Билеты по алгебре
I семестр

Тамарин Вячеслав

8 января 2020 г.

Вопрос 1 Векторное пространство

Def 1. Пусть $(V, +)$ — абелева группа, F — поле, и задана операция (умножение) $V \times F \to V$. Предположим, что $\forall u, v \in V$ и $\alpha, \beta \in F$ выполнены следующие свойства:

1. $v(\alpha\beta) - (v\alpha)\beta$
2. $v(\alpha + \beta) = v\alpha + v\beta$
3. $(v + u)\alpha = v\alpha + v\beta$
4. $v \cdot 1 = v$

Тогда V называется векторным пространством над F.

Property.

1. $v \cdot 0 = 0 \cdot \alpha = 0$
2. $v \cdot (-1) = -v$
3. $v \cdot (-\alpha) = (-v)\alpha = -(v\alpha)$
4. $v \cdot \sum \alpha_i = \sum v\alpha_i$
5. $\sum v_i \cdot \alpha = \sum v_i\alpha$

Exs.

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

Вопрос 2 Подпространство, линейная оболочка

Def 2. Подмножество $U \subseteq V$ называется подпространством, если оно само является векторным пространством относительно тех же операций, которые заданы в V.

Statement 1 (критерий подпространства)**.** *Подмножество $U \subseteq V$ является подпространством тогда и только тогда, когда $\forall u, v \in U,\ \alpha \in F : u + v, u\alpha \in U$.*

Def 3. Пусть $u_1, \ldots, u_n \in V$, $\alpha_1, \ldots, \alpha_n \in F$. Сумма

$$\sum_{k=1}^{n} u_k \alpha_k$$

называется линейной комбинацией векторов $u_1, \ldots, u_n$ с коэффициентами $\alpha_1, \ldots, \alpha_n$.

Линейная комбинация называется *тривиальной*, если все ее коэффициенты равны нулю.

Note. Пусть $S \subseteq V$, и задан набор чисел $\alpha_s \in F,\ s \in S$. Операция бесконечной суммы будет определена только в случае, когда почти все α_s равны нулю.

Def 4. Линейной оболочкой набора S называется подпространство, порожденное S, то есть наименьшее подпространство, содержащее S.

Designation. Линейная оболочка набора S обозначается $\langle S \rangle$.

Statement 2. $\langle S \rangle = \left\{ \sum\limits_{k=1}^{n} u_k \alpha_k \middle| u_k \in S,\ \alpha_k \in F \right\}$

Def 5. Если $\langle S \rangle = V$, то S называется системой образующих пространства V.

Def 6. Кортеж векторов $(u_1, \ldots u_n)$ называется линейно независимым, если любая нетривиальная линейная комбинация этих векторов не равна нулю.

Множество $S \subseteq V$ называется линейно независимым, если любой кортеж , составленный из конечного числа различных векторов из S, является линейно независимым.

Def 7. Базис — линейно независимая система образующих.

Вопрос 3 Матрицы

i Конечные матрицы

Def 8. Двумерный массив $m \times n$ элементов поля F называется матрицей размера $m \times n$ над F.

Designation. Множество таких матриц обозначается $M_{m\times n}(F)$. Если $m = n$, пишут $M_n(f)$. Элемент матрицы A в позиции (i, j) записывается a_{ij}.

Property.

- *Для двух матриц одинакового размера определена операция поэлементной суммы:* $(A+B)_{ij} = a_{ij} + b_{ij}$.
- *Также определено умножение матрицы на число:* $(A\alpha)_{ij} = a_{ij}\alpha$.
- *Произведением матрицы* $A \in M_{m\times n}(F)$ *на матрицу* $B \in M_{n\times k}$ *называется матрица* $C = AB \in M_{m\times k}(F)$ *элементы которой вычисляются по формуле*

$$c_{ij} = \sum_{l=1}^{n} a_{il} b_{lj}.$$

Theorem 1. *Множество $M_{m\times n}(F)$ с операциями сложения и умножения на число является векторным пространством над полем F.*

Доказательство. Произведение матриц ассоциативно, дистрибутивно и перестановочно с умножением на число:

$$\begin{cases}(AB)C = A(BC)\\ A(B+C) = AB+BC\\ (B+C)A = BA+CA\\ (AB)\alpha = A(B\alpha) = (A\alpha)B\end{cases}.$$

Все кроме первого свойства очевидны. Проверим ассоциативность:

$$\begin{aligned}((AB)C)_{il} &= \sum_{k\in K}(AB)_{ik}c_{kl} = \sum_{k\in K}\left(\sum_{j\in J}a_{ij}b_{jk}\right)c_{kl} =\\ &= \sum_{k\in K}\left(\sum_{j\in J}a_{ij}b_{jk}c_{kl}\right) =\\ &= \sum_{j\in J}\left(\sum_{k\in K}a_{ij}b_{jk}c_{kl}\right) =\\ &= \sum_{j\in J}a_{ij}\left(\sum_{k\in K}b_{jk}c_{kl}\right) = \sum_{j\in J}a_{ij}(BC)_{jl} = (A(BC))_{il}\end{aligned}.$$

Def 9. Квадратная матрица E с 1 на главной диагонали и остальными нулями называется единичной.

Property. *Умножение данной матрицы на единичную справа и слева не ее не изменяет.*

Матрица E_n является нейтральным элементом в $M_n(F)$. □

Обобщение конечных матриц

Пусть даны множества X_{ij}, Y_{jh}, коммутативные моноиды $(Z_{ih}, +)$, где $i = 1, \dots m,\ j = 1, \dots n,\ h = 1, \dots k$, и функции «умножения» $X_{ij} \times Y_{jh} \to Z_{ih},\ (x, y) \mapsto xy$. Обозначим через X, Y, Z наборы множеств X_{ij}, Y_{jh}, Z_{ih}, соответственно, через $M(X)$ — множество матриц A с элементами $a_{ij} \in X_{ij}$, и аналогично $M(Y), M(Z)$. Тогда можно определить произведение матриц $A \in M(X)$ и $B \in M(Y)$ как матрицу $C = AB \in M(Z)$, где $c_{ih} = \sum\limits_{j=1}^{n} a_{ij}b_{jh}$.

Если все X_{ij}, Y_{jh} будут коммутативными моноидами, а функция умножения дистрибутивной, умножение матриц тоже будет дистрибутивным и ассоциативным.

ii Произвольные матрицы

Пусть I, J — произвольные множества (возможно бесконечные), элементами которых мы будем индексировать строки и столбцы матриц. Пусть $\forall i \in I \wedge j \in J$ задано множество X_{ij}, и обозначим набор всех таких множеств через X. Тогда **матрицей размера** $I \times J$ **над** X называется функция $A : I \times J \to \bigcup X_{ij}\ (i, j) \mapsto a_{ij}$, такая что $a_{ij} \in X_{ij}$.

Designation. Множество матриц размера $I \times J$ над X обозначается $M_{I\times J}(X)$. Если $I = \{1\}$, то матрица размера $I \times J$ будут назваться столбцами длины J, а если $J = \{1\}$, то столбцами высоты I. Множества строк обозначим данной длины ${}^{J}X$, множество столбцов — X^{J}.

Будем считать, что все X_{ij} — абелевы группы в аддитивной записи. Тогда сумма двух матриц одного размера определяется поэлементно: $(A+B)_{ij} = a_{ij} + b_{ij}$. Если все X_{ij} — векторные пространства над полем F, также можно определить умножение на число: $(A\alpha)_{ij} = a_{ij}\alpha$.

Умножение матриц

Пусть все операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$ дистрибутивны (для $a \cdot 0 = 0$), и в каждом столбце матрицы Y почти все элементы равны 0.

Designation. Обозначим $M^{c.f.}_{J\times H}(Y) \subset M_{J\times H}(Y)$, состоящее из всех матриц B, у которых для любого фиксированного $h \in H$ почти все элементы b_{jh} равны 0.

Def 10. Пусть $\forall i \in I, j \in J, h \in H$ заданы операции умножения $X_{ij} \times Y_{jh} \to Z_{ih}$, причем $\forall x, x' \in X_{ij}$ и $\forall y, y' \in Y_{jh}$ выполнены равенства

$$(x + x')y = xy + x'y \wedge x(y + y') = xy + xy'.$$

Произведение матриц $A \in M_{i\times J}(X)$ и $B \in <^{c.f.}_{J\times H}(Y)$ как матрицу $AB \in M_{I\times H}(Z)$ с элементами

$$(AB)_{ih} = \sum_{j\in J} a_{ij} b_{jh}.$$

При этом суммы определены, так как почти все слагаемые равны нулю.

Note. Аналогично определяется умножение матриц $A \in M^{r.f.}_{I\times J}(X)$ и $B \in M_{J\times H}(Y)$.

Lemma 1. *Обычные свойства умножения матриц 1 выполнены, если определены все входящие в формулы операции.*

Если $\forall i, j, h \in I$ заданы дистрибутивные операции умножения $X_{ij} \times X_{jh} \to X_{ih}$, то множество $M^{c.f.}_{I\times I}(X)$ является кольцом с единицей.

Designation. Если X_{ij} одно и то же поле F для всех i, j, будем писать $M_{i\times J}(F)$ вместо $M_{I\times J}(X)$. Если $I = J$, то будем писать $M_I(F)$ вместо $M_{I\times I}(F)$. Если $I = \{1, \dots m\}, J = \{1, \dots n\}$, то можем писать $M_{m\times n}(F)$.

Другие характеристики матриц

Def 11. Множество обратимых элементов кольца $M_n(F)$ называется полной линейной группой степени n над F и обозначается $\mathrm{GL}_n(F)$.

Designation. Для множества $M^{c.f.}_{I\times\{1\}}(F)$ введем специальное обозначение F^I_{fin} и будем называть его множеством финитных столбцов высоты I над F. Другим словами, F^I_{fin} — множество финитных (у которых почти все значения равны 0) функций из I в F. Аналогично, ${}^JF_{fin} = M^{r.f.}_{\{1\}\times J}(F)$.

Def 12. Пусть $A \in M_{I\times J}(F)$. Матрица $A^T \in M_{J\times I}(F)$ с элементами $(A^T)_{ij} = a_{ji}$ называется транспонированной к A.

Statement 3. $(AB)^T = B^T A^T$

Note. Для обозначения столбца часто используется строка $(a_1, \dots a_n)^T$.

Вопрос 4 Эквивалентные определения базиса

Theorem 2 (Эквивалентные определения базиса)**.** *Следующие условия на подмножество v векторного пространства V эквивалентны:*

(1) *v — линейно независимая система образующих*
(2) *v — максимальная линейно независимая система*
(3) *v — минимальная система образующих*
(4) *любой элемент $x \in V$ представляется в виде линейной комбинации набора v, причем единственным образом*

Доказательство.

$\boxed{1 \Longrightarrow 2}$ Пусть v — не максимальная линейно независимая система. Мы знаем, что v — система образующих. Тогда любой элемент $a \in V$ представляется в виде линейной комбинации v, а значит любой набор, содержащий v, принадлежит линейной оболочке $\langle v \rangle$, следовательно, набор линейно зависимый.

$\boxed{2 \Longrightarrow 1}$ Так как v максимальная линейно независимая система, любой элемент $a \in V$ выражается через элементы v. Следовательно, v — система образующих.

$\boxed{1 \Longrightarrow 3}$ Пусть из v можно убрать некоторые элементы так, что полученный набор u будет минимальной системой образующих. Тогда любой элемент набора $v \setminus u$ представим в виде линейной комбинации u. Следовательно, v линейно зависим.

$\boxed{3 \Longrightarrow 1}$ Если v линейно зависим, то во всех линейных комбинациях набора v можно заменить один элемент на линейную комбинацию других. А тогда v не минимален.

$\boxed{1 \Longrightarrow 4}$ Так как v — система образующих $\langle v \rangle = V$. Теперь докажем, что представление единственно. Пусть $x = va = \sum_{y \in v} y a_y, \quad a \in F^v_{fin}$. Предположим, что $\exists b \in F^v_{fin} : x = vb$. Тогда $0 = va - vb \Longrightarrow 0 = v(a-b)$. Так как v линейно независим, можем сократить: $0 = a - b$, значит представление единственно.

$\boxed{4 \Longrightarrow 1}$ Так как любой элемент представим в виде линейной комбинации набора v, $\langle v \rangle = V$. Так как представление единственно, v линейно независим.

□

Вопрос 5 Существование базиса

Theorem 3 (О существовании базиса)**.** *Пусть $X, Y \subseteq V$, причем набор X линейно независим, а Y — система образующих. Тогда существует базис Z, содержащий X и содержащийся в Y.*

Доказательство. Пусть $\mathscr{A}$ — набор всех линейно независимых подмножеств Y, содержащих X. Этот набор не пуст, так как содержит X. Пусть $\mathscr{L}$ — линейно упорядоченный поднабор в $\mathscr{A}$. Обозначим через S объединение всех множеств из $\mathscr{L}$. Так как $\forall C \in \mathscr{L}$ лежит между X и Y, S обладает этим свойством. Рассмотрим конечное подмножество $\{v_1, \dots v_n\} \subseteq S$. По определению объединения множеств $\forall i = 1, \dots n \ \exists B_i \in \mathscr{L}$, содержащее v_i. Так как $\mathscr{L}$ — лум, среди множеств $B_1, \dots B_n$ найдется наибольшее B_k. Тогда $v_1, \dots v_n \in B_k$. Так как B_k линейно независимо, то и $\{v_1, \dots v_n\}$ линейно независимо. Следовательно, S линейно независимо, значит $S \in \mathscr{A}$. По лемме Цорна получаем, что $\mathscr{A}$ содержит максимальных элемент. Пусть это Z — максимальное из линейно независимых подмножеств Y, содержащих X.

Пусть $y \in Y \setminus Z$. Так как Z линейно независимо, $Z \cup \{y\}$ линейно зависимо, то есть $\exists a \in F^Z_{fin}, \ a_y \in F : y a_y + Za = 0$, где $a_y \neq 0$. Следовательно, $y \in \langle Z \rangle$. Тогда $Y \subseteq \langle Z \rangle$. С другой стороны, $V = \langle Y \rangle$ — наименьшее подпространство, содержащее Y. Значит $V \subseteq \langle V \rangle$, то есть Z — система образующих, следовательно, и базис.
□