Алгебра
Билеты к Экзамену

Роман Сергеевич Авдеев
Иван Владимирович Аржанцев

21 июня 2018 г.

Содержание

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

Определение 1.1. *Множество с бинарной операцией* — это множество M с заданным отображением
$$M \times M \to M, \quad (a,b) \mapsto a \circ b.$$

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

Определение 1.2. Множество с бинарной операцией $(M,\circ)$ называется *полугруппой*, если данная бинарная операция *ассоциативна*, т. е.

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

Не все естественно возникающие операции ассоциативны. Например, если $M = \mathbb{N}$ и $a \circ b := a^b$, то
$$2^{(1^2)} = 2 \neq (2^1)^2 = 4.$$

Другой пример неассоциативной бинарной операции: $M = \mathbb{Z}$ и $a \circ b := a - b$ (проверьте!).

Полугруппу обычно обозначают $(S,\circ)$.

Определение 1.3. 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 $a \in S$.

Замечание 1. Если в полугруппе есть нейтральный элемент, то он один. В самом деле, $e_1 \circ e_2 = e_1 = e_2$.

Определение 1.4. Моноид $(S,\circ)$ называется *группой*, если для каждого элемента $a \in S$ найдется *обратный элемент*, т. е. такой $b \in S$, что $a \circ b = b \circ a = e$.

Обратный элемент обозначается a^{-1}.

Группу принято обозначать $(G,\circ)$ или просто G, когда понятно, о какой операции идёт речь. Обычно символ $\circ$ для обозначения операции опускают и пишут просто ab.

Определение 1.5. Группа G называется *коммутативной* или *абелевой*, если групповая операция *коммутативна*, т. е. $ab = ba$ для любых $a,b \in G$.

Если в случае произвольной группы G принято использовать мультипликативные обозначения для групповой операции — gh, e, g^{-1}, то в теории абелевых групп чаще используют аддитивные обозначения, т. е. $a + b$, 0, $-a$.

Определение 1.6. *Порядок* группы G — это число элементов в G. Группа называется *конечной*, если её порядок конечен, и *бесконечной* иначе.

Порядок группы G обозначается $|G|$.

Приведём несколько серий примеров 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:

   $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) \neq 0\}$;

   $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}(n \times n, \mathbb{R}) \mid \det(A) = 1\}$.

4. Группы подстановок:
   симметрическая группа S_n — все подстановки длины n, $|S_n| = n!$;
   знакопеременная группа A_n — чётные подстановки длины n, $|A_n| = n!/2$.

5. Группы преобразований: симметрия, движение.

Определение 1.7. Подмножество H группы G называется *подгруппой*, если выполнены следующие три условия:
(1) $e \in H$;
(2) $ab \in H$ для любых $a,b \in H$;
(3) $a^{-1} \in H$ для любого $a \in H$.

В каждой группе G есть *несобственные* подгруппы $H = \{e\}$ и $H = G$. Все прочие подгруппы называются *собственными*. Например, чётные числа $2\mathbb{Z}$ образуют собственную подгруппу в $(\mathbb{Z},+)$.

Предложение 1.1. *Всякая подгруппа в* $(\mathbb{Z},+)$ *имеет вид* $k\mathbb{Z}$ *для некоторого целого неотрицательного* k.

Доказательство. Очевидно, что все подмножества вида $k\mathbb{Z}$ являются подгруппами в $\mathbb{Z}$.

1. Пусть $H \subseteq \mathbb{Z}$ подгруппа. Если $H = \{0\}$, то $H = 0\mathbb{Z}$.

   Иначе положим $k = min(H \cap \mathbb{N})(\neq 0)$.

   Тогда $k\mathbb{Z} \subseteq H$.

2. Покажем, что $k\mathbb{Z} = H$. Пусть $a \in H$. Поделим на k с остатком.

   $a = qk + r,$ где $q \in H, 0 \leq r \leq k$

   $\Rightarrow r = a - qk \in H$

   В силу выбора k получаем $r = 0$. $\Rightarrow a = qk$

□

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

$$g^n = \begin{cases} \underbrace{g...g}_{n}, \ n > 0 \\ e, \ n = 0 \\ \underbrace{g^{-1}...g^{-1}}_{n}, \ n < 0 \end{cases}$$

Свойства:

1. $g^m \cdot g^n = g^{m+n}, \forall n, m \in \mathbb{Z}$
2. $(g^k)^{-1} = g^{-k}, \forall k \in \mathbb{Z}$
3. $(g^n)^m = g^{nm}, \forall n, m \in \mathbb{Z}$

Определение 2.1. Пусть G — группа и $g \in G$. *Циклической подгруппой*, порождённой элементом g, называется подмножество $\{g^n \mid n \in \mathbb{Z}\}$ в G.

Циклическая подгруппа, порождённая элементом g, обозначается $\langle g \rangle$. Элемент g называется *порождающим* или *образующим* для подгруппы $\langle g \rangle$.

Например, подгруппа $2\mathbb{Z}$ в $(\mathbb{Z},+)$ является циклической, и в качестве порождающего элемента в ней можно взять $g = 2$ или $g = -2$. Другими словами, $2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$.

Определение 2.2. Группа G называется *циклической*, если найдётся такой элемент $g \in G$, что $G = \langle g \rangle$.

Определение 2.3. 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 $\operatorname{ord}(g)$. Заметим, что $\operatorname{ord}(g) = 1$ тогда и только тогда, когда $g = e$.

Следующее предложение объясняет, почему для порядка группы и порядка элемента используется одно и то же слово.

Предложение 2.1. *Пусть G — группа и $g \in G$. Тогда* $\operatorname{ord}(g) = |\langle g \rangle|$.

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 $e = g^0, g = g^1, g^2, \ldots, g^{m-1}$ попарно различны. Далее, для всякого $n \in \mathbb{Z}$ мы имеем $n = mq + r$, где $0 \leqslant r \leqslant m - 1$, и

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

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

Ясно, что всякая циклическая группа коммутативна и не более чем счётна. Примерами циклических групп являются группы $(\mathbb{Z},+)$ и $(\mathbb{Z}_n,+)$, $n \geq 1$.

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа.

Определение 3.1. Пусть G — группа, $H \subseteq G$ — подгруппа и $g \in G$. *Левым смежным классом* элемента g группы G по подгруппе H называется подмножество

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

Наряду с левым смежным классом можно определить *правый смежный класс* элемента g группы G по подгруппе H:

$$Hg = \{hg \mid h \in H\}.$$

Все дальнейшие доказательства для правых смежных классов формулируются и доказываются аналогично.

Лемма 3.1. *Пусть G — группа, $H \subseteq G$ — её подгруппа и $g_1, g_2 \in G$. Тогда либо $g_1H = g_2H$, либо $g_1H \cap g_2H = \varnothing$.*

Доказательство. Предположим, что $g_1H \cap g_2H \neq \varnothing$, 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. □

Лемма 3.2. *Пусть G — конечная 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 $|gH| = |H|$. □

Определение 3.2. 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 $[G : H]$.

Теорема 3.1. Теорема Лагранжа.
Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда

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

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

4 Пять следствий из теоремы Лагранжа.

Теорема Лагранжа. Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда

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

Рассмотрим некоторые следствия из теоремы Лагранжа.

Следствие 4.1. *Пусть G — конечная группа и $H \subseteq G$ — подгруппа. Тогда $|H|$ делит $|G|$.*

Следствие 4.2. *Пусть G — конечная группа и $g \in G$. Тогда* $\operatorname{ord}(g)$ *делит* $|G|$.

Доказательство. Это вытекает из следствия 1 и $|\langle g \rangle| = ord(g)$ □

Следствие 4.3. *Пусть G — конечная группа и $g \in G$. Тогда $g^{|G|} = e$.*

Доказательство. Пусть $k = ord(g)$. Тогда из следствия 2: $\mid G \mid = k \cdot s$
$\Rightarrow g^{|G|} = (g^{ks}) = (g^k)^s = e^s = e$ □

Следствие 4.4. *(малая теорема Ферма)*
p - простое число, НОД$(a, p) = 1 \Rightarrow a^{p-1} \equiv 1 \mod p$

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

Следствие 4.5. *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 $G = \langle g \rangle$. □

5 Нормальные подгруппы и факторгруппы.

Определение 5.1. Подгруппа H группы G называется *нормальной*, если $gH = Hg$ для любого $g \in G$.

Предложение 5.1. *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. Докажем циклом.

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

(3)⇒(1) Для произвольного $g \in G$ в силу (3) имеем $gH = gHg^{-1}g = Hg$.

□

Рассмотрим множество (неважно, левых или правых) смежных классов по нормальной подгруппе G/H.

Определим на G/H бинарную операцию, полагая $(g_1H)(g_2H) = (g_1g_2)H$

Корректность:

Пусть $g_1'H = g_1H$ и $g_2'H = g_2H$.
Тогда $g_1' = g_1h_1$, $g_2' = g_2h_2$, где $h_1, h_2 \in H$.

$$(g_1'H)(g_2'H) = (g_1'g_2')H = (g_1h_1g_2h_2)H = (g_1g_2(g_2^{-1}h_1g_2)h_2)H \subseteq (g_1g_2)H \Rightarrow (g_1'g_2')H = (g_1g_2)H$$

Структура группы G/H.

1. ассоциативность: очевидна.
2. нейтральный элемент: eH.
3. обратный к $gH : g^{-1}H$.

Определение 5.2. Множество G/H с указанной операцией называется *факторгруппой* группы G по нормальной подгруппе H.

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

6 Гомоморфизм групп. Простейшие свойства гомоморфизмов. Изоморфизмы группы. Ядро и образ гомоморфизма группы, их свойства

Определение 6.1. Пусть $(G, \circ)$ и $(F, *)$ две группы.
Отображение $\varphi : G \to F$ называется *гомоморфизмом*, если

$$\varphi(g_1 \circ g_2) = \varphi(g_1) * \varphi(g_2), \forall g_1, g_2 \in G$$

Замечание 2. Подчеркнём, что в этом определении произведение ab берётся в группе G, в то время как произведение $\varphi(a)\varphi(b)$ — в группе F.

Лемма 6.1. *Пусть* $\varphi\colon G \to F$ *— гомоморфизм групп, и пусть* e_G *и* e_F *— нейтральные элементы групп* G *и* F *соответственно.*

Тогда:

(а) $\varphi(e_G) = e_F$*;*

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

Доказательство. По пунктам:

(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 $\varphi(a^{-1}) = \varphi(a)^{-1}$.

□

Определение 6.2. Гомоморфизм групп $\varphi\colon G \to F$ называется *изоморфизмом*, если отображение φ биективно.

Упражнение 1. Пусть $\varphi\colon G \to F$ — изоморфизм групп. Проверьте, что обратное отображение $\varphi^{-1}\colon F \to G$ также является изоморфизмом.

Определение 6.3. Группы G и F называют *изоморфными*, если между ними существует изоморфизм.

Обозначение: $G \cong F$ (или $G \simeq F$).

В алгебре группы рассматривают с точностью до изоморфизма: изоморфные группы считаются «одинаковыми».

Определение 6.4. С каждым гомоморфизмом групп $\varphi\colon G \to F$ связаны его *ядро*

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

и *образ*

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

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

Лемма 6.2. *Гомоморфизм групп* $\varphi\colon G \to F$ *инъективен тогда и только тогда, когда* $\mathrm{Ker}(\varphi) = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен, то $\mathrm{Ker}(\varphi) = \{e_G\}$.
Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1}g_2 \in \mathrm{Ker}(\varphi)$, 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 $g_1 = g_2$. □

Следствие 6.1. *Гомоморфизм групп* $\varphi\colon G \to F$ *является изоморфизмом тогда и только тогда, когда* $\mathrm{Ker}(\varphi) = \{e_G\}$ *и* $\mathrm{Im}(\varphi) = F$.

Предложение 6.1. *Пусть* $\varphi\colon G \to F$ *— гомоморфизм групп. Тогда подгруппа* $\mathrm{Ker}(\varphi)$ *нормальна в* G.

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

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

□

7 Теорема о гомоморфизме для групп

Теорема 7.1. Теорема о гомоморфизме.

Пусть $\varphi\colon G \to F$ *— гомоморфизм групп. Тогда группа* $\mathrm{Im}(\varphi)$ *изоморфна факторгруппе* $G/\mathrm{Ker}(\varphi)$*.*

Доказательство. Рассмотрим отображение $\psi\colon G/\mathrm{Ker}(\varphi) \to \mathrm{Im}(\varphi)$, заданное формулой $\psi(g\mathrm{Ker}(\varphi)) = \varphi(g)$.

1. Корректность

   $g_1 Ker\varphi = g_2 Ker\varphi \Rightarrow g_1 h_1 = g_2 h_2$ для некоторых $h_1, h_2 \in Ker\varphi$

   $\psi(g_1 Ker\varphi) = \varphi(g_1) = \varphi(g_1 h_1) = \varphi(g_2 h_2) = \varphi(g_2) = \psi(g_2 Ker\varphi)$

2. ψ гомоморфизм.

   $\psi((g_1 Ker\varphi)(g_2 Ker\varphi)) = \psi((g_1 g_2) Ker\varphi) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1 Ker\varphi)\psi(g_2 Ker\varphi)$

3. Сюрьективность из построения.

4. Инъективность.

   $\psi(g_1 Ker\varphi) = \psi(g_2 Ker\varphi) \Rightarrow \varphi(g_1) = \varphi(g_2) \Rightarrow \varphi(g_1)\varphi(g_2)^{-1} = e_F \Rightarrow \varphi(g_1 g_2^{-1}) = e_F$

   $\Rightarrow g_1 g_2^{-1} \in Ker\varphi \Rightarrow g_1 Ker\varphi = g_2 Ker\varphi$

□

Тем самым, чтобы удобно реализовать факторгруппу G/H, можно найти такой гомоморфизм $\varphi\colon G \to F$ в некоторую группу F, что $H = \mathrm{Ker}(\varphi)$, и тогда $G/H \cong \mathrm{Im}(\varphi)$.

Пример 2. Пусть $G = (\mathbb{R},+)$ и $H = (\mathbb{Z},+)$. Рассмотрим группу $F = (\mathbb{C} \setminus \{0\},\times)$ и гомоморфизм

$$\varphi\colon G \to F, \quad a \mapsto e^{2\pi \imath a} = \cos(2\pi a) + i\sin(2\pi a).$$

Тогда $\mathrm{Ker}(\varphi) = H$ и факторгруппа G/H изоморфна окружности S^1, рассматриваемой как подгруппа в F, состоящая из комплексных чисел с модулем 1.

8 Классификация циклических групп

Классификация циклических групп. 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. $\varphi : \mathbb{Z} \mapsto G, \varphi : k \mapsto g^k$

   Это гомоморфизм и биекция $\Rightarrow$ изоморфизм.

2. $\varphi : \mathbb{Z}_n \mapsto G, \varphi : k \mapsto g^k$

   Рассмотрим, куда переходит $k + ns$, где $0 \leq k \leq n - 1$.

   $k + ns \mapsto g^{k+ns} = g^k g^{ns} = g^k (g^n)^s = g^k$

$\square$

9 Прямое произведение групп. Разложение конечной циклической группы.

Определение 9.1. *Прямым произведением* групп $G_1, \ldots, G_m$ называется множество

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

с операцией $(g_1, \ldots, g_m)(g'_1, \ldots, g'_m) = (g_1 g'_1, \ldots, g_m g'_m)$.

Ясно, что эта операция ассоциативна, обладает нейтральным элементом $(e_{G_1}, \ldots, e_{G_m})$ и для каждого элемента $(g_1, \ldots, g_m)$ есть обратный элемент $(g_1^{-1}, \ldots, g_m^{-1})$.

Замечание 3. Группа $G_1 \times \ldots \times G_m$ коммутативна в точности тогда, когда коммутативна каждая из групп $G_1, \ldots, G_m$.

Замечание 4. Если все группы $G_1, \ldots, G_m$ конечны, то $|G_1 \times \ldots \times G_m| = |G_1| \cdot \ldots \cdot |G_m|$.

Определение 9.2. Группа G *раскладывается в прямое произведение* своих подгрупп $H_1, \ldots, H_m$, если отображение $H_1 \times \ldots \times H_m \to G$, $(h_1, \ldots, h_m) \mapsto h_1 \cdot \ldots \cdot h_m$, является изоморфизмом.

Теорема 9.1. *Пусть $n = ml$ — разложение натурального числа n на два взаимно простых множителя. Тогда имеет место изоморфизм групп*

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

Доказательство. Рассмотрим отображение

$$\varphi \colon \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l, \quad (k \mod n) \mapsto (k \mod m, k \mod l).$$

Поскольку m и l делят n, отображение φ определено корректно. Ясно, что φ — гомоморфизм. Далее,

$a \mod n \in \mathrm{Ker}\varphi \Rightarrow a \mod m = 0, a \mod l = 0 \Rightarrow a \vdots m, a \vdots k$

Так как НОД$(m, l) = 1$, то $a \vdots (n = ml) \Rightarrow a \mod n = 0 \Rightarrow Ker\varphi = \{0\}$

Отсюда следует, что гомоморфизм φ инъективен.

Поскольку множества $\mathbb{Z}_n$ и $\mathbb{Z}_m \times \mathbb{Z}_l$ содержат одинаковое число элементов, отображение φ биективно. □

Следствие 9.1. *Пусть $n \geqslant 2$ — натуральное число и $n = p_1^{k_1} \ldots p_s^{k_s}$ — его разложение в произведение простых множителей (где $p_i \neq p_j$ при $i \neq j$). Тогда имеет место изоморфизм групп*

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}.$$

10 Примарные абелевы группы. Теорема о строении конечно порождённых абелевых групп, доказательство единственности.

Теорема 10.1. *A – конечная абелева группа. Тогда A изоморфна произведению циклических групп.*

$$A \simeq C_1 \times \ldots \times C_s,$$

где C_i – конечная циклическая группа

Эта теорема приводится без доказательства.

Определение 10.1. Конечная абелева группа A называется **примарной**, если $|A| = p^k$ для некоторого простого p.

Пример 3. $A = \mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p$
$A = \mathbb{Z}_{p^k}$

Теорема 10.2. *Всякая конечная абелева группа изоморфна прямому произведению примарных циклических групп, причем число и порядки множителей определяются однозначно.*

$$A \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}},$$

где p_i – простые числа (не обязятельно попарно различные).

Доказательство. По предыдущей теореме получаем:

$$A \simeq C_1 \times \ldots \times C_t$$

где C_i – циклическая.

Теперь применим следствие, которое гласит, что всякая циклическая группа раскладывается на произведение примарных циклических.

$$A \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}},$$

Теперь докажем *единственность.*

Зафиксируем простое p. Положим $T_p(A) := \{a \in A \mid \exists k \in \mathbb{N} : p^k a = 0\}$ (запись аддитивная).

Нетрудно заметить, что $T_p(A)$ – подгруппа в A. Тогда очевиден следующий факт:

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

Пусь $a = (a_1, \ldots, a_s) \in A$. Пусть $p^k \cdot a = 0$ для некоторого k. Тогда для каждого множителя верно:

$$p^k a \equiv 0 \mod p_i^{k_i}$$

Если $p_i \neq p$, то получаем, что $a_i \equiv 0 \mod p_i^{k_i}$. Отсюда следует противоположное включение:

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

Теперь будет достаточно показать, что разложение опеределено однозначно для каждого $T_p(A)$, поскольку сами $T_p(A)$ определены явно и однозначно.

Для сокращения записи обозначим $T_p(A)$ как B.

Знаем, что $B \simeq \mathbb{Z}_{p^{m_1}} \times \ldots \times \mathbb{Z}_{p^{m_r}}$, из чего следует достаточно простой факт: $|B| = p^m,\ m = m_1 + \ldots + m_r$.

Теперь докажем единственность разложения индукцией по m.

База: $m = 1$. Тогда $|B| = p \Rightarrow B \simeq \mathbb{Z}_p$ по следствию 5 теоремы Лагранжа.

Шаг: Рассмотрим группы $pB \simeq p\mathbb{Z}_{p^{m_1}} \times p\mathbb{Z}_{p^{m_r}}$, при этом если $\exists i : m_i = 1$, то множитель $\mathbb{Z}_{p^{m_i}}$ исчезает.

$|pB| < |B| \Rightarrow$ применяем предположение индукции. Тогда для каждого $i : m_i > 1$ однозначно определены числа $m_i - 1$, а значит, однозначно определены и они сами. Оставшиеся m_i, которые были равны 1, мы можем восстановить из равенства $m = m_1 + \ldots + m_r$. $\square$

11 Экспонента конечной абелевой группы и критерий цикличности.

Определение 11.1. *Экспонентой* конечной абелевой группы A называется число $\exp A$, равное наименьшему общему кратному порядков элементов из A. Легко заметить, что это равносильно следующему условию:

$$\exp A = \min\{n \in \mathbb{N} \mid na = 0 \text{ для всех } a \in A\}$$

Замечание 5. $\forall a \in A, ord(a)$ делит $|A| \Rightarrow |A|$ это общее кратное множества $\{ord(a) \mid a \in A\} \Rightarrow expA$ делит $|A|$.

В частности $expA \leq |A|$

Предложение 11.1. *$expA = |A| \iff A$ циклическая группа*

Доказательство. $|A| = n = p_1^{k_1} \dots p_s^{k_s}$ разложение на простые.

- $\Leftarrow$ A цикличесая $\Rightarrow$ ее порождающая имеет порядок $n \Rightarrow expA = n$.
- $\Rightarrow$ $expA = n$. $\forall i \; \exists a_i \in A$, такое что $ord(a_i) = p_i^{k_i} \cdot m_i$, (в аддитивной запись группы) где $m_i \in \mathbb{N}$

  Положим $c_i = m_i \cdot a_i$, тогда $ord(c_i) = p_i^{k_i}$ ($p_i^k \cdot (m_i \cdot a_i) = p_i^k \cdot c_i = 1$ – минимальное такое по определению порядка a_i, значит, порядок c_i именно такой).

  Возьмем $c = c_1 + \dots + c_s$.

  Пусть $mc = 0$ для некоторого $m \in \mathbb{N}$, то есть $mc_1 + \dots + mc_s = 0$.

  Для фиксированного $i = 1, \dots, s$ умножим выражение на $\dfrac{n}{p_i^{k_i}}$.

  При $j \neq i$:

  $$\frac{n}{p_i^{k_i}} \cdot m \cdot c_j = 0.$$

  (потому что в $n/p_i^{k_i}$ присутствуют все порядки как множители, кроме i).

  Тогда отдельно рассмотрим наше равенство с полученным знанием:

  $$\frac{n}{p_i^{k_i}} \cdot m \cdot c_i = 0 \Rightarrow \frac{n}{p_i^{k_i}} \cdot m \; \vdots \; p_i^{k_i} \Rightarrow m \; \vdots \; p_i^{k_i}$$

  Предпоследний переход связан с опеределением порядка, последний переход верен потому что в левом множителе заведомо нет делящихся множителей.

  Тогда получаем: $m \; \vdots \; p_i^{k_i}, \forall i \Rightarrow m \; \vdots \; n \Rightarrow ord(c) = n \Rightarrow A = \langle c \rangle$.

$\square$

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

Пусть у нас есть G - конечная абелева группа. И так же есть элемент $g \in \mathbb{G}$, для которого $ord(g)$ будет достаточно большим значением.

Задача 12.1. Задача дискретного логаримирования

Дано: $h \in \langle g \rangle$. Найти такое α, что $g^\alpha = h$.

Возведение в степень, задача более "простая"с технической стороны реализации – существует алгоритм бинарного возведения в степень: $g^{16} = (((g^2)^2)^2)^2$. А сама же задача нахождения степени решается только переборными и близкими к перебору способами.

Задача 12.2. Система Диффи-Хеллмана обмена ключами

G, g - известно 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^α. B совершает аналогичные действия, $\beta \in \mathbb{N}$, g^β.

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 шифрованный канал связи, к которому никто не имеет доступа. При этом действительно в силу сложности задачи дискретного логарифмирования по g^α и g^β нельзя быстро получить $g^{\alpha\beta}$.

Задача 12.3. Криптография Эль-Гамаля

$\mathbb{G}, g$ - известно всем, причем g имеет достаточно большой порядок.

A фиксирует свое секретное $\alpha \in \mathbb{N}$ и сообщает всем пользователям g^α.

B хочет передать для A элемент $h \in G$.

Для этого B фиксирует какое-то $k \in \mathbb{N}$ и объявляет пару $\{g^k, h \cdot (g^\alpha)^k\}$. Отсюда $h = (h \cdot (g^\alpha)^k) \cdot ((g^k)^\alpha)^{-1} = (h \cdot (g^\alpha)^k) \cdot (g^k)^{|G|-\alpha}$, то есть зная α можно легко получить h отсюда следует, что получить его может A, а всем остальным придется решать задачу дискретного логарифмирования.

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

Определение 13.1. *Кольцом* называется множество R с двумя бинарными операциями «+» (сложение) и «×» (умножение), обладающими следующими свойствами:

1. $(R,+)$ является абелевой группой (называемой *аддитивной группой* кольца R);
2. выполнены *левая и правая дистрибутивности*, т.е.

$$a(b+c) = ab + ac \quad \text{и} \quad (b+c)a = ba + ca \quad \forall\, a,b,c \in R.$$

   В этом курсе мы рассматриваем только ассоциативные кольца с единицей, поэтому дополнительно считаем, что выполнены ещё два свойства:

3. $a(bc) = (ab)c$ для всех $a,b,c \in R$ (*ассоциативность умножения*);
4. существует такой элемент $1 \in R$ (называемый *единицей*), что

$$a1 = 1a = a \ \forall\, a \in R.$$

Замечание 6. В произвольном кольце R выполнены равенства

$$a0 = 0a = 0 \text{ для всякого } a \in R.$$

В самом деле, имеем $a0 = a(0+0) = a0 + a0$, откуда $0 = a0$. Аналогично устанавливается равенство $0a = 0$.

Замечание 7. Если кольцо R содержит более одного элемента, то $0 \neq 1$. Это следует из соотношений выше.

Примеры колец:

(1) числовые кольца $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$;

(2) кольцо $\mathbb{Z}_n$ вычетов по модулю n;

(3) кольцо $\mathrm{Mat}(n \times n, \mathbb{R})$ матриц с коэффициентами из $\mathbb{R}$;

(4) кольцо $\mathbb{R}[x]$ многочленов от переменной x с коэффициентами из $\mathbb{R}$;

(5) кольцо $\mathbb{R}[[x]]$ *формальных степенных рядов* от переменной x с коэффициентами из $\mathbb{R}$:

$$\mathbb{R}[[x]] := \{\sum_{i=0}^{\infty} a_i x^i \mid a_i \in \mathbb{R}\};$$

(6) кольцо $\mathcal{F}(M, \mathbb{R})$ всех функций из множества M во множество $\mathbb{R}$ с операциями поточечного сложения и умножения:

$$(f_1+f_2)(m) := f_1(m)+f_2(m); \quad (f_1f_2)(m) := f_1(m)f_2(m) \quad \text{для всех} \quad f_1,f_2 \in \mathcal{F}(M,\mathbb{R}), m \in M.$$

Замечание 8. В примерах вместо $\mathbb{R}$ можно брать любое кольцо, в частности $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{C}$, $\mathbb{Z}_n$.

Замечание 9. Обобщая пример, можно рассматривать кольцо $\mathbb{R}[x_1, \ldots, x_n]$ многочленов от нескольких переменных $x_1, \ldots, x_n$ с коэффициентами из $\mathbb{R}$.

Определение 13.2. Кольцо R называется *коммутативным*, если $ab = ba$ для всех $a,b \in R$.

Все перечисленные в примерах кольца, кроме $\mathrm{Mat}(n \times n, \mathbb{R})$ при $n \geqslant 2$, коммутативны. Пусть R — кольцо.

Определение 13.3. Элемент $a \in R$ называется *обратимым*, если найдётся такой $b \in R$, что $ab = ba = 1$. Такой элемент b обозначается классическим образом через a^{-1}.

Замечание 10. Все обратимые элементы кольца R образуют группу относительно операции умножения.

Определение 13.4. Элемент $a \in R$ называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и найдётся такой $b \in R$, $b \neq 0$, что $ab = 0$ (соответственно $ba = 0$).

Замечание 11. В случае коммутативных колец понятия левого и правого делителей нуля совпадают, поэтому говорят просто о делителях нуля.

Замечание 12. Все делители нуля в R необратимы: если $ab = 0$, $a \neq 0$, $b \neq 0$ и существует a^{-1}, то получаем $a^{-1}ab = a^{-1}0$, откуда $b = 0$ — противоречие.

Определение 13.5. Элемент $a \in R$ называется *нильпотентом*, если $a \neq 0$ и найдётся такое $m \in \mathbb{N}$, что $a^m = 0$.

Замечание 13. Всякий нильпотент в R является делителем нуля: если $a \neq 0$, $a^m = 0$ и число m наименьшее с таким свойством, то $m \geqslant 2$ и $a^{m-1} \neq 0$, откуда $aa^{m-1} = a^{m-1}a = 0$.

Определение 13.6. *Полем* называется коммутативное ассоциативное кольцо K с единицей, в котором всякий ненулевой элемент обратим.

Замечание 14. Тривиальное кольцо $\{0\}$ полем не считается, поэтому $0 \neq 1$ в любом поле.

Примеры полей: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$.

Предложение 13.1. *Кольцо вычетов $\mathbb{Z}_n$ является полем тогда и только тогда, когда n — простое число.*

Доказательство. Если число n составное, то $n = mk$, где $1 < m, k < n$. Тогда $\overline{m}\overline{k} = \overline{n} = \overline{0}$. Следовательно, $\overline{k}$ и $\overline{m}$ — делители нуля в $\mathbb{Z}_n$, ввиду чего не все ненулевые элементы там обратимы.

Если $n = p$ — простое число, то возьмём произвольный ненулевой вычет $\overline{a} \in \mathbb{Z}_p$ и покажем, что он обратим. Тогда НОД$(a, p) = 1 \Rightarrow \ \exists r, s \in \mathbb{Z}$, такие что $ar + sp = 1 \Rightarrow \overline{ar} + \overline{sp} = \overline{1} \Rightarrow \overline{ar} = \overline{1}$ $(\overline{sp} = 0)$ $\square$

Определение 13.7. *Подкольцом* кольца R называется всякое подмножество $R' \subseteq R$, замкнутое относительно операций сложения и умножения (т. е. $a + b \in R'$ и $ab \in R'$ для всех $a,b \in R'$) и являющееся кольцом относительно этих операций. *Подполем* называется всякое подкольцо, являющееся полем.

Например, $\mathbb{Z}$ является подкольцом в $\mathbb{Q}$, а скалярные матрицы образуют подполе в кольце $\mathrm{Mat}(n \times n, \mathbb{R})$.

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

Определение 14.1. Подмножество I кольца R называется (*двусторонним*) *идеалом*, если оно является подгруппой по сложению и $ra \in I$, $ar \in I$ для любых $a \in I$, $r \in R$.

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

Замечание 15. Пусть R — коммутативное кольцо. С каждым элементом $a \in R$ связан идеал $(a) := \{ra \mid r \in R\}$.

Определение 14.2. Идеал I называется *главным*, если существует такой элемент $a \in R$, что $I = (a)$. (В этой ситуации говорят, что I порождён элементом a.)

Пример. В кольце $\mathbb{Z}$ подмножество $k\mathbb{Z}$ ($k \in \mathbb{Z}$) является главным идеалом, порождённым элементом k. Более того, все идеалы в $\mathbb{Z}$ являются главными.

Замечание 16. Главный идеал (a) является несобственным тогда и только тогда, когда $a = 0$ или a обратим.

Более общо, с каждым подмножеством $S \subseteq R$ связан идеал

$$(S) := \{r_1 a_1 + \ldots + r_k a_k \mid a_i \in S, r_i \in R, k \in \mathbb{N}\}.$$

(Проверьте, что это действительно идеал!) Это наименьший по включению идеал в R, содержащий подмножество S. В этой ситуации говорят, что идеал $I = (S)$ порождён подмножеством S.

Вернёмся к случаю произвольного кольца R. Поскольку любой идеал I является подгруппой абелевой группы $(R,+)$, мы можем рассмотреть факторгруппу R/I. Введём на ней умножение по формуле

$$(a + I)(b + I) := ab + I.$$

Покажем, что это определение корректно. Пусть элементы $a',b' \in R$ таковы, что $a' + I = a + I$ и $b' + I = b + I$. Проверим, что $a'b' + I = ab + I$. Заметим, что $a' = a + x$ и $b' = b + y$ для некоторых $x, y \in I$. Тогда

$$a'b' + I = (a + x)(b + y) + I = ab + ay + xb + xy + I = ab + I,$$

поскольку $ay, xb, xy \in I$ в силу определения идеала.

Замечание 17. Множество R/I является кольцом относительно имеющейся там операции сложения и только что введённой операции умножения.

Определение 14.3. Кольцо R/I называется *факторкольцом* кольца R по идеалу I.

Пример. $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$.

Определение 14.4. *Гомоморфизм* колец $f : A \to B$ это отображение, для которого выполнены свойства:

1. $f(a+b) = f(a) + f(b)$, $\forall a, b \in A$

2. $f(ab) = f(a)f(b)$, $\forall a, b \in A$

3. $f(1_A) = 1_B$

Определение 14.5. *Изоморфизмом* колец называется всякий гомоморфизм, являющийся биекцией.

Пусть $\varphi \colon R \to R'$ — гомоморфизм колец. Тогда определены его ядро $\mathrm{Ker}\varphi = \{r \in R \mid \varphi(r) = 0\}$ и образ $\mathrm{Im}\varphi = \{\varphi(r) \mid r \in R\} \subseteq R'$.

Лемма 14.1. *Ядро* $\mathrm{Ker}\varphi$ *является идеалом в* R.

Доказательство. Так как φ — гомоморфизм абелевых групп, то $\mathrm{Ker}\varphi$ является подгруппой в R по сложению. Покажем теперь, что $ra \in \mathrm{Ker}\varphi$ и $ar \in \mathrm{Ker}\varphi$ для произвольных элементов $a \in \mathrm{Ker}\varphi$ и $r \in R$.

Имеем $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, откуда $ra \in \mathrm{Ker}\varphi$. Аналогично получаем $ar \in \mathrm{Ker}\varphi$. □

Замечание 18. $\mathrm{Im}\varphi$ — подкольцо в R'.

Теорема 14.1. Теорема о гомоморфизме для колец.
Пусть $\varphi \colon R \to R'$ *– гомоморфизм колец. Тогда имеет место изоморфизм*

$$R/\mathrm{Ker}\,\varphi \cong \mathrm{Im}\varphi.$$

Доказательство. Положим для краткости $I = \mathrm{Ker}\varphi$ и рассмотрим отображение

$$\pi \colon R/I \to \mathrm{Im}\varphi, \quad a + I \mapsto \varphi(a).$$

Из доказательства теоремы о гомоморфизме для групп следует, что отображение π корректно определено и является изоморфизмом абелевых групп (по сложению). Покажем, что π — изоморфизм колец. Для этого остаётся проверить, что π сохраняет операцию умножения:

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

□

Пример 4.

1. Пусть $R = \mathcal{F}(M, \mathbb{R})$. Зафиксируем произвольную точку $m_0 \in M$ и рассмотрим гомоморфизм $\varphi \colon R \to \mathbb{R}$, $f \mapsto f(m_0)$. Ясно, что гомоморфизм φ сюръективен. Его ядром является идеал I всех функций, обращающихся в нуль в точке m_0. По теореме о гомоморфизме получаем $R/I \cong \mathbb{R}$.

2. Рассмотрим отображение $\varphi \colon \mathbb{R}[x] \to \mathbb{C}$, $f \mapsto f(i)$. Очевидно, что φ — гомоморфизм, причем сюръективный. Если многочлен f принадлежит ядру φ, то есть $f(i) = 0$, то $(x - i) \mid f$ в кольце $\mathbb{C}[x]$. Но и сопряженный к корню также будет являться корнем многочлена, так что дополнительно $(x+i) \mid f$. Итого, получаем, что $f \in (x-i)(x+i) = (x^2+1)$ и, соответственно, $\mathrm{Ker}\varphi \subseteq (x^2+1)$. В обратную сторону включение тем более очевидно. Далее, по теореме о гомоморфизме получаем $\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}$.

15 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

Далее в этой лекции всюду предполагается, что R — коммутативное кольцо без делителей нуля.

Определение 15.1. Говорят, что элемент $b \in R$ *делит* элемент $a \in R$ (b — *делитель* a, a *делится* на b; пишут $b \,|\, a$) если существует элемент $c \in R$, для которого $a = bc$.

Определение 15.2. Два элемента $a, b \in R$ называются *ассоциированными*, если $a = bc$ для некоторого обратимого элемента c кольца R.

Пример 5. В кольце $\mathbb{Z}$ ассоциированными элементами являются a и $-a$ (-1 обратим).

Замечание 19.

1. Легко видеть, что отношение ассоциированности является отношением эквивалентности на кольце R.

2. a, b ассоциированы $\Leftrightarrow a \mid b$ и $b \mid a$

Определение 15.3. *Наибольшим общим делителем* элементов a и b кольца R называется их общий делитель, который делится на любой другой их общий делитель. Он обозначается (a,b).

Определение 15.4. Кольцо R называется *кольцом главных идеалов*, если всякий идеал в R является главным.

Пример 6. Кольцо $\mathbb{Z}$, в котором все идеалы выглядят как $\langle k \rangle$.

Замечание 20. Если наибольший общий делитель двух элементов $a,b \in R$ существует, то он определён однозначно с точностью до ассоциированности, т. е. умножения на обратимый элемент кольца R.

Теорема 15.1. *Пусть R — кольцо главных идеалов и a,b — произвольные элементы. Тогда:*

1. *существует наибольший общий делитель (a,b);*

2. *существуют такие элементы $u,v \in R$, что $(a,b) = ua + vb$.*

Доказательство.

Способ 1: утверждение (1) получается применением (прямого хода) алгоритма Евклида, а утверждение (2) — применением обратного хода в алгоритме Евклида.

Способ 2: рассмотрим идеал $I = (a, b)$. Так как R — кольцо главных идеалов, то существует такой элемент $d \in R$, что $I = (d)$. Тогда $a = da', b = db' \Rightarrow d$ общий делитель элементов a, b. Также так как $(d) = (a,b)$, то получим, что всякий элемент (d) выражется какой-то комбинацией элементов a и b, то есть $d = ax + by$ для некоторых $x, y \in R$.

Теперь пусть d' – другой общий делитель a и b, тогда $d' \mid a$ и $d' \mid b$. Из линейного выражения понятно, что в таком случае $d' \mid d$, из чего нетрудно сделать вывод о том, что d действительно наибольший общий делитель.

□

16 Простые элементы. Факториальные кольца. Факториальность колец главных идеалов: доказательство существования разложения на простые множители

Здесь R коммутативное кольцо без делителей нуля.

Определение 16.1. Ненулевой необратимый элемент p кольца R называется *простым*, если он не может быть представлен в виде $p = ab$, где $a, b \in R$ — необратимые элементы.

Замечание 21. Простые элементы в кольце многочленов $K[x]$ над полем K принято называть *неприводимыми многочленами.*

Лемма 16.1. *Если простой элемент p евклидова кольца R делит произведение $a_1a_2 \ldots a_n$, то он делит один из сомножителей.*

Доказательство. Индукция по n. Пусть $n = 2$ и предположим, что p не делит a_1. Тогда $(p, a_1) = 1$ и по теореме о НОД найдутся такие элементы $u, v \in R$, что $1 = up + va_1$. Умножая обе части этого равенства на a_2, получаем

$$a_2 = upa_2 + va_1a_2.$$

Легко видеть, что p делит правую часть последнего равенства, поэтому p делит и левую часть, т. е. a_2.

При $n > 2$ применяем предыдущее рассуждение к $(a_1 \ldots a_{n-1})a_n$.
$p \mid a_1a_2...a_n \Rightarrow p \mid (a_1 \ldots a_{n-1})a_n$
$\Rightarrow$ либо $p \mid a_n$, либо $p \mid a_1 \ldots a_{n-1}$
$\Rightarrow$ применяем предположение индукции. □

Определение 16.2. Кольцо R называется *факториальным*, если всякий его ненулевой необратимый элемент «разложим на простые множители», т. е. представим в виде произведения (конечного числа) простых элементов, причём это представление единственно с точностью до перестановки множителей и ассоциированности.

Более формально единственность разложения на простые множители следует понимать так: если для элемента $a \in R$ есть два представления

$$a = p_1p_2 \ldots p_n = q_1q_2 \ldots q_m,$$

где все элементы p_i, q_j простые, то $n = m$ и q_j можно переставить так, что $\forall q_i = \varepsilon_i p_i$, где $\varepsilon_i \in R$ обр. элемент.

Докажем вспомогательную лемму:

Лемма 16.2. *R – кольцо главных идеалов и $I_1 \subseteq I_2 \subseteq I_3 \subseteq \ldots$ – бесконечная цепь вложенных идеалов.*

Тогда $\exists k : I_k = I_{k+1} = I_{k+1} = \ldots$.

Доказательство. Положим $I = \bigcup_{i=1}^{\infty} I_i$. Можно понять (это упражнение), что I – идеал. Тогда $\forall i : I_i \subseteq I$.

Так как R – кольцо главных идеалов, то $\exists a : I = (a)$. Из этого следует, что $\exists k : a \in I_k$. Тогда верна следующая цепочка:

$$I = (a) \subseteq I_k \subseteq I_{k+1} \subseteq \ldots$$

В силу обратного включения получаем:

$$I = I_k = I_{k+1} = \dots$$

□

Теорема 16.1. *R – кольцо главных идеалов $\Rightarrow$ R – факториально.*

Доказательство. Пусть $a \in R$ – необратимый ненулевой.

Покажем существование разложения на простые.

От противного – предположим, что a нельзя разложить на простые. Тогда a сам не является простым, из чего следует, что $a = a_1 b_1$. Теперь либо a_1, либо b_1 не разлагается на простые. Для определенности предположим, что a_1.

В таком случае он сам не является простым и $a_1 = a_2 b_2$ и так далее. Получаем бесконечную цепочку:

$$a, a_1, a_2, \dots$$

Причем её особенностью является то, что $a \vdots a_1, a_1 \vdots a_2, \dots$. Тогда у нас есть бесконечная цепочка вложенных и не совпадающих идеалов:

$$(a) \subset (a_1) \subseteq (a_2) \subseteq \dots$$

что является противоречием с предыдущей леммой. □

17 Простые элементы. Факториальные кольца. Факториальность колец главных идеалов: доказательство единственности разложения на простые множители

Теорема 17.1. *R – кольцо главных идеалов $\Rightarrow$ R – факториально.*

Доказательство. Докажем единственность разложения.

Пусть $a = p_1p_2\dots p_n = q_1q_2\dots q_m$ – два разложения на простые.

Индукция по n:

База: $n = 1$, то $a = p_1$ – простое, тогда и $m = 1 : p_1 = q_1$.

Шаг: $n \geqslant 2$. $p_1 \mid q_1 \dots q_m \Rightarrow \exists i : p_1 \mid q_i$ Поставим элемент i на первое место. В силу простоты q_1 получаем $q_1 = \varepsilon \cdot p_1$, где $\varepsilon \in R$ – обратимый.

Так как в R нет делителей нуля, то можем сократить по делителю:

$$ab = ac \Rightarrow ab - ac = 0 \Rightarrow a(b - c) = 0,\ a \neq 0 \Rightarrow b = c$$

В таком случае применяем предположение индукции и побеждаем. □

Далеко не все кольца факториальны:

Пример 7. $R = \mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} \mid a,b \in \mathbb{Z}\}$ не факториально:

$$6 = 2 \cdot 3 = (1 + \sqrt{-5})(1 - \sqrt{-5})$$

Можно убедиться, что это конечные разложения.

Но при этом не все факториальные кольца являются кольцами главных идеалов:

Пример 8. $R = K[x_1, x_2, \dots, x_k]$ не является кольцом главных идеалов: идеал (x_1, x_2) не главный.

18 Теорема о том, что кольцо многочленов над полем является кольцом главных идеалов

K – поле. Рассмотрим $K[x] := \{a_n x^n + \dots a_1 x + a_0 \mid a_i \in K\}$
Для любого $f \in K[x]$ определена его степень $\deg f$.

Теорема 18.1. *Деление с остатком*
$\forall f,g \in K[x],\ g \neq 0,\ \exists! q,r \in K[x]$,*такие что:*

$$f = q \cdot g + r,$$

где r называется остатком и либо $r = 0$, либо $\deg r < \deg g$.

Доказательство. Следует из алгоритма деления в столбик. □

Теорема 18.2. *K – поле $\Rightarrow K[x]$ – кольцо главных идеалов.*

Доказательство. Рассмотрим $I \subseteq K[x]$ – произвольный идеал.
Если $I = \{0\} \Rightarrow I = (0)$ – главный.
Теперь рассмотрим $I \neq \{0\}$. Рассмотрим элемент наименьшей степени $g \in I \Rightarrow (g) \subseteq I$.
Рассмотрим какой-то другой элемент $f \in I$. Поделим на g с остатком:

$$f = q \cdot g + r$$

В силу линейного выражения $q,r \in I$.
В силу минимальности степени g получаем, что $r = 0$, из чего следует, что $I = (g)$. □

Следствие 18.1. $\forall f,g \in K[x]\ \exists u,v$:

$$(f,g) = u \cdot f + v \cdot g$$

Замечание 22. (f,g) и линейное выражение можем находить при помощи алгоритма Евклида.

Следствие 18.2. *K – поле. Тогда $K[x]$ – факториально.*

Замечание 23. f – многочлен.

1. Если $\deg f = 1 \Rightarrow f$ – неприводимый.
2. $\deg f \geqslant 2$, f – неприводим, тогда f не имеет корней (простое следствие из теоремы Безу).
3. $\deg f \in \{2, 3\} \iff f$ не имеет корней.

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

Предлагается воспользоваться более адекватными конспектами.
Здесь

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

Здесь

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

Здесь

22 S-многочлены. Критерий Бухбергера.

Здесь

23 Базис Грёбнера идеала в кольце многочленов от нескольких переменных, теорема о трех эквивалентных условиях. Решение задачи вхождения многочлена в идеал

Здесь

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

Здесь

25 Лемма Диксона. Теорема о существовании конечного базиса Грёбнера в идеале многочленов от нескольких переменных. Теорема Гильберта о базисе идеала

Здесь

26 Характеристика поля и простое подполе

Мы знаем не так много примеров полей. Это бесконечные поля $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ и конечные поля $\mathbb{Z}_p$, где p — простое число. Конструкция поля отношений позволяет строить новые поля из уже имеющихся. А именно, если K — произвольное поле, то можно рассмотреть поле отношений $K(x)$ кольца многочленов $K[x]$ (это поле называется *полем рациональных дробей* над K). Элементами поля $K(x)$ являются дроби $f(x)/g(x)$, где $f(x), g(x) \in K[x]$ и $g(x) \neq 0$.

Несколько других примеров полей:

$$\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\},$$
$$\mathbb{Q}(\sqrt[3]{2}) = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\},$$
$$\mathbb{Q}(\sqrt{-1}) = \{a + b\sqrt{-1} \mid a, b \in \mathbb{Q}\}.$$

Определение 26.1. Пусть K — произвольное поле. *Характеристикой* поля K называется такое наименьшее натуральное число p, что $\underbrace{1 + \ldots + 1}_{p} = 0$. Если такого натурального p не существует, говорят, что характеристика поля равна нулю. Обозначение: $\mathrm{char} K$.

Например, $\mathrm{char}\mathbb{Q} = \mathrm{char}\mathbb{R} = \mathrm{char}\mathbb{C} = 0$ и $\mathrm{char}\mathbb{Z}_p = \mathrm{char}\mathbb{Z}_p(x) = p$.

Из определения следует, что всякое поле характеристики нуль бесконечно. Примером бесконечного поля характеристики $p > 0$ является поле $\mathbb{Z}_p(x)$.

Предложение 26.1. *Характеристика произвольного поля K либо равна нулю, либо является простым числом.*

Доказательство. Положим $p = \mathrm{char} K$ и предположим, что $p > 0$. Так как $0 \neq 1$ в K, то $p \geqslant 2$. Если число p не является простым, то $p = mk$ для некоторых $m, k \in \mathbb{N}$, $1 < m, k < p$. Тогда в K верно равенство

$$0 = \underbrace{1 + \ldots + 1}_{mk} = (\underbrace{1 + \ldots + 1}_{m})(\underbrace{1 + \ldots + 1}_{k}).$$

В силу минимальности числа p в последнем выражении обе скобки отличны от нуля, но такое невозможно, так как в поле нет делителей нуля. $\square$

Замечание 24. Пересечение любого семейства подполей фиксированного поля K является подполем в K. В частности, для всякого подмножества $S \subseteq K$ существует наименьшее по включению подполе в K, содержащее S. Это подполе совпадает с пересечением всех подполей в K, содержащих S.

Из приведённого выше замечания следует, что в каждом поле существует наименьшее по включению подполе, оно называется *простым подполем.*

Предложение 26.2. *Пусть K — поле и K_0 — его простое подполе. Тогда:*

1. *если* $\mathrm{char} K = p > 0$, *то* $K_0 \cong \mathbb{Z}_p$*;*
2. *если* $\mathrm{char} K = 0$, *то* $K_0 \cong \mathbb{Q}$.

Доказательство. Пусть $\langle 1 \rangle \subseteq K$ — циклическая подгруппа по сложению, порождённая единицей. Заметим, что $\langle 1 \rangle$ — подкольцо в K. Поскольку всякое подполе поля K содержит единицу, оно содержит и множество $\langle 1 \rangle$. Следовательно, $\langle 1 \rangle \subseteq K_0$.

Если $\mathrm{char} K = p > 0$, то мы имеем изоморфизм колец $\langle 1 \rangle \simeq \mathbb{Z}_p$. Но, как мы уже знаем, кольцо $\mathbb{Z}_p$ является полем, поэтому $K_0 = \langle 1 \rangle \simeq \mathbb{Z}_p$.

Если же $\mathrm{char} K = 0$, то мы имеем изоморфизм колец $\langle 1 \rangle \cong \mathbb{Z}$. Тогда, в силу того, что K_0 – поле, для любого $a \in \langle 1 \rangle \subseteq K_0$ существует обратный элемент $1/a$. Следовательно, K_0 содержит все дроби вида a/b, где $a,b \in \langle 1 \rangle$ и $b \neq 0$. Ясно, что все такие дроби образуют поле, изоморфное полю $\mathbb{Q}$. $\square$

27 Расширение полей. Конечное расширение и его степень. Степень композиции двух расширений.

Определение 27.1. Если K — подполе поля F, то говорят, что F — *расширение* поля K.

Например, всякое поле есть расширение своего простого подполя.

Определение 27.2. *Степенью* расширения полей $K \subseteq F$ называется размерность поля F как векторного пространства над полем K. Обозначение $[F : K]$.

Например, $[\mathbb{C} : \mathbb{R}] = 2$ и $[\mathbb{R} : \mathbb{Q}] = \infty$.

Определение 27.3. Расширение полей $K \subseteq F$ называется *конечным*, если $[F : K] < \infty$.

Предложение 27.1. *Пусть $K \subseteq F$ и $F \subseteq L$ — конечные расширения полей. Тогда расширение $K \subseteq L$ также конечно и $[L : K] = [L : F][F : K]$.*

Доказательство. Пусть $e_1, \ldots, e_n$ — базис F над K и $f_1, \ldots, f_m$ — базис L над F. Достаточно доказать, что множество

$$\{e_i f_j \mid i = 1, \ldots, n;\ j = 1, \ldots, m\}$$

является базисом L над K. Для этого сначала покажем, что произвольный элемент $a \in L$ представим в виде линейной комбинации элементов с коэффициентами из K.

$$a = \sum_{i=1}^{m} \alpha_i f_i,$$

где $\alpha_i \in F$,

$$\alpha_i = \sum_{j=1}^{n} \beta_{ij} e_j,$$

где $\beta_{ij} \in K$.

Тогда

$$a = \sum_{i=1}^{m} (\sum_{j=1}^{n} \beta_{ij} e_j) f_i = \sum_{i=1}^{m} \sum_{j=1}^{n} \beta_{ij} (e_j f_i).$$

Теперь проверим линейную независимость элементов.

Пусть

$$\sum_{i=1}^{m} \sum_{j=1}^{n} \gamma_{ij} (e_j f_i) = 0,$$

где $\gamma_{ij} \in K$. Переписав это равенство в виде

$$\sum_{j=1}^{m} \underbrace{(\sum_{i=1}^{n} \gamma_{ij} e_i)}_{F} f_j = 0$$

и воспользовавшись тем, что элементы $f_1, \ldots, f_m$ линейно независимы над F, мы получим $\sum\limits_{i=1}^{n} \gamma_{ij} e_i = 0$ для каждого $j = 1, \ldots, m$. Теперь из линейной независимости элементов $e_1, \ldots, e_n$ над K вытекает, что $\gamma_{ij} = 0$ при всех i,j. Таким образом, элементы базиса линейно независимы. $\square$

28 Критерий того, что фактокольцо кольца многочленов над полем является полем. Степень расширения этого поля.

K – поле. $h = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$, $\deg h = n > 0$.
Положим $F := K[x]/(h)$. $f \in K[x], \bar{f} = f + (h) \in F$.

Предложение 28.1. *F – поле $\iff$ h – неприводим.*

Доказательство.

- $\Rightarrow$ Пусть приводим, то есть $h = h_1 \cdot h_2, \deg h_i < \deg h$. Тогда $\bar{h}_1 \cdot \bar{h}_2 = \bar{h} = \bar{0}$. В связи с тем, что $\deg h_i < \deg h$ получем, что $h_1, h_2 \notin (h)$, откуда следует, что $\bar{h}_1, \bar{h}_2 \neq \bar{0}$, что означает существование делителей нуля, противоречие.

- $\Leftarrow$ Известно, что F – коммутативное кольцо с единицей. Достаточно показать, что всякий элемент обратим.

  Рассмотрим $f \in K[x], \bar{f} \neq 0$. Так как $f \not\vdots\, h \Rightarrow (f,h) = 1 \Rightarrow \exists u, v \in K[x]$:
  $$uf + vh = 1 \Rightarrow \bar{u}\bar{f} + \bar{v}\bar{h} = \bar{1} \Rightarrow \bar{u}\bar{f} = \bar{1}.$$
  Отсюда видно, что f обратим.

□

Пример 9.

1. $\mathbb{R}[x]/(x^2+1)$ – поле ($\simeq \mathbb{C}$).

2. $\mathbb{R}[x]/(x^2+x)$ – не поле.

Предложение 28.2. $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ *– базис F_K, в частности, расширение конечно и $[F : K] = n$.*

Доказательство.
1) $f \in K[x]$. Разделим на h с остатком:
$$f = g \cdot h + r, \begin{cases} r = 0 \\ \deg r < \deg h \end{cases}$$
Отсюда видно, что $\bar{f} = \bar{r} \in \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1} \rangle$.
Теперь покажем линейную независимость.
$$\beta_0 \bar{1} + \ldots + \beta_{n-1}\bar{x}^{n-1} = 0 \Rightarrow$$
$$\overline{\beta_0 + \ldots + \beta_{n-1} x^{n-1}} = \bar{0}.$$
Тогда $g = \beta_0 + \ldots + \beta_{n-1}x^{n-1} \in (h)$. Но поскольку $\deg g < \deg h \Rightarrow \beta_0 + \ldots + \beta_{n-1}x^{n-1} = 0$, откуда следует, что $\beta_i = 0$.
2) Покажем, что в F корнем многочлена h будет $\bar{x}$:
$$h(\bar{x}) = a_n \bar{x}_n^n + \ldots a_1 \bar{x} + a_0 \bar{1} = \overline{a_n x_n^n + \ldots a_1 x + a_0} = \bar{h}(x) = 0$$

□

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

Теорема 29.1. *Пусть K — произвольное поле и $f(x) \in K[x]$ — многочлен положительной степени. Тогда существует конечное расширение $K \subseteq F$, в котором многочлен $f(x)$ имеет корень.*

Доказательство. Если f – приводим, то он уже имеет корень, а значит, степень расширения равна 1.

Рассмотрим случай, когда f – неприводим. Тогда мы знаем, что $K[x]/(f)$ – поле, которое является конечным расширением K. Покажем, что его корнем будет $\bar{x}$:

$$h(\bar{x}) =$$
$$a_n\bar{x}^n + \ldots + a_1\bar{x} + a_0 = \overline{(a_nx^n + \ldots + a_0)} = \bar{h}(x) = 0$$

□

Следствие 29.1. $\forall f \in K[x] \exists F \subseteq K$ *– конечное расширение, что f разлагается на линейные множители.*

Доказательство. Индукция по $\deg f$.

База: $\deg f = 1$ – уже разлагается,

Шаг: Если у f есть корень α, то поделим многочлен на $x-\alpha$ и применим предположение индукции. Если же корня нет, то расширим поле и получим, что у него есть корень и снова применим предположение индукции. Так как на каждом из конечного числа шагов расширение конечное, то итоговое расширение также конечно. □

Говорят, что поле $K[x]/(p(x))$ получено из поля K *присоединением корня* неприводимого многочлена $p(x)$. Нетрудно проверить, что если α — некоторый корень многочлена $p(x)$ в $K[x]/(p(x))$, то поле $K[x]/(p(x))$ совпадает с подполем $K(\alpha)$.

Определение 29.1. Пусть K — некоторое поле и $f(x) \in K[x]$ — многочлен положительной степени. *Полем разложения* многочлена $f(x)$ называется такое расширение F поля K, что

(1) многочлен $f(x)$ разлагается над F на линейные множители;

(2) в F нет меньших подполей со свойством 1) $\Leftrightarrow$ корни многочлена $f(x)$ не лежат ни в каком меньшем подполе.

Пример 10. Рассмотрим многочлен $f(x) = x^4 + x^3 + x^2 + x + 1$ над $\mathbb{Q}$. Так как $(x-1)f(x) = x^5 - 1$, корнями многочлена $f(x)$ являются все корни степени 5 из единицы, отличные от единицы. Если присоединить к $\mathbb{Q}$ один из корней ϵ многочлена f, то его остальные корни можно получить, возводя число ϵ в натуральные степени. Таким образом, присоединение одного корня сразу приводит к полю разложения многочлена.

Пример 11. Многочлен $f(x) = x^3 - 2$ неприводим над полем $\mathbb{Q}$. Присоединение к полю $\mathbb{Q}$ корня этого многочлена приводит к полю $\mathbb{Q}[x]/(x^3 - 2) \cong \mathbb{Q}(\sqrt[3]{2})$. Данное поле не является полем разложения многочлена $f(x)$, поскольку в нём $f(x)$ имеет только один корень и не имеет двух других корней. Поскольку корнями данного многочлена являются числа

$$\sqrt[3]{2}, \quad \sqrt[3]{2}(-\frac{1}{2}+\frac{\sqrt{-3}}{2}), \quad \sqrt[3]{2}(-\frac{1}{2}-\frac{\sqrt{-3}}{2}),$$

полем разложения многочлена $f(x)$ является поле

$$F=\{\alpha_0+\alpha_1\sqrt[3]{2}+\alpha_2\sqrt[3]{4}+\alpha_3\sqrt{-3}+\alpha_4\sqrt[3]{2}\sqrt{-3}+\alpha_5\sqrt[3]{4}\sqrt{-3} \mid \alpha_i\in\mathbb{Q}\},$$

которое имеет над $\mathbb{Q}$ степень 6.

Теорема 29.2. *Поле разложения любого многочлена $f(x)\in K[x]$ существует и единственно с точностью до изоморфизма.*

30 Алгебраические и трансцендентные элементы. Минимальный многочлен алгебраического элемента и его свойства.

Пусть $K \subseteq F$ — расширение полей.

Определение 30.1. Элемент $\alpha \in F$ называется *алгебраическим* над подполем K, если существует ненулевой многочлен $f(x) \in K[x]$, для которого $f(\alpha) = 0$. В противном случае α называется *трансцендентным* элементом над K.

Пример 12. $\sqrt{2}, \sqrt{5}$ – алгебраические над $\mathbb{Q}$.
e, π – транцендентные над $\mathbb{Q}$

Определение 30.2. *Минимальным многочленом* алгебраического элемента $\alpha \in F$ над подполем K называется ненулевой многочлен $h_\alpha(x)$ наименьшей степени, для которого $h_\alpha(\alpha) = 0$.

Лемма 30.1. *Пусть $\alpha \in F$ — алгебраический элемент над K и $h_\alpha(x)$ — его минимальный многочлен. Тогда:*

(а) *$h_\alpha(x)$ определён однозначно с точностью до пропорциональности;*

(б) *для произвольного многочлена $f(x) \in K[x]$ равенство $f(\alpha) = 0$ имеет место тогда и только тогда, когда $h_\alpha(x)$ делит $f(x)$;*

(в) *$h_\alpha(x)$ является неприводимым многочленом над полем K (то есть, $h_\alpha(x)$ – простой элемент в поле $K[x]$).*

Доказательство.

Пусть $I \subseteq K[x]$ - идеал, состоящий из всех многочленов $f(x)$, таких что $f(\alpha) = 0$.

Т.к. $K[x]$ – кольцо главных идеалов, то $\exists g(x) \in K[x]$, такой что $I = (g(x)) \Rightarrow h \,\vdots\, g$
$\Rightarrow g = c \cdot h$ для некоторого $c \in K/\{0\}$

Отсюда сразу следуют (а) и (б).

Пусть $h(x) = h_1(x) \cdot h_2(x)$, где $degh_i(x) < degh(x)$.

Тк $h(\alpha) = 0$, то $\exists i$, такое что $h_i(\alpha) = 0$, что противоречит с минимальностью. □

31 Подполе в расширении полей, порожденное алгебраическим элементом.

Для каждого элемента $\alpha \in F$ обозначим через $K(\alpha)$ наименьшее подполе в F, содержащее K и α.

Предложение 31.1. *Пусть $\alpha \in F$ — алгебраический элемент над K и n — степень его минимального многочлена над K. Тогда*

$$K(\alpha) = \{\beta_0 + \beta_1\alpha + \ldots + \beta_{n-1}\alpha^{n-1} \mid \beta_0, \ldots, \beta_{n-1} \in K\}.$$

Кроме того, элементы $1, \alpha, \alpha^2, \ldots, \alpha^{n-1}$ линейно независимы над K.
В частности, $[K(\alpha) : K] = n$.

Иными словами, любой элемент из наименьшего подполя, содержащего K и α, представим в виде линейной комбинации степеней α, и степень расширения $K \subseteq K(\alpha)$ равна степени минимального многочлена.

Доказательство. Легко видеть, что

$$K(\alpha) = \{\frac{f(\alpha)}{g(\alpha)} \mid f(x), g(x) \in K[x], g(\alpha) \neq 0\}.$$

Действительно, такие элементы лежат в любом подполе поля F, содержащем K и α, и сами образуют поле. Теперь возьмём произвольный элемент $\frac{f(\alpha)}{g(\alpha)} \in K(\alpha)$ и покажем, что он представим в виде, указанном в условии. Пусть $h_\alpha(x) \in K[x]$ — минимальный многочлен элемента α над K. Поскольку $g(\alpha) \neq 0$, многочлен $h_\alpha(x)$ не делит $g(x)$. Но $h_\alpha(x)$ неприводим, поэтому $(g(x), h_\alpha(x)) = 1$. Значит, существуют такие многочлены $u(x), v(x) \in K[x]$, что $u(x)g(x)+v(x)h_\alpha(x) = 1$. Подставляя в последнее равенство $x = \alpha$, мы получаем $u(\alpha)g(\alpha) = 1$. Отсюда $\frac{f(\alpha)}{g(\alpha)} = f(\alpha)u(\alpha)$, и мы избавились от знаменателя. Теперь уменьшим степень числителя. Пусть $r(x)$ — остаток от деления $f(x)u(x)$ на $h_\alpha(x)$. Тогда $f(\alpha)u(\alpha) = r(\alpha)$ и, значит, $\frac{f(\alpha)}{g(\alpha)} = r(\alpha)$, что показывает представимость элемента $\frac{f\alpha)}{g(\alpha)}$ в требуемом виде.

Остаётся показать, что элементы $1, \alpha, \ldots, \alpha^{n-1}$ поля F линейно независимы над K. Если

$$\gamma_0 + \gamma_1\alpha + \ldots + \gamma_{n-1}\alpha^{n-1} = 0$$

для некоторых $\gamma_0, \gamma_1, \ldots, \gamma_{n-1} \in K$, то для многочлена $w(x) = \gamma_0 + \gamma_1 x + \ldots + \gamma_{n-1}x^{n-1} \in K[x]$ получаем $w(\alpha) = 0$. Тогда из условия $\deg w(x) < \deg h_\alpha(x)$ вытекает, что $w(x) = 0$, то есть $\gamma_0 = \gamma_1 = \ldots = \gamma_{n-1} = 0$. □

32 Порядок конечного поля. Автоморфизм Фробениуса.

Будем использовать следующее обозначение: $K^\times = (K \setminus \{0\}, \times)$ — мультипликативная группа поля K.

Пусть K — конечное поле. Тогда его характеристика отлична от нуля и потому равна некоторому простому числу p. Значит, K содержит поле $\mathbb{Z}_p$ в качестве простого подполя.

Теорема 32.1. *K - конечное поле, $charK = p \Rightarrow |K| = p^n$ для некоторого $n \in \mathbb{N}$*

Доказательство. $charK = p \Rightarrow$ простое подполе в K есть $\mathbb{Z}_p$
$\Rightarrow K$ векторное пространство над $\mathbb{Z}_p$, оно конечномерно
пусть $n = dim_{\mathbb{Z}_p}K$ и $(e_1, ..., e_n)$ базис k.
Тогда $K = \{a_1e_1 + ... + a_ne_n | a_i \in \mathbb{Z}_p\}$.
Для каждого a_i есть ровно p возможностей $\Rightarrow |K| = p^n$. □

Пусть K — произвольное поле характеристики $p > 0$. Рассмотрим отображение

$$\varphi\colon K \to K, \quad a \mapsto a^p.$$

Покажем, что φ — гомоморфизм. Для любых $a,b \in K$ по формуле бинома Ньютона имеем

$$(a+b)^p = a^p + \binom{p}{1}a^{p-1}b + \binom{p}{2}a^{p-2}b^2 + \ldots + \binom{p}{p-1}ab^{p-1} + b^p.$$

Так как p — простое число, то все биномиальные коэффициенты $\binom{p}{i}$ при $1 \leqslant i \leqslant p-1$ делятся на p. Это значит, что в нашем поле характеристики p все эти коэффициенты обнуляются, в результате чего получаем $(a+b)^p = a^p + b^p$. Ясно, что $(ab)^p = a^pb^p$, так что φ — гомоморфизм.

$\varphi(1) = 1 \neq 0 \Rightarrow Ker\varphi \neq K$ Ядро любого гомоморфизма колец является идеалом, поэтому $\mathrm{Ker}\varphi$ — идеал в K. Но в поле нет собственных идеалов, поэтому $\mathrm{Ker}\varphi = \{0\}$, откуда φ инъективен.

Если поле K конечно, то инъективное отображение из K в K автоматически биективно. В этой ситуации φ называется *автоморфизмом Фробениуса* поля K.

Предложение 32.1. *Пусть K — произвольное поле и ψ — произвольный автоморфизм (т. е. изоморфизм на себя) поля K. Тогда множество неподвижных точек $K^\psi = \{a \in K \mid \psi(a) = a\}$ является подполем в K.*

Доказательство. Проверим выполнение всех свойств подполя по определению:

Так как ψ – изоморфизм полей (колец), то $\psi(a+b) = \psi(a) + \psi(b)$ и $\psi(ab) = \psi(a)\psi(b)$. Отсюда следует, что если элементы a и b являются неподвижными (a, $b \in K^\psi$), то $\psi(a) + \psi(b) = a + b \in K^\psi$ и $\psi(a)\psi(b) = ab \in K^\psi$, значит, множество K^ψ замкнуто по сложению и умножению.

При любом гомоморфизме 0 переходит в 0, а 1 в 1, отсюда 1 и 0 лежат в K^ψ. Осталось проверить, что для любого ненулевого $a \in K^\psi$ существует обратный в K^ψ. Заметим, что в исходном поле K для a существует обратный элемент a^{-1}. Тогда $\psi(a \cdot a^{-1}) = \psi(a)\psi(a^{-1}) = a\psi(a^{-1})$. С другой стороны, по определению обратного элемента $\psi(a \cdot a^{-1}) = \psi(1) = 1$, откуда $a\psi(a^{-1}) = 1$. Следовательно, $\psi(a^{-1}) = a^{-1}$ и $a^{-1} \in K^\psi$.

Таким образом, K^ψ – подполе в K. □

33 Теорема о существовании и единственности для конечных полей.

Прежде чем перейти к следующей теореме, обсудим понятие формальной производной многочлена. Пусть $K[x]$ — кольцо многочленов над произвольным полем K. Формальной производной называется отображение $K[x] \to K[x]$, которое каждому многочлену $f(x) = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$ сопоставляет многочлен $f'(x) = na_n x^{n-1} + (n-1)a_{n-1}x^{n-2} + \ldots + a_1$. Из определения следует, что это отображение линейно. Легко проверить, что для любых $f,g \in K[x]$ справедливо привычное нам равенство $(fg)' = f'g + fg'$ (в силу дистрибутивности умножения проверка этого равенства сводится к случаю, когда f,g — одночлены).

Теорема 33.1. *Для всякого простого числа p и натурального числа n существует единственное (с точностью до изоморфизма) поле из p^n элементов.*

Доказательство. Положим $q = p^n$ для краткости.

Единственность. Пусть поле K содержит $p^n = q$ элементов. Тогда мультипликативная группа $K^\times$ имеет порядок $q-1$. По следствию 3 из теоремы Лагранжа ($|G| < \infty \Rightarrow g^{|G|} = e\ \forall\ g \in G$) мы имеем $a^{q-1} = 1$ для всех $a \in K^\times = K \setminus \{0\}$, откуда $a^q - a = 0$ для всех $a \in K$. Это значит, что все элементы поля K являются корнями многочлена $x^q - x \in \mathbb{Z}_p[x]$. Отсюда следует, что K является полем разложения многочлена $x^q - x$ над $\mathbb{Z}_p$. Из теоремы о полях разложения, следует, что поле K единственно с точностью до изоморфизма.

Существование. Пусть K — поле разложения многочлена $f(x) = x^q - x \in \mathbb{Z}_p[x]$. Тогда имеем $f'(x) = qx^{q-1} - 1 = -1$ (qx^{q-1} обнуляется, так как q делится на p, а p — характеристика поля $\mathbb{Z}_p$).

Покажем, что многочлен $f(x)$ не имеет кратных корней в K. Действительно, если α — корень кратности $m \geqslant 2$, то $f(x) = (x-\alpha)^m g(x)$ для некоторого многочлена $g(x) \in \mathbb{Z}_p[x]$. Но тогда $f'(x) = m(x-\alpha)^{m-1}g(x) + (x-\alpha)^m g'(x)$, откуда видно, что $f'(x)$ делится на $(x-\alpha)$. Но последнее невозможно, ибо $f'(x) = -1$ — многочлен нулевой степени.

Обозначим $K_f \subset K$ множество всех корней в K многочлена f.

У f нет кратных корней в $K \Rightarrow |K_f| = q$.

$a \in K_f \Leftrightarrow a^q = a \Leftrightarrow a^{p^n} = a \Leftrightarrow (((a^p)^p)...)^p = a \Leftrightarrow \varphi^n(a) = a$,

где φ автоморфизм Фробениуса, $\psi = \varphi^n$ тоже автоморфизм

$\Rightarrow K_f = K^\psi \Rightarrow K_f$ поле, оно содержит все корни f

$\Rightarrow K_f = K$ (т.к. K – поле разложения) □

Пример 13. Построим явно поле из четырёх элементов. Многочлен x^2+x+1 неприводим над $\mathbb{Z}_2$. Значит, факторкольцо $\mathbb{Z}_2[x]/(x^2+x+1)$ является полем и его элементы — это классы $\overline{0}, \overline{1}, \overline{x}, \overline{x+1}$ (запись $\overline{a}$ означает класс элемента a в факторкольце $\mathbb{Z}_2[x]/(x^2+x+1)$). Например, произведение $\overline{x} \cdot \overline{x+1}$ — это класс элемента x^2+x, который равен $\overline{1}$.

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

Предложение 34.1. *K - конечное поле $\Rightarrow$ группа $K^\times$ является циклической*

Доказательство. Пусть $q = |K|$. Пусть $m = exp(K^\times)$. Тогда $a^m = 1$, $\forall a \in K^\times$.

Но тогда все элементы из $K^\times$ являются корнями многочлена $x^m - 1$.

Если $m < q - 1 = |K^\times|$, то этот многочлен имеет $q - 1 > m$ корней (что больше, чем его степень). Противоречие.

Тогда $m = q - 1 \Rightarrow exp(K^\times) = |K^\times| \Rightarrow K^\times$ является циклической. □

Теорема 34.1. *Конечное поле F_q, где $q = p^n$, можно реализовать в виде $\mathbb{Z}_p[x]/(h(x))$, где $h(x)$ неприводимый многочлен степени n над $\mathbb{Z}_p$. В частности, для всякого $n \in \mathbb{N}$ в кольце $\mathbb{Z}_p[x]$ есть неприводимый многочлен степени n.*

Доказательство. Пусть α – порождающий элемент группы $F_q^\times$. Тогда минимальное подполе $\mathbb{Z}_p(\alpha)$ поля F_q, содержащее α, совпадает с F_q (так как содержит $K^\times$ и 0).

Значит поле F_q изоморфно полю $\mathbb{Z}_p[x]/(h(x))$, где $h(x)$ минимальный многочлен элемента α над $\mathbb{Z}_p$. Пусть d – степень h. Тогда $\mathbb{Z}_p[x]/(h)$ содержит p^d элементов, то $n = d$. □

35 Подполя конечного поля.

Теорема 35.1. *Пусть $q = p^n$, p - простое.*

1) $F \subseteq \mathbb{F}_q$ - подполе $\Rightarrow F \simeq \mathbb{F}_{p^m}$, где $m \mid n$.

2) $m \mid n \Rightarrow$ в $\mathbb{F}_q$ $\exists!$ подполе F, такое что $|F| = p^m$.

Доказательство. 1) $F \subseteq \mathbb{F}_q$ - подполе. Положим $s = [\mathbb{F}_q : F]$. Так как поле конечное, то $|F| = p^m$ для некоторого m. Тогда $p^n = (p^m)^s = p^{ms} \Rightarrow m \mid n$.

2) Пусть $m \mid n$, $n = m \cdot s$.

Рассмотрим многочлены:

$$f(x) = x^{p^n} - x = x(x^{p^n-1} - 1) \in \mathbb{Z}_p[x],$$
$$g(x) = x^{p^m} - x = x(x^{p^m-1} - 1) \in \mathbb{Z}_p[x]$$

Заметим, что $p^n - 1 = p^{ms} - 1 \,\vdots\, p^m - 1 \Rightarrow x^{p^n} - 1 \,\vdots\, x^{p^m} - 1 \Rightarrow f(x) \;\vee\; g(x)$

$f(x)$ над $\mathbb{F}_{p^n}$ разлагается на линейные множители (без кратностых корней), значит, $g(x)$ как его делитель также разлагается на линейные множители без корней. Тогда g в $\mathbb{F}_{p^n}$ имеет ровно p^m корней.

Тогда $g(a) = 0 \iff a^{p^m} = a \iff \varphi^m(a) = a$, где φ – автоморфизм Фробениуса. Тогда корни g образуют подполе в $\mathbb{F}_{p^m}$

Отсюда сразу единственность, так как все элементы $\mathbb{F}_{p^m}$ должны быть корнями многочлена $g(x)$. $\square$

36 Коды над конечным алфавитом. Расстояние Хэмминга. Минимальное расстояние кода. Коды, исправляющие t ошибок: определение, эквивалентные формулировки. Код с повторением.

Σ – конечный алфавит, $|\Sigma| = q$ (крайне важен случай, когда $\Sigma = \{0,1\}$.

Информация разбита на блоки длины k. Мы хотим её передавать по каналу связи с шумом.

Основная идея – передавать информацию с избытком.

$$\underbrace{a}_{\Sigma^k} \xrightarrow{f,\ k<n} \underbrace{c}_{\Sigma^n} \xrightarrow{errors} \underbrace{c'}_{\Sigma^n} \xrightarrow{g} \underbrace{a}_{\Sigma^k}$$

Ошибками в нашем случае является искажение символов, то есть замена буквы на другую произвольную.

Пример 14. Пусть в канале связи может быть не больше 1 ошибки. Тогда $w \to www$ – отличный способ кодирования для исправления этой ошибки.

Определение 36.1. *Расстояние Хэмминга* между словами a и b – это количество отличающихся символов между a и b:

$$\rho(a,b) := |\{i \mid a_i \neq b_i\}|$$

Пример 15. a – исходное сообщение, b – полученное сообщение $\Rightarrow \rho(a,b)$. Тогда $\rho(a,b)$ это в точности количество ошибок при передаче сообещния.

Замечание 25. ρ является метрикой в Σ^n.

Определение 36.2. Кодом длины n (над Σ) называется всякое подмножество $C \subseteq \Sigma^n$.

Определение 36.3. Говорят, что код $C \subseteq \Sigma^n$ исправляет t ошибок, если $\forall x \in \Sigma^n$ $\exists$ не более одного $c \in C$, такого что $\rho(x,c) \leqslant t$.

Задача 36.1. Строить такие коды, у которых слова находились бы на большем расстоянии друг от друга.

Определение 36.4. Число $d_{:=\min_{x \neq y \in} \rho(x,y)}$ называется минимальным расстоянием кода .

Определение 36.5. Шаром радиуса t с центром в точке x называется множество

$$B_t(x) := \{y \in \Sigma^n \mid \rho(x,y) \leqslant t\}$$

Теорема 36.1. *Для кода $C \subseteq \Sigma^n$ следующие условия эквивалентны:*

1. *C исправляет t ошибок.*
2. $\forall x \neq y \in C : B_t(x) \cap B_t(y) = \varnothing$
3. $d_C \geqslant 2t + 1$

Доказательство.

(1) $\Leftrightarrow$ (2) C исправляет t ошибок $\iff \forall x \in \Sigma^n\ \exists_{\leqslant 1} y \in C:\ x \in B_t(y) \iff B_t(x) \cap B_t(y) = \varnothing\ \forall x \neq y \in C$.

Можно представить геометрически: точка лежит не более чем в одном шаре размера t с центром в кодовом слове тогда и только тогда, когда эти шары не пересекаются – в противного случае точка пересечения будет покрыта хотя бы двумя кодовыми словами и мы не сможем определить, как его расшировать.

(2) $\Rightarrow$ (3) От противного: пусть $\exists a \neq b \in C : \rho(a,b) \leqslant 2t$.

Без ограничения общности можно считать, что $a_i = b_i$ при $i > 2t$, то есть мы перенумеровали координаты так, что они слова различаются только в первых $\leqslant 2t$ координатах.

Тогда рассмотрим следующий $x = (a_1, \ldots, a_t, b_{t+1}, \ldots, b_n)$.

$$\begin{cases} \rho(x,b) \leqslant t \\ \rho(x,a) \leqslant t \end{cases} \Rightarrow B_t(a) \cap B_t(b) \neq \varnothing$$

(3) $\Rightarrow$ (2) От противного: пусть $\exists a \neq b \in C$, такие что $B_t(a) \cap B_t(b) \neq \varnothing$.

Тогда $\exists x : \rho(a,x) \leqslant t,\ \rho(b,x) \leqslant t$.

Тогда по неравенству треугольника получаем, что $\rho(a,b) \leqslant 2t$ – противоречие.

$\square$

Пример 16. Код с повторениями.
$C = \{(a, \ldots, a) \mid a \in \Sigma\} \subseteq \Sigma^n$.
Можно понять, что $d_C = n \Rightarrow C$ исправляет $(n-1)/2$ ошибок.

37 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

Считаем, что Σ – конечное поле $\mathbb{F}_q$. Тогда Σ^n – векторное пространство над $\mathbb{F}_q$.
Идея: строить коды, являющиеся подпространствами в $\mathbb{F}_q^n$.

Определение 37.1. Код $C \subseteq (\mathbb{F}_q)^n$ называется линейным, если C является подпространством в $(\mathbb{F}_q)^n$.

$\dim C$ называется размерностью линейного кода.

$C \subseteq (\mathbb{F}_q)^n$ – линейный код, $\dim C = k$. Тогда C можно обозначит как (n, t), где первой координатой стоит длина, а второй – размерность.

Определение 37.2. Норма векттора $x \in \mathbb{F}_q^n$ – это число ненулевых координат:

$$||x|| := |\{i \mid x_i \neq 0\}|$$

Лемма 37.1. *$C \subseteq \mathbb{F}_q^n$ – линейный код* $\Rightarrow d_c = \min_{x \neq 0 \in C} ||x||$

Определение 37.3. $d_C = \min \rho(x,y) = \min ||x-y|| = \min ||x||$.

Все переходы за счет линейности.

Определение 37.4. $C \subseteq \mathbb{F}_q^n$ – линейный (n,k) код.

Матрица $H \subseteq Mat_{(n-k)\times n}(\mathbb{F}_q)$ называется проверочной матрицей кода C если $rk(H) = n-k$ и $\forall x = (x_1, \ldots, x_n) \in \mathbb{F}_q^n$ верно:

$$x \in C \iff H \cdot x^t = 0$$

Пример 17. C – код с повтрениями. Тогда

$$H = \begin{pmatrix} -1 & 1 & 0 & \cdots & 0 \\ -1 & 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & 0 & 0 & \cdots & 1 \end{pmatrix}$$

Это – линейный $(n,1)$ код.

Предложение 37.1. *C – линейный код с проверочной матрицей H.*

Тогда следующие условия эквивалентны:

1. $d_C \geqslant s+1$

2. *Любые s столбцов матрицы H линейно независимы.*

Доказательство. $d_C \leqslant s \iff \exists x \in C : ||x|| \leqslant s \iff$ в H есть s линейно зависимых столбцов. □

Пример 18. (бинарный код Хэмминга)

$q = 2$ фиксировано, $k \in \mathbb{N}$.

$H_k \in Mat_{k\times(2^k-1)}(\mathbb{F}_2)$.

Столбца H_k – это бинарная запись всех чисел от 1 до $2^k - 1$.

Пример: $k = 3$

$$H_3 = \begin{pmatrix} 0 & 0 & 0 & 1 & 1 & 1 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 1 & 0 & 1 & 0 & 1 \end{pmatrix}$$

Так как любые два стольца различны, а значит, линейно независимы ($\mathbb{F}_2$), то получаем, что $d_C = 3$. Первые 3 столбца линейно зависимы $\Rightarrow d_C = 3 \Rightarrow C$ исправляет 1 ошибку.

38 Коды БЧХ. Теорема о количестве ошибок, исправляемых кодом БЧХ. Оценка на размерность кода БЧХ

Отождествим $\mathbb{F}_q^n$ с кольцом $\mathbb{F}_q[x]/(x^m-1)$.

Тогда:

$$(c_0, c_1, \ldots, c_{n-1}) \mapsto c_0 + c_1 x + \ldots c_{n-1}x^{n-1}$$

Зафиксируем параметры n,q,m так, чтобы $n = q^m$.

Мы знаем, что группа $\mathbb{F}_{q^m}$ – циклическая, пусть α – её порождающий.

Зафиксируем t – количество ошибок, которые мы хотим исправлять. Теперь $\forall i \in \{1, \ldots, 2t\}$ положим $h_i(x) \in \mathbb{F}_q[x]$ – минимальный многочлен для α^i. Будем считать, что $2t < n$, так как в ином случае у нас бы некоторые α повторились бы.

Важно: $x^n - 1 \,\vdots\, h_i(x)$ (малая теорема Ферма).

Теперь положим $g(x) = \text{НОК}(h_1(x), \ldots, h_{2t}(x))$. Понятно, что $x^n - 1 \,\vdots\, g(x)$.

Определим БЧХ код так:

$$C = \{f \in \mathbb{F}_q[x]/(x^n-1) \mid f \,\vdots\, g\}$$

Теорема 38.1. *БЧХ код исправляет t ошибок.*

Доказательство. $f \in C \iff f \,\vdots\, g \iff \forall i \in \{1, \ldots, 2t\} : f(\alpha^i) = 0$.

В общем виде f записывается так:

$$f = c_0 + c_1 x + \ldots + c_{n-1}x^{n-1}$$

Тогда $f \in C \iff H \cdot c = 0$, где

$$H = \begin{pmatrix} 1 & \alpha & \alpha^2 & \alpha^3 & \cdots & \alpha^{n-1} \\ 1 & \alpha^2 & \alpha^4 & \cdots & \cdots & \alpha^{2n-2} \\ 1 & \alpha^3 & \cdots & \cdots & \cdots & \alpha^{3n-3} \\ \vdots & \vdots & \ddots & \ddots & \ddots & \vdots \\ 1 & \alpha^{2t} & \cdots & \cdots & \cdots & \alpha^{2t(n-1)} \end{pmatrix}$$

Достаточно показать, что любые $2t$ столбцов линейно независимы. Возьмем столбца $i_1, \ldots, i_{2t}$. Посчитаем определитель получившейся матрицы:

$$\begin{vmatrix} \alpha^{i_1} & \cdots & \alpha^{i_{2t}} \\ \alpha^{2i_1} & \cdots & \alpha^{2i_{2t}} \\ \vdots & \ddots & \vdots \\ \alpha^{2t(i_1)} & \cdots & \alpha^{2t(i_{2t})} \end{vmatrix} = \alpha^{i_1} \cdot \ldots \cdot \alpha^{i_{2t}} \cdot \begin{vmatrix} 1 & \cdots & 1 \\ \alpha^{i_1} & \cdot & \alpha^{i_{2t}} \\ \vdots & \ddots & \vdots \\ \alpha^{(2t-1)(i_1)} & \cdots & \alpha^{(2t-1)(i_{2t})} \end{vmatrix}$$

Это ничто иное, как определитель Вандермонда. Его мы знаем. Получаем:

$$\alpha^{i_1} \cdot \ldots \cdot \alpha^{i_{2t}} \cdot \prod_{k,l \in [1,2t]} (\alpha^{i_l} - \alpha^{i_k}) \neq 0$$

Последний переход верен так как $2t < n$, а так как α – порождающий мультипликативной группы поля, то все степени, $< n$, попарно различны.

Таким образом, действительно любые $2t$ столбцом линейно независимы. Больше быть не может, так как всего в матрице $2t$ строк. Итого получаем, что $d_c = 2t + 1$. $\square$

Предложение 38.1. *C – код БЧХ. Тогда* $\dim C \geqslant n - 2tm = n - 2t\log_q(n+1)$.

Доказательство. Из определения проверочной матрицы можно понять, что $\dim C = n - \deg g$. Имеем: $[\mathbb{F}_{q^m} : \mathbb{F}_q] = m$. Тогда $\forall i \in \{1, \ldots, 2t\} : [\mathbb{F}_{q^m} : \mathbb{F}_q] \leqslant m \Rightarrow \deg h_i \leqslant m \Rightarrow \deg h \leqslant 2tm$. $\square$