



Санкт-Петербургский
государственный
университет
www.spbu.ru

Лекции по алгебре

2 семестр, преподаватель Всемиров М. А.
Записали Костин П.А. и Щукин И.В.¹

¹Данный документ неидеальный, прошу сообщать о найденных недочетах [вконтакте](#) (можно присылать скрины неточностей с указанием билетов)

Содержание

1	Базис векторного пространства. Четыре эквивалентных переформулировки определения базиса.	7
2	Конечномерные пространства. Всякое линейно независимое семейство конечномерного пространства можно дополнить до базиса. Существование базиса конечномерного пространства.	9
3	Всякое семейство образующих конечномерного пространства содержит базис. Существование базиса конечномерного пространства.	10
4	Подпространства векторного пространства. Подпространство конечномерного пространства конечномерно.	11
5	Теорема о мощности базиса конечномерного пространства. Размерность пространства.	12
6	Координаты вектора в данном базисе. Матрица перехода от одного базиса к другому. Преобразование координат при замене базиса. Матрица преобразования координат.	13
7	Сумма и пересечение подпространств. Теорема о размерностях суммы и пересечения.	15
8	Прямая сумма подпространств. Эквивалентные переформулировки понятия прямой суммы подпространств.	18
9	Построение кольца многочленов.	19
10	Степень многочлена. Свойства степени. Область целостности. Кольцо многочленов над областью целостности есть область целостности.	21
11	Теорема о делении с остатком в кольце многочленов.	23
12	Корни многочлена. Теорема Безу.	24
13	Кратные корни многочлена. Теорема о числе корней многочлена над полем.	25

14	Функциональное и формальное равенство многочленов.	27
15	Характеристика поля.	28
16	Производная многочлена. Свойства производной. Многочлены с нулевой производной.	29
17	Теорема о кратности	31
18	Интерполяционная задача. Существование и единственность решения.	32
19	Интерполяционный метод Ньютона.	33
20	Интерполяционный метод Лагранжа.	34
21	Делимость и ассоциированность в кольце многочленов над полем.	35
22	Наибольший общий делитель в кольце многочленов над полем. Существование и линейное представление.	36
23	Взаимно простые многочлены. Свойства взаимно простых многочленов. Если многочлен делит произведение двух многочленов и взаимно прост с первым сомножителем, то он делит второй сомножитель.	38
24	Неприводимые многочлены. Теорема о разложении многочлена в произведение неприводимых (существование).	39
25	Теорема о разложении многочлена в произведение неприводимых (единственность).	42
26	Алгебраически замкнутые поля. Эквивалентные переформулировки. Алгебраическая замкнутость поля комплексных чисел. (б.д.)	43
27	Неприводимые многочлены над полем вещественных чисел. Теорема о разложении многочлена с вещественными коэффициентами в произведение неприводимых над \mathbb{R} .	45

28 Поле частных области целостности. Поле частных кольца многочленов (поле рациональных функций).	47
29 Простейшие дроби. Разложение рациональной функции в сумму многочлена и простейших дробей. (существование).	50
30 Разложение рациональной функции в сумму многочлена и простейших дробей. (единственность).	54
31 Факториальные кольца. Содержание многочлена над факториальным кольцом. Содержание произведения многочленов.	56
32 Теорема Гаусса о факториальности кольца многочленов над факториальным кольцом. Факториальность колец $K[x_1, \dots, x_n], \mathbb{Z}[x_1, \dots, x_n]$	58
33 Неприводимость над \mathbb{Q} и над \mathbb{Z} . Методы доказательства неприводимости многочленов с целыми коэффициентами (редукция по одному или нескольким простым модулям).	59
34 Критерий неприводимости Эйзенштейна.	60
35 Рациональные корни многочлена с целыми коэффициентами.	61
36 Верхняя оценка модуля корня многочлена с комплексными коэффициентами.	62
37 Симметрические функции. Коэффициенты многочлена из $C[x]$ как симметрические функции корней.	63
38 Алгоритм разложения на неприводимые множители многочлена с целыми коэффициентами.	64
39 Линейные отображения векторных пространств. Линейное отображение полностью задается своими значениями на базисных векторах.	65
40 Сумма линейных отображений, умножение на скаляр. Пространство линейных отображений.	66

41	Матрица линейного отображения для данных базисов. Матрица суммы отображений. Изоморфизм пространства линейных отображений и пространства матриц.	67
42	Композиция линейных отображений. Матрица композиции.	68
43	Преобразование матрицы линейного отображения при замене базисов.	69
44	Ядро и образ линейного отображения, их свойства. Критерий инъективности и сюръективности линейного отображения в терминах ядра и образа.	70
45	Выбор базисов, для которых матрица линейного отображения имеет почти единичный вид. Следствие для матриц. Теорема о размерности ядра и образа.	71
46	Критерий изоморфности конечномерных пространств	72
47	Двойственное пространство. Двойственный базис. Изоморфность конечномерного пространства и его двойственного. Пример пространства не изоморфного своему двойственному.	74
48	Каноническое отождествление конечномерного пространства со вторым двойственным.	75
49	Линейные операторы. Кольцо линейных операторов. Изоморфность кольца линейных операторов и кольца матриц.	76
50	Многочлены от оператора. Коммутирование многочленов от одного оператора.	77
51	Характеристический многочлен матрицы и оператора. Независимость характеристического многочлена оператора от выбора базиса.	78
52	Собственные числа и собственные векторы оператора и матрицы. Собственные числа как корни характеристического многочлена	79

53	Теорема Гамильтона-Кэли.	81
54	Диагонализируемые операторы. Критерий диагонализуемости. Примеры недиагонализируемых операторов	82
55	Инвариантные подпространства. Матрице линейного оператора, действующего на пространстве, разложенном в прямую сумму инвариантных подпространств.	84
56	Инвариантность ядра и образа многочлена от оператора.	85
57	Теорема о разложении $\text{Ker}(fg)(\phi)$ в прямую сумму инвариантных подпространств и следствия из неё.	86
58	Жорданова форма оператора. Жорданов базис. Формулировка теоремы о жордановой форме оператора. Сведение к случаю оператора с единственным собственным числом.	87
59	Относительная линейная независимость. Относительные базисы. Корневые пространства. Лемма о спуске для корневых подпространств.	88
60	Построение жорданова базиса и жордановой формы для оператора с единственным собственным числом.	89
61	Единственность жордановой формы оператора.	90

1 Базис векторного пространства. Четыре эквивалентных переформулировки определения базиса.

Опр

Пусть V - векторное пространство над полем K , тогда:

1. $\{v_\alpha\}_{\alpha \in A}$ - линейно независима, если $\sum_{\text{почти все } c_\alpha = 0} c_\alpha v_\alpha = 0 \Rightarrow \text{все } c_\alpha = 0$
2. $\{v_\alpha\}$ - семейство образующих V , если любой $v \in V$ - есть линейная комбинация $\{v_\alpha\}$, если любой $v \in V$ есть $\sum_{\text{почти все } c_\alpha = 0} c_\alpha v_\alpha$

Опр

Базис - лин. незав. сем-во образующих ($\bar{0} \notin$ базису)

Опр

Линейно независимое семейство векторов называется максимальным (по включению), если при добавлении \forall вектора новое семейство ЛЗ

Опр

Сем-во образующих называется минимальным по включению, если при выбрасывании \forall вектора сем-во не является семейством образующих

Теорема (Равносильные утверждения)

V - в.п. над K , $\{v_\alpha\}_{\alpha \in A}$, следующие условия равносильны:

1. $\{v_\alpha\}$ - базис V над K
2. $\{v_\alpha\}$ - max ЛН семейство
3. $\{v_\alpha\}$ - min семейство образующих
4. $\forall v \in V$ единственным образом представим в виде лин. комбинации векторов из $\{v_\alpha\}$

Док-во

(1 \Rightarrow 2):

Базис \Rightarrow ЛН.

Добавим $v \in V$ к $\{v_\alpha\}$: $v = \sum_{\text{Почти все } c_\alpha = 0} c_\alpha v_\alpha$,

но тогда $-v + \sum_{\text{Почти все } c_\alpha = 0} c_\alpha v_\alpha = 0 \Rightarrow$ новое семейство ЛЗ $\Rightarrow \{v_\alpha\}$ - ЛЗ

(2 \Rightarrow 1):

$\{v_\alpha\}$ - max ЛН

\Rightarrow при добавлении $\forall v \in V \exists c \neq 0 : 0 = cv + \sum_{\text{Почти все } c_\alpha = 0} c_\alpha v_\alpha$

$\Rightarrow v = \sum_{\text{Почти все } c_\alpha = 0} (c^{-1}c_\alpha)v_\alpha$ в силу произвольности v , $\{v_\alpha\}$ - базис.

(1 \Rightarrow 3):

$\{v_\alpha\}$ - базис \Rightarrow семейство образующих. Пусть $v \in \{v_\alpha\}$.

Если бы $\{v_\alpha\}$ без v было бы семейством образующих,

то $v = \sum_{\text{п.в. } c_\alpha = 0, v \notin \{v_\alpha\}} c_\alpha v_\alpha$, но тогда $0 = -v + \sum_{\text{п.в. } c_\alpha = 0, v \notin \{v_\alpha\}} c_\alpha v_\alpha$

(3 \Rightarrow 1):

$\{v_\alpha\}$ - min семейство образующих, нужно проверить что ЛН.

Пусть ЛЗ, тогда $\sum_{\text{п.в. } c_\alpha = 0} c_\alpha v_\alpha = 0 \Rightarrow c_{\alpha_0} \neq 0$.

Но тогда $v_{\alpha_0} = \sum_{\text{п.в. } c_\alpha = 0} (c_{\alpha_0}^{-1}c_\alpha)v_\alpha$, противоречие с min сем-ом обр.

(4 \Rightarrow 1):

4 формально сильнее

(1 \Rightarrow 4):

$$v = \sum_{\text{п.в. } c_\alpha = 0} c_\alpha v_\alpha = \sum_{\text{п.в. } c'_\alpha = 0} c'_\alpha v_\alpha \Rightarrow 0 = \sum_{\text{п.в. } c_\alpha - c'_\alpha = 0} c_\alpha v_\alpha$$

В силу единственности разложения нуля получаем $c_\alpha = c'_\alpha \forall \alpha$

2 Конечномерные пространства. Всякое линейно независимое семейство конечномерного пространства можно дополнить до базиса. Существование базиса конечномерного пространства.

Опр

V - в.п. над полем K , V называется конечномерным, если в V есть конечное сем-во образующих.

Пример

\mathbb{C} - ВП не являющееся конечномерным.

$V = \{(c_1, c_2, \dots), \text{ не все } c_i = 0\}$

Сложение, умножение на скаляр - некоординатно.

V - ВП над \mathbb{C} , пусть $v_1, \dots, v_k \in V$, $v_i = (c_{i1}, c_{i2}, \dots)$, почти все $c_{ij} = 0$

$\exists N : \forall j > N, \forall i \ c_{ij} = 0$

Теорема

Всякое линейно независимое сем-во конечномерного пространства можно дополнить до базиса.

Док-во

1) $\{v_\alpha\}$ - ЛН \Rightarrow либо порождает V , либо можно дополнить с сохранением условия ЛН.

То есть линейная оболочка $\{\sum c_\alpha v_\alpha\}$ либо равна $\forall v \in V$, тогда $\{v_\alpha\}$ - семейство образующих V , либо неравна, тогда v и $\{v_\alpha\}$ ЛН и можно им дополнить

2) V - конечномерно, пусть u_1, u_2, \dots, u_m - конечное семейство образующих V , тогда если v_1, v_2, \dots, v_n - его ЛК и $m > n$, то $\{u_\alpha\}$ - ЛЗ \Rightarrow всякое ЛН семейство из V содержит $\leq m$ векторов. Значит добавление векторов оборвётся.

Следствие

Во всяком конечномерном в.п. есть базис.

Док-во

Пустое сем-во ЛН

Дополним до базиса

3 Всякое семейство образующих конечномерного пространства содержит базис. Существование базиса конечномерного пространства.

Теорема

V - конечномерное в.п. над K

Всякое конечномерное сем-во образующих содержит базис.

Док-во

Пусть v_1, v_2, \dots, v_k - семейство образующих V . Если оно ЛН, то базис.

Если ЛЗ, то $\exists i: v_i$ - линейная комбинация остальных

$\Rightarrow \{v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_k\}$ - семейство образующих, а т.к. семейство конечно, то процесс выкидывания "оборвётся" и на каком-то шаге получится ЛН зависимое семейство, то есть базис.

Теорема

Во всяком конечномерном в.п. есть базис

Док-во

Возьмём конечное семейство образующих, по теореме оно содержит базис.

4 Подпространства векторного пространства. Подпространство конечномерного пространства конечномерно.

Опр

V - в.п над полем K , $U \neq \emptyset$ - подпр-во V (записывается $U \subseteq V$),
если U - само явл. в.п. над K

Предположение (1)

$$\emptyset \neq U \subseteq V \quad U \text{ - подпр-во } V \Leftrightarrow$$

1. $\forall u_1, u_2 \in U : \quad u_1 + u_2 \in U$
2. $\forall u \in U, \forall a \in K \quad au \in U$

Док-во

(\Rightarrow)

По определению ВП.

(\Leftarrow)

Операции сложения и умножения на скаляр определены на U . Осталось проверить аксиомы ВП:

1. $\forall x, y \in U \quad x + y = y + x$ по опр. сложения
2. $\forall x, y, z \in U \quad (x + y) + z = z + (y + z)$, аналогично
3. Т.к. $U \neq \emptyset$, то $\exists u \in U$. $0_V = u + (-1)u$.

По условию теоремы следует, что $0 \in U$, так как $u, (-1)u, u + (-1)u \in U$. $\forall u \in U: 0 + u = u, u + 0 = u$

4. $\forall u \in U \quad \exists -u = (-1)u, u - u = 0$

Остальные 4 аналогично.

Предположение (2)

V - конечномерное в.п над K

$$U \subseteq V \Rightarrow U \text{ - конечномерное}$$

Док-во

$\{\}$ - пустое семейство.

Будем добавлять к нему вектора из U с сохранением ЛН, пока не получим семейство образующих. Причем в V есть конечное семейство ЛН образующих.

Значит так как векторов в семействе U не может быть больше, чем в семействе V , то там тоже их конечное количество.

5 Теорема о мощности базиса конечномерного пространства. Размерность пространства.

Теорема

V - конечномерное пространство

$\{v_1, \dots, v_n\}, \{u_1, \dots, u_m\}$ - базисы V над K

$$\Rightarrow n = m$$

Док-во

u_1, \dots, u_m - лин.комб v_1, \dots, v_n

\Rightarrow по т. о линейной зависимости лин. комбинаций

$$m \leq n \text{ и аналогично } m \geq n \Rightarrow m = n$$

Опр

Размерность конечномерного пространства - размерность векторов в его базисе.

Обозначаем как $\dim_K V = \dim V$

Если пространство не конечно, то пишем $\dim V = \infty$

6 Координаты вектора в данном базисе. Матрица перехода от одного базиса к другому. Преобразование координат при замене базиса. Матрица преобразования координат.

Теорема

Пусть V - ВП над K , $n = \dim_K V < \infty$, v_1, \dots, v_n - базис V над K .

Тогда если $v \in V$, то $\exists!$ набор $\alpha_1, \dots, \alpha_n \in K : v = \alpha_1 v_1 + \dots + \alpha_n v_n$

Опр

$\alpha_1, \dots, \alpha_n$ будем называть координатами v в базисе $\{v_1, \dots, v_n\}$ и записывать как $\begin{pmatrix} \alpha_1 \\ \dots \\ \alpha_n \end{pmatrix}$, причем $v = \begin{pmatrix} \alpha_1 & \dots & \alpha_n \end{pmatrix} \begin{pmatrix} v_1 \\ \dots \\ v_n \end{pmatrix}$

Док-во

Пусть v_1, \dots, v_n - базис V

v'_1, \dots, v'_n - другой базис V

$$v'_i = c_{1i}v_1 + \dots + c_{ni}v_n$$

$$c = \begin{pmatrix} c_{11} & c_{21} & \dots & c_{n1} \\ c_{12} & \ddots & & \\ & & \ddots & \\ c_{1n} & & & c_{nn} \end{pmatrix} - \text{матрица перехода от базиса}$$

(v_1, \dots, v_n) к базису (v'_1, \dots, v'_n)

$$\begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = C \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} \quad \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix} = B \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix}$$

$$v_i = b_{1i}v'_1 + \dots + b_{ni}v'_n$$

$$B = \begin{pmatrix} b_{11} & & b_{n1} \\ b_{12} & & \\ & & \\ b_{1n} & & b_{nn} \end{pmatrix} - \text{матрица перехода от базиса } (v'_1, \dots, v'_n)$$

к базису (v_1, \dots, v_n)

$$v = a_1 v_1 + \dots + a_n v_n$$

$$v = a'_1 v'_1 + \dots + a'_n v'_n$$

C - матрица перехода от (v_1, \dots, v_n) к (v'_1, \dots, v'_n)

$$C^T = \begin{pmatrix} c_{11} & c_{1i} & & c_{1n} \\ & \ddots & & \\ c_{n1} & & \ddots & c_{nn} \end{pmatrix} = D - \text{матрица преобразования координат}$$

Теорема (в указанных выше обозначениях)

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = D \begin{pmatrix} a'_1 \\ \vdots \\ a'_n \end{pmatrix}$$

Док-во

$$v = (a'_1, \dots, a'_n) \begin{pmatrix} v'_1 \\ \vdots \\ v'_n \end{pmatrix} = (a'_1, \dots, a'_n) \cdot C \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

$$v = (a_1, \dots, a_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

В силу единственности разложения по базису

$$(a_1, \dots, a_n) = (a'_1, \dots, a'_n) \cdot C$$

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = C^T \begin{pmatrix} a'_1 \\ \vdots \\ a'_n \end{pmatrix}$$

7 Сумма и пересечение подпространств. Теорема о размерностях суммы и пересечения.

Опр

V - ВП над K , $U_1, \dots, U_m \subseteq V$

Пересечение: $\bigcap_{i=1}^n U_i = \{v \in V | v \in U_1, \dots, v \in U_n\}$

Сумма: $U_1 + \dots + U_n = \{v \in V | \exists u_1 \in U_1, \dots, u_n \in U_n : v = u_1 + \dots + u_n\}$

Теорема

1. Сумма $U_1 + \dots + U_m$ является подпространством

$$0 = 0 + \dots + 0 \in U_1 + \dots + U_m \Rightarrow \text{сумма} \neq \emptyset$$

$\forall u, v \in U_1 + \dots + U_m$:

$$u = u_1 + u_2 + \dots + u_m$$

$$v = v_1 + v_2 + \dots + v_m$$

$$u + v = \underbrace{(u_1 + v_1)}_{\in U_1} + \underbrace{(u_2 + v_2)}_{\in U_2} + \dots + \underbrace{(u_m + v_m)}_{\in U_m} \in U_1 + \dots + U_m$$

умножение на скаляр аналогично

2. Пересечение является подпространством

$$\bigcap_{i=1}^n U_i \ni u, v \quad a \in K$$

$$\begin{array}{ll} \forall i & u + v \in U_i \\ & u + v \in \bigcap_{i=1}^n U_i \\ & au \in U_i \\ & au \in \bigcap_{i=1}^n U_i \end{array}$$

не пусто, т.к.:

$$0_V \in \bigcap_{i=1}^n U_i \Rightarrow \bigcap_{i=1}^n U_i \subseteq V$$

$$\bigcap_{i=1}^n U_i \subseteq U_1 \subseteq U_1 + U_2 \supseteq U_2 \supset \bigcap_{i=1}^n U_i$$

Теорема

$U_1, U_2 \subseteq V$ U_1, U_2 - конечномерные

Тогда $U_1 \cap U_2$ и $U_1 + U_2$ - конечномерны

и $\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim(U_1) + \dim(U_2)$

Док-во

$U_1 \cap U_2 \subseteq U_1$, U_1 - конечномерно

$\Rightarrow U_1 \cap U_2$ - конечномерно

w_1, \dots, w_r - базис $U_1 \cap U_2$, ЛНЗ сем-во в U_1

Дополним до базиса U_1 :

$w_1, \dots, w_r, u_1, \dots, u_s$ - базис U_1

Аналогично w_1, \dots, w_r дополним до базиса U_2 :

$w_1, \dots, w_r, v_1, \dots, v_t$ - базис U_2

Проверим, что $w_1, \dots, w_r, u_1, \dots, u_s, v_1, \dots, v_t$ - базис $U_1 + U_2$:

1. Семейство образующих

$$z \in U_1 + U_2 \quad z = z_1 + z_2 \quad z_1 \in U_1 \quad z_2 \in U_2$$

$$z_1 = a_1 w_1 + \dots + a_r w_r + b_1 u_1 + \dots + b_s u_s$$

$$z_2 = c_1 w_1 + \dots + c_r w_r + d_1 v_1 + \dots + d_t v_t$$

$$z = (a_1 + c_1)w_1 + \dots + (a_r + c_r)w_r + b_1 u_1 + \dots + b_s u_s + d_1 v_1 + \dots + d_t v_t$$

$$\Rightarrow w_1, \dots, w_r, u_1, \dots, u_s, v_1, \dots, v_t - \text{сем-во образующих}$$

2. ЛНЗ

$$(*) 0 = a_1 w_1 + \dots + a_r w_r + b_1 u_1 + \dots + b_s u_s + c_1 v_1 + \dots + c_t v_t$$

$$z = \underbrace{a_1 w_1 + \dots + a_r w_r + b_1 u_1 + \dots + b_s u_s}_{\in U_1} = \underbrace{-c_1 v_1 - \dots - c_t v_t}_{\in U_2}$$

$$z \in U_1 \cap U_2 \Rightarrow z = d_1 w_1 + \dots + d_r w_r =$$

$$= d_1 w_1 + \dots + d_2 w_2 + 0 \cdot u_1 + 0 \cdot u_2 + \dots + 0 \cdot u_s$$

В силу единственности разложения по базису U_1

$$b_1 = b_2 = \dots = b_s = 0$$

$$\text{Из } (*) \Rightarrow a_1 w_1 + \dots + a_r w_r + c_1 v_1 + \dots + c_t v_t = 0$$

т.к. $w_1, \dots, w_r, v_1, \dots, v_t$ - базис U_2 , то

$$a_1 = \dots = a_r = c_1 = \dots = c_t = 0$$

$$\Rightarrow w_1, \dots, w_r, u_1, \dots, u_s, v_1, \dots, v_t - \text{ЛНЗ}$$

Знаем,

$$\dim(U_1) = r + s$$

$$\dim(U_2) = r + t$$

$$\dim(U_1 \cap U_2) = r$$

$$\dim(U_1 + U_2) = r + t + s$$

Значит,

$$\dim(U_1 \cap U_2) + \dim(U_1 + U_2) = \dim(U_1) + \dim(U_2)$$

8 Прямая сумма подпространств. Эквивалентные переформулировки понятия прямой суммы подпространств.

V - в.п. над K , $U_1, \dots, U_m \subseteq V$

Опр

$U_1 + \dots + U_m$ назыв. прямой суммой, если любой $z \in U_1 + \dots + U_m$ единственным образом представим в виде суммы:

$$z = u_1 + u_2 + \dots + u_m \quad u_i \in U_i \quad i = 1, \dots, m$$

Обозначение: $U_1 \oplus U_2 \oplus \dots \oplus U_m$

Замечание

Сумма $U_1 + \dots + U_m$ - прямая \Leftrightarrow

$$\Leftrightarrow 0 = u_1 + \dots + u_m \quad u_i \in U_i \Rightarrow u_1 = \dots = u_m = 0$$

Док-во

(\Rightarrow)

очевидно

(\Leftarrow)

$$z \in U_1 + \dots + U_m$$

$$z = u_1 + \dots + u_m = v_1 + \dots + v_m$$

$$0 = z - z = (u_1 - v_1) + \dots + (u_m - v_m)$$

$\in U_1 \qquad \qquad \qquad \in U_m$

$$\forall i \quad u_i - v_i = 0 \text{ т.е. } u_i = v_i$$

Предположение (1)

Сумма $U_1 + U_2$ - прямая $\Leftrightarrow U_1 \cap U_2 = \{0\}$

Предположение (2)

Сумма $U_1 + U_2$ - прямая \Leftrightarrow

\Leftrightarrow объединение базисов U_1 и U_2 - есть базис $U_1 + U_2$

Предположение (3)

$U_1 + \dots + U_m$ - прямая \Leftrightarrow

$$\Leftrightarrow \forall i = 1, \dots, m \quad U_i \cap (U_i + \dots + U_{i-1} + U_{i+1} + \dots + U_m) = \{0\}$$

Предположение (4)

Сумма $U_1 + \dots + U_m$ - прямая \Leftrightarrow

\Leftrightarrow объединение базисов $U_i \quad i = 1, \dots, m$ - базис $U_1 + \dots + U_m$

9 Построение кольца многочленов.

Опр

R - комм. кольцо с 1

$$R[x] := \{(a_0, a_1, a_2, \dots) : a_i \in R \quad i = 0, \dots \text{ п.в. } a_i = 0\}$$

$$(a_0, a_1, \dots), (b_0, b_1, \dots) \in R[x]$$

Сложение:

$$(a_0, a_1, \dots) + (b_0, b_1, \dots) = (a_0 + b_0, a_1 + b_1, \dots)$$

Замечание:

$$\begin{aligned} \forall n > N \quad a_i = 0 \\ \forall m > M \quad b_i = 0 \end{aligned} \Rightarrow \forall i > \max(N, M) \quad a_i + b_i = 0$$

Умножение:

$$(a_0, a_1, \dots) \cdot (b_0, b_1, \dots) = (c_0, c_1, \dots)$$

$$c_n = \sum_{i=0}^n a_i b_{n-i} = a_0 b_n + a_1 b_{n-1} + \dots + a_n b_0$$

Замечание:

$$\forall n > N \quad a_n = 0$$

$$\forall m > M \quad b_m = 0$$

$$\forall k > N + M \quad c_k = \sum_{i=0}^k a_i b_{k-i} = \sum_{i=0}^N a_i b_{k-i} + \sum_{i=N+1}^k a_i b_{k-i} = 0$$

$$i \leq N \quad k - i \geq k - N > N + M - N = M$$

Теорема

$$(R[x], +, \cdot) - \text{комм. кольцо с 1}$$

Док-во (ассоциативность умножения)

$$A = (a_0, a_1, \dots), \quad B = (b_0, b_1, \dots), \quad C = (c_0, c_1, \dots)$$

$$(AB)C \stackrel{?}{=} A(BC)$$

$$\text{Пусть } AB = D, \quad BC = E, \quad (AB)C = F, \quad A(BC) = G$$

$$\begin{aligned}
f_n &= \sum_{i=0}^n d_i c_{n-i} = \sum_{i=0}^n \left(\sum_{j=0}^i a_j b_{i-j} \right) c_{n-i} = \\
&= \sum_{i=0}^n \sum_{j=0}^i a_j b_{i-j} c_{n-i} = \sum_{j=0}^n a_j \left(\sum_{i=j}^n b_{i-j} c_{n-i} \right) \underset{\text{напр. движения индекса изменилось}}{=} \\
&= \sum_{j=0}^n a_j \left(\sum_{k=0}^{n-j} b_k c_{n-j-k} \right) = \sum_{j=0}^n a_j e_{n-j} = g_n
\end{aligned}$$

Упр

Остальное д-ть самостоятельно

Опр

Введем 0 и 1:

$$0 = (0, 0, \dots)$$

$$1 = (1, 0, \dots)$$

Нетрудно проверить, что они уд-ют необходимым свойствам

$R[x] \supset \{(a, 0, \dots); a \in R\}$ - подкольцо изоморфное R

$$(a, 0, \dots) + (b, 0, \dots) = (a + b, 0, \dots)$$

$$(a, 0, \dots) \cdot (b, 0, \dots) = (ab, 0, \dots)$$

$$(a, 0, \dots) = a \text{ (обозначение)}$$

$$x = (0, 1, 0, \dots)$$

$$x^i = (0, \dots, 0, \underset{i}{1}, 0, \dots)$$

$$\begin{aligned}
(a_0, a_1, \dots, a_n, 0, \dots) &= (a_0, 0, \dots) + (0, a_1, 0, \dots) + \dots + (0, \dots, a_n, 0, \dots) = \\
&= a_0 \cdot 1 + a_1(0, 1, \dots) + \dots + a_n(0, \dots, 1, \dots) =
\end{aligned}$$

$$= a_0 + a_1 x + a_2 x^2 + \dots + a_n x^n = \sum_{i=0}^n a_i x^i$$

10 Степень многочлена. Свойства степени. Область целостности. Кольцо многочленов над областью целостности есть область целостности.

Опр

$$f = a_0 + a_1x + \dots + a_nx^n \in R[x]$$

Наибольшее m , т.ч. $a_m \neq 0$ называется степенью f ($\deg f - degree$)
 $\deg 0 = -\infty$

Опр

Ком. кольцо R с 1 назыв. областью целостности (или кольцом без делителей 0)

$$\text{Если } \forall a, b \in R \quad (ab = 0 \Rightarrow a = 0 \text{ или } b = 0)$$

$$\forall a, b \in R (a \neq 0 \quad b \neq 0 \Rightarrow ab \neq 0)$$

Примеры

1. \mathbb{Z} - о.ц.
2. Любое поле - о.ц
3. $\mathbb{Z}/_m\mathbb{Z}$ - не всегда о.ц. $[a][b] = [m] = [0]$

Теорема (Свойства степени)

1. $\deg(f + g) \leq \max(\deg f, \deg g)$

$$\text{Если } \deg f \neq g, \text{ то } \deg(f, g) = \max(\deg f, \deg g)$$

2. $\deg(fg) \leq \deg f + \deg g$

$$\text{Если } R - \text{о.ц, то } \deg(fg) = \deg f + \deg g$$

Док-во

- 1) $N = \deg f \quad M = \deg g$

$$f = \sum_{i=0}^N a_i x^i \quad g = \sum_{i=0}^M b_i x^i$$

$$\forall n > \max(N, M) \quad a_n + b_n = 0 \Rightarrow \deg(f + g) \leq \max(N, M)$$

Равенства в общ. случае нет

$$\text{Если } N = M \quad a_N = -b_N \Rightarrow a_N + b_N = 0$$

$$\text{Если } N \neq M \quad \sqsubset N < M$$

$$a_M + b_M = 0 + b_M = b_M \neq 0$$

$$2) fg = \sum_{i=0} c_i x^i \quad c_i = 0 \text{ для всех } i > N + M$$

$$\deg(fg) \leq N + M = \deg f + \deg g$$

$$c_{N+M} = a_N b_M \quad \text{в общем случае:}$$

$$\text{Если } R \text{ не о.ц, } a_N \neq 0 \quad b_M \neq 0 \text{ то } a_N \cdot b_M \text{ м.б. } = 0$$

$$\text{Если } R - \text{о.ц, то } a_N \neq 0 \quad b_M \neq 0 \Rightarrow c_{N+M} \neq 0$$

$$\Rightarrow \deg fg = \deg f + \deg g$$

Следствие

$$\text{Если } R - \text{о.ц, то } R[x] - \text{о.ц}$$

Док-во

$$f, g \in R[x] \quad f \neq 0 \quad g \neq 0$$

$$\deg f \geq 0 \quad \deg g \geq 0$$

$$\deg(fg) = \deg f + \deg g \geq 0$$

$$\Rightarrow \text{в } fg \text{ есть хотя бы один ненулевой коэф.}$$

$$\Rightarrow fg \neq 0$$

Замечание

$$\text{Если } K - \text{поле} \quad K[x] - \text{о.ц}$$

Замечание

$$R \rightarrow R[x_1] \text{ с помощью индукции сделаем вывод}$$

$$R[x_1, x_2] = (R[x_1])[x_2]$$

$$R[x_1, \dots, x_n] = (R[x_1, \dots, x_{n-1}])[x_n]$$

$$\Rightarrow R - \text{о.ц} \Rightarrow R[x_1, \dots, x_n] - \text{о.ц}$$

11 Теорема о делении с остатком в кольце многочленов.

Теорема

R - комм. к. с ед., $f, g \in R[x]$,

$$g = a_0 + a_1x + \dots + a_nx^n, a_n \in R^* \text{ обр. элем.}$$

Тогда $\exists!$ мн-ны q и r такие, что:

$$f = q \cdot g + r, \quad \deg r < \deg g$$

Док-во

(Существование):

Индукция по $m = \deg f$

База. $\deg f < \deg g$

$$h := 0, \quad r := f$$

$$f = g \cdot 0 + f$$

Инд. переход. Пусть $m \geq n$ и утверждение доказано для всех многочленов меньшей степени $< m$

$$f = b_0 + b_1x + \dots + b_mx^m$$

$$f_1 := f - a_n^{-1}b_mx^{m-n}g = \cancel{b_mx^m} + \dots - (\cancel{a_n^{-1}b_ma_nx^m} + \dots) \Rightarrow \deg f_1 < m$$

$$f_1 = gh_1 + r_1, \quad \text{по инд.п. } \deg r_1 < \deg g$$

$$f = f_1 - a_n^{-1}b_mx^{m-n}g = \underbrace{(h_1 + a_n^{-1}b_mx^{m-n})}_=h g + \underbrace{r_1}_=r$$

$$\deg r = \deg r_1 < g$$

(Единственность):

$$f = gh + r = g\tilde{h} + \tilde{r}, \quad \deg r < \deg g, \quad \deg \tilde{r} < \deg g$$

$$g(\tilde{h} - h) = r - \tilde{r} \quad \deg(r - \tilde{r}) < \deg g$$

Если $\tilde{h} - h \neq 0$, то положим $d = \deg(\tilde{h} - h)$

$$\tilde{h} - h = \underset{\neq 0}{c_d}x^d + \dots$$

$$g(\tilde{h} - h) = \underset{\neq 0}{a_nc_d}x^{n+d} + \dots$$

(Если $a_nc_d = 0 \Rightarrow c_d = a_n^{-1}a_nc_d = a_n^{-1}0 = 0$, противоречие)

$$\deg(r - \tilde{r}) = \deg g(\tilde{h} - h) \geq g, \text{ но } \deg(r - \tilde{r}) < \deg g$$

Пример

В кольце $\mathbb{Z}[x]$

$x^2 + 1$ нельзя поделить на $2x + 1$

12 Корни многочлена. Теорема Безу.

Опр

R - ком. кольцо с 1

$$f \in R[x] \quad f = a_0 + a_1x + \dots + a_nx^n$$

Для данного мн-на определим отображение из R в R :

$$c \rightarrow a_0 + a_1c + \dots + a_nc^n = f(c)$$

Замечание

Разные мн-ны могут задавать одно и то же отображение

$$\mathbb{Z}/2\mathbb{Z} \quad f = 0 \quad 0 \rightarrow 0 \quad 1 \rightarrow 0$$

$$f = x^2 + x \quad 0 \rightarrow 0 \quad 1 \rightarrow 0$$

$$(f + g)(c) = f(c) + g(c)$$

$$(f \cdot g)(c) = f(c) \cdot g(c)$$

Опр

$f \in R[x] \quad c$ - корень f , если $f(c) = 0$

Теорема (Безу)

$f \in R[x] \quad c \in R$, тогда:

$$\exists q \in R[x] \quad f = (x - c)q + f(c)$$

Док-во

$g = x - c$, по т. о делении с остатком:

$$\exists q, r \in R[x] : f = (x - c)q + r$$

$$\deg r < \deg g = 1$$

$$\deg r \leq 0 \Rightarrow r \in R$$

$$f(c) = (c - c) \cdot q(c) + r = r \Rightarrow f = (x - c)q + f(c)$$

Следствие

$$c \text{ - корень } f \Leftrightarrow (x - c) \mid f$$

Док-во

(\Rightarrow) :

$$f(x) = (x - c)q(x) + f(c) = (x - c)q(x) \Rightarrow (x - c) \mid f$$

(\Leftarrow) :

$$f(x) = (x - c)q(x) \Rightarrow f(c) = (c - c)q(c) = 0$$

13 Кратные корни многочлена. Теорема о числе корней многочлена над полем.

Опр

K - поле $f \in K[x]$

Тогда a - корень f кратности k , если $(x - a)^k \mid f$ и $(x - a)^{k+1} \nmid f$

(т.е. $f(x) = (x - a)^k \cdot g(x)$ $(x - a) \nmid g$ $(\Leftrightarrow g(a) \neq 0)$)

Замечание

a - корень f_1 кратности k_1 , a - корень f_2 кратности k_2

$\Rightarrow a$ - корень $f_1 \cdot f_2$ кратности $k_1 + k_2$

Док-во

$f_1(x) = (x - a)^{k_1} g_1(x)$ $g_1(a) \neq 0$ $f_2(x) = (x - a)^{k_2} g_2(x)$ $g_2(a) \neq 0$

$\Rightarrow f_1(x) f_2(x) = (x - a)^{k_1 + k_2} g_1(x) g_2(x)$

(поле K - о.ц.)

Лемма

$f, g, h \in K[x]$, $b \in K$ b - не корень h

$f(x) = h(x)g(x)$

b - корень $f \Rightarrow b$ - корень g той же кратности

Док-во

1) b - корень f кр. $l \geq 1 \Rightarrow b$ - корень g кратности $\geq l$

Индукция по l . Б.И.:

$l = 1$ $f(b) = 0$ $h(b)g(b) = 0 \Rightarrow g(b) = 0$

b - корень $g \Rightarrow$ корень g кр. ≥ 1

Инд. переход $(l \rightarrow l + 1)$

b - корень f кр. $l + 1 \Leftrightarrow f(x) = (x - b)^{l+1} f_1(x)$

По предп. b - корень g $g(x) = (x - b)g_1(x)$

$(x - b)^{l+1} f_1(x) = (x - b)g_1(x)h_1(x)$ $(= f(x))$

В обл. целостности можем сократить на ненулевой множитель

$$(x - b)^l f_1(x) = g_1(x) h(x)$$

По инд. предп. b - корень кратности $\geq l$

$\Rightarrow b$ - корень g кр. $\geq l + 1$ (при перемножении кр-ти складываются)

2) $f(x) = h(x)g(x)$ и b - корень g кр-ти k

$$(x - b)^k \mid g(x) \Rightarrow (x - b)^k \mid f(x)$$

b - корень кр-ти не больше кр-ти корня f

Теорема

K - поле, $f \in K[x]$ $f \neq 0$

\Rightarrow число корней с учетом их кратности не превосходит $\deg f$

Док-во

Индукция по $\deg f$

Б.И.:

$\deg f = 0$ корней нет

И.П.:

a - корень f кр. $k \Rightarrow f(x) = (x - a)^k g(x)$

Пусть $b \neq a \Rightarrow b$ - корень $f \Leftrightarrow$

$\Leftrightarrow b$ - корень g , причем кратности совпадают (по лемме, т.к. $(x - b)^k \neq 0$)

По инд. предп. число корней g с учетом кратности $\leq \deg g$

(а это в точности все корни f , отличные от a)

Сумм. кр. корней $f = k + \text{сумм. кр. корней } g \leq k + \deg g = \deg f$

Замечание

Теор. не верна для $f \in R[x]$ (в случае произвольного комм. кольца R)

$$R = \mathbb{Z}_8\mathbb{Z}$$

$$x^2 = [1] \in R[x]$$

корни 1, 3, 5, 7 $\deg f = 2$

Следствие

Если $f(a_1) = \dots = f(a_n) = 0$ для попарно различных a_1, \dots, a_n

И $n > \deg f$, тогда $f = 0$

14 Функциональное и формальное равенство многочленов.

Следствие (пред. [теореме](#))

$f, g \in K[x] \quad |K| > \max(\deg f, \deg g),$
если f и g совп. функционально, то $f = g$

Док-во

Функ. рав-во: $\forall a \in K \quad f(a) = g(a) \Rightarrow (f - g)(a) = 0$

$$\deg(f - g) \leq \max(\deg f, \deg g) < |K|$$

по пред. [сл.](#) $f - g = 0 \Rightarrow f = g$

Замечание

Для беск. полей из функ. равенства мн-ов следует формальное

15 Характеристика поля.

Опр

K - поле $1 \in K$

$$n \cdot 1 = \underbrace{1 + \dots + 1}_n$$

Если $n \cdot 1 \neq 0$ для всех $n \geq 1$, то говорят, что поле K имеет характеристику 0: $\text{char } K = 0$

Если $\exists n \geq 1 : n \cdot 1 = 0$, то наименьшее такое положительное n называют характеристикой K

Примеры

1. $\text{char } \mathbb{Q} = 0, \quad \text{char } \mathbb{R} = 0, \quad \text{char } \mathbb{C} = 0$

2. p - простое $\text{char}(\mathbb{Z}/p\mathbb{Z}) = p$

Теорема

Характеристика поля либо 0, либо простое число

Док-во

1) не $\exists n \geq 1 \quad n \cdot 1 = 0 \Rightarrow \text{char } K = 0$

2) $\exists n : n \cdot 1 = 0$ возьмем наим. n и покажем, что n - простое

$$\square n \text{ - сост. } n = ab \quad 1 < a, b < n$$

$$0 = \underbrace{1 + \dots + 1}_n = (\underbrace{1 + \dots + 1}_a)(\underbrace{1 + \dots + 1}_b)$$

$$\Rightarrow \underbrace{1 + \dots + 1}_a = 0 \text{ или } \underbrace{1 + \dots + 1}_b = 0$$

противоречие с $\min n$

$$\Rightarrow n \text{ не сост.}; 1 \neq 0 \Rightarrow n \neq 1$$

$$\Rightarrow n \text{ - простое}$$

16 Производная многочлена. Свойства производной. Многочлены с нулевой производной.

Опр

K - поле, $f(x) \in K[x]$, $f(x) = \sum_{k=0}^n a_k x^k$

Тогда $f'(x) := \sum_{k=1}^n (k a_k) x^{k-1}$

$$k \cdot a_k = \underbrace{a_k \cdot \dots \cdot a_k}_k$$

Теорема (Свойства)

1. $(f + g)' = f' + g'$

$$f = \sum_{k=0}^n a_k x^k, \quad g = \sum_{k=0}^n b_k x^k, \quad f + g = \sum_{k=0}^n (a_k + b_k) x^k$$

$$\text{Действительно, } k(a_k + b_k) = k a_k + k b_k$$

2. $c \in K \quad (c \cdot f)' = c f'$

$$k(c a_k) = c(k a_k)$$

3. $(f \cdot g)' = f' g + g' f$ Док-во без $(\sum)'$:

(a) $f = x^n \quad g = x^m$

$$(x^{n+m})' = (n+m)x^{n+m-1}$$

$$(x^n)' x^m + x^n (x^m)' = n x^{n-1} \cdot x^m + m x^n \cdot x^{m-1} = (n+m)x^{n+m-1}$$

(b) $f = x^n \quad g = \sum_{k=0}^m a_k x^k$

$$(f \cdot g)' = \left(\sum_{k=0}^m a_k x^n x^k \right)' = \sum_{k=0}^m a_k (x^n \cdot x^k)' =$$

$$= \sum_{k=0}^m a_k ((x^n)' \cdot x^k + x^n (k x^{k-1})) =$$

$$(x^n)' \sum_{k=0}^m a_k x^k + x^n \left(\sum_{k=0}^m k a_k x^k \right) = f' g + f g'$$

(с) f, g - произвольные

$$f = \sum_{k=0}^n b_k x^k$$

$$\begin{aligned}(fg)' &= \sum_{k=0}^n b_k (x^k g)' = \left(\sum_k b_k \cdot k x^{k-1} \cdot g \right) + \left(\sum_k b_k x^k \cdot g' \right) = \\ &= f'g + fg'\end{aligned}$$

4. Ф-ла Лейбница

$$(f \cdot g)^{(k)} = \sum_{i=0}^k C_k^i f^{(i)} g^{(k-i)}$$

5. Если $\text{char } K = 0 \Rightarrow f' = 0 \Leftrightarrow f \in K$

Если $\text{char } K = p > 0$, то $f' = 0 \Leftrightarrow f \in K[x^p]$

$$(\text{т.е. } f = a_0 + a_p x^p + \dots + a_{kp} x^{kp})$$

Док-во

здесь когда-нибудь будет док-во

17 Теорема о кратности

Теорема

K - поле $\text{char} K = 0$

$f \in K[x]$ a - корень f кр. $l \geq 1$

Тогда a - корень f' кратности $l - 1$

Замечание

Если $\text{char} K = p > 0$, то теор. не верна

$\mathbb{Z}/p\mathbb{Z}$ $f = x^{2p+1}$ 0 - корень кр. p

$f' = (2p + 1)x^{2p} + px^{p-1} = x^{2p}$ 0 - корень кр. $2p$

Док-во (теоремы)

$f(x) = (x - a)^l \cdot g(x)$ $g(a) \neq 0$

$f' = l(x - a)^{l-1} \cdot g(x) + (x - a)^l \cdot g'(x) = (x - a)^{l-1}(lg(x) + (x - a)g'(x))$

a - корень f' кр $\geq l - 1$

$lg(a) + (a - a)g'(a) = l \cdot g(a) \neq 0$

a - корень f' кр $l - 1$

18 Интерполяционная задача. Существование и единственность решения.

Опр (интерполяционная задача)

K - поле. a_1, \dots, a_n - попарно различны, $y_1, \dots, y_n \in K$

Найти мн-н f , такой, что $f(a_i) = y_i$, где $i = 1..n$

Теорема

Для интерполяционной задачи:

$$\begin{array}{c|c} x & a_1 \dots a_n \\ \hline f & y_1 \dots y_n \end{array}$$

$\exists!$ решение f степени $< n$

Док-во

1) Единственность

f, h - решают одну и интер. задачу

$$\deg f, \deg h < n$$

$$\forall i = 1, \dots, n \quad f(a_i) = h(a_i) = y_i \Rightarrow f(a_i) - h(a_i) = 0$$

$f - h$ имеет $\geq n$ корней, а степ. $< n$

$$f - h = 0 \Rightarrow f = h$$

(теорема о числе корней мн-на)

2) Существование

$$f(x) = c_0 + c_1x + \dots + c_{n-1}x^{n-1}$$

$$c_0 + c_1a_i + \dots + c_{n-1}a_i^{n-1} = y_i$$

$$\begin{pmatrix} 1 & a_1 & a_1^2 & \dots & a_1^{n-1} \\ \vdots & & & & \vdots \\ 1 & a_n & a_n^2 & \dots & a_n^{n-1} \end{pmatrix} \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$A \begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

$$\det A = \prod_{j>i} (a_j - a_i) \neq 0 \quad \text{определитель Вандермонда}$$

A - обр.

$$\begin{pmatrix} c_0 \\ \vdots \\ c_{n-1} \end{pmatrix} = A^{-1} \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$$

19 Интерполяционный метод Ньютона.

Напоминание

Дана интерполяционная задача:

$$\begin{array}{c|c|c} x & a_1 & a_i \dots a_n \\ \hline f(x) & y_1 & y_i \dots y_n \end{array}$$

Опр (метод Ньютона)

Пусть f_{i-1} - интерпол. мн-н степени $\leq i-1$

и решающий интерпол. задачу для первых i точек

$f_0(x) = y_1$, где $f_0(a_1) = y_1$ - так можно задать начальный

\square построили f_{i-1} . Ищем f_i :

$(f_i - f_{i-1})(a_j) = 0 \quad j = 1, \dots, i$ - так должно быть

$$\Rightarrow f_i(x) = f_{i-1}(x) + c_i \cdot (x - a_1) \dots (x - a_i)$$

$\deg f_i \leq i$, найдем c :

$$y_{i+1} = f_i(a_{i+1}) = f_{i-1}(a_{i+1}) + c_i(a_{i+1} - a_1) \dots (a_{i+1} - a_i)$$

$$\Rightarrow c_i = \frac{y_{i+1} - f_{i-1}(a_{i+1})}{(a_{i+1} - a_1) \dots (a_{i+1} - a_i)}$$

20 Интерполяционный метод Лагранжа.

Опр

Хотим построить функцию, такую что:

$$\frac{x}{L_j(x)} \left| \begin{array}{c|c|c|c|c} a_1 & a_{j-1} & a_j & a_{j+1} & a_n \\ \hline 0 & 0 & 1 & 0 & 0 \end{array} \right.$$

Построим $M_j(x)$, который во всех точках кроме a_j равен 0:

$$M_j(x) := a_j(x - a_1) \dots (x - a_{j-1})(x - a_{j+1}) \dots (x - a_n)$$

$$L_j(a_j) = 1 \text{ - так должно быть}$$

$$L_j(x) := \frac{(x - a_1) \cdot \dots \cdot (x - a_{j-1})(x - a_{j+1}) \cdot \dots \cdot (x - a_n)}{(a_j - a_1) \cdot \dots \cdot (a_j - a_{j-1})(a_j - a_{j+1}) \cdot \dots \cdot (a_j - a_n)}$$

$$L_j(x) \text{ - интерп. мн-н Лагранжа}$$

$$L_j(a) = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases} \quad \begin{matrix} \deg L_j(x) = n - 1 \\ \deg f \leq n - 1 \end{matrix}$$

Теперь хотим решить интерполяционную задачу:

$$\frac{x}{f(x)} \left| \begin{array}{c|c} a_1 & a_n \\ \hline y_1 & y_n \end{array} \right.$$

$$f(x) = \sum_{j=1}^n y_j L_j(x) \quad f(a_i) = \sum_{j=1}^n y_j L_j(a_j) = y_i L_i(a_i) = y_i$$

Мн-н Лагранжа исп. в алгоритмах быстрого умножения

$\forall \varepsilon > 0 \quad \exists$ алг. умн., который для n -разрядных чисел требует $O(n^{1+\varepsilon})$ поразрядных операций

21 Делимость и ассоциированность в кольце многочленов над полем.

Опр

K - поле, $K[x]$

$f, g \in K[x]$ ассоциированы, если:

$$f \mid g \text{ и } g \mid f$$

Обозначение: $f \sim g$

Замечание

$$0 \sim 0$$

0 с другими не ассоц.

Док-во

$$f \neq 0 \quad g \neq 0 \quad f \mid g \quad g \mid f$$

$$\deg f \leq \deg g \quad \deg g \leq \deg f$$

$$\Rightarrow \deg f = \deg g$$

$$f = c \cdot g \quad c \in K^* = K \setminus \{0\}$$

$$0 = 1 \cdot 0$$

$$\text{Если } f = c \cdot g, c \in K^* \quad g = c^{-1}f \Rightarrow g \mid f, \quad f \mid g$$

Следствие

$$f \sim g \Leftrightarrow \exists c \in K^* \quad f = cg$$

Если $f \neq 0$, то в классе ассоц. с f мн-нов всегда можно выбрать мн-ен со старшим коэф 1.

Мн-н со старшим коэф. 1 называется унитарным, приведенным

Замечание

$$f \mid g \quad f \sim f_1 \quad g \sim g_1 \Rightarrow f_1 \mid g_1$$

Док-во

$$g = f \cdot h$$

$$cg = f(ch)$$

$$g = (cf)(c^{-1}h)$$

22 Наибольший общий делитель в кольце многочленов над полем.

Существование и линейное представление.

Опр

K - поле, $K[x]$, $f_1, \dots, f_n \in K[x]$

Тогда $g = \text{НОД}(f_1, \dots, f_n)$, если:

$$g \mid f_1, \dots, g \mid f_n$$

$$\text{И } \forall h \quad (h \mid f_1, \dots, h \mid f_n) \Rightarrow h \mid g$$

Замечание

НОД опред. не однозначно, а с точностью до ассоц.

$$\text{НОД}(0, \dots, 0) = 0$$

Если хотя бы один $f_1 \dots f_n \neq 0$, то в классе ассоц. с НОД можно выбрать приведенный

Теорема

$$\forall f_1, \dots, f_n \in K[x]$$

Тогда существует $g = \text{НОД}(f_1, \dots, f_n)$ и он допускает лин. предствление:

$$g = f_1 h_1 + \dots + f_n h_n \text{ для некоторых } h_1 \dots h_n \in K[x]$$

Док-во

$$1) f_1 = f_2 = \dots = f_n = 0 \quad \text{НОД}(0, \dots, 0) = 0$$

$$\text{Положим } h_1 = \dots = h_n = 1$$

$$2) \exists i \quad f_i \neq 0$$

$$I = \{f_1 h_1 + \dots + f_n h_n : h_1 \dots h_n \in K[x]\}$$

$$I \neq \{0\} \quad 0 \neq f_i \in I$$

Пусть g - мн-ен наим. степени в $I \setminus \{0\}$

Утверждается, что $g = \text{НОД}(f_1, \dots, f_n)$

$$f_j = g \cdot u_j + r_j \quad r_j = 0 \text{ или } \deg r_j < \deg g$$

$$r_j = -g \cdot u_j + f_j = -h_1 u_j f_1 - h_2 u_j f_2 + (-h_j u_j + 1) f_j - \dots$$

$$g = h_1 f_1 + \dots + h_n f_n \quad r_j \in I$$

Т.к. степ. g - наименьшая в $I \setminus \{0\}$:

$$\deg r_j < \deg g, \text{ то } r_j = 0$$

$$f_j = gu_j \quad g \mid f_j \quad j = 1, \dots, n$$

$$h \mid f_i, \dots, h \mid f_n$$

$$g = (\underbrace{f_1 h_1}_{\ddot{h}} + \dots + \underbrace{f_n h_n}_{\ddot{h}}) : h \Rightarrow h \mid g$$

23 Взаимно простые многочлены. Свойства взаимно простых многочленов. Если многочлен делит произведение двух многочленов и взаимно прост с первым сомножителем, то он делит второй сомножитель.

Опр

$f_1, \dots, f_n \in K[x]$ назыв. взаимно простыми, если $\text{НОД}(f_1, \dots, f_n) \sim 1$

Теорема (Свойства НОД)

1. $\text{НОД}(f, 0) \sim 1$
2. $\text{НОД}(f_1, \dots, f_n) = \text{НОД}(\text{НОД}(f_1, \dots, f_n), f_n)$
3. Если $g \sim \text{НОД}(f_1, \dots, f_n)$ (не все $f_i = 0$)

то $\frac{f_1}{g}, \dots, \frac{f_n}{g}$ - взаимно просты

4. $\text{НОД}(f, g) \sim \text{НОД}(f - gh, g)$
5. f_1, \dots, f_n - вз. просты $\Leftrightarrow 1$ допускает лин. представление

$$1 = h_1 f_1 + \dots + h_n f_n \quad h_i, \dots, h_n \in K[x]$$

Док-во

См. док-ва для \mathbb{Z} (Спасибо, Всемиров)

Теорема

$f \mid gh$ и f и g - вз. просты $\Rightarrow f \mid h$

Док-во

$$\exists u, v \in K[x]$$

$$fu + gv = 1$$

$$\underbrace{fuh + ghv}_{\ddot{f}} = h \Rightarrow h \overset{\cdot}{:} f$$

24 Неприводимые многочлены. Теорема о разложении многочлена в произведение неприводимых (существование).

Утв

K - поле $\Rightarrow K[x] = \{0\} \cup K^* \cup \{\text{мн-ны ст. } \geq 1\}$

т.к. обратимые эл-ты в кольце мно-ов - константы

Опр

$f \in K[x] \setminus K$ называются составными (или приводимым), если

$$f = gh \quad 1 \leq \deg g, \deg h < \deg f$$

В противном случае f - назыв. неприводимым

f - неприводим, если $f = gh \Rightarrow \deg h = 0$ или $\deg g = 0$

Опр

f - неприв. \Leftrightarrow все делители f - это константы и мн-ны $\sim f$

Примеры

1. $x - a$ неприводим при любом a

2. $x^2 + 1$ неприводим в $\mathbb{R}[x]$

3. $x^2 + 1$ в $\mathbb{C}[x]$ приводим: $x^2 + 1 = (x + i)(x - i)$

4. В $\mathbb{R}[x]$ $(x^2 + 1)(x^2 + 2)$ - приводим, но корней нет

5. Если $\deg f \geq 2$ есть корень в K , то f - приводим в $K[x]$
 $f = (x - a)g$ (по т. Безу)

Обратное неверно. Но для мн-нов степени 2 и 3 неприводимость в $K[x]$ равносильна отсутствию корней в K

Теорема

$f \in K[x]$ f - неприводим

$$f \mid g_1 \cdot \dots \cdot g_n \Rightarrow \exists i : f \mid g_i$$

Док-во

$n = 1$:

$f \mid g$ - доказано

$n = 2$:

$$f \mid g_1 g_2$$

Если $f \mid g$ - всё доказано

Пусть $f \nmid g_1$. Общие делители f и g - константы

$\text{НОД}(f, g_1) = 1$, по теореме из предыдущего билета, $f \mid g_2$

$n \geq 3$ (индукция по n):

$$f \mid (g_1 \dots g_{n-1}) g_n$$

Аналогично $f \mid g_n$ или $f \mid g_1 \dots g_{n-1}$

$$\Rightarrow \exists i : f \mid g_i$$

Теорема (алгоритм Евклида в $K[x]$)

$$f, g \in K[x], r_0 = f, r_1 = g$$

До тех пор пока $r_i \neq 0$

$$r_{i-1} = r_i q_i + r_{i+1} \quad \deg r_{i+1} < \deg r_i$$

Последний ненулевой остаток - это $\text{НОД}(r_0, r_1)$

Теорема (основная теорема арифметики в кольце многочленов)

Всякий ненулевой $f \in K[x]$ может быть представлен в виде

$$c \cdot \prod_{i=1}^n g_i$$

$c \in K^*$, а все g_i - приведенные неприводимые мн-ны. Причем такое произведение ед. с точностью до порядка сомножителей.

Замечание

$$\text{Для } f = c \in K^* \quad n = 0$$

Лемма (1)

Всякий $f: \deg f \geq 1$ делится хотя бы на один неприводимый.

Док-во

f - непр - все доказано

Если приводим, то $f = f_1 \cdot g_1 \quad 1 \leq \deg f_1 < \deg f$

Если f_1 неприв, то делитель найден

Если приводим $f_1 = f_2 g_2 \quad q \leq \deg f_2 \leq \deg f_1$

$\deg f > \deg f_1 > \dots \Rightarrow$ процесс оборвется

\Rightarrow найдем неприв. делитель f

Док-во (Существование)

Индукция по $\deg f$:

$\deg f = 0$:

$$f = c \in K^* \quad f = c \cdot \left(\prod_{i=1}^0 g_i \right)$$

Инд. переход $\deg f > 0$:

По лемме \exists неприв. g_1 : $g_1 \mid f$

Не умоляя общности g_1 - приведенный (с коэф. 1)

$$f = g_1 f_1 \quad \deg f_1 < \deg f - \deg g_1 < \deg f$$

По инд. предп.

$$f_1 = c \prod_{i=2}^n g_i \quad g_i - \text{приведенный неприводимый}$$

$$f = f_1 g_1 = c \prod_{i=1}^n g_i$$

25 Теорема о разложении многочлена в произведение неприводимых (единственность).

Теорема (основная теорема арифметики в кольце многочленов)

Всякий ненулевой $f \in K[x]$ может быть представлен в виде

$$c \cdot \prod_{i=1}^n g_i$$

$c \in K^*$, а все g_i - приведенные неприводимые мн-ны. Причем такое произведение ед. с точностью до порядка сомножителей.

Док-во (единственность)

$$(*) \quad f = c \prod_{i=1}^n g_i = \tilde{c} \prod_{i=1}^m \tilde{g}_i$$

$$\Rightarrow n = m \quad c = \tilde{c} \text{ иначе перенумеруем сомнож. } g_i = \tilde{g}_i$$

Не умоляя общ. $n \leq m$

Индукция по n . База инд.:

$$n = 0 \quad c = \tilde{c} \prod_{i=1}^n \tilde{g}_i \Rightarrow m = 0 \quad \tilde{c} = c$$

Инд. переход:

$$g_n \mid \tilde{c} \prod_{i=1}^m \tilde{g}_i \Rightarrow \exists i \quad g_n \mid \tilde{g}_i$$

$$\tilde{c} \neq 0$$

Не умоляя общности $i = m$ (иначе перенумеруем)

$$g_n = \widetilde{g_m}$$

В $(*)$ сократим на g_n

$$c \prod_{i=1}^{n-1} g_i = \tilde{c} \prod_{i=1}^{m-1} \tilde{g}_i \quad n-1 \leq m-1$$

По инд. предп. $n-1 = m-1 \quad (\Rightarrow n = m)$

$$c = \tilde{c} \text{ (после перенумерования)}$$

$$g_i = \tilde{g}_i \quad i = 1, \dots, n-1$$

$$g_n = \tilde{g}_n$$

26 Алгебраически замкнутые поля. Эквивалентные переформулировки. Алгебраическая замкнутость поля комплексных чисел. (б.д.)

Теорема

$\square K$ - поле, рассмотрим $K[x]$

Следующие условия равносильны

1. Все неприводимые в $K[x]$ - это в точности линейные мн-ны
2. Всякий мн-н $f \in K[x]$, $\deg f > 0$ раскладывается в произведение лин. множителей
3. Всякий $f \in K[x]$, $\deg f > 0$ делится на линейный
4. Всякий $f \in K[x]$, $\deg f > 0$ имеет в K хотя бы 1 корень
5. Всякий $f \in K[x]$, $\deg f > 0$ имеет в K в точности $n = \deg f$ корней с учетом кратности

Опр

Если для K и $K[x]$ выполнено любое из равносильных условий теоремы, то K называется алгебраически замкнутым

Док-во

$(1 \Rightarrow 2)$:

$$f \in K[x], \deg f > 0 \quad f \stackrel{\text{т-ма о разлож.}}{=} c \prod_{i=1}^n g_i, \quad g_i - \text{непр. мн-ль}$$

(неприводимые - линейные)

$(2 \Rightarrow 1)$:

Если $\deg f > 1$, то тогда f - неприводим и произв. лин. сомножителей

$$f = lh, \quad \deg l = 1, \quad \deg h = \deg f - 1 \geq 1$$

(линейные - неприводимые)

$(2 \Rightarrow 3)$:

2 формально сильнее 3

$(3 \Rightarrow 2)$:

Индукция по $\deg f$:

$\deg f = 1$ - утверждение верно

$\deg f > 1 \quad \exists l \in K[x] : \deg l = 1$

$f = lh \quad \deg h = \deg f - 1 \geq 1$

(по инд. предп. раскл. в произв. линейных)

(3 \Leftrightarrow 4):

По теореме Безу $(x - c) \mid f \Leftrightarrow f(c) = 0$

(5 \Rightarrow 4):

Есть n корней с учетом кратности $\Rightarrow_{\deg f \geq 1} 1$

(2 \Rightarrow 5):

$$f = \prod_{i=1}^k (x - a_i)^{d_i}, \quad a_i \text{ попарно различны}$$

$$\sum_{i=1}^k d_i = \deg f = n$$

a - корень f кр. $d_i \Rightarrow$ число корней f с учетом кр. $\geq n = \deg f$

Но число корней f с учетом кратности есть $\deg f$

Примеры

1. \mathbb{R}, \mathbb{Q} не алг. замкнуты
2. Любое конечное поле не алг. замкнуто
3. $|F| = q \quad \deg f = n > q$

Замечание

В 3 семестре докажем, что над конечным полем есть неприводимые любой заданной степени

Теорема (без д-ва)

\mathbb{C} - алг. замк.

Следствие

$$f \in \mathbb{C}[x], \quad \deg f > 0$$

$$f = c \prod_{i=1}^k (x - a_i)^{d_i} \quad a_i, c \in \mathbb{C}$$

27 Неприводимые многочлены над полем вещественных чисел. Теорема о разложении многочлена с вещественными коэффициентами в произведение неприводимых над \mathbb{R} .

Пример

Неприводимы:

$$x - c, \quad c \in \mathbb{R}$$

$$x^2 + ax + b \quad a^2 - 4b < 0 \quad a, b \in \mathbb{R} \text{ (нет вещ. корней)}$$

Теорема

Всякий неприв. в $\mathbb{R}[x]$ ассоциирован с линейным или с квадратичным с отриц. дискриминантом

Следствие

$$f \in \mathbb{R}[x] \quad f \neq 0$$

$$f = c \prod_{i=1}^m (x - c_i)^{d_i} \prod_{j=1}^k (x^2 + a_j x + b_j)^{l_j} \quad a_j^2 - 4b_j < 0$$

Лемма

$$f \in \mathbb{R}[x] \subseteq \mathbb{C}[x]$$

Если $z \in \mathbb{C}$ - корень f , то \bar{z} - корень f

Док-во (леммы)

$$f = a_0 + a_1 x + \dots + a_n x^n$$

$$a_0 + a_1 z + \dots + a_n z^n = 0$$

$$\Rightarrow \overline{a_0 + a_1 z + \dots + a_n z^n} = \bar{0} = 0 \text{ (сопряжение)}$$

$$= \overline{a_0} + \overline{a_1 z} + \dots + \overline{a_n z^n} = a_0 + a_1 \bar{z} + \dots + a_n (\bar{z})^n = f(\bar{z})$$

Док-во (теоремы)

Осталось показать, что все остальные f с $\deg f > 0$ - неприводимы $\deg f = 2$:

$$D = 0 \Rightarrow f = a(x - c)^2$$

$$D > 0 \Rightarrow f = a(x - c_1)(x - c_2), \quad c_1, c_2 \in \mathbb{R}$$

$\deg f \geq 3$:

Посмотрим на него, как на мн-н с компл.(?) коэффициентами

$$f \in \mathbb{C}[x] \quad z - \text{корень в } \mathbb{C}$$

а) $z \in \mathbb{R}$

$$\text{По теор. Безу } f(z) = 0 \quad f(x) = (x - z)h \quad h \in \mathbb{R}[x], \deg h \geq 2$$

б) $z \in \mathbb{C} \setminus \mathbb{R}$

$$\bar{z} \neq z$$

$$f(x) = (x - z)h_1 = (x - z)(x - \bar{z})h$$

$$\bar{z} - \text{корень } f \quad (\bar{z} - z) \neq 0 \Rightarrow \bar{z} - \text{корень } h_1$$

$$(x - z)(x - \bar{z}) = x^2 - (z + \bar{z})x + z\bar{z} = x^2 - 2 \underset{\in \mathbb{R}}{\operatorname{Re} z} x + \underset{\in \mathbb{R}}{|z|^2} \rightarrow \in \mathbb{R}[x]$$

$$D = 4(\operatorname{Re} z)^2 - |z|^2 = -4(\operatorname{Im} z)^2 < 0 \quad (\text{т.к. } z - \text{ чисто компл. число})$$

$$g(x) = x^2 - 2 \operatorname{Re} z x + |z|^2$$

$$f(x) = g(x)h(x)$$

$$\deg h = \deg f - 2 \geq 1$$

$$fg \in \mathbb{R}[x], \text{ поделим с остатком в } \mathbb{R}[x]:$$

$$f = gq + r \quad r = 0 \text{ или } \deg r \leq 1$$

Это равенство также верно и в $\mathbb{C}[x]$:

$$\left. \begin{array}{l} f = gq + r \\ f = gh + 0 \end{array} \right| \Rightarrow r = 0 \quad h = q \in \mathbb{R}[x]$$

28 Поле частных области целостности. Поле частных кольца многочленов (поле рациональных функций).

Опр

R - комм. кольцо с 1, о.ц.

Хотим построить поле K , содержащее подкольцо изоморфное R , состоящее из "дробей"

$$X = R \times (R \setminus \{0\}) = \{(a, b) : a \in R, b \in R, b \neq 0\}$$

На X введем отношение эквивалентности:

$$(a, b) \sim (c, d) \text{ если } ad = bc$$

УТВ

\sim - отношение эквив.

Док-во

1. $(a, b) \sim (a, b)$, т.к. $ab = ba$
2. $(a, b) \sim (c, d) \Rightarrow (c, d) \sim (a, b)$
3. $\begin{matrix} (a, b) \sim (c, d) \\ (c, d) \sim (e, f) \end{matrix} \xrightarrow{?} (a, b) \sim (e, f)$

$$\Leftrightarrow \begin{matrix} ad = bc \\ cf = dc \end{matrix} \xrightarrow{?} af = be$$

Чтобы не поделить на 0 при сокращении сделаем так:

$$\begin{matrix} adf = bcf \\ bcf = bde \end{matrix} \Rightarrow adf = bde \Rightarrow d(af - be) = 0 \Rightarrow af - be = 0$$

Опр

$$\frac{a}{b} = [(a, b)] - \text{класс эквив.}$$

$K = X_{/\sim}$ На K введем структуру поля

$$\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \quad b \neq 0 \quad d \neq 0 \Rightarrow bd \neq 0 \quad (ac, bd) \in X$$

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \quad (ad + bc, bd) \in X$$

Док-во (корректность определения)

Корректность определения - это независимость от выбора представителя в классе

$$\frac{a}{b} = \frac{a_1}{b_1} \quad \frac{c}{d} = \frac{c_1}{d_1} \quad \begin{array}{l} ab_1 = ba_1 \\ cd_1 = dc_1 \end{array}$$

$$b \neq 0, \quad d \neq 0 \Rightarrow bd \neq 0$$

Надо убедиться, что $(ac, bd) \sim (a_1c_1, b_1d_1)$

$$acb_1d_1 = bda_1c_1$$

$$?(ad + bc, bd) \sim (a_1d_1 + b_1c_1, b_1d_1)$$

$$?adb_1d_1 + bcb_1d_1 = bda_1d_1 + bdb_1c_1$$

Получится, если:

$$\begin{array}{l} ab_1 = ba_1 \quad | \cdot dd_1 \\ + \\ cd_1 = dc_1 \quad | \cdot bb_1 \end{array}$$

Теорема

$K, +, \cdot$ - поле

Док-во

Ассоциативность сложения, коммутативность умножения - упр.

Нулевой элемент:

$$0_K = \frac{0}{1} = \{(0, b) : b \in R \setminus \{0\}\} = \frac{0}{b}$$

$$(a, b) = \frac{0}{1} \Rightarrow a \cdot 1 = b \cdot 0$$

Проверим, что это действительно ноль:

$$\frac{a}{b} + \frac{0}{1} = \frac{a \cdot 1 + b \cdot 0}{b} = \frac{a}{b}$$

$$-\frac{a}{b} = \frac{-a}{b} \text{ - обр. элемент}$$

Ассоциативность умн., дистрибутивность - упр.

$$1_K = \frac{1}{1} = \{(a, a) : a \neq 0\} = \frac{a}{a}$$

$$(a, b) \in \frac{1}{1} \quad (a, b) \sim (1, 1) \Rightarrow a \cdot 1 = b \cdot 1 \Rightarrow a = b$$

$$\frac{a}{b} \cdot \frac{1}{1} = \frac{a \cdot 1}{b \cdot 1} = \frac{a}{b}$$

$$\frac{a}{b} \neq 0_k \Rightarrow a \neq 0 \Rightarrow (a, b) \in X$$

$$\frac{a}{b} \cdot \frac{b}{a} = 1_K$$

Осталось убедиться, что поле K содержит кольцо, изоморфное R

$$\varphi: R \rightarrow K \quad r \mapsto \frac{r}{1}$$

$$\varphi(r_1 + r_2) = \frac{r_1 + r_2}{1}$$

$$\varphi(r_1) + \varphi(r_2) = \frac{r_1}{1} + \frac{r_2}{1} = \frac{r_1 + r_2}{1}$$

$$\varphi(r_1 \cdot r_2) = \frac{r_1 \cdot r_2}{1}$$

$$\varphi(r_1) \cdot \varphi(r_2) = \frac{r_1}{1} \cdot \frac{r_2}{1} = \frac{r_1 \cdot r_2}{1}$$

Осталось убедиться, что отображение φ - сюръективно

$$\varphi(r_1) = \varphi(r_2) \Rightarrow \frac{r_1}{1} = \frac{r_2}{1} \Rightarrow (r_1, 1) \sim (r_2, 1) \Rightarrow r_1 \cdot 1 = r_2 \cdot 1 \Rightarrow r_1 = r_2$$

Значит $\varphi(R) \subset K$ и φ задаёт биекцию между R и $\varphi(R)$ - изоморфизм

Будем отождествлять $\varphi(R)$ и R

Опр

Поле K назыв. полем частных кольца R

Примеры

\mathbb{Q} - поле частных \mathbb{Z}

$K[x]$ - о.ц

Поле частных $K[x]$ обознач. $K(x)$ и назыв. полем рац. дробей или полем рац. функций

Рац. функ. не есть функции в смысле отобр.

29 Простейшие дроби. Разложение рациональной функции в сумму многочлена и простейших дробей. (существование).

Опр

$K(x)$, K - поле

$$0 \neq \frac{f}{g} \in K(x) \quad f, g \in K[x]$$

$\frac{f}{g}$ - правильная, если $\deg f < \deg g$

Лемма (1)

$$\frac{f}{g}; \quad \frac{f_1}{g_1} \text{ - прав. дроби} \Rightarrow \frac{f}{g} \cdot \frac{f_1}{g_1}; \quad \frac{f}{g} + \frac{f_1}{g_1} \text{ - прав. дроби}$$

Док-во

$$\deg(f \cdot f_1) = \deg f + \deg f_1 < \deg g + \deg g_1 = \deg(g \cdot g_1)$$

$$\frac{f}{g} + \frac{f_1}{g_1} = \frac{fg_1 + gf_1}{gg_1}$$

$$\deg(fg_1 + gf_1) \leq \max\{\deg(fg_1), \deg(gf_1)\} < \deg(gg_1)$$

$$\deg(fg_1) = \deg f + \deg g_1 < \deg g + \deg g_1 = \deg(gg_1)$$

$$\deg(gf_1) = \deg g + \deg f_1 < \deg g + \deg g_1 = \deg(gg_1)$$

Опр

Правильная дробь $\frac{f}{g}$ называется примарной, если $g = q^a$, q - неприв. многочлен

$$\frac{f}{g} = \frac{f}{q^a} \quad \deg f < a \deg q$$

Опр

Дробь назыв. простейшей, если она имеет вид

$$\frac{f}{q^a} \quad q \text{ - неприв } a \geq 1$$

$$\deg f < \deg q$$

Теорема

$\frac{f}{g} \in K(x)$, тогда $\frac{f}{g}$ ед. образом (с точностью до порядка слагаемых)

представима в виде суммы многочлена и простейших дробей

Лемма (2)

$\frac{f}{g} \in K(x)$ Тогда $\frac{f}{g} = h + \frac{f_1}{g}$, $h \in K(x)$, $\frac{f_1}{g}$ - прав дробь

Док-во

Делим с остатком: $f = gh + f_1$, $\deg f_1 < \deg g$

$\frac{f}{g} = h + \frac{f_1}{g}$ $\frac{f_1}{g}$ - прав. дробь

Лемма (3)

$\frac{f}{g}$ - прав. дробь, $g = g_1 \cdot g_2$, $\text{НОД}(g_1, g_2) = 1$

Тогда $\frac{f}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$, $\frac{f_1}{g_1}, \frac{f_2}{g_2}$ - прав. дроби

Док-во

По теореме о линейном представлении НОДв $K[x]$

$\exists u_1, u_2 \in K[x] : gu_1 + gu_2 = 1$

$g_1(u_2f) + g_2(u_1f) = f$

$u_1f = g_1h_1 + f_1$ $\deg f_1 < \deg g_1$

$f = g_1(u_2f) + g_2(u_1f) = g_1(u_2f) + g_2(g_1h_1 + f_1) =$

$= g_1(u_2f + g_2h_1) + g_2f_1 \Leftrightarrow \frac{f}{g} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$ $\frac{f_1}{g_1}, \frac{f_2}{g_2}$ - прав. дроби

Лемма (4)

Всякая правильная дробь есть сумма примарных

Док-во

$\frac{f}{g}$ н.у.о. старш. коэф. g равен 1

$$g = \prod_{i=0}^k q_i^{a_i}, \quad q_i - \text{попарно различные неприводимые со ст. коэф. 1}$$

Индукция по k :

$$k = 1 \quad \deg f < \deg q_1^{a_1}, \quad \text{т.к. дробь правильная}$$

$$\frac{f}{g} = \frac{f}{q_1^{a_1}} - \text{примарная}$$

Индукционный переход $k \rightarrow k+1, k \geq 2$

$$\frac{f}{g} = \frac{f}{q_1^{a_1} \dots q_k^{a_k}}$$

q_k - вз. просты с $q_1, \dots, q_{k-1} \Rightarrow$ вз. пр. с $q_1^{a_1}, \dots, q_k^{a_k} \Rightarrow q_k^k$ тоже вз. пр. с ними

По лемме 3:

$$\frac{f}{g} = \frac{F}{q_1^{a_1} \dots q_{k-1}^{a_{k-1}}} + \frac{f_k}{g_k^{a_k}} - \text{примарная}, \quad \deg f_k < a_k \deg q_k$$

По инд. предп. 1-е слагаемое есть сумма примарных.

Лемма (5)

Всякая примарная есть сумма простейших

Док-во

здесь когда-нибудь будет док-во

Док-во (существование)

По теореме о линейном представлении НОД в $K[x]$

$$\exists u_1, u_2 \in K[x]$$

$$g_1 u_2 + g_2 u_1 = 1 \mid \cdot f$$

$$g_1(u_2 f) + g_2(u_1 f) = f$$

$$g_2(u_1 f) = f - g_1(u_2 f)$$

$$u_1 f = g_1 h_1 + f_1 \quad (\text{делим с остатком})$$

$$f = g_1(u_2f) + g_2(u_1f) = g_1(u_2f) + g_2(g_1h_1 + f_1) = g_1 \underbrace{(u_2f + g_2h_1)}_{=f_2} + g_2f_1 =$$

$= g_1f_2 + g_2f_1$ - надо убедиться, что правильное

$$g_1f_2 = f - g_2f_1$$

$$\deg g_1 + \deg f_2 \leq \max\{\deg f; \deg g_2 + \deg f_1\} < \deg g_1 + \deg g_2$$

$$\deg f_2 < \deg g_2$$

$$\frac{f}{g} = \frac{f_2}{g_2} + \frac{f_1}{g_1}$$

30 Разложение рациональной функции в сумму многочлена и простейших дробей. (единственность).

Теорема

$\frac{f}{g} \in K(x)$ тогда $\frac{f}{g}$ ед. образом (с точностью до порядка слагаемых) представима в виде суммы многочлена и простейших дробей

Док-во (единственность)

Не умоляя общности можно считать, что в обоих разложениях одни и те же неприводимые

$$\frac{f}{g} = h + \sum_{i=1}^k \sum_{j=1}^{a_i} \frac{f_{ij}}{q_i^j}, \deg f_{ij} < \deg q_i = \tilde{h} + \sum_{i=1}^k \sum_{j=1}^{a_i} \frac{\widetilde{f_{ij}}}{q_i^j}, \deg \widetilde{f_{ij}} < \deg q_i$$

Не умоляя общности a_i одни и те же в обеих суммах.

$$h - \tilde{h} - \sum_{i=1}^k \sum_{j=1}^{a_i} \frac{f_{ij} - \widetilde{f_{ij}}}{q_i^j} = 0 \quad (*)$$

Положим не все $f_{ij} - \widetilde{f_{ij}} = 0 \Rightarrow \exists i, j : f_{ij} - \widetilde{f_{ij}} \neq 0$

Для такого i выберем наибольшее j из возможных. В $(*)$ наиб. степени q_i в дроби с ненулевым числителем равна q_i^j

Домножим $(*)$ на общее кратное знаменателей НОК = $q_i^j \cdot ()$ - произв. ост q в каких-то степенях

$$q_i(\dots) + q_i(\dots) + (f_{ij} - \widetilde{f_{ij}}) = 0 \Rightarrow$$

$$\deg(f_{ij} - \widetilde{f_{ij}}) \leq \max(\deg f_{ij}, \deg \widetilde{f_{ij}}) < \deg q_i$$

$$f_{ij} - \widetilde{f_{ij}} = 0?! \Rightarrow \text{в } (*) \text{ все } f_{ij} = \widetilde{f_{ij}}, \quad h = \tilde{h}$$

Пример *здесь когда-нибудь будет пример* !!! (начал писать, не закончил)

$$\frac{f}{q^a}, \quad q - \text{неприводимый}, \quad \frac{f}{q^a} - \text{правильная}$$

$$\frac{f}{q^a} = \frac{f_0}{q^a} + \frac{f_1}{q^{a-1}} + \dots + \frac{f_{a-1}}{q}$$

$$\frac{f_0 + f_1 q + \dots + f_{a-1} q^{a-1}}{q^a}$$

$$f = f_0 + f_1 q + \dots + f_{a-1} q^{a-1}$$

В частном случае:

1. $q = x - c$ Получим разложение f по степеням $x - c$

$$\frac{f}{(x - c)^a} \quad \text{раскл. } f \text{ по степеням } x - c \text{ и делим на } (x - c)^a$$

2. $g(x) = (x - c_1) \dots (x - c_k)$, c_k - попарно разл.

$$\frac{f}{g} \quad \deg f < \deg g = k$$

x	c_1	c_2	\dots	c_k
y	$f(c_1)$	$f(c_2)$	\dots	$f(c_k)$

Решение этой задачи - мн-н f

$$f(x) = \sum_{i=1}^k f(c_i) \frac{(x - c_1) \dots (x - c_k)}{(c_i - c_1) \dots (c_i - c_{i-1})(c_i - c_{i+1}) \dots (c_i - c_k)}$$

$$g^l(x) =$$

31 Факториальные кольца. Содержание многочлена над факториальным кольцом. Содержание произведения многочленов.

Опр

*здесь когда-нибудь будет определение

Утв

здесь когда-нибудь будет предложение

Док-во

здесь когда-нибудь будет док-во

Опр

R - о.ц

$$a \notin \{0\} \cup R^*$$

назыв неприводимым, если

$$a = bc \Rightarrow b \in R^* \text{ и } c \sim a$$

$$\text{или } c \in R^* \text{ и } b \sim a$$

(все делители a есть либо обр. элем R либо ассоц. с a)

Опр

О.ц. R называется факториальным кольцом, если в нем справедлива т-ма об однозначном разложении на множ., а именно, всякий ненулевой необр. элемент R есть произведение неприводимых элементов, причем это разложение ед. с точностью до порядка сомножителей и ассоциированности

$$a = p_1 \cdot \dots \cdot p_n = q_1 \cdot \dots \cdot q_m \quad q_i, p_i - \text{неприв} \Rightarrow n = m \text{ и}$$

$$\exists \text{ биекция } \sigma \text{ на } \{1, \dots, n\}$$

$$p_i = q_{\sigma(i)}$$

$$\mathbb{Z}, K[x] - \text{факт. кольца}$$

В факториальных кольцах можно определить НОД

$$a = \varepsilon_1 \prod_{i=1}^k q_i^{k_i} \quad b = p_1 \prod_{i=1}^n q_i^{l_i} \quad \varepsilon_1, p_1 \in R^* \quad q_i - \text{попарно ассоц. неприв}$$

$$\text{НОД}(a, b) = \prod_{i=1}^n q_i^{\min(k_i, l_i)}$$

$$ab = \varepsilon_1 p_1 \prod_{i=1}^n q_i^{(k_i + l_i)}$$

Пример

здесь когда-нибудь будет пример

Опр

Содержание многочлена f

$$\text{cont}(f) = \text{НОД}(a_1, a_2, \dots, a_n)$$

Опр

$f \in R[x]$ называется примитивным, если $\text{cont}(f) \sim 1$

В факториальном кольце \forall многочлен $f \in R[x]$ можно записать как $f(x) = \text{cont}(f) \cdot f_1$ - примитивный *здесь когда-нибудь будет дописана теория*

Лемма (Гаусса)

$$\text{cont}(f \cdot g) = \text{cont}(f) \cdot \text{cont}(g)$$

здесь когда-нибудь будет исправлена лемма

Док-во

здесь когда-нибудь будет док-во

**32 Теорема Гаусса о факториальности кольца многочленов
над факториальным кольцом. Факториальность колец**
 $K[x_1, \dots, x_n], \mathbb{Z}[x_1, \dots, x_n]$

Теорема

R - факториальное кольцо $\Rightarrow R[x]$ - факториальное

Лемма (Гаусса)

$f, g \in R[x]$ f, g - примитивны $\Rightarrow f \cdot g$ - примитивный

Док-во (теоремы)

здесь когда-нибудь будет док-во

Следствие

$\mathbb{Z}[x_1, \dots, x_n], K[x_1, \dots, x_n]$ - факториальны

33 Неприводимость над \mathbb{Q} и над \mathbb{Z} . Методы доказательства неприводимости многочленов с целыми коэффициентами (редукция по одному или нескольким простым модулям).

$$f \in \mathbb{Q}[x]$$

Хотим доказать, что f неприв над \mathbb{Q}

Не умоляя общности $f \in \mathbb{Z}[x]$ (можно домножить на знаменатель)

$\text{cont}(f) = 1$ коэфф. в совокупности вз. просты

Идея:

$$f = a_0 + \dots + a_n x^n$$

p - простое $p \nmid a_n$

$$\mathbb{Z}[x] \rightarrow \mathbb{Z}/p\mathbb{Z}[x]$$

каждый коэфф. заменяем на соотв. вычет

$$f \rightarrow \bar{f} = [a_0] + \dots + [a_n] \cdot x^n$$

Если $p \nmid a_n$ $\deg(\bar{f}) = \deg f$

Если f приводим над \mathbb{Q} , то по т. Гаусса

$$f = gh \quad g, h \in \mathbb{Z}[x]$$

$$\deg g, \deg h < \deg f$$

$$\bar{f} = \bar{g} \cdot \bar{h}$$

Если p не делит страш. коэфф f , то $p \nmid$ страш. коэфф. g и h

$$\deg \bar{g} = \deg g \quad \text{и} \quad \deg \bar{h} = \deg h$$

Тогда приводимость f влечет приводимость \bar{f}

Предположение

$$\text{Если } p \nmid a_n \quad f = a_0 + \dots + a_n x^n \quad \text{cont } f = 1$$

и \bar{f} - неприводим над $\mathbb{Z}/p\mathbb{Z}$, то f неприводим над $\mathbb{Z} (\Rightarrow$ и над $\mathbb{Q})$

Примеры

здесь когда-нибудь будут примеры

34 Критерий неприводимости Эйзенштейна.

Теорема

$$f \in \mathbb{Z}[x] \quad f = a_0 + a_1x + \dots + a_nx^n \quad \text{cont}(f) = 1$$

p - простое

Если $*p \nmid a_n$

$*p \mid a_i \quad i = 0, \dots, n-1$, то f неприводим над $\mathbb{Z} (\Rightarrow$ и над $\mathbb{Q})$

$*p^2 \nmid a_0$

Док-во

$$\square f = gh \quad g, h \in \mathbb{Z}[x] \quad \deg g, \deg h < n$$

$$\bar{f} = \bar{g} \cdot \bar{h}$$

$$\bar{f} = [a_n]x^n$$

$$\bar{g} \sim x^m \quad \bar{h} \sim x^{n-m} \quad 0 < m < n$$

$$g = b_mx^m + \dots + b_0 \quad b_m \not\equiv p, \quad b_{m-1}, \dots, b_0 \equiv p$$

$$h = c_{n-m}x^{n-m} + \dots + c_0$$

$$c_{n-m} \not\equiv p \quad c_{n-m}, \dots, c_0 \equiv p$$

$$\text{по усл. } a_0 = \underset{p^2}{\not\equiv} b_0 \cdot \underset{p}{\not\equiv} c_0 \underset{p}{\not\equiv} \text{ - противоречие}$$

Примеры

здесь когда-нибудь будут примеры

35 Рациональные корни многочлена с целыми коэффициентами.

Теорема

$$f \in \mathbb{Z}[x]$$

$$f = a_0 + \dots + a_n x^n \quad a_i \in \mathbb{Z}$$

$$a_n \neq 0 \quad a_0 \neq 0$$

Если некор. дробь $\frac{p}{q}$ - корень f , то $q \mid a_n$; $p \mid a_0$

Док-во

$$f\left(\frac{p}{q}\right) = 0$$

$$a_0 + a_1 \frac{p}{q} + \dots + a_n \frac{p^n}{q^n} = 0 \quad \Bigg| \cdot q^n$$

$$q^n a_0 + a_1 p q^{n-1} + \dots + a_{n-1} p^{n-1} q + a_n p^n = 0$$

$$q^n a_0 + a_1 p q^{n-1} + \dots + a_{n-1} p^{n-1} q = -a_n p^n$$

$$(p, q) = 1 \quad (q, p^n) = 1 \Rightarrow q \mid a_n$$

Аналогично $p \mid a_0$

36 Верхняя оценка модуля корня многочлена с комплексными коэффициентами.

Теорема

$$f = a_0 + a_1x + \dots + a_nx^n \in \mathbb{C}[x] \quad a_n \neq 0$$

$$M = \max_{i=0,\dots,n} \left\{ \frac{|a_i|}{|a_n|} \right\}$$

Тогда все корни многочлена f лежат в круге $|z| < M + 1$

Док-во

Возьмем z : $|z| \geq M + 1$, покажем, что z не корень f

$$z^n \frac{a_n}{a_n} + z^{n-1} \frac{a_{n-1}}{a_n} + \dots + \frac{a_0}{a_n} \neq 0$$

$$\begin{aligned} \left| \frac{a_{n-1}}{a_n} z^{n-1} + \dots + \frac{a_1}{a_n} z + \frac{a_0}{a_n} \right| &\leq M(|z|^{n-1} + \dots + |z| + 1) = M \frac{|z|^n - 1}{|z| - 1} \leq \\ &\leq M \frac{|z|^n - 1}{M} < |z|^n \end{aligned}$$

Нам нужно было бы получить $|\dots| = |z|^n$, получилось, что в первом выражении мы 0 не получим

37 Симметрические функции. Коэффициенты многочлена из $C[x]$ как симметрические функции корней.

Опр

$$f \in K[u_1, \dots, u_n]$$

f - симметрическая функция, если f не меняется при любой перестановке переменных

Пример

здесь когда-нибудь будет пример

Теорема (Виета)

здесь когда-нибудь будет теорема

Док-во

здесь когда-нибудь будет док-во

38 Алгоритм разложения на неприводимые множители многочлена с целыми коэффициентами.

Алгоритм

здесь когда-нибудь будет алгоритм

39 Линейные отображения векторных пространств. Линейное отображение полностью задается своими значениями на базисных векторах.

Опр

K - поле V - в.п. над K

$f : U \rightarrow V$ f - линейное, если $\forall u_1, u_2 \in U \quad \forall \alpha_1, \alpha_2 \in K$

1.

$$f(\alpha u_1 + \alpha u_2) = \alpha_1 f(u_1) + \alpha_2 f(u_2)$$

2. (a)

$$\forall u_1, u_2 \in U \quad f(u_1 + u_2) = f(u_1) + f(u_2)$$

(b)

$$\forall u \in U \quad \forall \alpha \in K \quad f(\alpha u) = \alpha f(u)$$

лин. отобр \equiv гомеоморфизм вект пр-в

Теорема (св-ва)

f - лин. отобр.

$$f(0_u) = 0_v$$

$$f(-u) = -f(u)$$

Примеры

здесь когда-нибудь будут дописаны примеры

$$K[x] \rightarrow K[x]$$

$$f \rightarrow f'$$

УТВ

U - в.п $\{u_i\}_{i \in I}$ - базис U

Достаточно задать лин. отобр. на базисных векторах

f - лин. отобр $f : U \rightarrow V$

$$u \in U \quad u = \sum \alpha_i u_i$$

$$f(u) = f\left(\sum \alpha_i u_i\right) = f\left(\sum_{\alpha_i \neq 0} \alpha_i u_i\right) = \sum_{\alpha_i \neq 0} \alpha_i f(u_i)$$

40 Сумма линейных отображений, умножение на скаляр. Пространство линейных отображений.

Утв

Пусть задано отображ. $h : \underset{\text{базис}}{\{u_i\}_{i \in I}} \rightarrow V$

\exists единств. лин. отображ. $f : U \rightarrow V$, такое что $\forall i \in I \quad f(u_i) = h(u_i)$

Опр

U, V - в.п. над K

$L(U, V)$ - мн-во всех линейных отображ. из U в V

$+: L(U, V) + L(U, V) \rightarrow L(U, V)$

$*: K \times L(U, V) \rightarrow L(U, V)$

Теорема

$L(U, V)$ - век. пр-во над K

этот билет когда-нибудь будет дополнен

41 Матрица линейного отображения для данных базисов. Матрица суммы отображений. Изоморфизм пространства линейных отображений и пространства матриц.

$$\dim U = m < \infty \quad \dim V = n < \infty$$

u_1, \dots, u_m - базис U ; v_1, \dots, v_n - базис V

$f : U \rightarrow V$ - лин. отобра.

$$f(u_j) = \sum_{i=1}^n a_{ij} v_i$$

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{1j} & & \\ a_{21} & & \ddots & \\ & a_{nj} & & a_{nm} \end{pmatrix}$$

a_{1j} - коэфф разложения $f(u_j)$ по базису $\{v_1, \dots, v_n\}$

A - матрица лин. отобра в базисах $\{u_1, \dots, u_m\}, \{v_1, \dots, v_n\}$

$$A = [f]_{\{u_j\}}^{\{v_j\}}$$

$$f(u) = c_1 f(u_1) + \dots + c_m f(u_m) = \sum_{j=1}^m c_j f(u_j) =$$

$$= \sum_{j=1}^m c_j \sum_{i=1}^n a_{ij} v_i = \sum_{i=1}^n \left(\sum_{j=1}^m c_j a_{ij} \right) v_i$$

где $u = c_1 u_1 + \dots + c_m u_m$

$$\begin{pmatrix} c_1 \\ \dots \\ c_m \end{pmatrix} = [u]_{\{u_i\}} \quad [v]_{\{v_i\}} = A \cdot [u]_{\{u_i\}}$$

$$[f+g]_{\{u_j\}}^{\{v_i\}} = [f]_{\{u_j\}}^{\{v_i\}} + [g]_{\{u_j\}}^{\{v_i\}}$$

Опр

U, V назыв. изоморфными, если $\exists f : U \rightarrow V$ 1) f - лин.
2) f - биекция

этот билет когда-нибудь будет дополнен

42 Композиция линейных отображений. Матрица композиции.

Опр

Предположение

u_1, \dots, u_m v_1, \dots, v_n w_1, \dots, w_k - базисы

$$[gf]_{\substack{\{u_i\} \\ \{w_k\}}} = [g]_{\substack{\{v_j\} \\ \{w_k\}}} [f]_{\substack{\{u_i\} \\ \{v_j\}}}$$

Док-во

i - ый столбец $[gf]$ - это коорд. $(gf)(u_i)$ в базисе $\{w_1, \dots, w_k\}$

$f(u_i)$ - коорд. этого вектора в базисе v_1, \dots, v_n - это i - ый столбец матрицы $[f]$

$[gf(u_i)]_{\{w\}}$ - это i - ый столбец $[gf]$

$[gf(u_i)]_{\{w\}} = [g] - i$ - ый столбец матр. $[f] = [g][f(u_i)]_{\{v_j\}}$

т.о. $[gf] = [g][f]$

этот билет когда-нибудь будет дополнен

43 Преобразование матрицы линейного отображения при замене базисов.

Опр

$f : U \rightarrow V$ - лин

u_1, \dots, u_m - базисы U v_1, \dots, v_n - базисы V
 u'_1, \dots, u'_m v'_1, \dots, v'_n

$$A = [f]_{\substack{\{u_i\} \\ \{v_j\}}} \quad A' = [f]_{\substack{\{u'_i\} \\ \{v'_j\}}}$$

C - матрица замены координат при переходе от $\{u_i\}$ к $\{u'_i\}$

D - матрица замены координат при переходе от $\{v_j\}$ к $\{v'_j\}$

i - ый столбец C - это коорд. u'_i в базисе u_1, \dots, u_m

i - ый столбец D - это коорд. v'_j в базисе v_1, \dots, v_k

$$[u]_{\{u_i\}} = C[u]_{\{u'_i\}}, \text{ аналогично для } D$$

Теорема

$$A' = D^{-1}AC$$

Док-во

здесь когда-нибудь будет док-во

**44 Ядро и образ линейного отображения, их свойства.
Критерий инъективности и сюръективности линейного
отображения в терминах ядра и образа.**

Опр

$$f : U \rightarrow V \quad f - \text{лин.}$$

$$f(U) = \{v \in V \mid \exists u \in U : v = f(u)\} = \text{Im} f \text{ (образ } f)$$

$$f^{-1}(\{0_v\}) = \{u \in U : f(u) = 0_v\} = \ker f \text{ (ядро } f)$$

Предположение

$$\text{Im} f \subseteq V; \quad \ker f \subseteq U$$

Док-во

здесь когда-нибудь будет док-во

Предположение

$$\text{а) лин. отобр. } f : U \rightarrow V \text{ сюръективно} \Leftrightarrow \text{Im} f = V$$

$$\text{б) инъективно} \Leftrightarrow \ker f = \{0_u\}$$

Док-во

здесь когда-нибудь будет док-во

45 Выбор базисов, для которых матрица линейного отображения имеет почти единичный вид. Следствие для матриц. Теорема о размерности ядра и образа.

Теорема

U, V - конечномерные; $f : U \rightarrow V$ - лин. Тогда \exists базисы пр-в U и V ,

в которых матрица f - почти единичная

$$[f]_{\substack{\{u_i\} \\ \{v_j\}}} = \begin{pmatrix} E_2 & 0 \\ 0 & 0 \end{pmatrix}$$

Док-во

здесь когда-нибудь будет док-во

Следствие (1)

$A \in M(n, m, K)$ Тогда \exists обрат. матрицы $C \in M(m, n, K)$ и

$$D \in M(n, m, K), \text{ такие, что } D^{-1}AC = \begin{pmatrix} E_2 & 0 \\ 0 & 0 \end{pmatrix}$$

Док-во

здесь когда-нибудь будет док-во

Следствие (2)

$\dim U < \infty$; V - произв.

$$f : U \rightarrow V$$

Тогда $\dim U = \dim \ker f + \dim \operatorname{Im} f$

Док-во

здесь когда-нибудь будет док-во

46 Критерий изоморфности конечномерных пространств

Опр

U, V изоморфны, если \exists биект. лин. отображение (изоморфизм) $f : U \rightarrow V$

$$U \cong V$$

Теорема

U, V - конечномерные в.п. над K

$$U \cong V \Leftrightarrow \dim U = \dim V$$

Док-во

$\Rightarrow f : U \rightarrow V, \quad f$ - биекция, лин.

f - инъект. $\Rightarrow \ker f = \{0\}$

f - сюръект. $\Rightarrow \operatorname{Im} f = V$

$$\dim V = \dim \operatorname{Im} f = \dim U - \dim \ker f = \dim U - 0 = \dim U$$

$$\Leftarrow \dim U = \dim V = n$$

u_1, \dots, u_n - базис U

v_1, \dots, v_n - базис V

Любой $u \in U$ единственным образом раскладывается в сумму

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n \quad \alpha_i \in K$$

$$f(u) = \alpha_1 v_1 + \dots + \alpha_n v_n$$

$$\tilde{u} = \tilde{\alpha}_1 u_1 + \dots + \tilde{\alpha}_n u_n$$

$$u + \tilde{u} = (\alpha_1 + \tilde{\alpha}_1) u_1 + \dots + (\alpha_n + \tilde{\alpha}_n) u_n$$

$$f(\tilde{u}) = \tilde{\alpha}_1 v_1 + \dots + \tilde{\alpha}_n v_n$$

$$f(u + \tilde{u}) = (\alpha_1 + \tilde{\alpha}_1) v_1 + \dots + (\alpha_n + \tilde{\alpha}_n) v_n$$

$$f(u + \tilde{u}) = f(u) + f(\tilde{u})$$

$$\text{Аналогично } f(\alpha u) = \alpha f(u)$$

Значит f - лин. отображ.

т.к. v_1, \dots, v_n - сем-во образующих $\Rightarrow f$ - сюръект.

$$v \in V \quad v = \alpha_1 v_1 + \dots + \alpha_n v_n$$

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n \quad f(u) = v$$

т.к. v_1, \dots, v_n - ЛНЗ, то f - инъект.

достаточно проверить, что $\ker f = \{0\}$

$$u = \alpha_1 u_1 + \dots + \alpha_n u_n$$

$$0 = f(u) = \alpha_1 v_1 + \dots + \alpha_n v_n \Rightarrow \alpha_1, \dots, \alpha_n = 0, u = 0 \Rightarrow \ker f = \{0\}$$

$\Rightarrow f$ - изоморфизм

47 Двойственное пространство. Двойственный базис.

Изоморфность конечномерного пространства и его двойственного. Пример пространства не изоморфного своему двойственному.

Опр

V - в.п. над K

$V^* = L(V, K)$ - двойственное пр-во к V

(пр-во линейных отображений из V в K)

элементы V^* - лин. функционалы V (лин. отображ.)

Пример

$V_{\mathbb{R}} = C([0; 1] \rightarrow \mathbb{R})$

$f \rightarrow \int_0^1 f(x) dx$

$a \in [0; 1] \quad f \rightarrow f(a)$

Опр

e_1, \dots, e_n - базис V

c_1, \dots, c_n - двойственный базис V , если

$$f(e_i, c_j) = \begin{cases} 1 & i = j \\ 0 & i \neq j \end{cases}$$

Теорема

$\dim V = n < \infty \Rightarrow V^* \cong V$

Док-во

v_1, \dots, v_n - базис V

это док-во когда-нибудь будет дополнено

Замечание

здесь когда-нибудь будет замечание

Пример

здесь когда-нибудь будет док-во

48 Каноническое отождествление конечномерного пространства со вторым двойственным.

здесь когда-нибудь будет что-то

49 Линейные операторы. Кольцо линейных операторов. Изоморфность кольца линейных операторов и кольца матриц.

V - в.п. над K

$L(v, v)$ эл-ты этого пр-ва назыв. линейными операторами на V

$$\text{End}(V) = L(V, V)$$

На $\text{End}(V)$ определена композиция (умножение операторов)

$$\square \dim V = n$$

зафиксируем базис v_1, \dots, v_n пр-ва V

$\text{End}(V) \rightarrow M_n(K)$ изморфизм в.п.

$f \rightarrow [f]_{\{v_i\}}$ - матрица оператора в базисе

Теорема

$(\text{End}(V), \cdot, +)$ - кольцо

когда-нибудь этот билет будет дополнен

50 Многочлены от оператора. Коммутирование многочленов от одного оператора.

Опр

V - в.п. над K $\varphi \in \text{End}(V)$

$$h = a_0 + a_1 t + \dots + a_m t^m \in K[t]$$

$$h(\varphi) = a_0 \text{id} + a_1 \varphi + \dots + a_m \varphi^m \in \text{End}(V)$$

Умножение = композиция операторов

$$A \in M_n(K)$$

$$h(A) = a_0 E + a_1 A + \dots + a_m A^m - \text{мн-н от матрицы}$$

$$(hg)(\varphi) = h(\varphi) \cdot g(\varphi)$$

этот билет когда-нибудь будет дополнен

51 Характеристический многочлен матрицы и оператора. **Независимость характеристического многочлена оператора от** **выбора базиса.**

Опр

$$A \in M_n(K)$$

Характеристический многочлен A

$$\det(A - tE) = \mathcal{X}_A(t)$$

$$\begin{vmatrix} a_{11} - t & a_{12} & \dots & a_{1n} \\ a_{21} & \ddots & & \\ \vdots & & \ddots & \\ a_{n1} & & & a_{nn} - t \end{vmatrix} = (-1)^n t^n + (-1)^{n-1} (a_{11} + \dots + a_{nn}) t^{n-1} + \dots + \det A$$

V - в.п. $\dim V = n < \infty$ v_1, \dots, v_n - базис V

$f \in \text{End}(V)$ $A = [f]_{\{v_i\}}$ - матрица оператора в базисе v_1, \dots, v_n

$$\mathcal{X}_f(t) = \mathcal{X}_A(t)$$

Лемма

Характеристический многочлен f не зависит от выбора базиса в V

Док-во

v_1, \dots, v_n - базисы V C - матрица преобр. координат
 v'_1, \dots, v'_n при переходе от $\{v_i\}$ к $\{v'_i\}$

$$A = [f]_{\{v_i\}}$$

$$A' = [f]_{\{v'_i\}}$$

$$A' = C'AC \quad (A \text{ и } A' \text{ сократимы при помощи } C)$$

$$\mathcal{X}_{A'}(t) = \mathcal{X}_A(t)$$

$$\begin{aligned} \mathcal{X}_{A'}(t) &= \det(C^{-1}AC - tE) = \det(C^{-1}AC - C^{-1}(tE)C) = \\ &= \det(C^{-1}(A - tE)C) = \det(C^{-1}) \cdot \det(A - tE) \cdot \det(C) = \\ &= \det(A - tE) = \mathcal{X}_A(t) \end{aligned}$$

52 Собственные числа и собственные векторы оператора и матрицы. Собственные числа как корни характеристического многочлена

Опр

$$f \in \text{End}(V) \quad \lambda \in K$$

λ - собственное число f , если $\exists v \neq 0; \quad v \in V : f(v) = \lambda \cdot v$

Если λ - собс. число $f \quad v \in V \quad f(v) = \lambda v$, то v - собс вектор

Опр

$$\lambda - \text{с.ч. } f \Rightarrow V_\lambda = \{v : f(v) = \lambda v\}$$

Поэтому удобно 0 считать с.в.

Опр

$$A \in M_n(K)$$

$$\lambda - \text{с.ч. } A, \text{ если } \exists v \neq \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix} \in K^n : A_n v = \lambda_n v$$

Теорема

$$A \in M_n(K)$$

$$\lambda \in K - \text{с.ч. } A \Leftrightarrow \lambda - \text{корень } \mathcal{X}_A(t)$$

Док-во

$$\exists v \neq 0 \quad Av = \lambda v$$

$$(A - \lambda E)v = 0$$

Рассмотрим коэф. столбца V как неизвестные

$$\lambda - \text{с.ч. } A \Leftrightarrow (A - \lambda E)v = 0 - \text{имеет нетривиальный ранг}$$

$$\Leftrightarrow \det(A - \lambda E) = 0 \Leftrightarrow \mathcal{X}_A(\lambda) = 0 \Leftrightarrow \lambda - \text{корень } \mathcal{X}_A(t)$$

Следствие

$$\dim V = n < \infty \quad f \in \text{End}(V)$$

$$\lambda \in K - \text{с.ч. } f \Leftrightarrow \lambda - \text{корень } \mathcal{X}_f(t)$$

Док-во

Фиксируем базис v_1, \dots, v_n

$$f \rightarrow [f] = A \quad v \rightarrow \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = [v]$$

$$\Leftrightarrow v - \text{с.в. } f, \text{ отвеч. } \lambda \quad \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} - \text{с.в. } A, \text{ отвеч. } A$$

53 Теорема Гамильтона-Кэли.

Теорема

$$A \in M_n(K) \quad \mathcal{X}_A(A) = 0_{M_n(K)}$$

Док-во

здесь когда-нибудь будет док-во

Следствие

здесь когда-нибудь будет следствие

Док-во

здесь когда-нибудь будет док-во

54 Диагонализируемые операторы. Критерий диагонализуемости. Примеры недиагонализуемых операторов

Опр

V - в.п. над K $\dim V = n < \infty$

$\varphi \in \text{End}(V)$

φ - диагонализуем, если \exists базис V , в котором матрица φ - диагональна

Теорема

V - в.п. $\dim V = n < \infty$

$\varphi \in \text{End}(V)$

φ - диагонализуем $\Leftrightarrow \exists$ базис V , состоящий из собс. векторов φ

Док-во

$\Rightarrow v_1, \dots, v_n$ - базис

$$[\varphi]_{\{v_i\}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

$\varphi(v_i) = \lambda_i v_i \quad v_i \neq 0 \Rightarrow v_i$ - с.в.

$\Leftarrow v_1, \dots, v_m$ - базис из с. в. φ

$\varphi(v_i) = \lambda_i v_i \quad \lambda \in K$

$\varphi(v_i) = 0 \cdot v_1 + \dots + 0 \cdot v_{i-1} + \lambda_i v_i + 0 \cdot v_{i+1} + \dots$

$$[\varphi]_{\{v_i\}} = \begin{pmatrix} \lambda_1 & & 0 \\ & \ddots & \\ 0 & & \lambda_n \end{pmatrix}$$

Пример

$V = \mathbb{C}^2$

$$\varphi(x) = A \cdot x \quad A = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

$\mathcal{X}_\varphi(t) = \mathcal{X}_A(t) = t^2 \quad \text{с.ч } \lambda = 0$

$Ax = 0$

$\text{rk } A = 1 \quad 2 \text{ перем} \Rightarrow \text{пр-во решений одномерно}$

\Rightarrow все с.в. лежат в одномерном пр-ве \Rightarrow непорожд \mathbb{C}^2

\Rightarrow не диагонализ.

Пример

$$V = K[x]_n = \{f \in K[x]; \deg f \leq n\}$$

$$\text{char } K = 0$$

$$\varphi = \frac{\partial}{\partial x} \quad \varphi(f) = f'$$

$$\text{с.ч. } \lambda = 0$$

с.в. пр. : константы

$$\dim V = n + 1 \quad (n \geq 1 \Rightarrow \varphi - \text{не диагонализ})$$

55 Инвариантные подпространства. Матрице линейного оператора, действующего на пространстве, разложенном в прямую сумму инвариантных подпространств.

здесь когда-нибудь будет что-то

Примеры

здесь когда-нибудь будут примеры

Теорема (1)

здесь когда-нибудь будет теорема

Док-во

здесь когда-нибудь будет док-во

Теорема (2)

здесь когда-нибудь будет теорема

Док-во

здесь когда-нибудь будет док-во

56 Инвариантность ядра и образа многочлена от оператора.

здесь когда-нибудь будет что-то

Теорема

здесь когда-нибудь будет теорема

Док-во

здесь когда-нибудь будет док-во

57 Теорема о разложении $\text{Ker}(fg)(\phi)$ в прямую сумму инвариантных подпространств и следствия из неё.

Теорема

здесь когда-нибудь будет теорема

Док-во

здесь когда-нибудь будет док-во

58 Жорданова форма оператора. Жорданов базис.
Формулировка теоремы о жордановой форме оператора.
Сведение к случаю оператора с единственным собственным
числом.

Опр

$$\lambda \in K$$

$$\mathfrak{J}(\lambda) = \begin{pmatrix} \lambda & & & 0 \\ 1 & \ddots & & \\ & \ddots & \ddots & \\ 0 & & 1 & \lambda \end{pmatrix} - \text{жордан. клетка размера } n \text{ отвечающей } \lambda$$

A - жорд. матрица, если A - блочно диаг, а диг. блоки - жорд. клетки

$$\mathfrak{J}_1 = (\lambda)$$

$$\mathfrak{J}_2 = \begin{pmatrix} \lambda & 0 \\ 0 & \lambda \end{pmatrix}$$

$$A = \begin{pmatrix} \mathfrak{J}_{m_1}(\lambda_1) & & & 0 \\ & \mathfrak{J}_{m_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & \mathfrak{J}_{m_k}(\lambda_k) \end{pmatrix}$$

Теорема (1)

$$K - \text{алг. замк. } V, \quad \dim V = n < \infty$$

$$\varphi \in \text{End}(V)$$

Тогда \exists базис пр-ва V , в котором матрица φ является жордановой матрицей. Причем клетки опред. однозначно с точностью до перестановки диаг. блоков

здесь когда-нибудь это будет дописано

Следствие

здесь когда-нибудь будет замечание

Теорема (1')

здесь когда-нибудь будет теорема

59 Относительная линейная независимость. Относительные базисы. Корневые пространства. Лемма о спуске для корневых подпространств.

здесь когда-нибудь будет что-то

Лемма (1)

здесь когда-нибудь будет лемма

здесь когда-нибудь будет вывод

здесь когда-нибудь будет что-то

60 Построение жорданова базиса и жордановой формы для оператора с единственным собственным числом.

здесь когда-нибудь будет что-то

Лемма (1)

здесь когда-нибудь будет лемма

Док-во

здесь когда-нибудь будет док-во

61 Единственность жордановой формы оператора.

здесь когда-нибудь будет что-то

Следствие

здесь когда-нибудь будет следствие

Следствие

здесь когда-нибудь будет следствие