1. Базис векторного пространства. Четыре эквивалентных переформулировки определения базиса.

<u>Опр</u>

V - в.п. над полем K

$$\{v_\alpha\}_{\alpha \in A} \text{ - лин. незав., если}$$

$$0 = \sum c_\alpha v_\alpha \Rightarrow \text{ все } c_\alpha = 0$$

<u>Опр</u>

$$\{v_\alpha\}_{\alpha \in A} \text{ - сем-во образующих, если}$$

$$\forall v \in V \quad v = \sum c_\alpha v_\alpha$$

<u>Опр</u>

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

<u>Опр</u>

лин. независ. сем-во назыв. максимальным по включению, если при добавлении $\forall$ нового вектора сем-во явл-ся ЛЗ

<u>Опр</u>

Сем-во образующих назыв. минимальным по включению, если при выбрасывании $\forall$ вектора сем-во не является сем-вом образующих

<u>Теор</u> (Равносильные утверждения)

1.

$$\{v_\alpha\} \text{ - базис } V \text{ над полем } K$$

2.

$$\{v_\alpha\} \text{ - макс. ЛНЗ сем-во}$$

3.

$$\{v_\alpha\} \text{ - мин. семейство образующих}$$

4. *$\forall v \in V$ единственным образом представим в виде лин. комбинации векторов из $\{v_\alpha\}$*

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.

Теор

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

След

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.

Теор

V - конечномерное в.п. над K Всякое сем-во образующих содержит базис.

Док-во

$\{u_1, ..., u_k\}$ *- сем-во*

если $\{u_1, ..., u_k\}$ *- ЛНЗ, то это базис*

иначе $\exists i : v_i$ *- лин. комб. остальных*

$\Rightarrow \{u_1, ..., u_{i-1}, u_{i+1}, ..., u_k\}$ *- сем-во образующих*

сем-во конечно $\Rightarrow$ *процесс оборвется* $\Rightarrow$
$\Rightarrow$ *получим ЛНЗ подсемейство, явл. образующим*

Теор

Во всяком конечномерном в.п. есть базис

Док-во

Пустое сем-во ЛНЗ
Дополним до базиса

4. Подпространства векторного пространства. Подпространство конечномерного пространства конечномерно.

Опр

$$V \text{ - в.п над полем } K$$

$$\varnothing \neq U \subseteq V \quad U \text{ - подпр-во } V\text{, если}$$

$$U \text{ - само явл. в.п. над } K$$

Предп **(1)**

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

1.

$$\forall u_1, u_2 \in U \quad u_1 + u_2 \in U$$

2.

$$\forall u \in U \ \forall a \in K \quad au \in K$$

(Операции, которые должны быть определены в векторном пр-ве)
$\Rightarrow$ *раз* U *- в.п. над полем* K*, эти операции определены*
$\Leftarrow$ *Операции определены, но в.п ли это? Надо проверить аксиомы в.п (комм., ассоц. сложения,* $\exists\overline{0}$*, обратного отно-но сложения, ассоц. умножения,* $\exists 1$*, две дистрибутивности)*

Предп **(2)**

$$V \text{ - конечномерное в.п над } K$$

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

Док-во

$$\{ \quad \} \subseteq U$$

Будем добавлять к этом сем-ву вектора с сохранением условия ЛН до тех пор, пока не получим семейство образующих U
В V *есть конечное сем-во образующих*
$U \subseteq V$ *не может быть больше, чем векторов в сем-ве образующих* $V \Rightarrow$ *процесс оборвется, и мы найдем конечный базис*

5. Теорема о мощности базиса конечномерного пространства. Размерность пространства.

Теор

V - конечномерное пространство

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

$\Rightarrow n = m$

Док-во

$u_1, ..., u_m$ - лин.комб $v_1, ..., v_n$

по т. о линейной зависимости лин. комбинаций

$m \leq n$ и обратно $m \geq n \Rightarrow m = n$

Опр

Размерность конечномерного в.п - кол-во векторов в базисе

$dimV$

Если V не конечномерно, $dimV = \infty$

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

<u>Опр</u>

$$V \text{ - в.п. над полем } K$$

$$n = dimV < \infty$$

$$v_1, ..., v_n \text{ - базис } V \text{ над } K$$

$$v \in V \quad \exists \text{ единственный набор } \alpha_1, ..., \alpha_n \in K$$

$$v = \alpha_1 v_1 + ... + \alpha_n v_n$$

$$\begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{pmatrix} \quad \alpha_i \forall i \text{ - координаты вектора } v \text{ в базисе } \{v_1, ..., v_n\}$$

$$v = (\alpha_1, ..., \alpha_n) \begin{pmatrix} v_1 \\ \vdots \\ v_n \end{pmatrix}$$

$$\text{Пусть } v_1, ..., v_n \text{ - базис } V$$

$$v'_1, ..., v'_n \text{ - другой базис } V$$

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

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

$$(v_1, ..., v_n) \text{ к базису } (v'_1, ..., v'_n)$$

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

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

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

к базису $(v_1, ..., v_n)$

$v = a_1 v_1 + ... + a_n v_n$

$v = a'_1 v'_1 + ... + a'_n v'_n$

C *- матрица перехода от* $(v_1, ..., v_n)$ *к* $(v'_1, ..., v'_n)$

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

<u>Теор</u> (В указанных выше обозначениях)

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

<u>Док-во</u>

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

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

В силу единственности разложения по базису

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

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

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

Теор

1. *Сумма является подпространством*

$$U_1 + ... + U_m$$

$$0 = 0 + ... + 0 \in U_1 + ... + U_m \Rightarrow \text{ \textit{сумма} } \neq \varnothing$$

$$\forall u, v \in U_1 + ... + U_m$$

$$u = u_1 + u_2 + ... + u_m$$

$$v = v_1 + v_2 + ... + v_m$$

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

умножение на скаляр аналогично

2. *Пересечение является подпространством*

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

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

не пусто, т.к.

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

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

Теор

$U_1, U_2 \subseteq V \quad U_1, U_2$ - *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

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

$\Rightarrow U_1 \cap U_2$ - *конечномерно*

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

Дополним до базиса U_1

$w_1, ..., w_r, u_1, ..., u_s$ - *базис* U_1

Аналогично $w_1, ..., w_r$ *дополним до базиса* U_2

$w_1, ..., w_r, v_1, ..., v_t$ - *базис* U_2

Проверим, что $w_1, ..., w_r, u_1, ..., u_s, v_1, ..., v_t$ - *базис* $U_1 + U_2$

1. *Семейство образующих*

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

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

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

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

$\Rightarrow w_1, ..., w_r, u_1, ..., u_s, v_1, ..., v_t$ - *сем-во образующих*

2. *ЛНЗ*

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

$$z = \underbrace{a_1 w_1 + ... + a_2 w_2 + b_1 u_1 + ... + b_s u_s}_{\in U_1} = \underbrace{-c_1 v_1 - ... - c_t v_t}_{\in U_2}$$

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

$$= d_1 w_1 + ... + d_2 w_2 + 0 \cdot u_1 + 0 \cdot u_2 + ... + 0 \cdot U_s$$

В силу единственности разложения по базису U_1

$$b_1 = b_2 = ... = b_s = 0$$

Из $(*) \Rightarrow a_1 w_1 + ... + a_2 w_r + c_1 v_1 + ... + c_t v_t = 0$

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

$$a_1 = ... = a_r = c_1 = ... = c_t = 0$$

$\Rightarrow w_1, ..., w_r, u_1, ..., u_s, v_1, ..., v_t$ - *ЛНЗ*

8. Прямая сумма подпространств. Эквивалентные переформулировки понятия прямой суммый подпротранств.

Опр

V - *в.п. над* K

$U_1, ..., U_m \subseteq V$

$U_1 + ... + U_m$ *назыв. прямой суммой, если любой* $z \in U_1 + ... + U_m$

едиственным образом представим в виде суммы

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

Обозначение: $U_1 \bigoplus U_2 \bigoplus ... \bigoplus U_m$

Замеч

Сумма $U_1 + ... + U_m$ *- прямая* $\Leftrightarrow$

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

$\Rightarrow u_1 = ... = u_m = 0$

Док-во

$\Rightarrow$ *очевидно*

$\Leftarrow z \in U_1 + ... + U_m$

$z = u_1 + ... + u_m$

$z = v_1 + ... + v_m$

$0 = z - z = (\underset{\in U_1}{u_1 - v_1}) + ... + (\underset{\in U_m}{u_m - v_m})$

$\forall i \quad u_i - v_i = 0$ *т.е.* $u_i = v_i$

Предп (1)

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

Предп (2)

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

<u>Предп</u> (3)

$$U_1 + ... + U_m \text{ - } \textit{прямая} \ \Leftrightarrow$$

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

<u>Предп</u> (4)

$$\textit{Сумма } U_1 + ... + U_m \text{ - } \textit{прямая} \ \Leftrightarrow$$

$$\Leftrightarrow \ \textit{объединение базисов } U_i \quad i = 1, ..., m \text{ - } \textit{базис } U_1 + ... + U_m$$

9. Построение кольца многочленов.

Опр

R - комм. кольцо с 1

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

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

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

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

$\forall m > M \quad b_i = 0 \Rightarrow \forall i > \max(N, M) \quad a_i + b_i = 0$

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

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

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

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

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

$i \le N \quad k - i \ge k - N > N + M - N = M$

Теор

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

Опр

$0 = (0, 0, ...)$

$1 = (1, 0, ...)$

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

$(a, 0, ...) + (b, 0, ...) = (a + b, 0, ...)$

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

<u>Опр</u>

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

$$x = (0, 1, 0, ...)$$

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

$$(a_0, a_1, ..., a_n, 0, ...) = (a_0, 0, ...) + (0, a_1, 0, ...) + ... + (0, ..., a_n, 0, ...) =$$

$$= a_0 \cdot 1 + a_1(0, 1, ...) + ... + a_n(0, ..., 1, ...) =$$

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

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

Опр

$$f = a_0 + a_1 x + ... + a_n x^n \in R[x]$$

наиб. m, т.ч. $a_m \neq 0$ назыв. степенью f
$\deg f - degree$

$$\deg 0 = -\infty$$

Опр

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

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

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

$\mathbb{Z}$ - о.ц.
любое поле - о.ц
$\mathbb{Z}_{/m}\mathbb{Z}$ - не о.ц. $\qquad [a][b] = [m] = [0]$

Теор (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)

$$N = \deg f \quad M = \deg g$$

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

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

Равенства в общ. случае нет

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

Если $N \neq M \quad \sqsupset N < M$

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

2)

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

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

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

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

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

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

<u>След</u>

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

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

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

$$\deg(fg) = \deg f + \deg g \geq 0 \Rightarrow \text{в } fg \text{ есть хотя бы один ненулевой коэф.}$$

$$\Rightarrow fg \neq 0$$

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

<u>Опр</u>

$$R \quad R[x_1]$$

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

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

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

11. Теорема о делении с остатком в кольце многочленов.

Теор

R - комм. к. с ед.

$f, g \in R[x]$

$g = a_0 + a_1 x + ... + a_n x^n, a_n \in R^*$ *обр. элем.*

$\Rightarrow \exists!$ *мн-ны q и r такие, что*

$f = qg + r \quad \deg r < \deg g$

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*

$R[x] \ni f \quad f = a_0 + a_1 x + ... + a_n x^n$

для данного мн-на опред. отображение

$c \to a_0 + a_1 c + ... + a_n c^n = f(c)$

отобр. из R *в* R

Замеч

Разные мн-ны могут задавать одно и то же отображение

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

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

Опр

$f \in R[x] \quad c$ *- корень* f

Если $f(c) = 0$

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

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

Теор (Безу)

$f \in R[x] \quad c \in R$

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

Док-во

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

$\exists q, r \in R[x]$

$f = (x - c)q + r$

$\deg r < \deg g = 1$

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

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

$r = f(c)$

<u>След</u>

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

<u>Док-во</u>

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

$$\Leftarrow f(x) = (x-c)q(x)$$

$$f(c) = (c-c)q(c) = 0$$

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

Опр

$$K \text{ - поле} \qquad K[x]$$

$$f \in K[x]$$

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

$$f(x) = (x-a)^k \cdot g(x) \quad (x-a) \nmid g$$

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

Замеч

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

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

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

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

$$g_1(a) g_2(a) \neq 0 \qquad \text{поле } K \text{ - о.ц.}$$

Лемма

$$f, g, h \in K[x]$$

$$b \in K \qquad b \text{ - не корень } h$$

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

$$b \text{ - корень } f \Rightarrow b \text{ - корень } g \text{ той же кратности}$$

Теор

$$K \text{ - поле, } f \in K[x] \quad f \neq 0$$

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

Замеч

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 $\quad \deg f = 2$

След

$$\textit{Если } f(a_1) = ... = f(a_n) = 0$$

$$\textit{для попарно различных } a_1, ..., a_n; \quad n > \deg f, \textit{ то } f = 0$$

14. Функциональное и формальное равенство многочленов.

<u>**Опр**</u>

$$f, g \in K[x] \quad |K| > \max(\deg f, \deg g)$$

если f и g совп. функционально, то $f = g$

<u>**Замеч**</u>

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

15. Характеристика поля.

<u>**Опр**</u>

$$K \text{ - } \textit{поле} \quad 1 \in K$$

$$n \cdot 1 = \underbrace{1 + ... + 1}_{n}$$

Если $n \cdot 1 \neq 0$ *для всех* $n \geq 1$, *то говорят, что поле* K *имеет х-ку 0*
$char K = 0$
Если $\exists n \geq 1 \quad n \cdot 1 = 0$, *то наименьшее такое положительное* n *называют х-кой* K

<u>**Примеры**</u>

$char\, \mathbb{Q} = 0,\ char\, \mathbb{R} = 0,\ char\, \mathbb{C} = 0$
p *- простое* $\quad char(\mathbb{Z}_{/p}\mathbb{Z})$

<u>**Теор**</u>

Характеристика поля либо 0, либо простое число

<u>**Док-во**</u>

1) не $\exists n \geq 1 \quad n \cdot 1 = 0 \quad \Rightarrow \quad char K = 0$
2) $n \cdot 1 = 0$ *возьмем наим.* n *и покажем, что* n *- простое*

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

$$0 = \underbrace{1 + ... + 1}_{n} = (\underbrace{1 + ... + 1}_{a})(\underbrace{1 + ... + 1}_{b})$$

$$\Rightarrow \underbrace{1 + ... + 1}_{a} = 0 \text{ } \textit{или} \text{ } \underbrace{1 + ... + 1}_{b} = 0$$

противоречие с $\min n$

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

$\Rightarrow n$ *- простое*

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

Опр

$$K \text{ - } \textit{поле}$$

$$f(x) \in K[x]$$

$$f(x) = \sum_{k=0}^{n} a_k x^k$$

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

$$k \cdot a_k = \underbrace{a_k \cdot ... \cdot a_k}_{k}$$

Теор (Свойства)

1.
$$(f+g)^{'} = f^{'} + g^{'}$$

2.
$$c \in K \quad (c \cdot f^{'}) = cf^{'}$$

3.
$$(f \cdot g)^{'} = f'g + g'f$$

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

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

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

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

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

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

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

(c)

f, g - *произвольные*

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

$$(fg)' = \sum_{k=0}^{n} b_k (x^k g)' = (\sum_{k} b_k \cdot kx^{k-1} \cdot g) + (\sum_{k} b_k x^k \cdot g') =$$

$$= f'g + fg'$$

(d) *Ф-ла Лейбница*

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

(e) *Если* $char\ K = 0 \Rightarrow f' = 0 \Leftrightarrow f \in K$
Если $char\ K = p > 0$ *то* $f' = 0 \Leftrightarrow f \in K[x^p]$

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

17. Теорема о кратности

<u>Теор</u>

K - поле $\quad char K = 0$

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

тогда a - корень f' кр $l-1$

<u>Замеч</u>

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

$\mathbb{Z}_{/p}\mathbb{Z} \quad f = x^{2p+1} \qquad O$ *- корень кр. p*

$f' = (2p+1)x^{2p} + px^{p-1} = x^{2p} \qquad O$ *- корень кр. $2p$*

18. Интерполяционная задача. Существование и единственность решения. для интерпол. задачи

x	a_1 ... a_n
f	y_1 ... y_n

$\exists!$ решение f степени $< n$

Док-во

1) ед

$$f, h \text{ - решают одну и интер. задачу}$$

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

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

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

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

(теорема о числе корней мн-на)

2) существование

$$\text{1 сл} \quad f(x) = c_0 + c_1 x + ... + c_{n-1} x^{n-1}$$

$$c_0 + c_1 a_i + ... + c_{n-1} a_i^{n-1} = y_i$$

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

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

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

$$A \text{ - обр.}$$

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

19. Интерполяционный метод Ньютона.

<u>**Опр**</u>

x	a_1	a_i ... a_n
$f(x)$	y_1	y_i ... y_n

f_{i-1} - *интерпол. мн-ен степени* $\leq i-1$

и решающий интерпол. задачу для первых i точек

$f_0(x) = y_1$

$f_0(a_1) = y_1$

$\sqsupset$ *построли* f_{i-1} *Ищем* f_i

$(f_i - f_{i-1})(a_j) = 0 \quad j = 1, ..., i$

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

$\deg f_i \leq i$

$y_i + 1 = f_i(a_{i+1}) = f_{i-1}(a_{i+1}) + c_i(a_{i+1} - a_i)...(a_{i+1} - a_i)$

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

20. Интерполяционный метод Лагранжа.

Опр

x	a_1	a_{j-1}	a_j	a_{j_i}	a_n
$f(x)$	0	0	1	0	0

$$L_j(x) = a_j(x-a_1)...(x-a_{j-1})(x-a_{j+1})...(x-a_n)$$

$$L_j(a_j) = 1$$

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

$L_j(x)$ - *интерп. мн-ен Лагранжа*

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

x	a_1	a_n
$f(x)$	y_1	y_n

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

Мн-ен Лагранжа исп. в алг. быстрого умножения
$\forall \mathcal{E} > 0$ $\exists$ *алг. умн., который для n-разрядных чисел требует* $O(n^{1+\mathcal{E}})$ *поразрядных операций*

21. Делимость и ассоциированность в кольце многочленов над полем.

<u>Опр</u>

$$K \text{ - поле, } K[x]$$

$$f, g \in K[x] \text{ ассоциирован, если}$$

$$f \mid g \text{ и } g \mid f$$

$$f \sim g \quad : \ f \text{ и } g \text{ ассоц.}$$

$$0 \sim 0$$

0 с другими не ассоц.

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

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

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

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

$$0 = 1 \cdot 0$$

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

<u>След</u>

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

Если $f \neq 0$, то в классе ассоц. с f мн-нов всегда можно выбрать мн-ен со старшим коэф 1.
Мн-ен со старшим коэф. 1 назыв. унитарным, <u>приведенным</u>

<u>Замеч</u>

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

$$\Rightarrow f_1 \mid g_1$$

$$g = f \cdot h$$

$$cg = f(ch)$$

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

22. Наибольший общий делитель в кольце многочленов над полем. Существование и линейное представление.

Опр

$$K \text{ - поле, } K[x]$$

$$f_1, ..., f_n \in K[x]$$

$$g \text{ - НОД } f_1, ..., f_n, \text{ если}$$

$$g \mid f_1, ..., g \mid f_n$$

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

Замеч

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

$$\text{НОД}(0, ..., 0) = 0$$

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

Теор

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

$$\text{Существует } g = \text{НОД}(f_1, ..., f_n) \text{и он допускает лин. предствление}$$

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

Док-во

1)

$$f_1 = f_2 = ... = f_n = 0 \qquad \text{НОД}(0, ..., 0) = 0$$

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

2)

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

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

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

g - мн-ен наим. степени в $I \setminus \{0\}$
Утверждается, что g – НОД$(f_1, ..., f_n)$

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

$$= -h_1 u_j f_1 - h_2 u_j f_2 + (-h_j u_j + 1) f_i - ...$$

$$g = h_1 f_1 + ... + h_n f_n \qquad r_j \in I$$

Т.к.

$$\deg r_j < \deg g \text{ а степень } g \text{ наим в } I \setminus \{0\}$$

$$\text{то } r_j = 0$$

$$f_j = g u_j \quad g \mid f_j \quad j = 1, ..., n$$

$$h \mid f_i, ..., h \mid f_n$$

$$g = \underset{\vdots h}{f_1} h_1 + ... + \underset{\vdots h}{f_n} h_n \vdots h \Rightarrow h \mid g$$

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

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

Теор (Свойства)

1. Если $g \sim$ НОД$(f_1, ..., f_n)$ (не все $f_i = 0$)

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

2. $f_1, ...f_n$ - вз. просты $\Leftrightarrow 1$ допускает лин. представление

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

Док-во

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

Теор

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

Док-во

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

$$fu + gv = 1$$

$$\underset{\vdots f}{fuh} + \underset{\vdots f}{ghv} = h \quad \Rightarrow h \vdots f$$

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

Опр

$$K[x] = \{0\} \cup K^* \cup \{\textit{мн-ны ст } \geq 1\}$$

$f \in K[x] \setminus K$ *назыв сост, если* *(или приводимым)*

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

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

$x - a$ *неприводим при любом* a

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

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

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

Если $gf \quad \deg f \geq 2$ *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

Теор

$f \in K[x] \quad f$ *- неприводим*

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

Теор (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.*

Замеч

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

Лемма (1)

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

Док-во

f *- непр - все доказано*
Если приводим, то $f = f_1 \cdot g_1 \qquad 1 \leq \deg f_1 < \deg f$
Если f_1 *неприв, то делитель найден*
Если приводим $f_1 = f_2 g_2 \qquad q \leq \deg f_2 \leq \deg f_1$
$\deg f > \deg f_1 > ...$ *процесс оборвется*
$\Rightarrow$ *Найдем неприв. делитель* f

Док-во (Существование)

Инд. по $\deg f$
1)

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

инд. преход $\deg f > 0$
по лемме $\exists$ *неприв.* $g_1 \quad g_1 \mid f$
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.

$$f_1 = c \prod_{i=2}^{n} g_i \quad g_i \text{ - прив. неприв.}$$

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

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

<u>**Док-во**</u>

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

$\Rightarrow n = m \quad c = \widetilde{c}$ *иначе перенумеруем сомнож.* $g_i = \widetilde{g_i}$

Не умоляя общ. $n \leq m$

Инд. по n

$$n = 0 \quad c = \widetilde{c}\prod_{i=1}^{n} \widetilde{g_i}$$

$\Rightarrow m = 0 \quad \widetilde{c} = c$

Инд. переход

$$g_n \mid \widetilde{c}\prod_{i=1}^{m} \widetilde{g_i} \Rightarrow \exists i \quad g_n \mid \widetilde{g_i}$$

$\widetilde{c} \neq 0$

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

$$g_n \mid \widetilde{g_m} \Rightarrow g_n = \widetilde{g_m}$$

В $(*)$ *сократим на* g_n

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

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

$c = \widetilde{c}$ *(после перенумерования)*

$g_i = \widetilde{g_i} \quad i = 1, ..., n-1$

$g_n = \widetilde{g_n}$

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

Теор

$$\urcorner\ K \text{ - поле, рассмотрим } K[x]$$

Следующие условия равносильны

1. *Все неприводимые в $K[x]$ - это в точности линейные мн-ны*
2. *Всякий мн-н $f \in K[x], \deg f > 0$ рассклaдывается в произведение лин. множителей*
3. *Всякий $f \in K[x], \deg f > 0$ делится на линейный*
4. *Всякий $f \in K[x], \deg > 0$ 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 $K \quad K[x]$ выполнено любое из равносильных усл., то K назыв. алгебр. замкн.

Примеры

$\mathbb{R}, \mathbb{Q}$ *не алг. замкнуты*
Любое конечное поле не алг. замкнуто

$$|F| = q \quad \deg f = n > q$$

Теор (б.д.)

$\mathbb{C}$ *- алг. замк.*

След

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

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

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

Опр

Неприводимы:

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

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

Теор

Всякий неприв. в $R[x]$ ассоциирован с лин. или квадратичным с отр. дискр.

След

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

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

Лемма

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

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

Док-во

$$f = a_0 + a_1x + ... + a_nx^n$$

$$a_0 + a_1z + ... + a_nz^n = 0$$

$$\overline{a_0 + a_1z + ... + a_nz^n} = \overline{0} = 0 \text{ (сопряжение)}$$

$$\overline{a_0} + \overline{a_1z} + ... + \overline{a_n}(\overline{z})^n$$

$$a_0 + a_1\overline{z} + ... + a_n(\overline{z})^m = f(\overline{z})$$

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 эквив.

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

$\sim$ *- отношение эквив.*

$$(a,b) \sim (a,b)$$
$$(a,b) \sim (c,d) \Rightarrow (c,d) \sim (a,b)$$

$$\begin{matrix}(a,b) \sim (c,d) \\ (c,d) \sim (e,f)\end{matrix} \Rightarrow (a,b) \sim (e,f)$$

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

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

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

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

Корректность опредения (независимость от выбора представителя в классе)

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

$$(ac, bd) \sim (a_1c_1, b_1d_1) \qquad acb_1d_1 = bda_1c_1$$

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

$$adb_1d_1 + bcb_1d_1 = bda_1d_1 + bdb_1c_1$$

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

Теор

$K, +, \cdot$ - *поле*

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

$$K(x) \quad K \text{ - } \textit{поле}$$

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

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

Лемма (1)

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

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*

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

Опр

Дробь назыв. простейшей, если она имеет вид

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

$$\deg f < \deg q$$

Теор

$$\frac{f}{g} \in K(x) \text{ *тогда* } \frac{f}{g}$$

единственным образом (с точностью до порядка слагаемых) представима в виде суммы многочлена и простейших дробей

Лемма (2)

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

Док-во

$$\text{Делим с остатком: } f = gh + f_1, \quad \deg f_1 < \deg g$$

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

Лемма (3)

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

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

Док-во

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

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

$$g_1u_2 + g_2u_1 = 1 \mid \cdot f$$

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

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

$$u_1f = g_1h_1 + f_1 \text{ (делим с остатком)}$$

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

$= g_1 f_2 + g_2 f_1$ - *надо убедиться, что правильное*

$g_1 f_2 = f - g_2 f_1$

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

$\deg f_2 < \deg g_2$

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

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

Док-во

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

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

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

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

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

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

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

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

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

<u>Опр</u>

R - о.ц

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

называется 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)

<u>Опр</u>

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

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

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

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

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

В факториальных кольцах можно определить НОД

$$a = \mathcal{E}_1 \prod_{i=1}^{k} q_i^{k_i} \qquad b = p_1 \prod_{i=1}^{n} q_i^{l1} \qquad \mathcal{E}_1, p_1 \in R^* \quad q_i \text{ - попарно ассоц. неприв}$$

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

$$ab = \mathcal{E}_1 p_1 \prod_{i=1}^{n} q_i^{(k_i + l_i)}$$

<u>Опр</u>

Содержание многочлена f

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

Опр

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

В факториальном кольце $\forall$ *многочлен* $f \in R[x]$ *можно записать как* $f(x) = cont(f) \cdot f_1$ *- примитивный*

Лемма (Гаусса)

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

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

Теор

$$R \text{ - } \textit{факториальное кольцо } \Rightarrow R[x] \text{ - } \textit{факториальное}$$

Лемма (Гаусса)

$$f, g \in R[x] \quad f, g \text{ - } \textit{примитивны } \Rightarrow f \cdot g \text{ - } \textit{примитивный}$$

След

$$\mathbb{Z}[x_1, ..., x_n], K[x_1, ..., x_n] \text{ - } \textit{факториальны}$$

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:

$f = a_0 + ... + a_n x^n$

p - простое $p \nmid a_n$

$\mathbb{Z}[x] \to \mathbb{Z}_{/p}\mathbb{Z}[x]$

каждый коэфф. заменяем на соотв. вычет

$f \to \overline{f} = [a_0] + ... + [a_n] \cdot x^n$

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

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

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

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

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

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

$\deg \overline{g} = \deg g$ и $\deg \overline{h} = \deg h$

Тогда приводимость f влечет приводимость $\overline{f}$

<u>Предп</u>

Если $p \nmid a_n \quad f = a_0 + ... + a_n x^n \qquad \mathit{cont}\ f = 1$

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

34. Критерий неприводимости Эйзенштейна.

Теор

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

p - *простое*

$$\textit{Если} \ \begin{array}{l} * \, p \nmid a_n \\ * \, p \mid a_i \quad i = 0, ..., n-1, \ \textit{то } f \textit{ неприводим над } \mathbb{Z} (\Rightarrow \ \textit{и над } \mathbb{Q}) \\ * \, p^2 \nmid a_0 \end{array}$$

Док-во

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

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

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

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

$$g = b_mx^m + ... + b_0 \qquad b_m \not\vdots \, p, \quad b_{m-1}, ..., b_0 \vdots \, p$$

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

$$c_{n-m} \not\vdots \, p \qquad c_{n-m}, ..., c_0 \vdots \, p$$

$$\textit{по усл. } \underset{\not\vdots \, p^2}{a_0} = \underset{\vdots \, p}{b_0} \cdot \underset{\vdots \, p}{c_0} \ \textit{- противоречие}$$

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

Опр

$$K \text{ - поле} \qquad V \text{ - в.п. над } K$$

$$f : U \to V \qquad f \text{ - линейное, если } \forall u_1, u_2 \in U \quad \forall \alpha_1, \alpha_2 \in K$$

1.

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

2. (a)

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

(b)

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

лин. отобр $\equiv$ *гомеоморфизм вект пр-в*

Теор (св-ва)

$$f \text{ - лин. отобр.}$$

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

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

Пример

$$K[x] \to K[x]$$

$$f \to f'$$

$$U \text{ - в.п} \qquad \{u_i\}_{i \in I} \text{ - базис } U$$

Достаточно хадать лин. отобр. на базисных векторах

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

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

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

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

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

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

$u_1, ..., u_m$ - базис U; $\quad v_1, ..., v_n$ - базис V

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

$\alpha : U \to V$ - лин. отобр.

$$A = (a_{ij}) = \begin{pmatrix} a_{11} & a_{12} & \\ a_{21} & \ddots & \\ & & a_{nm} \end{pmatrix}$$

- коэфф разложения $f(u_i)$ по базису $\{v_1, ..., v_n\}$

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

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

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

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

где $u = c_1 u_1 + ... + c_m u_m$

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

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

$$\{v_i\} \qquad \{v_i\} \qquad \{v_i\}$$

u, v назыв. изоморфными, если $\exists f : U \to V$ $\quad$ 1)f - лин.

2)f - биекция

42. Композиция линейных отображений. Матрица композиции.

<u>Опр</u>

$$
\begin{tikzcd}
U \arrow[r, "f"] \arrow[rr, bend right, "g \circ f"'] & V \arrow[r, "g"] & W
\end{tikzcd}
$$

43. Преобразование матрицы линейного отображения при замене базисов.

Опр

$f : U \to V$ *- лин*

$$\begin{matrix} u_1, ..., u_m \\ u'_1, ..., u'_m \end{matrix} \text{ - \textit{базисы} } U \qquad \begin{matrix} v_1, ..., v_n \\ v'_1, ..., v'_n \end{matrix} \text{ - \textit{базисы} } V$$

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

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* $u_1, ..., u_m$
i *- ый столбец* D *- это коорд.* v'_j *в базисе* $v_1, ..., v_k$

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

Теор

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

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

Опр

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

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

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

Предп

$$Imf \subseteq V; \quad \ker f \subseteq U$$

Предп

а) лин. отобр. $f : U \to V$ *сюрbективно* $\Leftrightarrow Imf = V$

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

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

Теор

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

в которых матрица f - почти единичная

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

След (1)

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

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

След (2)

$\dim U < \infty$; $\quad V$ *- произв.*

$f : U \to V$

Тогда $\dim U = \dim \ker f + \dim Imf$

46. Критерий изоморфности конечномерных пространств

Опр

$$U, V \text{ изоморфны, есди } \exists \text{ биект. лин. отображение (изоморфизм)} f : U \to V$$

$$U \cong V$$

Теор

U, V - *конечномерные в.п. над* K

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

Док-во

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

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

f - *сюръект.* $\Rightarrow Imf = V$

$\dim V = \dim Imf = \dim U - \dim \ker f = \dim U - 0 = \dim U$

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

$u_1, ..., u_n$ - *базис* U

$v_1, ..., v_n$ - *базис* V

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

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

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

$\widetilde{u} = \widetilde{\alpha_1} u_1 + ... + \widetilde{\alpha_n} u_n$

$u + \widetilde{u} = (\alpha_1 + \widetilde{\alpha}) u_1 + ... + (\alpha_n + \widetilde{\alpha_n}) u_n$

$f(\widetilde{u}) = \widetilde{\alpha}_1 v_1 + ... + \widetilde{\alpha}_n v_n$

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

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

Аналогично $f(\alpha u) = \alpha f(u)$

Значит f - *лин. отобр*

т.к. $v_1, ..., v_2$ *- сем-во образующих* $\Rightarrow f$ *- сюръект.*

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

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

т.к. $v_1, ..., v_n$ *- ЛНЗ, то* f *- инъект.*

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

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

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

$\Rightarrow f$ *- изоморфизм*

47. Двойственное пространство. Двойственный базис. Изоморфность конечномерного пространства и его двойственного. Пример пространства не изоморфного своему двойственному.

Опр

$$V \text{ - в.п. над } K$$

$$V^* = L(V, K) \text{ - двойственное пр-во к } V$$

$$(\text{пр-во линейных отображений из } V \text{ в } K)$$

$$\text{элементы } V^* \text{ - лин. функционалы } V \text{ (лин. отобр)}$$

Пример

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

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

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

Опр

$$e_1, ..., e_n \text{ - базис } V$$

$$c_1, ..., c_n \text{ - двойственнй базис } V, \text{ если}$$

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

Теор

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

Док-во

$$v_1, ..., v_n \text{ - базис } V$$

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

$End(V) = L(V, V)$

На $End(V)$ определена композиция (умножение операторов)

$\sqsupset \dim V = n$

зафиксируем базис $v_1, ..., v_n$ пр-ва V

$End(V) \to M_n(K)$ изморфизм в.п.

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

<u>**Теор**</u>

$(End(V), \cdot, +)$ - *кольцо*

50. Многочлены от оператора. Коммутирование многочленов от одного оператора.

V - в.п. над K $\qquad \phi \in End(V)$

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

$h(\phi) = a_0 id + a_1\phi + ... + a_m\phi^m \in End(V)$

Умножение = композиция операторов

$A \in M_n(K)$

$h(A) = a_0 E + a_1 A + ... + a_m A^m$ - мн-н от матрицы

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

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

Опр

$$A \in M_n(K)$$

Характеристический многочлен A

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

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