Part I

Алгебра

Chapter 1

Линейная алгебра. Векторные пространства

1.1 Лекция 1

X - множество
$* : X \times X \to X$
$(x, y) \mapsto x * y$
Аксиомы:

1. $\forall x, y, z \in X : x * (y * z) = (x * y) * z$ (ассоциативность)
2. $\exists e \in X \; \forall a \in X : e * a = a * e = a$ (нейтральный элемент)
3. $\forall a \in X \; \exists a' \in X : a * a' = a' * a = e$ (обратный элемент)
4. $\forall a, b \in X : a * b = b * a$ (коммутативность)

Определение 1. Множество X с операцией $*$, удовлетворяющее аксиоме 1, называется **полугруппой**

Определение 2. Множество X с операцией $*$, удовлетворяющее аксиомам 1-2, называется **моноидом**

Определение 3. Множество X с операцией $*$, удовлетворяющее аксиомам 1-3, называется **группой**

Определение 4. Множество X с операцией $*$, удовлетворяющее аксиомам 1-4, называется **коммутативной** или **абелевой группой**

Примеры.

1. $(\mathbb{Z}, +)$ – группа
2. $(\mathbb{N}, +)$ – полугруппа
3. $(\mathbb{N}_0, +)$ – моноид

4. $(\mathbb{R}\backslash\{0\}, \cdot)$ – группа

5. Пусть A - множество
   $X :=$ множество биективных отображений $A \to A$
   id_A– нейтральный элемент
   Если $f(x) = y$, то $\tilde{f}(y) = x$ – обратная функция $(f \circ \tilde{f} = \tilde{f} \circ f = id_A)$.
   $f(x) = x + 1,\ g(x) - 2x,\ id_A(x) = x$
   $f \circ g(x) = f(g(x)) = f(2x) = 2x + 1$
   $g \circ f(x) = g(f(x)) = g(x + 1) = 2x + 2 \neq 2x + 1$
   Следовательно, $(X, \circ)$ – не коммутативная группа

Обозначение.

- $\cdot$ – мультипликативность, 1, x^{-1}
- $+$ – аддитивность, 0, $-x$
- $\circ$ – относительно композиции, id, x^{-1}
- $*$ – абстрактная операция, e, x^{-1}

Пусть $(R, +)$ – абелева группа
Определим отображение

$$\cdot : R \times R \to R$$

$$(a, b) \mapsto a \cdot b$$

Для $(R, +, \cdot)$ могут быть верны следующие аксиомы:

5. $a(b + c) = ab + ac$
   $(b + c)a = ba + ca$ (дистрибутивность)

6. $a(bc) = (ab)c$ (ассоциативность)

7. $\exists 1_R\, \forall a \in R : 1_R \cdot a = a \cdot 1_R = a$ (нейтральный элемент)

8. ab = ba (коммутативность)

9. $0_R \neq 1_R$

10. $\forall a \neq 0_R\, \exists a^{-1} : a \cdot a^{-1} = a^{-1} \cdot a = 1_R$ (обратный элемент)

1.2 Лекция 2

Определение 5. $(R, +, \cdot)$, удовлетворяющее аксиоме 5, называется **не ассоциативным кольцом без единицы**.

Определение 6. $(R, +, \cdot)$, удовлетворяющее аксиомам 5-6, называется **ассоциативным кольцом без единицы**.

Определение 7. $(R, +, \cdot)$, удовлетворяющее аксиоме 5-7, называется **ассоциативным кольцом с единицей**.

Определение 8. $(R, +, \cdot)$, удовлетворяющее аксиомам 5-8, называется **коммутативным кольцом**.

Примеры.

1. $\mathbb{Z}$ –коммутативное кольцо

2. $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ – поля

3. Рассмотрим $\mathbb{Z}_n = 0, \dots, n-1$ с операциями $+_n, \cdot_n$:
   $a +_n b = (a+b)\%n$
   $a \cdot_n b = (a \cdot b)\%n$
   Обратимые элементы:
   $ax = 1 + ny$
   $ax - ny = 1$
   Если $(a, n) = 1$, есть решение, иначе – нет. $\mathbb{Z}_p$– поле $\Leftrightarrow p \in \mathbb{P}$

Определение 9. V – векторное пространство над полем F , если $(V, +)$ – абелева группа, задано отображение $V \times F \to V$
$(x, \alpha) \mapsto x \cdot \alpha$, удовлетворяющее аксиомам $\forall x, y \in V, \forall a, b \in F$:

5. $x \cdot (\alpha \cdot \beta) = (x \cdot \alpha) \cdot \beta$

6. $(x + y) \cdot \alpha = x \cdot \alpha + y \cdot \alpha$
   $x \cdot (\alpha + \beta) = x \cdot \alpha + x \cdot \beta$

7. $x \cdot 1_F = x$

$A \in M_n(F), \alpha \in F$
$(A, \alpha)_{ij} = a_{ij} \cdot \alpha$
$(AB)\alpha = A(B\alpha)$

Примеры.

1. Множество векторов в $\mathbb{R}^3$

2. $F^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} \mid a_i \in F \right\}$
   $$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$$

3. X - множество, $F^X = \{f \mid f : X \to F\}$
   $f, g : X \to F$
   $(f+g)(x) = f(x) + g(x)$
   $(f\alpha)(x) = f(x)\alpha$

4. $F[t]$ - многочлены от одной переменной t

5. V - абелева группа, в которой $\forall a \in V : \underbrace{a + a + \ldots + a}_{p \in \mathbb{P}} = 0$ Тогда V - векторное пространство над $\mathbb{Z}_p$ $k \cdot a = \underbrace{a + \ldots + a}_{k}$

1.3 Лекция 3

Определение 10. Алгебра A над полем F – кольцо, являющееся векторным пространством над F ("$+$" - операция в кольце и в векторном пространстве), такое что $(ab)\alpha = a(b\alpha) \quad a, b \in A, \alpha \in F$

Пример. $(\mathbb{R}^3, +, \times)$ - не ассоциативная алгебра на $\mathbb{R}$

Определение 11. Матрица размера $I \times J$ (I, J - множества индексов) над множеством X - это функция

$$A : I \times J \to X, \qquad (i, j) \to a_{ij}.$$

Пусть определено умножение $X \times Y \to Z, \qquad (x, y) \to xy$
(Z - коммутативный моноид относительно "$+$")

Определение 12. Строка - матрица размера $\{1\} \times J$
Столбец - матрица размера $J \times \{1\}$

A - строка длины J над X
B - строка длины J над Y
Тогда произведение $AB = \sum\limits_{j \in J} a_{1j} b_{j1} \in Z$
$x \to x_e$ - координаты вектора x

$$\underbrace{x \cdot y}_{\text{скалярное произведение}} = x_e^T \cdot y_e$$

Определение 13. Транспонирование матрицы.
D - матрица $I \times J$ над X
D^T - матрица $J \times I$ над $X : (D^T)_{ij} = (D)_{ji}$

Замечание. Пусть в X есть элемент $0 : 0 \cdot y = 0 \quad \forall y \in Y$. Все кроме конечного числа $a_j = 0$. Тогда AB имеет смысл, даже когда $|J| = \infty$.
"почти все" $=$ кроме конечного количества

Обозначение.

$$a_{i*} \text{ - } i\text{-я строка матрицы } A$$

$$a_{*j} \text{ - } j\text{-й столбец матрицы } A$$

1.3.1 Произведение матриц

$$A \text{ - матрица } I \times J \text{ над } X.$$

$$B \text{ - матрица } J \times K \text{ над } Y.$$

$$AB \text{ - матрица } I \times K \text{ над } Z = X \cdot Y, \qquad (AB)_{ik} = a_{i*} \cdot b_{*k} = \sum_{j \in J} a_{ij} \cdot b_{jk}.$$

$$(x_1, \dots x_n) \cdot \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = va, \qquad v \in V, a \in F.$$

1.4 Лекция 4

Определение 14. $(G, *), (H, \#)$– группа
$\varphi : G \to H$- гомоморфизм, если:

$$\varphi(g_1 * g_2) = \varphi(g_1) \# \varphi(g_2)$$

Определение 15. R, S -кольца
$\varphi : R \to S$ - гомоморфизм, если:

$$\varphi(r_1 + r_2) = \varphi(r_1) + \varphi(r_2)$$

$$\varphi(r_1 \cdot r_2) = \varphi(r_1) \cdot \varphi(r_2)$$

Для колец с 1:$\varphi(1) = 1$

Определение 16. U, V - векторные пространства над F
$\varphi : U \to V$ - линейное отображение, если:

$$\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2)$$

$$\varphi(u\alpha) = \varphi(u)\alpha$$

Замечание. Изоморфизм – биективный гомоморфизм.

Определение 17. V - векторное пространство над полем F
v - строка элементов "длины" I над V
a - столбец "высоты" I, почти все элементы которого равны 0
Тогда va - линейная комбинация набора v с коэффициентами .

Замечание. $U \subset V$
U является векторным пространством относительно тех же операций, которые заданы в V. Тогда U - подпространство V

Лемма. $U \subseteq V$
$\forall u_1, u_2 \in U, \alpha \in F$:
$u_1 + u_2 \in U, u_1\alpha \in U$ *Тогда* U *- подпространство. Если* U *- подпространство в* V*, то пишут* $U \subseteq V$*.*

Определение 18. $v = \{v_i | i \in I\}$, где $v_i \in V\ \forall i \in I$
$< v >$ - наименьшее подпространство, содержащее все v_i

Лемма. $< v >= \{va | a-$ *столбец высоты* I *над* F*, где почти всюду элементы равны нулю* $\} = U$

Доказательство. $v_i \in < v > \Rightarrow v_i a_i \in < v >$
$\Rightarrow v_{i_1} a_{i_1} a + ... + v_{i_k} a_{i_k} \in < v >$
$\Rightarrow < v >$ содержит все варианты комбинаций. $va + vb = v(a + b) \in U$
$(va)\alpha = v(a\alpha) \in U$
$\Rightarrow$ множество линейных комбинаций – подпространство U - подпространство, содержащее $v_i \forall i \in I$
$< v >$а – наименьшее подпространство, содержащее v_i
$\Rightarrow < v > \subseteq U$ тогда $< v >= U$ □

Определение 19. Если $< v >= V$, то v – система образующих пространство V
Базис – система образующих.

Обозначение. F^I – множество функций из I в F = множество столбцов высоты I
${}^I V$– множество строк длины I

Набор элементов из V , заиндексирванных множеством I – это функция $f : I \to V$
$i \mapsto f_c$

Определение 20. $v \in {}^I V$
v – **линейно независим**, если $\forall a \in F^I, a \neq 0 \Rightarrow va \neq 0$

Теорема 1.4.1. $v \subseteq V$ *(можно считать, что* v *- строка длины* v
Следующие утверждения эквивалентны:

1. v *- линейно независимая система образующих*
2. v *- максимальная линейно-независимая система*
3. v *- минимальная система образующих*
4. $\forall x \in V \exists! a \in F^v : x = va = \sum\limits_{t \in v} t \cdot a_t$ *(почти все элементы равны 0)*

Доказательство. (1) $\Rightarrow$ (4) – доказали ранее (1) $\Rightarrow$ (2)
$x \in V \setminus v$
$x = va (a \in F^v)$
$va = x \cdot 1 = 0$ – линейная зависимость набора $v \cup x$
Т.о. любой набор , строго содержащий v, линейно зависим $\Rightarrow v$ – максимальный.

(1) $\Rightarrow$ (2)
$x \in V\setminus$
$v \subseteq V \cup x$–линейно зависим
$va + xa_x = 0$
$a \neq 0$
Если $a_x = 0 \Rightarrow va = 0 \Rightarrow a = 0$?!
Значит $a_x \neq 0$
$va = c \cdot (-a_x)$
$x = v \cdot \frac{a}{-a_x} \Rightarrow v$ –система образующих.

$\square$

Лемма. *(Цорн) Пусть $\mathbb{A}$ – набор подмножеств (не всех) множества X.*
Если объединение любой цепи из $\mathbb{A}$, принадлежащей $\mathbb{A}$, то в $\mathbb{A}$ существует максимальный элемент.
$M \in \mathbb{C}$ - максимальная, если $M \subseteq M' \subseteq \mathbb{A} \Rightarrow M = M'$

Теорема 1.4.2. *(о существовании базиса) V – векторное пространства*
X – линейное независимое подмножество V
Y – система образующих V
$X \leq Y$
Тогда существует базис Z пространства $V : X \leq Z \leq Y$

Доказательство. $\mathbb{A}-$множество всех линейно независимых подмножеств, лежащих между X и Y. $X \in \mathbb{A}$
$\mathbb{C} \leq \mathbb{A}$
$X \leq \cup C \in \mathbb{C} \leq Y$
Пусть $\cup C \in \mathbb{C}$ – линейно зависимый. То есть$\exists u_1, ..., u_2 \in /...$
...
Пусть v - базис V.

$$\forall x \in V \ \exists! x_v \in F^v : x = v \cdot x_v$$
$$v = (v_1, \ldots, v_n), \ x_v = ;$$

$$x = v_1\alpha_1 + \ldots = v \cdot x_v$$

$\square$

1.5 Лекция 5

1.6 Лекция 6

1.7 Лекция 7

Утверждение.

$$U \leq W \quad \exists V \leq W : W = U \oplus V$$

Доказательство. Выберем базис u в U. Дополним до базиса $u \cup v$ пространства W и положим $V =< v >$.

$$< u >= U < v >= V < u \cup v >=< u > + < v >= U \oplus V = W$$

$$x \in U \cap V \Rightarrow x = ua = vb \Leftrightarrow ua - vb = 0 \Rightarrow a = 0, b = 0(u \cup v - \text{линейно независимый}$$

□

Следствие.

$$u - \text{ базис } U, v - \text{ базис } V, U, V \leq W$$

$$u \cup v - \text{ базис } W \Leftrightarrow U \oplus V$$

25.09.2019

1.8 Лекция 8

$$v - (v_1, v_2, \dots v_n) \in n^V$$

$$M_n(F) - \text{ алгебра матриц размера } n \times n \text{ над } F$$

$$GL_n(F) = M_n(F)^* - \text{ полная линейная группа степени } n \text{ над } F$$

Лемма.

$$v \in n^V, A \in GL_n(F)$$

$$v - \textit{ линейно независимый } \Leftrightarrow vA - \textit{ линейно независимый}$$

$$< v >=< vA >$$

Доказательство. $(vA)A^{-1} = v(AA^{-1}) = vE = v$, поэтому можно доказывать только в одну строну.
v - линейно независимый.
$vAb = 0 \Rightarrow A^{-1}Ab = 0 \Rightarrow b = 0$, т.е vA - линейно независимый.
$(vA)b = v(Ab) \in< v >, < vA >\leq< v >$ □

Утверждение. *u, v - два разных базиса пространства V.*
Тогда $\exists!$ матрица $A \in GL_n(F) : u = vA$
При этом $a_{*k} = (u_k)_v \qquad \forall k = 1, \dots n$. Такая матрица обозначается $C_{v\to u}$ и называется матрицей перехода от v к u.

$$C_{v\to u}C_{u\to v} = C_{v\to u}C_{u\to v} = E$$

Доказательство. Положим $a_{*k} = (a_k)_v \Rightarrow u_k = va_{*k} \Rightarrow u = vA$.
$vA = vB \Leftrightarrow A = B$ то есть A - единственно.
Далее:

$$\left.\begin{array}{r} u = vC_{v\to u} \\ v = uC_{u\to v} \end{array}\right\}$$

$$uE - uC_{v\to u}C_{v\to u}$$

$$E = C_{u\to v}C_{v\to u}$$

□

Следствие. v - базис V
$f : GL_n(F) \to$ множество базисов пространства V
$f(A) = vA$ - биекция.

Доказательство.

$$|F| = q \qquad \dim V = u$$

$$(q^n - 1)(q^n - q)\dots(q^n - q^{n-1}) - \text{количество базисов}$$

$\mathbb{F}$ - поле из q элементов. □

Утверждение. *Если матрица двусторонне обратима, то она квадратная.*

Следствие. u, v - базисы V

$$x \underset{u}{=} C_{u\to v}x_v$$

Доказательство.

$$x = ux_u = vx_v$$

$$v = uC_{u\to v}$$

$$ux_u = uC_{u\to v}x_v \Rightarrow x_u = C_{u\to v}x_v$$

□

Следствие. (Матричные линейные отображения)

$$L : U \to V, \quad u - \text{ базис } U, v - \text{базис } V$$

Тогда $\exists!$ матрица $L_{v,u}(L_u^v : \forall x \in U L(x)_v = L_u^v x_u$
При этом $(L_u^v)_{*k} = L(u_k)_v$

Замечание.

$$u = (u_1, \dots u_n) \in n^U$$

$$L : U \to V$$

$$L(a) := (L(u_1), \dots, L(u_n))$$

$$L(ua) = L(u)a \qquad a \in F^n$$

$$\varphi_v : V \to F^n$$

$$\varphi_v(g) = y_v \qquad \forall q \in V$$

φ_v - линейно $\Rightarrow (L(u)a)_v = L(u)_v a$

$$L(u)_v := (L(u_1)_v, \dots L(u_n))v)$$

Доказательство.

$$x = ux_u$$

$$L(x) = L(u)x_u$$

$$L(x)_v = L(u)_v x_u$$

Положим $L_u^v := L(u)_v$.

$$\forall x \in U : L(x)_v = L_u^v x_u$$

При $x = u_k : L(u_k)_v = L_u^v (u_k)_u = (L_u^v)_k$ □

Замечание. Если $Ax = Bx \quad \forall x \in F^n$, то $A = B$

26.09.2019

1.9 Лекция 9

Примеры.

1. $V = \mathbb{R}[t]_3$ - многочлены степени не более 3

$$D(p) = p' \qquad V \to V$$

$$v = (1, t, t^2, t^3).$$

$$D(1) = 0, D(t) = 1, D(t^2) = 2t.$$

$$D_v = \begin{pmatrix} 0 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}.$$

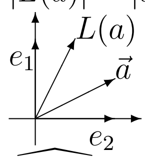
$$v^{(1)} = (1, \frac{t}{1!}, \frac{t^2}{2!}, \frac{t^3}{3!}).$$

2. $V = \mathbb{R}[t]$

$$v = (1, t, \frac{t^2}{2}, \dots, \frac{t^n}{n!}, \dots).$$

$$D(v_0) = 0, D(v_k) = v_{k-1}.$$

$$\begin{pmatrix} 0 & 1 & & \cdots \\ & 0 & 1 & \cdots \\ & & 0 & 1 \\ \vdots & \vdots & & \ddots \end{pmatrix}$$

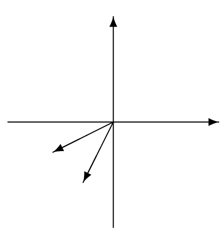
3. $V = \mathbb{R}^3$
   $|L(a)| = |a|$
   

   $\widehat{a, L(a)} = \varphi$
   $e = (e_1, e_2)$- базис

$$L(e_1)_e = \begin{pmatrix} \cos\varphi \\ \sin\varphi \end{pmatrix}$$

$$L(e_2)_e = \begin{pmatrix} -\sin\varphi \\ \cos\varphi \end{pmatrix}$$

$$L_e = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix}.$$



$$a_e = \begin{pmatrix} \cos\psi \\ \sin\varphi \end{pmatrix}$$

$$L(a)_e = \begin{pmatrix} \cos(\psi + \varphi) \\ \sin(\psi + \varphi) \end{pmatrix}.$$

$$L(a)_e = L_e \cdot a_e = \begin{pmatrix} \cos\varphi & -\sin\varphi \\ \sin\varphi & \cos\varphi \end{pmatrix} \cdot \begin{pmatrix} \cos\psi \\ \sin\psi \end{pmatrix} = \begin{pmatrix} \cos\varphi\cos\psi - \sin\varphi\sin\psi \\ \cos\varphi\sin\psi + \sin\varphi\cos\psi \end{pmatrix}.$$

Утверждение. $L : U \to V$
u, u' − базис U
v, v' − базис V
Тогда $L_{u'}^{v'} = C_{v' \to v} \quad L_u^v C_{u \to u'}$

Доказательство.

$$L(x)_v = L_u^v x_u.$$

$$C_{v' \to v} L(x)_v = L(x)_{v_1} = L_{u'}^{v'} x_{u'} = L_{u'}^{v'} C_{u' \to u} x_u.$$

$\forall x_u \in F^{dimU}$

$$L(x)_v = C_{v\to v'} L_{u'}^{v'} C_{u'\to u} x_k.$$

$$L_u^v = C_{v\to v'} L_{u'}^{v'} C_{u'\to u}.$$

$\square$

Замечание.

$$\text{Если } U = V \qquad u = v, u' = v'.$$

$$L_{u'} = C_{u'\to u} L_u C_{u\to u'}.$$

Утверждение. *Линейное отображение однозначно определяется образом базисных векторов.*
$u = (u_1, \dots u_n) -$ *базис* U
Для любого векторного пространства V*:*

$$\forall v_1, \dots v_n = V$$

$$\exists! \text{ линейное отображение } (*) L : U \to V : L(u_k) = v_k \quad \forall k$$

Доказательство.

$$L(ua) := va$$

$$\forall L^* : L(ua) = L(u)a = va$$

$\square$

При этом L - инъективно тогда и только тогда, когда v - линейно независимый
L - сюрьективно тогда и только тогда, когда v - система образующих
L - изоморфизм тогда и тоько тогда, когда v - базис.

Утверждение. $V, \quad v, v' -$ *базис* V
$L : V \to V -$ *линейно*
$L(v_k) = v'_k \qquad \forall k$

$$(L_v)_k = L(v_k)_v = (v'_k)_v$$

$$L_v = C_{v\to v'}.$$

(по другому)

$$(Id_{v'}^v)_k = Id(v'_k)_v = (v'_k)_v.$$

Тогда $L_v = C_{v\to v'} = Id_{v'}^v$

Определение 21. $f : X \to Y$
$Imf = \{f(x) \mid x \in X\}$
$L : U \to V$ - линейное отображение
$ImL = \{L(x) \mid x \in U\}$
$\ker L = L^{-1}(0) = \{x \in U \mid L(x) = 0\}$

Лемма.
$imL \leq V$
$\ker L \leq U$
Пусть $L(x) = y$

$$\forall y \in V : L^{-1} = x + \ker L$$
$$L^{-1}(y) = \{z \in U \mid L(z) = y\}$$
$$x + \ker L = \{x + z \mid z \in \ker L\}$$