Линейная алгебра
Векторные пространства

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

Обозначения

- $\cdot$ – 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)

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 $\mathbb{Z}_n = 0, \ldots, n-1$ 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. $x \cdot 1_F = x$

Примеры:

1. Множество векторов в $\mathbb{R}^3$
2. $F^n = \left\{ \begin{pmatrix} a_1 \\ a_2 \\ \vdots \\ a_n \end{pmatrix} | a_i \in F \right\}$
   $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} + \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix} = \begin{pmatrix} a_1 + b_1 \\ \vdots \\ a_n + b_n \end{pmatrix}$

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

Определение 1
$(G, *), (H, \#)$– группа
$\varphi : G \to H$- гомоморфизм, если:

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

Определение 2
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 3
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 4
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 .

Определение 5
$Uanal \in V$
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 6
$v = \{v_i | i \in I\}$, 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 $v_i \forall i \in I$
$< v >$a – наименьшее подпространство, содержащее v_i
$\Rightarrow < v > \subseteq U$ тогда $< v >= U$

Определение 7
Если $< v >= V$, то v – система образующих пространство V
Базис – система образующих.

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 8
$v \in {}^I V$
v – **линейно независим**, если $\forall a \in F^I, a \neq 0 \Rightarrow va \neq 0$

Теорема
$v \subseteq V$(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.
$(1) \Rightarrow (2)$
$x \in V \backslash$
$v \subseteq V \cup x$–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.

Лемма Цорна
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 (о существовании базиса)
V – векторное пространства
X – линейное независимое подмножество V
Y – система образующих V
$X \subseteq Y$
Тогда существует базис Z пространства $V : X \subseteq Z \subseteq Y$
Доказательство
$\mathbb{A}-$множество всех линейно независимых подмножеств, лежащих между X и Y. $X \in \mathbb{A}$
$\mathbb{C} \subseteq \mathbb{A}$
$X \subseteq \cup C \in \mathbb{C} \subseteq Y$
Пусть $\cup C \in \mathbb{C}$ – линейно зависимый. То есть$\exists u_1, ..., u_2 \in /...$
$\ldots$
Пусть v - базис V.

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

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