1. Линейное пространство над числовым полем: определение, свойства и примеры.

***Определение:***
*Множество **L** называется **векторным (линейным) пространством**, над числовым полем **k**, если:*

а) *Задан закон (сложение), по которому $\forall x, y \in L$ сопоставляется т.н. сумма $x+y \in L$;*
б) *Задан закон (умножение на число), по которому $\forall x \in L$ и $\forall \alpha \in k$ сопоставляется произведение $\boldsymbol{\alpha x} \in \boldsymbol{L}$;*
в) *$\underline{\forall x, y, z \in L}$ и $\underline{\forall \alpha, \beta \in k}$ выполнены следующие **аксиомы**:*
- $x + y = y + x$,
- $(x + y) + z = x + (y + z)$,
- $\exists\, 0 \in L$: $x + 0 = x$,
- $\exists$ '$-x$' $\in L$: $x + (-x) = 0$,
- $1 \cdot x = x$,
- $\alpha(\beta x) = (\alpha\beta)x$,
- $(\alpha + \beta)x = \alpha x + \beta x$,
- $\alpha(x + y) = \alpha x + \alpha y$,

- *Элементы **L** называются **векторами**;*
- ***0** называется **нулевым вектором (нулем)**;*
- ***'-x'** называется **противоположным** вектору x.*

***Свойства:***
***Лемма 1.*** *Любое числовое поле включает в себя подполе рациональных чисел $\mathbb{Q}$.*
***Лемма 2.***
1) *В любом векторном пространстве L существует **единственный** нулевой вектор.*
2) *В любом векторном пространстве для любого вектора существует **единственный** противоположный вектор.*
3) $\forall x \in L$: $0 \cdot x = 0$.
4) $\forall x \in L$: $(-1) \cdot x = -x$.

***Примеры:***
1) $V_3$ и $V_2$ *над* $\mathbb{R}$ - *пространства геометрических векторов;*
2) $\mathbb{C}$ *над* $\mathbb{R}$; $\mathbb{C}$ *над* $\mathbb{C}$; $\mathbb{C}$ *над* $k$; $\mathbb{R}$ *над* $\mathbb{Q}$ *и т.п. – поле над подполем;*
3) $k_n = \{x = (\alpha_1,\ \alpha_2, \dots, \alpha_n)^T\}$, $\alpha_j \in k$ – *пространство векторов-столбцов;*
4) $M_{m,n}(k)$ – *пространство матриц размера* $m \times n$;
5) $k[t]$ – *пространство всех многочленов от* $t$;
6) $k_{\leq n}[t]$ – *пространство многочленов степени не выше* $n$;

7) $\mathbb{R}(a; b)$ – *пространство вещественных непрерывных функций на* $[a; b]$;
8) *Пространство решений ОСЛУ;*
9) *0 = {0} – нулевое пространство.*

2. Базис и размерность линейного пространства. Координаты вектора. Теорема о существовании базиса.

***Определение базиса:***
*Если в пространстве L (над полем k) существует такая совокупность векторов* $x_1, x_2, \dots, x_m$, *что любой вектор из L является их линейной комбинацией, то эта совокупность называется порождающей системой векторов пространства L.*

*Упорядоченная порождающая и при этом линейно независимая система векторов называется* ***Базисом*** *пространства L.*

***Определение координат вектора:***
*Коэффициенты линейной комбинации* $\alpha_1, \alpha_2, \dots, \alpha_n$ *называется координатами вектора x относительно базиса* $e_1, e_2, \dots, e_n$.

***Определение размерности линейного пространства:***
*Если в пространстве L можно найти n линейно независимых векторов, а всякие n+1 векторов этого пространства линейно зависимы, то число n называется размерностью пространства L, а L называется n-мерным.*

$$n = dimL; \quad dim0 = 0$$

*Векторное пространство, в котором можно указать сколь угодно большое число линейно независимых векторов, называется бесконечномерным.*

$$dim_{\mathbb{C}}\mathbb{C} = 1, \qquad dim_{\mathbb{R}}\mathbb{C} = 2, \qquad dim_{\mathbb{Q}}\mathbb{C} = \infty$$

***Теорема о существовании базиса:***
*В пространстве* ***L*** *размерности* ***n*** *существует* ***базис*** *из* ***n*** *векторов; более того, любая из* ***n*** *линейно независимых векторов пространства* ***L*** *является* ***базисом*** *этого пространства.*
***Доказательство:***
*Пусть* $e_1, e_2, \dots, e_n$ *линейно независимы,* $x \in L$.

$$\alpha_0 x + \alpha_1 e_1 + \alpha_2 e_2 + \dots + \alpha_n e_n = 0$$

$\alpha_0 \neq 0$ *(от противного)* $\Rightarrow x = -\frac{\alpha_1}{\alpha_0} e_1 - \frac{\alpha_2}{\alpha_0} e_2 - \dots - \frac{\alpha_n}{\alpha_0} e_0$
***Ч.Т.Д.***

***Лемма.*** *Коэффициенты разложения вектора x по базису* $e_1, e_2, \dots, e_n$ *определяются однозначно.*

***Теорема.*** *При сложении двух векторов пространства L их координаты* *складываются. При умножении вектора на число все его координаты умножаются на это число.*

3. Признак линейной независимости системы векторов. Следствия.

***<u>Теорема линейной независимости системы векторов:</u>***
*Система из m векторов $x_1, x_2, \dots, x_m$ линейно независима тогда и только тогда, когда ранг матрицы из координат векторов $x_1, x_2, \dots, x_m$ равен числу этих векторов.*

***<u>Следствие:</u>***
*Если в пространстве L имеется базис, то размерность этого пространства равна числу базисных векторов.*

***<u>Следствие:</u>***
*Система из **n** векторов в **n-мерном** векторном пространстве **линейно независима** тогда и только тогда, когда определитель из координат этих векторов относительно произвольного базиса **отличен** от нуля.*

4. Преобразование координат вектора при замене базиса пространства.

*Два базиса пространства L: «старый» $e_1, e_2, \dots, e_n$ и «новый» $g_1, g_2, \dots, g_n$.*

$$\begin{cases} g_1 = \alpha_{11}e_1 + \alpha_{21}e_2 + \dots + \alpha_{n1}e_n \\ g_2 = \alpha_{12}e_1 + \alpha_{22}e_2 + \dots + \alpha_{n2}e_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ g_n = \alpha_{1n}e_1 + \alpha_{2n}e_2 + \dots + \alpha_{nn}e_n \end{cases}$$

$x \in L \qquad x = \lambda_1 e_1 + \lambda_2 e_2 + \dots + \lambda_n e_n = \mu_1 g_1 + \mu_2 g_2 + \dots + \mu_n g_n$

$$\begin{cases} \lambda_1 = \alpha_{11}\mu_1 + \alpha_{12}\mu_2 + \dots + \alpha_{1n}\mu_n \\ \lambda_2 = \alpha_{21}\mu_1 + \alpha_{22}\mu_2 + \dots + \alpha_{2n}\mu_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ \lambda_n = \alpha_{n1}\mu_1 + \alpha_{n2}\mu_2 + \dots + \alpha_{nn}\mu_n \end{cases}$$

$$X_e = \begin{pmatrix} \lambda_1 \\ \lambda_2 \\ \dots \\ \lambda_n \end{pmatrix}; \ X_g = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \dots \\ \mu_n \end{pmatrix}; \ A_{e\to g} = \begin{pmatrix} \alpha_{11} & \alpha_{12} & \dots & \alpha_{1n} \\ \alpha_{21} & \alpha_{22} & \dots & \alpha_{2n} \\ \dots & \dots & \dots & \dots \\ \alpha_{n1} & \alpha_{n2} & \dots & \alpha_{nn} \end{pmatrix}$$

$$\boxed{X_e = A_{e\to g} X_g}$$

*Матрица $A_{e\to g}$ называется <u>матрицей перехода</u> от старого базиса $\{e_j\}$ к новому базису $\{g_j\}$. В её столбцах <u>стоят координаты нового базиса в старом.</u>*

***<u>Правило преобразования координат:</u>***
*Новый координатный столбец равен произведению матрицы перехода от нового базиса к старому на старый координатный столбец.*

$$\left|A_{e\to g}\right| \neq 0 \Rightarrow \ \exists A_{e\to g}^{-1}$$

$$\boxed{X_g = A_{e\to g}^{-1} X_e = A_{g\to e} X_e}$$

5. Подпространства. Лемма о базисе подпространства. Пересечение подпространств.

***<u>Определение подпространства:</u>***
*Подмножество M линейного (векторного) пространства L называется <u>подпространством</u>, если оно само является линейным (векторным) пространством относительно тех же самых операций, что были в L (сложение и умножение на число).*

*$L \supset M$ M – подпространство конечного пространства L*

***<u>Леммы:</u>***
1. *Базис любого подпространства можно дополнить до базиса всего пространства.*
   *<u>Док-во:</u>*
   *Пусть m=dim < n=dimL и $x_1, x_2, \dots, x_m$ - базис M.*
   *$\exists x_{m+1} \notin M \ \Rightarrow \ x_{1,} x_2, \dots, x_m, x_{m+1}$ – линейно независимы и т.д.*
2. *P и Q – подпространства L ⇒ P ∩ Q – подпространство L.*

6. Сумма подпространств. Теорема о размерностях суммы и пересечения подпространств.

***<u>Сумма подпротсранств:</u>***
*P+Q $\stackrel{\text{def}}{=}$ {x + y: x ∈ P, y ∈ Q} – сумма подпространств P и Q*

***<u>Теорема о размерностях суммы и пересечения подпространств:</u>***
*dim(P + Q) + dim(P ∩ Q) = dimP + dimQ.*
*<u>Док-во:</u>*
*Пусть S=P + Q, T=P ∩ Q и $x_1,\ x_2, \dots,\ x_t$ – базис T ≠ O.*
*$T \subset P \quad x_1,\ x_2, \dots,\ x_t,\ x_{t+1}, \dots,\ x_p$ – базис P*
*$T \subset Q \quad x_1,\ x_2, \dots,\ x_t,\ x'_{t+1}, \dots,\ x'_q$ – базис Q*
*a)* $x_1,\ x_2, \dots,\ x_t,\ x_{t+1}, \dots,\ x_p,\ x'_{t+1}, \dots,\ x'_q$ *- порождающая система для S*
*b)* $\alpha_1 x_1 + \ \dots \alpha_t x_t + \alpha_{t+1} x_{t+1} + \dots + \alpha_p x_p + \alpha'_{t+1} x'_{t+1} + \ \dots + \alpha'_q x'_q = 0$
$\alpha_1 x_1 + \ \dots \alpha_t x_t + \alpha_{t+1} x_{t+1} + \dots + \alpha_p x_p = -\alpha'_{t+1} x'_{t+1} - \ \dots - \alpha'_q x'_q = y$

$y \in T \Rightarrow \ \alpha_{t+1} = \dots = \alpha_p = 0 \ \Rightarrow \ \alpha_1 = \dots = \alpha_t = \alpha'_{t+1} = \dots = \alpha'_q = 0$

$x_1, x_2, \dots, x_t, x_{t+1}, \dots, x_p, x'_{t+1}, \dots, x'_q$ *- базис S* $\Rightarrow$ *dimS = p + (q - t)*

*Ч.Т.Д.*

7. Теорема о прямой сумме подпространств.

*Сумма подпространств P и Q называется прямой (обозначение P⊕Q), если любой вектор* ***z ∈ P + Q*** *записывается в виде* ***z = x + y****, где x ∈ P и y ∈ Q , единственным способом.*

***Теорема 2.***

*Если P и Q – два подпространства векторного пространства, то равносильны следующие три утверждения:*

1) *Сумма P + Q прямая;*
2) *P ∩ Q = O;*
3) *Объединение базисов P и Q – базис P + Q.*

8. Евклидово пространство. Неравенство Коши - Буняковского. Линейная независимость ортогональной системы векторов.

***Определение:***

*Вещественное векторное пространство L называется евклидовым, если*

*а) задано правило, по которому* $\forall x, y \in L$ *сопоставляется число (скалярное произведение) (x, y)∈* $\mathbb{R}$*;*

*б) это правило* $\forall x, y, z \in L$ *и* $\forall \lambda \in \mathbb{R}$ *удовлетворяет следующим требованиям:*

1. *(x, y) = (y, x),*
2. *(x + y, z) = (x, z) + (y, z),*
3. $(\lambda x, y) = \lambda(x, y)$,
4. $(x, x) > 0$, *если* $x \neq 0$, *и* $(0,0) = 0$.

***Неравенство Коши-Буняковского:***

*Для любых векторов в евклидовом пространстве*

$$(x, y)^2 \le \|x\|^2 \cdot \|y\|^2.$$

*Док-во:*

$$\forall t \in \mathbb{R}(x - ty, x - ty) \ge 0 \Leftrightarrow$$
$$\Leftrightarrow t^2\|y\|^2 - 2t(x, y) + \|x\|^2 \ge 0 \Leftrightarrow (x, y)^2 - \|x\|^2 \cdot \|y\|^2 \le 0$$

*Ч.Т.Д.*

***Определение ортогональных векторов:***

*Векторы называются ортогональными, если (x, y) = 0.*

***Линейная независимость ортогональной системы векторов:***

*Лемма:*

*Ортогональная система векторов линейно независима.*

*Док-во:*

*Пусть* $x_1, x_{2,\dots}, x_k$ *ортогональны.*

$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_k x_k = 0$

$\alpha_j(x_j, x_j) = \alpha_i \|X_j\|^2 = 0 \Rightarrow \alpha_j = 0\ \forall j$

*Ч.Т.Д.*

9. Теорема об ортогонализации. Следствия.

***Теорема об ортогонализации Грамма-Шмидта:***

*Пусть* $\boldsymbol{v_1}, \boldsymbol{v_2}, \dots, \boldsymbol{v_k}$ *– линейно независимая система векторов в евклидовом пространстве. Исходя из неё, можно построить ортогональную систему векторов* $\boldsymbol{v'_1}, \boldsymbol{v'_2}, \dots, \boldsymbol{v'_k}$*, такую что* $\boldsymbol{v'_1} = \boldsymbol{v_1}$, $\boldsymbol{v'_2} = \boldsymbol{v_2} + \boldsymbol{\gamma_{21} v_1}$; $\boldsymbol{v'_3} = \boldsymbol{v_3} + \boldsymbol{\gamma_{31} v_1} + \boldsymbol{\gamma_{32} v_2}$; …; $\boldsymbol{v'_k} = \boldsymbol{v_k} + \boldsymbol{\gamma_{k1} v_1} + \boldsymbol{\gamma_{k2} v_2} + \dots + \boldsymbol{\gamma_{k,k-1} v_{k-1}}$.

*Док-во:*

*Индукция по k.*

*k = 1 – очевидно.*

*Пусть верно для k – 1.*

$$v'_k = v_k + \beta v'_1 + \dots + \beta_k v'_{k-1}$$

$$(v_n^1, v_i^1) = (v_k, v'_i) + \beta_i(v'_i, v'_i) = 0 \ \Rightarrow\ \beta_i = -\frac{(v_k, v'_i)}{(v'_i, v'_i)}\ (1 \le i \le k-1)$$

$v'_k = v_k + \beta_1 v_1 + \beta_2(v_2 + \gamma_{21} v_1) + \dots = v_k + \gamma_{k1} v_1 + \dots + \gamma_{k,k-1}, v'_k \neq 0$ *(!)*

*Ч.Т.Д.*

***Следствия:***

1. *В любом евклидовом пространстве существует ортогональный базис.*
2. *В любом евклидовом пространстве существует ортогональный и нормированный (ортонормированный) базис. (если норма каждого базиса равна 1, то базис называется нормированным).*

10. Ортогональное дополнение подпространства, свойства.

***Определение:***

$S \supset P \quad dimS = n \quad dimP = k \quad (0 \le k \le n)$

*Ортогональное дополнение подпространства P:*

$P^\perp \overset{\text{def}}{=} \{x \in S: (x, y) = 0\ \forall y \in P\}$

*Множество, в котором все векторы из пространства S, которые ортогональны всем векторам из P. (определение.)*

$O^\perp = S, S^\perp = O$

*Лемма.*
*Ортогональное дополнение $P^{\perp}$ - подпространство евклидова пространства S.*

*Теорема.*
*Ортогональное дополнение $P^{\perp}$ подпространства P – это подпространство, натянутое на вектора, дополняющие ортогональный базис P до ортогонального базиса S.*
*Док-во:*
$e_1, e_2, \dots, e_k$ *– ортогональный базис подпространства P – дополним до ортогонального базиса пространства S:* $e_1, e_2, \dots, e_k, e_{k+1}, \dots, e_n$.

Q= $\langle e_{k+1}, \dots, e_n \rangle$ *– линейная оболочка этих векторов.*
*а)* $Q \subset P^{\perp}$;
*б)* $x = \lambda_1 e, +\lambda_2 e_2 + \cdots + \lambda_n e_n \in P^{\perp}$
$(x, e_i) = \lambda_i (e_i, e_i) = \lambda_i \|e_i\|^2 \Rightarrow \lambda_i = 0 \quad \forall i = 1,2, \cdots k$
$x \in Q \Rightarrow P^{\perp} \subset Q$
$P^{\perp} = Q$

***Свойства:***

- $dimP^{\perp} = dimS - dimP$;
- $(P^{\perp})^{\perp} = P$;
- $P_1 \subset P_2 \Rightarrow P_1^{\perp} \supset P_2^{\perp}$;
- $(P_1 + P_2)^{\perp} = P_1^{\perp} \cap P_2^{\perp}$;
- $(P_1 \cap P_2)^{\perp} = P_1^{\perp} + P_2^{\perp}$;
- $S = P \bigoplus P^{\perp}$ *(ортогональная сумма).*

11. Проекция вектора на подпространство. Матрица Грама.

***Проекция вектора на подпространство:***
$S = P \bigoplus P^{\perp} \quad \forall c \in S \quad c = a + b \quad \alpha \in P, b \in P^{\perp}$
*a – ортогональная проекция вектора c на подпространство P*
*b – ортогональная составляющая (проекция на* $P^{\perp}$*)*

*Пусть* $e_1, e_2, \dots, e_k$ *– ОНБ пространства P*
$a = \gamma_1 e_1 + \gamma_2 e_2 + \cdots + \gamma_k e_k$
$b = c - a \perp P \quad (c - a, e_i) = 0 \quad \forall i = 1, 2, 3, \dots, k$
$(c, e_i) = (a, e_i) = \gamma_i$

$$a = \sum_{i=1}^{k} (c, e_i) e_i, \quad b = c - a$$

*Лемма.*

*Проекция линейной комбинации векторов равна той же линейной комбинации проекций.*

***Матрица Грама:***

*Пусть* $x_1, x_2, \dots, x_k$ *– любой базис подпространства P*

$a = \gamma_1 x_1 + \gamma_2 x_2 + \dots + \gamma_k x_k \qquad (c, x_i) = (a, x_i) \quad \forall i = 1, 2, \dots, k$

$$(c, x_i) = (x_1, x_i)\gamma_1 + (x_2, x_i)\gamma_2 + \dots + (x_k, x_i)\gamma_k$$

*Матрица Грама:* $G = \begin{pmatrix} (x_1, x_1) & (x_2, x_1) & \dots & (x_k, x_1) \\ \dots & \dots & \dots & \dots \\ (x_1, x_k) & (x_2, x_k) & \dots & (x_k, x_k) \end{pmatrix} =$

$$= \begin{pmatrix} (x_1, x_1) & (x_1, x_2) & \dots & (x_1, k) \\ \dots & \dots & \dots & \dots \\ (x_k, x_1) & (x_k, x_2) & \dots & (x_k, x_k) \end{pmatrix}$$

*Определитель Грама:* $g(x_1, x_2, \dots, x_k) = |G| \neq 0$

12. Линейные операторы. Матрица линейного оператора. Изменение матрицы оператора при замене базиса.

***Линейные операторы:***

*L, M – векторные пространства над полем k*

$\mathcal{A}: L \to M$ *– оператор (отображение) из L в M*

$x \in L \;\; y = \mathcal{A}x \in M$ *y – образ вектора x, x – прообраз вектора y*

$\mathcal{A}$ *- линейный оператор, если*

*1)* $\mathcal{A}(x_1 + x_2) = \mathcal{A}x_1 + \mathcal{A}x_2 \quad \forall x_1, x_2 \in L;$

*2)* $\mathcal{A}(\mu x) = \mu\mathcal{A}x \quad \forall \mu \in k, \forall x \in L. \quad (\Rightarrow \mathcal{A}0 = 0)$

***Матрица линейного оператора:***

*dimL = n, dim = m,* $\mathcal{A}: L \to M$

$e_1, e_2, \dots, e_n$ *– базис L,* $g_1, g_2, \dots, g_m$ *– базис M*

$$\begin{cases} \mathcal{A}e_1 = a_{11}g_1 + a_{21}g_2 + \dots + a_{m1}g_m \\ \mathcal{A}e_2 = a_{12}g_1 + a_{22}g_2 + \dots + a_{m2}g_m \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots. \\ \mathcal{A}e_n = a_{1n}g_1 + a_{2n}g_2 + \dots + a_{mn}g_m \end{cases}$$

$$\mathscr{A} e_j = \sum\nolimits_{i=1}^{m} a_{ij} g_i \quad (j = 1, 2, \dots, n)$$

$A_{g,e} = \begin{pmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} \end{pmatrix}$ *– матрица оператора $\mathscr{A}$ в базисах $\{e_j\}$ и $\{g_i\}$.*

*Столбцами матрицы $A_{g,e}$ являются координаты векторов $\mathscr{A}e_1, \mathscr{A}e_2, \dots, \mathscr{A}e_n$ относительно базиса $g_1, g_2, \dots, g_m$.*

$$x \in L; \quad x = \sum_{j=1}^{n} \mu_j e_j; \quad y = \mathscr{A} x = \sum_{i=1}^{m} v_i g_i \in M$$

$$y = \sum_{i=1}^{m} v_i g_i = \mathscr{A}\left(\sum_{\mathrm{j}=1}^{\mathrm{n}} \mu_j e_j\right) = \sum_{i=1}^{n} \mu_j \mathscr{A} e_j = \sum_{i=1}^{n} \mu_j \left(\sum_{i=1}^{m} a_{ij} g_i\right) =$$

$$= \sum\nolimits_{i=1}^{m} \left(\sum\nolimits_{j=1}^{n} a_{ij}\mu_j\right) g_i$$

$$v_i = \sum_{i=1}^{n} a_{ij}\mu_j \quad (i = 1, 2, \dots, m)$$

$$(*)\begin{cases} v_1 = a_{11}\mu_1 + a_{12}\mu_2 + \cdots + a_{1n}\mu_n \\ v_2 = a_{21}\mu_1 + a_{22}\mu_2 + \cdots + a_{2n}\mu_n \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ v_m = a_{m1}\mu_1 + a_{m2}\mu_2 + \cdots + a_{mn}\mu_n \end{cases}$$

$$X_e = \begin{pmatrix} \mu_1 \\ \mu_2 \\ \dots \\ \mu_n \end{pmatrix} \quad Y_g = \begin{pmatrix} v_1 \\ v_2 \\ \dots \\ v_m \end{pmatrix} \quad (*) \quad \boxed{Y_g = A_{g,e} X_e} \qquad (A_{e,e} = A_e)$$

*Пусть теперь A=$\{a_{ij}\}_{m,n}$ – произвольная матрица из $M_{n,k}(k)$.*

*Если $x = \sum\nolimits_{j=1}^{n} \mu_j e_j$, то по (*) находим $y = \sum_{i=1}^{m} v_i g_i$. Получили оператор (линейный!) с матрицей $A_{g,e} = A$ в базисах $\{e_j\}$ и $\{g_i\}$.*

***<u>Изменение матрицы оператора при замене базиса:</u>***

$\mathscr{A}$ : L $\to L$, $\{e_i\}$ и $\{g_i\}$ *– два базиса L*

*$x \in L$, $y = \mathscr{A}x \Rightarrow$* $Y_e = A_e X_e$ и $Y_g = A_g X_g$ $(A_g = ?)$

$$X_e = T_{e \to g} X_g, \;\; Y_e = T_{e \to g} Y_g \;\Rightarrow\; T_{e \to g} Y_g = A_e T_{e \to g} X_g$$

*($T_{e\to g}$ – матрица перехода от базиса $\{e_i\}$ к базису $\{g_i\}$)*

$$Y_g = T_{e\to g}^{-1} A_e T_{e\to g} X_g = T_{g\to e} A_e T_{e\to g} X_g$$

$$\boxed{A_g = T_{g\to e} A_e T_{e\to g} = T_{e\to g}^{-1} A_e T_{e\to g}}$$

*Лемма.*

*Определитель матрицы линейного оператора не зависит от выбора базиса.*

13. Ядро и образ линейного оператора. Теорема о размерностях ядра образа.

$\mathcal{A} : L \to M$

$\ker \mathcal{A} = \{x \in L : \mathcal{A}x = 0\}$ – ядро оператора $\mathcal{A}$

$\operatorname{im} \mathcal{A} = \mathcal{A}L = \{y \in M : \exists x \in L$ такой, что $\mathcal{A}x = y\}$ – *образ оператора* $\mathcal{A}$

*Теорема.*

*Ядро и образ линейного оператора $\mathcal{A}$ – подпространства соответствующих пространств L и M.*

$\dim \ker\mathcal{A} = d_{\mathcal{A}}$ – *дефект оператора* $\mathcal{A}$

$\dim \operatorname{im}\mathcal{A} = r_{\mathcal{A}}$ – *ранг оператора* $\mathcal{A}$

*Теорема.*

$$\boxed{d_{\mathcal{A}} r_{\mathcal{A}} = dimL}$$

*Док-во:*

*Пусть* $b_1, b_2, \dots, b_r$ – *базис* $im\mathcal{A}$. *Пусть* $\forall i\ a_i \in L$ *такой, что* $\mathcal{A}a_i = b_i$ $(1 \le i \le r)$. $\{a_i\}$ *линейно независимы.*

*Пусть* $P = \langle\{a_i\}\rangle \subset L$, $\dim P = r$. *Докажем, что* $L = P \oplus ker\mathcal{A}$.

*а)* $P \cap ker\mathcal{A} = 0$

*Пусть* $a \in P \cap ker\mathcal{A}$. $\quad a = \sum_{i=1}^{r} \gamma_i a_i$

$\mathcal{A}a = \sum_{i=1}^{\gamma} \gamma_i \mathcal{A} a_i = \sum_{i=1}^{\gamma} \gamma_i b_i = 0 \Rightarrow \gamma_i = 0\ \forall i \Rightarrow a = 0$

*б)* $L = P + ker\mathcal{A}$

*Пусть* $a \in L$. $\quad \mathcal{A}a = \sum_{i=1}^{\sigma} \beta_i b_i$

*Пусть* $a_0 = \sum_{i=1}^{\gamma} \beta_i a_i$, $c = a - a_0$.

$\mathcal{A}c = \mathcal{A}a - \mathcal{A}a_0 = 0 \Rightarrow c \in ker\mathcal{A} \qquad a = a_0 + c$

$$L = P \oplus ker\mathcal{A} \Rightarrow \dim L = \dim P + \dim ker\mathcal{A}$$

*Ч.Т.Д.*

14. Собственные векторы и собственные значения линейного оператора. Свойства собственных векторов.

*L – пространство над полем k,* $\mathscr{A}: L \to L$
*Если существует ненулевой вектор* $x \in L$ *и число* $\lambda \in k$*, такие что*
$\mathscr{A}x = \lambda x,$
*то число* $\lambda$ *называется собственным значением (собственным числом) оператора* $\mathscr{A}$*, а вектор x – собственным вектором оператора* $\mathscr{A}$*.*

*Лемма 1. Любому собственному вектору соответствует единственное собственное значение.*

$$\mathscr{A}x = \lambda_1 x, \mathscr{A}x = \lambda_2 x \Rightarrow (\lambda_1 - \lambda_2)x = 0 \Rightarrow \lambda_1 = \lambda_2$$

*Лемма 2. Если* $x_1$ *и* $x_2$ *– собственные вектора оператора* $\mathscr{A}$ *с одним и тем же собственным значением* $\lambda$*, то любая их линейная комбинация или равна 0, или является собственным вектором оператора* $\mathscr{A}$ *с собственным значением* $\lambda$*.*

$$\mathscr{A}(\mu_1 x_1 + \mu_2 x_2) = \mu_1 \mathscr{A}x_1 + \mu_2 \mathscr{A}x_2 = \mu_1 \lambda x_1 + \mu_2 \lambda x_2 = \lambda(\mu_1 x_1 + \mu_2 x_2)$$

*Следствие. Для любого собственного значения λ все собственные вектора вместе с нулевым вектором образуют подпространства пространства L.*

*Следствие. В n-мерном пространстве линейный оператор не может иметь более n собственных векторов с различными собственными значениями.*

15. Теорема о характеристическом многочлене линейного оператора.

*Теорема 1. Все собственные значения линейного оператора совпадают с корнями характеристического многочлена матрицы этого оператора в каком-нибудь базисе.*
*Замечание. Характеристические многочлены подобных матриц равны:*
*Пусть* $B = T^{-1}AT$*, тогда*

$$B - \lambda E = T^{-1}AT - \lambda E = T^{-1}AT - \lambda T^{-1}ET = T^{-1}(A - \lambda E)T$$

*По лемме* $|B - \lambda E| = |A - \lambda E|$

*Т.о.,* $\varphi(\lambda)$ *можно называть характеристическим многочленом оператора* $\mathscr{A}$*.*

*n = 2*

$$A\begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \Rightarrow \varphi(\lambda) = \begin{vmatrix} a_{11} - \lambda & a_{12} \\ a_{21} & a_{22} - \lambda \end{vmatrix} = \lambda^2 - (a_{11} + a_{22})\lambda + \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix}$$

*Для произвольного n:*

$$A = \{a_{ij}\}_{n,n} \Rightarrow \varphi(\lambda) = (-1)^n \lambda^n + (-1)^{n-1}(a_{11} + a_{22} + \cdots + a_{nn})\lambda^{n-1} + \cdots + |A|$$

*Теорема 2.(Гамильтона-Кэли) Если* $\varphi(\lambda)$ *– характеристический многочлен* *оператора $\mathscr{A}$, то $\varphi(\mathscr{A}) = 0$.*

16. Теорема о линейной независимости собственных векторов. Матрица линейного оператора в базисе из собственных векторов.

*Теорема. Собственные вектора $x_1, x_2, \dots, x_m$ оператора $\mathscr{A}$, имеющие попарно различные собственные значения $\lambda_1, \lambda_2, \dots, \lambda_m$ , линейно независимы.*

*Док-во (индукцией по m):*

*1) m=1.*

*2) Пусть теорема верна для m – 1.*

*3) Предположим, что $x_1, x_2, \dots, x_m$ линейно независимы.*

$$\alpha_1 x_1 + \alpha_2 x_2 + \dots + \alpha_m x_m = 0 \quad (*)$$

*и пусть $\alpha_1 \neq 0$*

$$\alpha_1 \mathscr{A} x_1 + \alpha_2 \mathscr{A} x_2 + \dots + \alpha_m \mathscr{A} x_m = 0$$

$$\alpha_1 \lambda_1 x_1 + \alpha_2 \lambda_2 x_2 + \dots + \alpha_m \lambda_m x_m = 0$$

$$(*) \cdot \lambda_m = \alpha_1 \lambda_m x_1 + \alpha_2 \lambda_m x_2 + \dots + \alpha_m \lambda_m x_m = 0$$

$$\alpha_1(\lambda_1 - \lambda_m) x_1 + \alpha_2(\lambda_2 - \lambda_m) x_2 + \dots + \alpha_{m-1}(\lambda_{m-1} - \lambda_m) x_{m-1} = 0$$

$$\alpha_1 = \alpha_2 = \dots = \alpha_{m-1} = 0 \text{ – \textit{противоречие.}}$$

*Ч.Т.Д.*

*Матрица:*

$$\mathscr{A} g_1 = \lambda_1 g_1 + 0 \cdot g_2 + \dots + 0 \cdot g_n \text{ \textit{и т.д.}} \Rightarrow A_g = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \dots & 0 \\ \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & \lambda_n \end{pmatrix}$$

*<u>Теорема.</u> Пусть $\mathscr{A}$ – действующий в n-мерном пространстве над полем k линейный оператор. Если характеристический многочлен оператора в $\mathscr{A}$ имеет n различных корней в поле k, то матрица этого оператора в базисе из собственных векторов является диагональной, и диагональные элементы этой матрицы – это собственные значения оператора $\mathscr{A}$.*

*<u>Геометрический смысл.</u> В пространстве L имеется n таких «направлений», что любой вектор, имеющий одно из этих «направлений», преобразуется оператором $\mathscr{A}$ в коллинеарный.*

*<u>Замечание.</u> В случае кратных корней характеристического многочлена оператора его матрица всё равно <u>может</u> оказаться диагонализируемой (если число линейно независимых собственных векторов совпадет с размерностью пространства).*

17.Сопряженные операторы в евклидовом пространстве.

*Пусть $\mathcal{A}$ – линейный оператор в евклидовом пространстве S. Линейный оператор $\mathcal{A}^*$ называется сопряженным с $\mathcal{A}$, если для всех $x, y \in S$*

$$(\mathcal{A}x, y) = (x, \mathcal{A}^* y)$$

*Теорема 1. Для любого линейного оператора $\mathcal{A}$ существует единственный сопряженный оператор. Его матрица в любом ОНБ является транспонированной к матрице оператора $\mathcal{A}$.*

*Док-во:*

$$A = \{a_{ij}\}_{n,n}, X = (x_1, x_2, \dots, x_n)^T, Y = (y_1, y_2, \dots, y_n)^T$$

$$(\mathcal{A}x, y) = (AX, Y)_n = \left(\left(\sum_{i=1}^{n} a_{1i}x_i, \dots, \sum_{i=1}^{n} a_{ni}x_i\right)^T, (y_1, \dots, y_n)^T\right) =$$

$$= \sum_{i=1}^{n} a_{1i}x_i y_1 + \dots + \sum_{i=1}^{n} a_{ni}x_i y_n = x_1 \sum_{j=1}^{n} a_{j1}y_j + \dots + x_n \sum_{j=1}^{n} a_{jn}y_j =$$

$$= (X, A^T Y)_n = (x, \mathcal{A}^* y)$$

*Ч.Т.Д.*

*Единственность доказывается от противного:*

$$(\mathcal{A}x, y) = (x, \mathcal{A}^* y) = \left(x, \tilde{\mathcal{A}}y\right) \Rightarrow \left(x, \left(\mathcal{A}^* - \tilde{\mathcal{A}}\right)y\right) = 0 \quad \forall x \Rightarrow \left(\mathcal{A}^* - \tilde{\mathcal{A}}\right)y = 0 \quad \forall y$$

$$\Rightarrow \mathcal{A}^* - \tilde{\mathcal{A}} = O \Rightarrow \mathcal{A}^* = \tilde{\mathcal{A}}$$

*Замечание. Свойства $\mathcal{A}^*$ соответствуют всем свойствам $A^T$.*

18.Ортогональные матрицы. Ортогональные операторы.

***Определение ортогональной матрицы:***

*Вещественная матрица P называется ортогональной, если $P^{-1} = P^T$.*

$PP^T = E$ ⇒ *строки матрицы P ортогональны и нормированы*

$P^T P = E$ ⇒ *столбцы матрицы P ортогональны и нормированы*

***Определение ортогонального оператора:***

*Оператор $\mathcal{P}$ называется ортогональным, если для всех $x, y \in S$*

$(\mathcal{P}x, \mathcal{P}y) = (x, y)$.

*Свойства ортогонального оператора $\mathcal{P}$:*

1) $\mathcal{P}^* = \mathcal{P}^{-1}$;

2) $\forall x\ \|\mathcal{P}x\| = \|x\|$;

3) *$\mathcal{P}$ сохраняет углы;*

4) *$\mathcal{P}$ переводит любую ортонормированную систему векторов;*

5) *Матрица $\mathcal{P}$ в ОНБ ортогональна;*

6) *Все вещественные собственные значения $\mathcal{P}$ равны или 1, или -1.*

*Замечание. Все мнимые корни характеристического многочлена оператора $\mathscr{P}$, если они есть, также имеют модуль, равный 1.*

19.Свойства собственных значений симметричного оператора.

*Все собственные значения симметричного оператора – вещественные.*
*Док-во:*

$$\mathscr{A}x = \lambda x, x \neq 0, \lambda \in \mathbb{C}$$

*В выбранном ОНБ* $AX = \lambda X, X \in \mathbb{C}_n$

*а)* $\overline{AX} = \overline{\lambda X} \Rightarrow A\bar{X} = \bar{\lambda}\bar{X} \Rightarrow X^T A\bar{X} = \bar{\lambda} X^T \bar{X} = \bar{\lambda} \sum_{k=1}^{n} |x_k|^2$

*б)* $(AX)^T = (\lambda X)^T \Rightarrow X^T A = \lambda X^T \Rightarrow X^T A\bar{X} = \lambda X^T \bar{X} = \lambda \sum_{k=1}^{n} |x_k|^2$

$$\bar{\lambda} = \lambda \Leftrightarrow \lambda \in \mathbb{R}$$

*Ч.Т.Д.*

20.Свойства собственных векторов симметричного оператора.

*Собственные вектора симметричного оператора, принадлежащие разным собственным значениям, ортогональны.*
*Док-во:*

$$\mathscr{A}x = \lambda x, \mathscr{A}y = \mu y, (\mathscr{A}x, y) = (x, \mathscr{A}y)$$

$$(\lambda x, y) = (x, \mu y) \Rightarrow \lambda(x, y) = \mu(x, y) \Rightarrow (\lambda - \mu)(x, y) = 0 \Rightarrow (x, y) = 0$$

*Ч.Т.Д.*

*Теорема 2.*
*Если $\mathscr{A}$ – симметричный оператор в евклидовом пространстве S, то в S существует ОНБ, состоящий из собственных векторов оператора $\mathscr{A}$.*

21.Квадратичные формы, матричная запись. Линейное преобразование переменных в квадратичной форме.

*Квадратичной формой называется однородный многочлен* $f = f(x_1, x_2, \dots, x_n) \in k[x_1, x_2, \dots, x_n]$ *второй степени от n переменных.*

$$[f(tx_1, tx_2, \dots, tx_n) = t^2 f(x_1, x_2, \dots, x_n)]$$

$$(*) \quad \begin{aligned} f(x_1, x_2, \dots, x_n) = a_{11}x_1^2 + a_{12}x_1x_2 + \dots + a_{1n}x_1x_n + \\ a_{21}x_2x_1 + a_{22}x_2^2 + \dots + a_{2n}x_2x_n + \dots + \\ + a_{n1}x_nx_1 + a_{n2}x_nx_2 + \dots + a_{nn}x_n^2 \end{aligned}$$

$$\underline{a_{ij} = a_{ji} \quad \forall i, j}$$

$$A = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{pmatrix}$$ *– матрица квадратичной формы (симметрическая!)*

*Линейное преобразование:*

$$\begin{cases} x_1 = c_{11}y_1 + c_{12}y_2 + \dots + c_{1n}y_n \\ x_2 = c_{21}y_1 + c_{22}y_2 + \dots + c_{2n}y_n \\ \dots \\ x_n = c_{n1}y_1 + c_{n2}y_2 + \dots + c_{nn}y_n \end{cases} \qquad X = CY$$

*Если* $|C| \neq 0$*, то* $Y = C^{-1}X$ *(невырожденное линейное преобразование).*

$$f(x_1, x_2, \dots, x_n) = X^TAX = (CY)^TACY = Y^TC^TACY = Y^T(C^TAC)Y$$
$$B = C^TAC, \;\; B^T = C^TA^TC = C^TAC = B, \;\; Y^TBY = g(y_1, y_2, \dots, y_n)$$

22. Метод Лагранжа приведения квадратичной формы к диагональному виду. Закон инерции (без док-ва).

***Теорема (Лагранжа).*** Любая квадратичная форма при помощи невырожденного линейного преобразования может быть приведена к диагональному виду.

Док-во: индукция по числу переменных.

*1) n = 1*

*2) Пусть для n - 1 утверждение теоремы верно.*

*3) см. (*) из 21 вопр. Считаем, что* $a_{11} \neq 0$.

$$f(x_1, x_2, \dots, x_n) = a_{11}x_1^2 + 2a_{12}x_1x_2 + \dots + 2a_{1n}x_1x_n + g(x_2, x_3, \dots, x_n)$$
$$= a_{11}\left(x_1 + \frac{a_{12}}{a_{11}}x_2 + \dots + \frac{a_{1n}}{a_{11}}x_n\right)^2 + f_1(x_2, x_3, \dots, x_n)$$

$$\begin{cases} y_1 = x_1 + \frac{a_{12}}{a_{11}}x_2 + \dots + \frac{a_{1n}}{a_{11}}x_n \\ y_k = x_k \quad \forall k \geq 2 \end{cases} \qquad \begin{cases} x_1 = y_1 + \frac{a_{12}}{a_{11}}y_2 + \dots + \frac{a_{1n}}{a_{11}}y_n \\ x_k = y_k \quad \forall k \geq 2 \end{cases}$$

$$f(x_1, x_2, \dots, x_n) = a_{11}y_1^2 + f_1(y_2, y_3, \dots, y_n)$$

$y_1 = z_1$*; существует невырожденное преобразование:*

$$f_1(y_2, y_3, \dots, y_n) = \alpha_2 z_2^2 + \alpha_3 z_3^2 + \dots + \alpha_n z_n^2 \Rightarrow \underline{f = a_{11}z_1^2 + \alpha_2 z_2^2 + \dots \alpha_n z_n^2}$$

***Закон инерции.*** *Число положительных и отрицательных коэффициентов в диагональном виде вещественной квадратичной формы не зависит от способа приведения этой формы вещественными невырожденными преобразованиями к диагональному виду.*

23. Приведение квадратичной формы к диагональному виду ортогональным преобразованием.

<u>$k = \mathbb{R}$</u>

*Теорема (приведение квадратичной формы к главным осям). Любая вещественная квадратичная форма $f(x_1, x_2, \dots, x_n)$ с матрицей A при помощи некоторого ортогонального преобразования переменных X = CY может быть приведена к диагональному виду*

$$\lambda_1 y_1^2 + \lambda_2 y_2^2 + \dots + \lambda_n y_n^2 \qquad (1)$$

*Коэффициенты $\lambda_1, \lambda_2, \dots, \lambda_n$ совпадают с собственными значениями матрицы A. Столбцы $T_1, T_2, \dots, T_n$ ортогональной матрицы C являются собственными векторами матрицы A, соответствующими собственным значениям $\lambda_1, \lambda_2, \dots, \lambda_n$.*

*Док-во:*

1) *Пусть получен вид (1), тогда*

$$C^T A C = \begin{pmatrix} \lambda_1 & 0 & \dots & 0 \\ 0 & \lambda_2 & \cdots & 0 \\ \dots & \dots & \cdots & \dots \\ 0 & 0 & \cdots & \lambda_n \end{pmatrix} = B \quad (2)$$

$$\varphi_B(\lambda) = |B - \lambda E| = (\lambda_1 - \lambda)(\lambda_2 - \lambda)\dots(\lambda_n - \lambda)$$

$$C^T A C = C^{-1} A C = B \Rightarrow \varphi_A(\lambda) = \varphi_B(\lambda) = (\lambda_1 - \lambda)(\lambda_2 - \lambda)\dots(\lambda_n - \lambda)$$

$$(2) \Rightarrow AC = CB: \;\; A(T_1 T_2 \dots T_n) = (T_1 T_2 \dots T_n)B \Rightarrow AT_1 = \lambda, T_1 \text{ и т.д.}$$

2) *Существование преобразования - по индукции.*
   *n = 1 (любая форма от одной переменной диагональна)*

   *Пусть для n – 1 утверждение верно.*

   $AT = \lambda T, \|T\| = 1; \quad \lambda \in \mathbb{R},$ *т.к.* $A^T = A;$
   $T, T_2, T_3, \dots, T_n$ – *ОНБ* $\mathbb{R}_n \qquad C_1 = (TT_2 \dots T_n)$ – *ортогональная матрица*

   $X = C_1 Y \qquad C_1^T A C_1 = C_1^T A (TT_2 \dots T_n) = C_1^T (AT\ AT_2 \dots AT_n) =$

$$\begin{pmatrix} T^T \\ T_2^T \\ \dots \\ T_n^T \end{pmatrix} (\lambda T \dots \dots) = \begin{pmatrix} \lambda T^T T & \vdots & \vdots \\ \lambda T_2^T T & \dots & \dots \\ \dots & & \\ \lambda T_n^T T & \cdots & \dots \end{pmatrix} = \begin{pmatrix} \lambda & \vdots & \vdots \\ 0 & \dots & \dots \\ \dots & & \\ 0 & \cdots & \dots \end{pmatrix} = \begin{pmatrix} \lambda & 0 & \dots & 0 \\ 0 & \vdots & \cdots & \vdots \\ \vdots & \vdots & \dots & \dots \\ 0 & \dots & \dots & \dots \end{pmatrix}$$

$$f(x_1, x_2, \dots, x_n) = \lambda y_1^2 + g(y_2, y_3, \dots, y_n)$$

*Пусть* $g(y_2, y_3, \dots, y_n) = \lambda_2 z_2^2 + \dots + \lambda_n z_n^2$ *– с помощью ортогонального преобразования с матрицей D (порядка n – 1).*

$C_2 = \begin{pmatrix} 1 & 0 \\ 0 & D \end{pmatrix}$ *– ортогональная матрица.* $Y = C_2 Z$:

$y_1 = z_1$ *и* $g(y_2, y_3, \dots, y_n) = \lambda_2 z_2^2 + \dots + \lambda_n z_n^2$

$C = C_1 C_2$ *– ортогональная матрица.* $X = CZ$:

$$f(x_1, x_2, \dots, x_n) = \lambda_1 z_1^2 + \lambda_2 z_2^2 + \dots + \lambda_n z_n^2$$

*Ч.Т.Д.*

*Замечания.*

*1. Если C – ортогональная матрица из собственных векторов матрицы A, то X = CY и приводит форму к диагональному виду.*

*2. Собственные векторы, соответствующие разным собственным значениям уже ортогональны.*

24.Классификация центральных поверхностей второго порядка.

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz + b_1 x + b_2 y + b_3 z + d = 0$$
$(\exists a_{ij} \neq 0)$

$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ *– матрица (симметрическая) квадратичной формы*

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz$$

$C^T A C = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}$, $\lambda_1 > 0$, $C^{-1} = C^T$

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz = \lambda_1 x_1^2 + \lambda_2 y_1^2 + \lambda_3 z_1^2$$

*I)* $r_A = 3$ *(центральные поверхности 2-го порядка)*

*a)* $\lambda_1 > 0, \lambda_2 > 0, \lambda_3 > 0$: $\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2}$ *=1 или -1, или 0*

$\frac{x^2}{a^2} + \frac{y^2}{b^2} + \frac{z^2}{c^2} = 1$ *– эллипсоид*

*Симметричен относительно координат плоскостей, осей и НК.*

*(0;0;0) – центр эллипсоида;*

*Точки пересечения с координатными осями – вершины эллипсоида;*

*a, b, c – полуоси эллипсоида (a ≥ b ≥ c в каноническом уравнении).*

*б)* $\lambda_1 > 0, \lambda_2 > 0, \lambda_3 < 0$: $\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2}$ *=1 или -1, или 0*

$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 1$ *– однополостный гиперболоид*

$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = -1$ *– дву(х)полостный гиперболоид*

*Симметричны относительно координатных плоскостей, осей и НК.*
*(0;0;0) – центр гиперболоидов;*
*Точки пересечения с координатными осями – вершины гиперболоидов;*
*a, b – поперечные полуоси гиперболоидов (*$a \geq b$ *в канонических уравнениях), c – продольная полуось.*

$\frac{x^2}{a^2} + \frac{y^2}{b^2} - \frac{z^2}{c^2} = 0$ *– конус 2-го порядка*
*(*$a \geq b$ *в канонических уравнениях)*

*Симметричен относительно координатных плоскостей, осей и НК.*
*(0;0;0) – центр и вершина конуса.*
*Сечение конуса может быть эллипсом (если плоскость пересекает все образующие), гиперболой (если плоскость параллельна двум образующим), параболой (если плоскость параллельна одной образующей).*

25.Классификация нецентральных поверхностей второго порядка.

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz + b_1x + b_2y + b_3z + d = 0$$
$$\left(\exists a_{ij} \neq 0\right)$$

$A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$ *– матрица (симметрическая) квадратичной формы*

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz$$

$C^T A C = \begin{pmatrix} \lambda_1 & 0 & 0 \\ 0 & \lambda_2 & 0 \\ 0 & 0 & \lambda_3 \end{pmatrix}, \lambda_1 > 0,\ C^{-1} = C^T$

$$a_{11}x^2 + a_{22}y^2 + a_{33}z^2 + 2a_{12}xy + 2a_{13}xz + 2a_{23}yz = \lambda_1 x_1^2 + \lambda_2 y_1^2 + \lambda_3 z_1^2$$

*II)* $r_A = 2$
*а)* $\lambda_1 > 0, \lambda_2 > 0, \lambda_3 = 0$: $\frac{x^2}{a^2} + \frac{y^2}{b^2} = z$ *или 1, или -1, или 0*
$\frac{x^2}{a^2} + \frac{y^2}{b^2} = z$ *– эллиптический параболоид*
*(*$a \geq b$ *в каноническом уравнении)*

*(0;0;0) – вершина эллиптического параболоида.*
*Oz – ось симметрии (есть плоскости симметрии, как и у всех поверхностей 2-го порядка)*

$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 1$ *– эллиптический цилиндр*

$\frac{x^2}{a^2} + \frac{y^2}{b^2} = 0$ - *прямая* $\frac{x}{0} = \frac{y}{0} = \frac{z}{0}$
*(*$a \geq b$ *в каноническом уравнении)*

*б)* $\lambda_1 > 0, \lambda_2 < 0, \lambda_3 = 0$: $\frac{x^2}{a^2} - \frac{y^2}{b^2} = z$ *или 1, или 0*
$\frac{x^2}{a^2} - \frac{y^2}{b^2} = z$ *– гиперболический параболоид*

*(0;0;0) – вершина гиперболического параболоида.*
*Oz – ось симметрии*

$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 1$ *– гиперболический цилиндр*

$\frac{x^2}{a^2} - \frac{y^2}{b^2} = 0$ *– две пересекающиеся плоскости* $bx \pm ay = 0$

*III)* $r_A = 1$
*а)* $\lambda_1 > 0, \lambda_2 = \lambda_3 = 0$: $\frac{x^2}{a^2} = y$ *или 1, или -1, или 0*
$\frac{x^2}{a^2} = y$ *– параболический цилиндр*

*Замечания.*
*1) уравнения вида* $\lambda_1 x^2 + c_2 y + c_3 z + d = 0$ *ортогональным преобразованием (поворотом плоскости Oyz) приводится к виду* $\lambda_1 x^2 + c_2' y + d = 0$.
*2)Ортогональным преобразованием уравнение параболического цилиндра можно привести к виду* $y^2 = 2px$ *(p > 0).*

$y^2 = 2px$ *– параболический цилиндр*
$x^2 = a^2$ *– две параллельные плоскости* $x \pm a = 0$
$x^2 = 0$ *– плоскость x = 0*

## 26.Группы. Симметрические группы. Подгруппы.

*Множество G с бинарной операцией «·» называется группой, если:*
*Операция «·» ассоциативна; в G существует нейтральный элемент e; для*

*любого $a \in G$ существует обратный элемент, т.е. такой элемент $a' \in G$, что $a \cdot a' = a' \cdot a = e$.*

*Если, кроме того, операция «·» коммутативна, то группа G называется коммутативной, или абелевой.*

*<u>Теорема.</u> Пусть группа G – группа с нейтральным элементом e. Тогда e – единственный нейтральный элемент в группе. Кроме того, любой элемент группы G обладает единственным обратным элементом.*

*<u>Док-во:</u> предположим, что какой-то элемент c также является нейтральным элементом группы G. Тогда c = ce = e. Если же $a'$ и b – два обратных элемента для $a \in G$, то b = be = b(ad) = (ba) $a'$=e$a'$=$a'$.*

*Ч.Т.Д.*

*Если M = $\{1, 2, \dots, n\}$, то любое отображение M на себя – это подстановка*

$$s = \begin{pmatrix} 1 & 2 & \dots & n \\ a_1 & a_2 & \dots & a_n \end{pmatrix}, \text{ где } a_i = s(i) \quad \forall i = 1, 2, \dots, n.$$

*$\{a_1, a_2, \dots, a_n\}$ – это перестановка $\{1, 2, \dots, n\}$, их число n! равно числу элементов группы S($\{1, 2, \dots, n\}$) = $S_n$. Она называется симметрической группой степени n.*

*Подгруппой группы G = (G,·) называется такое подмножество $H \subset G$, которое само является группой относительно операции «·», заданной в G*
*(запись: H <G).*

*Теорема. H < G = (G,·)$\Leftrightarrow$ $\forall a, b \in H \;\; ab \in H; \; \forall a \in H \;\; a^{-1} \in H$.*
*Замечания:*
*1) H <G,·)$\Leftrightarrow$ $\forall a, b \in H \;\; ab^{-1} \in H$*
*2) Если H – конечное подмножество группы G, то H < G $\Leftrightarrow$ $\forall a, b \in H \;\; ab \in H$*

*Теорема 2. Пересечение двух (и вообще любого количества) подгрупп группы является подгруппой той же группы.*

27. Гомоморфизмы групп. Гомоморфный образ и полный прообраз подгруппы. Теорема Кэли (без док-ва).

*Пусть ($G_1$,·) и ($G_2$,∗) – две группы, а f – отображение множества $G_1$ в множество $G_2$. Отображение f называется гомоморфизмом группы $G_1$ в группу $G_2$, если для любых $\forall a, b \in G_1$ имеет место равенство f(a·b)=f(a)∗f(b).*

*Гомоморфизм $f: G_1 \to G_2$ называется эпиморфизмом $G_1$ на $G_2$, если каждый элемент из $G_2$ является образом хотя бы одного элемента из $G_1$, т.е. $f(G_1) =$
$= G_2$.*

*Гомоморфизм $f: G_1 \to G_2$ называется мономорфизмом $G_1$ на $G_2$, если он разные* *элементы $G_1$ отображает в $G_2$.*

*Если $f: G_1 \to G_2$ – гомоморфизм групп, то образ всей группы $f(G_1)$ называют также образом гомоморфизма f и обозначают $\mathrm{im}\, f$.*
*Ядром гомоморфизма f (запись: ker f) называется полный прообраз подгруппы $\{e_2\}$, состоящей из одного нейтрального элемента $e_2$ группы $G_2$.*
*Теорема Кэли.*
*Всякая конечная группа порядка n изоморфна некоторой подгруппе симметрической группы $S_n$.*
*Следствие. Существует лишь конечное число неизоморфных конечных групп фиксированного порядка n.*

28. Смежные классы. Индекс подгруппы в группе. Теорема Лагранжа.

*H <G = (G, ·); на G определим отношение эквивалентности ~:*

$$a \sim b \Leftrightarrow a^{-1}b \in H$$

*(другими словами, b =ah, где $h \in H$, или короче: $b \in aH$).*
*Соответствующие классы эквивалентности $K_a = aH$ называются левыми смежными классами группы G по подгруппе H.*

*Аналогично определяют правые смежные классы Ha с помощью условия $ba^{-1} \in H$ при введении отношения эквивалентности. В коммутативных группах понятия левых и правых смежных классов совпадают, поскольку aH = Ha.*

*<u>Замечание.</u> Если подгруппа H конечна, то все смежные классы по этой подгруппе имеют одинаковое число элементов, равное | H |.*

*Индексом (G: H) подгруппы H в группе G называется число различных левых (равно как и правых) смежных классов по подгруппе H, если это число конечно.*

*Теорема Лагранжа.*
*Порядок конечной группы G равен произведению порядка подгруппы H на индекс этой подгруппы, т.е. $|G| = |H| \cdot (G: H)$.*

*Следствие.*
*Порядок подгруппы конечной группы является делителем порядка группы.*

29. Нормальные подгруппы. Лемма о ядре гомоморфизма. Факторгруппы. Теорема о гомоморфизмах групп (без док-ва).

*Подгруппа H группы G называется нормальной подгруппой (запись: $H \lhd G$), если $\forall a \in G$ левый aH и правый Ha смежные классы совпадают (т.е. каждое произведение $ah_1$, где $h_1 \in H$, равно произведению $ah_2$ при каком-то $h_2 \in H$).*

*В коммутативных группах все подгруппы нормальны.*

*Лемма. Пусть* $f_i G_1 \to G_2$ *– гомоморфизм. Ядро* $\ker f$ *является нормальной подгруппой; смежные классы по ядру – это полные прообразы элементов из* $imf \subset G_2$.

*Док-во:*

$H = \ker f$ *– подгруппа; докажем, что она нормальна в* $G_1$. $\forall h \in H$ *и* $\forall x \in G_1$:

$f(x^{-1}hx) = f(x^{-1})f(h)f(x) = f(x^{-1})e_2 f(x) = f(x^{-1})f(x) = f(x^{-1}x) =$
$= f(e_1) = e_2$, *откуда* $x^{-1}Hx \subset H \Leftrightarrow Hx \subset xH$. *Аналогично проверяется, что* $xH \subset Hx$. *Следовательно,* $xH = Hx$. $kerf \lhd G_1$. *Ясно, что* $\forall x \in G_1$ *все элементы из xH и только они отображаются гомоморфизмом f в элемент f(x).*

*Ч.Т.Д.*

*Пусть* $H \lhd G$. *G\H – множество смежных классов по H.*

$$aH \cdot bH \stackrel{\text{def}}{=} (ab)H \quad (*)$$

$H \lhd G \Rightarrow$ *определение (*) корректно и G\H становится группой (нейтральный элемент eH=H,* $(aH)^{-1} = a^{-1}H$*).*

*Факторгруппой группы G по нормальной подгруппе H называется фактормножество G\H с бинарной операцией (*). Факторгруппа обозначается G \ H.*

$\varphi: G \to G\ /\ H$ *по правилу* $\varphi(x) = xH = Hx \Rightarrow \varphi$ *– эпиморфизм.*

*Теорема. Гомоморфный образ группы изоморфен факторгруппе этой группы по ядру гомоморфизма.*

30.Циклические группы. Теорема о порядке элементов конечной группы.

$a \in (G,\cdot) \quad f: \mathbb{Z} \to G$: $f(n) = a^n$ *– гомоморфизм*

$D = imf = \{a^n : n \in \mathbb{Z}\} < G$ и $D \cong \mathbb{Z}/kerf$

*Группа* $\langle a \rangle$*, состоящая из степенной одного элемента* $a$*, называется циклической группой, порожденной этим элементом.*

*Теорема. Подгруппа D, порожденная элементом* $a$ *группы G, изоморфна либо бесконечной циклической группе* $\mathbb{Z}$*, либо циклической группе* $C_m$ *порядка* $m \geq 1$.

$D = \{a^n : n \in \mathbb{Z}\} \cong \mathbb{Z}/kerf$*, где* $f(n) = a^n, n \in \mathbb{Z}$.

$kerf = \{0\} \Rightarrow D \cong \mathbb{Z}$

$kerf \neq \{0\} \Rightarrow \exists m \in \mathbb{N}: kerf = m\mathbb{Z} \Rightarrow D \cong \mathbb{Z}/m\mathbb{Z} \cong C_m$

*Порядком элемента $a$ из группы $G$ называется порядок конечной циклической подгруппы, порожденной этим элементом. Если же эта подгруппа изоморфна $\mathbb{Z}$, то будем говорить, что элемент $a$ имеет бесконечный порядок.*

*Теорема. В конечной группе порядок любого элемента есть делитель порядка группы.*

*Следствие. Любая группа простого порядка циклична.*

31.Кольца. Делители нуля. Обратимые элементы кольца.

*(Непустое) множество A называется кольцом, если на нем определены две бинарные операции + (сложение) и · (умножение), обладающие следующими свойствами:*

*(A, +) является абелевой группой;*

*Умножение · ассоциативно;*

*Операции сложения и умножения связаны дистрибутивными законами $(a + b)\, c = ac + bc$, $c\,(a + b) = ca + cb \quad \forall a, b, c \in A$.*

*Теорема. Если в кольце один из сомножителей равен нулю, то и всё произведение равно нулю.*

*Док-во:* $a \cdot 0 + a \cdot 0 = a \cdot (0 + 0) = a \cdot 0 \Rightarrow a \cdot 0.$

*Аналогично для* $0 \cdot a$.

*Замечание. Обратное утверждение верно, но не во всех кольцах.*

*Элементы $a$ и $b$ кольца, для которых $ab = 0$ или $ba = 0$ и при этом $a \neq 0, b \neq 0$, называются делителями нуля.*

*Теорема. Если $ab = ac$ или $ba = ca$, то $b = c$, если только $a \neq 0$ и не является делителем нуля.*

*Обратимый элемент — элемент кольца с единицей, для которого существует обратный элемент относительно умножения.*

32.Поля. Теорема о конечных кольцах без делителей нуля.

*Полем называется коммутативное кольцо K, содержащее не менее двух элементов, в котором все ненулевые элементы образуют группу по умножению (мультипликативную группу K*).*

*Замечание. Из определения следует, что поле всегда содержит единицу.*

*Теорема. Поле не имеет делителей нуля.*

*Док-во:*

$ab = 0$ *и* $a \neq 0 \Rightarrow 0 = a^{-1}ab = 1 \cdot b = b$

*Теорема. Всякое конечное коммутативное кольцо без делителей нуля, содержащее более одного элемента, является полем.*

*Док-во:*

$a \in K \setminus \{0\} \quad \varphi: K \to K: \varphi(x) = ax \Rightarrow \varphi: K \leftrightarrow K$

$\exists 1\ (\varphi(1) = a); \quad \exists a^{-1}(\varphi(a^{-1}) = 1)$

33. Идеалы коммутативных колец. Главные идеалы. Идеалы в полях.

*Подкольцо H коммутативного кольца A называется идеалом, если произведение* $ha = ah$ *лежит в H при любых* $a \in A$ *и* $h \in H$.

*Теорема 1.*

*В кольце A множество* $\{xa: x \in A\}$ *всех кратных любого фиксированного элемента* $a \in A$ *является идеалом в A.*

*Идеал кольца A, состоящий из кратных элемента a, называется главным идеалом, порожденным элементом a, и обозначается (a).*

*Теорема 2.*

*Любое поле не содержит идеалов, отличных от нулевого или единичного.*

*Док-во: пусть H – идеал поля K,* $H \neq 0$; $h \in H, h \neq 0$.

$$\exists h^{-1} \in K \Rightarrow hh^{-1} = 1 \in H \Rightarrow H = K$$

34. Кольца классов вычетов. Идеалы кольца целых чисел. Кольца $\mathbb{Z}_n = \mathbb{Z}/(n)$ .

*Пусть H = (h) – идеал коммутативного кольца A.*

*Два элемента a и b кольца A называются сравнимыми по модулю h (или по идеалу H), если их разность a – b принадлежит идеалу H.*

*Запись:* $a \equiv b(mod\ h)$.

*'≡' – отношение эквивалентности,* $K_a = a + H$, *т.к. (H, +)* $\lhd$ *(A, +).*

*Смежный класс a + H называется классом вычетов по модулю h (или по идеалу H).*

*Кольцо A / H называется кольцом классов вычетов по модулю h (или по идеалу H).*

*Пример:* **$\mathbb{Z}_n = \mathbb{Z}/(n)$, *n = 2, 3, 4, …***

*Следствие из теоремы о простом идеале. Кольцо классов вычетов кольца целых чисел по модулю n является полем тогда и только тогда, когда n – простое число.*

## 35.Характеристика кольца. Теорема о характеристике кольца без делителей нуля.

*Пусть A ≠ 0 – кольцо с единицей. Число* $m \in \mathbb{N}$ *называется характеристикой кольца A, если* $m \cdot 1 = 1 + 1 + \cdots + 1 = 0$ *(кол-во единиц равно m) и никакое положительное число, меньшее m, эти свойством не обладает.*

*Если указанное свойство не имеет места ни для какого положительного числа, то говорят, что кольцо имеет характеристику 0.*

*Теорема. Характеристика m любого кольца без делителей нуля (в частности, поля) или равна 0, или является простым числом.*

*Док-во:*

*Пусть* $m = kl, k > 1, l > 1 \Rightarrow 0 = m \cdot 1 = (kl) \cdot 1 = (k \cdot 1) \cdot (l \cdot 1) \Rightarrow k \cdot 1 = 0$ или $l \cdot 1 = 0$. *Противоречие.*

*Ч.Т.Д.*

## 36.Простые идеалы. Поля GF(p).

*Идеал H кольца A называется простым, если из того, что* $ab \in H$, *следует, что* $a \in H$ *или* $b \in H$.

*Теорема. Идеал H кольца A называется простым, тогда и только тогда, когда кольцо классов вычетов A/H не содержит делителей нуля.*

*Док-во:*

*A/H не имеет делителей нуля*$\Leftrightarrow ((a+H)(b+H) = H \Rightarrow a + H = H$ или $b + H = H) \Leftrightarrow (ab \in H \Rightarrow a \in H$ или $b \in H)$.

*Следствие. Кольцо классов вычетов кольца целых чисел по модулю n является полем тогда и только тогда, когда n – простое число.*

*Поле классов вычетов по простому модулю – поля из p элементов обозначаются как GF(p).*

## 37.Евклидовы кольца. Идеалы евклидова кольца.

*Евклидовым кольцом называется кольцо D без делителей нуля, в котором каждому ненулевому элементу a сопоставляется целое неотрицательное число* $v(a)$, *называемое нормой, со следующими свойствами:*

*а)* $v(ab) \geq v(a)$ *для всех* $a \neq 0, b \neq 0$ *из D;*

*б) для любых* $a, b \in D,\ b \neq 0$, *существует элемент* $q \in D$ *такой, что* $a = bq + r$, *где r = 0 или* $v(r) < v(b)$.

*Теорема. В евклидовом кольце все идеалы главные.*

*Док-во:*

*Пусть H ≠ 0 – идеал евклидова кольца D. Выберем в H элемент* $a \neq 0$ *с наименьшей нормой* $v(a)$. *Тогда любой* $b \in H$ *можно представить в виде* $b = aq + r$, *откуда* $r = b - aq$. *Не может быть, чтобы* $v(r) < v(a)$, *следовательно,* $r = 0$ и $H = (a)$.

Ч.Т.Д.

*Следствие. Любое евклидово кольцо содержит единицу.*

*Док-во: применим теорему к единичному идеалу, которым является все кольцо D. Тогда D = (a) ⇒* $b = qa = qae = be$.

Ч.Т.Д.

38. Теорема о наибольшем общем делителе.

*Теорема:*

*В евклидовом кольце D любые два элемента a и b имеют наибольший общий делитель d, который представляется в виде d = sa + tb, где s, t* $\in D$.

*Док-во:*

$\{sa + tb : s, t \in D\}$ *– идеал! По теореме 1 этот идеал главный, т.е.* $\{sa + tb\} = (d)$. *Следовательно,* $\exists s, t, g, h \in D$ *такие, что* $d = sa + tb, a = gd, b = hd$.

39. Кольца многочленов. Приводимость многочленов над полем.

*Многочленом (полиномом) от неизвестной x над кольцом A называется выражение вида*

$a_0x^n + a_1x^{n-1} + \cdots + a_{n-1}x + a_n = \sum_{k=0}^{n} a_kx^{n-k}, a_k \in A$

*(*$a_nx^0$ *полагаем равным* $a_n \in A$*).*

*Многочлен g(x) из кольца K[x] называется приводимым (над полем K), если g(x) =* $g_1(x)g_2(x)$ *для подходящих непостоянных многочленов* $g_1, g_2 \in K[x]$; *в противном случае многочлен g(x) называется неприводимым.*

40. Теорема о кольцах класса вычетов K[$x$] / (g($x$)).

*Кольцо классов вычетов L = K[x]/(g(x)) по модулю неприводимого многочлена есть поле.*

*Док-во:*

*Пусть* $f(x) \notin (g(x)) \Rightarrow \text{НОД}(f(x), g(x)) = 1$, *т.к g(x) неприводим.*
*Следовательно,* $\exists s(x),\ t(x) \in K[x]:\ s(x)f(x) + t(x)g(x) = 1$.

$$s(x)f(x) \equiv 1(mod\ g(x)) \Rightarrow s(x) \in (f(x) + (g(x)))^{-1}$$

*Т.к.* $a \leftrightarrow a + \big(g(x)\big), a \in K$, *то* $K \subset L$.

41.Расширения полей. Поля Галуа GF$(p^n)$.

***<u>Теорема о кольцах класса вычетов K[x] / (g(x)).</u>***

*Кольцо классов вычетов L = K[x]/(g(x)) по модулю неприводимого многочлена есть поле.*

*По теореме о кольцах класса вычетов K[x]/(g(x)), поле L называется расширением поля K.*

*Конечные поля, содержащие* $\mathrm{p}^{\mathrm{n}}$ *элементов (они существуют для любого* $\mathrm{n}$*), называются полями Галуа и обозначаются GF*$(\mathrm{p}^{\mathrm{n}})$*. В частности* $\mathbb{Z}_p = GF(p)$.

42.Малая теорема Ферма для конечных полей.

*Теорема 1. Пусть* $q = p^n$ *– степень простого числа. Любой ненулевой элемент поля GF(q) удовлетворяет уравнению* $x^{q-1} - 1 = 0$.

<u>*Для q = p:* $a^p \equiv a(mod\ p)\ \ \forall a \in \mathbb{Z}$. *(малая теорема ферма)*</u>

43.Мультипликативная группа конечного поля.

*Мультипликативная группа K* поля K – это группа, содержащая все ненулевые элементы из K, и операция в ней совпадает с операцией умножения в K.*

44.Логарифмы Якоби.

*Теорема. Число примитивных элементов поля GF(q) равно* $\varphi(q-1)$.

*Если* $\alpha$ *– примитивный элемент поля GF(q), то все ненулевые элементы имеют вид* $\alpha^n$.

*Логарифм Якоби* $\mathrm{L(n)}$ *определяется равенством* $1 + \alpha^n = \alpha^{L(n)}$.
*Тогда* $\alpha^n + \alpha^m = \alpha^m(1 + \alpha^{n-m}) = \alpha^{m+(n-m)}$*. Добавим символ:* $\alpha^{-\infty} = 0$.