Алгебра

Содержание

Вопрос 1

1.1 Бинарные операции.

Пусть M — некоторое множество.

Определение:

Бинарная операция на множестве M это отображение $\circ : M \times M \to M$, $(a, b) \mapsto a \circ b$.

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

Классические примеры с бинарной операцией, знакомые со школы, — это операция сложение(+) и умножение($\times$) на множестве $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$.

1.2 Полугруппы, моноиды и группы.

Пусть $(M, \circ)$ — множество с бинарной операцией.

Определение:

I. $(M, \circ)$ называется *группой*, если выполнены следующие три условия(аксиомы):

  (1) $(a \circ b) \circ c = a \circ (b \circ c)$ $\forall a, b, c \in M$(*ассоциативность*);

  (2) существует *нейтральный элемент*, то есть такой $e \in M$, что $e \circ a = a \circ e = a$, $\forall a \in M$;

  (3) для всякого $a \in M$ существует *обратный элемент*, то есть такой $b \in M$, что $a \circ b = b \circ a = e$.

II. Если требуется выполнение только условия (1), то $(M, \circ)$ называется *полугруппой.*

III. Если требуется выполнение только условий (1) и (2), то $(M, \circ)$ называется *моноидом.*

Примеры для II и III:

$(\mathbb{N}, +)$ — это полугруппа, но не моноид.

$(\mathbb{N} \cup \{0\}, +)$ — моноид, но не группа.

Замечание:

1. Ассоциативность довольно редкое свойство.
   Примеры неассоциативных бинарных операций: $M = \mathbb{Z}, a \circ b := a - b$ или $M = \mathbb{N}, a \circ b := a^b$.

2. Нейтральный элемент в моноиде (и группе) единствен: если $e_1, e_2 \in M$ — два нейтральных элемента, то $e_1 = e_1 \circ e_2 = e_2$.

3. Обратный элемент в группе единствен: если b_1, b_2 — два обратных к a элемента, то

$$b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2.$$

   Ввиду единственности обратный к a элемент обозначается символом a^{-1}.

4. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$:

$$(a \circ b) \circ (b^{-1} \circ a^{-1}) = a \circ (b \circ b^{-1}) \circ a^{-1} = a \circ e \circ a^{-1} = a \circ a^{-1} = e.$$

Соглашение: вместо $(G, \circ)$ будем писать G, вместо $a \circ b$ будем писать ab и операцию $\circ$ будем называть умножением.

1.3 Коммутативные группы.

Определение:

Группа G называется *коммутативной* (или *абелевой*), если $ab = ba$ для всех $a, b \in G$.

При работе с абстрактными группами для обозначения групповой операции, нейтрального и обратного элементов принято использовать *мультипликативную запись*: ab, e, a^{-1}. Однако в теории абелевых групп употребляется *аддитивная запись*: $a+b$, 0, $-a$ (при этом сама операция называется сложением).

1.4 Примеры групп.

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

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

3) Группы матриц (с операцией умножения):

$\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) \mid \det A \neq 0\}$ — полная линейная группа;

$\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{M}_n(\mathbb{R}) \mid \det A = 1\}$ — специальная линейная группа.

4) Группы перестановок (с операцией композиции):

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

знакопеременная группа A_n — все четные перестановки длины n, $|A_n| = n!/2$.

1.5 Порядок группы.

Определение:

Порядком группы G называется число элементов в ней.

Группа называется *конечной*, если ее порядок конечен, и *бесконечной* иначе.

Обозначение: $|G|$.

1.6 Подгруппы.

Определение:

Подмножество H группы G называется *подгруппой*, если

1) $e \in H$;

2) $a, b \in H \Longrightarrow ab \in H$;

3) $a \in H \Longrightarrow a^{-1} \in H$;

В каждой группе есть *несобственные* подгруппы $H = \{e\}$ и $H = G$.

Остальные подгруппы называются *собственными*.

1.7 Описание всех подгрупп в группе $(\mathbb{Z}, +)$.

Предложение:

Всякая подгруппа в $(\mathbb{Z}, +)$ имеет вид $k\mathbb{Z}$ для некоторого $k \geqslant 0$.

Доказательство:

Пусть $H \subseteq \mathbb{Z}$ — некоторая подгруппа. Если $H = \{0\}$, то $H = 0 \cdot \mathbb{Z}$. Далее считаем $H \neq \{0\}$. По определению подгруппы для всякого $x \in H$ имеем $-x \in H$, поэтому множество $H \cap \mathbb{N}$ не пусто, и мы положим $k = \min(H \cap \mathbb{N})$. Тогда опять же по определению подгруппы получаем $k\mathbb{Z} \subseteq H$. Пусть теперь $a \in H$ — произвольный элемент. Поделим его на k с остатком: $a = qk + r$, $0 \leqslant r < k$. Снова воспользовавшись определением подгруппы, мы получаем $r = a - qk \in H$, откуда в силу минимальности k вытекает $r = 0$ и $a \in k\mathbb{Z}$. Значит, $k\mathbb{Z} = H$. $\square$

Вопрос 2

2.1 Подгруппы.

Пусть G — группа, $g \in G$ и $n \in \mathbb{Z}$. Определим n-ю степень g^n следующим образом:

$$g^n := \begin{cases} \underbrace{g \cdot \ldots \cdot g}_{n}, & \text{если } n > 0; \\ e, & \text{если } n = 0; \\ \underbrace{g^{-1} \cdot \ldots \cdot g^{-1}}_{|n|}, & \text{если } n < 0. \end{cases}$$

Замечание:

Если G — абелева группа с операцией сложения, то в аддитивной записи определенная выше «n-я степень» элемента $g \in G$ будет не чем иным, как ng (то есть кратным элемента g).

Свойства:

1) $g^n g^m = g^{n+m}$:

$$g^n g^m = \underbrace{g \cdot \ldots \cdot g}_{n} \cdot \underbrace{g \cdot \ldots \cdot g}_{m} = \underbrace{g \cdot \ldots \cdot g}_{m+n} = g^{n+m};$$

2) $(g^n)^{-1} = g^{-n}$:

$$g^n \cdot g^{-n} = g^{n-n} = g^0 = e;$$

3) $(g^m)^n = g^{mn}$:

$$(g^m)^n = (\underbrace{g \cdot \ldots \cdot g}_{m})^n = \underbrace{\underbrace{g \cdot \ldots \cdot g}_{m} \cdot \ldots \cdot \underbrace{g \cdot \ldots \cdot g}_{m}}_{n} = g^{mn}.$$

Для каждого $g \in G$ положим $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$. В силу упомянутых выше свойств $\langle g \rangle$ является подгруппой в G.

2.2 Циклические подгруппы.

Определение:

Подгруппа $\langle g \rangle$ называется *циклической подгруппой* в G, порождаемой элементом g. При этом g называется *образующим* или *порождающим* элементом для $\langle g \rangle$.

Пример:

$2\mathbb{Z} \in \mathbb{Z}$ — циклическая подгруппа, $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Замечание:

Циклическая подгруппа $\langle g \rangle$ всегда коммутативна.

2.3 Циклические группы.

Определение:

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

Пример:

Группы $(\mathbb{Z}, +), (\mathbb{Z}_n, +)$ при $n \geqslant 1$ являются циклическими.

Замечание:

Если G — циклическая группа, то G коммутативна и не более чем счётна.

2.4 Порядок элемента.

Пусть G — группа и $g \in G$. Рассмотрим множество $M(g) = \{n \in \mathbb{N} \mid g^n = e\}$.

Определение:

Порядок элемента g — это величина

$$\operatorname{ord}(g) := \begin{cases} \min M(g), & \text{если } M(g) \neq \varnothing; \\ \infty, & \text{если } M(g) = \varnothing. \end{cases}$$

Замечание:

$\operatorname{ord}(g) = 1 \iff g = e.$

2.5 Связь между порядком элемента и порядком порождаемой им циклической подгруппы.

Предложение:

$\operatorname{ord}(g) = |\langle g \rangle|.$

Доказательство:

Пусть $k, s \in \mathbb{Z}$, такие что $g^k = g^s$. Тогда домножая обе части равенства на g^{-s}, получаем, что

$$g^k = g^s \iff g^{k-s} = e. \tag{$*$}$$

Далее рассмотрим два случая.

1) Если $\operatorname{ord}(g) = \infty$, то нет таких двух различных чисел $k, s \in \mathbb{Z}$, что $g^{k-s} = e$, а значит, в силу $(*)$ все элементы в подгруппе различны $\implies |\langle g \rangle| = \infty$.

2) Если $\operatorname{ord}(g) = m < \infty$, то элементы $e = g^0, g = g^1, g^2, \ldots, g^{m-1}$ попарно различны в силу $(*)$.

   Покажем, что эти элементы исчерпывают всю группу $\langle g \rangle$. Возьмем произвольное $n \in \mathbb{Z}$ и разделим его на m с остатком: $n = qm + r,\ 0 \leqslant r < m$. Тогда $g^n = g^{qm} \cdot g^r = (g^m)^q \cdot g^r = e^q \cdot g^r = e \cdot g^r = g^r$.

   Получили, что всякий элемент из $\langle g \rangle$ принадлежит $\{e, g, g^2, \ldots, g^{m-1}\} \implies \langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$, значит, $|\langle g \rangle| = m$.

$\square$

Вопрос 3

3.1 Смежные классы.

Пусть теперь G — группа, $H \subseteq G$ — подгруппа. Определим на G отношение L_H следующим образом: $(a, b) \in L_H \iff a^{-1}b \in H$.

Предложение:

L_H — отношение эквивалентности.

Доказательство:

Проверим все необходимые свойства, они вытекают аккурат из определения подгруппы.

1. Рефлексивность: $a^{-1}a = e \in H$.
2. Симметричность: $a^{-1}b \in H \implies b^{-1}a = (a^{-1}b)^{-1} \in H$.
3. Транзитивность: $a^{-1}b \in H, b^{-1}c \in H \implies a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

□

Теперь заметим, что $a^{-1}b \in H \iff b \in aH$, поэтому класс эквивалентности элемента $a \in G$ для отношения L_H совпадает с множеством aH.

Определение:

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

Из предложения и общих фактов об отношениях эквивалентности вытекает, что группа G разбивается в объединение попарно непересекающихся левых смежных классов по подгруппе H.

Следующая лемма показывает, что в случае конечной подгруппы H все левые смежные классы содержат одинаковое число элементов, равное $|H|$.

Лемма:

Если $|H| < \infty$, то $|aH| = |H|$ для всех $a \in G$.

Доказательство:

Из определения следует, что $|aH| \leqslant |H|$. Если $ah_1 = ah_2$ для каких-то $h_1, h_2 \in H$, то, умножая на a^{-1} слева, получаем $h_1 = h_2$, откуда $|aH| = |H|$. □

3.2 Индекс подгруппы.

Определение:

Индекс подгруппы H в группе G — это число левых смежных классов G по H.

Обозначение: $[G : H]$.

Отметим, что индекс подгруппы — это либо натуральное число, либо бесконечность.

3.3 Теорема Лагранжа.

Теорема:

Пусть G — конечная группа, $H \subseteq G$ — подгруппа, тогда $|G| = |H| \cdot [G : H]$.

Доказательство:

Следует из предложения и леммы: группа G разбивается в объединение попарно непересекающихся левых смежных классов в количестве $[G : H]$ штук, а каждый класс содержит ровно $|H|$ элементов. $\square$

Вопрос 4

4.1 Пять следствий из теоремы Лагранжа.

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

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

Доказательство:

Это вытекает из следствия 1 и предложения 2.5. □

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

Доказательство:

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

Следствие 4 (Малая теорема Ферма). Пусть $\bar{a}$ — ненулевой вычет по простому модулю p. Тогда

$$\bar{a}^{p-1} = \bar{1}.$$

Доказательство:

Вытекает из следствия 3, примененного к группе $(\mathbb{Z}_p \setminus \{\bar{0}\}, \times)$. □

Следствие 5. Пусть G — группа и $|G|$ — простое число. Тогда G — циклическая группа, порождаемая любым своим неединичным элементном.

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. Так как $|G|$ — простое число, то последнее возможно только при $|\langle g \rangle| = |G|$, откуда $G = \langle g \rangle$. □

Вопрос 5

По аналогии с отношением L_H на группе G можно определить другое отношение R_H следующим образом: $(a, b) \in R_H \leftrightarrow ba^{-1} \in H$. Совершенно аналогично показывается, что R_H — тоже отношение эквивалентности на G и что классом элемента a будет множество $Ha := \{ha \mid h \in H\}$, называется *правым смежным классом* элемента a.

Для нейтрального элемента $e \in G$ имеем $eH = H = He$, так что левый и правые смежные классы для e равны между собой и совпадают с H. Подчеркнем однако, что в общем случае для одного и того же элемента $a \in G$ смежные классы aH и Ha вполне могут оказаться разными множествами даже несмотря на то, что сам элемент a принадлежит каждому из них.

Таким образом, мы выяснили, что, с одной стороны, группа G разбивается в объединение попарно непересекающихся левых смежных классов, а с другой стороны, G разбивается в объединение попарно непересекающихся левых смежных классов. Вообще говоря, это **два разных разбиения**. А вот ситуация, когда эти два разбиения совпадают, заметно выделяется среди остальных наличием замечательных свойств, которые мы сейчас и обсудим.

5.1 Нормальные подгруппы.

Определение:

Подгруппа $H \subseteq G$ называется *нормальной*, если $gH = Hg$ для всех $g \in G$.

Обозначение: $H \triangleleft G$.

Примеры:

1) G абелева $\Longrightarrow$ всякая подгруппа в G автоматически нормальна.

2) $G = S_3, H = \{id, (12)\} \Longrightarrow H$ не является нормальной подгруппой в G.

3) $H = \{e\}$ или $H = G$ (то есть H — несобственная подгруппа) $\Longrightarrow H \triangleleft G$.

Следующее предложение дает несколько эквивалентных условий, определяющих нормальную подгруппу.

Предложение:

Пусть H — подгруппа группы G. Тогда следующие условия эквивалентны:

(1) $H \triangleleft G$;

(2) $gHg^{-1} = H \ \forall g \in G$;

(3) $gHg^{-1} \subseteq H \ \forall g \in G$.

Доказательство:

(1)$\Rightarrow$(2) Если $gH = Hg$, то, умножая обе части на g^{-1} справа, получаем $gHg^{-1} = H$.

(2)$\Rightarrow$(3) Тривиально.

(3)$\Rightarrow$(1) Пусть $gHg^{-1} \subseteq H$. Умножая обе части на g^{-1} справа, получаем $gH \subseteq Hg$. Поскольку условие (3) верно для любого $g \in G$, то оно останется верным после замены в нем g на g^{-1}, так что $g^{-1}Hg \subseteq H$. Умножая обе части последнего включения на g слева, получаем $Hg \subseteq gH$. Значит, $gH = Hg$. □

5.2 Факторгруппы.

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 введем 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 берем 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 $g_1'H = g_1H$ и $g_2'H = g_2H$ (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 $h_1, h_2 \in H$. Следовательно,

$$(g_1'H) \cdot (g_2'H) = (g_1'g_2')H = (g_1h_1g_2h_2)H = (g_1g_2\underbrace{g_2^{-1}h_1g_2}_{\in H}h_2)H \subseteq (g_1g_2)H \Longrightarrow (g_1'g_2')H = (g_1g_2)H$$

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 $g^{-1}H$:

$$(g^{-1}H)(gH) = (g^{-1}g)H = H = (gg^{-1})H = (gH)(g^{-1}H).$$

Определение:

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 $G/H = (\mathbb{Z}_n, +)$ — знакомая нам группа вычетов.

Подчеркнем, что группу $(\mathbb{Z}_n, +)$ довольно затруднительно определить в обход конструкции факторгруппы.

Вопрос 6

Пусть G, F — две группы.

6.1 Гомоморфизмы групп.

Определение:

Отображение $\varphi : G \to F$ называется *гомоморфизмом*, если $\varphi(ab) = \varphi(a) \cdot \varphi(b)$ для любых $a, b \in G$.

6.2 Простейшие свойства гомоморфизмов.

Пусть $\varphi : G \to F$ — гомоморфизм групп, тогда выполнены следующие простейшие свойства:

1) Если $e_G \in G$ и $e_F \in F$ — нейтральные элементы, то $\varphi(e_G) = e_F$. Иными словами, при гомоморфизме групп нейтральный элемент переходит в нейтральный. Действительно, имеем

$$\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G).$$

Умножая на $\varphi(e_G)^{-1}$ (слева или справа — без разницы), получаем $e_F = \varphi(e_G)$.

2) $\varphi(a^{-1}) = (\varphi(a))^{-1}$ для всякого $a \in G$. Иными словами, при гомоморфизме обратный элемент переходит в обратный. Действительно, имеем $\varphi(a^{-1}) \cdot \varphi(a) = \varphi(a^{-1} \cdot a) = \varphi(e_G) = e_F$ и аналогично $\varphi(a) \cdot \varphi(a^{-1}) = e_F$, откуда и следует требуемое.

6.3 Изоморфизмы групп.

Определение:

Гомоморфизм $\varphi : G \to F$ называется *изоморфизмом*, если φ — биекция.

Замечание:

Если $\varphi : G \to F$ — изоморфизм, то обратное отображение $\varphi^{-1} : F \to G$ — тоже изоморфизм. Обратное отображение сохраняет биективность, остается проверить на гомоморфизм: пусть $\varphi(a) = a'$ и $\varphi(b) = b'$, тогда получаем

$$\varphi^{-1}(a'b') = \varphi^{-1}(\varphi(a) \cdot \varphi(b)) = \underbrace{\varphi^{-1}(\varphi}_{Id}(ab)) = ab = \varphi^{-1}(a') \cdot \varphi^{-1}(b')$$

получили, что φ^{-1} — это биекция и гомоморфизм $\Longrightarrow$ изоморфизм.

Определение:

Группы G, F называются *изоморфными*, если существует изоморфизм $\varphi : G \to F$.

Обозначение: $G \simeq F,\ G \cong F, G \xrightarrow{\sim} F$.

Можно показать, что отношение «G изоморфна F» на множестве всех групп является отношением эквивалентности, и тогда все группы разбиваются на классы изоморфизма таким образом, что внутри одного класса все группы изоморфны между собой. Изоморфные группы с алгебраической точки зрения рассматриваются как «одинаковые», и в этом основная ценность самого понятия изоморфности.

Пример:

Отображение взятия экспоненты $\varphi : \mathbb{R} \to \mathbb{R}_{>0}, a \mapsto e^a$, является изоморфизмом между группами $(\mathbb{R}, +)$ и $(\mathbb{R}_{>0}, \times)$. Обратный изоморфизм дается отображением логарифмирования $a \mapsto \ln a$.

6.4 Ядро и образ гомоморфизма групп, их свойства.

Пусть $\varphi : G \to F$ — гомоморфизм групп.

Определение:

Ядро гомоморфизм φ — это множество $\operatorname{Ker}\varphi := \{g \in G \mid \varphi(g) = e_F\} \subseteq G$.

Образ гомоморфизма φ — это множество $\operatorname{Im}\varphi := \varphi(G) \subseteq F$.

Свойства:

1. $\operatorname{Ker}\varphi$ — подгруппа в G, $\operatorname{Im}\varphi$ — подгруппа F. Проверка:

   - Принадлежность нейтрального элемента:
     из простейших свойств гомоморфизма получаем, что $\varphi(e_G) = e_F \Longrightarrow e_G \in \operatorname{Ker}\varphi$ и $e_F \in \operatorname{Im}\varphi$.
   - Замкнутость множества относительно бинарной операции:
     Ядро: пусть $a, b \in \operatorname{Ker}\varphi$, тогда $\varphi(ab) = \varphi(a) \cdot \varphi(b) = e_F \cdot e_F = e_F \Longrightarrow ab \in \operatorname{Ker}\varphi$.
     Образ: пусть $a', b' \in \operatorname{Im}\varphi$, где $\varphi(a) = a'$ и $\varphi(b) = b'$, тогда $\varphi(ab) = \varphi(a) \cdot \varphi(b) = a'b' \Longrightarrow a'b' \in \operatorname{Im}\varphi$.
   - Принадлежность обратного элемента:
     Ядро: пусть $a \in \operatorname{Ker}\varphi$, тогда $e_F = \varphi(e_G) = \varphi(a \cdot a^{-1}) = \varphi(a) \cdot \varphi(a^{-1}) = e_F \cdot \varphi(a^{-1}) = \varphi(a^{-1}) \Longrightarrow a^{-1} \in \operatorname{Ker}\varphi$.
     Образ: пусть $y \in \operatorname{Im}\varphi$, где $\varphi(x) = y$, тогда $y^{-1} = (\varphi(x))^{-1} = \varphi(x^{-1}) \Longrightarrow y^{-1} \in \operatorname{Im}\varphi$, в последнем переходе воспользовались простейшим свойством гомоморфизма.

2. φ инъективен тогда и только тогда, когда $\operatorname{Ker}\varphi = \{e\}$.

   Доказательство:

   От противного: предположим, что $f(a) = f(b)$, где $a \neq b$, тогда домножим справа на $f(b^{-1})$ и получим $f(a) \cdot f(b^{-1}) = e_F \Longleftrightarrow f(ab^{-1}) = e_F \Longrightarrow ab^{-1} = e_G \Longrightarrow a = b$. $\square$

3. φ — изоморфизм тогда и только тогда, когда $\operatorname{Ker}\varphi = \{e\}$ и $\operatorname{Im}\varphi = F$.

   Доказательство:

   Из условия известно, что φ гомоморфизм, получаем, что в данном случае изоморфизм равносилен биективности.

   Известно, что отображение называется биекцией, когда оно одновременно инъективно и сюръективно. Условие $\operatorname{Im}\varphi = F$ это прямое следствие из определения сюръективности, а эквивалентность условия $\operatorname{Ker}\varphi = \{e\}$ и инъективности следует из предыдущего свойства. $\square$

Лемма:

$\operatorname{Ker}\varphi$ — нормальная подгруппа в G.

Доказательство:

Покажем, что $g(\operatorname{Ker}\varphi)g^{-1} \subseteq \operatorname{Ker}\varphi$ для всякого $g \in G$. Действительно, для каждого $x \in \operatorname{Ker}\varphi$ имеем $\varphi(gxg^{-1}) = \varphi(g) \cdot \varphi(x) \cdot \varphi(g^{-1}) = \varphi(g) \cdot e_F \cdot \varphi(g^{-1}) = \varphi(g) \cdot (\varphi(g))^{-1} = e_F$, откуда $gxg^{-1} \in \operatorname{Ker}\varphi$, что и требовалось. $\square$

Из леммы следует, что определена факторгруппа $G/\operatorname{Ker}\varphi$.

Вопрос 7

7.1 Теорема о гомоморфизме для групп.

Теорема:

$G/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi$.

Доказательство:

Определим отображение $\psi : G/\operatorname{Ker}\varphi \to \operatorname{Im}\varphi$, положив $\psi(g\operatorname{Ker}\varphi) := \varphi(g)$ для всех $g \in G$.

1) Корректность: если $g\operatorname{Ker}\varphi = g'\operatorname{Ker}\varphi$, то $g' = gh$ для некоторого $h \in \operatorname{Ker}\varphi$, и тогда

$$\psi(g'\operatorname{Ker}\varphi) = \varphi(g') = \varphi(gh) = \varphi(g)\cdot\varphi(h) = \varphi(g)\cdot e = \varphi(g) = \psi(g\operatorname{Ker}\varphi).$$

2) Покажем, что φ — гомоморфизм. Имеем

$$\psi((g_1\operatorname{Ker}\varphi)(g_2\operatorname{Ker}\varphi)) = \psi((g_1g_2)\operatorname{Ker}\varphi) = \varphi(g_1g_2) = \varphi(g_1)\cdot\varphi(g_2) = \psi(g_1\operatorname{Ker}\varphi)\cdot\psi(g_2\operatorname{Ker}\varphi).$$

3) Отображение ψ сюръективно по определению.

4) Проверим, что ψ инъективно. Пусть $\psi(g_1\operatorname{Ker}\varphi) = \psi(g_2\operatorname{Ker}\varphi)$ для некоторых $g_1, g_2 \in G$, тогда

$$\varphi(g_1) = \varphi(g_2) \Longrightarrow e = \varphi(g_1)^{-1}\varphi(g_2) = \varphi(g_1^{-1}g_2) \Longrightarrow g_1^{-1}g_2 \in \operatorname{Ker}\varphi \Longrightarrow g_1\operatorname{Ker}\varphi = g_2\operatorname{Ker}\varphi.$$

Таким образом, мы показали, что ψ является изоморфизмом. □

Примеры:

1) Пусть $G = (\mathbb{R}, +)$, $H = (\mathbb{Z}, +)$, что представляет собой факторгруппа G/H?

Положим $F = (\mathbb{C}\setminus\{0\}, \times)$ и рассмотрим отображение $\varphi : G \to F, a \mapsto e^{2\pi i a} = \cos(2\pi a) + i\sin(2\pi a)$. Легко видеть, что φ — гомоморфизм. Тогда $\operatorname{Im}\varphi$ есть просто единичная окружность $S^1 := \{z \in \mathbb{C} \mid |z| = 1\}$ (с операцией умножения, она же сложение аргументов = углов). С другой стороны, легко видеть, что $\operatorname{Ker}\varphi = H$, и по теореме о гомоморфизме мы окончательно получаем $G/H \simeq S^1$.

2)Для произвольной группы G рассмотрим тождественное отображение $id : G \to G, g \mapsto g$, по очевидным причинам оно является гомоморфизмом группы G в себя. Тогда $\operatorname{Ker} id = \{e\}, \operatorname{Im} id = G$, и по теореме о гомоморфизме мы получаем $G/\{e\} \simeq G$.

3)Снова возьмем произвольную группу G и рассмотрим отображение $\varphi : G \to \{e\}, g \mapsto e$, оно также является гомоморфизмом. Тогда $\operatorname{Ker} id = \{e\}, \operatorname{Im} id = G$, и по теореме о гомоморфизме мы получаем $G/\{e\} \simeq G$.

Отметим, что в примерах 2) и 3) мы вычислили факторгруппы произвольной группы по ее обеим несобственным подгруппам.

Вопрос 8

8.1 Классификация циклических групп.

Предложение:

Пусть G — циклическая группа. Тогда

(а) $|G| = \infty \Longrightarrow G \simeq (\mathbb{Z}, +)$;

(б) $|G| = n \Longrightarrow G \simeq (\mathbb{Z}_n, +)$.

Доказательство:

Пусть $G = \langle g \rangle$. Рассмотрим отображение $\varphi : \mathbb{Z} \to G, k \mapsto g^k$. Тогда $\varphi(k+l) = g^{k+l} = g^k g^l = \varphi(k)\varphi(l)$, поэтому φ — гомоморфизм. Из определения циклической группы следует, что φ сюръективен, то есть $\operatorname{Im} \varphi = G$. Тогда по теореме о гомоморфизме мы получаем $G \simeq \mathbb{Z}/\operatorname{Ker} \varphi$. Так как $\operatorname{Ker} \varphi$ — подгруппа в $\mathbb{Z}$, то по предложению 1.7 получаем $\operatorname{Ker} \varphi = m\mathbb{Z}$ для некоторого $m \geqslant 0$.

Если $m = 0$, то $\operatorname{Ker} \varphi = \{0\}$, откуда $G \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$.

Если $m > 0$, то $G \simeq \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. □

Вопрос 9

9.1 Прямое произведение групп.

Пусть $G_1, \ldots, G_m$ — группы.

Определение:

Прямое произведение групп $G_1, \ldots, G_m$ — это множество $G_1 \times \ldots \times G_m$ с бинарной операцией $(g_1, \ldots, g_m)(g_1', \ldots, g_m') := (g_1 g_1', \ldots, g_m g_m')$.

Проверим, что $G_1 \times \ldots \times G_m$ — действительно группа:

1. Ассоциативность:

$$((g_1, \ldots, g_m)(g_1', \ldots, g'm))(g_1'', \ldots, g_m'') = ((g_1 g_1')g_1'', \ldots, (g_m g_m')g_m'') =$$

$$= (g_1(g_1' g_1''), \ldots, g_m(g_m' g_m'')) = (g_1, \ldots, g_m)((g_1', \ldots, g_m')(g_1'', \ldots, g_m''));$$

2. Нейтральный элемент — $e_{G_1}, \ldots, e_{G_m}$:

$$(e_{G_1}, \ldots, e_{G_m})(g_1, \ldots, g_m) = (e_{G_1} g_1, \ldots, e_{G_m} g_m) = (g_1, \ldots, g_m) =$$

$$= (g_1 e_{G_1}, \ldots, g_m e_{G_m}) = (g_1, \ldots, g_m)(e_{G_1}, \ldots, e_{G_m});$$

3. Обратный к $(g_1, \ldots, g_m)$ элемент — это $(g_1^{-1}, \ldots, g_m^{-1})$:

$$(g_1, \ldots, g_m)(g_1^{-1}, \ldots, g_m^{-1}) = (g_1 g_1^{-1}, \ldots, g_m g_m^{-1}) = (e_{G_1}, \ldots, e_{G_m}) =$$

$$= (g_1^{-1} g_1, \ldots, g_m^{-1} g_m) = (g_1^{-1}, \ldots, g_m^{-1})(g_1, \ldots, g_m)$$

Как видно, и тут все необходимые свойства вытекают из того, что $G_1, \ldots, G_m$ — группы.

Пример:

1) $\underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{n} = \mathbb{R}^n$ — знакомый нам из курса линейной алгебры объект.

2) $\underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}_{n} = \mathbb{Z}^n$ — это подгруппа в $\mathbb{R}^n$, состоящая из всех векторов с целочисленными координатами.

Группа $\mathbb{Z}^n$ называется *решеткой* ранга n.

Замечание:

1) Группа $G_1 \times \ldots \times_m$ абелева тогда и только тогда, когда все группы $G_1, \ldots, G_m$ абелевы.

2) Если группы $G_1, \ldots, G_m$ конечны, то $|G_1 \times \ldots \times G_m| = |G_1| \cdot \ldots \cdot |G_m|$.

Обратим внимание, что для каждого $i = 1, \ldots, m$ естественный гомоморфизм

$$G_i \to G, g \mapsto (e_{G_1}, \ldots, e_{G_{i-1}}, g, e_{G_{i+1}}, \ldots, e_{G_m}),$$

является вложением, ввиду чего G_i обычно отождествляется с его образом и рассматривается как подгруппа $\{(e_{G_1}, \ldots, e_{G_{i-1}}, g, e_{G_{i+1}}, \ldots, e_{G_m})) \mid g \in G_i\}$ группы $G_1 \times \ldots \times G_m$.

Пусть G — некоторая группа и $H_1, \ldots, H_m$ — ее подгруппы.

Определение:

Говорят, что G *разлагается в прямое произведение* своих подгрупп $H_1, \ldots, H_m$, если отображение $H_1 \times \ldots \times H_m \to G,\ (h_1, \ldots, h_m) \mapsto h_1 \cdot \ldots h_m$, является изоморфизмом.

В этой ситуации обычно допускают вольность в обозначениях и пишут $G = H_1 \times \ldots \times H_m$, хотя формально G и $H_1 \times \ldots \times H_m$ — это разные группы. Как говорят, G и $H_1 \times \ldots \times H_m$ отождествляются по указанному выше изоморфизму между ними.

Возвращаясь к ситуации определения 9.1 и отождествляя каждую группу G_i с подгруппой в $G_1 \times \ldots \times G_m$, как выше, мы теперь можем сказать, что группа $G_1 \times \ldots \times G_m$ является прямым произведением своих подгрупп $G_1, \ldots, G_m$.

Конструкцию прямого произведения в смысле определения 9.1 иногда называют внешним прямым произведением, а в смысле определения 9.1 — внутренним прямым произведением. Однако ввиду сделанных выше отождествлений на практике зачастую не делается различий между этими двумя понятиями.

Далее мы будем работать только с абелевыми группами и в соответствии с этим будем пользоваться аддитивной записью групповой операции.

9.2 Разложение конечной циклической группы.

Теорема:

Пусть числа $n, m, l \in \mathbb{N}$ такомы, что $n = ml$ и НОД$(m,l) = 1$. Тогда $\mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l$.

Доказательство:

Рассмотрим отображение $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l$, $\varphi(a \mod n) := (a \mod m,\ a \mod l)$, и покажем, что оно является изоморфизмом.

1) Корректность: есть, так как из делимости на n автоматически следует делимость на m и l.

2) φ — гомоморфизм:

$$\varphi((a+b) \mod n) = ((a+b) \mod m, (a+b) \mod l) =$$

$$= (a \mod m, a \mod l) + (a \mod m, a \mod l) = \varphi(a \mod n) + \varphi(b \mod n).$$

3) Инъективность: если $\varphi(a \mod n) = (0,0)$, то $a \mathrel{\vdots} m$ и $a \mathrel{\vdots} l$, откуда $a \mathrel{\vdots} n$ в силу НОД$(m,l) = 1$, откуда $a \mod n = 0$. Значит, $\operatorname{Ker}\varphi = \{0\}$ и φ инъективно.

4) Сюръективность: имеем $|\mathbb{Z}_n| = n = m \cdot l = |\mathbb{Z}_m \times \mathbb{Z}_l|$, и тогда требуемое следует из 3), поскольку всякое инъективное отображение между двумя конечными множествами одной мощности автоматически сюръективно. $\square$

Следствие (*Разложение конечной циклической группы*).

Пусть $n \leqslant 2$ — натуральное число и $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ — его разложение на простые множители ($p_i \neq p_j$ при $i \neq j$). Тогда $\mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}$.

9.3 Теорема о строении конечных абелевых групп.

Определение:

Конечная абелева группа A называется *примарной*, если $|A| = p^k$, где p — простое и $k \in \mathbb{N}$.

Следующая важная теорема дает классификацию всех конечных абелевых групп с точностью до изоморфизма. Поскольку этот результат нам не понадобится в дальнейшем, мы не будем тратить время на его доказательство.

Теорема:

Пусть A — конечная абелева группа. Тогда $A \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_t^{k_t}}$, где $p_1, \ldots, p_t$ — простые числа (не обязательно попарно различные!) и $k_1, \ldots, k_t \in \mathbb{N}$. Более того, набор примарных циклических множителей $\mathbb{Z}_{p_1^{k_1}}, \ldots, \mathbb{Z}_{p_t^{k_t}}$ определен однозначно с точностью до перестановки.

Глобальный смысл этой теоремы заключается в том, что конечные абелевы группы устроены очень просто и все они получаются конструкцией прямого произведения из примарных циклических групп (играющих здесь роль «кирпичиков», из которых все строится). Отметим, что частным случаем теоремы случит следствие 5 из теоремы Лагранжа, согласно которому (с учетом классификации циклических групп) вообще любая (не обязательно абелева) конечная группа простого порядка p изоморфна $\mathbb{Z}_p$.

Вопрос 10

10.1 Экспонента конечной абелевой группы и критерий цикличности.

Пусть A — конечная абелева группа.

Определение:

Экспонентой группы A называется число

$$\exp A := \min\{m \in \mathbb{N} \mid ma = 0 \text{ для всех } a \in A\}.$$

Замечание:

1) Так как $ma = 0 \iff m \vdots \operatorname{ord}(a)$ для всех $a \in A$ и $m \in \mathbb{Z}$, то определение экспоненты можно переписать еще в таком виде: $\exp A = \text{НОК}\{\operatorname{ord}(a) \mid a \in A\}$.

2) Так как $|A| \vdots \operatorname{ord}(a)$ для всех $a \in A$ (следствие 2 из теоремы Лагранжа), то $|A|$ — общее кратное множества $\{\operatorname{ord}(a) \mid a \in A\}$, а значит, $|A| \vdots \exp A$. В частности, $\exp A \leqslant |A|$.

В дальнейшем нам понадобится следующий факт *(Критерий цикличности)*, который показывает, когда в последнем неравенстве достигается равенство.

Предложение:

$\exp A = |A| \iff$ группа A является циклической.

Доказательство:

Положим $n = |A|$ и рассмотрим разложение на простые множители: $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$, где p_i — простое и $k_i \in \mathbb{N}$ для всех $i = 1, \ldots, s, p_i \neq p_j$ при $i \neq j$.

($\Leftarrow$) Если $A = \langle a \rangle$, то $\operatorname{ord}(a) = n$, откуда в силу неравенства сразу получаем $\exp A = n$.

($\Rightarrow$) Если $\exp A = n$, то для каждого $i = 1, \ldots, s$ существует элемент $c_i \in A$, такой что $\operatorname{ord}(c_i) = p_i^{k_i} m_i$, где $m_i \in \mathbb{N}$. Для каждого $i = 1, \ldots, s$ положим $a_i = m_i c_i$, тогда $\operatorname{ord}(a_i) = p_i^{k_i}$. Теперь рассмотрим элемент $a = a_1 + \ldots + a_s$ и покажем, что $\operatorname{ord}(a) = n$. Пусть $ma = 0$ для некоторого $m \in \mathbb{N}$, то есть $ma_1 + \ldots + ma_s = 0$. При фиксированном $i \in \{1, \ldots, s\}$ умножим обе части последнего равенства на $n_i := n/p_i^{k_i}$. Легко видеть, что $mn_i a_j = 0$ при всех $i \neq j$, поэтому в левой части выживет только слагаемое $mn_i a_i$, откуда получаем $mn_i a_1 = 0$. Следовательно, $mn_i \vdots p_i^{k_i}$, а так как n_i не делится на p_i, то $m \vdots p_i^{k_i}$. В силу произвольности выбора i отсюда вытекает, что $m \vdots n$. Так как $na = 0$, то мы окончательно получаем $\operatorname{ord}(a) = n$. Значит, $A = \langle a \rangle$ — циклическая группа. □

Вопрос 11

Расскажем об одном весьма элементарном, однако очень важном и используемом на практике применении конечных циклических групп к задачам криптографии с открытым ключом. Одним из основных примеров групп, к которым применяются описанные ниже криптосистемы, служит мультипликативная группа вычетов $G = (\mathbb{Z}_p \setminus \{0\}, \times)$ по простому модулю p. Поэтому мы вернемся к мультипликативным обозначениям.

11.1 Задача дискретного логарифмирования.

Пусть G — конечная группа и $g \in G$ — элемент достаточно большого порядка. Для данного элемента $h \in \langle g \rangle$ найти такое $k \in \mathbb{N}$, что $h = g^k$.

11.2 Криптография с открытым ключом.

Метод шифрования информации с открытым ключом основан на предположении о том, что для данных элементов g и h решение задачи дискретного логарифмирования трудоемко и при подходящих входных данных и текущем уровне вычислительных мощностей практически не реализуемо. Напротив, возведение элемента в заданную степень можно произвести достаточно эффективно, использую, например, метод повторного возведения в квадрат.

Следующий метод позволяет двум участникам переписки у всех на глазах добиться того, что у них появляется элемент, известный только им двоим.

11.3 Система Диффи-Хеллмана обмена ключами (1976).

Всем участникам переписки известны конечная группа G и элемент $g \in G$ достаточно большого порядка. Каждый участник A загадывает свое натуральное число a, которое держит в секрете, и сообщает всем значение g^a. После этого каждая пара участников A и B может составить общий для нее ключ: A возводит элемент g^b в степень a, а B возводит g^a в степень b. В результате элемент g^{ab} есть только у A и B, и они могут использовать его в качестве ключа для дальнейшей конфиденциальной переписки.

11.4 Криптосистема Эль-Гамаля (1985).

Сначала обсудим основную идею. обсудим основную идею. Пусть все так же, как в описании системы Диффи-Хеллмана, и участники A и B уже сгенерировали свой секретный ключ g^{ab}. В дальнейшем участнику A понадобится также элемент $(g^{ab})^{-1}$, который, зная g^b и a, можно сразу вычислить как $(g^b)^{|G|-a}$ (вспомним следствие 3 из теоремы Лагранжа). Если теперь участник B хочет конфиденциально передать участнику A элемент $h \in G$ (кодирующий какое-то важное сообщение), то он вычисляет и сообщает всем элемент $y = hg^{ab}$. Теперь участник A может восстановить h, домножая y справа на $\left(g^{ab}\right)^{-1}$, то есть по формуле $h = y\left(g^b\right)^{|G|-a}$. Заметим, что никто из толпы шпионов, наблюдающих за данной перепиской, не в состоянии определить элемент h по y, так как не знает секретного ключа g^{ab}.

Теперь опишем собственно криптосистему Эль-Гамаля. По существу в ней происходит все то же самое, что описано выше, однако генерация секретного ключа для участников A и B происходит не заранее, а встроена в сам процесс обмена информацией.

Итак, снова всем участникам переписки известны конечная группа G и элемент $g \in G$ достаточно большого порядка. Каждый участник A загадывает свой натуральное число a, которое держит в секрете, и сообщает всем значение g^a. Если участник B хочет передать участнику A элемент $h \in G$, он случайным образом выбирает натуральное b и сообщает всем пару $(x, y) = (g^b, h(g^a)^b)$. По этим данным восстановить элемент h может только A, и делает он это так: $h = yx^{|G|-a}$.

Важная особенность криптосистемы Эль-Гамаля: если участнику B нужно передать много сообщений для A, то для каждого следующего сообщения он может использовать новое случайное значение параметра b, что многократно повышает надежность всей системы.

Вопрос 12

12.1 Кольца.

12.2 Коммутативные кольца.

12.3 Обратимые элементы, делители нуля и нильпотенты.

12.4 Примеры колец.

12.5 Поля.

12.6 Критерий того, что кольцо вычетов является полем.

Вопрос 13

13.1 Идеалы колец.

13.2 Факторкольцо кольца по идеалу.

13.3 Гомоморфизмы и изоморфизмы колец.

13.4 Ядро и образ гомоморфизма колец.

13.5 Теорема о гомоморфизме для колец.

Вопрос 14

14.1 Кольцо многочленов от одной переменной над полем.

14.1.1 Деление с остатком.

14.1.2 Наибольший общий делитель двух многочленов.

14.1.3 Теорема о существовании НОД'а и о его линейном выражении.

Вопрос 15

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

Вопрос 16

16.1 Неприводимые многочлены.

16.2 Факториальность кольца многочленов от одной переменной над полем.

Вопрос 17

17.1 Критерий того, что факторкольцо $K[x]/(h)$ является полем.

17.2 Базис и размерность факторкольца $K[x]/(h)$ как векторного пространства над полем K.

Вопрос 18

18.1 Лексикографический порядок на множестве одночленов от нескольких переменных.

18.2 Лемма о конечности убывающих цепочек одночленов.

Вопрос 19

19.1 Старший член многочлена от нескольких переменных.

19.2 Элементарная редукция многочлена относительно другого многочлена.

19.3 Лемма о конечности цепочек элементарных редукций относительно системы многочленов.

Вопрос 20

20.1 Остаток многочлена относительно заданной системы многочленов.

20.2 Система Грёбнера.

20.3 Характеризация систем Грёбнера в терминах цепочек элементарных редукций.

Вопрос 21

21.1 S-многочлены.

21.2 Критерий Бухбергера.

Вопрос 22

22.1 Базис Грёбнера идеала в кольце многочленов от нескольких переменных.

22.1.1 Теорема о трех эквивалентных условиях.

22.2 Решение задачи вхождения многочлена в идеал.

Вопрос 23

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

23.2 Алгоритм Бухбергера построения базиса Грёбнера идеала.

Вопрос 24

24.1 Теорема Гильберта о базисе идеала.

Вопрос 25

25.1 Редуцируемость к нулю S-многочлена двух многочленов с взаимно простыми старшими членами.

Вопрос 26

26.1 Характеристика поля.

26.2 Расширение полей.

26.3 Конечное расширение и его степень.

26.4 Степень композиции двух расширений.

Вопрос 27

27.1 Присоединение корня неприводимого многочлена.

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

Вопрос 28

28.1 Алгебраические и трансцендентные элементы.

28.2 Минимальный многочлен алгебраического элемента и его свойства.

Вопрос 29

29.1 Подполе в расширении полей, порожденное алгебраическим элементом.

Вопрос 30

30.1 Порядок конечного поля.

30.2 Автоморфизм Фробениуса.

Вопрос 31

31.1 Теорема существования для конечных полей.

Вопрос 32

32.1 Цикличность мультипликативной группы конечного поля.

32.2 Неприводимые многочлены над $\mathbb{Z}_p$.