Алгебра: Лекции

Авдеев Р. С.

Содержание

1 Лекция №1

Лекция 07.04.2020

1.1 Бинарные операции

Пусть M – некоторое множество

Определение.

Бинарная операция на множестве M – это отображение $\circ : M \times M \mapsto M$. Пара $(M, \circ)$ называется множеством с бинарной операцией

1.2 Полугруппы, моноиды, группы, коммутативные (абелевы) группы

Определение.

1. $(M, \circ)$ называется группой, если выполнены следующие условия:
   (a) $(a \circ b) \circ c = a \circ (b \circ c)$ – ассоциативность
   (b) $\exists$ нейтральный элемент, то есть такой $e \in M$, что $\forall a \in M : e \circ a = a \circ e = a$
   (c) $\forall a \in M$ $\exists$ обратный элемент (a^{-1}), то есть такой b, что $a \circ b = b \circ a = e$
2. $(M, \circ)$ называется полугруппой, если требуется только условие (a)
3. $(M, \circ)$ называется моноидом, если требуются только (a) и (b)

Пример.

$(\mathbb{N}, +)$ – полугруппа, но не моноид
$(\mathbb{N} \cup \{0\}, +)$ – моноид

Замечание.

1. Примеры неассоциативных операций: $(\mathbb{Z}, -)$, $(\mathbb{N}, a \circ b = a^b)$
2. Нейтральный элемент единственен (если существует)
   Если e_1, e_2 – два нейтральных, то $e_1 = e_1 \circ e_2 = e_2$
3. Обратный элемент единственен (если существует)
   b_1, b_2 – два обратных к $a \Rightarrow b_1 = b_1 \circ e = b_1 \circ (a \circ b_2) = (b_1 \circ a) \circ b_2 = e \circ b_2 = b_2$
4. $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$

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

Определение.

Группа G называется коммутативной (абелевой), если $\forall a, b \in G : ab = ba$

Абстрактные группы: мультипликативная запись: ab, e, a^{-1}
Абелевы группы: аддитивная запись: $a + b, 0, -a$

1.3 Порядок группы

Определение.

Порядок группы G – это число элементов в ней. Обозначается $|G|$.
G называется конечной, если $|G| < \infty$, бесконечной, если $|G| = \infty$

1.4 Примеры групп

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

2. Числовые мультипликативные группы:
   $(\mathbb{Q} \setminus \{0\}, \times), (\mathbb{R} \setminus \{0\}, \times), (\mathbb{C} \setminus \{0\}, \times), (\mathbb{Z}_n \setminus \{\bar{0}\}, \times)$

3. Группы матриц (операция $\times$):
   $GL_n(\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) \bigm| \det A \neq 0\}$ – полная линейная группа
   $SL_n(\mathbb{R}) = \{A \in \mathrm{Mat}_n(\mathbb{R}) \bigm| \det A = 1\}$ – специальная линейная группа

4. Группы перестановок (операция $\times$):
   симметрическая группа S_n – все перестановки длины n, $|S_n| = n!$
   знакопеременная группа A_n – все чётные перестановки длины n, $|A_n| = n!/2$

1.5 Подгруппы

Определение.

Подмножество H группы G называется подгруппой, если

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

Несобственные подгруппы: $\{e\} \subseteq G, G \subseteq G$.
Остальные подгруппы называются собственными

Пример.

$2\mathbb{Z}$ (все целые числа кратные 2) – подгруппа в $(\mathbb{Z}, +)$

1.6 Описание всех подгрупп в группе целых чисел по сложению

Предложение.

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

Доказательство.

Пусть $H \in \mathbb{Z}$ – подгруппа.
Если $H = \{0\}$, то $H = 0\mathbb{Z}$
Пусть теперь $H \neq \{0\}$. Тогда $x \in H \Leftrightarrow -x \in H$
Положим $k = \min(H \underset{\neq \varnothing}{\cap} \mathbb{N})$
Тогда $k\mathbb{Z} \subseteq H$(если мы k сложим с собой много раз, то результат тоже будет лежать в подгруппе)
Пусть $a \in H \Rightarrow$ разделим a на k с остатком: $a = q \cdot k + r$, $0 \leqslant r < k$
Тогда $r = \underset{\in H}{a} - q \cdot \underset{\in H}{k} \in H$
Так как k – минимальна $\Rightarrow r = 0 \Rightarrow a = q \cdot k \Rightarrow a \in k\mathbb{Z} \Rightarrow k\mathbb{Z} = H$

$\boxdot$

1.7 Циклические подгруппы

Пусть G – группа, $g \in G, n \in \mathbb{Z}$

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

Определение.

Пусть $g \in G$. $\langle g \rangle := \{g^n \mid n \in \mathbb{Z}\}$ называется циклической подгруппой, порождаемой элементом g

g – образующий или порождающий элемент

Пример.

$2\mathbb{Z} = \langle 2 \rangle = \langle -2 \rangle$

1.8 Порядок элемента группы

Пусть G – группа, $g \in G$
$M(g) = \{n \mid g^n = e\}$

Определение.

Порядок элемента g – это

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

Замечание.

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

1.9 Связь между порядком элемента и порядком порождаемой им циклической подгруппы

Предложение.

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

Доказательство.

Имеем $g^k = g^s \Rightarrow g^{k-s} = e \ (\star)$

1. $\operatorname{ord}(g) = \infty \underset{(\star)}{\Rightarrow} \forall k > s : g^k \neq g^s \Rightarrow |\langle g \rangle| = \infty$

2. $\operatorname{ord}(g) = m < \infty \Rightarrow$ элементы $g^0 = e, g^1 = g, g^2, \ldots, g^{m-1}$ попарно различны (если $\exists\, k, s :$ $g^k = g^s \Rightarrow g^{k-s} = e$, но $\operatorname{ord}(g) = m$)

   $n \in \mathbb{Z} \Rightarrow n = q \cdot m + r, 0 \leqslant r < m$
   $\Rightarrow g^n = g^{qm} \cdot g^r = \overset{e}{(g^m)^q} \cdot g^r = g^r$
   $\Rightarrow \langle g \rangle = \{e, g, g^2, \ldots, g^{m-1}\} \Rightarrow |\langle g \rangle| = m = \operatorname{ord}(g)$

$\boxdot$

1.10 Циклические группы

Определение.

Группа G называется циклической, если $G = \langle g \rangle$ для некоторого $g \in G$

Пример.

$(\mathbb{Z}, +) = \langle 1 \rangle$

Замечание.

G циклична $\Leftrightarrow$ G – коммутативна и $\leqslant$ счётна

1.11 Левые смежные классы группы по подгруппе, разбиение группы на левые смежные классы

Пусть G – группа, $H \subseteq G$ – подгруппа

Отношение L_H на G:
$(a, b) \in L_H \Leftrightarrow a^{-1}b \in H$

Предложение.

L_H – отношение эквивалентности

Доказательство.

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

$\boxdot$

Замечание.

$a^{-1}b \in H \Leftrightarrow b \in aH \Rightarrow$ класс элемента a это в точности множество aH.

Определение.

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

Лемма.

Если $|H| < \infty$, тогда $\forall a \in G : |aH| = |H|$

Доказательство.

По определению имеем $|aH| \leqslant |H|$
Если $\exists h_1, h_2 \in H : ah_1 = ah_2$, то, домножим на a^{-1} слева, получим $h_1 = h_2$. Итого $|aH| = |H|$

$\boxdot$

2 Лекция №2

Лекция 14.04.20

2.1 Индекс подгруппы, теорема Лагранжа

Определение.

Индекс подгруппы H – это число левых смежных классов G по H
Обозначение: $[G; H]$

Теорема.

Если $|G| < \infty$, $H \subseteq G$ – подгруппа $\Rightarrow |G| = |H| \cdot [G; H]$

Доказательство.

Так как вся группа G разбивается на попарно не пересекающиеся смежные классы, а в каждом смежном классе ровно $|H|$ элементов $\Rightarrow |G| = |H| \cdot [G; H]$

$\boxdot$

2.2 Пять следствий из теоремы Лагранжа

Следствие.

1. $|G| < \infty$, $H \subseteq G$ – подгруппа $\Rightarrow |G| \vdots |H|$
2. $|G| < \infty$, $g \in G \Rightarrow |G| \vdots \operatorname{ord}(g)$

   Так как $\operatorname{ord} g = |\langle g \rangle|$, а $\langle g \rangle$ является подгруппой в $G \Rightarrow |G| \vdots \operatorname{ord} g$
3. $|G| < \infty \Rightarrow \forall g \in G : g^{|G|} = e$

   $|G| \vdots \operatorname{ord} g \Leftrightarrow |G| = \operatorname{ord} g \cdot s \Rightarrow \left(g^{\operatorname{ord} g}\right)^s = e^s = e$
4. (малая теорема Ферма) $p \in \mathbb{N}$ – простое число, $\bar{a} \in \mathbb{Z}_p \setminus \{0\} \Rightarrow \bar{a}^{p-1} = \bar{1}$
   В группе вычетов по модулю простого числа каждый элемент обратим $\Rightarrow |G| = p - 1 \Rightarrow \forall \bar{a} \in G : \bar{a}^{|G|} = \bar{a}^{p-1} = \bar{1}$
5. Если $|G| = p$, где p – простое $\Rightarrow G$ – циклическая группа, причём $\forall g \in G \setminus \{e\} : |G| = \langle g \rangle$

   Пусть $g \in G \setminus \{e\} \Rightarrow |G| \vdots |\langle g \rangle|$. Так как $g \neq e$, то $|\langle g \rangle| = \operatorname{ord}(g) > 1$. Но так как $|G|$ – простое число $\Rightarrow \operatorname{ord}(g) = p \Rightarrow |\langle g \rangle| = |G| \Rightarrow \langle g \rangle = G$

2.3 Нормальные подгруппы

Определение.

Отношение R_H на G: $(a, b) \in R_H \Leftrightarrow ba^{-1} \in H$ – это тоже отношение эквивалентности

Определение.

Подгруппа $H \subseteq G$ называется нормальной, если $\forall g \in G : gH = Hg$
Обозначение: $H \triangleleft G$

2.3.1 Примеры

1. G – коммутативна $\Rightarrow \forall H \subseteq G$ нормальна
2. $G = S_3$, $H = \{\mathrm{id}, (1\ 2)\} \Rightarrow H$ – не нормальная подгруппа
3. $H = \{e\}$ или $H = G \Rightarrow H \triangleleft G$

Предложение.

Следующие условия эквиваленты:

1. $H \triangleleft G$
2. $\forall g \in G : gHg^{-1} = H$
3. $\forall g \in G : gHg^{-1} \subseteq H$

Доказательство.

1. $\to$ 2. $gH = Hg \Rightarrow$ умножая на g^{-1} справа, получаем $gHg^{-1} = H$
2. $\to$ 3. тривиально
3. $\to$ 1. $gHg^{-1} \subseteq H \Rightarrow$ домножая на g^{-1} справа, получаем $gH \subseteq Hg$. Так как 3. верно $\forall g \in G$, то верно и для $g^{-1} : g^{-1}Hg \subseteq H \Rightarrow$ умножая на g слева получаем $Hg \subseteq gH \Rightarrow$. Итого $gH = Hg$

$\boxdot$

2.4 Факторгруппа группы по нормальной подгруппе

Определение.

$H \triangleleft G \rightsquigarrow {}^{G}\!/_{H}$ – множество $\underset{\text{=правых}}{\text{левых}}$ смежных классов G по H

Определим на ${}^{G}\!/_{H}$ бинарную операцию, полагая

$$(g_1H) \cdot (g_2H) = (g_1g_2)H$$

Корректность:

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

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

$\left({}^{G}\!/_{H}, \circ\right)$:

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

Итог: $\left({}^{G}\!/_{H}, \circ\right)$ является группой

Определение.

$\left({}^{G}\!/_{H}, \circ\right)$ называется факторгруппой группы G по нормальной подгруппе H

Пример.

$G = (\mathbb{Z}, +)$, $H = n\mathbb{Z}$, $n \in \mathbb{N} \Rightarrow {}^{G}\!/_{H} = (\mathbb{Z}_n, +)$

2.5 Гомоморфизмы групп, простейшие свойства

G, F – группы

Определение.

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

Свойства.

$\varphi : G \to F$ – гомоморфизм $\Rightarrow$

1. $\varphi(e_G) = e_F$
   $\varphi(e_G) = \varphi(e_G \cdot e_G) = \varphi(e_G) \cdot \varphi(e_G) \Rightarrow e_F = \varphi(e_G)$
2. $\varphi(g^{-1}) = (\varphi(g))^{-1}$
   $\varphi(g^{-1}) \cdot \varphi(g) = \varphi(g^{-1}g) = \varphi(e_G) = e_F$
   $\varphi(g) \cdot \varphi(g^{-1}) = \varphi(gg^{-1}) = e_F$

2.6 Изоморфизм групп, изоморфные группы

Определение.

Гомоморфизм $\varphi : G \to F$ называется изоморфизмом, если φ является биекцией

Определение.

Группа G и F называются изоморфными, если $\exists$ изоморфизм $\varphi : G \to F$
Обозначение: $G \simeq F$, $G \cong F$, $\varphi : G \xrightarrow{\sim} F$

Пример.

$G = (\mathbb{R}, +)$, $F = (\mathbb{R}_{>0}, \times)$, $\varphi : G \to F : x \mapsto e^x$
φ – гомоморфизм, биективен $\Rightarrow \varphi$ – изоморфизм

2.7 Ядро и образ гомоморфизма групп

$\varphi : G \to F$ – гомоморфизм групп

Определение.

Ядро $\ker\varphi := \{g \in G \mid \varphi(g) = e_F\} \subseteq G$
Образ $\operatorname{Im}\varphi := \varphi(G) \subseteq F$

Лемма.

$\ker\varphi \triangleleft G$

Доказательство.

Покажем, что $g(\ker\varphi)g^{-1} \subseteq \ker\varphi$
$x \in \ker\varphi$, $g \in G$: $\varphi(gxg^{-1}) = \varphi(g) \cdot \underset{e_F}{\varphi(x)} \cdot \varphi(g^{-1} = \varphi(g) \cdot \varphi(g^{-1}) = e_F$

$\boxdot$

$\ker\varphi \triangleleft G \Rightarrow$ определена $G/_{\ker\varphi}$

2.8 Теорема о гомоморфизме для групп

Пусть $\varphi : G \to F$ – гомоморфизм групп

Теорема.

$G/_{\ker\varphi} \simeq \operatorname{Im}\varphi$

Доказательство.

Рассмотрим отображение $\psi : G/_{\ker\varphi} \to \operatorname{Im}\varphi : \psi(g\ker\varphi) := \varphi(g)\ \forall g$

1. корректность:
   $g\ker\varphi = g'\ker\varphi$, то $g' = g \cdot h$ для некоторого $h \in \ker\varphi$
   $\psi(g'\ker\varphi) = \varphi(g') = \varphi(gh) = \varphi(g) \cdot \underset{e_F}{\varphi(h)} = \varphi(g) = \psi(g'\ker\varphi)$

2. ψ – гомоморфизм
   $\psi(g_1 \ker\varphi \cdot g_2 \ker\varphi) = \psi(g_1 g_2 \cdot \ker\varphi) = \varphi(g_1 g_2) = \varphi(g_1) \cdot \varphi(g_2) = \psi(g_1 \ker\varphi) \cdot \psi(g_2 \ker\varphi)$

3. сюръективность: любой элемент из образа представим в виде $\varphi(g) \Rightarrow g$ представим в виде $g \ker\varphi \Rightarrow \varphi(g)$ представим в виде $\psi(g \ker\varphi)$

4. инъективность: если $\psi(g_1 \ker\varphi) = \psi(g_2 \ker\varphi)$, тогда $\varphi(g_1) = \varphi(g_2)$
   $\Rightarrow e_F = \varphi(g_1)^{-1} \cdot \varphi(g_2) = \varphi(g_1^{-1} g_2) \Rightarrow g_1^{-1} g_2 \in \ker\varphi \Rightarrow g_2 \ker\varphi = g_1 \ker\varphi$

$\boxdot$

3 Лекция №3

Лекция 21.04.20

3.1 Классификация циклических групп с точностью до изоморфизма

Предложение.

Пусть G – циклическая группа. Тогда:
(а) если $|G| = \infty$, то $G \simeq (\mathbb{Z}, +)$
(б) если $|G| = n$, то $G \simeq (\mathbb{Z}_n, +)$

Доказательство.

Пусть $G = \langle g \rangle$. Рассмотрим отображение $\varphi : \mathbb{Z} \to G : k \mapsto g^k$.
Тогда φ – это гомоморфизм:

$$\varphi\left(k + l\right) = g^{k+l} = g^k \cdot g^l = \varphi\left(k\right) \cdot \varphi\left(l\right)$$

φ – сюръективен $\Rightarrow \operatorname{Im}\varphi = G \Rightarrow G \simeq \mathbb{Z}/\ker\varphi$
Так как $\ker\varphi$ – это подгруппа в $\mathbb{Z}$, то $\ker\varphi = m\mathbb{Z}$ для некоторого $m \geqslant 0$.
Если $m = 0$, то $\ker\varphi = \{0\} \Rightarrow G \simeq \mathbb{Z}/\{0\} \simeq \mathbb{Z}$.
Если $m > 0$, то $G \simeq \mathbb{Z}/m\mathbb{Z} \simeq \mathbb{Z}_m$.

$\boxdot$

3.2 Прямое произведение групп и разложение группы в прямое произведение подгрупп

Пусть $G_1, \ldots, G_m$ – группы

Определение.

Прямое произведение групп $G_1, \ldots, G_m$ – это множество $G_1 \times \ldots \times G_m$ с бинарной операцией

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

1. ассоциативность: очевидна

2. нейтральный элемент: $(e_{G_1}, \ldots, e_{G_m})$

3. обратный к $(g_1, \ldots, g_m)$ элемент: $\left(g_1^{-1}, \ldots, g_m^{-1}\right)$

$\Rightarrow G_1 \times \ldots \times G_m$ – группа

Пример.

1. $\mathbb{R}^n = \underbrace{\mathbb{R} \times \ldots \times \mathbb{R}}_{n}$

2. $\mathbb{Z}^n = \underbrace{\mathbb{Z} \times \ldots \times \mathbb{Z}}$ – подгруппа в $\mathbb{R}^n$, состоящая из вектором с целыми координатами: "решётка ранга n"

Замечание.

1. $G_1 \times \ldots \times G_m$ абелева $\Leftrightarrow G_i$ – абелевы
2. Если все G_i конечны, то $|G_1 \times \ldots \times G_m| = |G_1| \times \ldots \times |G_m|$
3. $\forall i = 1, \ldots m$: G_i отождествляется с подгруппой

$$\left\{ \left(e_{G_1}, \ldots, e_{G_{i-1}}, g, e_{G_{i+1}}, \ldots, e_{G_m} \right) \mid g \in G_i \right\}$$

Пусть $H_1, \ldots, H_m \subseteq G$ – набор подгрупп

Определение.

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

3.3 Разложение конечной циклической группы

Теорема.

Пусть $n, m, l \in \mathbb{N}$, $n = m \cdot l$, $\gcd(m, l) = 1 \Rightarrow \mathbb{Z}_n \simeq \mathbb{Z}_m \times \mathbb{Z}_l$

Доказательство.

Рассмотрим отображение $\varphi : \mathbb{Z}_n \to \mathbb{Z}_m \times \mathbb{Z}_l : \varphi(a \mod n) = (a \mod n, a \mod l)$

1. корректность: следует из того, что $n \,\vdots\, m$ и $n \,\vdots\, l$
2. φ – гомоморфизм:

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

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

3. φ – инъективен: достаточно проверить, что $\ker \varphi = \{\bar{0}\}$

$$\varphi(a \mod n) = (0, 0) \Rightarrow a \,\vdots\, m,\ a \,\vdots\, l, \text{ но } \gcd(m, l) = 1 \Rightarrow a \,\vdots\, \underset{n}{ml} \Rightarrow a \equiv 0 \mod n$$

4. φ – сюръективен: $|\mathbb{Z}_n| = n = ml = |\mathbb{Z}_m \times \mathbb{Z}_l| \Rightarrow$ инъективное отображения между двумя равномощными множествами биективно

$\boxdot$

Следствие.

$n \in \mathbb{N}, n \geqslant 2, n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ – разложение на простые множители

$$\Rightarrow \mathbb{Z}_n \simeq \mathbb{Z}_{p_1^{k_1}} \times \ldots \times \mathbb{Z}_{p_s^{k_s}}$$

3.4 Примарные абелевы группы

Определение.

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

3.5 Теорема о разложении конечной абелевой группы в прямое произведение примарных циклических групп (формулировка)

Теорема.

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

3.6 Экспонента конечной абелевой группы, критерий цикличности

Определение.

Экспонента группы A – это число

$$\exp A := \min \left\{ n \in \mathbb{N} \;\middle|\; na = 0 \right\} = \operatorname{lcm} \left\{ \operatorname{ord}(a) \;\middle|\; a \in A \right\}$$

Замечание.

Так как $\forall a \in A : |A| \vdots \operatorname{ord}(a)$, то порядок группы является общим кратным всех $\operatorname{ord}(a)$ $\Rightarrow |A| \vdots \exp A \Rightarrow \exp A \leqslant |A|$.

Предложение.

$\exp A = |A| \Leftrightarrow A$ – циклическая группа

Доказательство.

Пусть $|A| = n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s}$ – разложение на простые множители

$\Leftarrow$: $A = \langle a \rangle \Rightarrow \operatorname{ord}(a) = n \Rightarrow \exp A = n$
$\Rightarrow$: $\exp A = n$. $\operatorname{lcm} = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} \Rightarrow$ чтобы его получить $\forall i = 1, \ldots, s : \exists c_i : \operatorname{ord}(c_i) = p_i^{k_i} \cdot \underset{\in \mathbb{N}}{m_i}$
Положим $a_i = m_i \cdot c_i$, тогда $\operatorname{ord}(a_i) = p_i^{k_i}$
Пусть $a = a_1 + \ldots + a_s$
Пусть $ma = 0$ для некоторого $m \in \mathbb{N} \Rightarrow ma_1 + \ldots + ma_s = 0$ $(\star)$
При фиксированном i умножим $(\star)$ на $n_i = {}^{n}\!/_{p_i^{k_i}}$
Тогда $\forall j \neq i : n_i m \vdots p_j^{k_j} \Rightarrow n_i m a_j = 0 \Rightarrow n_i m a_i \Rightarrow n_i m \vdots p_i^{k_i}$, но $n_i \not\vdots\, p_i \Rightarrow m \vdots p_i^{k_i}$
Так как i – произвольное $\Rightarrow m \vdots n$, но $na = 0$ (так как $n = |A|$) $\Rightarrow \operatorname{ord}(a) = n$
Получается $A = \langle a \rangle \Rightarrow A$ – циклическая группа

$\boxdot$

4 Лекция №4

Лекция 26.04.20

4.1 Понятие кольца

Определение.

Кольцо – это множество R, на котором заданы две бинарные операции $"+"$ (сложение) и $"\cdot"$ (умножение), удовлетворяющие следующим условиям:

1. $(\mathbb{R}, +)$ – абелева группа (аддитивная группа кольца R)

2. $\forall a, b, c \in R$:
$$a \cdot (b + c) = ab + ac \quad \text{(левая дистрибутивность)}$$
$$(a + b) \cdot c = ac + bc \quad \text{(правая дистрибутивность)}$$
3. $\forall a, b, c \in R : (ab)c = a(bc)$ (ассоциативность умножения)
4. $\exists 1 \in R$ такой, что $\forall a \in R : a \cdot 1 = 1 \cdot a = a$ (единица)

Пример.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$
2. $\mathbb{Z}_n$ – кольцо вычетов
3. $\mathrm{Mat}_{n\times n}(\mathbb{R})$ – кольцо матриц
4. $\mathbb{R}[x]$ – кольцо многочленов от одной переменной x с коэффициентами из $\mathbb{R}$
5. $\mathcal{F}(M, \mathbb{R})$ – кольцо функций из множества M в $\mathbb{R}$ (с поточечными операциями сложения и умножения):
$$(f_1 + f_2)(m) := f_1(m) = f_2(m), \ \ (f_1 \cdot f_2)(m) := f_1(m) \cdot f_2(m)$$

4.2 Коммутативные кольца

Определение.

Кольцо R называется коммутативным, если $\forall a, b \in R : a \cdot b = b \cdot a$

4.3 Обратимые элементы, делители нуля, нильпотенты

Определение.

Элемент $a \in R$ называется обратимым, если $\exists b \in R$ такой, что $a \cdot b = b \cdot a = 1$. Обозначается a^{-1}

Замечание.

Все обратимые элементы в R образуют группу по умножению

Определение.

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

Замечание.

Если R коммутативно, то { левые делители нуля } = { правые делители нуля } $\Rightarrow$ называются просто делителями нуля

Замечание.

Все делители нуля необратимы: пусть $a, b \neq 0$ и $ab = 0$. Если $\exists a^{-1}$, то домножим слева на a^{-1}, получим $b = 0$ – противоречие

Определение.

Элемент $a \in R$ называется нильпотентом, если $a \neq 0$ и $\exists n \in \mathbb{N}$ такой, что $a^n = 0$

Замечание.

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

4.4 Поля

Определение.

Кольцо R называется полем, если оно коммутативно (ассоциативно с 1), $0 \neq 1$ и $\forall$ ненулевой элемент обратим

Замечание.

В поле нет делителей нуля

4.5 Критерий того, что кольцо вычетов является полем

Предложение.

Кольцо $\mathbb{Z}_n$ является полем $\Leftrightarrow$ n – простое число

Доказательство.

Согласование: $a \in \mathbb{Z} \rightsquigarrow \bar{a} \in \mathbb{Z}_n$ – вычет $a \mod n$

$\Rightarrow$: если $n = 1$, то $Z_n = \{0\}$ – не поле

если $n > 1$ и $n = m \cdot k$, где $1 < m, k < n$, то $\bar{m} \cdot \bar{k} = \bar{0} \Rightarrow$ в $\mathbb{Z}_n$ есть делители нуля $\Rightarrow \mathbb{Z}_n$ – не поле

$\Leftarrow$: Пусть $n = p$ – простое число, $a \in \mathbb{Z}_p \setminus \{0\}$

Тогда $\gcd(a, p) = 1 \Rightarrow \exists k, l \in \mathbb{Z}$ такие, что $ak + pl = 1 \Rightarrow \bar{a} \cdot \bar{k} + \bar{p} \cdot \bar{l} = \bar{1} \Rightarrow \bar{a} \cdot \bar{k} = \bar{1} \Rightarrow a$ – обратим

$\boxdot$

4.6 Подкольца, подполя, гомоморфизмы, изоморфизмы

Пусть R – кольцо

Определение.

Подмножество $S \subseteq R$ называется подкольцом , если $\forall a, b \in S : a + b \in S,\ ab \in S$ и S само является кольцом относительно этих операций

Определение.

Подполе в R – это подкольцо, являющиеся полем

Определение.

Пусть R и S – два кольца, тогда отображение $\varphi : R \to S$ называется гомоморфизмом (колец), если $\forall a, b \in R : \varphi(a + b) = \varphi(a) + \varphi(b),\ \varphi(ab) = \varphi(a) \cdot \varphi(b)$

Изоморфизм – это биективный гомоморфизм

4.7 Идеалы в кольце

Пусть R – кольцо

Определение.

Подкольцо $I \subseteq R$ называется (двусторонним) идеалом, если

(1): I – подгруппа по сложению

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

Обозначение: $I \lhd R$

4.8 Главные идеалы и идеалы, порождённые подмножеством коммутативного кольца

Пусть R – коммутативное кольцо, $a \in R$

Определение.

Множество $(a) := \{ra \mid r \in R\}$ называется главным идеалом, порожденным элементом a

Замечание.

(1): $(a) = R \Leftrightarrow a$ – обратим
(2): $(a) = \{0\} \Leftrightarrow a = 0$

Определение.

$S \subseteq R$ – подмножество $\Rightarrow$

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

называется идеалом, порожденным подмножеством S

4.9 Факторкольцо кольца по идеалу

Пусть R – кольцо, $I \triangleleft R$

Рассмотрим факторгруппу $({}^{R}\!/_{I}, +)$ и введём на ней операцию умножения, полагая $(a+I)(b+I) := ab + I$

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

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

4.10 Ядро и образ гомоморфизма колец

Пусть $\varphi : R \to R'$ – гомоморфизм колец

Определение.

$\ker \varphi := \{r \in R \mid \varphi(r) = 0\} \triangleleft R$
$\operatorname{Im} \varphi := \varphi(R) \subseteq R'$

4.11 Теорема о гомоморфизме для колец

Теорема.

${}^{R}\!/_{\ker \varphi} \simeq \operatorname{Im} \varphi$

Доказательство.

Пусть $I := \ker \varphi$, тогда из доказательства теоремы о гомоморфизме для групп отображение $\psi : {}^{R}\!/_{I} \to \operatorname{Im} \varphi$, где $\psi(a + I) = \varphi(a)$ является изоморфизмом групп по сложению

Остаётся показать, что ψ – гомоморфизм колец

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

$\boxdot$

5 Лекция №5

Лекция 28.04.2020

5.1 Кольцо $K[x]$ многочленов от одной переменной над полем

Пусть K – поле, $K[x]$ – кольцо многочленов от x с коэффициентами из k

$$K[x] = \left\{a_nx^n + \ldots + a_1x + a_0 \,\middle|\, n \geqslant 0,\ a_i \in K\right\}$$

$\forall f \in K[x]$ 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 $K[x]$: $\left\{f \,\middle|\, \deg f = 0\right\}$
Делители нуля в $K[x]$: их нет

5.2 Деление с остатком

Пусть K – поле

Теорема.

Для любых двух многочленов $f, g \in K[x]$, $g \neq 0$, существует единственные многочлены $q, r \in K[x]$, для которых $f = q \cdot g + r$ и либо $r = 0$, либо $\deg r < \deg g$

Доказательство.

Существование: индукция по $\deg f$

Если $f = 0$, то можно брать $q = r = 0$. Теперь считаем, что $\deg f = n \geqslant 0$

Пусть $f = a_nx^n + \ldots + a_1x + a_0$ ($a_n \neq 0$), $g = b_mx^m + \ldots + b_1x + b_0$ ($b_m \neq 0$). Если $\deg f < \deg g \Rightarrow$ достаточно взять $q = 0, r = f$

Иначе, положим $h = f - {}^{a_n}\!/_{b_m} x^{n-m} \cdot g$, тогда $\deg h < \deg f$

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

Единственность: Пусть $f = q_1 \cdot g + r_1 = q_2 \cdot g + r_2$ – два представления многочлена f. Тогда $(q_1 - q_2) \cdot g = r_2 - r_1$. Пусть $q_1 \neq q_2$, тогда $\deg{(q_1 - q_2) \cdot g} \geqslant \deg g > \deg{(r_2 - r_1)}$ – противоречие $\Rightarrow q_1 = q_2 \Rightarrow r_1 = r_2$

$\boxdot$

5.3 Наибольший общий делитель двух многочленов, теорема о его существовании и линейном выражении

Определение.

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.

Наибольший общий делитель многочленов $f, g \in K[x]$ – это такой многочлен $h \in K[x]$, что
(1) h делит оба f и g
(2) h имеет максимальную возможную степень

Теорема.

Пусть $f, g \in K[x]$ и $(f, g) \neq (0, 0)$, тогда
(1) $\exists \gcd(f, g) =: h$
(2) $\exists u, v \in K[x]$ такие, что $h = uf + vg$

Доказательство.

(1) прямой ход алгоритма Евклида (деление одного на другого)

(2) обратный ход алгоритма Евклида (расширенный алгоритм Евклида)

$\boxdot$

Замечание.

$\gcd(f, g)$ определён с точностью до пропорциональности

5.4 Теорема о том, что $K[x]$ является кольцом главных идеалов

Определение.

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

Предложение.

$K[x]$ – КГИ

Доказательство.

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

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

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 $r = \underset{\in I}{f} - q \cdot \underset{\in I}{g} \in I$. Так как $\deg g$ – наименьший $\Rightarrow r = 0 \Rightarrow f \in (g) \Rightarrow I \subseteq (g)$.

$\boxdot$

5.5 Неприводимые многочлены

Определение.

Многочлен $h \in K[x], \deg h > 0$ называется неприводимым, если его нельзя представить в виде $h = h_1 \cdot h_2$, где $\deg h_1, \deg h_2 < \deg h$. Иначе h называется приводимым

Замечание.

(1) $h \in K[x]$, $\deg h = 1 \Rightarrow$ h неприводим (множители не могут быть степени 0, так как $\deg h_1 + \deg h_2 = \deg h$)

(2) $h \in K[x]$, $\deg h \geqslant 2$, h – неприводим $\Rightarrow h$ не имеет корней в K (по теореме Безу, в обратную сторону неверно: можно взять два неприводимых многочлена, перемножить и получить приводимый многочлен)

(3) $h \in K[x]$, $\deg h = \{1, 2\} \Rightarrow h$ – неприводим $\Leftrightarrow h$ не имеет корней в K

Лемма.

Если $h \in K[x]$ – неприводимый многочлен, 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 $\gcd(g_1, h) = 1 \Rightarrow \exists u, v \in K[x]$ такие, что $1 = ug_1 + vh$. Умножим на g_2: $g_2 = \underset{\vdots h}{ug_1g_2} + \underset{\vdots h}{vhg_2} \Rightarrow r_2 \vdots h$

Для $k > 2$ применяем предыдущее рассуждение для $(g_1 \cdot \ldots \cdot g_{k_1}) \cdot g_k$. Если $g_k \vdots h$ – всё ОК, иначе $\exists i \in \{1, \ldots, k-1\}$: $g_i \vdots h$ по предположению индукции

$\boxdot$

5.6 Факториальность кольца $K[x]$

Теорема.

Пусть $f \in K[x]$ и $\deg f \geqslant 1$, тогда

(1) $\exists$ разложение $f = h_1 \cdot \ldots \cdot h_k$, где h_i – неприводимы

(2) это разложение единственно, с точностью до перестановки множителей и пропорциональности

Доказательство.

Пусть $\deg f = n$. Индукция по n:

$n = 1 \Rightarrow f$ – неприводим, единственность есть

$n > 1$:

Существование: если f – неприводим, то он и есть разложение. Если f приводим, то $f = f_1 \cdot f_2$, $\deg f_1, \deg f_2 < n \Rightarrow$ 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 – неприводимые. Тогда $f = g_1 \cdot \ldots \cdot g_p \cdot h_1 \cdot \ldots \cdot h_q$ – разложение f

Единственность: Пусть $f = h_1 \cdot \ldots \cdot h_k = h'_1 \cdot \ldots \cdot h'_m$ – два разложения на неприводимые множители. h_1 делит $h'_1 \cdot \ldots \cdot h'_m \Rightarrow$ по лемме $\exists i$ такой, что h делит h'_i. Переставив множители, будем считать, что h_1 делит h'_1. Так как h_1 и h'_1 неприводимые, то $h_1 = \varepsilon \cdot h_2$, где $\varepsilon \in K \setminus \{0\}$. Так как в $K[x]$ нет делителей нуля, то можем сократить на h_1, получим $h_2 \cdot \ldots \cdot h_k = \varepsilon \cdot h'_2 \cdot \ldots \cdot h'_m$. Так как мы понизили степень $\Rightarrow$ по предположению индукции они пропорциональны и равны $\Rightarrow$ при добавлении h_1 они такими остаются.

$\boxdot$

Замечание.

(1) всякое КГИ факториальна

(2) $K[x_1, \ldots, x_n]$, где $n \geqslant 2$ – это не КГИ, но тоже факториальна

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

Пусть $h = a_n x^n + \ldots + a_1 x + a_0 \in K[x]$, $\deg h = n > 0$

Рассмотрим факторкольцо $K[x]/(h)$, $f \in K[x] \rightsquigarrow \bar{f} := f + (h) \in F$

Предложение.

F – поле $\Leftrightarrow$ h – неприводим

Доказательство.

$\Rightarrow$: если $h = h_1 \cdot h_2$, $\deg h_i < n \Rightarrow \bar{h} = \bar{h}_1 \cdot \bar{h}_2$. Так как $\bar{h} = 0$, то $\bar{h}_1 \cdot \bar{h}_2 = 0 \Rightarrow$ в F есть делители нуля (так как h_1, h_2 ненулевые) $\Rightarrow$ противоречие

$\Leftarrow$: пусть $f \in K[x]$, $\bar{f} \neq \bar{0} \Rightarrow f \not\vdots\, h \Rightarrow \gcd(f, h) = 1 \Rightarrow \exists u, v \in K[x]$ такие, что $1 = uf + vh \Rightarrow \bar{1} = \bar{u}\bar{f} + \bar{v}\underbrace{\bar{h}}_{=\bar{0}} = \bar{u}\bar{f} \Rightarrow \bar{f}$ – обратим $\Rightarrow F$ – поле

$\boxdot$

5.8 Базис факторкольца $K[x]/(h)$ как векторного пространства над полем K

Рассмотрим отображение $K \to F$, $\alpha \mapsto \overline{\alpha} = \alpha + (h)$, оно инъективно $\Rightarrow K$ является подполем в $F \Rightarrow F$ становится векторным пространством над K

Предложение.

Элементы $\bar{1}, \bar{x}, \ldots, \bar{x}^{n-1}$ – образуют базис в F над K. В частности, $\dim_K F = n$

Доказательство.

$\bar{f} \in F$, $f \in K[x]$. Поделим f на h с остатком:

$$f = q \cdot h + r \Rightarrow \bar{f} = \bar{q} \cdot \underbrace{\bar{h}}_{=\bar{0}} + \bar{r} = \bar{r} \in \langle \bar{1}, \bar{x}, \ldots, \bar{x}^{n-1} \rangle$$

Если $b_0\bar{1} + \ldots + b_{n-1}\bar{x}^{n-1} = 0$ для некоторых $b_i \in K$, то $b_0 + \ldots + b_{n-1}x^{n-1} \vdots h \Rightarrow b_0 = \ldots = b_{n-1} = 0$.

$\boxdot$

6 Лекция №6

Лекция 13.05.2020

K – поле, $R = K[x_1, \ldots, x_n]$
$M = \left\{ ax_1^{k_1} \cdot \ldots \cdot x_n k_n \;\middle|\; a \in K \setminus \{0\},\ k_i \geqslant 0 \right\}$ – все одночлены от $x_1, \ldots, x_n$.

6.1 Лексикографический порядок на одночленах от нескольких переменных

Определение.

$ax_1^{i_1} \cdot \ldots \cdot x_n^{i_n} \succ bx_1^{j_1} \cdot \ldots \cdot x_n^{j_n} \Leftrightarrow \exists k : i_1 = j_1, i_2 = j_2, \ldots, i_{k-1} = j_{k-1}, i_k > j_k$

Замечание.

(1) $m_1, m_2, m_3 \in M, m_1 \prec m_2 \Rightarrow m_1 \cdot m_3 \prec m_2 \cdot m_3$
(2) $m_1, m_2, m_3 \in M, m_1 \prec m_2, m_2 \prec m_3 \Rightarrow m_1 \prec m_3$

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

6.2 Лемма о конечности убывающих цепочек одночленов

Лемма.

Не существует бесконечных убывающих цепочек

$$m_1 \succ m_2 \succ m_3 \succ \ldots,\ \text{где } \forall i \in \mathbb{N} : m_i \in M$$

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:
$k_1(1) \geqslant k_1(2) \geqslant k_1(3) \geqslant \ldots \Rightarrow \exists i_1 \in \mathbb{N} : \forall i \geqslant i_1 : k_1(i) = k_1(i_1)$
$k_2(i_1) \geqslant k_2(i_1 + 1) \geqslant k_2(i_2 + 2) \geqslant \ldots \Rightarrow \exists i_2 \geqslant i_1 \in \mathbb{N} : \forall i \geqslant i_2 : k_2(i) = k_2(i_2)$
и так далее $\exists i_n \geqslant i_{n-1} : \forall i \geqslant i_n : k_n(i) = k_n(i_n)$
Итого: при $i \geqslant i_n$ все m_i имеют одинаковые наборы степеней $\Rightarrow$ противоречие.

6.3 Старший член ненулевого многочлена

Определение.

$f \in R \setminus \{0\} \Rightarrow$ старший член $L(f)$ – это наибольший в лексикографическом порядке одночлен, присутствующий в f.

6.4 Лемма о старшем члене

Лемма.

Пусть $f, g \in R \setminus \{0\} \Rightarrow L(fg) = L(f) \cdot L(g)$.

Доказательство.

Пусть $u \in M(f), v \in M(g) \Rightarrow u \preceq L(f), v \preceq L(g)$.

$$uv \preceq L(f) \cdot v \preceq L(f) \cdot L(g) \Rightarrow uv \preceq L(f) \cdot L(g)$$

Причём '=' $\Leftrightarrow u = L(f)$ и $v = L(g)$.
$\Rightarrow L(f) \cdot L(g)$ больше любого другого одночлена в $fg \Rightarrow L(f) \cdot L(g) = L(fg)$.

$\boxdot$

6.5 Элементарная редукция многочлена относительно ненулевого многочлена

Пусть $g, f \in R \setminus \{0\}$, g содержит одночлен m такой, что $m \,\vdots\, L(f) \Rightarrow m = L(f) \cdot m'$, 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.

g редуцируется к g' при помощи F, если $\exists$ конечная цепочка элементарных редукций

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

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

g нередуцируем относительно F, если $\forall m \in M(g)$ и $\forall f \in F$: $m \not\vdots\, L(f)$

6.6 Лемма о конечности цепочек элементарных редукций

Лемма.

Пусть $F \subseteq R \setminus \{0\} \Rightarrow$ всякая последовательность элементарных редукций относительно F за конечное число шагов приводит к нередуцироемому многочлену.

Доказательство.

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

От противного: пусть существует бесконечная цепочка элементарных редукций

$$g \xrightarrow{f_1} g_1 \xrightarrow{f_2} g_2 \xrightarrow{f_3} \ldots$$

В силу леммы 1 имеем:
$L(g_1) \succeq L(g_2) \succeq L(g_3) \succeq \ldots \Rightarrow \exists i_1 : \forall i \geqslant i_1 : L(g_i) = L(g_{i_1})$
$L_2(g_{i_1}) \succeq L_2(g_{i_1+1}) \succeq L_3(g_{i_1+2}) \succeq \ldots \Rightarrow \exists i_2 \geqslant i_1 : \forall i \geqslant i_2 : L_2(g_i) = L_2(g_{i_2})$
* и так далее *
Итого: $L(g_{i_1}) = L(g_{i_2}) \succ L_2(g_{i_2}) = L_2(g_{i_3}) \succ L_3(g_{i_3}) = L_3(g_{i_4}) \succ \ldots$
$\Rightarrow L(g_{i_1}) \succ L_2(g_{i_2}) \succ \ldots$ – бесконечная убывающая цепочка одночленов $\Rightarrow$ противоречие.

$\boxdot$

6.7 Остаток многочлена относительно заданной системы многочленов

Определение.

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

Замечание.

Остаток определён неоднозначно.

6.8 Системы Грёбнера

Определение.

Множество F называется системой Грёбнера, если $\forall g \in R$ остаток g относительно F определён однозначно, то есть не зависит от цепочки приводящих к нему элементарных редукций.

6.9 Характеризация систем Грёбнера в терминах цепочек элементарных редукций

Предложение.

Следующие условия эквивалентны:

(1) F – система Грёбнера

(2) $\forall g \in R$ обладает следующим свойством: если $g \xrightarrow{f_1} g_1$ и $g \xrightarrow{f_2} g_2$ – две элементарные редукции, то $\exists g' \in R$ такой, что $g_1 \overset{F}{\rightsquigarrow} g'$ и $g_2 \overset{F}{\rightsquigarrow} g'$.

Доказательство.

Аллах так сказал!

$\boxdot$

6.10 S-многочлены

Пусть $f_1, f_2 \in R$, рассмотрим $m = \operatorname{lcm}(L(f_1), L(f_2))$.
Пусть $m_1, m_2 \in M$ таковы, что $m = m_1 \cdot L(f_1)$ и $m = m_2 \cdot L(f_2)$.

Определение.

Многочлен $S(f_1, f_2) := m_1 f_1 - m_2 f_2$ называется S-многочленом (S-полиномом), построенным по f_1 и f_2.

Замечание.

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

7 Лекция №7

Лекция 19.05.2020

7.1 Критерий Бухбергера

Теорема.

Для системы $F \subseteq R \setminus \{0\}$ следующие условия эквиваленты:

(1) F – система Грёбнера

(2) $\forall f_1, f_2 \in F$: $S(f_1, f_2) \overset{F}{\rightsquigarrow} 0$.

Доказательство.

(1) $\Rightarrow$ (2): положим $m = \operatorname{lcm}(L(f_1), L(f_2)) = m_1 \cdot L(f_1) = m_2 \cdot L(f_2)$.

Тогда

$$m_1 \cdot f_1 \xrightarrow{f_1} m_1 \cdot f_1 - m_1 \cdot f_1 = 0$$

$$m_1 \cdot f_1 \xrightarrow{f_2} m_1 \cdot f_1 - m_2 \cdot f_2 = S(f_1, f_2) \overset{F}{\rightsquigarrow} r_0$$

Поскольку остаток определен однозначно $\Rightarrow S(f_1, f_2) \overset{F}{\rightsquigarrow} 0$.

(2) $\Rightarrow$ (1): пусть $g \in R, m_1, m_2 \in M(g)$ и мы сделали элементарные редукции m_1 при помощи $f_1 \in F$ и m_2 при помощи $f_2 \in F$.

$$m_1 = m_1' \cdot L(f_1), \;\; m_2 = m_2' \cdot L(f_2)$$

$$g \xrightarrow{f_1} g_1 = g - m_1' \cdot f_1$$

$$g \xrightarrow{f_2} g_2 = g - m_2' \cdot f_2$$

Теперь достаточно показать, что $g_1 - g_2 = m_2' \cdot f_2 - m_1' \cdot f_1 \overset{F}{\rightsquigarrow} 0$.

Случай 1: $L(m_2' \cdot f_2)$ и $L(m_1' \cdot f_1)$ не пропорциональны.

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

Случай 2: $L(m_2' \cdot f_2) = L(m_1' \cdot f_1)$. Тогда $\exists m \in M$ такой, что

$$m_2' \cdot f_2 - m_1' \cdot f_1 = m \cdot S(f_1, f_2) \overset{F}{\rightsquigarrow} 0$$

Случай 3: $L(m_2' \cdot f_2) = \alpha \cdot L(m_1' \cdot f_1)$ при $\alpha \neq 1$. Тогда

$$L(m_2' \cdot f_2 - m_1' \cdot f_1) = (\alpha - 1) \cdot L(m_1' \cdot f_1)$$

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

$L(m_2' \cdot f_2) = L(\alpha \cdot m_1' \cdot f_1) \Rightarrow$ попали в случай 2.

$\boxdot$

7.2 Базис Грёбнера идеала, теорема о трёх эквивалентных условиях

Определение.

Множество $F \subseteq R \setminus \{0\}$ называется *базисом Грёбнера* идеала I, если $I = (F)$ и F – система Грёбнера.

Теорема.

Пусть $F \subseteq I \setminus \{0\} \Rightarrow$ следующие условия эквивалентны:

(1) F – базис Грёбнера в I

(2) $\forall g \in I$: $g \overset{F}{\rightsquigarrow} 0$

(3) $\forall g \in I \setminus \{0\}$: $\exists f \in F$: $L(g) \,\vdots\, L(f)$

Доказательство.

(1) $\Rightarrow$ (2): $I_0 = \left\{ g \in I \;\middle|\; g \overset{F}{\rightsquigarrow} 0 \right\} \subseteq I$

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 $g = (g_1 + g_2) - g_2 \overset{F}{\rightsquigarrow} 0 \Rightarrow \exists$ остаток r такой, что

$$\begin{cases} g_1 + g_2 \overset{F}{\rightsquigarrow} r \\ g_2 \overset{F}{\rightsquigarrow} r \end{cases} \Rightarrow g_1 + g_2 \overset{F}{\rightsquigarrow} 0$$

4) $g \in I_0 \Rightarrow \forall m \in R$: $m \cdot g \in I_0$
1) - 3) $\Rightarrow I_0$ – подгруппа по сложению в I
3) - 4) $\Rightarrow I_0$ – идеал в R. $F \subseteq I_0 \Rightarrow I = (F) \subseteq I_0 \Rightarrow I = I_0$
(2) $\Rightarrow$ (1):

$$g \in I \Rightarrow g \overset{F}{\rightsquigarrow} 0 \Rightarrow g = m_1 \cdot f_1 + \ldots + m_k \cdot f_k$$

где $m_1, \ldots, m_k \in M$ и $f_1, \ldots, f_k \in F$.
$\Rightarrow g \in (F) \Rightarrow I \subseteq (F)$. Но $F \subseteq I \Rightarrow I = (F)$.
Пусть $f_1, f_2 \in F \Rightarrow S(f_1, f_2) \in (F) = I \Rightarrow S(f_1, f_2) \overset{F}{\rightsquigarrow} 0 \Rightarrow F$ – система Грёбнера

(2) $\Rightarrow$ (3): $\forall g \in I$: $g \overset{F}{\rightsquigarrow} 0 \Rightarrow$ в соответствующей цепочке элементарных редукций есть одна, примененная к $L(g) \Rightarrow \exists f \in F$: $L(g) \vdots L(f)$.

(3) $\Rightarrow$ (2): $g \in I$, $g \overset{F}{\rightsquigarrow} r$ – остаток $\Rightarrow$

$$r = \underbrace{g}_{\in I} - \underbrace{m_1 \cdot f_1 - \ldots - m_k \cdot f_k}_{\in I}, \text{ где } m_i \in M, f_i \in F$$

$\Rightarrow r \in I$. Если $r \neq 0 \Rightarrow \exists f \in F$: $L(r) \vdots L(f) \Rightarrow r$ можно редуцировать дальше – противоречие $\Rightarrow r = 0$.

$\boxdot$

7.3 Решение задачи вхождения многочлена в идеал

F – базис Грёбнера в $I \Rightarrow$
(1) $\forall g \in I$ любая цепочка элементарных редукций относительно F приводит к нулю
(2) $\forall g \in R$: $g \in I \Leftrightarrow$ остаток относительно F равен нулю

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

Лемма.

Не существует бесконечная последовательность одночленов $m_1, m_2, \ldots$ такая, что $\forall i > j$: $m_i \not\vdots\, m_j$.

Доказательство.

Индукция по n (число переменных).
$n = 1$: степени убывают $\Rightarrow$ конечна.
Пусть доказано для $< n$, докажем для n.

Пусть есть бесконечная последовательность $m_1, m_2, \ldots$ $m_i \not\vdots\, m_j$ при $i > j$

$$m_i = a_i x_1^{k_1(i)} \cdot \ldots \cdot x_n^{k_n(i)}$$

Тогда $\forall j \geqslant 2$: $m_j \not\vdots\, m_1 \Rightarrow \exists i \in \{1, \ldots, n\}$ такой, что $k_i(j) < k_i(1)$.

$\Rightarrow \exists i \in \{1, \ldots, n\}$ такой, что $k_i(j) < k_i(1)$ для бесконечного числа значений j.

Без ограничений общности считаем, что $i = n$. Перейдя к подпоследовательности можно считать, что $\forall j \geqslant 2$: $k_n(j) < k_n(1)$.

Тогда $k_n(j)$ принимает лишь конечное число значений $\Rightarrow$ какой-то из этих значений встречается бесконечно много раз, значит он не влияет на результат.

Снова перейдя к подпоследовательности, можно считать $k_n(1) = k_n(2) = \ldots$.

Полагая $x_n = 1$, получаем последовательность из $x_1, \ldots, x_{n-1}$ с тем же свойством – противоречие.

$\boxdot$

7.5 Теорема Гильберта о базисе идеала

Теорема.

Всякий идеал в R порождается конечным числом элементов.

Доказательство.

$I \triangleleft R$. Если $I = \{0\} \Rightarrow I = (0)$ – ОК.

$I \neq \{0\}$. Выберем $r_1 \in I \setminus \{0\}$. Если $I = (r_1)$ – 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 $I = (r_1, r_2)$ – ОК, иначе продолжаем процесс.

Если процесс не закончится, то получим бесконечную последовательность $r_1, \ldots$ такую, что $\forall i > j$: $L(r_i) \not\vdots\, L(r_j)$ – противоречие.

$\boxdot$

7.6 Алгоритм Бухбергера построения базиса Грёбнера идеала

Дано: $I = (F)$, где $F = \{f_1, \ldots, f_k\}$.

Перебираем все пары $i < j$. Если $\exists i < j$ такой, что $S(f_i, f_j) \overset{F}{\rightsquigarrow} r_1 \neq 0$, то добавляем r_1 в F и повторяем процедуру для $F \cup \{r_1\}$.

Алгоритм закончится за конечное число шагов $\Rightarrow$ F – система Грёбнера по критерию Бухбергера $\Rightarrow$ F – базис Грёбера в I.

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

Предложение.

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

Доказательство.

Достаточно показать: $\{f_1, f_2\}$ – 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 не так.

Тогда $L(h_1 f_1) = -L(h_2 f_2)$, то есть они сократились.

$L(h_1) = L(f_2) \cdot m$ и $L(h_2) = -L(f_1) \cdot m$, где $m \in M$.

Положим $h_1' = h_1 - f_2 m$ и $h_2' = h_2 + f_1 m$.

Имеем $g = h_1' f_1 + h_2' f_2$ и $L(h_1' f_1) = -L(h_2' f_2)$. Повторяя процедуру, получим бесконечную цепочку равенств, причем $L(h_1) \succ L(h_1') \succ \ldots$ – противоречие.

$\boxdot$

8 Лекция №8

Лекция 27.05.2020

8.1 Поля

Знакомые нам поля: $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{Z}_p$ (p – простое), ${}^{K[x]}\!/_{h}$ (k – поле, h – неприводимый многочлен).

8.2 Характеристика поля

Определение.

Характеристика поля K – это наименьшее $p \in \mathbb{N}$ такое, что $\underbrace{1+1+\ldots+1}_{p} = 0$.

Обозначение: $\operatorname{char} K$

Пример.

$\operatorname{char}\mathbb{Q} = \operatorname{char}\mathbb{R} = \operatorname{char}\mathbb{C} = 0$, $\operatorname{char}\mathbb{Z}_p = p$.

Предложение.

K – поле $\Rightarrow \operatorname{char} K = 0$ или $\operatorname{char} K$ – простое число.

Доказательство.

Пусть $\operatorname{char} K = p$, где $p \geqslant 2$, так как в полях выполнено условие $0 \neq 1$.
Если $p = mk$, где $m, k < p$, то

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

Так как

$$\underbrace{(1+\ldots+1)}_{m} \neq 0 \text{ и } \underbrace{(1+\ldots+1)}_{k} \neq 0$$

$\Rightarrow$ в K есть делители нуля – противоречие $\Rightarrow p$ – простое.

$\boxdot$

8.3 Расширение полей, его степень

Определение.

K, F – поля, $K \subseteq F$ называется расширением поля K ($K \subseteq F$ – расширением полей).

Определение.

Степень расширения полей $K \subseteq F$ – это размерность F как векторного пространства над K. То есть элементы F представляются в виде линейной комбинации элементов с коэффициентами из K.

Обозначение: $[F : K]$.

Пример.

$[\mathbb{C} : \mathbb{R}] = 2$: $\begin{pmatrix} a \\ b \end{pmatrix} \in K \rightsquigarrow a + bi \in F$.

$[\mathbb{R} : \mathbb{Q}] = \infty$ (иррациональные числа, например, не представимы).

Определение.

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

8.4 Степень композиции двух расширений

Лемма.

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

Доказательство.

Пусть $e_1, \dots, e_n$ – базис F над K и $f_1, \dots, f_m$ – базис L над F.
Покажем, что $\{e_i \cdot f_j\}$ – базис L над K.
(1)

$$a \in L \Rightarrow a = \sum_{j=1}^{m} \alpha_j \cdot f_j, \text{ где } \alpha_j \in K : \alpha_j = \sum_{i=n}^{n} \beta_{ij} \cdot e_i, \text{ где } \beta_{ij} \in K$$

$$\Rightarrow a = \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \beta_{ij} \cdot e_i f_j \right) \Rightarrow L = \langle e_i f_j \rangle$$

(2) Если

$$\sum_{j=1}^{m} \sum_{i=1}^{n} \gamma_{ij} \cdot e_i f_j = 0, \text{ где } \gamma_{ij} \in K, \text{ то } \sum_{j=1}^{m} \left(\sum_{i=1}^{n} \gamma_{ij} \cdot e_i \right) f_j = 0$$

$\{f_j\}$ – базис L над $F \Rightarrow$

$$\forall j : \sum_{i=1}^{n} \gamma_{ij} \cdot e_i = 0$$

$\{e_i\}$ – базис F над $K \Rightarrow \forall i, j : \gamma_{ij} = 0$. То есть система $\{e_i f_j\}$ линейно независима.

$\boxdot$

8.5 Присоединение корня неприводимого многочлена

K – поле, $h = \alpha_n x^n + \alpha_{n-1} x^{n-1} + \ldots + \alpha_1 x + \alpha_0 \in K[x]$, $\deg h = n$.
Если h неприводим, то $F := {K[x]}/{(h)}$ – поле, где $K \subseteq F$ и $[F : K] = n$.
Обозначим $\forall f \in K \rightsquigarrow \bar{f} := f + (h) \in F$.

Предложение.

Элемент $\bar{x}$ является корнем многочлена $h \in F$.

Доказательство.

$$h(\bar{x}) = \alpha_n \bar{x}^n + \alpha_{n-1} \bar{x}^{n-1} + \ldots + \alpha_1 \bar{x} + \alpha_0 = \bar{h} = \bar{0} \text{ (в } F)$$

Определение.

Переход от K к F называется присоединением корня неприводимого многочлена h.

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

Следствие.

$\forall f \in K[x]$, $\deg f \geqslant 1$: существует конечное расширение $K \subseteq F$ такое, что f имеет корень в F.

Доказательство.

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

$\boxdot$

<u>*Следствие.*</u>

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

<u>*Доказательство.*</u>

Предыдущее следствие, теорема Безу и индукция по $\deg f$.

$\boxdot$

8.7 Алгебраические и трансцендентные элементы

Пусть $K \subseteq F$ – расширение полей.

<u>*Определение.*</u>

Элементы $\alpha \in F$ называются алгебраическими над k, если $\exists f \in K[x]$, $\deg f \geqslant 1$ такой, что $f(\alpha) = 0$, и трансцендентным иначе.

<u>*Пример.*</u>

$\sqrt{2} \in \mathbb{R} \rightsquigarrow x^2 - 1 \in \mathbb{Q}[x]$, $\sqrt[3]{3} \rightsquigarrow x^3 - 3$.

$i \in \mathbb{C}$ – алгебраический над $\mathbb{Q}$: $x^2 + 1$.

e, π – трансцендентные числа над $\mathbb{Q}$.

8.8 Минимальный многочлен алгебраического элемента и его свойства

<u>*Определение.*</u>

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

<u>*Лемма.*</u>

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

<u>*Доказательство.*</u>

Положим $I := \left\{ f \in K[x] \;\middle|\; f(\alpha) = 0 \right\}$. Тогда I идеал в $K[x]$.

Так как $K[x]$ – кольцо главных идеалов, то $\exists g \in I : I = (g)$.

Тогда $h(\alpha) = 0 \Rightarrow h \in I \Rightarrow h \,\vdots\, g$.

h пропорционален g в силу минимальности $\Rightarrow$ условия (1) и (2).

(3): Если h приводим, значит найдётся многочлен h': $\deg h' < \deg h$ и $h'(\alpha) = 0$ – противоречие.

$\boxdot$

8.9 Поле, порождённое алгебраическим элементом

Пусть $K \subseteq F$, $\alpha \in F$ – элемент, алгебраический над K, h_α – минимальный многочлен для α.

Положим $K(\alpha) :=$ пересечение всех подполей в F, содержащих K и $\alpha =$ наименьшее подполе в F, содержащее K и α.

Замечание.

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

Предложение.

Существует изоморфизм ψ: $K[x]/(h_\alpha) \simeq K(\alpha)$ такой, что $\psi(\bar{x}) = \alpha$.

Доказательство.

Рассмотрим гомоморфизм φ: $K[x] \to F$, $f \mapsto f(\alpha)$.

Тогда $\ker \varphi = (h_\alpha)$ по (2) пункту из леммы $\Rightarrow$ по теореме о гомоморфизме для колец получается изоморфизм

$$\psi : K[x]/(h_\alpha) \simeq \operatorname{Im} \varphi, \text{ где } \psi(\bar{x}) = \varphi(\bar{x}) = \alpha$$

Так как $K[x]/(h_\alpha)$ – поле, то $\operatorname{Im} \varphi$ – подполе в F, $K \in \operatorname{Im} \varphi$, $\alpha = \psi(\bar{x}) \in \operatorname{Im} \varphi \Rightarrow K(\alpha) \subseteq \operatorname{Im} \varphi$.

С другой стороны $\operatorname{Im} \varphi = \left\{ f(\alpha) \mid f \in K[x] \right\}$ – содержится в любом поле, содержащим $\alpha \Rightarrow \operatorname{Im} \varphi \subseteq K(\alpha)$.

$\boxdot$

Следствие.

$\forall y \in K(\alpha)$ единственным образом представим в виде

$$y = \beta_0 + \beta_1 \alpha + \ldots + \beta_{n-1} \alpha^{n-1}, \text{ где } \beta_i \in K$$

8.10 Порядок конечного поля

Пусть K – конечное поле, тогда $\operatorname{char} K = p > 0$ – простое число.

Пусть $\langle 1 \rangle \subseteq K$ – подгруппа по сложению, порожденная 1. Заметим, что $\langle 1 \rangle$ – подкольцо, изоморфное $\mathbb{Z}_p \Rightarrow \langle 1 \rangle$ – поле, изоморфное $\mathbb{Z}_p$.

Далее отождествляем $\langle 1 \rangle$ с $\mathbb{Z}_p$, то есть $\mathbb{Z}_p \in K$.

Теорема.

$|K| = p^n$, где $n = \dim_{\mathbb{Z}_p} K$.

Доказательство.

$\mathbb{Z}_p \subseteq K \Rightarrow K$ векторное пространство над $\mathbb{Z}_p$.

Пусть $n = \dim \mathbb{Z}_p K$. Выберем базис $e_1, \ldots, e_n$ в K над $\mathbb{Z}_p$. Тогда

$$K = \left\{ a_1 e_1 + \ldots + a_n e_n \mid a_i \in \mathbb{Z}_p \right\}$$

Для всех a_i есть ровно p вариантов $\Rightarrow |K| = p^n$.

$\boxdot$

8.11 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 $n \Rightarrow |F| = p^n$.

8.12 Поле из четырёх элементов

$4 = 2^2$ – выбираем неприводимый многочлен степени 2 из поля $\mathbb{Z}_2$.

$$h = x^2 + x + 1 \in \mathbb{Z}_2[x] \Rightarrow F = {}^{\mathbb{Z}_p}\!\diagup_{(h)}$$

F – векторное пространство над $\mathbb{Z}_2$ с базисом $\bar{1}, \bar{x} \Rightarrow$

$$F = \{\bar{0}, \bar{1}, \bar{x}, \bar{x} + \bar{1}\}$$

С операциями $+$: по модулю 2, $\times$: умножить многочлены и понизить степень по правилу $\bar{x}^2 = \bar{x} + \bar{1}$.