30.09.17. Алгебра Лекция 7

Теорема 2 (теорема Кронекера – Капелли)
Система лин. уравнений совместна $\Leftrightarrow$ ранг матрицы её коэф. = рангу расширенной матрицы.
(Это то же, что было на 1 лекции: сист. совместна $\Leftrightarrow$ кол-во ступеней матрицы коэф. = кол-ву ступеней расширенной матрицы. А мы доказали, что кол-во ступеней = рангу.)

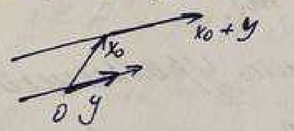
Теорема 3 Совместная система лин. уравнений определённая $\Leftrightarrow$ ранг матрицы её коэф равен числу неизвестных (опять см. лекцию 1).

Пусть теперь система $AX=B$ неопределённая.

Предположение 1 Если X_0 – какое-либо решение системы лин. уравнений $AX=B$, то мн-во всех её решений получается прибавлением к X_0 всех решений системы однородных лин. уравнений $AY=0$.
Док-во. $AX=B$; Пусть X_0 – частное решение $AX=B \Rightarrow B=AX_0$
$\Rightarrow AX=AX_0 \Rightarrow A\underbrace{(X-X_0)}_{Y}=0 \Rightarrow X-X_0=Y \Rightarrow X=X_0+Y$. (если X – решение $AX=B$, то $X-X_0=Y$ – решение однородной системы $AY=0$).

Предположение 2 Множество решений системы однородных лин. уравнений является подпространством в K^n.
Док-во: $AY_1=0$; $AY_2=0$; $\Rightarrow A(Y_1+Y_2)=0+0=0$.
$AY=0 \Rightarrow A(\lambda Y)=\lambda(AY)=\lambda 0=0$.

Если $n=2$



(т.е. мн-во решений неод. системы – это прямая ∥ y, только проходящая не через начало координат, а через x_0).

Теорема 4 Размерность пространства решений системы однородных линейных уравнений $\underset{[m\times n]}{AX=0}$ с n неизвестными равна $n-\mathrm{rk}A$.
Док-во: Приведём систему к ступенчатому виду с помощью элем. преобразований. В полученной матрице будет $r=\mathrm{rk}A$ ненулевых строк (r ступенек). Для удобства записи перенумеруем неизвестные так, чтобы элементы ненулевых строк стояли в первых r столбцах. Тогда первые r неизвестных можно объявить главными, а остальные – свободными. И тогда общее решение системы будет иметь вид:

$$\begin{cases} x_1 = c_{11}x_{r+1} + c_{12}x_{r+2} + \ldots + c_{1n-r}x_n \\ x_2 = c_{21}x_{r+1} + c_{22}x_{r+2} + \ldots + c_{2n-r}x_n \end{cases}$$
$- - -$
$$x_r = c_{r1}x_{r+1} + c_{r2}x_{r+2} + \ldots + c_{2n-r}x_n.$$

$$X=(x_1 \ldots x_r, x_{r+1} \ldots x_n) = x_{r+1}\overset{u_1}{(c_{11}\, c_{21} \ldots c_{r1}; 1; 0; 0; \ldots 0)} + x_{r+2}\overset{u_2}{(c_{12}; c_{22}; \ldots c_{r2}; 0; 1; 0 \ldots 0)} + \ldots + x_n\overset{u_{n-r}}{(c_{1n-r}; c_{2n-r}; \ldots c_{rn-r}; 0; 0; \ldots 0; 1)}.$$

Рассмотрим эти частные решения, получаемые, когда одна из свободных неизв. $=1$, а остальные $=0$.
Это будет $\{u_1; u_2 \ldots u_{n-r}\}$.

$u_1 = (c_{11}; c_{21}; \dots c_{r1}; 1, 0 \dots 0)$
$u_2 = (c_{12}; c_{22}; \dots c_{r2}; 0; 1 \dots 0)$
. . . — — —
$u_{n-r} = (c_{1\,n-r}; c_{2\,n-r}; \dots c_{r\,n-r}; 0; 0 \dots 0\, 1)$.

Докажем, что $\{u_1; u_2 \dots u_{n-r}\}$ – базис пространства решений.
Во-первых, $\lambda_1 u_1 + \lambda_2 u_2 + \dots + \lambda_{n-r} u_{n-r}$ – тоже решение, значения свободных неизвестных в котором равно $\lambda_1 \lambda_2 \dots \lambda_{n-r}$. А так как любое решение однозначно определяется значениями свободных неизвестных, то таким образом можно получить любое решение (просто взять в качестве λ_i то значение i-й свободной неизвестной, которое мы хотим).
Во-вторых, они лин. независимы.
Пусть нет. Тогда $\lambda_1 u_1 + \dots + \lambda_{n-r} u_{n-r} = 0$.
Смотрим на $r+1$-е место. Там только $\lambda_1 \cdot 1 = 0 \Rightarrow \lambda_1 = 0$. Смотрим на $r+2$-е место $\Rightarrow \lambda_2 = 0 \Rightarrow \lambda_1 = \lambda_2 = \dots = \lambda_{n-r} = 0$. $\Rightarrow$ эта лин. комб. не нетривиальная. ◢

Теорема 5 Ранг матрицы равен рангу системы её столбцов.

<u>Док-во:</u> ▶ $\underset{[m \times n]}{A} = (a_{ij})$; $A_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ – j-й столбец.

$\lambda_1 A_1 + \dots + \lambda_n A_n = 0 \Leftrightarrow \sum_{j=0}^{n} a_{ij} \lambda_j = 0 \ (i = 1 \dots m)$.

$\Rightarrow \begin{pmatrix} \lambda_1 \\ \dots \\ \lambda_n \end{pmatrix}$ – решение системы однородных лин. уравнений $AX = 0$.

$\Rightarrow$ при элем. преобр. строк матрицы A лин. зависимость между столбцами не меняется (ну прост у всех столбцов i и j член переставили, или сложили, или домножили на λ). Или по-нормальному:
Всякую лин. зависимость между частью столбцов матрицы A можно рассматривать как лин. зависимость между всеми столбцами, в которой остальные столбцы входят с нулевыми коэф. Поэтому св-во лин. зависимости (независимости) какой-то системы столбцов матрицы A сохраняется при таком элем. преобразовании строк. А ранг – это кол-во max лин. независимых векторов $\Rightarrow$ ранг системы столбцов матрицы не меняется при элем. преобразовании строк $\Rightarrow$ после приведения к ступенчатому виду ранг этой матрицы в столбцах будет = рангу исходной матрицы столбцов $\Rightarrow$ надо док-ть только для ступенчатой матрицы.

$$A = \begin{pmatrix} a_{1j_1} & * & * & * \\ 0 & a_{2j_2} & * & * \\ 0 & 0 & \ddots & * \\ 0 & 0 & 0 & a_{rj_r} \end{pmatrix} \quad a_{kj_k} \neq 0.$$

Докажем, что столбцы с номерами $j_1; j_2 \dots j_r$ образуют лин. независимую систему столбцов.
Пусть нет. Тогда $\lambda_1 A_{j_1} + \lambda_2 A_{j_2} + \dots + \lambda_r A_{j_r} = 0$.

вычитая r-ю координату, получаем $\lambda_r a_{ij_r} = 0 \Rightarrow \lambda_r = 0$.
С учётом этого, вычитаем $(r-1)$-ю коорд, получаем $\lambda_{r-1} = 0$ и т.д.
В конце $\lambda_1 = \ldots = \lambda_r = 0$. Хорошо, оказали. независимо.
Почему это max лин. независимая система?
Очевидно, что на лин. зависимость столбцов матрицы A не влияют последние $m-r$ нулевых коорд $\Rightarrow$ столбцы матрицы A можно рассматривать как элементы пространства K^r — всех столбцов высоты r. $\Rightarrow \operatorname{rk} A \leq r$. А столбцы $j_1 \ldots j_r$ — лин. независимые $\Rightarrow$ они образуют базис этого пространства. Но больше r невозможно $\Rightarrow$ они образуют макс. лин. независимую систему столбцов матрицы $A \Rightarrow \operatorname{rk} A = r$. ▲

Следствие 1: Ранг матрицы не меняется при элем. преобразованиях её столбцов.

Док-во: При элем. преобр. столбцов не меняется лин. оболочка, и, значит, не меняется ранг системы столбцов.

Транспонирование матриц

$$\underset{[m\times n]}{A} = (a_{ij}) \ ; \ \underset{[n\times m]}{A^T} \ (a_{ij}^T) \ ; \ a_{ij}^T = a_{ji}$$

$$A = \begin{pmatrix} 0 & 1 & -1 \\ 2 & 0 & 3 \end{pmatrix} \quad A^T = \begin{pmatrix} 0 & 2 \\ 1 & 0 \\ -1 & 3 \end{pmatrix}$$

Следствие 2 $\operatorname{rk} A^T = \operatorname{rk} A$ (т.к. ранг матрицы = рангу столбцов = рангу строк)

$$\underset{m\times n \ n\times p}{AB} = \underset{m\times p}{C} \ ; \ c_{ik} = \sum_j a_{ij} b_{jk}$$

При фиксированном k получаем, что k-й столбец матрицы C равен лин. комб столбцов матрицы A с коэф. из k-го столбца матрицы B.
Аналогично, при фиксированном i получаем, что i-я строка матрицы C равна лин. комб. строк матрицы B с коэф. из i-й строки матрицы A.

Теорема 6: $\operatorname{rk} AB \leq \operatorname{rk} A$; $\operatorname{rk} AB \leq \operatorname{rk} B$.

Док-во: каждый столбец матрицы $C = AB$ есть лин. комб. столбцов матрицы $B \Rightarrow$ лин. оболочка столбцов C содержится в лин. оболочке столбцов B. А размерность лин. оболочки есть ранг сист. векторов $\Rightarrow \operatorname{rk} C \leq \operatorname{rk} B$.
Аналогично, строки матрицы C лин. выражаются через строки матрицы A. $\Rightarrow \operatorname{rk} C \leq \operatorname{rk} A$. ▲

Примеры умножения матриц

1°. Умножение на диагональную матрицу $D = \begin{pmatrix} d_1 & & 0 \\ & \ddots & \\ 0 & & d_n \end{pmatrix}$
Матрица $\underset{n\times m}{DA}$ получается из A умножением её строк на $d_1; d_2 \ldots d_n$ соответственно.

27.09.17. Алгебра лекция 6.

Опр. Система векторов $\{a_1 \ldots a_n\}$ векторного пространства V называется **базисом**, если она лин. независима и порождает пространство V т.е. $\forall x \in V \quad x = x_1 e_1 + \ldots + x_n e_n$

Это выражение единственно, т.к. если бы их было два:

$x_1 e_1 + \ldots + x_n e_n = x_1' e_1 + \ldots + x_n' e_n \Rightarrow (x_1 - x_1')e_1 + \ldots + (x_n - x_n')e_n = 0.$

но $e_1 \ldots e_n$ – линейно независима $\Rightarrow$ все коэф. $= 0$. $\Rightarrow x_1 = x_1'; \ldots; x_n = x_n'$.

Эти коэф. называются **координатами** вектора x в базисе $e_1 \ldots e_n$.

А он вообще существует? Сколько их? кол-во векторов в базисах одинаковое или нет?

Теорема 1. В любом конечномерном векторном пространстве существует базис, причём 1) все базиса состоят из одного и того же числа векторов (равномощны).

Док-во: ▶1) Пусть $\{a_1 \ldots a_n\}$ – порождающая система векторов. Если она лин. независима, то она является базисом. Если она лин. зависима, то хотя бы один из её векторов лин. выражается через другие остальные. Пусть для определённости это a_n. Тогда $a_1 \ldots a_{n-1}$ также порождают пространство V. Если они лин. независимы, то они составляют базис. Иначе опять один выражается через другие, опять его вычеркнем и т.д. В конце концов получим базис.

2) Почему все базиса состоят из одного кол-ва векторов.

Пусть $\{e_1 \ldots e_n\}$ и $\{f_1 \ldots f_m\}$ – два базиса. и $m \neq n$. Пусть, например, $m > n$. Так как вектора $f_1 \ldots f_m$ лин. выражаются через $e_1 \ldots e_n$, то по основной лемме о лин. зависимости они лин. зависимы $\Rightarrow \{f_1 \ldots f_m\}$ не может быть базисом. ◀

$\Rightarrow$ в конечномерном пространстве все базиса равномощны.

Опр. Число векторов базиса (конечномерного) векторного пространства V называется **размерностью** этого пространства.

Обозначение: $\dim V$ (dimension)

Примеры

1°. $\dim E^2 = 2$; $\dim E^3 = 3$.

2°. $\dim K^n = n$ (пространство строк); базис – единичные строки; $e_i = (00 \ldots 0\underset{i}{1}0 \ldots 0)$.

$x = (x_1 \ldots x_n) = x_1 e_1 + \ldots + x_n e_n$; $(e_1 \ldots e_n)$ – базис (но он не единственный).

3°. $\mathbb{C}$ как векторное пространство над $\mathbb{R}$. $\dim \mathbb{C} = 2$, т.к. базисные вектора это 1 и i. Каждое комплексное число единственным образом представимо в виде $a + bi$.

Опр. Отображение $f: V \to U$ над полем K векторных пространств называется **изоморфизмом**, если оно биективно и сохраняет операции, т.е.

1) $f(x+y) = f(x) + f(y) \quad \forall x, y \in V$ (образ суммы = сумме образов)

2) $f(\lambda x) = \lambda f(x), \quad \forall x \in V, \lambda \in K$.

$\Rightarrow$ Если какие-то вектора в V лин. зависимы, то они в U тоже линейно зависимы с теми же коэф.

Векторные пространства V и U называются изоморфными, если между ними существует изоморфизм.

Когда конечномерные векторные пространства изоморфны?

Если векторные пространства V и U изоморфны и V конечномерно, то и U конечномерно, т.к. если V порождается $\langle a_1 \dots a_n \rangle$, то U порождается их образами.

Теорема 2 Конечномерные пространства V и U изоморфны $\Leftrightarrow$ их размерности одинаковы.

Док-во: $\Rightarrow$ 1) Пусть V и U изоморфны, т.е. $f: V \to U$ – изоморфизм. Тогда, если $\{e_1 \dots e_n\}$ – базис пространства V, то образы этих элементов $\{f(e_1), f(e_2) \dots f(e_n)\}$ – базис пространства U, т.к., во-первых, они порождают U, а во-вторых, они лин. независимы, т.к. если бы они были лин. зависимы, то вектора $e_1 \dots e_n$ были бы зависимы с теми же коэф. Действительно, пусть
$\lambda_1 f(e_1) + \dots + \lambda_n f(e_n) = 0$, но это $= f(\lambda_1 e_1 + \dots + \lambda_n e_n) = 0$.
Но если образ вектора $=0$, то и сам вектор $=0$ (т.к. биекция).
$\Rightarrow \{f(e_1), f(e_2) \dots f(e_n)\}$ – базис $\Rightarrow$ размерности одинаковы.

2) Пусть $\dim V = \dim U = n$ и $\langle e_1 \dots e_n \rangle$ – базис пространства V. $\{f_1 \dots f_n\}$ – базис пространства U. Рассмотрим отображение $f: V \to U$, устроенное так: если $x = x_1 e_1 + \dots + x_n e_n \in V$, то положим $f(x) = x_1 f_1 + \dots + x_n f_n$.

Это биективное отображение, т.к. разложение по базису существует (каждый будет образом) и единственно (он – образ единственного элемента) (ну, для $x_1 f_1 + \dots + x_n f_n$ – прообраз $x_1 e_1 + \dots + x_n e_n$; а если есть 2 разложения, то $(x_1 - x_1')f_1 + \dots + (x_n - x_n')f_n = 0 \Rightarrow$ все коэф $= 0 \Rightarrow x_i = x_i'$). Оно сохраняет операции, т.к. при сложении векторов их соотв. координаты складываются $\Rightarrow$

$$\Rightarrow f(x+y) = f(x_1 e_1 + \dots + x_n e_n + y_1 e_1 + \dots + y_n e_n) = f(e_1(x_1+y_1) + \dots + e_n(x_n+y_n)) =$$
$$= f(e_1(x_1+y_1)) + \dots + f(e_n(x_n+y_n)) = f_1(x_1+y_1) + \dots + f_n(x_n+y_n) = f_1 x_1 + \dots + f_n x_n +$$
$$+ f_1 y_1 + \dots + f_n y_n = f(x) + f(y).$$

Аналогично проверим, что $f(\lambda x) = \lambda f(x)$. $\Rightarrow$ это изоморфизм.

В частности, n-мерное векторное пространство над полем K изоморфно пространству K^n.

Теорема 3 Всякую лин. независимую систему векторов конечномерного вект. пространства можно дополнить до базиса.

Док-во: Пусть $\{e_1 \dots e_n\}$ – лин. независимая система векторов и пусть $\dim V = n$. Возьмём и добавим ещё вектор, ещё, ещё. Мы когда-нибудь остановимся, и именно в момент, когда $m = n$, т.к. более $m > n$ векторов лин. зависимы (по основной лемме о лин. зависимости). Вот мы получили max лин. независимую систему векторов $\{e_1 \dots e_m\}$. Тогда $\forall x \in V$ система

$\{e_1 \dots e_m; x\}$ – будет лин. зависимой ⇒ x лин. выражается через $e_1 \dots e_m$.
Значит, $e_1 \dots e_m$ ~~~~ составляют базис ($\dim = n$) ◄

Пусть S – любое подмножество (конечное или бесконечное) n-мерного векторного пространства V. Тогда в S существует макс. лин. независимое подмн-во (т.е. нельзя добавить элемент, чтобы осталось лин. независ.)

Теорема 4 Любое макс. лин. независимое подмножество множества S является базисом линейной оболочки.

Док-во: ⇒ Пусть $\{e_1 \dots e_r\} \subset S$ – макс. лин. независимое подмножество. Тогда при добавлении любого вектора из S мы получим линейно зависимое подмножество. Т.е. $\forall x \in S$ система $\{e_1 \dots e_r; x\}$ – лин. зависима (если $x \neq e_i$, то т.к. это макс. подмн-во, если $x = e_i$, то т.к. там два одинаковых вектора).
⇒ x лин. выражается через $e_1 \dots e_n$ ⇒ все вектора лин. оболочки выражаются через $e_1 \dots e_r$ ⇒ это базис лин. оболочки ◄

Следствие Все max лин. независимые подмн-ва мн-ва S состоят из одного и того же числа векторов = размерности ~~пр-ва~~ лин. оболочки. Это число называется **рангом** мн-ва S. Обозначается: $\mathrm{rk}\, S$ (rank)

Рассмотрим подпространство. Что с его размерностью?

Теорема 5 ▶ Пусть U – подпр-во n-мерного векторного пр-ва V. Тогда $\dim U \le n$ и если $\dim U = n$, то $U = V$.

Док-во: Рассмотрим макс. лин. независимую систему векторов в подпространстве U. Тогда эти $\{e_1 \dots e_m\}$ по теореме 4 являются базисом подпр-ва U. Теперь этот базис можно дополнить (по теореме 3) до базиса всего пр-ва V: $\{e_1 \dots e_m; \dots e_n\}$ ⇒ $\dim U = m \le n$. Если $m = n$, то $U = V$ (больше тоже не может, т.к. векторов $m > n$ лин. зависима, а дополн-ть, т.к. $\{e_1 \dots e_m; x\}$ будет лин. зависима ⇒ x выражается). ◄

Ранг матрицы

Опр. **Рангом** матрицы называется ранг системы строк (как вект. пространства K^n)

$$\underset{[m \times n]}{A} = \underbrace{\begin{pmatrix} \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{pmatrix}}_{n} \Big\} m$$

По опр. ранг – это max. кол-во лин. независимых строк.

Как найти ранг матрицы?

Теорема 1 ▶ Ранг матрицы равен числу ненулевых строк ступенчатой матрицы, к которой она приводится путём элементарных преобразований строк.

Док-во: 1) Докажем сначала, что ранг матрицы не меняется при элем. преобразованиях строк. ~~Тогда все стр.~~ Пусть матрица B получается из A одним элем. преобразованием строк. Тогда все строки матрицы B лин. выражаются через строки матрицы A. И, следовательно, лин. оболочка строк матрицы B содержится в лин. оболочке строк матрицы A. Но матрица A

получается из B обратными преобразованиями строк (также элементарными). ⇒ лин. оболочка строк A содержится в лин. оболочке строк B ⇒ они друг в друге содержатся ⇒ они совпадают. А ранг системы векторов есть размерность лин. оболочки ⇒ $rk\,A = rk\,B$.
⇒ если ранг не меняется при 1 элем. преобразовании, то он не меняется и при цепочке преобразований.

в) Приведём матрицу к ступенчатому виду с помощью элем. преобразований строк. Ранг не изменится ⇒ для док-ва теоремы достаточно док-ть, что ранг ступенчатой матрицы = числу её ненулевых строк. Рассмотрим ступенчатую матрицу A:

$$\begin{pmatrix} a_{1j_1} & * & * & * & * \\ 0 & a_{2j_2} & * & * & * \\ 0 & 0 & \dots & * & * \\ 0 & 0 & & a_{rj_r} & * \\ 0 & 0 & 0 & & \end{pmatrix}$$

Докажем, что первые r строк лин. независимы. Предположим, что их ~~лин~~ нетрив. лин. комб = 0. Рассмотрим j_1-ю координату. $\lambda_1 a_{1j_1} = 0 \Rightarrow \lambda_1 = 0$. Рассмотрим j_2-ю координату: $\lambda_1 * + \lambda_2 a_{2j_2} = 0$, но $\lambda_1 = 0 \Rightarrow \lambda_2 = 0$. И так дальше. Получим, что $\lambda_1 = \dots = \lambda_r = 0$
⇒ это не нетрив. лин. комб ⇒ они лин. независимы. ◀

Следствие как бы мы матрицу ни приводили к ступенчатому виду, ~~ранг~~ всё равно кол-во ненулевых ступеней будет одинаковым (т.к. при элем. преобр. ранг не меняется, а ранг = кол-ву ненулевых ступеней).

20.09.17. Алгебра. Лекция 5.

Векторные пространства.

Опр. **Векторным пространством** над полем K называется мн-во V с операциями сложения и умножения на элементы поля, удовлетворяющее следующим условиям:

1) V есть абелева группа по сложению
2) $\lambda(a+b) = \lambda a+\lambda b$ — дистрибутивность, где $\lambda \in K$; $a, b \in V$.
3) $(\lambda+\mu)a = \lambda a+\mu a$, где $\lambda, \mu \in K$; $a \in V$.
4) $(\lambda\mu)a = \lambda(\mu a)$, где $\lambda, \mu \in K$; $a \in V$.
5) $1 \cdot a = a$; где $a \in V$.

Элементы векторного пространства называются векторами.

Примеры: 1° Пространство "геометрических" векторов E^2; E^3

2° Пространство строк K^n

Пространство $(m \times n)$ матриц с элементами поля K — то же, что K^{mn}

3° Пространство функций: $F(X, K)$

4° Если L — расширение поля K, то L можно рассматривать как векторное пространство над K.

5° Нулевое векторное пространство 0

Простейшие следствия аксиом векторного пространства.

1° $\lambda \cdot 0 = 0$ (т.к. если $0 \cdot a = x \Rightarrow x+x = (0+0) \cdot a = 0 \cdot a = x \Rightarrow x = 0$).

2° $\lambda(-a) = -\lambda a$ (т.к. $\lambda(-a)+\lambda a = \lambda(a+(-a)) = \lambda 0 = 0$).

3° $\lambda(a-b) = \lambda a-\lambda b$ (т.к. $\lambda(a-b)+\lambda b = \lambda(a-b+b) = \lambda a$)

4° $0 \cdot \vec{a} = \vec{0}$ аналогично 1°.

5° $(-1)\vec{a} = -\vec{a}$ аналогично 2° (только вместо 2 аксиома пользуемся 3)

6° $(\lambda-\mu)a = \lambda a-\mu a$ аналогично 3°.

Опр. **Подпространством** векторного пр-ва V называется подмножество $U \in V$, удовлетворяющее следующим условиям.

1) U есть подгруппа по сложению.
2) $\forall a \in U$, $\lambda \in K$, $\lambda a \in U$ (т.е. замкнуто по умножению на элемент группы).

Всякое подпространство само является векторным пространством относительно тех же операций.

Примеры: 1° Подпространство в E^3, состоящее из векторов $\parallel$ какой-нибудь заданной плоскости.

2° Подпространство непрерывных функций в $F(R, R)$.

3° Подпространство многочленов

4° Подпространство чётных функций (они и подгруппа, и подпространство).

Пусть V — векторное пространство, $a_1 \ldots a_n \in V$.

Всякое выражение вида $\lambda a_1+\ldots+\lambda_n a_n$ $(\lambda_1 \ldots \lambda_n \in K)$ называется **линейной комбинацией** векторов $a_1 \ldots a_n$.

Линейная комбинация называется **тривиальной**, если все её коэффициенты $=0$ ($\lambda_1 = \dots = \lambda_n = 0$).

Вектор b линейно выражается через $a_1 \dots a_n$, если $\exists \lambda_1 \dots \lambda_n \in K : b = \lambda_1 a_1 + \dots + \lambda_n a_n$

<u>Опр.</u> Система векторов $\{a_1 \dots a_n\}$ называется **линейно зависимой**, если некоторая их нетривиальная линейная комбинация $=0$, и **линейно независимой** в противном случае.

$\{a_1\}$ лин. зависима $\Leftrightarrow a_1 = 0$.

$\{a_1, a_2\}$ лин. зависима $\Leftrightarrow \left[\begin{array}{l} a_1 = \lambda a_2 \\ a_2 = \mu a_1 \end{array}\right.$ (т.е. вектора пропорциональны.)

Если какая-либо подсистема системы $\{a_1 \dots a_n\}$ линейно зависима, то и вся система линейно зависима (ну просто к нетривиальной маленькой линейной комбинации добавим остальные вектора с нулевыми коэффициентами)

Лемма 1. Система векторов $a_1 \dots a_n$ линейно зависима $\Leftrightarrow$ существует такой номер i, что вектор a_i линейно выражается через остальные вектора системы.

<u>Док-во.</u> <u>туда</u> пусть a_n линейно выражается через $a_1 \dots a_{n-1}$.

$\Rightarrow a_n = \mu_1 a_1 + \dots + \mu_{n-1} a_{n-1}$. Тогда $\mu_1 a_1 + \dots + \mu_{n-1} a_{n-1} - a_n = 0 \Rightarrow$ но нашли нетривиальную линейную комбинацию $=0$.

<u>обратно</u> Пусть есть нетривиальная лин. комб. $\lambda_1 a_1 + \dots + \lambda_n a_n = 0$. Докажем, что a_n выражается через $a_1 \dots a_{n-1}$ (пусть для определённости $\lambda_n \neq 0$). $\Rightarrow a_n = -\frac{\lambda_1}{\lambda_n} a_1 - \dots - \frac{\lambda_{n-1}}{\lambda_n} a_{n-1}$.

Но важно, что для линейной зависимости необязательно каждый вектор должен выражаться через другие. например, система из двух векторов: №1 нулевой, №2 — не нулевой. ненулевой через нулевой не выражается.

Лемма 2 Пусть $\{a_1 \dots a_n\}$ — линейно независимая система векторов и b — какой-то вектор. тогда $\{a_1 \dots a_n, b\}$ — линейно зависимая система $\Leftrightarrow$ b линейно выражается через $a_1 \dots a_n$.

<u>Док-во:</u> 1) Пусть $b = \lambda_1 a_1 + \dots + \lambda_n a_n$. тогда $\lambda_1 a_1 + \dots + \lambda_n a_n - b = 0$. $\Rightarrow \exists$ нетрив. лин. комб. $=0$.

2) пусть $\lambda_1 a_1 + \dots + \lambda_n a_n + \mu b = 0$ — нетрив. лин. комб. $\mu \neq 0$ — т.к. иначе есть нетрив. лин. комб. для векторов $a_1 \dots a_n \Rightarrow$ они не лин. независимы

$\Rightarrow b = -\frac{\lambda_1}{\mu} a_1 - \dots - \frac{\lambda_n}{\mu} a_n$

Лемма 3 (Основная лемма о линейной зависимости).

Пусть вектора $b_1 \dots b_m$ лин. выражаются через вектора $a_1 \dots a_n$. Если $m > n$, то вектора $b_1 \dots b_m$ — лин. зависимы.

<u>Док-во:</u> Пусть $b_i = \sum_{j=1}^{n} \mu_{ij} a_j$ $(i = 1 \dots m)$

Вычислим лин. комбинацию $\lambda_1 b_1 + \dots + \lambda_m b_m$ с неопределёнными коэффициентами (потом подберём).

$\sum_i \lambda_i b_i = \sum_{ij} \lambda_i \mu_{ij} a_j = \sum_j \left(\left(\sum_i \mu_{ij} \lambda_i \right) a_j \right)$ (*)

Мы хотим подобрать λ_i так, чтобы это выражение было $=0$.

Если $\forall j$ $\sum \mu_{ij} \lambda_i = 0$, то $\sum_i \lambda_i b_i = 0$. (следует из *)

Рассмотрим эти равенства как систему однородных лин. уравнений относительно $\lambda_1 \dots \lambda_m$.

Число уравнений = n; число неизвестных = m; Если m>n (т.е. число ур-й < числа неизвестных), то система уравнений имеет ненулевое решение и, значит, вектора $b_1 \dots b_m$ линейно зависимы. чтд □

Пусть $S \subset V$ – какое-то подмножество. Совокупность всех линейных комбинаций $\lambda_1 a_1 + \dots + \lambda_n a_n$ ($a_1 \dots a_n \in S$; $\lambda_1 \dots \lambda_n \in K$) является подпространством (ну проверили, что сумма лин.комб = лин.комб; 0 = лин.комб, − лин.комб = лин.комб, произведение лин.комб. на число – тоже лин.комб).
То, что получилось – это наименьшее подпространство, содержащее S. потому что подпространство, содержащее S, содержит все лин. комб. с элементами из S.
Это называется **линейной оболочкой** мн-ва S и обозначается <S>.
Если <S> совпадает с V, то говорят, что мн-во S **порождает** пространство V (т.е. всякий элемент из V выражается через вектора из S), или что S является порождающим ~~мн~~ множеством.

Опр. Векторное пространство V называется **конечномерным**, если оно порождается конечным числом векторов.

Следствие леммы 3 Если векторное пространство V порождается n векторами, то всякие m>n векторов линейно зависимы.

Примеры конечномерных пространств

E^2; E^3;

K^n – пространство строк; порождающие – единичные строки: $e_i = (0\,0 \dots \underset{i}{1} \dots 0)$.

ℂ – как векторное пространство над ℝ, порождается 1, i.

Примеры бесконечномерных пространств.

- Пространство функций $F(\mathbb{R}, \mathbb{R})$. Почему оно бесконечномерное? надо показать, что тут существуют линейно независимые системы сколь угодно многих векторов. например, $1, x, x^2 \dots x^n$. Они лин. независимы, т.к. иначе некий многочлен тождественно = 0. но тогда все его коэф. = 0 ⇒ ~~ком~~ лин. комб. тривиальная.
Или проще: функция равная единице в какой-то точке и нулю во всех остальных. И так для n разных точек. но они плохи тем, что они не непрерывные.

- ℝ как векторное пространство над ℚ. Оно бесконечномерное, т.к. линейных комбинаций из рац. чисел с рац. коэф счётно (т.к. ℚ – счётное, а счётное × счётное = счётное).

06.09.17 Алгебра Лекция 2 Группы, кольца, поля.

$\begin{cases} a+b\sqrt{2} \ (a, b \in \mathbb{Q} \text{ — рациональные числа}) \\ a+b\sqrt{-1} \ (a, b \in \mathbb{R}) \end{cases}$

(теория про уравнения пройдёт, несмотря на то что строилась для вещественных чисел.

А на $\mathbb{Z}$ не пройдёт — т.к. не всегда можно делить.

Абелева группа

Есть множество с 1 операцией

Опр **Аддитивной абелевой (=коммутативной) группой** называется множество A с операцией сложения, удовлетворяющее следующим условиям:

1) $a+b=b+a$ (коммутативность)
2) $(a+b)+c = a+(b+c)$ (ассоциативность)
3) $\exists\, 0$ (нуль): $a+0=a \ \forall a \in A$
4) $\forall a \in A \ \exists -a$ (противоположный элемент): $a+(-a)=0$.

Простейшие следствия аксиом

1) Нуль единственен. (т.к. если есть 0_1 и 0_2, то $0_1 = 0_1+0_2 = 0_2 \Rightarrow 0_1 = 0_2$)
2) противоположный элемент единственен

(т.к. если есть $(-a)_1$ и $(-a)_2$, то $(\underbrace{(-a)_1+a}_{=0})+(-a)_2 = (-a)_1+(\underbrace{a+(-a)_2}_{=0})$

$\Rightarrow (-a)_1 = (-a)_2$)

3) Уравнение $x+a=b$ имеет единственное решение $\forall a, b$

Док-во: $x+a=b \Rightarrow x+a+(-a) = b+(-a) \Rightarrow x = b+(-a) \Rightarrow$ не более 1 решения

проверим, что это решение.

$(b+(-a))+a = b+((-a)+a) = b+0 = b$. Обозначаем: $b-a = b+(-a)$

Примеры абелевой группы по сложению: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, а также мн-ва векторов, строк $(a_1, \ldots a_n), a_i \in \mathbb{R}$ (сложение покомпонентно), функции образуют абелеву группу по умножению.

Опр **Мультипликативной абелевой группой** называется множество A с операцией умножения, удовлетворяющее следующим условиям:

1) $ab = ba$
2) $(ab)c = a(bc)$
3) $\exists e$ (единица): $ae = a \ \forall a \in A$
4) $\forall a \in A \ \exists a^{-1}$ (обратный элемент): $a \cdot a^{-1} = e$

Простейшие следствия аксиом.

1) Единица единственна
2) обратный элемент единственен
3) Уравнение $ax=b$ имеет единственное решение

Примеры мультипликативных групп: $\mathbb{Q}^*=\mathbb{Q}\setminus\{0\}$; $\mathbb{R}^*=\mathbb{R}\setminus\{0\}$;
$A=\{\pm1\}$ ($\mathbb{Z}$ не является, т.к. почти у всех элементов (e.g. 2, 3...) нет обратного; $\mathbb{Q}$ не является, т.к. у нуля нет обратного)

Опр. **подгруппой аддитивной абелевой группы** называется подмножество $B\subset A$, удовлетворяющее следующим условиям:
1) $a,b\in B \Rightarrow a+b\in B$ (замкнутость относительно сложения)
2) $0\in B$
3) Если $a\in B \Rightarrow -a\in B$.

подгруппа абелевой группы тоже является абелевой группой по относительно этой операции.

Примеры подгрупп в аддитивной абелевой группе: $\mathbb{Z}\subset\mathbb{Q}\subset\mathbb{R}$

Примеры подгрупп в мультипликативной абелевой группе: $\{\pm1\}\subset\mathbb{Q}^*\subset\mathbb{R}$

Опр. **подгруппой мультипликативной абелевой группы** A называется подмножество $B\subset A$, удовлетворяющее следующим условиям:
1) $a,b\in B \Rightarrow ab\in B$ (замкнутость относительно умножения)
2) $e\in B$
3) Если $a\in B \Rightarrow a^{-1}\in B$.

подгруппа мультипликативной абелевой группы тоже мультипликативная абелева группа.

примеры подгрупп: • вектора $\parallel$ одной прямой (в аддитивной группе векторов)
• в функциях — все функции вида $y=ax+b$ или вида $y=c$.
• все многочлены степени $\leq n$.
• чётные (нечётные) функции
• непрерывные функции
• функции, обращающиеся в ноль в какой-то фиксированной точке

А вообще движения плоскости — это тоже группа. Она ассоциативная, но не коммутативная, но там хотя бы есть единица и обратный элемент.

Кольца и поля

Опр. **Кольцом** называется множество K с операциями сложения и умножения, удовлетворяющее следующим условиям:
1) K есть абелева группа по сложению (т.е. сложение ассоциативно и коммутативно, есть ноль и противоположный элемент)
2) $a(b+c)=ab+ac$ | дистрибутивность
$(a+b)c=ac+bc$

Простейшие следствия аксиом

1) $0 \cdot a = a \cdot 0 = 0 \ \forall a \in K$

(Пусть $0 \cdot a = b$. Тогда $b + b = 0 \cdot a + 0 \cdot a = (0+0)a = 0 \cdot a = b$. Прибавим с обеих сторон $(-b)$ и получим $b = 0 \Rightarrow 0 \cdot a = 0$. Аналогично для $a \cdot 0$)

2) $(-a)b = a(-b) = -ab$

($(-a)b + ab = (-a+a)b = 0 \cdot b = 0 \Rightarrow (-a)b$ – элемент, противоположный к ab)
Аналогично для $a(-b)$.

3) $a(b-c) = ab - ac$; $(a-b)c = ac - bc$ ← дистрибутивность умножения относительно вычитания

($a(b-c) + ac = a(b-c+c) = ab \Rightarrow a(b-c) = ab - ac$
Аналогично для $(a-b)c = ac - bc$)

Кольцо K называется **коммутативным (ассоциативным)**, если умножение в нём коммутативно (ассоциативно)

Единицей кольца называется такой элемент 1, что
$a \cdot 1 = 1 \cdot a = a \ \forall a \in K$.

Если единица существует, то она единственна (т.к. $1_1 = 1_1 \cdot 1_2 = 1_2$)

Примеры: • $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$ – коммутативное, ассоциативное кольца
• $2\mathbb{Z}$ – коммутативное, ассоциативное кольцо с единицей
• вектора – кольцо относительно сложения и векторного произведения без единицы.
(это когда получается вектор $\perp a$ и b и равный площади пар-а на a и b)
$a \times b$, a, b но это кольцо ~~неко~~ не коммутативное и не ассоциативное.
Там есть "антикоммутативность": $a \times b = -b \times a$.
А вместо ассоциативности: $(a \times b) \times c + (b \times c) \times a + (c \times a) \times b = 0$.

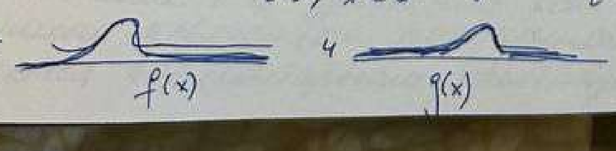
Опр **Полем** называется коммутативное ассоциативное кольцо (т.е. сложение и умножение ассоц. и коммут., есть 0 и 1, есть противоположный ~~и обратный элемент~~ и дистрибутивность) с единицей, в котором каждый ненулевой элемент имеет обратный.

$\Rightarrow$ мн-во ненулевых элементов поля является абелевой группой по умножению. (Если K – поле, то $K^* = K \setminus \{0\}$ – аб. гр. по умнож)

А почему там вообще умножение определено, т.е. почему не может быть так: ~~разве~~ $a, b \neq 0$, но $ab = 0$?
Пусть $ab = 0$. Тогда $(ab)b^{-1} = 0$ (т.к. $ab = 0$). Но $(ab)b^{-1} = a$. Но $a \neq 0$. Противоречие.
То есть в поле если произведение $= 0$, то хотя бы один из них $= 0$.
А в кольце – нет. Бывает, что произведение 2 ненулевых $= 0$.
(произведение = композиция)

Например: $f(x) = \begin{cases} 1, & x \geq 0 \\ 0, & x < 0 \end{cases}$ $\quad g(x) = \begin{cases} 0, & x \geq 0 \\ 1, & x < 0 \end{cases}$ Тогда $g(f(x)) = 0$.

Или



Если в кольце $ab = 0$, но $a, b \neq 0$, то говорят, что a, b — делители нуля

Опр. подкольцом кольца K называется подмножество $L \subset K$, удовлетворяющее следующим условиям:

1) L есть подгруппа по сложению (т.е. $B \subset A$, $0 \in B$; $a, b \in B \Rightarrow a+b \in B$; $-b \in B$)
2) Если $a, b \in L \Rightarrow ab \in L$ (замкнутость относительно умножения)

подкольцо само является кольцом относительно тех же операций

Пример • $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R}$ • в кольце функций констант — подкольцо (а линейные — нет, трёхчлены — нет) • $\forall n \; n\mathbb{Z} \subset \mathbb{Z}$.

Опр. подполем поля K называется подкольцо $L \subset K$, такое что:

1) $1 \in L$
2) $\forall a \in L$, $a \neq 0$ $a^{-1} \in L$

подполе само является полем относительно тех же операций.

Примеры полей: $\mathbb{Q}$; $\mathbb{R}$

Ещё пример поля: $K = \{0; 1\}$

+	0	1
0	0	1
1	1	0

×	0	1
0	0	0
1	0	1

Задача Док-ть, что не существует поля из 6 элементов.
(пытаемся построить таблички, перебираем все возможности для несразу определённых клеток, все невозможны)