Алгебра. Экзамен

Бобень Вячеслав
@darkkeks, GitHub
За билеты начиная с 17-го спасибо Даниэлю Хайбулину и Анастасии Григорьевой
@kiDaniel, @weifoll

2020

> “Какой-то ты слишком идеальный, редуцируем его!”.
>
> — Bottom text

Содержание

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

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*, то есть

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

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 $a \circ b := a - b$.

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

Определение 1.3. Полугруппа $(S, \circ)$ называется *моноидом*, если в ней есть *нейтральный элемент*, то есть такое элемент $e \in S$, что $e \circ a = a \circ e = a$ для любого $a \in S$.

Замечание. 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*, то есть 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 $\circ$ обозначения операции опускают и пишут просто ab.

Определение 1.5. Группа G называется *коммутативной* или *абелевой*, если групповая операция *коммутативна*, то есть $ab = ba$ 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, то есть $a + b, 0, -a$.

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 $|G|$.

Приведем 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:
   $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n\times n}(\mathbb{R}) \mid \det A \neq 0\}$ — полная линейная группа;
   $\mathrm{SL}_n(\mathbb{R}) = \{A \in \mathrm{Mat}_{n\times n}(\mathbb{R}) \mid \det A = 1\}$ — специальная линейная группа.
4. Группы перестановок (с операцией композиции):
   симметрическая группа S_n — все перестановки длины n, $|S_n| = n!$;
   знакопеременная группа A_n — чётные подстановки длины n, $|A_n| = \dfrac{n!}{2}$.
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 $\mathbb{Z}$.

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

Иначе положим $k = \min(H \cap \mathbb{N}) \neq 0$. (это множество непусто, так как $\forall x \implies -x \in H$)

Тогда $k\mathbb{Z} \subseteq H$.

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

$a = qk + r$, где $k \in H$, $0 \leqslant r < k \implies r = a - qk \in H$.

В силу выбора k получаем $r = 0 \implies a = qk \in k\mathbb{Z}$. ■

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

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

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

Свойства:

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

Определение 2.1. Пусть G — группа и $g \in G$. *Циклической подгруппой*, порожденной 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 найдется 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 $\mathrm{ord}(g)$. Заметим, что $\mathrm{ord}(g) = 1$ тогда и только тогда, когда $g = e$.

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

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, $\langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\}$ и $|\langle g \rangle| = m$. ■

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

3 Смежные классы. Индекс подгруппы. Теорема Лагранжа

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

Предложение 3.1. L_H — отношение эквивалентности.

Доказательство.
1. $a^{-1}a = e \in H$;
2. $a^{-1}b \in H \implies b^{-1}a = (a^{-1}b)^{-1} \in H$;
3. $a^{-1}b \in H, b^{-1}c \in H \implies a^{-1}c = (a^{-1}b)(b^{-1}c) \in H$.

■

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

Определение 3.1. *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:

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

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

Лемма 3.1. 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 (предложение 3.1) и каждый из них содержит по $|H|$ элементов (лемма 3.1). ■

4 Пять следствий из теоремы Лагранжа

Теорема 4.1 (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. Вытекает из следствия 1 и факта, что $\operatorname{ord}(g) = | \langle g \rangle |$. ∎

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

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

Следствие 4.4 (малая теорема Ферма)**.** Пусть $\overline{a}$ — ненулевой вычет по простому модулю p. Тогда $\overline{a}^{p-1} = 1$.

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

Следствие 4.5. Пусть G — группа. Предположим, что $|G|$ — простое число. Тогда G — циклическая группа, порождаемая любым своим неединичным элементов.

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 $g \in G$.

Пример.

1. G — абелева. Тогда любая подгруппа H нормальная.
2. $G = S_3$, $H = \{\mathrm{Id}, (12)\}$. Тогда H не является нормальной.
3. Несобственные подгруппы $H = G$ и $H = \{0\}$ нормальны.

Предложение 5.1. Для подгруппы $H \subseteq G$ следующие условия эквивалентны:

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

Доказательство.

(1) $\implies$ (2) $gH = Hg \implies gHg^{-1} = H$.

(2) $\implies$ (3) Очев.

(3) $\implies$ (1) $gHg^{-1} \subseteq H \implies gH \subseteq Hg$. Теперь возьмем $g = g^{-1}$. Тогда $g^{-1}Hg \subseteq H \implies Hg \subseteq gH \implies gH = Hg$. ∎

Рассмотрим множество 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 $h_1, h_2 \in H$.

$$(g_1'H)(g_2'H) = (g_1'g_2')H = (g_1h_1g_2h_2)H = (g_1g_2\underbrace{g_2^{-1}h_1g_2}_{\in H})h_2H \subseteq (g_1g_2)H \implies (g_1'g_2')H = (g_1g_2)H.$$

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

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

Определение 6.1. Пусть $(G, \circ)$ и $(F, \cdot)$ — две группы.

Отображение $\varphi\colon G \to F$ называется *гомоморфизмом*, если

$$\varphi(g_1 \circ g_2) = \varphi(g_1) \cdot \varphi(g_2), \quad \forall g_1, g_2 \in G.$$

Замечание. Пусть $\varphi\colon G \to F$ — гомоморфизм групп, и пусть e_G и e_F — нейтральные элементы группы G и F соответственно. Тогда:
1. $\varphi(e_G) = e_F$.
2. $\varphi(a^{-1}) = \varphi(a)^{-1}$ для любого $a \in G$.

Доказательство.

1. Имеем $\varphi(e_G) = \varphi(e_G e_G) = \varphi(e_G)\varphi(e_G)$.

   Теперь умножая крайние части этого равенства на $\varphi(e_G)^{-1}$, получим $e_F = \varphi(e_G)$.

2. $\varphi(g \cdot g^{-1}) = e_F = \varphi(g)\varphi(g^{-1})$. Умножив обе части на $\varphi(g)^{-1}$ получаем необходимое. ■

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

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

Обозначение: $G \simeq F$.

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

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

$$\ker \varphi = \{g \in G \mid \varphi(g) = e_f\},$$

и *образ*

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

Ясно, что $\ker \varphi \subseteq G$ и $\operatorname{Im} \varphi \subseteq F$ — подгруппы.

Лемма 6.1. Гомоморфизм групп $\varphi\colon G \to F$ инъективен тогда и только тогда, когда $\ker \varphi = \{e_G\}$.

Доказательство. Ясно, что если φ инъективен то $\ker \varphi = \{e_G\}$.

Обратно, пусть $g_1, g_2 \in G$ и $\varphi(g_1) = \varphi(g_2)$. Тогда $g_1^{-1} g_2 \in \ker \varphi$, 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 $\ker \varphi = \{e_G\}$ и $\operatorname{Im} \varphi = F$.

Предложение 6.1. Пусть $\varphi\colon G \to F$ — гомоморфизм групп. Тогда подгруппа $\ker \varphi$ нормальна в G.

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

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

7 Теорема о гомоморфизме для групп

Теорема 7.1 (Теорема о гомоморфизме)**.** *Пусть* $\varphi\colon G \to F$ *— гомоморфизм групп. Тогда группа* $\operatorname{Im}\varphi$ *изоморфна факторгруппе* $G/\ker\varphi$.

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

1. Корректность.

   $g_1\ker\varphi = g_2\ker\varphi \implies g_1h_1 = g_2h_2$ для некоторых $h_1, h_2 \in \ker\varphi$.

   $\psi(g_1\ker\varphi) = \varphi(g_1) = \varphi(g_1h_1) = \varphi(g_2h_2) = \varphi(g_2) = \psi(g_2\ker\varphi)$.

2. ψ — гомоморфизм.

   $\psi\left((g_1\ker\varphi)(g_2\ker\varphi)\right) = \psi((g_1g_2)\ker\varphi) = \varphi(g_1g_2) = \varphi(g_1)\varphi(g_2) = \psi(g_1\ker\varphi)\psi(g_2\ker\varphi)$.

3. Сюръектинвость из построения.

4. Инъективность.

   $\psi(g_1\ker\varphi) = \psi(g_2\ker\varphi) \implies \varphi(g_1) = \varphi(g_2) \implies \varphi(g_1)\varphi(g_2)^{-1} = e_F \implies \varphi(g_1g_2^{-1}) = e_F \implies g_1g_2^{-1} \in \ker\varphi \implies$ $g_1\ker\varphi = g_2\ker\varphi$. ∎

Тем самым, чтобы удобно реализовать факторгруппу G/H, можно найти такой гомоморфизм $\varphi\colon G \to F$ в некоторую группу F, что $H = \ker\varphi$, и тогда $G/H \simeq \operatorname{Im}\varphi$.

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

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

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

8 Классификация циклических групп

Пусть G — циклическая группа. Тогда

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

Доказательство. Пусть $G = \langle g \rangle$. Рассмотрим отображение $\varphi\colon \mathbb{Z} \to G$, $k \mapsto g^k$.

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 сюръективет, то есть $\operatorname{Im}\varphi = G$. Тогда по теореме о гомоморфизме мы получаем $G \simeq \mathbb{Z}/\ker\varphi$. Так как $\ker\varphi$ — подгруппа в $\mathbb{Z}$, то получаем $\ker\varphi = m\mathbb{Z}$ для некоторого $m \geqslant 0$. (так как любая подгруппа $\mathbb{Z}$ имеет вид $k\mathbb{Z}$) Если $m = 0$, то $\ker\varphi = \{0\}$, откуда $G \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$. Если $m > 0$, то $G \simeq \mathbb{Z}/m\mathbb{Z} = \mathbb{Z}_m$. ■

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

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

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

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

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

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

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

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

Доказательство. Рассмотрим отображение

$$\varphi \colon \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l, \quad \varphi(a \bmod n) = (a \bmod m, a \bmod l).$$

1. Корректность следует из того, что $n \vdots m$, $n \vdots l$;
2. φ — гомоморфизм:
$$\varphi((a+b) \bmod n) = \varphi(a \bmod n) + \varphi(b \bmod n).$$
3. φ инъективен:
   Если $\varphi(a \bmod n) = (0, 0)$, то a делится на m и на l. Но так как НОД$(m, l) = 1$, получаем что a кратно n.
   А значит $a \equiv 0 \pmod n$. То есть $\ker \varphi = \{0\}$.
4. φ сюръективно, так как $|\mathbb{Z}_n| = n = m \cdot l = |\mathbb{Z}_m \times \mathbb{Z}_l|$. ■

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

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

Определение 9.3. Конечная абелева группа A называется *примарной*, если $|A| = p^k$, где p — простое и $k \in \mathbb{N}$.

Теорема 9.2. *Пусть A — конечная абелева группа. Тогда $A \simeq \mathbb{Z}_{p_1^{k_1}} \times \cdots \times \mathbb{Z}_{p_t^{k_t}}$, где $p_1, \ldots, p_t$ — простые числа (не обязательно 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 (в частности, число этих множителей определено однозначно).*

10 Экспонента конечной абелевой группы и критерий цикличности

Определение 10.1. *Экспонентой* конечной абелевой группы A называется число

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

Замечание.

1. Так как $ma = 0 \iff m \,\vdots\, \mathrm{ord}(a) \ \forall a \in A$ и $m \in \mathbb{Z}$, то определение экспоненты можно переписать ещё в виде $\exp A = \text{НОК}\{\mathrm{ord}(a) \mid a \in A\}$.

2. Так как $|A| \,\vdots\, \mathrm{ord}(a) \ \forall a \in A$, то $|A|$ — общее кратное множества $\{\mathrm{ord}(a) \mid a \in A\}$, а значит, $|A| \,\vdots\, \exp A$.

   В частности, $\exp A \leqslant |A|$.

Предложение 10.1. $\exp A = |A| \iff A$ — циклическая группа.

Доказательство. Пусть $|A| = n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ — разложение на простые множители, где p_i — простое и $k_s \in \mathbb{N}$. ($p_i \neq p_j$ при $i \neq j$)

$\Longleftarrow$ Если $A = \langle a \rangle$, то $\mathrm{ord}\, a = n$, откуда сразу получаем $\exp A = n$.

$\Longrightarrow$ Если $\exp A = n$, то для $i = 1, \ldots, s$ существует элемент $c_i \in A$, такой что $\mathrm{ord}\, c_i = p_i^{k_i} m_i$, где $m_i \in \mathbb{N}$. Для каждого $i = 1, \ldots, s$ положим $a_i = m_i c_i$, тогда $\mathrm{ord}(a_i) = p_i^{k_i}$. Теперь рассмотрим элемент $a = a_1 + \cdots + a_s$ и покажем, что $\mathrm{ord}(a) = n$. Пусть $ma = 0$ для некоторого $m \in \mathbb{N}$, то есть $ma_1 + \cdots + ma_s = 0$. 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 $mn_i a_i = 0$. 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 $\mathrm{ord}(a) = n$. Значит, $A = \langle a \rangle$ — циклическая группа. ∎

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

Пусть G — конечная абелева группа (например, $G = (\mathbb{Z}_p \setminus \{0\}, \times)$, где p — большое простое число) и $g \in G$ — элемент достаточно большого порядка.

Задача 11.1. Задача дискретного логарифмирования.

Дано $g \in G$, $\operatorname{ord}(g) \gg 0$, $h \in \langle g \rangle$. Найти такое $k \in \mathbb{N}$, что $g^k = h$.

При этом задача возведения в степень имеет быстрый алгоритм — повторное возведение в квадрат.

$$g^{16} = \left(\left(\left(g^2\right)^2\right)^2\right)^2 \quad g^{15} = \left(\left(g^2 \cdot g\right)^2 \cdot g\right)^2 \cdot g.$$

Сама же задача нахождения степени решается только переборными и близкими к перебору способами.

Задача 11.2. Система Диффи-Хеллмана обмена ключами (1976).

G и g известны всем.

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

Боб совершает аналогичные действия — $\beta \in \mathbb{N}, g^\beta$.

Теперь Алиса и Боб возводят элемент другого в свою секретную степень, оба получают $(g^\alpha)^\beta = \left(g^\beta\right)^\alpha = g^{\alpha\beta}$.

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 11.3. Криптосистема Эль-Гамаля.

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

Боб хочет передать Алисе элемент $h \in G$.

Для этого Боб фиксирует какое-то $\beta \in \mathbb{N}$ и объявляет пару $\{g^\beta, h \cdot (g^\alpha)^\beta\}$.

Отсюда $h = \left(h \cdot (g^\alpha)^\beta\right) \cdot ((g^\beta)^\alpha)^{-1} = (h \cdot (g^\alpha)^\beta) \cdot (g^\beta)^{|G|-\alpha}$, то есть зная α можно легко получить h.

Следовательно, получить его может только Алиса, а всем остальным придется решать задачу дискретного логарифмирования.

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

Определение 12.1. *Кольцо* — это множество R, на котором заданы две бинарные операции «$+$» (сложение) и «$\cdot$» (умножение), удовлетворяющее следующим условиям:

1. $(R, +)$ — абелева группа;
2. $\forall a, b, c, \in R \quad a(b + c) = ab + ac$ и $(a + b)c = ac + bc$;
3. $\forall a, b, c, \in R \quad (ab)c = a(bc)$.
4. $\exists 1 \in R$, такой что $1 \cdot a = a \cdot 1 = a \quad \forall a \in R$.

Замечание.

1. $0 \cdot a = a \cdot 0 = 0 \quad \forall a \in R$;
2. Если $|R| > 1$, то $1 \neq 0$.

Доказательство.

1. $a0 = a(0 + 0) = a0 + a0$, откуда $0 = a0$.
2. Следует из условий выше.

∎

Пример.

1. числовые кольца $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$;
2. кольцо $\mathbb{Z}_n$ вычетов по модулю n;
3. кольцо матриц $\mathrm{Mat}_{n\times n}(\mathbb{R})$;
4. $\mathbb{R}[x]$ — кольцо многочленов от переменной x с коэффициентами из $\mathbb{R}$;
5. $\mathbb{R}[x_1, \ldots, x_n]$ — кольцо многочленов от нескольких переменных $x_1, \ldots, x_n$ с коэффициентами из $\mathbb{R}$;
6. $F(M, \mathbb{R})$ — кольцо функций из множества M в $\mathbb{R}$ (с поточечными операциями сложения и умножения): $(f_1 + f_2)(m) := f_1(m) + f_2(m), \quad (f_1 \cdot f_2)(m) := f_1(m) \cdot f_2(m)$.

Определение 12.2. Кольцо R называется *коммутативным*, если $ab = ba$ для всех $a, b \in R$.

Определение 12.3. Элемент $a \in R$ называется *обратимым*, если найдется такой $b \in R$, что $ab = ba = 1$.

Замечание. Все обратимые элементы кольца R образуют группу по умножению.

Определение 12.4. Элемент $a \in R$ называется *левым* (соответственно *правым*) *делителем нуля*, если $a \neq 0$ и $\exists b \in R$, $b \neq 0$, такой что $ab = 0$ (соответственно $ba = 0$).

Замечание. Если R коммутативно, то множества левых и правых делителей нуля совпадают. Тогда левые и правые делители нуля называются просто «делителями нуля».

Замечание. 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 $b = 0$ — противоречние.

Определение 12.5. Элемент $a \in R$ называется *нильпотентным* (*нильпотентом*), если $a \neq 0$ и найдется такое $n \in \mathbb{N}$, что $a^n = 0$.

Замечание. Всякий нильпотент является делителем нуля: если $a \neq 0$ и n минимально, то $a \cdot a^{n-1} = 0$.

Определение 12.6. Кольцо R называется *полем*, если оно коммутативно (ассоциативно с 1), $0 \neq 1$ и любой ненулевой элемент обратим.

Пример. $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_2$.

Предложение 12.1. Кольцо вычетов $\mathbb{Z}_n$ является полем $\iff$ n — простое число.

Доказательство. Соглашение: $a \in \mathbb{Z} \rightsquigarrow \overline{a} \in \mathbb{Z}_n$ — вычет $a \bmod n$.

$\Longrightarrow$ Если $n = 1$, то $\mathbb{Z}_n = \{0\}$ — не поле.

Если $n > 1$ и $n = m \cdot k$, где $1 < m, k < n$, то $\overline{m} \cdot \overline{k} = \overline{0} \implies$ в $\mathbb{Z}_n$ есть делитель нуля $\implies \mathbb{Z}_n$ — не поле.

$\Longleftarrow$ $n = p$ — простое. Пусть $\overline{a} \in \mathbb{Z}_p \setminus \{\overline{0}\}$.

Тогда НОД$(a, p) = 1 \implies \exists k, l \in \mathbb{Z}$, такие что $ak + pl = 1$.

Значит, $\overline{a} \cdot \overline{k} + \overline{p} \cdot \overline{l} = \overline{1} \implies \overline{a} \cdot \overline{k} = \overline{1} \implies \overline{a}$ обратим. ∎

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

Определение 13.1. Подмножество $I \subseteq R$ называется *(двусторонним) идеалом*, если

1. I — подгруппа по сложению;
2. $\forall a \in I \; \forall r \in R \quad ar \in I, ra \in I$.

Обозначение $I \lhd R$.

Пример. Несобственные идеалы $\{0\}, R$. Остальные называются *собственными.*

Определение 13.2. Множество $(a) := \{ra \mid r \in R\}$ называется *главным идеалом*, порождаемым элементом a.

Пример. $(k) = k\mathbb{Z}$ — главный идеал в $\mathbb{Z}$.

Замечание.
$(a) = R \iff a$ обратим,
$(a) = \{0\} \iff a = 0$.

Определение 13.3. Если $S \subseteq R$ — подмножество, то

$$(S) := \{r_1 s_1 + \dots + r_k s_k \mid r_i \in R, s_i \in S\}$$

называется *идеалом, порожденным подмножеством* S.

Рассмотрим факторгруппу $(R/I, +)$ и введём на ней операцию умножения, полагая $(a+I)\cdot(b+I) := ab + I$.

Корректность $a + I = a' + I$, $b + I = b' + I \implies a' = a + x$, $b' = b + y$, где $x, y \in I$. Тогда,

$$(a'+I)(b'+I) = a'b' + I = (a+x)(b+y) + I = ab + \underbrace{ay + xb + xy}_{\in I} + I = ab + I.$$

Замечание. R/I — кольцо.

Определение 13.4. R/I называется *факторкольцом* кольца R по идеалу I.

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

Определение 13.5. Если R, S — два кольца, то отображение $\varphi\colon R \to S$ называется *гомоморфизмом* колец, если $\varphi(a+b) = \varphi(a) + \varphi(b)$ и $\varphi(ab) = \varphi(a)\cdot\varphi(b)$.

Изоморфизм — биективный гомоморфизм.

Пусть $\varphi\colon R \to R'$ — гомоморфизм колец.
Тогда $\ker\varphi := \{r \in R \mid \varphi(r) = 0\} \subseteq R$
$\operatorname{Im}\varphi := \varphi(R) \subseteq R'$

Замечание.
1. $\ker\varphi \lhd R$;
2. $\operatorname{Im}\varphi$ — подкольцо в R'.

Доказательство.

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

   Имеем $\varphi(ra) = \varphi(r)\varphi(a) = \varphi(r)0 = 0$, откуда $ra \in \ker\varphi$. Аналогично для $ar \in \ker\varphi$. ∎

Теорема 13.1 (Теорема о гомоморфизме колец)**.** $R/\ker\varphi \simeq \operatorname{Im}\varphi$.

Доказательство. Пусть $I := \ker\varphi$. Тогда из доказательства теоремы о гомоморфизме для групп отображение $\psi\colon R/I \to \operatorname{Im}\varphi$, $\psi(a+I) := \varphi(a)$ является изоморфизмом групп (по сложениею).

Остается проверить, что ψ — гомоморфизм колец.

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

Пример. K — поле, $a \in K$, $\quad \varphi\colon K[x] \to K, \quad f \mapsto f(a)$.
Это гомоморфизм, он сюръективен ($b = \varphi(b)$).
$\ker\varphi = (x-a) \implies K[x]/(x-a) \simeq K$.

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

Пусть K — поле, $K[x]$ — кольцо многочленов от x с коэффициентами из K.

$$K[x] = \{a_n x^n + \dots + a_1 x + a_0 \mid n \geqslant 0, a_i \in K\}.$$

Тогда $\forall f \in K[x] \setminus \{0\}$ определена степень $\deg f$.
Удобно полагать, что $\deg 0 = -\infty$.
Тогда $\deg(fg) = \deg f + \deg g$,

$\deg(f+g) \leqslant \max(\deg f, \deg g)$

Обратимые элементы в $K[x] : \{f \mid \deg f = 0\} \not\ni 0$.
Делителей нуля нет.

Теорема 14.1 (деление с остатком). $\forall f \in K[x]\ \forall g \in K[x] \setminus \{0\}\quad \exists! q, r \in K[x]$, *такие что* $f = q \cdot g + r$ *и либо* $r = 0$, *либо* $\deg r < \deg g$.

Доказательство.

Существование Индукция по $\deg f$.

Если $f = 0$, то можно взять $q = r = 0$. Далее считаем $\deg f = n \geqslant 0$.

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

Если $\deg f < \deg g$, то достаточно взять $q = 0$ и $r = f$.

Иначе положим $h = f - \frac{a_n}{b_m} x^{n-m} g$, тогда $\deg h < \deg f$.

По предположению индукции $h = q \cdot g + r$, где либо $r = 0$, либо $\deg r < \deg g$. Тогда $f = \left(q + \frac{a_n}{b_m} x^{n-m}\right) g + r$ — искомое представление.

Единственность Пусть $f = q_1 g + r_1 = q_2 g + r_2$ — два представления.

Тогда $(q_1 - q_2) g = r_2 - r_1$. Если $q_1 - q_2 \neq 0$, то $\deg(q_1 - q_2) g \geqslant \deg g > \deg(r_2 - r_1)$ — противоречие. Значит, $q_1 = q_2$ и тогда $r_1 = r_2$. ■

Замечание. Доказательство дает алгоритм деления «в столбик».

Определение 14.1. Пусть $f, g \in K[x]$, $g \neq 0$. Говорят, что f *делится* на g (g *делит* f), если $\exists h \in K[x]$, такой что $f = g \cdot h$.

Определение 14.2. *Наибольший общий делитель* многочленов $f, g \in K[x]$ — это такой $h \in K[x]$, что

1. h делит оба f, g;
2. h имеет максимальную возможную степень.

Теорема 14.2. *Пусть* $f, g \in K[x]$ *и* $(f, g) \neq (0, 0)$. *Тогда*

1. $\exists$ *НОД*$(f, g) =: h$;
2. $\exists u, v \in K[x]$, *такие что* $h = u \cdot f + v \cdot g$.

Доказательство.

1. Прямой ход алгоритма Евклида;
2. Обратный ход алгоритма Евклида. ■

Замечание. НОД(f, g) определен однозначно с точностью до пропорциональности.
$2 = \text{НОД}(2x^2, 2x + 1) = 1$.

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

Определение 15.1. Коммутативное кольцо R без делителей нуля называется *кольцом главных идеалов* (КГИ), если всякий идеал в R является главным.

Пример. $\mathbb{Z}$ — все идеалы это $k\mathbb{Z} = (k)$ $(k \geqslant 0)$ — главные.

Предложение 15.1. $K[x]$ — КГИ.

Доказательство. Пусть $I \lhd K[x]$. Если $I = \{0\}$, то $I = (0)$ — главный.

Если $I \neq \{0\}$, то выберем в I многочлен наименьшей степени $g \neq 0$.

Тогда $(g) \subseteq I$. Пусть $f \in I$, разделим f на g с остатком:

$f = q \cdot g + r$, где либо $r = 0$, либо $\deg r < \deg g$. Но тогда $r = f - q \cdot g \in I$.

Так как $\deg g$ минимально, то $r = 0 \implies f \in (g) \implies I \subseteq (g)$.

Итог: $I = (g)$. ∎

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

Определение 16.1. Многочлен $h \in K[x]$, $\deg h > 0$ называется *неприводимым*, если его нельзя представить в виде $h = h_1 h_2$, где $\deg h_1 < \deg h$ и $\deg h_2 < \deg h$.

Иначе h называется *приводимым*.

Замечание.

1. $h \in K[x]$, $\deg h = 1 \implies h$ неприводим;
2. $h \in K[x]$, $\deg g \geqslant 2$, h неприводим $\implies h$ не имеет корней в K (следствие теоремы Безу);
3. $h \in K[x]$, $\deg h \in \{2, 3\} \implies [h$ неприводим $\iff h$ не имеет корней в $K]$.

Пример. $K = \mathbb{C}$, $h \in \mathbb{C}[x]$, $\deg h \geqslant 1$.
Если $\deg h \geqslant 2$, то h имеет корень $\implies$ h неприводим $\iff \deg h = 1$.

Лемма 16.1. Если $h \in K[x]$ — неприводим и h делит $g_1 \cdot \ldots \cdot g_k$ для некоторых $g_1, \ldots, g_k \in K[x]$, то $\exists i : h$ делит g_i.

Доказательство. Индукция по k.
$k = 1$ — ясно.
$k = 2$. Пусть $g_1 \not\vdots\, h$. Так как h неприводим, то НОД$(g_1, h) = 1 \implies \exists u, v \in K[x]$, такие что $1 = ug_1 + vh$. Умножим на g_2:

$$g_2 = u \cdot \underbrace{g_1 \cdot g_2}_{\vdots\, h} + v \cdot \underbrace{h \cdot g_2}_{\vdots\, h} \implies g_2 \;\vdots\; h.$$

Для $k > 2$ надо применить предыдущее рассуждение для $(g_1 \cdot \ldots \cdot g_{k-1}) \cdot g_k$ и воспользоваться предположением индукции. ■

Теорема 16.1. *Пусть $f \in K[x]$ и $\deg f \geqslant 1$. Тогда*

1. *$\exists$ разложение $f = h_1 \cdot \ldots \cdot h_k$, где все h_i неприводимы;*
2. *это разложение единственно с точностью до перестановки множителей и пропорциональности. Точнее, если $f = h'_1 \cdot \ldots \cdot h'_m$ — другое такое разложение, то $k = m$ и после подходящей перестановки множителей h_i и h'_i пропорциональны.*

Пример. $f = 6x^3 + 6x \implies f = (3x)(2x^2 + 2) = (x^2 + 1)(6x)$ — одинаковые разложения с точки зрения теоремы.

Доказательство. Пусть $\deg f = n$. Индукция по n.
$n = 1 \implies f$ неприводим, единственность есть.

$n > 1$

Существование f неприводим $\implies$ уже есть разложение.

Если же f приводим, то $f = f_1 \cdot f_2$, $\deg f_i < n$.

Тогда по предположению индукции $f_1 = g_1 \cdot \ldots \cdot g_p$, $f_2 = h_1 \cdot \ldots \cdot h_q$, где g_i, h_j — неприводимы.

Значит, $f = g_1 \cdot \ldots g_q \cdot h_1 \cdot \ldots \cdot h_q$ — разложение f на неприводимые.

Единственность Пусть $f = h_1 \cdot \ldots \cdot h_k = h'_1 \cdot \ldots \cdot h'_m$ — два разложение на неприводимые множители.

Если h_1 делит $h'_1 \cdot \ldots \cdot h'_m$, то по лемме существует i, такое что h_1 делит h'_i.

Переставив множители, будем считать, что h_1 делит h'_1. Так как h_1, h'_1 неприводимы, то $h' = \varepsilon \cdot h$, где $\varepsilon \in K \setminus \{0\}$. Так как в $K[x]$ нет делителей нуля, то можем сократить на h_1, получим

$$h_2 \cdot \ldots \cdot h_k = \varepsilon h'_2 \cdot \ldots \cdot h'_m \quad \leftarrow \deg < n.$$

Осталось применить предположение индукции. ■

Замечание.

1. Всякое КГИ факториально;
2. $K[x_1, \ldots, x_n]$, $n \geqslant 2$ — это не КГИ, но тоже факториально.

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

Пусть $h = a_n x^n + \dots + a_1 x + a_0 \in K[x]$ — многочлен, $\deg h = n > 0$.
Тогда, рассмотрим $F := K[x]/(h) \quad f \in K[x] \rightsquigarrow \overline{f} := f + (h) \in F$.

Замечание. $\overline{f} = \overline{0} \iff f \,\vdots\, h$.

Предложение 17.1. F — поле $\iff$ h неприводим.

Доказательство.

$\implies$ Если $h = h_1 \cdot h_2$ и $\deg h_i < n$, то $\overline{h} = \overline{h_1} \cdot \overline{h_2}$.
Так как $\overline{h} = 0$, то $\overline{h_1} \cdot \overline{h_2} = 0$. Значит в F есть делители нуля $\implies$ F — не поле — противоречие.

$\impliedby$ $f \in K[x]$, $\overline{f} \neq \overline{0} \implies f \not\vdots\, h \implies$ НОД$(f, h) = 1$.
Значит, $\exists u, v \in K[x]$, такие что $1 = uf + vh$. Отсюда $\overline{1} = \overline{u} \cdot \overline{f} + \overline{v} \cdot \overline{h} = \overline{u} \cdot \overline{f}$.
Получили, что $\overline{f}$ обратим $\implies$ F — поле. ∎

Пример.

1. $\mathbb{R}[x]/(x^2 + 1)$ — поле ($\simeq \mathbb{C}$).
2. $\mathbb{R}[x]/(x^2)$ — не поле, $\overline{x}$ — нильпотент, $\overline{x}^2 = \overline{0}$.

Рассмотрим отображение $K \to F, \quad \lambda \mapsto \overline{\lambda} = \lambda + (h)$, оно инъективно. Тогда K отождествляется с подполем в F, значит F становится векторным пространством над K.

Предложение 17.2. Элементы $\overline{1}$, $\overline{x}$, $\dots$, $\overline{x}^{n-1}$ образуют базис в F над K. В частности $\dim_K F = n$.

Доказательство. Пусть $\overline{f} \in F$, $f \in K[x]$. Поделим f на h с остатком:
$f = q \cdot h + r$, где $r = 0$ или $\deg r < n$. Тогда, $\overline{f} = \underbrace{\overline{q} \cdot \overline{h}}_{=\overline{0}} + \overline{r} = \overline{r} \in \left\langle \overline{1}, \overline{x}, \dots, \overline{x}^{n-1} \right\rangle$.

Если $b_0\overline{1} + b_1\overline{x} + \dots + b_{n-1}\overline{x}^{n-1} = \overline{0}$ для некоторых $b_i \in K$, то $b_0 + b_1 x + \dots + b_{n-1}x^{n-1} \,\vdots\, h \implies b_0 = b_1 = \dots = b_{n-1} = 0$. ∎

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

Пусть K — поле, $R = K[x_1, \dots, x_n]$.
$M := \{ax_1^{k_1} \cdot \ldots \cdot x_n^{k_n} \mid a \in K \setminus \{0\}, k_i \in \mathbb{N} \cup \{0\}\}$ — все одночлены от $x_1, \dots, x_n$.

Определение 18.1 (Лексикографический порядок на M)**.**

$$ax_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \succ bx_1^{j_1} \cdot \ldots \cdot x_n^{j_n} \quad \Longleftrightarrow \quad \begin{aligned} & i_1 = j_1 \\ & i_2 = j_2 \\ & \ldots \\ & i_{k-1} = j_{k-1} \\ & i_k > j_k. \end{aligned}$$

Пример. $x_1^2 x_2 \succ x_1^2 x_3^{228}$.

Замечание.

1. $m_1, m_2, m_3 \in M$, $m_1 \prec m_2 \implies m_1 m_3 \prec m_2 m_3$;
2. $m_1, m_2, m_3 \in M$, $m_1 \prec m_2$, $m_2 \prec m_3 \implies m_1 \prec m_3$.

$g \in R \rightsquigarrow M(g) := \{$все одночлены входящие в $g\}$.

Лемма 18.1. Не существует бесконечных убывающих цепочек $m_1 \succ m_2 \succ m_3 \succ \ldots$, где $m_i \in M$ $\forall i$.

Доказательство. От противного.
Пусть $m_1 \succ m_2 \succ m_3 \succ \ldots$ — бесконечная убывающая цепочка. Пусть $m_i = a_i x_1^{k_1(i)} \cdot \ldots \cdot x_n^{k_n(i)}$ $\forall i \in \mathbb{N}$.
Имеем

$$\begin{array}{ccccccccc} k_1(1) & \geqslant & k_1(2) & \geqslant & k_1(3) & \geqslant & \ldots & \Longrightarrow & \exists i_1 \in \mathbb{N} : k_1(i) = k_1(i_1)\ \forall i \geqslant i_1 \\ k_2(i_1) & \geqslant & k_2(i_1+1) & \geqslant & k_2(i_1+2) & \geqslant & \ldots & \Longrightarrow & \exists i_2 \geqslant i_1 : k_2(i) = k_2(i_2)\ \forall i \geqslant i_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \Longrightarrow & \exists i_n \geqslant i_{n-1} : k_n(i) = k_n(i_n)\ \forall i \geqslant i_n \end{array}$$

Итог: при $i \geqslant i_n$ все m_i имеют одинаковые наборы степеней — противоречие. ∎

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

Определение 19.1. $f \in R\backslash\{0\} \implies$ *старший член* $L(f)$ — это наибольший в лексикографическом порядке одночлен, присутствующий в f.

Лемма 19.1 (Лемма о старшем члене)**.** Пусть $f, g \in R \setminus \{0\}$. Тогда, $L(f, g) = L(f) \cdot L(g)$.

Доказательство. $u \in M(f),\ v \in M(g) \implies u \preccurlyeq L(f),\ v \preccurlyeq L(g)$.

$uv \preccurlyeq L(f) \cdot v \preccurlyeq L(f) \cdot L(g) \implies uv \preccurlyeq L(f) \cdot L(g)$, причем равенство достигается при $\begin{cases} u = L(f), \\ v = L(g). \end{cases}$

Значит, $L(f) \cdot L(g)$ больше любого другого одночлена в $fg \implies L(f) \cdot L(g) = L(f \cdot g)$. ■

Пусть $f, g \in R \setminus \{0\}$, g содержит одночлен m, такой что $m \,\vdots\, L(f)$. Тогда $m = L(f) \cdot m'$, где $m' \in M$.
Элементарная редукция: $g \xrightarrow{f} g' := g - m' \cdot f$.
В g одночлен m заменяется суммой нескольких меньших одночленов.

Пусть $F \subseteq R \setminus \{0\}$.

Определение 19.2. g *редуцируем* к g' при помощи F, если существует конечная цепочка элементарных редукций

$$g \xrightarrow{f_1} g_1 \xrightarrow{f_2} g_2 \xrightarrow{f_3} \dots \xrightarrow{f_k} g_k = g', \text{ где } f_i \in F.$$

Обозначение: $g \overset{F}{\rightsquigarrow} g'$.

g *нередуцируем* относитльно F, если $\forall m \in M(g)\ \forall f \in F \quad m \not\vdots\, L(f)$.

Лемма 19.2 (Конечность цепочек элементарных редукций)**.** $F \subseteq R \setminus \{0\} \implies$ всякая последовательность элементарных редукций относительно F за коненчое число шагов приводит к нередуцируемому многочлену.

Обозначение: $L_k(g)$ — k-й по старшинству одночлен в $g \in R$.

Доказательство. От противного.

Пусть существует бесконечная цепочка элементарных редукций $g_1 \xrightarrow{f_1} g_2 \xrightarrow{f_2} g_3 \xrightarrow{f_3} \dots$
В силу леммы о конечности убывающих цепочек одночленов имеем

$$\begin{array}{ccccccccc} L(g_1) & \succcurlyeq & L(g_2) & \succcurlyeq & L(g_3) & \succcurlyeq & \dots & \implies & \exists i_1 \in \mathbb{N} : L(g_i) = L(g_{i_1})\ \forall i \geqslant i_1 \\ L_2(g_{i_1}) & \succcurlyeq & L_2(g_{i_1} + 1) & \succcurlyeq & L_2(g_{i_1} + 2) & \succcurlyeq & \dots & \implies & \exists i_2 \geqslant i_1 : L_2(g_i) = L_2(g_{i_2})\ \forall i \geqslant i_2 \\ \dots & \dots & \dots & \dots & \dots & \dots & \dots & & \end{array}$$

Итог: $L(g_{i_1}) = L(g_{i_2}) \succ L_2(g_{i_2}) = L_2(g_{i_3}) \succ L_3(g_{i_3}) = L_3(g_{i_4}) \succ \dots \implies L(g_{i_1}) \succ L_2(g_{i_2}) \succ L_3(g_{i_3}) \succ \dots$ — бесконечно убывающая цепочка одночленов — противоречие. ■

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

Определение 20.1. Если $g \overset{F}{\rightsquigarrow} r$ и r нередуцируем, то r называется *остатком* многочлена g относительно F.

Замечание. Вообще говоря, остаток определен неоднозначно.

Определение 20.2. Множество F называется *системой Грёбнера*, если $\forall g \in R$ остаток g относительно F определен однозначно, то есть не зависит от цепочки приводящих к нему элементарных преобразований.

Предложение 20.1. Следующие условия эквивалентны:

1. F — система Грёбнера;
2. $\forall g \in R$ обладает свойством:

   Если $g \xrightarrow{f_1} g_1$ и $g \xrightarrow{f_2} g_2$ — две элементарных редукции, то $\exists g' \in R$, такой что $g_1 \overset{F}{\rightsquigarrow} g'$ и $g_2 \overset{F}{\rightsquigarrow} g'$.

Доказательство.

(1) $\implies$ (2) В качестве g' можно взять остаток g относительно F.

(2) $\implies$ (1) Пусть

$B(F) :=$ «все многочлены из R, для которых остаток относительно F определен неоднозначно».

$E_F(g)$ — множество всех элементарных редукций многочлена g относительно F.

Пусть $B(F) \neq \varnothing$ и $g \in B(F)$.

Если $E_F(g) \cap B(F) \neq \varnothing$, то возьмём $g_1 \in E_F(g) \cap B(F)$.

Если $E_F(g_1) \cap B(F) \neq \varnothing$, то возьмём $g_2 \in E_F(g_1) \cap B(F)$.

И так далее.

По лемме о конечности цепочек элементарных редукций, $\exists i \in \mathbb{N}$, такой что $E_F(g_i) \cap B(F) = \varnothing$.

Тогда $\exists$ две такие цепочки элементарных редукций

$$\left.\begin{array}{l} g_i \to h_1 \to \cdots \to r_1 \\ g_i \to h_2 \to \cdots \to r_2 \end{array}\right\} \text{ остатки } r_1 \neq r_2.$$

По условию $\exists r \in R$ — нередуцируемый многочлен, такой что $h_1 \rightsquigarrow r$, $h_2 \rightsquigarrow r$.

Так как $h_1, h_2 \notin B(F)$, то $r_1 = r = r_2$ — противоречие. ∎

Замечание.

1. $g \overset{F}{\rightsquigarrow} g_1 \implies \forall m \in M \quad mg \overset{F}{\rightsquigarrow} mg_1$;
2. $g_1 - g_2 \overset{F}{\rightsquigarrow} 0 \implies \exists g' : g_1 \rightsquigarrow g'$ и $g_2 \rightsquigarrow g'$.

21 S-многочлены. Критерий Бухбергера

Пусть $f_1,\ f_2 \in R$.
Рассмотрим $m = \text{НОК}(L(f_1), L(f_2)) \in M$.
Пусть $m_1, m_2 \in M$ таковы, что $m = m_1 L(f_1) = m_2 L(f_2)$.

Определение 21.1. Многочлен $S(f_1, f_2) := m_1 f_1 - m_2 f_2$ называется *S-многочленом*, построенным по $f_1,\ f_2$.

Замечание. $S(f_2, f_1) = -S(f_1, f_2)$.

Теорема 21.1 (Критерий Бухбергера). *Для системы $F \subseteq R \setminus \{0\}$ следующие условия эквивалентны:*

1. *F — система Грёбнера;*
2. *$\forall f_1, f_2 \in F \quad S(f_1, f_2) \overset{F}{\rightsquigarrow} 0$.*

Доказательство.

(1) $\implies$ (2) $m = \text{НОК}(L(f_1), L(f_2)) = m_1 \cdot L(f_1) = m_2 \cdot L(f_2)$.

Значит $m_1 f_1 \xrightarrow{f_1} 0$ и $m_1 f_1 \xrightarrow{f_2} [m_1 f_1 - m_2 f_2] = S(f_1, f_2) \overset{F}{\rightsquigarrow} r$ — остаток.

Но так как F — система Грёбнера, $r = 0$.

(2) $\implies$ (1) Пусть $g \in R$, $m_1, m_2 \in M(g)$ и мы сделали элементарную редукцию m_1 при помощи $f_1 \in F$ и m_2 при помощи f_2.

$$m_1 = m_1' \cdot L(f_1), \quad m_2 = m_2' \cdot L(f_2)$$
$$g \xrightarrow{f_1} g_1 = g - m_1' f_1, \quad g \xrightarrow{f_2} g_2 = g - m_2' f_2.$$

Достаточно показать, что $\underbrace{g_1 - g_2}_{m_2' f_f - m_1' f_1} \overset{F}{\rightsquigarrow} 0$.

Случай 1 $L(m_2' f_2)$ и $L(m_1' f_1)$ не пропорциональны, можно считать $L(m_2' f_2) \succ L(m_1' f_1)$.

$$m_2' f_2 - m_1' f_1 \xrightarrow{f_2} -m_1' f_1 \xrightarrow{f_1} 0.$$

Случай 2 $L(m_2' f_2) = L(m_1' f_1)$. Тогда $\exists m \in M$, такое что $m_2' f_2 - m_1' f_1 = m S(f_1, f_2) \overset{F}{\rightsquigarrow} 0$.

Случай 3 $L(m_2' f_2) = \alpha L(m_1' f_1)$ при $\alpha \neq 1$. Тогда $L(m_2' f_2 - m_1' f_1) = (\alpha - 1) L(m_1' f_1)$. Значит,

$$m_2' f_2 - m_1' f_1 \xrightarrow{f_1} m_2' f_2 - m_1' f_1 - (\alpha - 1) m_1' f_1 = m_2' f_2 - \alpha m_1' f_1.$$

Получили $L(m_2' f_2) = L(\alpha m_1' f_1)$, а значит попали в случай 2. ■

Следствие 21.1. Если $f_1, f_2 \in F, \quad S(f_1, f_2) \overset{F}{\rightsquigarrow} r$ — остаток и $r \neq 0$, то F — не система Грёбнера.

Доказательство. Если F — система Грёбнера, то $S(f_1, f_2) \rightsquigarrow 0$ и $S(f_1, f_2) \rightsquigarrow r$. Так как остаток определен однозначно, то $r = 0$ — противоречие. ■

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

Пусть $I \triangleleft R$ – идеал.

Определение. Множество F называется **базисом Грёбнера** идеала I, если
(1) $I = (F)$
(2) F – система Грёбнера.

Теорема. $F \subseteq I \backslash \{0\} \Rightarrow$ следующие условия эквивалентны:
(1) F – базис Грёбнера в I
(2) $\forall\, g \in I\, g \overset{F}{\rightsquigarrow} 0$
(3) $\forall\, g \in I \backslash \{0\}\ \exists f \in F:\ L(g) \vdots L(f)$

Доказательство. (1) $\Rightarrow$ (2): пусть $I_0 = \{g \in I | \overset{F}{\rightsquigarrow} 0\}$, тогда
1) $0 \in I_0$
2) $g \in I_0 \Rightarrow -g \in I_0$
3) $g_1, g_2 \in I_0 \Rightarrow g_1 + g_2 \in I_0$ Пусть $g = (g_1 + g_2) - g_2 \overset{F}{\rightsquigarrow} 0 \Rightarrow$ существует остаток r, такой что $g_1 + g_2 \overset{F}{\rightsquigarrow} r, g_2 \overset{F}{\rightsquigarrow} r$
Но F – базис Грёбнера $\Rightarrow$ остаток определён однозначно и для g_2 получаем $r = 0$.
$\Rightarrow g_1 + g_2 \overset{F}{\rightsquigarrow} 0$
4) $g \in I_0 \Rightarrow \forall m \in M\ mg \in I_0$
1) – 3) $\Rightarrow I_0$ – подгруппа в I по сложению.
3) – 4) $\Rightarrow I_0$ – идеал в R.
$F \subseteq I_0 \Rightarrow I = (F) \subseteq I_0 \Rightarrow I_0 = I$
(2) $\Rightarrow$ (1) $g \in I \Rightarrow g \overset{F}{\rightsquigarrow} 0 \Rightarrow g = m_1 f_1 + ... + m_k f_k$, где $m_1,...,m_k \in M, f_1,...,f_k \in F$
$\Rightarrow g \in (F) \Rightarrow I \subseteq (F)$. Но $F \subseteq I \Rightarrow (F) \subseteq I \Rightarrow I = (F)$
$f_1 f_2 \in F \Rightarrow S(f_1,f_2) \in (F) = I \Rightarrow S(f_1,f_2) \overset{F}{\rightsquigarrow} 0 \Rightarrow F$ – система Грёбнера по критерию Бухбергера.
(3) $\Rightarrow$ (2) $g \in I, g \overset{F}{\rightsquigarrow} r$, где r – остаток. $\Rightarrow r = \underset{I}{g} - m_1 f_1 - \underset{I}{...} - m_k f_k,\ m_i \in M, f_i \in F$

$\Rightarrow r \in I$, если $r \neq 0$, то $L(r) \vdots L(f)$ для некоторого $f \in F$
$\Rightarrow r$ редуцируем дальше – противоречие $\Rightarrow r = 0$ (2) $\Rightarrow$ (3)$\forall g \in I, g \overset{F}{\rightsquigarrow} 0 \Rightarrow$ в соотв. цепочке элементарных редукций есть одна, применяемая к $L(g) \Rightarrow \exists f \in F:\ L(g) \vdots L(f)$ ■

Следствие. F – базис Грёбнера в I $\Rightarrow$
1) $\forall\ g \in I$ любая цепочка элементарных редукций относительно F приводит к 0
2) $\forall\ g \in R:\ g \in I \Leftrightarrow$ остаток g относительно системы f равен 0

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

Лемма. $\nexists$ бесконечных последовательностей одночленов $m_1, m_2, \ldots$, таких что $m_i \not\vdots\, m_j\ \forall i > j$.

Доказательство. Индукция по n: $n = 1 \Rightarrow$ степени убывают $\Rightarrow$ цепочка конечна.

Пусть доказано для $< n$, докажем для n. Пусть есть бесконечная последовательность $m_1, m_2, \ldots,\ m_i \not\vdots\, m_j \quad \forall i > j$: $m_i = a_i x_1^{k_1(i)} \cdot \ldots \cdot x_n^{k_n(i)}$. Тогда $\forall j \geqslant 2\ m_j \not\vdots\, m_1 \Rightarrow \exists i \in \{1, \ldots, n\}$, такое что $k_i(j) < k_i(1)$ для **бесконечного числа значений** j.
Без ограничения общности считаем $i = n$. Перейдя к подпоследовательности, можем считать, что $k_n(j) < k_n(1)$, $\forall j \geqslant 2$. Тогда $k_n(j)$ принимает лишь конечное число значений $\Rightarrow$ какое–то из этих значений встретится бесконечно много раз. Снова перейдя к подпоследовательности, можем считать, что $k_n(1) = k_n(2) = \ldots$, полагая $x_n = 1$, получим последовательность от $x_1, \ldots, x_{n-1}$ с тем же свойством – противоречие. ■

Алгоритм Бухбергера построения базиса Грёбнера идеала.
Дано: $I = (F), F = f_1, \ldots, f_k$
Перебираем все пары $i < j$. Если $\exists\ i < j$, такое что $S(f_i, f_j) \overset{F}{\rightsquigarrow} r_1 \neq 0$, r_1 - остаток, то добавляем r_1 в F и повторяем процедуру для $F \cup \{r_1\}$. В итоге получаем $\forall i, j : S(f_i, f_j) \overset{F \cup \{r_n\}}{\rightsquigarrow} 0$. Полученное F – это система Грёбнера по критерию Бухбергера $\Rightarrow F$ - базис Грёбнера в I. Если алгоритм не закончится за конечное число шагов, то получим бесконечную последовательность $r_1, r_2, r_3, \ldots$, такую что $L(r_i) \not\vdots\, L(r_j)$ при $i > j$ – противоречие с леммой.

24 Теорема Гильберта о базисе идеала

Теорема. Всякий идеал в R порождается конечным числом элементов.

Доказательство. $I \triangleleft R$.
$I = \{0\} = I = (0)$ – ок.
$I \neq 0$. Выберем $r_1 \in I \setminus \{0\}$. Если $I = (r_1)$, то ок;
Иначе выберем $f_2 \in I \setminus (r_1)$, $f_2 \overset{\{r_1\}}{\rightsquigarrow} r_2$ – остаток.
Тогда $r_2 \in I \setminus (r_1), L(r_2) \not\vdots L(r_1)$. Если $I = (r_1, r_2)$, то ок.
Иначе выберем $f_3 \in I \setminus (r_1, r_2), f_3 \overset{\{r_1, r_2\}}{\rightsquigarrow} r_3$ – остаток.
Тогда $r_3 \in I \setminus (r_1, r_2), L(r_3) \not\vdots L(r_1), L(r_2)$.
...
Если процесс не закончится, то получится бесконечная последовательность $r_1, r_2, \ldots$, такая что $L(r_i) \not\vdots L(r_j)$ при $i > j$ - невозможно по лемме $\Rightarrow \exists k : I = (r_1, \ldots, r_k)$ ■

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

Предложение. $f_1, f_2 \in R \setminus \{0\}, \text{НОД}(L(f_1), L(f_2)) = 1 \Rightarrow S(f_1, f_2) \overset{\{f_1, f_2\}}{\rightsquigarrow} 0$

Доказательство. Достаточно показать, что f_1, f_2 – базис Грёбнера в идеале (f_1, f_2).

Пусть $g \in (f_1, f_2)$ и $g = h_1 f_1 + h_2 f_2$, где $h_1, h_2 \in R$. Покажем, что $L(g) \vdots L(f_1)$ или $L(g) \vdots L(f_2)$.
Пусть это не так, тогда $L(h_1 f_1) = -L(h_2 f_2) \Rightarrow$ [по лемме о старшем члене] $\Rightarrow L(h_1) = L(f_2) \cdot m, L(h_2) = -L(f_1) \cdot m, m \in M$.
Положим $h_1' = h_1 - f_2 m, h_2' = h_2 + f_1 m; L(h_1') \prec L(h_1), L(h_2') \prec L(h_2)$. Имеем $g = (h_1' + f_2 m) f_1 + (h_2' - f_1 m) f_2 = h_1' f_1 + h_2' f_2$ и $L(h_1' f_1) = -L({}'_2 f_2)$. Повторяя процедуру, получим бесконечную цепочку равенств $g = h_1 f_1 + h_2 f_2 = h_1' f_1 + h_2' f_2 = \ldots = h_1^{(i)} f_1 + h_2^{(i)} f_2 = \ldots$, причём $L(h_1) \succ L(h_1') \succ \ldots \succ L(h_1^{(i)}) \succ \ldots$ – противоречие. ■

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

Поля $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$, где p – простое. $K[x]/(h)$ (K – поле, h – неприводимый многочлен)
Определение. Характеристика поля k – наименьшее $p \in \mathbb{N}$, такое что $\underbrace{1+1+...+1}_{p} = 0$

Если такого p не существует, то говорят, что характеристика поля K равна 0.
Обозначение: $\operatorname{char} K$
Примеры: $\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{C} = \operatorname{char}\mathbb{R} = 0$, $\operatorname{char}\mathbb{Z}_p = p$
Предложение. K – поле $\Rightarrow$ либо $\operatorname{char} K = 0$, либо $\operatorname{char} K$ – простое число.

Доказательство. $\operatorname{char} K = p$, пусть $p > 0$. Так как $0 \neq 1$, то $p \geqslant 2$.
Если $p = m \cdot k$, тогда $0 = \underbrace{1+...+1}_{p} = \underbrace{1+...+1}_{m\cdot k} = \underbrace{(1+...+1)}_{m} \cdot \underbrace{(1+...+1)}_{k}$. Но мы знаем, что $\underbrace{1+..+1}_{k} \neq 0$ и $\underbrace{1+..+1}_{m} \neq 0$, а значит в K есть делители нуля, из чего следует, что K – не поле. Противоречие.
$\Rightarrow p$ – простое. ■

Определение. K, F – поля, $K \subseteq F \Rightarrow F$ называется **расширением** поля K.
($''K \subseteq F''$ – расширение полей)

Определение. Степень расширения полей $K \subseteq F$ – это размерность F как векторного пространства над K.
Обозначение: $[F : K]$
Примеры: $[\mathbb{C} : \mathbb{R}] = 2$, $[\mathbb{R} : \mathbb{Q}] = \infty$

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

Лемма о степени композиции расширения полей.
Пусть $K \subseteq F, F \subseteq L$ – конечные расширения полей. Тогда $K \subseteq L$ – тоже конечное расширение, причём $[L : K] = [L : F] \cdot [F : K]$

Доказательство. Пусть e_1,...,e_n – базис F над K, f_1,...,f_m – базис L над F.
Покажем, что $\{e_i f_j\}$ – базис L над K.
1) $a \in L \Rightarrow a = \sum_{j=1}^{m} a_j f_j$, где $a_j \in F$.
При этом a_j раскладывается по базису e_1,...,e_m: $a_j = \sum_{i=1}^{n} b_{ij} e_i$, где $b_i j \in K$
$\Rightarrow a = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} b_{ij} e_i\right) f_j = \sum_{j=1}^{m} \sum_{i=1}^{n} b_{ij} e_i f_j$ Итог: $L = \langle e_i f_j \rangle$
2) Если $\sum_{j=1}^{m} \sum_{i=1}^{n} c_{ij} e_i f_j = 0$, где $c_{ij} \in K$, то $= \sum_{j=1}^{m} \left(\sum_{i=1}^{n} c_{ij} e_i\right) f_j = 0$
$\{f_j\}$ – базис L над $F \Rightarrow \ \forall\, j \ \sum_{i=1}^{n} c_{ij} e_i = 0$, знаем, что $\{e_i\}$ – базис F над K
$\Rightarrow \forall\, i,j :\ c_{ij} = 0 \Rightarrow$ Система $\{e_i f_j\}$ линейно независима. ■

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

K – поле, $h = a_n x^n + ... + a_1 x + a_0 \in K[x], a_n \neq 0$, $\deg h = n$
h неприводим $\Rightarrow F := K[x]/(h) \quad K \subseteq F \quad [F : K] = n$
$\forall f \in K[x] \rightsquigarrow \overline{f} = f + (h) \in F$
Предложение. Элемент $\overline{x}$ является корнем многочлена h в F.

Доказательство. $h(\overline{x}) = a_n \overline{x}^n + ... + a_1 \overline{x} + a_0 = \overline{h} = \overline{0}$ в поле F. ■

Замечание. Переход от K к F называется присоединением корня неприводимого многочлена h.
Следствие. $f \in K[x], \deg f \geqslant 1$ $\exists$ конечное расширение $K \subseteq F$, такое что f имеет корень в F.

Доказательство. Достаточно взять $F := K[x]/(h)$, где h – неприводимый делитель f. ■

Следствие. $\forall$ $f \in K[x], \deg f \geqslant 1$ $\exists$ конечное расширение $K \subseteq F$, такое что f разлагается на линейные множители над F.

Доказательство. Предыдущее следствие + следствие из теоремы Безу + индукция по $\deg f$. ■

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

$K \subseteq F$

Определение. Элемент $\alpha \in F$ называется **алгебраическим** над K, если $\exists\ f \in K[x], \deg f \geqslant 1$, такой что $f(\alpha) = 0$ и **трансцендентным** иначе.

Определение. **Минимальным многочленом** элемента $\alpha \in F$, алгебраического над K, называется такой $h \in K[x], \deg h \geqslant 1$, что $h(\alpha) = 0$ и h имеет минимальную степень.

Свойства минимального многочлена

Пусть $K \subseteq F$ – расширение полей, $\alpha \in F$ – элемент, алгебраический над K, и $h \in K[x]$ – его минимальный многочлен. Тогда:

1) h определён однозначно с точностью до пропорциональности.

2) Для всякого $f \in K[x]$ имеем $f(\alpha) = 0 \Leftrightarrow f \vdots h$

3) h неприводим над K

Доказательство. Положим $I = \{f \in K[x] \mid f(\alpha) = 0\}$. Тогда I – идеал в $K[x]$.
Так как $K[x]$ – КГИ, то $\exists\ g \in I : I = (g)$.

$h(\alpha) = 0 \Rightarrow h \in I \Rightarrow h \vdots g \Rightarrow h$ пропорционален g в силу минимальности $\Rightarrow$ (1) и (2)
(3) Если $h = h_1 h_2$, $\deg h_i < \deg h,\ i = 1{,}2$. Тогда либо $h_1(\alpha) = 0$ либо $h_2(\alpha) = 0$, ну а это противоречие, так как мы выбирали минимальный h. ∎

29 Подполе в расширении полей, порождённое алгебраическим элементом

$K \subseteq F, \alpha \in F$ – элемент, алгебраический над K, h_α – минимальный многочлен для α
$K(\alpha) :=$ пересечение всех подполей в F, содержащих K и α = наименьшее подполе в F, содержащее K и α.

Замечание. $K(\alpha) = \left\{ \dfrac{f(\alpha)}{g(\alpha)} \,\middle|\, f,g \in K[x], g(\alpha) \neq 0 \right\}$

Теорема. Существует изоморфизм $\psi : K[x]/(h_\alpha) \xrightarrow{\sim} K(\alpha)$, такое что $\psi(\overline{x}) = \alpha$

Доказательство. Рассмотрим гомоморфизм $\varphi : K[x] \to F, f \to f(\alpha)$
Тогда $\ker \varphi = (h_\alpha) \Rightarrow$ по теореме о гомоморфизме для колец получаем изоморфизм $\psi : K[x]/(h_\alpha) \xrightarrow{\sim} Im\varphi, \overline{x} \to \alpha$
Так как $K[x]/(h_\alpha)$ – поле, то $Im\varphi$ – подполе в F, $K \subseteq Im\varphi,\ \alpha = \psi(\overline{x}) \in Im\varphi$
$\Rightarrow K[\alpha]\varphi \subseteq Im\varphi$
С другой стороны, $Im\varphi = \{f(\alpha) \mid f \in K[x]\}$ – содержится в любом поле, содержащем K и α.
$\Rightarrow Im\varphi \subseteq K(\alpha)$ ∎

Следствие. $\forall y \in K(\alpha)$ единственным образом представим в виде $y = \beta_0 + \beta_1\alpha + ... + \beta_{n-1}\alpha^{n-1}$, где $\beta_i \in K$.

30 Порядок конечного поля. Автоморфизм Фробениуса

К – конечное поле $\operatorname{char} K = p > 0$ – простое число.
Пусть $\langle 1 \rangle \subseteq K$ – подгруппа по сложению, порождаемая 1.
Заметим, что $\langle 1 \rangle$ – подкольцо, изоморфное $\mathbb{Z}_p \Rightarrow \langle 1 \rangle$ – поле, изоморфное $\mathbb{Z}_p$.
Теорема. $|K| = p^n$, где $n = \dim_{\mathbb{Z}_p} K$

Доказательство. $K \supseteq \mathbb{Z}_p \Rightarrow K$ – векторное пространство над $\mathbb{Z}_p$.
Пусть $n = \dim_{\mathbb{Z}_p} K$. Выберем базис $e_1,...,e_n$ в K над $\mathbb{Z}_p$.
Тогда $K = \{a_1e_1 + ... + a_ne_n \mid a_i \in \mathbb{Z}_p\}$
$\forall\ a_i$ есть ровно p вариантов $\Rightarrow |K| = p^n$ ■

Общая конструкция конечных полей.
Выбираем неприводимый многочлен $h \in \mathbb{Z}_p[x],\ \deg h = n$. Тогда $F := \mathbb{Z}_p[x]/(h)$ – поле, векторное пространство над $\mathbb{Z}_p$ размерности $n \Rightarrow |F| = p^n$.

Автоморфизм Фробениуса.
$a,b \in K \Rightarrow$

$(a+b)^p = a^p + C_p^1 a^{p-1}b + C_p^2 a^{p-2}b^2 + ... + C_p^{p-1}ab^{p-1} + b^p = a^p + b^p$, так как $C_p^k \,\vdots\, p$ при $1 \leqslant k \leqslant p-1$
Рассмотрим отображение $\varphi : K \to K, a \to a^p$. Имеем:
$\varphi(a+b) = (a+b)^p = a^p + b^p = \varphi(a) + \varphi(b)$,
$\varphi(ab) = (ab)^p = a^p b^p = \varphi(a) \cdot \varphi(b)$
$\Rightarrow \varphi$ – гомоморфизм колец.
$\ker\varphi$ – идеал в K, но в поле нет собственных идеалов $\Rightarrow$ либо $\ker\varphi = K$, либо $\ker\varphi = \{0\}$. Так как $\varphi(1) = 1$, то $\ker\varphi \neq K \Rightarrow \ker\varphi = \{0\} \Rightarrow \varphi$ инъективно.
Если $|K| < \infty$, то φ – биекция. В этом случае φ называется **автоморфизмом Фробениуса**. ("автоморфизм"="изоморфизм в себя")

31 Теорема существования для конечных полей

Замечание. Если K – поле и $\psi : K \to K$ – автоморфизм, то подмножество $K^{\psi} := \{x \in K \mid \psi(x) = x\}$ неподвижных элементов всегда является подполем в K.

Теорема. Для любого простого числа p и всякого $n \in \mathbb{N}$ существует единственное с точностью до изоморфизма поле K, такое что $|K| = p^n$

Доказательство. **Существование.** Положим $q = p^n$.
Рассмотрим многочлен $f = x^q - x \in \mathbb{Z}_p[x]$. Пусть $F \subseteq \mathbb{Z}_p, |F| < \infty$ – конечное расширение, такое что f разлагается в F на линейные множители.
Пусть $K \subseteq F$ – это множество всех корней многочлена f в F.

Покажем, что $|K| = q = p^n$. Если это не так, то $\exists\ \alpha \in K$, такое что $f \vdots (x-\alpha)^2 \Rightarrow f = (x-\alpha)^2 \cdot g$, где $g \in K[x]$. Тогда $f' = 2(x-\alpha) \cdot g + (x-\alpha)^2 \cdot g' \vdots (x-\alpha)$.

Но $f = x^q - x \Rightarrow f' = q \cdot x^{q-1} - 1 = p^n \cdot x^{q-1} - 1 = -1 \not\vdots (x-\alpha)$ – противоречие $\Rightarrow |K| = q$.
$a \in K \Leftrightarrow f(a) = 0 \Leftrightarrow a^q - a = 0 \Leftrightarrow a^q = a \Leftrightarrow a^{p^n} = a \Leftrightarrow \varphi^n(a) = a \Leftrightarrow a$ – неподвижный элемент для автоморфизма $\psi = \varphi^n$
Вывод: $K = F^{\psi} \Rightarrow K$ – подполе в F. ■

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

Обозначение: Поле из q элементов обозначается $\mathbb{F}_q$
Обозначение: K – поле $\Rightarrow K^{\times} = (K \backslash \{0\}, \times)$ – мультипликативная группа поля K.

Предложение. Группа $\mathbb{F}_q^{\times}$ является циклической.

Доказательство. Положим $m = \exp(\mathbb{F}_q^{\times}), m \leqslant q-1$. Если $\mathbb{F}_q^{\times}$ не циклическая, то $m < q-1$. Но тогда $a^m = 1$ $\forall a \in \mathbb{F}_q^{\times}$ $\Rightarrow$ многочлен $x^m - 1$ имеет $\mathbb{F}_q$ не меньше $q-1$ корней, но это невозможно, так как $m < q-1$ ■

Предложение. Пусть p – простое и $n \in \mathbb{N}$. Тогда поле $\mathbb{F}_q$ можно реализовать в виде $\mathbb{Z}_p[x]/(h)$, где $h \in \mathbb{Z}_p[x]$ – неприводимый многочлен, $\deg h = n$. В частности, $\forall n \in \mathbb{N}$ в $\mathbb{Z}_p[x]$ существуют неприводимые многочлены степени n.

Доказательство. Пусть $\alpha \in \mathbb{F}_q^{\times}$ – порождающий элемент циклической группы $\mathbb{F}_q^{\times}$. $\mathbb{Z}_p \subseteq F_q \Rightarrow Z_p(\alpha)$ содержит $\alpha, ..., \alpha^{q-1}$ $(q = p^n)$ $\Rightarrow \mathbb{Z}_p(\alpha) = \mathbb{F}_q \Rightarrow \mathbb{F}_q \simeq \mathbb{Z}_p[x]/(h)$, где h – минимальный многочлен для α над $\mathbb{Z}_p$.
Если $\deg h = d$, то $|\mathbb{Z}_p[x]/(h)| = p^d$
$\Rightarrow p^d = p^n \Rightarrow d = n$ ■

Теорема. Пусть $q = p^n$, где p – простое.
1) $F \subseteq \mathbb{F}_q$ – подполе, то $F \simeq \mathbb{F}_{p^m}$, где $m|n$
2) $\forall$ $m \in \mathbb{N}$, $m|n$, существует единственное подполе $F \subseteq \mathbb{F}_q$, такое что $|F| = p^m$