажем сюръективность.  $a \in A \Rightarrow \text{ord}(a) = p_1^{m_1} \cdot \dots \cdot p_s^{m_s}$  по следствию 7 о разложении конечной циклической группы.  $\langle a \rangle = \langle b_1 \rangle \times \dots \times \langle b_s \rangle$ , где  $b_i \in \langle a \rangle$  и  $\text{ord}(b_i) = p_i^{m_i} \Rightarrow a = a_1 + \dots + a_s$ , где  $a_i \in \langle b_i \rangle \subseteq T_{p_i}(A)$ .  $\square$

 <https://youtu.be/1oceAPu3b8o?t=1635>

## 11 Примарные абелевы группы. Теорема о строении конечных абелевых групп, доказательство единственности.

### 11.1 Примарные абелевы группы.

**Определение 21.** Конечная абелева группа  $A$  называется **примарной**, если  $|A| = p^k$  для некоторого простого  $p$ .

 <https://youtu.be/1oceAPu3b8o?t=2379>


### 11.2 Теорема о строении конечных абелевых групп, доказательство единственности.

**Теорема 4.** Пусть  $|A| < \infty$  – конечная абелева группа. Тогда  $A \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}$ , где  $p_i$  – (не обязательно различные) простые числа ( $k_i \geq 1$ ), причем в этом разложении число примарных циклических множителей и их порядки (с точностью до перестановки) определены однозначно.

*Доказательство.* Существование следует из утверждений 7 и 8. Докажем единственность. Зафиксируем простое  $p$ . Тогда в разложении  $A \simeq \mathbb{Z}_{p_1^{k_1}} \times \dots \times \mathbb{Z}_{p_s^{k_s}}$

$$\prod_{p_i=p} \mathbb{Z}_{p_i^{k_i}} \subseteq T_p(A).$$


Пусть  $a \in A$ . Тогда  $a = (n_1, \dots, n_s)$ ,  $n_i \in \mathbb{Z}_{p_i^{k_i}}$ . Если  $p^k \cdot a = 0$  для некоторого  $k$ , то для любого  $i$   $p^k \cdot n_i$  делится на  $p_i^{k_i}$ . Если  $p \neq p_i$ , то  $n_i$  делится на  $p_i^{k_i} \Rightarrow n_i \equiv 0 \pmod{p_i^{k_i}} \Rightarrow a \in T_p(A) \Leftrightarrow$  для любого  $i$  с условием  $p \neq p_i$   $n_i = 0$  в  $\mathbb{Z}_{p_i^{k_i}} \Rightarrow T_p(A) \subseteq \prod_{p_i=p} \mathbb{Z}_{p_i^{k_i}}$ . Итог: достаточно доказать единственность каждого  $T_p(A)$ . Теперь пусть  $B = T_p(A) \simeq \mathbb{Z}_{p^{m_1}} \times \dots \times \mathbb{Z}_{p^{m_r}}$ . Индукция по  $|B|$ . База:  $|B| = p \Rightarrow$  по следствию 4 из теоремы Лагранжа  $B \simeq \mathbb{Z}_p$ . Теперь пусть  $|B| > p$ ,  $|B| = p^m$ , где  $m = m_1 + \dots + m_r$ . Рассмотрим подгруппу  $pB \subseteq B$ , где  $pB = \{pb \mid b \in B\} \Rightarrow pB \simeq \mathbb{Z}_{p^{m_1-1}} \times \dots \times \mathbb{Z}_{p^{m_r-1}}$ , в частности  $|pB| < |B|$ . Если  $m_i = 1$ , то соответствующий множитель исчезает. По предположению индукции набор ненулевых чисел среди  $m_1 - 1, \dots, m_r - 1$  определен однозначно с точностью до перестановки. Следовательно, однозначно восстанавливаются все  $m_i$  с условием  $m_i > 1$ . Число  $m_i = 1$  однозначно восстанавливается из условия  $m_1 + \dots + m_r = m$ .  $\square$

 <https://youtu.be/1oceAPu3b8o?t=2507>

## 12 Экспонента конечной абелевой группы и критерий цикличности.

**Определение 22.** Пусть  $A$  – конечная абелева группа. *Экспонента* группы  $A$  – это число


$$\exp(A) = \text{НОК}\{\text{ord}(a) \mid a \in A\} = \min\{n \in \mathbb{N} \mid na = 0 \forall a \in A\}$$

 <https://youtu.be/1oceAPu3b8o?t=3792>

**Утверждение 9.** Пусть  $A$  – конечная абелева группа. Тогда  $\exp(A) = |A| \Leftrightarrow A$  – циклическая группа.

*Доказательство.*  $\Leftarrow A$  – циклическая  $\Rightarrow A \simeq \mathbb{Z}_n \Rightarrow \text{ord}(a) = n = |A| \Rightarrow \exp(A) = |A|$

$\Rightarrow \exp(A) = |A|$  Знаем, что  $A \simeq T_{p_1}(A) \times \dots \times T_{p_s}(A)$ , где  $|A| = p_1^{k_1} \cdot \dots \cdot p_s^{k_s}$ . Пусть  $b_i \in T_{p_i}(A)$  – элемент наибольшего порядка  $\Rightarrow \text{ord}(b_i) = p_i^{m_i}$ . Тогда для любого  $a_i \in T_{p_i}(A), \dots, a_s \in T_{p_s}(A)$  получаем  $\text{ord}(a_i) = p_i^{l_i}$ , где  $l_i \leq m_i$ .  $\text{ord}(a_1 + \dots + a_s) = \text{ord}(a_1) \cdot \dots \cdot \text{ord}(a_s)$  делит  $\text{ord}(b_1) \cdot \dots \cdot \text{ord}(b_s) = \text{ord}(b_1 + \dots + b_s)$ . Следовательно,  $\exp(A) = \text{ord}(b_1 + \dots + b_s) \Rightarrow |A| = \exp(A) = |\langle b_1 + \dots + b_s \rangle| \Rightarrow \langle b_1 + \dots + b_s \rangle = A \Rightarrow A$  – циклическая группа.  $\square$

 <https://youtu.be/1oceAPu3b8o?t=4028>



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

Пусть у нас есть  $G$  – конечная абелева группа. И также есть элемент  $g \in G$ , для которого  $\text{ord}(g)$  будет достаточно большим значением.


### 13.1 Задача дискретного логарифмирования.

Дано:  $h \in \langle g \rangle$ . Найти такое  $\alpha$ , что  $g^\alpha = h$ . Возведение в степень – задача более простая с технической стороны реализации. Существует алгоритм бинарного возведения в степень:  $g^{16} = (((g^2)^2)^2)^2$ . Задача нахождения степени решается только перебором или близким к перебору способом.

 <https://youtu.be/1oceAPu3b8o?t=4480>

### 13.2 Система Диффи-Хеллмана обмена ключами.

Группа  $G$  и некоторый ее элемент  $g$  известны всем, причем  $g$  имеет достаточно большой порядок. Пусть есть два пользователя системы –  $A$  и  $B$ .  $A$  фиксирует свое секретное  $\alpha \in \mathbb{N}$  и сообщает всем пользователям  $g^\alpha$ .  $B$  совершает аналогичные действия: фиксирует  $\beta \in \mathbb{N}$  и сообщает всем пользователям  $g^\beta$ . Теперь  $A$  и  $B$  опять совершают аналогичные действия – каждый из них возводит элемент другого в свою секретную степень, они оба получают элемент  $g^{\alpha\beta}$ , который известен только им двоим. Теперь по этому ключу можно устроить зашифрованный канал связи, к которому никто не имеет доступа. В силу сложности задачи дискретного логарифмирования по  $g^\alpha$  и  $g^\beta$  нельзя быстро получить  $g^{\alpha\beta}$ .

 <https://youtu.be/mNd30oeCugc?t=78>

### 13.3 Криптосистема Эль-Гамала.

Группа  $G$  и некоторый ее элемент  $g$  известны всем, причем  $g$  имеет достаточно большой порядок. Пусть есть два пользователя системы –  $A$  и  $B$ .  $A$  фиксирует свое секретное  $\alpha \in \mathbb{N}$  и сообщает всем пользователям  $g^\alpha$ .  $B$  хочет передать для  $A$  элемент  $h \in G$ . Для этого  $B$  фиксирует какое-то  $k \in \mathbb{N}$  и объявляет пару  $\{g^k, h \cdot (g^\alpha)^k\}$ .

 <https://youtu.be/mNd30oeCugc?t=360>

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

### 14.1 Кольца.

**Определение 23.** *Кольцо* (ассоциативное кольцо с единицей) – это множество  $R$  с двумя бинарными операциями: сложение и умножение, удовлетворяющее следующим условиям

1.  $(R, +)$  – абелева группа
2. для любых  $a, b, c \in R$  выполняется  $a(b+c) = ab+ac$  (левая дистрибутивность) и  $(a+b)c = ac+bc$  (правая дистрибутивность)
3. для любых  $a, b, c \in R$  выполняется  $(ab)c = a(bc)$  (ассоциативность умножения)
4. существует  $1 \in R$  такая что  $1 \cdot a = a \cdot 1 = a$  для любого  $a \in R$

 <https://youtu.be/mNd30oeCugc?t=690>

### 14.2 Коммутативные кольца.

**Определение 24.** Кольцо  $R$  называется **коммутативным**, если  $ab = ba$  для любых  $a, b \in R$ .

 <https://youtu.be/mNd30oeCugc?t=1287>

### 14.3 Обратимые элементы, делители нуля и нильпотенты.

**Определение 25.** Пусть  $R$  – кольцо. Элемент  $a \in R$  называется обратимым, если существует такое  $b \in R$ , что  $ab = ba = 1$ .

**Определение 26.** Пусть  $R$  – кольцо. Элемент  $a \in R$  называется левым (правым) **делителем нуля**, если  $a \neq 0$  и существует  $b \in R \setminus \{0\}$ , такое что  $ab = 0$  ( $ba = 0$ ).

**Определение 27.** Пусть  $R$  – кольцо. Элемент  $a \in R$  называется **нильпотентным** (нильпотентом), если  $a \neq 0$  и существует такое  $n \in \mathbb{N}$ , что  $a^n = 0$ .

 <https://youtu.be/mNd30oeCugc?t=1374>

### 14.4 Примеры колец.

1.  $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$
2.  $\mathbb{Z}_n$  – кольцо вычетов
3.  $M_n(\mathbb{R})$  – кольцо матриц
4.  $\mathbb{R}[x]$  – кольцо многочленов от переменной  $x$  с коэффициентами из  $\mathbb{R}$

 <https://youtu.be/mNd30oeCugc?t=1115>

### 14.5 Поля.

**Определение 28.** *Поле* – это коммутативное (ассоциативное) кольцо (с единицей), в котором  $0 \neq 1$  и всякий ненулевой элемент обратим.

 <https://youtu.be/mNd30oeCugc?t=2243>

## 14.6 Критерий того, что кольцо вычетов является полем.


**Утверждение 10.** Пусть  $n \in \mathbb{N}$ . Тогда  $\mathbb{Z}_n$  – поле  $\Leftrightarrow n$  – простое число.

*Доказательство.*  $\Rightarrow n = 1 \Rightarrow \mathbb{Z}_n = \{0\}$  – не поле.

$n > 1$  и  $n$  составное  $\Rightarrow n = ml$ , где  $1 < m < n, 1 < l < n \Rightarrow$  в кольце  $\mathbb{Z}_n ml = 0 \Rightarrow$  есть делители 0  $\Rightarrow$  не поле.

$\Leftarrow n = p$  – простое,  $a \in \mathbb{Z}$ ,  $\text{НОД}(a, p) = 1 \Rightarrow$  существуют  $k, l \in \mathbb{Z}$ , такие что  $ak + pl = 1 \Rightarrow ak = 1 \Rightarrow$  любой ненулевой элемент обратим.

□

 <https://youtu.be/mNd30oeCugc?t=2484>

## 15 Идеалы колец. Факторкольцо кольца по идеалу. Гомоморфизмы и изоморфизмы колец. Ядро и образ гомоморфизма колец. Теорема о гомоморфизме колец.

### 15.1 Идеалы колец.

**Определение 29.** Пусть  $R$  – кольцо. Подмножество  $I \subseteq R$  называется идеалом, если


1.  $I$  – подгруппа в  $R$  по сложению

2.  $\forall r \in R, a \in I : ar, ra \in I$

Обозначение:  $I \triangleleft R$ .

В каждом кольце  $R$  есть **несобственные идеалы**  $I = \{0\}$  и  $I = R$ . Все остальные идеалы называются **собственными**.

**Определение 30.** Идеал  $I$  называется **главным**, если существует такой элемент  $a \in R$ , что  $I = (a)$ . (В этой ситуации говорят, что  $I$  порожден элементом  $a$ .)

 <https://youtu.be/mNd30oeCugc?t=3367>

### 15.2 Факторкольцо кольца по идеалу.

Пусть  $R$  – кольцо,  $I \triangleleft R$ ,  $R/I$  – факторгруппа по сложению. Введем на  $R/I$  операцию умножения по формуле  $(a + I)(b + I) = ab + I$ .


**Утверждение 11.** Указанная выше операция корректна.

*Доказательство.*  $a + I = a' + I, b + I = b' + I \Rightarrow a' = a + x, b' = b + y$ , где  $x, y \in I$ .

$$(a' + I)(b' + I) = a'b' + I = (a + x)(b + y) + I = ab + ay + xb + xy + I = ab + I \text{ (т.к. } ay, xb, xy \in I).$$

Ясно, что  $R/I$  – кольцо. □


**Определение 31.**  $R/I$  называется **факторкольцом** кольца  $R$  по идеалу  $I$ .

 <https://youtu.be/mNd30oeCugc?t=3984>

### 15.3 Гомоморфизмы и изоморфизмы колец.

**Определение 32.** Пусть  $R, S$  – кольца. Отображение  $\varphi : R \rightarrow S$  называется **гомоморфизмом**, если  $\varphi(a + b) = \varphi(a) + \varphi(b)$  и  $\varphi(ab) = \varphi(a)\varphi(b)$  для любых  $a, b \in R$ .

**Определение 33.** Пусть  $R, S$  – кольца. Гомоморфизм  $\varphi : R \rightarrow S$  называется **изоморфизмом**, если  $\varphi$  – биекция.


 <https://youtu.be/mNd30oeCugc?t=3152>

### 15.4 Ядро и образ гомоморфизма колец.

Пусть  $\varphi : R \rightarrow S$  – гомоморфизм колец.

**Определение 34.** Множество  $\text{Ker}(\varphi) = \{a \in R \mid \varphi(a) = 0\}$  называется **ядром** гомоморфизма  $\varphi$ .

**Определение 35.** Множество  $\text{Im}(\varphi) = \varphi(R)$  называется **образом** гомоморфизма  $\varphi$ .

 <https://youtu.be/mNd30oeCugc?t=4420>

## 15.5 Теорема о гомоморфизме колец.

**Теорема 5.** Если  $\varphi : R \rightarrow S$  – гомоморфизм колец, то  $R/\text{Ker}(\varphi) \simeq \text{Im}(\varphi)$ .


*Доказательство.* Пусть  $I = \text{Ker}(\varphi)$ .

$$\psi : R/I \rightarrow \text{Im}(\varphi), r + I \mapsto \varphi(r)$$

Из теоремы о гомоморфизме групп известно, что  $\psi$  – изоморфизм групп  $(R/I, +)$  и  $(\text{Im}(\varphi), +)$ . Осталось проверить, что  $\psi$  – гомоморфизм колец:

$$\psi((a + I)(b + I)) = \psi(ab + I) = \varphi(ab) = \varphi(a)\varphi(b) = \psi(a + I)\psi(b + I).$$

□

 <https://youtu.be/YdjrTEepVpg>


## 16 Делимость и ассоциированные элементы в коммутативных кольцах без делителей нуля. Наибольший общий делитель. Кольца главных идеалов. Существование наибольшего общего делителя и его линейного выражения в кольце главных идеалов.

### 16.1 Делимость и ассоциированные элементы в коммутативных кольцах без делителей нуля.

Пусть  $R$  – коммутативное кольцо без делителей нуля,  $a, b \in R$ .


**Определение 36.** Говорят, что  $b$  делит  $a$  (« $a$  делится на  $b$ », « $b$  делитель  $a$ »), если  $a = bc$  для некоторого  $c \in R$ .

**Определение 37.** Говорят, что  $a$  и  $b$  ассоциированы, если  $a = bc$ , где  $c \in R$  – обратимый элемент.

 <https://youtu.be/YdjrTEepVpg?t=343>


### 16.2 Наибольший общий делитель.

**Определение 38.** Наибольший общий делитель элементов  $a$  и  $b$  – это их общий делитель, который делится на любой другой общий делитель. Обозначение:  $(a, b)$ .

 <https://youtu.be/YdjrTEepVpg?t=879>

### 16.3 Кольца главных идеалов.

**Определение 39.**  $R$  называется **кольцом главных идеалов**, если всякий идеал в  $R$  является главным.

 <https://youtu.be/YdjrTEepVpg?t=1253>

### 16.4 Существование наибольшего общего делителя и его линейного выражения в кольце главных идеалов.

**Теорема 6.** Пусть  $R$  – кольцо главных идеалов. Тогда для любых  $a, b \in R$

1. Существует наибольший общий делитель  $(a, b)$ .
2.  $(a, b) = au + bv$  для некоторых  $u, v \in R$ .

**Доказательство.** Рассмотрим идеал  $I = \{ax + by \mid x, y \in R\}$ . Заметим, что  $a = a \cdot 1 + b \cdot 0 \in I$  и  $b = a \cdot 0 + b \cdot 1 \in I$ . Так как  $R$  – кольцо главных идеалов, то существует  $d \in R$ , такое что  $I = (d)$ . Следовательно,  $a$  делится на  $d$  и  $b$  делится на  $d$ , т.е.  $d$  общий делитель  $a$  и  $b$ .  $d \in I \Rightarrow d = au + bv$  для некоторых  $u, v \in R$ . Если  $d'$  – какой-то общий делитель  $a$  и  $b$ , то  $d'$  делит  $d$ . Таким образом,  $d$  – наибольший общий делитель  $a$  и  $b$ .  $\square$

 <https://youtu.be/YdjrTEepVpg?t=1435>

## 17 Деление с остатком в кольце многочленов от одной переменной над полем. Теорема о том, что это кольцо является кольцом главных идеалов.

Пусть  $K$  – поле,  $K[x]$  – кольцо многочленов от переменной  $x$ .

### 17.1 Деление с остатком в кольце многочленов от одной переменной над полем.

**Теорема 7.** Для любого  $f \in K[x]$  и  $g \in K[x] \setminus \{0\}$  существуют единственные  $q, r \in K[x]$ , такие что


1.  $f = q \cdot g + r$
2. либо  $r = 0$  либо  $\deg(r) < \deg(g)$

При этом  $q$  – **неполное частное**, а  $r$  – **остаток**.

*Доказательство.* Докажем существование индукцией по  $\deg(f) = n$ . Если  $f = 0$ , то можно взять  $q = r = 0$ . Пусть теперь  $n > 0$ . Если  $n < \deg(g)$ , то можно взять  $q = 0, r = f$ . Остался случай  $n \geq \deg(g)$ .

$$f = a_n x^n + \dots + a_1 x + a_0, \quad g = b_m x^m + \dots + b_1 x + b_0 \quad a_n \neq 0 \neq b_m$$


Положим  $h = f - \frac{a_n}{b_m} x^{n-m} \cdot g$ . Тогда  $\deg(h) < n$ . Следовательно, по предположению индукции  $h = q \cdot g + r$ , где либо  $r = 0$  либо  $\deg(r) < \deg(g)$ . Тогда  $f = h + \frac{a_n}{b_m} x^{n-m} \cdot g = \left(q + \frac{a_n}{b_m} x^{n-m}\right) \cdot g + r$ . Докажем единственность. Пусть  $q_1 \cdot g + r_1 = q_2 \cdot g + r_2$ , где  $\forall i$  либо  $r_i = 0$  либо  $\deg(r_i) < \deg(g)$ . Тогда  $(q_1 - q_2) \cdot g = r_2 - r_1$ . Если  $q_1 \neq q_2$ , то  $\deg((q_1 - q_2)g) \geq \deg(g) > \deg(r_2 - r_1) = \deg((q_1 - q_2)g)$  – противоречие. Таким образом,  $q_1 = q_2$  и  $r_1 = r_2$ .  $\square$

 <https://youtu.be/YdjrTEepVpg?t=3216>

### 17.2 Теорема о том, что это кольцо является кольцом главных идеалов.

**Теорема 8.**  $K[x]$  – кольцо главных идеалов.

*Доказательство.* Пусть  $I \triangleleft K[x]$ . Если  $I = \{0\}$ , то  $I = (0)$  – главный идеал. Пусть  $I \neq \{0\}$ . Возьмем в  $I \setminus \{0\}$  элемент  $g$  наименьшей степени. Тогда  $(g) \subseteq I$ . Пусть теперь  $f \in I$ . Разделим  $f$  на  $g$  с остатком  $f = q \cdot g + r$ , где  $r = 0$  или  $\deg(r) < \deg(g)$ . Тогда  $r = f - q \cdot g \in I$  (т.к.  $f \in I$  и  $q \cdot g \in I$ ). В силу минимальности  $\deg(g)$  получаем  $r = 0 \Rightarrow f = q \cdot g \in (g) \Rightarrow I \subseteq (g) \Rightarrow I = (g)$ .  $\square$

 <https://youtu.be/YdjrTEepVpg?t=4017>

## 18 Простые элементы. Факториальные кольца. Факториальность кольца многочленов от одной переменной над полем. (todo)


### 18.1 Простые элементы.

**Определение 40.** Элемент  $p \in R$  называется **простым**, если  $p$  необратим и его нельзя представить в виде  $p = ab$ , где  $a, b \in R$  необратимы.

 <https://youtu.be/YdjrTEepVpg?t=1859>

### 18.2 Факториальные кольца.

**Определение 41.** Пусть  $R$  – коммутативное кольцо без делителей 0.  $R$  называется **факториальным кольцом**, если любой ненулевой необратимый элемент  $a \in R$  представим в виде  $a = p_1 \cdot \dots \cdot p_n$ , где  $p_i$  – простое, причем такое разложение определено однозначно с точностью до перестановки множителей и ассоциированности.

 <https://youtu.be/YdjrTEepVpg?t=2446>

### 18.3 Факториальность кольца многочленов от одной переменной над полем.

— 



**19** Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов. (todo)

**19.1** Лексикографический порядок на множестве одночленов от нескольких переменных.

—

**19.2** Лемма о конечности убывающих цепочек одночленов.

—

**20** Лексикографический порядок на множестве одночленов от нескольких переменных. Лемма о конечности убывающих цепочек одночленов. (todo)

**20.1** Лексикографический порядок на множестве одночленов от нескольких переменных.

—

**20.2** Лемма о конечности убывающих цепочек одночленов.

—

**21** Остаток многочлена относительно заданной системы многочленов. Системы Гребнера. Характеризация систем Гребнера в терминах цепочек элементарных редукций. (todo)

**21.1** Остаток многочлена относительно заданной системы многочленов.

—

**21.2** Системы Гребнера.

—

**21.3** Характеризация систем Гребнера в терминах цепочек элементарных редукций.

—

## 22 S-многочлены. Критерий Бухбергера. (todo)

### 22.1 S-многочлены.

—

### 22.2 Критерий Бухбергера.

—

**23** Базис Гребнера идеала в кольце многочленов от нескольких переменных, теорема о трех эквивалентных условиях. Решение задачи вхождения многочлена в идеал. (todo)

**23.1** Базис Гребнера идеала в кольце многочленов от нескольких переменных, теорема о трех эквивалентных условиях.

—

**23.2** Решение задачи вхождения многочлена в идеал.

—

24 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих. Алгоритм Бухбергера построения базиса Гребнера идеала. (todo)

24.1 Лемма о конечности цепочек одночленов, в которых каждый следующий одночлен не делится ни на один из предыдущих.

—

24.2 Алгоритм Бухбергера построения базиса Гребнера идеала.

—

25 Редуцируемость к нулю  $S$ -многочлена двух многочленов с взаимно простыми старшими членами. (todo)

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

**26.1** Характеристика поля.

—

**26.2** Расширение полей.

—

**26.3** Конечное расширение и его степень.

—

**26.4** Степень композиции двух расширений.

—



27 Критерий того, что факторкольцо кольца многочленов от одной переменной над полем является полем. Степень расширения этого поля. (todo)

27.1 Критерий того, что факторкольцо кольца многочленов от одной переменной над полем является полем.

—

27.2 Степень расширения этого поля.

—

28    Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители. Поле разложения многочлена. (todo)

28.1    Существование конечного расширения исходного поля, в котором заданный многочлен (а) имеет корень; (б) разлагается на линейные множители.

—

28.2    Поле разложения многочлена.

—

**29** Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства. (todo)

**29.1** Алгебраические и трансцендентные элементы.

—

**29.2** Минимальный многочлен алгебраического элемента и его свойства.

—

30 Подполе в расширении полей, порожденное алгебраическим элементом. (todo)

—

## 31 Порядок конечного поля. Автоморфизм Фробениуса. (todo)

### 31.1 Порядок конечного поля.

—

### 31.2 Автоморфизм Фробениуса.

—

## 32 Теорема существования и единственности для конечных полей. (todo)

—

### 33 Цикличность мультипликативной группы конечного поля и неприводимые многочлены над $\mathbb{Z}_p$ (todo)

—

## 34 Подполя конечного поля. (todo)

—



35 Коды над конечным алфавитом. Расстояние Хэмминга. Минимальное расстояние кода. Коды, исправляющие  $t$  ошибок: определение и эквивалентные переформулировки. Код с повторением. (todo)

35.1 Коды над конечным алфавитом.

—

35.2 Расстояние Хэмминга.

—

35.3 Минимальное расстояние кода.

—

35.4 Коды, исправляющие  $t$  ошибок: определение и эквивалентные переформулировки.

—

35.5 Код с повторением.

—

36 Линейные коды. Проверочная матрица. Связь минимального расстояния линейного кода с его проверочной матрицей. Бинарный код Хэмминга, его минимальное расстояние и число ошибок, которое он может исправлять. (todo)

36.1 Линейные коды.

—

36.2 Проверочная матрица.

—

36.3 Связь минимального расстояния линейного кода с его проверочной матрицей.

—

36.4 Бинарный код Хэмминга, его минимальное расстояние и число ошибок, которое он может исправлять.

—

## 37 Коды БЧХ. Теорема о количестве ошибок, исправляемых кодом БЧХ. Оценка на размерность кода БЧХ. (todo)

### 37.1 Коды БЧХ.

—

### 37.2 Теорема о количестве ошибок, исправляемых кодом БЧХ.

—

### 37.3 Оценка на размерность кода БЧХ.

—