Повесть о родео и Джульетте

Содержание

1 Лекция 1. Вектороные пространства. Начало беды

1.1 Векторные пространства

Definition 1.1. Векторное пространство

Пусть K - поле, тогда в.п. над K называется тройка $(V, +, *)$, где

1. V множество
2. $+ : V \times V \to V$
3. $* : K \times V \to V$

Со следующими аксиомами

1-4) : $(V, +)$ - абелева группа ($\overline{0}$ - нейтральный элемент)
5) $(\lambda + \mu)v = \lambda v + \mu v$
6) $\lambda(v + u) = \lambda v + \lambda u$
7) $(\lambda\mu)v = \lambda(\mu v)$
8) $1 * v = v$

Элементы V - векторы, а элементы K - скаляры.

Reminder. $0 * v = \overline{0}$, *т.к.* $(0 + 0)v = 0 * v$
$(-1) * v = -v$, *т.к.* $\overline{0} = 0 * v = (1 - 1)v$

Exercise 1.1.

Аксиома $v + u = u + v$ следует из остальных

Example 1.1.

$Vect_2$ - вектора на плоскости. Откладываем направленные отрезки из точки 0.
Задав систему координат получим биекцию между векторами и точками в $\mathbb{R}^2$, где последнее рассматриваем как столбцы высоты 2. Мы получили, что векторные пространства $Vect_2$ и $\mathbb{R}^2$ изоморфны(определение будет ниже).

Definition 1.2. Арифметическое векторное пространство

Пусть K - поле. Арифметическое векторное простарнство это

$$K^n = \left\{ \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} : x_i \in K \right\}$$

То есть множество столбцов высоты n с покомпонентными операциями. Тривочев все аксиомы выполнены(т.к. они выполнены для самого K). $\overline{0}$ - вектор из нулей.

Definition 1.3. Гомоморфизм в.п.

V_1, V_2 - в.п. над K, тогда $f : V_1 \to V_2$ - гомоморфизм (линейное отображение), если

$$f(v_1 + v_2) = f(v_1) + f(v_2)$$
$$f(kv) = kf(v)$$
$$v \in V,\ k \in K$$

Definition 1.4. Изоморфизм в.п.

$V_1, V_2,\ f : V_1 \to V_2$ изоморфизм, если это биективный гомоморфизм.
В этом случае V_1, V_2 называют изоморфными.

Example 1.2.

Пусть $V = K[x]$ или $K[x]_n$ - многочлены $deg \leq n$.
Аксиомы выполнены как частные случаи аксиомы кольца многочленов.
$f \in K[x],\ f = \sum a_i x^i,\ f = (a_i)_i$.

В $K[x]_n$ очевидна биекция $f \iff \begin{pmatrix} a_0 \\ \vdots \\ a_n \end{pmatrix}$ и это изоморфизм $K[x]_n$ и K^{n+1}.

Он не единственен. Можно сопоставить коэффициенты $f = \sum a'_i (x-1)^i$

Другой изоморфизм: зафиксируем $b_0, \dots b_n$ и будем сопоставлять $\begin{pmatrix} f(b_0) \\ \vdots \\ f(b_n) \end{pmatrix}$

Ещё: если $K = \mathbb{C}$, тогда $f = a\prod(x - x_i)$. Тогда можем закодировать $\begin{pmatrix} a \\ \vdots \\ x_n \end{pmatrix}$, но это плохое соответствие, не гомоморфизм(даже не отображение)...

Example 1.3.

Рассмотрим $U = \{(x_1, x_2, \dots) \mid x_i \in \mathbb{R}, x_{i+2} = x_i + x_{i+1}\}$ - последовательности фибоначчиевого типа.
Понятно, что сумма двух последовательностей и умноженная на скаляр последовательность лежит в U. То есть это в.п. над $\mathbb{R}$.
При этом каждую последовательность определяют первые два члена, то есть имеем $F : U \to \mathbb{R}^2$, где $(x_1, x_2, \dots) \mapsto (x_1, x_2)$ - изоморфизм в.п.

Example 1.4.

$K = \mathbb{Z}/2\mathbb{Z}$, M какое-то множетсво(конечное размера n). И $V = 2^M$.
Зададим $1 * N = N,\ 0 * N = \emptyset$. $N_1 + N_2 = (N_1 \cup N_2) \setminus (N_1 \cap N_2) = N_1 \Delta N_2$
Любое подмножество кодируется строкой из 0 и 1.(содержит или не содержит соответствующий элемент)
Имеем биекцию $V \to \mathbb{Z}/2\mathbb{Z}^n$ и это гомоморфизм.

Definition 1.5. Линейная комбинация

Пусть V - в.п. над K и есть $\{v_i\}_{i\in I}$ система векторов из V. (если I конечно, то можно считать $v_1, \dots, v_n$).
Пусть $\{a_i\}_{i\in I}$ система элементов K т.ч. количество $a_i \neq 0$ конечно.
Тогда $\sum_{i\in I} a_i v_i$ называется линейной комбинацией векторов v_i с коэф. a_i.

Далее I конечно(но это не важно).

Definition 1.6. Линейная оболочка

Множество линейных комбинаций векторов $v_1, \dots, v_n$ называется их линейной оболочкой и обозначается $\langle v_1, \dots, v_n\rangle = \{\sum a_i x_i \mid a_i \in K\}$.

Remark 1.1.

1. $\langle v_1, \dots, v_n\rangle$ является векторным пространством относительно тех же операций. Нужно проверить замкнутость относительно сложения и умножения на константу.
2. U подпространство V и $v_i \in U$, тогда $\langle v_1, \dots, v_n\rangle \subset U$ (лин.оболочка - наименьшее такое подпространство, содержащее все v_i)

Example 1.5.

Рассмотрим $Vect_3$. $\langle v_1\rangle$ - прямая через v_1, $\langle v_1, v_2\rangle$ - плоскость(или прямая, если они совпадают), натянутая на эти векторы.

Definition 1.7. Порождающий набор

V в.п., набор $\{v_i\}$ называется порождающим, если его лин.оболочка $= V$.

Definition 1.8. Конечномерное пространство

V называется конечномерным, если существует конечная порождающая система.

Example 1.6.

$\mathbb{R}^n, K[x]_n$ конечномерные
$K[x]$ нет. Пусть есть какой-то $\{f_i\}$ - порождающий, но тогда для любого $f = \sum a_i f_i \Rightarrow deg(f) \leq \max_i deg(f_i)$.

Definition 1.9. Линейная независимость

Система векторов v_i называется линейно независимой, если выполнено одно из двух равносильных условий

1. $\forall i,\ v_i \notin \langle\{v_j\}_{j\neq i}\rangle$
2. $\forall a_1, \dots, a_n \in K$, $\sum a_i v_i = 0 \Rightarrow \forall i\ a_i = 0$

Доказательство. Пусть $v_i \in \langle\{v_j\}_{j\neq i}\rangle \Rightarrow v_i = \sum_{j\neq i} a_j v_j \Rightarrow 0 = -v_i + \sum_{j\neq i} \Rightarrow 0 = -1$ из второго пункта.

Обратно. $\forall i\ v_i \notin \langle \{v_j\}_{j\neq i}\rangle$ и $\sum a_i v_i = 0$ и есть не нулевая a_i, тогда $v_i = -\frac{1}{a_i}(\sum a_j v_j)$ - противоречие. $\square$

Definition 1.10. Базис

V - в.п. над K. $v_1, \dots, v_n \in V$ называется базисом, если он порождающий и линейно независимый

Example 1.7. Стандартный базис

$V = K^n$, e_i - столбец из всех 0 кроме 1 на i-м месте. Тогда верно $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} = \sum a_i e_i$.

Theorem 1.1. Эквивалентные определения базиса

Следующие условия равносильны:

1. $v_1, \dots, v_n$ - базис V
2. $\forall v \in V$, $\exists!\, a_i\ :\ v = \sum a_i v_i$
3. v_i макс. лин.независимая система, то есть $\forall v \in V$, $v_1, \dots, v_n, v$ - лин. завис.
4. $v_1, \dots, v_n$ - мин. порождающая, то есть $\forall i\ v_1, \dots, v_{i-1}, v_{i+1}, \dots, v_n$ не порождающая

Доказательство. $1 \Rightarrow 2$. $v \in V, v = \sum a_i v_i$ т.к. $\{v_i\}$ порождающий. Если есть $v = \sum a_i v_i = \sum b_i v_i \Rightarrow \sum (a_i - b_i) v_i = 0 \Rightarrow a_i = b_i \forall i$.

$2 \Rightarrow 1$. $\{v_i\}$ порождающий. $\sum a_i v_i = 0 = \sum 0 * v_i \Rightarrow a_i = 0$.

$1 \Rightarrow 4$. Пусть есть v_i, т.ч. без него все ещё порождающая, но тогда $v_i \in \langle v_j \rangle$ - противоречие определению лин.нез

$4 \Rightarrow 1$. Пусть она лин. зависима, т.е. есть $v_i = \sum a_j v_j$, тогда мы можем её выкинуть и все ещё получим порождающую систему. $(V = \langle x_i \rangle = \langle x_j,\ j \neq i \rangle)$

Остальное упр. $\square$

Theorem 1.2. Существование базиса

В любом конечномерном пространстве есть конечный базис.

Доказательство. Пусть

$V = \langle v_i \rangle$ - конечная порождающая система.

Будем выкидывать v_i из набора с сохранением свойства порождаимости. За конечное число шагов придем к минимальной порождающей, то есть к базису. $\square$

Corollary. *Пусть V - к-м. пространство, тогда $\exists n\ : V \cong K^n$.*

Доказательство. Существует базис $v_1, \dots, v_n$. Рассмотрим отображение $f : K^n \to V$, где $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \mapsto \sum a_i v_i$.

Это очевидно гомоморфизм.(сумма раскрывается по дистрибутивности).

Это биекция по второму определению базиса. $\square$

Remark 1.2.

Если V - бесконечномерное, то базис всегда существует.
$V = K[x]$, базис x^i
$V = K[[x]]$, базис есть но предъявить нельзя..
$V = \mathbb{R}$ как в.п. над $\mathbb{Q}$(или над $\mathbb{R}$, но тогда это одномерное пространство). Существует бесконечный базис, который не выражается...

Definition 1.11. Размерность

Пусть V конечномерное, его размерность $\dim V$ это такое n, что $V \cong K^n$.
Другое определение: $\dim V$ это количество векторов в базисе.

Пока не знаем, единственно ли такое n.

Theorem 1.3. Количество элементов в базисе

Если $v_1, \dots, v_n$ и $u_1, \dots, u_m$ - базисы, то $m = n$.

Lemma 1.1. О линейной зависимости линейных комбинаций(лкзк)

Пусть есть два набора $u_1, \dots, u_m$ и $v_1, \dots, v_n$ при этом $n > m$ и $v_i \in \langle u_i \rangle$, тогда v_i линейно зависимы.

Доказательство. Если v_i, u_i - базисы и $n > m$, то т.к. u - порождающее по лемме v_i будут линейно зависимые, что противоречит определению базиса. Это доказывает теорему.

Сама лемма: Индукция по m. База $m = 0$. $\langle ... \rangle = \{0\}$. Очев..

Переход $m \to m+1$. $v_1, \dots, v_n \in \langle u_1, \dots, u_{m+1} \rangle$, $n > m+1$.

$v_i = \sum a_{ij} u_j$. Посмотрим на $a_{i,m+1}$. Если все равны 0, тогда $v_1, \dots, v_n \in \langle u_1, \dots, u_m \rangle \Rightarrow$ по индукционному предположению v_i - лин. зависимы.

Пусть не все равны 0. Н.У.О. $a_{1,m+1} \neq 0$. Рассмотрим вектора $\widetilde{v_2}, \dots, \widetilde{v_n}$ $\widetilde{v_i} = v_i - \frac{a_{i,m+1}}{a_{1,m+1}} v_1 = \sum_{j=1}^{m} (a_{ij} - \frac{a_{i,m+1}}{a_{1,m+1}} a_{1j}) u_j$. Сумма ровно до m т.к. коэф. при $j = m+1$ равен 0(мы так выбрали коэффициент).

Их $n-1$, по условию $n > m+1$, т.е. $n - 1 > m$. По индукции $\widetilde{v_i}$ лин. зависимы, тогда и v_i-е. $0 = \sum b_i (v_i - \frac{a_{i,m+1}}{a_{1,m+1}} v_1) = \sum b_i' v_i$ - нетривиальная лин. комбинация. □

Lemma 1.2.

e_i - базис в $K^n \cong V$. Тогда $f(e_i)$ - базис в V, где f - изоморфизм.

Доказательство. $v = \sum a_i e_i \Rightarrow f(v) = \sum a_i f(e_i) \Rightarrow V = \langle f(e_i) \rangle$

$v = \sum a_i f(e_i) = \sum b_i f(e_i)$. f - инъекция, значит $\sum a_i e_i = \sum b_i e_i$. А т.к. e_i базис следует равенство $a_i = b_i$. □

Итого, для любого конечномерного V существует **единственное** n, т.ч. $V \cong K^n$. Т.к. $K^n \cong V \cong K^m \Rightarrow n = \dim V = m$.

2 Лекция 2. Базисные войны

Corollary. *Любую линейно независимую систему можно дополнить до базиса.*

Доказательство. Напоминание: v_i - базис $\iff$ v_i - макс. линейно независимая система.

Пусть $dimV = N$ и $V = \langle u_i \rangle$ - базис. А $v_1, \dots, v_k$ - лин. независимы.

Если набор максимальный, то это уже базис. Иначе добавим v_{k+1}, чтобы набор $v_1, \dots, v_{k+1}$ тоже был линейно независим.

Повторяем процесс. Он точно закончится, когда k станет N.

Более точно: если набрали $N+1$ вектор, каждый лежит в $\langle u_i \rangle$, но тогда он линейно зависимы(по предыдущей лемме). Значит $\exists s \ \ v_1, \dots, v_s$ - базис. По однозначности размера базиса $s = N$. □

Remark 2.1.

Пусть $v_1, \dots, v_k \in V$, $dimV = n$. Тогда

1. v_i - ЛНЗ $\Rightarrow k \leq n$
2. v_i - порождающие $\Rightarrow k \geq n$
3. Есть их n и они линейно независимы $\Rightarrow$ они базис
4. Их n и они порождающие $\Rightarrow$ они базис.

Lemma 2.1. Размерность подпространства

V - в.п. над K, U - подпространство. Тогда $dim(U) \leq dim(V)$. Если равна, то $U = V$

Доказательство. Выберем базис U — $u_i, i = 1 \dots k$. Это линейно независимая система. По лемме её можно дополнить до базиса V.

Значит $k \leq n$. Если $k = n$, то мы дополнили 0 векторов, значит $U = \langle u_i \rangle = V$ □

Example 2.1. Числа Фибоначчи

Рассмотрим S - фиб. последвательности над $\mathbb{R}$.
Мы обсуждали ранее, что в нем есть базис $s_1 = (1, 0, 1, 1, 2, 3, \dots)$ и $s_2 = (0, 1, 1, 1, 2, 3, \dots)$.
Рассмотрим $s_0 = (1, 1, 2, 3, \dots) \in S$. Хотим явную формулу для u_n - n-е число в s_0.
Рассмотрим другой базис. $f_1 = (1, \varphi, \varphi^2, \dots)$ и $f_2 = (1, (-\frac{1}{\varphi}), (-\frac{1}{\varphi})^2, \dots)$, где $\varphi, -\frac{1}{\varphi}$ - корни $x^2 - x - 1 = 0$.
$f_1, f_2 \in S$ исходя из уравнения. При этом f_1, f_2 очевидно линейно независимы(одна возрастает, друга убывает, значит не могут отличаться на константу). Значит это базис S.
$\exists a, b \, : s_0 = af_1 + bf_2$. Найдем коэф. из уравнений на u_1.

$$\begin{cases} a + b = 1 = u_1 \\ a\varphi - \frac{b}{\varphi} = 1 = u_2 \end{cases} \Rightarrow \text{находим } a, b$$

Example 2.2. Алгебраические числа

$\sqrt[5]{3}$ - корень уравнения $x^5 - 3 \in \mathbb{Z}[x]$.
Целые алгебраические числа - корни многочленов из $\mathbb{Z}[x]$.
Что они образуют? Является ли сумма целых алгебраических таковым?
Утв: Алгебраические числа образуют кольцо.

Lemma 2.2.

Если α - алгебраическое, $p \in \mathbb{Z}[x]$, то $p(\alpha)$ тоже алгебраическое.

Доказательство. Рассмотрим $\mathbb{C}$ как в.п. над $\mathbb{Q}$. Пусть $\alpha \in \mathbb{C}_{\mathbb{Q}}$, $q(\alpha) = 0$, $q \in \mathbb{Q}[x]$ и $deg(q) = n$
Рассмотрим $V \leq \mathbb{C}_{\mathbb{Q}}$, $V = \langle 1, \alpha, \alpha^2, \dots, \alpha^{n-1} \rangle_{\mathbb{Q}}$.
Утв.: $\forall N \in \mathbb{N} : \alpha^N \in V$.

Доказательство. Степени $\leq n-1$ по определению там. $q(\alpha) = \sum_{i=0}^{n} b_i \alpha^i = 0$. Значит $\alpha^n = -\sum_{i=0}^{n-1} \frac{b_i}{b_n} \alpha^i \in V (b_n \neq 0$ из-за степени).
Далее $\alpha^{n+1} = \alpha * \alpha^n = -\sum \frac{b_i}{b_n} \alpha^{i+1} \in V$ так как $i + 1 \leq n$ и все они уже лежат.
И так далее. □

Мы поняли, что если мы возьмем $\langle 1, \alpha, \alpha^2, \dots \rangle = V$.
Пусть $p \in \mathbb{Q}[x]$. Рассмотрим $1, p(\alpha), p(\alpha)^2, \dots, p(\alpha)^n \in V$, $dim(V) = n$. Их $n+1$, значит они линейно зависимы над $\mathbb{Q}$, то есть $\exists c_i \in \mathbb{Q}$ т.ч. $\sum c_i p(\alpha)^i = 0$.
Значит $p(\alpha)$ - корень $\sum c_i x^i \in \mathbb{Q}[x]$.

□

Remark 2.2.

Если является корнем многочлена из $\mathbb{Q}[x]$, то и многочлена из $\mathbb{Z}[x]$.(умножим на общий знаменатель коэффициенты)

2.1 Матрицы

Reminder. *Каждому вектору $v \in V$ соответствует* $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$ *- координаты в базисе v_i.*

Координаты зависят от базиса.

Рассмотрим K^n. Пусть зафиксированы $v_1, \dots, v_m \in K^n$, их компоненты $v_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix}$

Пусть $b \in K^n$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$ Что значит, что $b \in \langle v_i \rangle$?

$\sum x_i v_i = b$. Приравняем все координаты. Получим систему n линейных уравнений и m неизвестных.

$$\begin{cases} \sum a_{1j}x_j = b_1 \\ \vdots \\ \sum a_{nj}x_j = b_n \end{cases}$$

То есть $b \in \langle v_i \rangle \iff$ система имеет решение.

Definition 2.1. Матрица

Пусть R - кольцо. Матрица над R это отображение

$$I \times J \to R$$

где I, J индексирующие множества.

У нас обычно R - поле, I, J - конечные и $I = \{1, 2, \ldots, n\}$ и $J = \{1, 2, \ldots, m\}$

Множество таких матриц будем обозначать $M_{n,m}(R)$ - матрицы размера n на m.

$R = K$ - поле. Зададим на $M_{n,m}(K)$ структуру в.п. покомпонентно.

$$(a_{ij})_{ij} + (b_{ij})_{ij} = (a_{ij} + b_{ij})_{ij}$$
$$k * (a_{ij})_{ij} = (k * a_{ij})_{ij}$$

Получили (очев) в.п. над K.

Частный случай $m = 1$. Тогда возникает канонический изоморфизм $M_{n,1}(K) \cong K^n$, а если $n = 1$, то $M_{1,m} \cong {}^mK$ - строки длины m.

$dimM_{n,m}(K) = m * n$. Базис e_{ij} - матрица с 1 на пересечении i-й строки и j-го столбца и 0 иначе(матричные единички).

Зададим операции:

1. Можем задать операцию ${}^nK \times K^n \to K$: $(x_1, \ldots, x_n) * \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = \sum x_i y_i$
2. $M_{m,n}(K) \times K^n \to K^m$.

   $A \in M_{m,n}(K)$. Представим её как $A = \begin{pmatrix} r_1 \\ \vdots \\ r_m \end{pmatrix}$, где r_i - строки длины n. $B \in K^n$

   Тогда зададим $A \cdot b = \begin{pmatrix} r_1 * b \\ \vdots \\ r_m * b \end{pmatrix}$ (внутри произведение из предыдущего пункта)

   Поэтому СЛУ записывается как $Ax = B$, где A - матрица коэф., x - столбец x_i, а b - столбец правой части системы.
3. $M_{m,n}(K) \times M_{n,k}(K) \to M_{m,k}(K)$

   $$A \cdot C = A \cdot (c_1|c_2|\ldots|c_k) = (A \cdot c_1|\ldots|A \cdot c_k)$$

   где c_i - столбцы матрицы C длины n.

   Другими словами: формула свертки $(a_{ij}) \cdot (b_{ij}) = (c_{ij})$, где $c_{ij} = \sum_{l=1}^n a_{il} * b_{lj}$.

Свойства операций:

1 $A(X+Y)=AX+AY$
2 $A(kX)=kAX$, где $k\in K$

Это следует из дистрибутивности в поле.

3 Ассоциативность $A(BC)=(AB)C$, если все произведения существуют: то есть $A\in M_{k,l}$, $B\in M_{l,m}$, $C\in M_{m,n}$

Доказательство. Если верим в свойства 1-2, то достаточно проверять ассоциативность на базисе:
$(e_{ij}*\hat{e}_{kl})\tilde{e}_{mn}=e_{ij}(\hat{e}_{kl}*\tilde{e}_{mn})$ где e-шки матричные единицы из соответствующих пространств. Равенство левых и правых частей проверяется прямым вычислением. □

Частный случай $m=n=k$. Тогда $M_n(K)$ - кольцо квадратных матриц. Кольцо так как можем умножать. Нулевая матрица - матрица из нулей. $-A=(-a_{ij})$. Единица E - 1 на диагонали и 0 вне.

При этом $M_n(K)$ - не коммутативное кольцо.(при $n>1$ почти никакие две не коммутируют $(n=1\Rightarrow M_1(K)=K)$).

Definition 2.2. Однородная система уравнений

$Ax=0$ - однородная система уравнений.

Очевидное свойство - столбец из 0 всегда решение(тривиальное).

Существует нетривиальное решение $\iff$ $\exists x_i$ не все 0, т.ч. $Ax=0$, то есть

$$(c_1|\dots|c_m)\begin{pmatrix}x_1\\ \vdots\\ x_m\end{pmatrix}=\begin{pmatrix}0\\ \vdots\\ 0\end{pmatrix}$$

То есть есть нетривиальное решение $\sum x_ic_i=0$ $\iff$ столбцы линейно зависимы.

ЛЗЛК говорит, что если $m>n$, $c_1,\dots c_m\in K^n$, то c_i - лин.зависимы.

Другими словами: если $m>n$(переменных больше, чем уравнений), то однородная система имеет нетривиальное решение.

Lemma 2.3.

Множество решений $Ax=0$ - векторное пространство(подпространство в K^m).

Доказательство. $Ax=0,\ Ay=0\Rightarrow A(x+y)=0$ и $A(kx)=kA(x)=0$ □

2.2 Линейные отображения

Definition 2.3. Линейное отображение

Если U, V - в.п. над K.

$$\varphi : U \to V$$

называется линейным отображением(или гомоморфизмом) если

$$\varphi(u_1 + u_2) = \varphi(u_1) + \varphi(u_2)$$
$$\varphi(ku) = k\varphi(u)$$

Example 2.3.

Пусть $A \in M_{m,n}(K)$. Она задает $\mathcal{A} : K^n \to K^m$, т.ч. $\mathcal{A}(X) = A \cdot X$
Частный случай, когда $m = 1$.
Отображение $\mathcal{A} : V_K \to K$ - линейный функционал.
Если $V_K = K^n$. $A = (a_1, \dots, a_n)$. То $\mathcal{A} : K^n \to K$ т.ч. $\begin{pmatrix} x_1 \\ \dots \\ x_n \end{pmatrix} \mapsto \sum a_i x_i$

Любое линейное отображение из K^l в K^n это умножение на матрицу

Example 2.4.

$\mathcal{A} : Vect_2 \to Vect_2$.
$\mathcal{A} = r_\alpha$ - поворот вокруг 0 на α или $\mathcal{A} = S_e$ - сим. относительно прямой e(проходящая через 0).

Lemma 2.4. Простейшие свойства

1. $\mathcal{A}(0) = 0$ $(\mathcal{A}(0) = \mathcal{A}(0 + 0) = \mathcal{A}(0) + \mathcal{A}(0))$
2. Если v_i - линейно зависимы $\Rightarrow \mathcal{A}(v_i)$ тоже.
   $\sum a_i v_i = 0 \Rightarrow A(0) = 0 = A(\sum a_i v_i) = \sum a_i A(v_i)$.
   При этом линейная независимость не обязательно сохраняется(можем взять отображение, все отправляющее в 0).

Definition 2.4. Ядро и образ

Пусть $\mathcal{A} : V_1 \to V_2$ — линейное отображение.
$Ker(\mathcal{A}) = \{v \in V_1 \mid \mathcal{A}(v) = 0\} \subset V_1$ - ядро
$Im(\mathcal{A}) = \{v \in V_2 \mid v = \mathcal{A}(u)$ для некоторого u из $V_1\} \subset V_2$ - образ.

Lemma 2.5. Свойства ядра и образа

1. $Ker(\mathcal{A}), Im(\mathcal{A})$ - подпространства
2. $Im(\mathcal{A}) = V_2 \iff \mathcal{A}$ - сюръективно
   $Ker(\mathcal{A}) = \{0\} \iff \mathcal{A}$ - инъективно

Доказательство. 1) $x, y \in Ker(\mathcal{A})$. По линейности $\mathcal{A}(x+y) = \mathcal{A}(x) + \mathcal{A}(y) = 0$ и $\mathcal{A}(kx) = k\mathcal{A}(x) = 0$.

$x, y \in Im(\mathcal{A})$. Значит $x = \mathcal{A}(u), y = \mathcal{A}(v)$. По линейности $x + y = \mathcal{A}(u+v) \Rightarrow x + y \in Im(\mathcal{A})$ и аналогично kx.

2) Про образ очевидно по определению.

Пусть $\mathcal{A}$ - инъективно и $\mathcal{A}(x) = 0$. Мы знаем, что $\mathcal{A}(0) = 0$. Но тогда по инъективности $x = 0$.

Обратно: пусть ядро тривиально и $\mathcal{A}(x) = \mathcal{A}(y) \Rightarrow \mathcal{A}(x-y) = 0 \Rightarrow x - y = 0$. □

Lemma 2.6.

Пусть V_1, V_2 - в.п. над K и в первом пространстве зафиксировали базис v_i. А в V_2 зафиксировали столько же случайных векторов v_i'.
Тогда существует единственное линейное отображение $\mathcal{A} : V_1 \to V_2$ т.ч. $\mathcal{A}(v_i) = v_i'$.

Доказательство. *Существование*: $\forall v \in V_1\ \exists! a_i \in K$ такие что $\sum a_i v_i = v$. Положим $\mathcal{A}(v) = \sum a_i v_i'$.
В частности $\mathcal{A}(v_i) = \mathcal{A}(0 * v_1 + \dots + 1 * v_i + \dots + 0 * v_n) = v_i'$.

Если $v = \sum a_i v_i$, а $u = \sum b_i v_i$, то $v + u = \sum (a_i + b_i) v_i$ и $\mathcal{A}(v+u) = \sum (a_i + b_i) v_i' = \mathcal{A}(v) + \mathcal{A}(u)$.

Аналогично при kv.

Единственность: Пусть $\mathcal{A}$ - линейно и $\mathcal{A}(v_i) = v_i'$.

Тогда $\mathcal{A}(v) = \mathcal{A}(\sum a_i v_i) \underset{\text{линейность}}{=} \sum a_i \mathcal{A}(v_i) = \sum a_i v_i'$ - та же формула. □

Example 2.5.

1. Пусть $\mathcal{A} : \mathbb{R}^2 \to \mathbb{R}^2$ т.ч. $\mathcal{A}(x) = 0\ \forall x$. Тогда $Ker(\mathcal{A}) = \mathbb{R}^2$ и $Im(\mathcal{A}) = \{0\}$.
2. Пусть $\mathcal{A} : \mathbb{R}^2 \to \mathbb{R}^2$ т.ч. $\mathcal{A}$ - поворот. Тогда $Ker(\mathcal{A}) = \{0\}$ и $Im(\mathcal{A}) = \mathbb{R}^2$.
3. Пусть $\mathcal{A}$ - проекция на Ox. Тогда $Im(\mathcal{A})$ - ось Ox, а $Ker(\mathcal{A})$ - ось Oy.

Theorem 2.1. Теорема о размерности ядра и образа

Пусть $\mathcal{A} : V_1 \to V_2$ - лин. отображение. Тогда
1. $\exists$ базис $v_1, \dots, v_n$ пространства V_1 т.ч. $v_1, \dots, v_k$ это базис $Ker(\mathcal{A})$ и $\mathcal{A}(v_{k+1}), \dots, \mathcal{A}(v_n)$ - базис V_2.
2. $dimKer(\mathcal{A}) + dimIm(\mathcal{A}) = dim(V_1)$

Доказательство. $1 \Rightarrow 2$. В условиях пункта 1. $dimKer\mathcal{A} = k$, $dimIm\mathcal{A} = n - k$.

$k + n - k = n = dim(V_1)$

1. Выберем базис $Ker(\mathcal{A})$: $v_1, \dots, v_k$. И дополним до базиса всего пространства.

Докажем, что $\mathcal{A}(v_{k+1}), \dots \mathcal{A}(v_n)$ - базис образа.

Они линейно независимы. Пусть $\sum_{i=1}^{n-k} a_{k+i} \mathcal{A}(v_{k+i}) = 0 \Rightarrow \sum_{i=1}^{n-k} a_{k+i} v_{k+i} \in Ker(\mathcal{A}) \Rightarrow \sum_{i=1}^{n-k} a_{k+i} v_{k+i} = \sum_{i=1}^{k} (-a_i) v_i \Rightarrow \sum_{i=1}^{n} a_i v_i = 0$. А раз v_i базис, то все $a_i = 0$.

Ещё надо проверить, что $\mathcal{A}(v_{k+1}), \dots, \mathcal{A}(v_n)$ порождают $Im\mathcal{A}$.

Пусть $u \in Im(\mathcal{A})$. Значит $u = \mathcal{A}(v)$. $v = \sum a_i v_i$.

$$\mathcal{A}(v) = \mathcal{A}(\sum_{i=1}^{k} a_i v_i + \sum_{i=1}^{n-k} a_{k+1} v_{k+1}) = \sum_{i=1}^{n-k} a_{k+i} \mathcal{A}(v_{k+i})$$

так как первые v_i лежат в ядре. $\square$

2.3 Операции над подпространствами

V - в.п. над K. $\mathcal{V} = \{U \leq V\}$ - множество подпространств V.
На 2^V есть $\cup$ и $\cap$, а на $\mathcal{V}$?

Lemma 2.7. Пересечение подпространств

$V_1, V_2 \leq V \Rightarrow V_1 \cap V_2$ тоже (док-во - очев)

Remark 2.3.

Объединение как правило не подпространство.
Пример - 2 прямые на плоскости. Их объединение не содержит суммы векторов.

Definition 2.5. Сумма подпространств

V_1, V_2 - подпространства V.
$V_1 + V_2 = \{v_1 + v_2 \,|v_1 \in V_1,\ v_2 \in V_2\}$ - сумма подпространств.
И это тоже подпространство!

Доказательство.

$$(x_1 + y_1) + (x_2 + y_2) = (x_1 + x_2) + (y_1 + y_2) \in V_1 + V_2$$

Для $k(x_1 + y_1)$ аналогично. $\square$

Definition 2.6. Прямая сумма

Пусть V_1, V_2 какие-то в.п. над K. Тогда определим $V_1 \oplus V_2 = \{(v_1, v_2)|v_1 \in V_1, v_2 \in V_2\}$ с покоординатными операциями.

Remark 2.4.

v_i - базис V, u_i - базис U. Тогда $(v_i, 0), (0, u_i)$ - базис $V \oplus U$.
Поэтому $dim(V \oplus U) = dim(V) + dim(U)$

Lemma 2.8. Формула Грассмана

V - в.п. над K. $V_1, V_2 \leq V$, тогда $dim(V_1 + V_2) = dim(V_1) + dim(V_2) - dim(V_1 \cap V_2)$.

3 Лекция 3. Ранги. Битва образа с ядром

Доказательство. Рассмотрим очевидно линейное отображение $\mathcal{A} : V_1 \oplus V_2 \to V$. $\mathcal{A}((v_1, v_2)) = v_1 + v_2$. $\mathcal{A}$.
Применим теорему о размерности ядра и образа.

$$dimKer(\mathcal{A}) + dimIm(\mathcal{A}) = dim(V_1 \oplus V_2) = dim(V_1) + dim(V_2)$$

При этом по определению $Im(\mathcal{A}) = V_1 + V_2$, то есть $dimIm(\mathcal{A}) = dim(V_1 + V_2)$.

Осталось доказать, что $dimKer(\mathcal{A}) = dim(V_1 \cap V_2)$.

$$Ker(\mathcal{A}) = \{(v_1, v_2) \in V_1 \times V_2 \,|v_1 + v_2 = 0\} = \{(v, -v) \in V_1 \times V_2\}$$

Последнее значит, что $v \in V_1, -v \in V_2 \iff v \in V_1 \cap V_2$.

Следовательно существует изоморфизм $f : V_1 \cap V_2 \to Ker(\mathcal{A})$, т.ч. $f(v) = (v, -v)$. Это биекция по предыдущей строчке и очевидно линейное отображение.

Итого $dim(V_1 \cap V_2) + dim(V_1 + V_2) = dim(V_1) + dim(V_2)$ □

Рассмотрим следующую ситуацию: $U = K^n, V = K^m, \mathcal{A} : U \to V$: $\mathcal{A}(x) = Ax$, $A \in M_{m,n}(K)$.

Что такое ядро и образ?

$$Ker(\mathcal{A}) = \{x \,:\, Ax = 0\} - \text{множество решений однородной системы с матрицей } A$$

А образ? Образ это такие $b \in K^n$, что $Ax = b$ имеет решение.

Выберем стандартный базис в K^n. Запишем матрицу столбцами столбцы $A = (c_1| \ldots |c_n)$. $A(e_i) = c_i$. Другими словами

$$Im(\mathcal{A}) = \langle A(e_i) \rangle = \langle c_i \rangle - \text{ линейная оболочка столбцов}$$

Definition 3.1. Столбцовый ранг

$dimIm(\mathcal{A}) = dim\langle c_i \rangle = rg(A)$ - столбцовый ранг матрицы A(максимальное количество линейно независимых столбцов матрицы).
$dimKer(\mathcal{A}) = n - rg(A)$ - дефект матрицы.

У нулевой матрицы ранг 0, а у единичной n.

Пусть $A \in M_{m,n}(K)$. Это система линейных уравнений с m уравнениями и n неизвестными.

$\mathcal{A} : K^n \to K^m$. И знаем, что $dimKer(\mathcal{A}) = n - dimIm(\mathcal{A}) \geq n - m$, т.к. образ не более чем m-мерный(если $n \geq m$).

То есть пространство решений однородной линейной системы с m уравнениями и n неизвестными хотя бы $n - m$ мерно(если $n \geq m$).

Theorem 3.1. Дирихле для к-м пространств

Пусть $\mathcal{A} : U \to U$ - линейное, U - конечномерное.
Тогда $\mathcal{A}$ — инъективно $\iff$ $\mathcal{A}$ — сюръективно.

Доказательство. $\mathcal{A}$ - инъективно $\iff$ $Ker(\mathcal{A}) = 0 \iff dimIm(\mathcal{A}) = n \iff \mathcal{A}$ - сюръективно. □

Proposition 3.1.

Пусть есть система линейных уравнений, n уравнений и неизвестных с матрицей A и произвольной правой частью.

1. Если о.с.л.у. $Ax = 0$ имеет единственное решение, то при любом b, $Ax = b$ тоже имеет единственное решение.
   Т.к. иъънекция $\Rightarrow$ сюръекция $\Rightarrow$ биекция, то есть $\forall b$ $\exists!$ прообраз относительно A
2. Если $Ax = 0$ имеет не единственное решение. Тогда $\forall b$, $Ax = b$ имеет либо 0, либо много($\geq |K|$) решений.
   Т.к. $dimKer(\mathcal{A}) > 0 \Rightarrow dimIm(\mathcal{A}) < n$, значит $\exists b \notin Im(\mathcal{A})$ - для них нет решений.
   Пусть $b \in Im(\mathcal{A})$. То есть $\exists x_0 \ : Ax_0 = b$. Тогда $Ax = b \iff A(x - x_0) = 0 \Rightarrow x - x_0 \in Ker(\mathcal{A}) \Rightarrow x = x_0 + Ker(\mathcal{A})$ - сдвинутое подпространство решений не нулевой размерности.

Example 3.1.

$\mathcal{A} : \mathbb{R}^2 \to \mathbb{R}^2$
Пусть $dimKer(\mathcal{A}) = 1 \Rightarrow dimIm(\mathcal{A}) = 1$. Ядро - какая-то прямая, проходящая через 0. Возьмем произвольный вектор v, проведем прямую $v + Ker(\mathcal{A})$ - это все пробразы $A(v)$. В итоге вся плоскость поделится на прямые.

3.1 Матрица линейного отображения.

Пусть $\mathcal{A} : U \to V$ - линейное. Зафиксируем базисы $\{u_i\}_{i=1}^n, \{v_j\}_{j=1}^m$.
Знаем, что задать $\mathcal{A}$ это то же самое, что и задать $\mathcal{A}(u_1), \dots \mathcal{A}(u_n) \in V$.

Запишем $\forall i$: $\mathcal{A}(u_i) = \sum_{j=1}^m a_{ji}v_j$. Другими словами $\begin{pmatrix} a_{1i} \\ \vdots \\ a_{mi} \end{pmatrix}$ - координаты $\mathcal{A}(u_i)$ в базисе v_i.

Тогда $(a_{ij}) = (\mathcal{A}(u_1)_{\{v_i\}} | \dots | \mathcal{A}(u_n)_{\{v_i\}})$ называется **матрицей линейного отображения** $\mathcal{A}$ в базисах $\{u_i\}, \{v_i\}$.
Обозначим $A = [\mathcal{A}]_{\{u_i\},\{v_i\}}$

Lemma 3.1.

В обозначениях выше:
Пусть $u \in U$, $x_u \in K^n$ - координаты u в базисе $u_1, \dots, u_n$. Тогда, $A \cdot x_u \in K^m$ - координаты $\mathcal{A}(u)$ в базисе $v_1, \dots, v_m$.

Доказательство. Пусть $x_u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. То есть $u = \sum x_i u_i$.

Тогда $\mathcal{A}(u) = \mathcal{A}(\sum x_i u_i) = \sum x_i \mathcal{A}(u_i) = \sum_{i=1}^n x_i (\sum_{j=1}^m a_{ji} v_j) = \sum_{j=1}^m v_j (\sum_{i=1}^n a_{ji} x_i)$. Итого, получили, что $\mathcal{A}(u) = \begin{pmatrix} \sum_i a_{1i} x_i \\ \vdots \\ \sum_i a_{mi} x_i \end{pmatrix}$ - ровно умножение матрицы A на столбец x_u. $\square$

Remark 3.1.

U, V - в.п. над K. $u_1, \ldots, u_n$, $v_1, \ldots, v_m$ - базисы.
$A \in M_{m,n}(K)$. Тогда отображение $x_u \mapsto Ax_u$, где x_u - координаты $u \in U$ задает линейное отображение $\mathcal{A} : U \to V$.

Definition 3.2. Пространство линейных отображений

U, V - в.п. над K. Обозначим $Lin(U, V)$ - множество линейных отображений из U в V.
Зададим $(f+g)(u) \stackrel{\text{def}}{=} f(u) + g(u)$ и $(k \cdot f)(u) \stackrel{\text{def}}{=} k * f(u)$.
Очевидно, что сумма линейных - линейна и линейное, умноженное на скаляр, тоже!
То есть $Lin(U, V)$ - векторное пространство над K.

Theorem 3.2. Изоморфизм матриц и линейных отображений

В предыдущих обозначениях

$$C : Lin(U, V) \to M_{m,n}(K)$$

т.ч. $\mathcal{A} \mapsto [A]_{u_i, v_i}$ является изоморфизмом векторных пространств.

Итак, $Lin(U, V) \cong M_{m,n}(K)$. В частности $dimLin(U, V) = mn$. (изоморфизм зависит от выбора базиса и каждый выбор дает новый изоморфизм)

Remark 3.2.

Композиция линейных отображений тоже линейна!

Lemma 3.2.

Пусть $U \underset{\mathcal{A}}{\to} V \underset{\mathcal{B}}{\to} W$ — U, V, W - в.п. над K, $\mathcal{A}, \mathcal{B}$ - линейные. И в каждом выбран базис(размеры n, m, k соответственно).
$[\mathcal{A}]_{u_i, v_i} \in M_{m,n}(K)$, $[\mathcal{B}]_{v_i, w_i} \in M_{k,m}(K)$, $[\mathcal{B} \circ \mathcal{A}]_{u_i, w_i} \in M_{k,n}(K)$.
Тогда $[\mathcal{B} \circ \mathcal{A}] = [\mathcal{B}] \cdot [\mathcal{A}]$.

Доказательство. Пусть $[\mathcal{A}] = A, [\mathcal{B}] = B$. $u \in U$, $x_u \in K^n$ - координаты u в выбранном базисе. Тогда Ax_u - координаты $\mathcal{A}(u)$ в базисе v_i.

Значит $B(A(x_u))$ - координаты $\mathcal{B}(\mathcal{A}(u))$ в базисе w_i. Мы знаем ассоциативность умножения матриц. $B(A(x_u)) = (BA)(x_u)$.

Итого матрица BA переводит координаты x по базису u_i в координаты $\mathcal{B}(\mathcal{A}(x))$ по базису w_i. Что и значит, что BA - матрица $\mathcal{B} \circ \mathcal{A}$ в соответствующих базисах. $\square$

Definition 3.3. Кольцо линейных операторов

Пусть $U = V$. $Lin(V, V) = End(V)$ - кольцо эндоморфизмов(гомоморфизм в себя) V или линейных операторов(отображений в себя) на V.
При этом выбираем один базис $v_1, \dots, v_n$. И сопоставляем $\mathcal{A} \to [A]_{v_i, v_i}$(один базис нужен для корректного определения композиции).
Тогда

1. $End(V)$ - кольцо относительно сложения и композиции
2. $End(V) \cong M_n(K)$, где $n = dim(V)$.

Доказательство. Знаем, что $End(V) \cong M_n(K)$ как в.п(теорема выше). В частности сложение переходит в сложение.

А из прошлого утверждения композиция соответствует умножению матриц. Значит сохраняется и сложение и композиция. Если C - изомофризм из теоремы, то

$C(\mathcal{A} + \mathcal{B}) = C(\mathcal{A}) + C(\mathcal{B})$ и $C(\mathcal{A} \cdot \mathcal{B}) = C(\mathcal{A}) \cdot C(\mathcal{B})$.

И $C(Id) = E_n$. Потому что $[Id]_{u_i, u_i} = E$, т.к. $Id(u_i) = u_i = 0u_1 + \dots + 1 * u_i + \dots 0 * u_n$. ☐

Definition 3.4. Полная линейная группа

$End(V) \cong M_n(K)$. Рассмотрим группу биективных операторов $GL(V) \overset{\text{def}}{=} End(V)^* \cong M_n(K)^* \overset{\text{def}}{=} Gl(n, K)$ - группа обратимых матриц(полная линейная группа).

Example 3.2.

Пусть $n = 2$. $\mathcal{A} : \begin{pmatrix} 1 \\ 0 \end{pmatrix} \mapsto \begin{pmatrix} a \\ c \end{pmatrix}$ и $\begin{pmatrix} 0 \\ 1 \end{pmatrix} \mapsto \begin{pmatrix} b \\ d \end{pmatrix}$

$\mathcal{A}$ - изоморфизм $\iff dim\langle \begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix} \rangle = 2 \iff ad \neq bc$.

То есть матрица $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in Gl(2, K) \iff ad - bc \neq 0$

Example 3.3. Комплексные числа

Пусть $K = \mathbb{R}$. Рассмотрим $\begin{pmatrix} a & b \\ -b & a \end{pmatrix}$ - обратима, если $a^2 + b^2 \neq 0 \iff a \neq 0 \vee b \neq 0$. То есть они все в $Gl(2, K)$.

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} + \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} a+c & b+d \\ -(b+d) & a+c \end{pmatrix}$$

$$\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \cdot \begin{pmatrix} c & d \\ -d & c \end{pmatrix} = \begin{pmatrix} ac-bd & ad+bc \\ -(bc+ad) & ac-bd \end{pmatrix}$$

Умножение как у комплексных чисел. Значит мы нашли в $Gl(2, \mathbb{R})$ копию комплексных чисел.

$$\{\begin{pmatrix} a & b \\ -b & a \end{pmatrix} \mid a, b \in \mathbb{R}\} \cong \mathbb{C}$$

3.2 Матрица перехода.

Definition 3.5. Матрица перехода

Пусть V - в.п. над K. u_i - базис V. v_i - другой базис V. Матрицей перехода от базиса u_i к базису v_i называется $[Id]_{u_i,v_i}$.
Другими словами $u_j = \sum_i a_{ij} v_i$. Тогда $C = (a_{ij})$ - матрица перехода(обозначаем $C_{u_i \to v_i}$).
То есть столбцы матрицы перехода это старый базис, разложенный по новому.

Знаем: $u \in U$. $x_u = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$ - координаты в базисе u_i.

Координаты $Id(u) = u$ в базисе v_i - это $Cx_u = \begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix}$

То есть формула замены координат при изменении базиса: $\begin{pmatrix} x'_1 \\ \vdots \\ x'_n \end{pmatrix} = C \cdot \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, где C - матрица перехода.

Свойства матрицы перехода:

1. $C_{u_i \to u_i} = E_n$
2. Пусть есть 3 базиса u_i, v_i, w_i. Тогда $C_{v_i \to w_i} \cdot C_{u_i \to v_i} = C_{u_i \to w_i}$.
3. Обозначим $C_{u_i \to v_i} = C$, тогда $C_{v_i \to u_i} = C^{-1}$.

Corollary. *Матрицы перехода* $= Gl_n(K)$.

Доказательство. По предыдущему пункту, если $C = C_{u_i \to v_i}$, то существует обратная, значит $C \in Gl_n(K)$.

Пусть $C \in Gl_n(K)$. Возьмем какой-то базис u_i. В качестве $(v_1, \dots, v_n) = (u_1, \dots, u_n) \cdot C$, то есть C - матрица перехода $C_{v_i \to u_i}$.

Осталось понять, что v_i - базис.

$(v_1, \dots, v_n) = (u_1, \dots, u_n) \cdot C \Rightarrow (v_1, \dots, v_n)C^{-1} = (u_1, \dots, u_n)$. То есть u_i - линейные комбинации v_i, значит v_i - порождающая система $\Rightarrow$ базис. $\square$

3.3 Матрица линейного отображения при замене базиса

Пусть U, V - в.п. над K. u_i - базис U, v_i - базис V и $\mathcal{A} : U \to V$ - линейное отображение, A - его матрица в базисах u_i, v_i.

Пусть u_i', v_i' другие базисы U, V соответственно.

Как устроена $[\mathcal{A}]_{u_i', v_i'} = A'$?

$$U_{u_i'} \underset{Id_u}{\to} U_{u_i} \underset{\mathcal{A}}{\to} V_{v_i} \underset{Id_v}{\to} V_{v_i'}$$

Тогда $A' = [Id_v \circ \mathcal{A} \circ Id_u] = [Id_v] \cdot A \cdot [Id_u] = D \cdot A \cdot C^{-1}$, где D- матрица перехода $v_i \to v_i'$, а C - матрица перехода $u_i \to u_i'$.

Частный случай $\mathcal{A} \in End(V)$. Есть базис v_i, A - матрица $\mathcal{A}$ в базисе v_i.

Тогда если v_i' - новый базис с матрицей перехода C, тогда $A' = C \cdot A \cdot C^{-1}$

Вопрос на будущее: Пусть есть $\mathcal{A}\, V \to V$. Как найти базис v_i, такой что матрица A была бы *попроще*?

Другая задача:

Дана A. Хотим к*ак можно более простую* CAC^{-1}.

$\mathcal{A} : U \to V$. Хотим базисы u_i, v_i, что A *была бы попроще...*

Theorem 3.3. Канонический вид линейного отображения

$\forall \mathcal{A} : U \to V$ существует базис u_i и базис v_i т.ч. матрица $\mathcal{A}$ является *полуединичной.*

То есть имеет вид $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$ - единичная матрица и все остальное нули. Где $r = rg\mathcal{A}$.

Доказательство. Мы знаем, что существует базис U, такой, что $u_1, \dots, u_k$ - базис ядра, а $\mathcal{A}(u_{k+1}), \dots, \mathcal{A}(u_n)$ - базис образа. Перенумеруем в обратном порядке. То есть $\mathcal{A}(w_1), \dots, \mathcal{A}(w_{n-k})$ - базис образа, а остальные базис ядра.

Дополним $\mathcal{A}(w_1), \dots, \mathcal{A}(w_{n-k})$ до базиса V(обозначим v_i). Получим искомую матрицу т.к. $\mathcal{A}(w_i) = v_i$, $i \leq n - k$, $\mathcal{A}(w_i) = 0$ иначе. $\square$

4 Лекция 4. Опасное приключение в перестановках столбцов

Proposition 4.1.

$A, \tilde{A} \in M_{m,n}(K)$. Они являются матрицами одного и того же отображения, записанные в разных базисах, если существует обратимые C, D, т.ч. $\tilde{A} = CAD$
Можно завести эквивалентность: $A \sim \tilde{A}$, если выполнено условие выше.

Мы доказали, что в каждом классе эквивалентности есть представитель вида $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$.

Remark 4.1.

Если $\begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix} \sim \begin{pmatrix} E_s & 0 \\ 0 & 0 \end{pmatrix} \Rightarrow s = r$.
Т.к. $s = r = dimIm$

Definition 4.1. Строчный ранг

$rk_r(A)$ - максимальное количество линейно независимых строк матрицы A.

Theorem 4.1. Равенство строчного и столбцового ранга

$rk(A) = rk_r(A)$(докажем позже)

Definition 4.2. Транспонирование

Пусть $A = (a_{ij}) \in M_{m,n}(K)$. Тогда транспонированная к A — $A^T = (b_{ij}) \in M_{n,m}(K)$, где $b_{ij} = a_{ji}$.

Remark 4.2.

$^T : M_{m,n}(K) \to M_{n,m}(K)$ т.ч. $(A+B)^T = A^T + B^T$ и $(kA)^T = kA^T$.
То есть транспонирование - изоморфизм в.п.

Remark 4.3.

Пусть $A \in M_{m,n}(K)$, $B \in M_{n,l}(K)$. Тогда $(AB)^T = B^T A^T$(очев проверяется прямым вычислением).

Lemma 4.1. Свойства ранга

1. $rk(A+B) \leq rk(A) + rk(B)$, где $A, B \in M_{m,n}$.
2. $rk(AB) \leq \min(rkA, rkB)$, где $A \in M_{m,n}$, $B \in M_{n,l}$
3. Пусть $A, B \in M_n(K)$ и $B \in GL_n(K)$(обратима). Тогда $rk(AB) = rk(BA) = rk(A)$.
4. $A \in M_n(K)$, то $rk(A) = rk(A^T) \iff rk(A) = rk_r(A)$.

Remark 4.4.

$AA^{-1} = E \Rightarrow (AA^{-1})^T = E^T = E \Rightarrow (A^{-1})^T A^T = E$.
То есть A^T - обратима $\iff$ A оборатима

Доказательство.

1. Пусть $u_1, \dots, u_n$ - столбцы A, $v_1, \dots, v_n$ - столбцы B, $u_i + v_i$ - столбцы $A + B$.
   Пусть $U = \langle u_i \rangle = \langle u_{i_1}, \dots, u_{i_k} \rangle$ и $V = \langle v_i \rangle = \langle v_{i_1}, \dots, v_{i_l} \rangle$.
   Тогда $u_i + v_i \in U + V = \langle u_{i_1}, \dots, v_{i_l} \rangle$.
   При этом $dim(U + V) \leq k + l$. Значит $rk(A + B) \leq k + l = rk(A) + rk(B)$.
2. Хотим доказать, что $dimIm(\mathcal{A} \circ \mathcal{B}) \leq min(dimIm(\mathcal{A}), dimIm(\mathcal{B}))$.
   Заметим, что $Im(\mathcal{A} \circ \mathcal{B}) = \{\mathcal{A}(\mathcal{B}(u))\} \subset \{A(v)\} = Im(\mathcal{A})$, значит $dimIm(\mathcal{A} \circ \mathcal{B}) \leq dimIm(\mathcal{A})$.
   $Im(\mathcal{A} \circ \mathcal{B}) = \{\mathcal{A}\mathcal{B}(u)\} = \{A(v)\, | v \in Im(\mathcal{B})\} = Im(\mathcal{A}_{|Im(\mathcal{B})})$(сужение на образ $\mathcal{B}$).
   $dimIm(\mathcal{A}_{|Im(\mathcal{B})}) = dimIm(\mathcal{B}) - Ker(\mathcal{A}_{|Im(\mathcal{B})}) \leq dimIm(\mathcal{B})$.
3. $B \in GL_n(K)$. $rk(AB) \leq rk(A)$ по п.2. Но $rk(A) = rk((AB)B^{-1}) \leq rk(AB)$. Аналогично с умножением на B слева.
4. $A \in M_n$. Мы знаем, что $\exists C, D$, что $CAD = \begin{pmatrix} E_r & 0 \\ 0 & 0 \end{pmatrix}$ и $C, D \in GL_n(K)$.

   По предыдущему пункту $rk(A) = rk(CAD) = r = rk((CAD)^T)$, т.к. матрица и её транспонированная равны.
   То есть $rk(A) = rk((CAD)^T) = rk(D^T A^T C^T) = rk(A^T)$ т.к. $D^T, C^T \in GL_n(K)$.

$\square$

Вопрос: есть группа $GL_n(K)$. Хотим для неё придумать какую-нибудь порождающую систему из простых матриц.

Definition 4.3. Трансвекция

Трансвекция $t_{ij}(a) \in M_n(K)$, где $i \neq j \in [1, \dots, n]$, $a \in K$ это матрица $E + ae_{ij}$(единички на диагонали, a в позиции i, j и 0 иначе).

Действует она так: $t_{ij}(a) \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_i + ax_j \\ \vdots \\ x_n \end{pmatrix}$ — прибавление j к i с коэф. a.

Это называется элементарное преобразование первого типа.

Remark. *Ясно, что $t_{ij}(a) \in GL_n(K)$, т.к. существует обратная : $t_{ij}(-a)$.*

Definition 4.4. Дилатация

Дилатация $i \in [1, \ldots, n]$, $a \in K^*$. Тогда $m_i(a) = E + (a-1)e_{ii}$(a на позиции ii, 1 на диагонали, иначе 0).

$m_i(a)\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ ax_i \\ \vdots \\ x_n \end{pmatrix}$ — умножение i на a.

Это - элементарное преобразование второго рода.

Remark. *Ясно, что* $m_i(a) \in GL_n(K)$, *т.к. существует обратная* : $m_i(a^{-1})$.

Definition 4.5. Транспозиция

Элементарное преобразование третьего рода: транспозиция (меняем местами i, j)

$$\begin{pmatrix} x_1 \\ \vdots \\ x_i \\ \vdots \\ x_j \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} x_1 \\ \vdots \\ x_j \\ \vdots \\ x_i \\ \vdots \\ x_n \end{pmatrix}$$

$s_{ij} = E - e_{ii} - e_{jj} + e_{ij} + e_{ji}$.

Remark 4.5.

Третий тип не нужен, так как он выражается через первые два.

$$\begin{pmatrix} a \\ b \end{pmatrix} \underset{t_{12}(1)}{\rightarrow} \begin{pmatrix} a+b \\ b \end{pmatrix} \underset{t_{21}(-1)}{\rightarrow} \begin{pmatrix} a+b \\ -a \end{pmatrix} \underset{t_{12}(1)}{\rightarrow} \begin{pmatrix} b \\ -a \end{pmatrix} \underset{m_2(-1)}{\rightarrow} \begin{pmatrix} b \\ a \end{pmatrix}$$

То есть $s_{ij} = m_2(-1)t_{ij}(1)t_{ji}(-1)t_{ij}(1)$

Действие $t_{ij}(a), m_i(a)$ **на матрицы**.

$t_{ij}(a) \cdot A$ - матрица, получающаяся из A, прибавлением j-й строки, умноженной на a к i-й.

$m_i(a) \cdot A$ - матрица, получающаяся из A, умножением i-й строки на a.

Что будет, если умножаем справа?

$A \cdot m_i(a) = ((A \cdot m_i(a))^T)^T = (m_i(a)A^T)^T$ - умножили i-й столбец на a.

$A \cdot t_{ij}(a)$ - матрица, полученная из A, прибавлением i-го столбца, умноженного на a к j-му(т.к. $t_{ij}(a)^T = t_{ji}(a)$).

s_{ij} меняет i и j строку, если умножаем слева и столбцы, если справа.

Все эти элементарные матрицы обратимы, значит умножение на них с любой стороны не меняет ранга(то есть и элементарные преобразования не меняют ранга).

Метод Гаусса в наших терминах берет A, делает какие-то элементарные преобразования и получает матрицу трапецевидного вида, которую можно привести к полуединичной.

Получили алгоритмическое определение ранга - количество ненулевых строк после алгоритма Гаусса.

Remark. *Для не квадратных матриц все в силе!*

Theorem 4.2.

1. Пусть $A \in M_{m,n}(K)$, тогда $\exists$ элементарные матрицы $e_1, \dots, e_k$, т.ч. $e_1 \dots e_k A$ имеет треугольный вид(под главной диагональю 0).
2. Пусть $A \in GL_n(K)$, тогда $\exists$ элементарные e_i, т.ч. $e_1 \dots e_n A = E$.
3. Пусть $A \in GL_n(K)$, тогда $\exists$ элементарные f_i, т.ч. $A = f_1 \dots f_l$.
4. Пусть $A \in M_{m,n}(K)$. Тогда $\exists$ элементарные $e_1, \dots, e_k \in GL_m,\ f_1, \dots, f_l \in GL_n$ т.ч. $e_1 \dots e_k A f_1 \dots f_l$ - полуединичная матрица

Example 4.1.

Рассмотрим $A = \begin{pmatrix} 1 & 2 & \dots & n \\ 0 & 0 & \dots & 0 \end{pmatrix}$ - никак не упростить преобразованиями над строками, а если добавить преобразования над столбцами, то получим 1 в 1 клетке и 0 иначе.

Доказательство. $2 \iff 3$. e_i - элем $\Rightarrow e_i^{-1}$ существует и тоже элем.
Если $e_1 \dots e_n A = E$. Домножим на $e_n^{-1} \dots e_1^{-1}$. Получим $A = e_n^{-1} \dots e_1^{-1} = f_1 \dots f_k$.
$2 \Rightarrow 4$. $\forall A\, \exists C, D \in GL$, т.ч. CAD - полуединичная, но $C = e_1 \dots e_k$ и $D = f_1 \dots f_m$.

Доказательство 1). Индукция по n. База $n = 1$. Матрица имеет вид $\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix}$. Либо все 0, тогда все хорошо. Иначе существует a_j не 0. Применим s_{1j}. В этом случае можем привести к виду $\begin{pmatrix} a_1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$ операциями $t_{i1}(-\frac{a_j}{a_1})$ - элементарные матрицы.

Переход: $n - 1 \to n$. Посмотрим на первый столбец $\begin{pmatrix} a_{11} \\ \vdots \\ a_{m1} \end{pmatrix}$. Делаем то же, что и в базе. Получим $\begin{pmatrix} x_1 \\ \vdots \\ 0 \end{pmatrix}$. По индукционному предположению оставшуюся часть матрицы($\tilde{A}$) сможем привести к треугольному виду.

2) Пусть A - обратима. По пункту 1 приведем к треугольному виду $\tilde{A}$. $\tilde{A}$ - обратима как произведение обратимых.

Lemma 4.2.

Если есть треугольная матрица, то она обратима $\iff \forall i\ a_i \neq 0$.

Доказательство. $\Rightarrow$ Пусть есть $a_i = 0$. $A = (c_1|\dots|c_n)$, то $c_1, \dots, c_i \in \langle e_{11}, \dots, e_{i-1,i-1}\rangle$. Значит они линейно зависимы, то есть и все столбцы линейно зависимы.

$rk(A) < n \Rightarrow n = rk(E) = rk(AA^{-1}) < n$ - противоречие. □

Итак, у нас $\tilde{A}$ треугольная и все a_i не 0. Применим $\prod m_i(\frac{1}{a_i})$. Получим треугольную с 1 на диагонали.

Делаем метод гаусса в обратную сторону. Сначала для последнего столбца занулим все кроме пoслнеднего. То есть применим $t_{in}(-a_{in})$. Это даст нам последний столбец - 1 на n-м месте и 0 иначе. И так далее. □

Theorem 4.3.

Следующие условия для $A \in M_n(K)$ равносильны:

1. $A \in GL_n(K)$
2. строки A линейно независимы
3. столбцы A линейно независимы
4. $rk(A) = n$
5. Любая система с матрицей A имеет единственное решение
6. A является матрицей отображения $\mathcal{A}$, где $\mathcal{A}$ - изоморфизм
7. $\exists$ элементарные преобразования, т.ч. $A \to$ треугольную с не нулями на диагонали.
8. $\forall$ элементарных преобразований, т.ч. они превращают A в треугольную все a_i не 0.

Доказательство. 2) $rk_r(A) = n$, 3) $rk(A) = n$, мы знаем $rk(A) = rk_r(A)$.

1) $\Rightarrow$ 4) т.ч. $AA^{-1} = E \Rightarrow n = rk(E) \leq rk(A) \leq n$.

4) $\Rightarrow$ 1) Существует $e_1 \dots e_m$, что $e_1 \dots e_m A$ - треугольная $\tilde{A}$. При e_i - обратимы, значит $rk(\tilde{A}) = n$. Из доказательства леммы все диагональные элементы не 0. Значит $\tilde{A}$ приводится к E - обратима, то есть и A - обратима. □

Remark 4.6. Алгоритм поиска обратной матрицы

Пусть $A \in M_n(K)$ и она обратима. То есть $\exists e_1, \dots, e_k : e_1 \dots e_k A = E$. Значит $A^{-1} = e_1 \dots e_k$.
Алгоритм: напишем матрицу $(A|E)$. Применяем расширенного(приводим к E) Гаусса к A. Будем применять элементарные преобразования к строкам $(A|E)$.
Таким образом получим $(e_1 \dots e_k A | e_1 \dots e_k)$.
Если слева стоит E, тогда справа стоит A^{-1}.

5 Лекция 5. Треуголки и подготовка к аду

5.1 Треугольные матрицы

Definition 5.1.

$A \in M_n(K)$. Называется верхнетреугольной ($A \in UT_n$), если $a_{ij} = 0$ при $i > j$.
Строго верхнетреугольной, если при $i \geq j$.
Унитреугольной, если A - верхнетреугольная и $a_{ii} = 1$.
Аналогично нижнетреугольная (LT_n), если $a_{ij} = 0$ при $i < j$ и так далее...

Remark. *Для нижнетреугольных тоже все верно,так как они транспонированные к верхнетреугольным...*

Lemma 5.1.

1. UT_n — подкольцо в $M_n(K)$
2. $A, B \in UT_n$. $A \cdot B$ имеет на диагонали произведения диагональных элементов A, B.
3. $A \in UT_n^* \iff \forall a_{ii} \neq 0$
4. $A \in UT_n$ нильпотентна($\exists n \ : \ A^n = 0$) $\iff$ A строго верхнетреугольная
5. $A \in UT_n \iff A(\langle e_1, \ldots, e_k \rangle) \subset \langle e_1, \ldots, e_k \rangle \, \forall k$.

Доказательство. 1) Замнкутость по сложению очев. $0, E$ очевидно верхнетреугольные.

Замкнутность относительно умножения. Пусть $(a_{ij}) = A$, $B = (b_{ij})$ - верхнетреугольные. $C = AB$.

Пусть $i > j$. Тогда $\forall k$ либо $i > k$ либо $k > j$, значит $a_{ik} = 0 \vee b_{kj} = 0$, поэтому

$$c_{ij} = \sum_k a_{ik} b_{kj} = 0$$

2) Если $i = j$, тогда $c_{ii} = \sum_k a_{ik} b_{ki} = a_{ii} b_{ii}$ т.к. если $k < i$, то $a_{ik} = 0$, или $k > i$ то $b_{ki} = 0$.

5) $a_{ij} = 0$ при $i > j$ то есть j-й столбец $\begin{pmatrix} c_1 \\ \ldots \\ c_j \\ 0 \\ \ldots \\ 0 \end{pmatrix}$

То есть $Ae_j \in \langle e_1, \ldots, e_j \rangle$.

Таким образом верхнетреугольные матрицы сохраняют цепочку вложенных друг в друга подпространств $\langle e_1 \rangle \subset \langle e_1, e_2 \rangle \subset \langle e_1, e_2, e_3 \rangle \ldots$

4) Пусть A не строго верхнетреугольная, то есть $\exists a_{ii} \neq 0$. По предыдущему пункту A^N имеет ненулевой элемент на диагонали, значит не нильпотентная.

Пусть строго верхнетреугольная. $A(e_k) \in \langle e_1, \ldots, e_{k-1} \rangle \; \forall k$.

Значит $A^2(e_k) \in \langle Ae_1, \ldots, Ae_{k-1} \rangle \subset\in \langle e_1, \ldots, e_{k-2} \rangle$

Так получим $A^k(e_k) = 0$.

Другими словами: $A^n = (b_{ij})$. $b_{ij} = \sum a_{i,i_1} a_{i_1,i_2} \ldots a_{i_{n-1},j}$. Каждое слагаемое не 0, если последовательность индексов $i, i_1, \ldots, i_{n-1}, j$ строго возрастающая. Но их $n + 1$. Значит все нули.

(при возведении в квадрат появится ещё одна нулевая диагональ, выше диагональной...)

Proposition 5.1.

Пусть A - верхнетреугольная с ненулевой диагональю. Рассмотрим $B = (b_{ij})$, где $b_{ii} = \frac{1}{a_{ii}}$.
A - обратима $\iff$ BA - обратима
BA - унитреугольная, то есть $BA = E + N$, где N - нильпотентна.
$E + N$ - обратима, т.к. если $N^k = 0$, то

$$(E+N)(E - N + N^2 - \dots \pm N^{k-1}) = E^K \pm N^k = E$$

□

Lemma 5.2. LU-разложение

Итак, UT_n, LT_n - подкольца. $UT_n \cap LT_n = D_n$ - диагональные ($D_n \cong K^n$ как кольцо)
Мы знаем, что если $A \in M_n(K)$, то существуют элементарные e_i, что $e_1 \dots e_k A$ - верхнетреугольная.
Обычно мы делали: $e_l = t_{ij}(a)$, где $i > j$. Иногда $e_l = s_{ij}$.
Предположим, что не было s_{ij}. Тогда все $e_i \in LT_n(K)$. Значит их произведение тоже.
То есть существует $C \in LT_n^*$ т.ч. $CA = B \in UT_n$. То есть $A = C^{-1}B$, где $B \in UT_n$, а $C^{-1} \in LT_n$.
Последнее верно, так как $C = e_k^{-1} \dots e_1^{-1}$ - тоже все нижнетреугольные.

Lemma 5.3.

Пусть $A \in GL_n(K)$. Рассмотрим $A_k = (a_{ij})_{i,j=1,\dots k}$(левый верхний угол размера k)
И пусть A т.ч. $A_1, \dots, A_n$ - обратимы, тогда в Гауссе можно использовать, только $t_{ij}(a)$, где $i > j$.

Доказательство. Рассмотрим $\langle r_1^k, \dots, r_k^k \rangle$ - пространство строк матрицы A_k.

Пока применяем t_{ij} с $i > j$ это пространство не меняется(если r_i заменяем на $r_i + ar_j$ то оболочка не меняется).

Индукция по k. A можно привести к верхнетреугольному виду, только с t_{ij}, где $i > j$.

База $a_{11} \neq 0$(т.к. A_1 - оборатима), значит можем получить нули в первом столбце под a_{11} ничего не переставляя.

Переход $k-1 \to k$. Пусть получили нолики под диагональю в первых $k-1$ столбцах. Надо, чтобы $a_{kk} \neq 0$. Но если она 0, тогда первые k строк A_k линейно зависимы — противоречие с обратимостью. Значит не 0, то есть сможем под ним получить нолики с помощью трансвекций. □

Lemma 5.4.

Пусть A - обратима. Тогда можно переставить строки так, что для новой матрицы $\tilde{A}$ будет выполнено условие прошлой леммы.

Доказательство. Индукция: можно переставить так, чтобы первые k были обратимы. База: $k = 1$.

A - обратима, значит первый столбец не нулевой($\exists\, a_{j1} \neq 0$). Тогда переставим первую строку с j-й.

Переход: $A_1, \dots, A_k$ - обратимы. Посмотрим на строки r_i первых $k+1$ столбцов.

B - матрица из первых $k+1$ столбцов.

$rkB = k+1$, иначе первые $k+1$ столбцов линейнозависимы(у матрицы A, а она обратима).

Значит $dim\langle r_1, \dots, r_n\rangle = k+1$. Значит, что $\exists l > k\ r_l \notin \langle r_1, \dots, r_k\rangle$. Тогда сделаем перестановку $s_{k+1,l}$.

Теперь они линейно независимы, значит A_{k+1} обратима. $\square$

Theorem 5.1.

Пусть $A \in GL_n(K)$. $s_1, \dots, s_k$ перестановки, т.ч. $\underbrace{s_1 \dots s_k}_{P} A$ удовлетворяет первой лемме.

Тогда PA приводится к верхнетреугольному виду нижнетреугольными преобразованиями. То есть $\exists L \in LT_n^*$, что $LPA = U \in UT_n$
Или $A = P^{-1}L^{-1}U$, где $U \in UT_n, L \in LT_n, P$ - матрица перестановки строк.

Remark. *Матрица перестановки* $P = (p_{ij})$, $\exists \pi \in S_n$, *т.ч.* $P_{i\pi(i)} = 1$ *и 0 иначе.*

5.2 Явные формулы линейной алгебры(определитель)

В чем смысл $ad - bc$ для матрицы $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$?

$ad - bc$ площадь параллелограмма, натянутого на $\begin{pmatrix} a \\ c \end{pmatrix}$ и $\begin{pmatrix} b \\ d \end{pmatrix}$

Аксиомы "площади"$(v_1, v_2) \to S(v_1, v_2)$

$$S(kv_1, v_2) = kS(v_1, v_2), k > 0 - \text{однородность по 1-му(2-му) аргументу}$$
$$S(v_1, v_1) = 0 - \text{кососимметричность}$$
$$S(v_1 + v_1', v_2) = S(v_1, v_2) + S(v_1', v_2) - \text{аддитивность по 1-му(2-му) аргументу}$$
$$S(e_1, e_2) = 1$$

Аддитивность + однородность = линейность.

Следствие из аксиом: $S(v_1 + kv_2, v_2) = S(v_1, v_2)$.

С помощью аксиом любой параллелограмм можем превратить в квадрат 1 на 1.

$S(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} b \\ d \end{pmatrix}) = S(\begin{pmatrix} a \\ c \end{pmatrix}, \begin{pmatrix} 0 \\ d - \frac{bc}{a} \end{pmatrix}) = a * (d - \frac{bc}{a})S(\begin{pmatrix} 1 \\ \frac{c}{a} \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix}) = (ad - bc)S(\begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix})$

Definition 5.2. Полилинейное отображение

$V_1, \dots, V_k$ - в.п. над K. Тогда $f : V_1 \times \dots \times V_k \to K$ называется полилинейным, если

$$\forall i\ f(v_1, \dots, v_i' + v_i'', \dots, v_k) = f(v_1, \dots, v_i', \dots, v_k) + f(v_1, \dots, v_i'', \dots, v_k)$$

И константа выносится.
То есть если зафиксировать все аргументы кроме одного, то будет линейная функция.

Example. *Билинейность:* $f(u' + ku'', v) = f(u', v) + kf(u'', v)$ *и* $f(u, v' + kv'') = f(u, v') + kf(u, v'')$

Definition 5.3.

Пусть f - полилинейное, тогда f называется кососиметричным, если $\forall i, j,\ v_1, \dots, v_n$ т.ч. если $v_i = v_j \Rightarrow f(v_1, \dots, v_n) = 0$.

Lemma 5.5.

Пусть f - кососимметрично, тогда

$$f(v_1, \dots, v_i, \dots, v_j, \dots, v_n) = -f(v_1, \dots, v_j, \dots, v_i, \dots, v_n)$$

Доказательство. Пусть $n = 2$ для удобства записи.

$$f(v_1 + v_2, v_1 + v_2) = 0 = f(v_1, v_1) + f(v_1, v_2) + f(v_2, v_1) + f(v_2, v_2) = f(v_1, v_2) + f(v_2, v_1) = 0$$

Обратное верно в поле характеристики не 2. □

Как задать полилинейное отображение?

Пусть теперь $V_i = K^n$, а $V = K$. То есть рассматриваем полилинейные отображения $(K^n)^n \cong M_n(K) \to K$

Theorem 5.2.

Пусть $f_1, f_2 : (K^n)^n \to K$ - полилинейные, кососимметричные и оба не тождественные нули.
Тогда $\exists c \in K^* \ :\ f_2 = cf_1$.

Доказательство. Рассмотрим $v_1, \dots, v_n \in K^n$ и зафиксируем базис $e_1, \dots, e_n$. $v_i = \sum a_{ij} e_j$.
Тогда $f(v_1, \dots, v_n) = \sum_{j_1, \dots, j_n} a_{1j_1} \dots a_{n,j_n} f_1(e_{j_1}, \dots, e_{j_n}) = \sum_{\{j_1, \dots, j_n\} = \{1, \dots, n\}} (\prod a_{i,j_i}) f(e_{j_1, \dots, j_n}) = \sum_{\{j_1, \dots, j_n\} = \{1, \dots, n\}} \pm (\prod_i a_{i,j_i}) f_1(e_1, \dots, e_n)$
Причем знак не зависит от f_1. Аналогично с f_2.

Ясно, что раз $f_1, f_2 \neq 0 \Rightarrow f_i(e_1, \dots, e_n) \neq 0$.

То есть $f_2(e_1, \dots, e_n) = cf_1(e_1, \dots, e_n)$ □

Definition 5.4. Определитель

Определителем называется полилинейное, кососимметричное отображение

$$det\ :\ (K^n)^n \to K$$

т.ч. $det(e_1, \dots, e_n) = 1$, где e_i - стандартный базис.

Мы доказали, что существует не более одной такой функции.

Definition 5.5. Знак перестановки

Пусть S_n - группа перестановок — биекций из $[1,\dots,n] \to [1,\dots,n]$.
Тогда существует единтсвенный гомоморфизм групп $\mathrm{sign}\ : S_n \to \{1,-1\}$ т.ч. $\mathrm{sign}(t) = -1$, где t - транспозиция($\exists i,j\ :\ t(i)=j, t(j)=i, t(k)=k$ иначе).

Доказательство позже.

Theorem 5.3.

Определитель существует $\forall n \in \mathbb{N}$

Доказательство. $v_1,\dots,v_n \to (a_{ij}) = A$. Определим $det(A) = \sum_{\pi \in S_n} \mathrm{sign}(\pi) a_{1,\pi(1)} \dots a_{n,\pi(n)}$
Проверим, что все хорошо.
$det(E) = \mathrm{sign}(Id)\prod_i a_{i,i} = 1$.

Полилинейность: $c_i = \begin{pmatrix} a_{1i} \\ \vdots \\ a_{ni} \end{pmatrix} = \begin{pmatrix} a'_{1i} \\ \vdots \\ a'_{ni} \end{pmatrix} + k \begin{pmatrix} a''_{1i} \\ \vdots \\ a''_{ni} \end{pmatrix}$

Тогда $\exists! l = \pi^{-1}(i)$

$$det(A) = \sum_{\pi \in S_n} \mathrm{sign}(\pi) a_{1,\pi(1)} \dots (a'_{li} + k a''_{li}) \dots a_{n,\pi(n)} = det(c_1,\dots,c'_i,\dots,c_n) + k det(c_1,\dots,c''_i,\dots,c_n)$$

□

6 Лекция 6. Рождение det-а

Definition 6.1. Аксиоматическое определение определителя

$det :\ M_n(K) \to K$ — полилинейное по столбцам, кососимметричное отображение, т.ч. $det(E) = 1$.

Lemma 6.1.

$det(A) = \sum_{\pi \in S_n} \mathrm{sign}(\pi) \prod_i a_{i,\pi(i)}$ удовлетворяет аксиомам.

Доказательство. Кососимметричность: $A = (c_1|\dots|c_n)$, $c_i = c_j \Rightarrow det(A) = 0$.
Имеем $\forall k = 1,\dots,n\ a_{k,i} = a_{k,j}$. Разобъём перестановки на пары:
Рассмотрим перестановку $\pi : a_{1,\pi(1)} \dots a_{\pi^{-1}(i),i} \dots a_{\pi^{-1}(j),j} \dots a_{n,\pi(n)}$ и
$\tilde{\pi}$: $a_{1,\pi(1)} \dots a_{\pi^{-1}(j),i} \dots a_{\pi^{-1}(i),j} \dots a_{n,\pi(n)}$. На самом деле $a_{\pi^{-1}(i),j} = a_{\pi^{-1}(i),i}$ и $a_{\pi^{-1}(j),i} = a_{\pi^{-1}(j),j}$.
То есть произведение в этих слагаемых равны, но знак разный.
Проверим, что $\mathrm{sign}(\pi) = -\mathrm{sign}(\tilde{\pi})$. Это верно, так как $\tilde{\pi} = (ij) \circ \pi$, а $\mathrm{sign}(ij) = -1$. □

Theorem 6.1. Существование знака

Существует гомоморфизм $\mathrm{sign} :\ S_n \to \{-1,1\}$ т.ч. $\mathrm{sign}(ij) = -1\ \forall i,j$.

Доказательство. Пусть $\pi : \begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$.

Определим $inv(\pi) = \{(i,j) \,|i < j \wedge \pi(i) > \pi(j)\}$. Пусть $\operatorname{sign}(\pi) = (-1)^{|inv(\pi)|}$.

Lemma 6.2.

Если t - транспозиция, тогда $\operatorname{sign}(t \circ \pi) = -\operatorname{sign}(\pi)$

Доказательство. Пусть π: $\begin{pmatrix} 1 & 2 & \dots & n \\ \pi(1) & \pi(2) & \dots & \pi(n) \end{pmatrix}$. Пусть $t = (\pi(i), \pi(j))$.

Тогда $t \circ \pi$ - мы поменяли местами $\pi(i)$ и $\pi(j)$ в таблице.

Как меняется множество inv? Достатно рассмотреть фрагмент $\pi(i), a_1, \dots, a_k, \pi(j)$, так как остальные инверсии остались.

Рассмотрим следующую последовательность преобразований

$$\pi(i), a_1, \dots, a_k, \pi(j) \to a_1, \pi(i), \dots, a_k, \pi(j) \to \dots \to a_1, \dots, a_k, \pi(i), \pi(j)$$

$$a_1, \dots, a_k, \pi(j), \pi(i) \to \dots \to \pi(j), a_1, \dots, a_k, \pi(i)$$

При каждой операции размер inv изменяется на единицу. А таких операций $2k+1$.

То есть транспозиция поменяла четность $|inv|$. □

Lemma 6.3.

Любая перестановка является композицией транспозиций.

Доказательство. очев точка(сначала на первое место ставим нужный элемент транспозицией, потом второй на нужный и так далее...) □

Возвращемся к теореме. $\pi = t_1 \circ \dots \circ t_k$. По первой лемме $\operatorname{sign}(\pi) = (-1)^k \operatorname{sign}(Id) = (-1)^k$.

В частности если $\operatorname{sign}(t) = -1$. $\operatorname{sign}(\pi_1 \circ \pi_2) = \operatorname{sign}(t_1 \dots t_l) = (-1)^{k+l} = (-1)^k * (-1)^l = \operatorname{sign}(\pi_1) * \operatorname{sign}(\pi_2)$

Пусть $\pi = t_1 \dots t_k = t_1 \dots t_l \Rightarrow k \equiv_2 l$ т.к. это все сравнимо с четностью перестановки. Значит наше определение корректно! □

Remark. $\operatorname{sign}(\pi)$ *не зависит от нумерации переставляемых элементов.*

Lemma 6.4.

$\operatorname{sign}(\pi) = \operatorname{sign}(\pi^{-1})$

Доказательство. $1 = \operatorname{sign}(Id) = \operatorname{sign}(\pi) * \operatorname{sign}(\pi^{-1})$ □

Theorem 6.2.

$det(A) = det(A^T)$

Доказательство. Пусть a' - элементы A^T.

$$det(A) = \sum_{\pi \in S_n} \text{sign}(\pi) \prod_i a_{i,\pi(i)} = \sum_{\pi \in S_n} \text{sign}(\pi^{-1}) \prod_i a_{\pi^{-1}(i),i} =$$
$$= \sum_{\pi \in S_n} \text{sign}(\pi^{-1}) \prod_i a'_{i,\pi^{-1}(i)} = \sum_{\sigma \in S_n} \text{sign}(\sigma) \prod_i a'_{i,\sigma(i)} = det(A^T)$$

□

Proposition 6.1.

det - полилинеен и кососимметричен по строкам

Доказательство. Кососимметричность: транспонируем строки — получаем столбцы

$$det(\begin{pmatrix} r_1 \\ \vdots \\ r_i \\ \vdots \\ r_i \\ \vdots \\ r_n \end{pmatrix}) = det(r_1|\dots|r_i|\dots|r_i|\dots|r_n) = 0$$

Полилинейность аналогично. □

Theorem 6.3.

1. $det(t_{ij}(a)A) = det(A) = det(At_{ij}(a))$
2. $det(m_i(a)A) = a * det(A) = det(Am_i(a))$
3. $det(s_{ij}A) = -det(A) = det(As_{ij})$

Доказательство. Достаточно проверить для столбцов.

2) из определения полилинейности.

3) кососимметричность

1) $det(a_1|\dots|a_i{+}aa_j|\dots|a_j|\dots|a_n) = det(a_1|\dots|a_i|\dots|a_j|\dots|a_n){+}a{*}det(a_1|\dots|a_j|\dots|a_j|\dots|a_n) = det(A) + a * 0 = det(A)$ □

Proposition 6.2.

Пусть $A \in M_n(K)$. Мы знаем, что существуют трансвекции $e_1, \dots, e_k$ - т.ч. $e_1 \dots e_k A$ имеет треугольный вид.
Тогда $det(A) = det(\text{треугольной}) =$ произведение диагональных элементов, так как это единственное произведение без нулей.

Theorem 6.4.

$A \in M_n(K)$. A - обратима $\iff$ $det(A) \neq 0$.

Доказательство. Любую обратимую можем привести к треугольному виду $\tilde{A}$.
$\tilde{A}$ обратима $\iff$ на диагонали $\prod a_{ii} \neq 0 \iff det(\tilde{A}) \neq 0 \iff det(A) \neq 0$. □

Theorem 6.5.

$det: M_n(K) \to K$ — гомоморфизм групп по умножению:
$det(AB) = det(A)det(B)$, $det(E) = 1$, $det(A^{-1}) = \frac{1}{det(A)}$

Доказательство. $B = (c_1|\dots|c_n)$. Тогда $AB = (Ac_1|\dots|Ac_n)$

Рассмотрим $f: B \mapsto det(AB)$. Докажем, что f полилинейно по столбцам и кососимметрично. Пусть $c_1 = c_1' + c_1''$

$det(AB) = det(A(c_1' + c_1'')|Ac_2|\dots|Ac_n)) = det(A(c_1')|Ac_2|\dots|Ac_n) + det(A(c_1'')|Ac_2|\dots|Ac_n)) = det(AB') + det(AB'')$.

Кососимметричность аналогично.

Итак, $B \to det(AB)$ - полилинейно и кососимметрично. Значит $f(B) = c * det(B)$. Подставим $B = E$, тогда $f(E) = det(A) = c * det(E) = c$.

Значит $f(B) = det(A)det(B)$. □

Theorem 6.6.

Пусть $A = \begin{pmatrix} B & D \\ 0 & C \end{pmatrix}$ $(B, C, D$ - матрицы). Тогда $det(A) = det(B) * det(C)$.

Corollary. *Для произвольной блочно-треугольной матрицы* $det = \prod_i det(A_i)$, *где* A_i *- матрицы на диагонали..*

Доказательство. Случай 1. $det(\begin{pmatrix} E & D \\ 0 & E \end{pmatrix})$. Элементарными преобразованиями приведем к виду $\begin{pmatrix} E & 0 \\ 0 & E \end{pmatrix}$, её определитель 1.

Случай 2. Пусть $\begin{pmatrix} A & D \\ 0 & E \end{pmatrix}$. Фиксируем D. $A = (c_1|\dots|c_k)$. Тогда $f : A \mapsto det(\begin{pmatrix} A & D \\ 0 & E \end{pmatrix})$ аналогично предыдущей теореме полилинейная, кососимметричная функция от c_i. Значит $det(\begin{pmatrix} A & D \\ 0 & E \end{pmatrix}) = c * det(A)$. Подставляем $A = E$. Получаем, что $c = 1$.

Общий случай. Фиксируем A, D. Тогда функция $C \mapsto \begin{pmatrix} A & D \\ 0 & C \end{pmatrix}$ полилинейна и кососимметрична.

Тогда $det(\begin{pmatrix} A & D \\ 0 & C \end{pmatrix}) = c * det(C)$. Подставляем $C = E$. Получим, что $c = det(A)$.

Значит $det(\begin{pmatrix} A & D \\ 0 & C \end{pmatrix}) = det(A) * det(C)$ □

Theorem 6.7. Разложение по строке/столбцу

Пусть $A \in M_n(K)$. $A = (a_{ij})$. Обозначим A_{ij} - определитель матрицы без i-й строки и j-го столбца.
Тогда $\forall i$ $det(A) = \sum_{j=1}^{n}(-1)^{i+j}a_{ij}A_{ij}$ - разложение по строке.
И $\forall j$ $det(A) = \sum_{i=1}^{n}(-1)^{i+j}a_{ij}A_{ij}$ - по столбцу.

Доказательство. Для солбцов аналогично.

Пусть i-я строка $(a_{i1}, \dots, a_{in}) = \sum_j a_{ij}e_j$. Тогда по полилинейности определителя

$det(A) = \sum_j a_{ij}det(\tilde{A}_j)$, где $\tilde{A}_j$ - матрица A, но вместо i-й строки стоит e_i.

Переставим строки и столбцы так, чтобы i-я строка стала первой и j-й столбец первым, а остальные сохранили порядок: свайпаем i с $i-1$, $i-1$ с $i-2$ и так далее.

$\begin{pmatrix} 1 & 0 \\ * & B \end{pmatrix}$. Её определитель отличается от $det(\tilde{A})$ на $(-1)^{i+j-2}$.

По теореме о блочной матрице $det(\begin{pmatrix} 1 & 0 \\ 0 & B \end{pmatrix}) = det(B) = det(A_{ij})$.

То есть $det(A) = \sum_j (-1)^{i+j-2}a_{ij}A_{ij}$. $\square$

Definition 6.2. Алгебраическое дополнение

$(-1)^{i+j}A_{ij}$ - алгебраическое дополнение элемента a_{ij}

Lemma 6.5.

$\sum_j (-1)^{i+j}a_{kj}A_{ij} = 0$, если $k \neq i$.

Доказательство. Заменим в A строчку r_i на r_k. Пусть новая матрица B. A_{ij} не изменился.
$\sum(-1)^{i+j}a_{kj}A_{ij} = det(B) = 0$ $\square$

Lemma 6.6. Явная формула обратной матрицы

$a'_{ij} \overset{\text{def}}{=} (-1)^{i+j}A_{ji}$. Тогда по теореме и следствию

$\sum_k a_{ik}a'_{kj} = \sum_k a_{ik}(-1)^{k+j}A_{jk} = \begin{cases} 0, \ i \neq j \\ det(A), \ i = j \end{cases}$

То есть $(a_{ij}) * (a'_{ij}) = det(A) * E$.
Пусть $det(A) \neq 0$. Тогда $\frac{1}{det(A)} * (a'_{ij}) = A^{-1}$.

Theorem 6.8. Формула Крамера

Пусть дана СЛУ $Ax = b$, где $A \in M_n(K)$. Пусть $det(A) \neq 0$. Тогда
$\forall i$ $x_i = \frac{\Delta_i}{\Delta}$, где $\Delta = det(A)$, $\Delta_i = det(c_1|\dots|\underset{i}{b}|\dots|c_n)$

Доказательство. $det(A) \neq 0$, значит $x = A^{-1}b = \frac{(a'_{ij})b}{det(A)}$

То есть $x_i = (i\text{-я строка } A^{-1})$ * b $= \frac{1}{det(A)} * \sum_j b_j * (a'_{ij})$

$$x_i = \frac{1}{det(A)} \sum_j b_j(-1)^{i+j} A_{ji} = \frac{\Delta_i}{\Delta}$$

□

Мотивирующий вопрос:

Пусть есть $\{A_n\}$, $A_n \in M_k(\mathbb{R})$. И $A_n \to A$. Существуют A_n^{-1}. Верно ли, что существует ли $A_n^{-1} \to A^{-1}$.

НЕ ВЕРНО $A_n = \frac{1}{n}E$.

А предел необратимых необратим, так как det - непрерывная фукнция(многочлен от элементов матрицы).

Условие $rkA < n$ задается уравнением $det(A) = 0$.

Утв: условие $rkA < k$ задается системой полиномиальных уравнений

Lemma 6.7. Ранг матрицы через миноры

$rkA = max\{k \,|\exists$подматрица размера k т.ч. её $det \neq 0$ $\}$
То есть все миноры порядка $< k$ нулевые(матрица из любых k строчек и столбцов имеет нулевой определитель).

7 Лекция 7. Восстановление в полях частных

7.1 Локализация и поля частных

Вопрос: верно ли, что для любого кольца R существует поле K, т.ч. $R \subset K$.

Аксиомы для такого кольца:

1. R — коммутативно и с 1.
2. R без делителей нуля.

Example 7.1.

Для $R = \mathbb{Z}/4\mathbb{Z}$, $\nexists$ поле K: $K \supset R$, т.к. $\overline{2} \cdot \overline{2} = 0$

Факт: $\forall$ ассоц. коммут. кольца без делителя 0 (область целостности) можно вложить в поле, и при том универсальным образом

Definition 7.1. Мультипликативня система

Пусть R кольцо, $S \subset R$ - мультипликативная система, если она замкнута относительно умножения и $0 \notin S$

Example 7.2.

$x \in \mathbb{Z} \setminus \{0\}$: $\{x,\ x^2,\ x^3,\ ...\}$ - мультипликативная система

Example 7.3.

Пусть R - область целостности, тогда $S = R \setminus \{0\}$ - мультипликативная система.

Хотим выполнение универсальное свойство:

Построить кольцо $K(R)$ и инъект. гомоморфизм $i : R \to K(R)$ т.ч.

1. $\forall s \in S \Rightarrow i(S) \in K(R)^*$
2. Если $j : R \to R'$ - инъективный гомоморфизм, т.ч $j(s) \in R^* \Rightarrow \exists! h$ — гомоморфизм: $j = h \circ i$

$$\begin{tikzcd}
R \arrow[r, "i"] \arrow[dr, "j"'] & K(R) \arrow[d, dashed, "\exists! h"] \\
& R'
\end{tikzcd}$$

Example 7.4.

Рассмотрим другую универсальную задачу:
Хотим гомоморфзим $f : R \to K$, K - поле, т.ч. $\forall$ гомоморфизма $f' : R \to K'$, K' - поле пропускается через f то есть существует h: $f' = h \circ f$
Существует ли такой f? Не всегда:
$R = \mathbb{Z}$
$\mathbb{Z} \to \mathbb{Q}$ и $\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$
Но гомоморфизмов между $\mathbb{Q}$ и $\mathbb{Z}/2\mathbb{Z}$ не существует.
Нет универсального гомоморфизма из $\mathbb{Z}$ в поле(но есть универсальный инъективный гомоморфизм).

Theorem 7.1. Построение поля частных

Пусть R - кольцо, S - мультипликативная система. Тогда унив. задача выше имеет решения.

Доказательство. Для случа R — области целостности $S = R \setminus \{0\}$, построим $i : R \to K$, K - поле, i - вложение

Рассмотрим *картинки* вида $\frac{a}{b}$, $a, b \in R,\ b \neq 0$.

Рассмотрим $R \times (R \setminus \{0\}) \overset{\text{def}}{=} \widetilde{K}$ и зададим на $\widetilde{K}$ отношение: $(a, b) \sim (c, d) \iff ad = bc$. Это отношение эквивалентности.

Очев (для всех, кроме автора)

1. $(a, b) \sim (a, b)$ т.к. $ab = ab$
2. $(a, b) \sim (c, d) \iff ab = cd \iff cb = da \iff (c, d) \sim (a, b)$
3. $\begin{cases} (a, b) \sim (c, d) \\ (c, d) \sim (e, f) \end{cases} \Rightarrow \begin{cases} ad = bc \\ cf = de \end{cases} \Rightarrow adcf = bcde \underset{\text{мы в области целостности}}{\Rightarrow} af = be$ т.е. $(a, b) \sim (e, f)$. Если $c \neq 0$.
   Если $c = 0$ очев.

Пусть $K = \widetilde{K}/\sim$.

Зададим на K $+, *$.

$$\overline{(a,b)} * \overline{(c,d)} = \overline{(ac,bd)}, bd \neq 0 \text{ т.к. область целостности}$$
$$\overline{(a,b)} + \overline{(c,d)} = \overline{(ad+bc,bd)}$$

Надо проверить корректность операций.

$$(a,b) \sim (a',b') \Rightarrow ab' = a'b \Rightarrow b'dac = a'cbd \Rightarrow (a,b)*(c,d) = (a',b')*(c,d)$$

Для сложения аналогично.
Проверим(нет), что K это поле!
$0 = \overline{(0,1)}$, $1 = \overline{(1,1)}$.
Ассоциативность, коммутативность умножения очев.
Коммутативность сложения очев.
$\overline{(a,b)} + \overline{(-a,b)} = \overline{(ab-ba,b^2)} = \overline{(0,b^2)} = \overline{(0,1)} = 0$. То есть у любого есть противоположный.
Ассоциативность:

$$(\overline{(a,b)}+\overline{(c,d)})+\overline{(e,f)} = \overline{(ad+bc,bd)}+\overline{(e,f)} = \overline{(adf+bcd+bde,bdf)} = \dots = \overline{(a,b)}+(\overline{(c,d)}+\overline{(e,f)})$$

Дистрибутивность: $\overline{(a,b)}(\overline{(c,d)}+\overline{(e,f)}) = \overline{(a,b)} \cdot \overline{(cf+de,df)} = \overline{(acf+ade,bdf)}$
$\overline{(a,b)} \cdot \overline{(c,d)} + \overline{(a,b)} \cdot \overline{(e,f)} = \overline{(ac,bd)} + \overline{(ae,bf)} = \overline{(acbf+bdae,bdbf)} \sim \overline{(acf+ade,bdf)}$, т.к. $(acf+ade)\cdot bdbdf = (acbf+bdae)\cdot bdf$
Пусть $a \neq 0 \in R$, тогда $\overline{(a,b)} * \overline{(b,a)} = \overline{(ab.ab)} = \overline{(1,1)}$. То есть существует $\overline{(a,b)}^{-1}$.
Если $a = 0$, то $\overline{(0,b)} = \overline{(0,1)} = 0$.
Построим $i : R \to K$, т.ч. $a \mapsto \overline{(a,1)}$.
i - инъективно: $\overline{(a,1)} = \overline{(b,1)} \Rightarrow a = b$.
i - гомоморфизм $i(a+b) = \overline{(a+b,1)} = \overline{(a,1)} + \overline{(b,1)}$, для умножения аналогично.
Универсальность: Пусть $j : R \to R'$ - гомоморфизм, т.ч. $\forall r \in R \setminus \{0\}$, $j(r)$ - обратим. Хотим построить h:

$$\begin{tikzcd} R \arrow[r, "i"] \arrow[dr, "j"'] & K(R) \arrow[d, dashed, "\exists! h"] \\ & R' \end{tikzcd}$$

$h \circ i = j$. То есть $h(\overline{(r,1)}) = j(r)$.
$h(\overline{(1,1)}) = 1_R$, а значит $h(\overline{(1,r)}) = j(r)^{-1}$.
А тогда $\forall a,b,\ h(\overline{(a,b)}) = j(a)\cdot j(b)^{-1}$. С другой стороны формула $h(\overline{(a,b)}) = j(a)\cdot j(b)^{-1}$ корректно задает гомоморфизм.
$\overline{(a,b)} = \overline{(a',b')} \Rightarrow ab' = ba' \Rightarrow j(ab') = j(ba') \Rightarrow j(a)\cdot j(b)^{-1} = j(a')\cdot j(b')^{-1}$. Значит h не зависит от выбора представителя. ☐

Definition 7.2. Поле частных

K называется полем частных кольца R и элементы записывают $\frac{a}{b} \overset{\text{def}}{=} \overline{(a,b)}$

Remark. *В общем случае* (R, S) *доказательство такое же.*

Example 7.5.

$R = K[x]$, $S = \{x, x^2, \dots\}$. Тогда получим $R \to R[S^{-1}] = \{\frac{a_n}{x^n} + \dots + \frac{a_1}{x} + a_0 + \frac{b_1}{x} + \frac{b_n}{x^n}\} = K[x, \frac{1}{x}]$ - многочлены Лорана.

Example 7.6.

Пусть $R = \mathbb{Z}$, $S = \{x : p \nmid x\}$, p - простое. Тогда $R[S^{-1}] = \{\frac{a}{b} : b \nmid p\}$ - здесь единственное простое число p.

Remark 7.1.

Пусть R - факториальное кольцо, K - поле частных. Тогда $\forall x \in K$ $\exists (a, b)$ с точностью до ассоциированности, т.ч. $x = \frac{a}{b}$ и $gcd(a, b) = 1$(т.к. в факториальном кольце есть нод, на который можем сократить).

Definition 7.3.

Поле частных кольца $K[x]$ называется полем дробно рациональных функций

$$K(x) = \{\frac{p}{q} : p, q \in K[x], q \neq 0\}$$

можно считать, что $(p, q) = 1$ и q - унитарный(старший коэф - 1).

Ясно, что $K(x)^* = \langle c, p \mid c \in K, p - \text{унитарный} \rangle$

Вопрос: $K(x)$ - векторное пространство над K. Какой у него базис?

Lemma 7.1.

1. $U = \{\frac{f}{g} \mid deg(f) < deg(g) \vee f = 0\}$ - подпространство $K(x)$.
2. $K(x) = U \oplus K[x]$.

Доказательство. 1) Корректность определения. Пусть $\frac{f}{g} = \frac{f'}{g'} \Rightarrow fg' = f'g \Rightarrow deg(f) + deg(g') = deg(f') + deg(g)$, тогда $deg(f) < deg(g) \iff deg(f') < deg(g')$

$deg(f_i) < deg(g_i) \Rightarrow deg(f_1g_2 + f_2g_1) \leq max(deg(f_1g_2), deg(f_2g_1)) = max(deg(f_1) + deg(g_2), deg(f_2) + deg(g_1)) \leq deg(g_1) + deg(g_2) \Rightarrow \frac{f_1g_2 + f_2g_1}{g_1g_2}$ — правильная

2) $U \cap K[x] = \{0\}$. Достаточно доказать, что $\forall f \in K(x)$: $f = p + g$, $p = U$, $g \in K[x]$.

Пусть $f = \frac{s}{h}$. $s = hq + r$. Тогда $f = q + \frac{r}{h}$. По определению деления с остатком $\frac{r}{h}$ - правильная. $\square$

Corollary. *Базис* $K(x)$ *можно искать в виде* $\{$*базис* $U\} + \{$*базис* $K[x]\}$

Definition 7.4. Примарная дробь

$f \in K[x]$, f называется примарный, если $f = \frac{p}{q^k}$, где q - неприводим.

Lemma 7.2.

Любую правильную дробь можно разложить в сумму правильных примарных.

Доказательство. $f \in K(x) \Rightarrow f = \frac{p}{q_1^{a_1} \ldots q_k^{a_k}}$, q_i — неприводимые и $(q_i^{a_i}, q_j^{a_j}) = 1$.

Достаточно доказать:

Если f - правильная дробь, $f = \frac{p}{s_1 s_2}$, где $\gcd(s_1, s_2) = 1$, то: $f = \frac{p_1}{s_1} + \frac{p_2}{s_2}$, где $\frac{p_i}{s_i}$ — правильные.

Доказательство. $\exists h_1, h_2 \in K[x]: \ h_1 s_1 + h_2 s_2 = 1$.

Тогда $f = \frac{p}{s_1 \cdot s_2} = \frac{(h_1 s_1 + h_2 s_2) p}{s_1 \cdot s_2} = \frac{h_1 s_1 p}{s_1 s_2} + \frac{h_2 s_2 p}{s_1 s_2} = \frac{h_1 p}{s_2} + \frac{h_2 p}{s_2} = (p_1 + \frac{t_2}{s_2}) + (p_2 + \frac{t_1}{s_2}) = (p_1 + p_2) + \frac{t_2}{s_2} + \frac{t_1}{s_1} \Rightarrow$ $p_1 + p_2 = f - \frac{t_2}{s_2} - \frac{t_1}{s_1}$, это равентсво $0 = 0$, т.к. слева многочлены, а справа правильные дроби $\Rightarrow p_1 + p_2 = 0$ □

Применим это k раз $f = \frac{p_1}{q_1^{a_1}} + \frac{p_2}{q_2^{a_2} \ldots q_k^{a_k}} = \ldots = \sum \frac{p_i}{q_i^{a_i}}$ □

Итак $U = \langle \frac{p}{q^k} \mid deg(p) < deg(q^k), q - \text{неприводим} \rangle$

Definition 7.5. Простейшая дробь

$f \in K(x)$ - простейшая, если $f = \frac{p}{q^k}$, q - неприводим и $deg(p) < deg(q)$.

Lemma 7.3.

$\forall$ правильная примарная дробь — сумма простейших

Доказательство. Пусть f - такая дорбь. Тогда $f = \frac{p}{q^k}$, q - неприводим. Индукция по k. *База* $k = 1$, $f = \frac{p}{q}$ – очевидно простейшая.

Переход. $k \to k+1$. $\exists h, \ r$: $p = q \cdot h + r, \ deg(r) < deg(q)$.

$f = \frac{p}{q^{k+1}} = \frac{qh + r}{q^{k+1}} = \frac{h}{q^k} + \frac{r}{q^{k+1}}$. По предположению $\frac{h}{q^k}$ — сумма простейших, вторая и так простейшая $\Rightarrow f$ — сумма простейших □

Lemma 7.4.

$\forall f \in K(x): \ f = p + \sum \frac{p_i}{q_i}, \ p \in K[x], \ \frac{p_i}{q_i}$ - простейшие

Доказательство. $f \underset{Lm.1}{=} p + u \underset{Lm.2}{=} p + (u_1 + u_2 + \ldots + u_k) \underset{Lm.3}{=} p + \text{сумма простейших}$ □

Example 7.7.

Пусть $K = \mathbb{C}$. Если p - неприводим, то $p = x - z$. Простейшая дробь $\frac{c}{(x-a)^k}$, $c \in \mathbb{C}$.
То есть $f \in K(x) \Rightarrow f = \sum \frac{c_i}{(x-a_i)^{k_i}}$
Если $K = \mathbb{R}$, то p - неприводим, если $p = x - a$ или $x^2 - px + q$, где $p^2 - 4q < 0$.
Тогда $f \in K(x) \Rightarrow f = \sum \frac{c_i}{(x-a)^{k_i}} + \sum \frac{b_i x + c_i}{(x^2 - p_i x + q_i)^{k_i}}$
Частные случаи: Пусть $f = \frac{p}{\prod\limits_{i=1}^{n}(x-a_i)}$, $deg(p) < n$. Тогда $f = \sum_i \frac{c_i}{x-a_i}$.
Была формула $p = \sum p(a_i)\frac{\prod_i (x-a_i)}{\prod (a_i - a_j)}$. Поделим на $\prod(x - a_i)$. Тогда получим $\frac{p}{\prod(x-a_i)} = \sum_i \frac{p(a_i)}{(x-a_i)\prod_j(a_i-a_j)}$
Если $q = \prod_i (x - a_i)$, тогда $q' = \sum_i \prod_{j \neq i}(x - a_j)$. Значит $q'(a_{i_0}) = \prod_{j \neq i_0}(a_{i_0} - a_j)$.
Таким образом $f = \frac{p}{q} = \sum_i \frac{p(a_i)}{q'(a_i)(x-a_i)}$
Если $f = \frac{p}{(x-a)^n}$, тогда $f = \sum \frac{\frac{p^{(k)}(a)}{k!}}{(x-a)^{n-k}}$.

8 Лекция 8. Групповые группы

8.1 Опять группы

Фан факты:

Пусть G - конечная абелева группа, тогда $G \cong \mathbb{Z}/n_1\mathbb{Z} \times \cdots \times \mathbb{Z}/n_k\mathbb{Z}$.

Если G - произвольная, то очень сложно!!!

Самые важные группы:

1. Конечные: S_n - группа перестановок
2. "Алгебраические": $GL_n(K)$ - обратимые матрицы над полем K, что есть группа преобразований n-мерного пространства.

Remark. *Можно считать, что $S_n \subset GL_n(K)$. Если зафиксируем базис $V - e_i$. Каждой перестановке π сопоставим отображение $\pi(e_i) = e_{\pi(i)}$. Её матрица имеет вид $a_{i,\pi(i)} = 1$ иначе 0.*

Theorem 8.1. Теорема Кэли

Пусть G - конечная группа, тогда $\exists n, i \ : \ G \to S_n$ — инъективный гомоморфизм(вложение). То есть G можно рассматривать как подгруппу в S_n.

Доказательство. Возьмем $n = |G|$, $g \in G$. Сопоставим ему следующую функцию $f_g(x) = gx$, $f : G \to G$. Она очевидно биекция, потому что существует обратная $f_{g^{-1}}$. То есть $f \in S(G)$ - группа преобразований множества G.

Понятно, что $S(G) \cong S_n$.

Построим $i \ : G \to S(G)$, $g \mapsto f_g$. i - инъекция, так как если $f_g = f'_g \Rightarrow f_g(e) = f'_g(e) \Rightarrow g = g'$.

i - гомоморфизм. Так как $(i(g_1) \circ i(g_2))(x) = g_1 * (g_2 * x) = (g_1 * g_2) * x = i(g_1 * g_2)$ из ассоциативности. $\square$

Remark. *Такие n, i совсем не единственные(упр).*

Было в $\mathbb{Z}$, $a \sim b \iff a - b \,\vdots\, n$. Получили новую группу $\mathbb{Z}/n\mathbb{Z}$.

Другими словами $a \sim b \iff a - b \in \langle n \rangle$ - подгруппа.

Можно ли в этой конструкции заменить $(\mathbb{Z}, \langle n \rangle)$ на (G, H), где G - любая группа, а H - подгруппа.

Example 8.1. Аналогичные конструкции

Пусть $G = (K^2, +)$. $v_0 \in K^2$. Рассмотрим $\langle v_0 \rangle$. Положим $v_1 \sim v_2 \iff v_1 - v_2 = kv_0$.
Какой у этого смысл? Класс эквивалентности v_1 это прямая, параллельная v_0 из конца v_1. Вся наша плоскость расслоилась в объединение непересекающихся прямых, параллельных v_0 - *классы по модулю* v_0.
$K^2/v_0 = \{kv_3\}$ - для любой прямой не коллинеарной v_0 получим единственное пересечение с каждым классом.

Example 8.2.

Пусть $G = (\mathbb{Z}/p\mathbb{Z})^*$, $H = \langle x^2 \,|x \in (\mathbb{Z}/p\mathbb{Z})^* \rangle$. То есть $a \sim b \iff a = x^2 b$.
Получим два класса эквивалентности - квадраты и не квадраты. $G/H \cong \mathbb{Z}/2\mathbb{Z}$, так как такая же таблица умножения! Квадрат*квадрат=квадрат и т.д.

Общая конструкция: $H \leq G$, $a \sim b \iff ab^{-1} \in H$. (или $b^{-1}a \in H$)

Можно рассматривать два разных отношения. Если $\sim_1 = \sim_2$, тогда $\overline{a \circ b} = \overline{a} \circ \overline{b}$ превращает $G/\sim$ в новую группу.

Lemma 8.1.

G - группа, H - подгруппа, $a \sim_1 b \iff ab^{-1} \in H$, $a \sim_2 b \iff b^{-1}a \in H$. Тогда $\sim_1, \sim_2$ - отношения эквивалентности и $\overline{a}_1 = \{ha,\ h \in H\} = Ha$, $\overline{a}_2 = \{ah,\ h \in H\} = aH$.

Доказательство. Рефлексивность: $aa^{-1} = e \in H$.

Симметричность: $ab^{-1} \in H$, тогда $ba^{-1} = (ab^{-1})^{-1} \in H$.

Транзитивность: $ab^{-1} \in H, bc^{-1} \in H \Rightarrow ab^{-1}bc^{-1} = ac^{-1} \in H$.

Везде пользуемся, что H - подгруппа.

Пусть a - фикс, тогда $ab^{-1} = h \in H$, если $a \sim b$, тогда $a = hb \iff h^{-1}a = b$, то есть все подходящие b имеют вид ha.

Для $\sim_2$ аналогично. $\square$

Definition 8.1. Классы смежности

aH, Ha - классы смежности. Один из них левый, другой - правый.
Будем считать Ha - левым.

Remark. *Смежные классы непересекаются или совпадают, так как это классы эквивалентности.*

То есть $G = \bigsqcup_i Ha_i$ *и* $Ha_i \cap Ha_j = \varnothing$.

Частный случай, если $n = |G| < \infty$, тогда $m = |H| < \infty$. При этом $\forall a$, $|Ha| = m$(т.к. $h_1 a \neq h_2 a \iff h_1 \neq h_2$). Следовательно $n \,\vdots\, m$ и $\frac{n}{m}$ - количество смежных классов.

$\frac{n}{m} \overset{\text{def}}{=} |G : H|$ - индекс G по H.

Theorem 8.2. Теорема Лагранжа

G - конечна, $H \leq G \Rightarrow |G| \vdots |H|$ и $|G| = |H| \cdot |G : H|$.

Частный случай: $H = \langle h \rangle \Rightarrow |G| \vdots ord(h)$ - было в первом модуле!

Обозначаем G/H - множество правых смежных классов($H \backslash G$ - левых).

Можем рассматривать разбиение $G = \bigsqcup_i Ha_i = \bigsqcup_i b_i H$.

Theorem 8.3.

Пусть G - группа, $H \leq G$. Следующие условия равносильны

1. $(aH) \cdot (bH) \overset{\text{def}}{=} abH$ корректно задает структуру группы на G/H.
2. То же самое на левых
3. $\sim_1 = \sim_2$
4. $\forall a \; aH = Ha$
5. $\forall h \in H, g \in G \; : g^{-1}hg \in H$.

Доказательство. 3 $\iff$ 4 т.к. $a \sim_1 b \iff b \in aH$, $a \sim_2 b \iff b \in Ha$.

3 $\iff$ 5 $\Rightarrow$

Пусть $g \in G$, $h \in H$. $a = g^{-1}hg \in G \Rightarrow ga = hg$.

$$ga = hg \sim_1 g \Rightarrow ga \sim_2 g \Rightarrow ga = g\tilde{h} \Rightarrow a \in H$$

$\Leftarrow$ Пусть $g_1 \sim_1 g_2 \Rightarrow g_2 = g_1 h$, $h \in H$.

$g_2 g_1^{-1} = g_1 h g_1^{-1} \in H \Rightarrow g_2 \sim_2 g_1$.

$3, 5 \Rightarrow 1$. Надо показать, что такое определение не зависит от выбора представителя.

$a_1 = ah_1$, $b_1 = bh_2$.

$$(a_1 H)(b_1 H) = (a_1 b_1 H) = (ah_1 bh_2 H)$$

Т.к. $bH = Hb$, то $h_1 b = bh_1' \Rightarrow (abh_1' h_2 H) = (abH)$.

Мы использовали, что $(ahH) = \{ahh_1 \mid h_1 \in H\} = \{ah' \mid h' \in H\}$, так как умножение на h - биекция.

Получилась группа:

$((aH)(bH))(cH) = ((ab)cH) = (a(bc)H) = (aH)((bH)(cH))$.

$eH = H$ - нейтральный элемент.$(aH)^{-1} = a^{-1}H$. $\square$

Definition 8.2. Факторгруппа

Группа из предыдущей теоремы обозначается G/H и называется факторгруппа G по H.

Definition 8.3. Нормальная подгруппа

H удовлетворяющая условиям теоремы называется нормальной подгруппой и обозначается $H \trianglelefteq G$.

Example 8.3.

G - абелева, то любая подгруппа нормальная!
Рассмотрим S_3, $H = \langle (1,2) \rangle = \{e, (1,2)\}$.
Пусть $g = (1,3)$. Тогда $gH = \{(13), (123)\}$, $Hg = \{(13), (132)\}$ - ненормальная.
$H_1 = \langle (123) \rangle$ нормальная.

Делаем это затем, чтобы получить из G более *простую* группу. Как её интерпретировать?

Definition 8.4. Ядро и образ

Пусть $f : G \to H$ - гомоморфизм групп. Определим его ядро и образ

$$Im(f) = \{f(g) \,|g \in G\}, ker(f) = \{g \,|f(g) = e_H\}$$

Lemma 8.2.

$Im(f) \leq H$, $ker(f) \trianglelefteq G$.
f - сюръективен, если $Im(f) = H$. Инъективен, если $ker(f) = \{e_G\}$.

Доказательство. Почти все как в линейной алгебре. Например:
$ker(f) = e_H \Rightarrow f(g_1) = f(g_2) \Rightarrow f(g_1 g_2^{-1}) = e \Rightarrow g_1 = g_2$.
Нормальность ядра:

$$g \in G, h \in ker(f) \Rightarrow f(g^{-1}hg) = f(g^{-1})f(h)f(g) = f(g^{-1})f(g) = f(e) = e$$

Остальное упр. □

Theorem 8.4. О гомоморфизме

Пусть G, H - группы, $f : G \to H$ - гомоморфизм, тогда $Im(f) \cong G/ker(f)$.

Remark. *Хотим интерпретацию для G/G_1, где $G_1 \trianglelefteq G$. Можем придумать гомоморфизм и группу $f : G \to H$, т.ч. $ker(f) = G_1 \Rightarrow G/G_1 \cong Im(H)$.*

Доказательство. Построим изоморфизм: $i : G/ker(f) \to Im(f)$.
$\overline{g} \in G/ker(f) \Rightarrow i(\overline{g}) = f(g)$.
Проверим корректность и изоморфизм.
Корректность: $f(g) \in Im(f)$. Пусть $g_1 \sim g \iff g_1 = gh$, где $h \in ker(f)$.

$$i(g_1) = f(gh) = f(g)f(h) = f(g)e = i(g)$$

Гомоморфность:
Сюръективность: g - произвольный, поэтому $Im(i) = Im(f)$.
Инъективность: $i(\overline{g}) = f(g) = e \Rightarrow g \in ker(f) \Rightarrow g = \overline{e} \Rightarrow ker(i) = \{\overline{e}\}$ □

Example 8.4.

Пусть $G = S_n$. $\text{sign}(\pi)$ - гомоморфизм групп.
Что такое $ker(\text{sign}) = \{\pi \,|\, \text{sign}(\pi) = 1\}$ - четные перестановки. Они образуют подгруппу A_n.
$A_n \trianglelefteq S_n$, т.к. $A_n = ker(\text{sign})$.
Значит $S_n/A_n \cong \mathbb{Z}/2\mathbb{Z}$.

Example 8.5.

Пусть $f\ (\mathbb{Z}, +) \to (\mathbb{C}, *)$, т.ч. $f(k) = e^{\frac{2\pi ik}{n}}$.
Очевидно гомоморфизм. $Im(f)$ - корни n степени из единицы. $ker(f)$ - числа кратные n.
Получим по теореме $\mathbb{Z}/n\mathbb{Z} \cong \mu_n(\mathbb{C})$

Example 8.6. *Тривиальный*

Рассмотрим $G = G_1 \times G_2$ и гомоморфизм $f\ : G \to G_2,\ f(g_1, g_2) \to g_2$.
$Im(f) = G_2,\ ker(f) = \{(g_1, e)\} \cong G_1$.
Получим $G/G_1 \cong G_2$.

Remark. *Пусть G - какая-то(большая) группа. Хотим её изучить. Попробуем найти в ней нетривиальную нормальную подгруппу.*

Можем рассмотреть её факторгруппу. И думать вместо G о двух группах(поменьше) $(H, G/H)$.

Верно ли, что по $H, G/H$ однозначно восстанавливается G? НЕТ.

Так как любая группа может быть получена тривиальным гомоморфизмом.

9 Лекция 9. Групповые группы. Вторая битва

9.1 Продолжаем группы

H — нормальная подгруппа G, условие нормальности: $\forall h \in H,\ g \in G : g^{-1}hg \in H$, тогда $\exists$ факторгруппа G/H. $G \to (H,\ G/H)$

$G = G_1 \times G_2 \Rightarrow G \to G_2$ и $(G)/G_1 \cong G_2$. $(G_1 \times G_2) \to (G_1, G_2)$.

Внешнее прямое произведение: на декартовом произведение задаем покомпонентные операции

Внутреннее прямое произведение: $G_1, G_2 \leq G$ и хотим понять, что $G \cong G_1 \times G_2$.

Theorem 9.1.

$G_1, G_2 \leq G$. Рассмотрим отображение $i\ : G_1 \times G_2 \to G$, т.ч. $(g_1, g_2) \mapsto g_1 \circ g_2$.
Тогда i - изоморфизм $\iff$

1. $\forall g \in G,\ \exists g_1, g_2\ : g = g_1 * g_2$.
2. $G_1 \cap G_2 = \{e\}$
3. $\forall g_1 \in G_1,\ g_2 \in G_2 \Rightarrow g_1 g_2 = g_2 g_1$

Доказательство. $\Leftarrow$. i - гомоморфизм.

$$i((g_1g_1', g_2g_2')) = g_1g_1'g_2g_2' = g_1g_2g_1'g_2' = i((g_1, g_2)) * i((g_1'g_2'))$$

Среднее равенство верно по пункту 3.

i - сюръекция по 1.

Инъективность $\iff$ $Ker(i) = \{e\}$. Пусть $(g_1, g_2) \in Ker(i) \Rightarrow g_1g_2 = e \Rightarrow g_1 = g_2^{-1} \Rightarrow g_1 \in G_1 \cap G_2 = \{e\} \Rightarrow g_1 = e = g_2$.

Обратно УПР. □

Exercise 9.1.

Вместо условия 3 можно потребовать $G_1, G_2 \trianglelefteq G$.

Вопрос: как что-то доказать или классифицировать про группы? Например про конечные...

Идея такая: Индукция по порядку группы. Реализация: Пусть $|G| = n$. Доказали что-то для всех меньших n. Тогда рассмотрим $H \trianglelefteq G$, к H и G/H применяем индукцию и потом доказываем для G.

Не работает, если у G нет нетривиальных нормальных подгрупп.

Definition 9.1. Простая группа

Группа G называется простой, если $\forall H \trianglelefteq G \Rightarrow H = G \vee H = \{e\}$.

Одна из главных задач - классификация простых групп.

Example 9.1.

$\mathbb{Z}/p\mathbb{Z}$ - нет нетривиальных подгрупп.
$A_n \trianglelefteq S_n$ - четные перестановки (теорема Галуа говорит, что A_n проста при $n \geq 5$).
$GL(n, K)$ - не проста. Рассмотрим $SL(n, K) \trianglelefteq GL(n, K)$ - матрицы с определителем 1. (нормальность: $det(A) = 1 \Rightarrow det(CAC^{-1}) = det(A) = 1$).
$GL(n, K)/SL(n, K) \cong K^*$ по теореме о гомоморфизме: $det : GL_n(K) \to K$. Его ядро это $SL_n(K)$, а образ все K^*.
То есть $GL(n, K) \cong SL_(n, K) \times K^*$. K^* - абелева группа, тут все просто...
А $SL(n, K)$? Тоже нет! Есть подгруппа $Z(SL(n, K)) = \{kE | det(kE) = 1\}$. Она нормальная. Соответствующая факторгруппа называется $PSL(n, K)$ - обычно уже проста.

Theorem 9.2. Классификация конечных простых групп

Пусть G - конечная простая группа. Тогда

1. $G \cong \mathbb{Z}/p\mathbb{Z}$
2. $G \cong A_n$, $n \geq 5$
3. $G \cong PSL(n, K)$, K - конечное поле
4. G принадлежит одной из 15 серий, аналогичных пункту 3. (серия - подгруппа в $GL(n, K)$ с некоторым свойством).
5. G одна из 26 исключительных простых групп.

9.2 Группы перестановок

Рассматриваем S_n - симметрическую группу.

Базовые элементы: $t_{i,j}$ - транспозиция (ij).

Theorem 9.3.

S_n порождена $t_{i,j}$.

Более точно: S_n порождается $t_{k,k+1}$. (любую перестановку получим из тождественной свапая элементы в нужное место через соседние)

На самом деле $S_n = \langle (12), (123\dots n) \rangle$. Где $t_{12} = (12)$, $(123\dots n) = \pi$, т.ч. $pi(i) = i+1$.

Как работать с t_{ij}? Есть базовые соотношения:

$s_i = t_{i,i+1}$. Есть $s_1, \dots, s_{n-1}$. Они обладают следующими свойствами. $s_i^2 = e$. Почти всегда $s_i s_j = s_j s_i$(или $(s_i s_j)^2 = e$). Точно равно, когда они непересекаются ($|i-j| > 1$) или равны...

$s_i s_{i+1} s_i = s_{i+1} s_i s_{i+1} \iff (s_i s_{i+1})^3 = e$. (упр для настоящих гулей (c) со-автор)

Theorem 9.4.

Любое соотношение между s_i следует из базовых.

Цикловое разложение перестановки

Цикл $(i_1, \dots, i_k)$ это перестановка π т.ч. $\pi(i_l) = i_{l+1}$, $\pi(i_k) = i_1$ и $\pi(i) = i$ иначе.

Частный случай - транспозиция - цикл длины 2.

Lemma 9.1.

Любая перестановка однозначно раскладывается на произведение независимых(попарно непересекающихся) циклов длины > 1.

Доказательство. Существование разложения: индукция по количеству i т.ч. $\pi(i) \neq i$ (подвижных точек).

База: $\pi(i) = id$ - пустое произведение циклов.

Переход: $\to n \neq 0$. Пусть $\pi(x) \neq x$. Положим $x_1 = x, x_{i+1} = \pi(x_i)$. Тогда $\exists k, l \; x_k = x_l \Rightarrow x_{k-1} = x_{l-1} \Rightarrow x_m = x_1$. Теперь рассмотрим перестановку $\tilde{\pi} = (x_1 \dots x_m)^{-1}\pi$. Она $\tilde{\pi}(x_i) = x_i$ и $\tilde{\pi}(x) = \pi(x)$.

Это перестановка на меньшем множестве неподвижных точек $\{1, 2, \dots, n\} \setminus \{x_1, \dots, x_m\}$. По индукции получаем $\tilde{\pi} = c_1 \dots c_k \Rightarrow \pi = (x_1, \dots, x_m) c_1 \dots c_k$.

□

Definition 9.2. Цикловой тип

Цикловой тип перестановки равен $a_1 + a_2 + \dots + a_m$, если $\pi = c_1 \dots c_m$, где c_i - независимые циклы длины a_i.

Example. *Транспозиция: перестановка типа 2.*

Что значит, что у двух перестановок одинаковый цикловой тип?

Это значит, что можно перенумеровать элементы множества $\{1, 2, ..., n\}$ так, чтобы $\pi_1 \mapsto \pi_2$

$x \to "y" \iff \exists \tau: \ \pi_2 = \tau \circ \pi_1 \tau^{-1}$
У соавтора садится ноутбук, бб читатель =(

Definition 9.3.

Элементы g и ugu^{-1} называются сопряженными.

Lemma 9.2.

g_1 и g_2 сопряжены в $S_n \iff$ имеют одинаковый цикловой тип

Exercise 9.2. Сопряженные элементы

Сопряженность это отношение эквивалентости

Remark 9.1.

H - нормальная подгруппа $\iff H \leq G$ и H состоит из классов сопряженности.
H - проста: никакой набор классов сопряженности не образуют нетривиальную подгруппу.

Remark 9.2.

H -абелева, тогда класс сопряженности состоят из самого элемента.

9.3 Действие групп на множествах

Definition 9.4.

Действие группы G на множестве M это бинарная операция $f \ : G \times M \to M$, т.ч. $(g, m) \mapsto g \cdot m$. Такая что

1. $e \cdot m = m$
2. $(g_1 g_2) \cdot m = g_1 \cdot (g_2 \cdot m)$

Другими словами определим $f_g(m) = g \cdot m$ - отображение $M \to M$. Задать действие = задать f_g. Аксиомы превращаются в

1. $f_e = id_M$
2. $f_{g_1 g_2} = f_{g_1} \circ f_{g_2}$

Итого отображение $G \to S(M)$, $g \mapsto f_g$ это гомоморфизм групп.
Задано перестановочное представление группы G. В частности $f_g \in S(M)$, т.е. f_g - биекция, т.к. существует $f_{g^{-1}}$.
Обозначаем $G \curvearrowright M$

Всем ку от соавтора =)

Example 9.2.

S_n действует на $I_n = \{1, 2, \dots, n\}$. $\pi \cdot i = \pi(i)$.
S_n действует на $I_n \times I_n$ $\pi(a, b) = (\pi(a), \pi(b))$.
На неупорядоченных парах $\pi(\{x, y\}) = \{\pi(x), \pi(y)\}$.
На всех подмножествах 2^{I_n}. $\pi \cdot A = \pi(A)$.
На функции $I_n \to \mathbb{R}$: $f : I_n \to \mathbb{R}$, хотим задать $(\pi \circ f)(x) = f(\pi(x))$, тогда $(\pi_1 \cdot \pi_2 \cdot f)(x) = f(\pi_1\pi_2(x))$, $(\pi_1(\pi_2 f))(x) = \pi_2 f(\pi_1(x)) = f(\pi_2\pi_1(x))$. Не выполнилась аксиома(.
Правильное определение $(\pi \circ f)(x) = f(\pi^{-1}(x))$. Тогда аксиомы будут выполняться.

Example 9.3.

Ещё один примерчик, их много не бывает =)
Рассмотрим $M = \mu_3(\mathbb{C}) = \{1, w, w^2\}$. $G = \mu_3(\mathbb{C})$. Действует на $\mathbb{C}$ умножением как обычные комплексные числа.
f_w - поворот на $\frac{2\pi}{3}$.
$G = \langle f_w, \overline{z} \rangle \leq S(\mathbb{C})$, где $\alpha(z) = \overline{z}$. Тогда $G \cong S_3$. $f_w(\mu_3) \in \mu_3$, $\alpha(\mu_3) \in \mu_3$. G действует на μ_3.
f_g - всевозможные перестановки μ_3. Можно сказать, что G действует самосовмещениями треугольника, то есть движения плоскости, которые треугольник $1, w, w^2$ переходит сам в себя.

Example 9.4. Группа самосовмещений квадрата

$D_4 = \{f : \mathbb{R}^2 \to \mathbb{R}^2\}$, т.ч. f - движение и $f(K) = K$, где K - квадрат.
$|D_4| = 8$. $id, r_{\frac{\pi}{2}}, r_\pi, r_{\frac{3\pi}{2}}$ и 4 осевых симметрии.
D_4 действует на вершинах квадрата или на серединах сторон, или на самих сторонах.

Definition 9.5. Орбита и стабилизатор

Пусть G действует на M. $m \in M$. Орбита m это $G \cdot m = \{g \cdot m \mid g \in G\} \subset M$.
Слабилизатор $G_m = \{g \in G \mid g \cdot m = m\}$.

Lemma 9.3.

1. G_m - подгруппа G.
2. Любые две орбиты не пересекаются или совпадают.

Доказательство. 1) $e \cdot m = m$, $g_1 \cdot m = m \wedge g_2 \cdot m = m \Rightarrow g_1 g_2 \cdot m = m$.
2) Пусть $m_1 \sim m_2 \iff \exists g : gm_1 = m_2$. Это отношение эквивалентности.

1. $em_1 = m_1$
2. $gm_1 = m_2 \iff m_1 = g^{-1}m_2$
3. $gm_1 = m_2$, $hm_2 = m_3 \Rightarrow hgm_1 = m_3$

Орбиты - классы эквивалентности. □

Lemma 9.4.

Пусть G действует на M. И $|Gm| < \infty$. Пусть $n \in Gm \Rightarrow n = g_0 m$. Как найти все $g : n = gm$.
$n = gm \Rightarrow g_0^{-1} n = g_0^{-1} gm \iff m = g_0^{-1} gm \Rightarrow g_0^{-1} g \in G_m$. То есть g и g_0 действуют одинаково $\iff$ они в одном классе смежности по G_m.
То есть имеется биекция между $Gm \to G/G_m$.
Если $|G|$ конечна, то $|Gm| = |G/G_m| = \frac{|G|}{|G_m|}$.
Другими словами $|G| = |G_m||Gm|$.

Example 9.5.

В случае D_4 на вершины квадрата, то $GA = \{A, B, C, D\}$ - 4, $G_A = \{id, S_{AC}\}$.
$G_{AC} = \{AC, BD\}$, $G_{AC} = \{id, S_{AC}, S_{BD}, r_\pi\}$.

Lemma 9.5. Лемма Бернсайда

Пусть G действует на M. Все конечно. $Fix(g) = \{m \in M \mid gm = m\}$.
Тогда количество орбит(M/G) действия $G = \frac{1}{|G|} \sum_g |Fix(g)|$.

Доказательство. $N = \{(g, m) \mid gm = m\}$. Посчитаем его размер двумя способами.

С одной стороны $N = \sum_g \{(g, m) | gm = m\} = \sum_g |Fix(g)|$.

С другой $N = \sum_m \{g\ gm = m\} = \sum_m |G_m|$

Итого $\sum_g |Fix(g)| = \sum_m |G_m| = |G| \sum_m \frac{1}{|Gm|}$.

То есть $\frac{1}{|G|} \sum_g |Fix(g)| = \sum_m \frac{1}{|Gm|}$.

Пусть есть орбита $|Gm| = k$. Дает в правую часть вклад $\frac{1}{k}$, и таких k. Следовательно правая часть это просто число орбит. $\square$

10 Лекция 10. Соавтор не придумал (соавтор в процессе додумки)

Example 10.1.

Пусть на плоскости есть правильный n-угольник. G - его группа симметрий - такие движения, которые переводят многоугольник в себя.
Какой порядок G?
Пусть вершины - $v_1, \dots, v_n$. G действует на множестве вершин.
Что такое орбита одной вершины? Это все вершины, так как можем повернуть на нужный угол. Значит длина орбиты n.
То есть порядок $|G|$ - $n * |G_{v_1}|$. Что такое стабилизатор v_1? Движения, сохраняющие v_1 на месте.
Пусть v_2 соседняя. $G_{v_1}v_2$ это v_2, v_n(так как v_2 соединена с v_1, а она остается на месте. Можем только ничего не сделать и отразить симметрично прямой через v_1). Значит $|Gv_1| = |G_{v_1}v_2||G_{v_1,v_2}| = 2$.
При этом движений, сохраняющих две точки кроме тождественного нет. Поэтому верно последнее равенство.
Итого $|G| = 2n$

Exercise 10.1.

Посчитать такие же группы для куба и тетраэдра.

Example 10.2. т. Бернсайда

Он позволяет считать варианты с точностью до изоморфизма.
Пример: Сколько графов на n вершинах? Если вершины помечены, то ответ $2^{\binom{n}{2}}$(любое ребро либо проведем, либо нет).
А если непомеченных(то есть с точностью до изоморфизма)? Это нерешенная задача...
Для $n = 3$ ответ 4. Они определяются количеством ребер. В общем случае примерно $\frac{2^{\binom{n}{2}}}{n!}$, но это не точно.

Example 10.3. Ожерелья

Рассмотрим ожерелья с n бусинами. Каждая бусина может быть черной или белой. Например $n = 12$. Сколько существует ожерелий

1. с точностью до поворотов
2. с точностью до поворотов и симметрий

Решение:

1. Рассмотрим M - ожерелья "прибитые к столу"(позиции фиксированы). $|M| = 2^{12}$. Действуем на неё поворотами $G = \langle\frac{\pi}{6}\rangle$. Хотим узнать количество орбит. Так как орбите соответствуют все ожерелья, равные с точностью до поворота.
Их $= \sum_g \frac{|Fix(g)|}{|G|} = \frac{1}{12}\sum_{k=0}^{11}|Fix(r^k)|$, где r - поворот.
$Fix(r^0) = M$ - все ожерелья сохраняются после тождественного преобразования.
$Fix(r)$ - такие расстановки, что $a_i = a_{i+1}$ - поворот на одно деление сохраняет расстановку. Таких ровно 2 - полностью черные/белые.
$Fix(r^2)$ - расстановки $a_{i+2} = a_i$ - их 4(фиксируем 2 первых элемента).
$Fix(r^3)$ - 8, $Fix(r^4)$ - 16.
$Fix(r^5)$ - 2. Потому что $(12, 5) = 1$, то есть это опять одноцветные ожерелья.
$Fix(r^6) - 64$, $Fix(r^7) - 2$, $Fix(r^8) - 16$, $Fix(r^9)$ - 8, $Fix(r^{10})$ - 4, $Fix(r^{11})$ - 2.
Итого $\frac{1}{12}(2^{12} + 2*4 + 4*2 + 8*2 + 16*2 + 64) = \frac{4224}{12} = 352$ - число ожерелий с точностью до поворотов.

10.1 Действия в теории групп

Definition 10.1. Изоморфизм действий

$G \curvearrowright M_1$, $G \curvearrowright M_2$ изоморфны, если существует биекция $M_1 \to M_2$, сохраняющее действие: $f(gm) = gf(m)$.

1. $G \curvearrowright G$ сдвигами: $f_g(h) = gh$, $f_g \in S(G)$.
Что такое орбита и стабилизатор. $Gg = \{gg_1 \,|\, g_1 \in G\} = G$, $G_g = \{e\}$. Такое действие называется **регулярным**(одна орбита и тривиальный стабилизатор). Любое регулярные изоморфно такому...
2. Пусть $H \leq G$. Тогда есть G/H - множество смежных классов. $G \curvearrowright G/H$. $g(g'H) \overset{\text{def}}{=} (gg')H$ - перестановка смежных классов.
$G(gH) = G/H$ по тем же причинам. А стабилизатор $G_{gH} = H$, если H - нормальна, иначе ... - упр.
Действия с одной орбитой называются **транзитивными**. Любое транзитивное действие изоморфно такому...
Любое действие $G \curvearrowright M$ изоморфно такому: $G \curvearrowright G/H_1 \cup G/H_2 \cup \ldots G/H_k$. H_k необязательно различные.
3. Действие сопряжениями. $G \curvearrowright G$: $g * g_1 = gg_1g^{-1}$.
Это действие: $(gh) * g_1 = ghg_1(gh)^{-1} = ghg_1h^{-1}g^{-1} = g * (hg_1g^{-1}) = g * (h * g_1)$.
Более того $\forall g$: f_g будет являться автоморфизмом(изоморфизм в себя):
$$f_g(xy) = gxyg^{-1} = gxg^{-1}gyg^{-1} = f_g(x)f_g(y)$$
Обозначение $g * x \overset{\text{def}}{=} {}^g x$.
Что такое орбита? $\{{}^g x \; g \in G\}$ - класс сопряженности элемента G(обозначаем $C(g)$).
Следствие: $|C(g)|$ - делитель $|G|$, так как это индекс стабилизатора.

$X_g = \{g \ : \ gxg^{-1} = x\} = \{g \ : \ gx = xg\} = C(x)$ - элементы, коммутирующие с x - централизатор x.

Можно также рассмотреть действие сопряжениями $H \curvearrowright G$, где $H \leq G$. Если H нормальная, то можем рассмотреть также $G \curvearrowright H$, так как сопряжение будет оставаться в H.

Можно рассмотретьи $G \curvearrowright$ подгруппы G.

Definition 10.2.

$H \leq G$. G действует сопряжениями на подгруппы, то стабилизатор $G_H = \{g : gHg^{-1} = H\} = N_G(H)$ - нормализатор H. (если $N_G(H) = G \Rightarrow H$ - нормальна). Это самая большая подгруппа, в которой H - нормальна.

Example 10.4.

Рассмотрим S_n, $H = \{x \mid x(1) = 1\}$ - стабилизатор 1 элемента. Что такое ${}^gH$. Это $\{y \mid y(g(1)) = g(1)\}$, то есть стабилизатор $g(1)$.

Exercise 10.2.

S_4, $H = \langle(123)\rangle$. Тогда
$C(123) = H$. $N_{S_4}(H) = S_3$.

Вопрос: $n \in \mathbb{N}$. Есть группа порядка n. Какие варианты у группы G?

Хотим описать с точностью до изоморфизма все группы порядка n.

Знаем: $g \ : ord(g) = n \Rightarrow |G| \,\vdots\, n$. Если $H \leq G \Rightarrow |G| \,\vdots\, |H|$.

Верно ли, что обратное верно? $|G| \,\vdots\, n \Rightarrow \exists g \; ord(g) = n$ - нет. $\exists\ H \leq G$, $|H| = n$ - тоже нет.

Theorem 10.1. Теорема Коши

Пусть $|G| \,\vdots\, p$, p-простое $\Rightarrow \exists g \; ord(g) = p$.

Доказательство. Рассмотрим $M = \{g_1 g_2 \dots g_p \mid g_1 g_2 \dots g_p = e\}$ - последовательности длины p с произведением e.

Хотим $g^p = e$, $g \neq e$. То есть хотим найти строчку $gg \dots g \in M$.

$g_1(g_2 \dots g_p) = e \iff (g_2 \dots g_p) g_1 = e$(умножаем все на g_1^{-1} слева, потом на g_1 справа). То есть M замкнута относительно циклического сдвига. То есть $\mathbb{Z}/p\mathbb{Z} \curvearrowright M$. $k(g_1 \dots g_p) = g_{k+1} \dots g_p g_1 \dots g_k$.

$|M| = |G|^{p-1} \,\vdots\, p$ - выбираем как угодно $p-1$, добавляем обратный к их произведению. Значит $|M| \,\vdots\, p$.

$\forall m \in M$ чему равна длина орбиты? Это делитель p, то есть либо 1 либо p.

M - объединение орбит. $|M| = \sum p + \sum 1$, значит количество орбит длины 1 делится на p.

То есть количество $g \ : g^p = e$ - делится на p. И их не 0, так как $e^p = e$. $\square$

Example 10.5.

$|G| = 35$, значит есть элементы g порядка 7 и h - 5. При этом $\{g^i h^k\} = G$, так как их ровно 35 различных.

Если $|G| \vdots n$. Существует подгруппа порядка n если $n = p^k$.

Definition 10.3. Силовская подгруппа

Пусть $|G| = n$, $v_p(n) = k$. Тогда подгруппа $P \leq G$, т.ч. $|P| = p^k$ называется силовской подгруппой.

Theorem 10.2. Теорема Силова

G - конечная

1. $\forall p \, \exists P \leq G$ - силовская p-подгруппа, p - простое
2. P_1, P_2 - силовские p подгруппы, тогда $\exists g \, : gP_1g^{-1} = P_2$
3. $P \leq G$, $|P| = p^l \Rightarrow \exists P'$ - силовская p подгруппка, т.ч. $P \leq P'$.
4. Количество силовский p-подгрупп делитель $|G|$, $\equiv 1(mod p)$.

Example 10.6.

Пусть $|G| = 35$. Существует H_5, H_7 - подгруппы порядка 5 и 7(1 теорема Силова или Коши).
Третья теорема говорит, что количество подгрупп порядка 5 - 1. Порядка 7 тоже.
В G элементов порядка 5 - 4 и 6 элементов порядка 7. 1 элемент порядка 1. Значит у остальных по теореме лагранжа порядок 35. То есть G - циклическая.

Доказательство. 1) Рассмотрим M - всевозможные подмножества G порядка p^k, где $k = v_p(|G|)$. Тогда $G \curvearrowright M$ сдвигами $(g * \{a_i\} = \{ga_i\})$.

Lemma 10.1.

Порядок M не делится на p.

Доказательство. $n = p^k l$, $|M| = \binom{n}{p^k} = \frac{n(n-1)\dots(n-(p^k-1))}{1\dots p^k}$.

$v_p(n) = v_p(p^k)$. Если $a < p^k$, то $v_p(a) = v_p(n-a) = min(v_p(n), v_p(a)) = v_p(a)$.

То есть в числителе p столько же, сколько в знаменателе. □

$|M|$ не делится на p, M - объединение орбит, значит $\exists m \, : Gm$ не делится на p.

То есть $|G_m| = |G|/|Gm|$ делится на p^k. Но в m всего p^k элементов(m_i-е). При этом $g \in G_m$ должен иметь вид $gm_1 = m_i \Rightarrow g = m_i m_1^{-1} \leq p^k$ вариантов для g. Значит $|G_m| \leq p^k$ элементов. Но тогда $|G_m| = p^k$.

Нашли силовскую подгруппу.

2) По 1 пункту существует P_1 - силовская порядка p^k. Пусть P_2 другая порядка p^m.

Рассмотрим $M = G/P_1$ - смежные классы. $P_2 \curvearrowright M$ сдвигами.

$|M| = l$ - не делится на p. Значит есть орбита длины, не делящаяся на p. То есть $\exists g \in G \, : |P_2 * gP_1|$ не делится на p. Но это делитель $|P_2| = p^m$. Значит орбита состоит из 1 элемента.

То есть

$$\forall h \in P_2\; hgP_1 = gP_1 \Rightarrow \forall h \in P_2\; hge \in gP_1 \Rightarrow h = gpg^{-1} \Rightarrow g^{-1}hg \in P_1,\, \forall h \in P_2 \Rightarrow {}^{g}P_2 \subset P_1$$

Если $|P_2| = p^k$, значит достигается равенство.

Заметим, что мы доказали $P_2 \leq gP_1g^{-1} = {}^{g}P_1$ - силовская p-подгруппа.

Мы использовали, что ${}^{g}H$ тоже подгруппа$(gxg^{-1}gyg^{-1} = gxyg^{-1} \in {}^{g}H)$.

3) $G \curvearrowright$ силовские подгруппы сопряжением. В нем одна орбита по 2 пункту. Следовательно количество силовских p подгрупп = длина орбиты = делитель $|G|$.

Пусть P одна из подгрупп. Рассмотрим $P \curvearrowright$ силовские подгруппы.

Длины орбит - дилители $|P|$ - либо 1 либо p. Докажем, что есть единственная орбита длины 1.

Ясно, что $PPP^{-1} = P$ - одна орбита длины 1. Пусть есть другая $PP'P^{-1} = P'$.

Это значит $P \leq N_G(P')$. $P' \leq N_G(P')$ - очевидно. Значит они силовские подгруппы в $N_G(P')$. Значит они там сопряжены. Но это не так, потому что P' нормальна в $N_G(P')$. Противоречие! Других орбит длины 1 нет. $\square$