Линейная Алгебра (Лекции)

Игорь Энгель

10 июня 2020 г.

Содержание

0. Конкспект по лекциям

Это конспект сгруппированный по лекциям, потому-что так его удобнее писать. **Ошибки в этой версии конспекта не исправляются**. Этот конспект может обновляться чуть раньше основного.

1. Лекция 1

Замечание.

В $\mathbb{R}$ существуют неприводимые многочлены с $\deg p(x) \geqslant 2$.

Это неудобно.

Хотим найти поле содержащие $\mathbb{R}$ в котором таких многочленов нет.

***Определение* 1.1.** Пусть K, L - поля. K - подкольцо внутри L. Тогда L называется расширением поля K.

Рассмотрим многочлен $x^2 + 1$. Назовём его корень i.

1. $i \in L$
2. $\mathbb{R} \subset L$
3. Тогда $a + bi \in L$ если $a, b \in \mathbb{R}$

Так-же поле L содержит выражения вида $a + bi + ci^2$, но так-как i^2 по определению равен -1. Значит, такие выражения сводятся к $a' + bi$. Аналогично для больших степеней.

Рассмотрим операции поля:

$$(a + bi) + (c + di) = (a + c) + (b + d)i.$$

$$(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i = a' + b'i.$$

Значит, эти выражения задают подкольцо в L.

Возьмём множество пар вещественных чисел $\mathbb{R}^2$.

Введём на нём сложение: $\langle a, b\rangle + \langle c, d\rangle = \langle a + c, b + d\rangle$.

Введём умножения: $\langle a, b\rangle \cdot \langle c, d\rangle = \langle ac - bd, ad + bc\rangle$.

Заметим, что сущетсвует корень многочлена $x^2 + 1 \in \mathbb{R}^2[x]$: $\langle 0, 1\rangle \cdot \langle 0, 1\rangle = \langle 0 - 1, 0 + 0\rangle = \langle -1, 0\rangle$.

Теорема 1.1. $\mathbb{R}^2$ с этими операциями - кольцо.

Доказательство. $\mathbb{R}^2$ - абелева группа, как произведение абелевых групп.

TODO:

Дистрибутивность:

Ассоциативность:

Коммутативность:

Единица: □

***Определение* 1.2.** Полем комплексных чисел $\mathbb{C}$ называется $\langle \mathbb{R}^2, +, \cdot \rangle$

Элементы $\mathbb{C}$ записываются как $a + bi$ (соответсвуют элементам вида $\langle a, b\rangle$)

Теорема 1.2. $\mathbb{C}$ - поле

Доказательство. Найдём обратный элемент для $a + bi$.

$$(a+bi)(a-bi) = a^2 - b^2i^2 = a^2 + b^2.$$

Если $a + bi \neq 0$, то $a^2 + b^2 \neq 0$.

Поделим:

$$\frac{(a+bi)(a-bi)}{a^2+b^2} = 1.$$

Значит, $\frac{a-bi}{a^2+b^2}$ - обратный к $a + bi$. $\square$

Замечание. В $\mathbb{C}$ любой вещественный многочлен степени 2 раскладывается на линейные множители.

Доказательство. Рассмотрим многочлен $x^2 + bx + c$. $b, c \in \mathbb{R}$.

Тогда его корни имеют вид

$$x_{1,2} = \frac{-b \pm \sqrt{b^2 - 4c}}{2}.$$

Если $D = b^2 - 4c \geqslant 0$, то у него есть вещественный корень.

Если $D < 0$, то вещественных корней нет.

Тогда $D = -1 \cdot |D|$.

$$x_{1,2} = \frac{-b \pm \sqrt{(-1)|D|}}{2} = \frac{-b \pm \sqrt{|D|}\sqrt{-1}}{2} = \frac{-b \pm |D|i}{2}.$$ $\square$

Свойства. Пусть $z = a + bi \in \mathbb{C}$.

$a = \operatorname{Re} z$ - вещественная часть

$b = \operatorname{Im} z$ - мнимая часть

$\overline{z} = a - bi$ - комплексно-сопряжённое к z число

$|z| = \sqrt{a^2 + b^2}$ - модуль z

***Определение* 1.3.** R_1, R_2 - кольца. $f : R_1 \to R_2$ называется гомоморфизмом колец, если

1. $f(a + b) = f(a) + f(b)$
2. $f(a \cdot b) = f(a) \cdot f(b)$
3. $f(1) = 1$ - если кольцо с единицей.

***Определение* 1.4.** Если $f : R_1 \mapsto R_2$ гомоморфизм колец и биекция, то f - изоморфизм колец.

Утверждение 1.3. Комплексное сопряжения - изоморфзим $\mathbb{C} \mapsto \mathbb{C}$.

Доказательство.

$$\overline{(a+bi)+(c+di)} = \overline{(a+c)+(b+d)i} = (a+c) - (b+d)i.$$

$$\overline{a+bi} + \overline{c+di} = (a-bi) + (c-di) = (a+c) - (b+d)i.$$

$$\overline{(a+bi)(c+di)} = \overline{(ac-bd)+(ad+bc)i} = (ac-bd)-(ad+bc)i.$$
$$\overline{a+bi}\cdot\overline{c+di} = (a-bi)(c-di) = (ac-(-b)(-d)) + (a(-d)+(-b)c)i = (ac-bd)-(ad+bc)i.$$
$$\overline{1+0i} = 1+0i.$$
□

Лемма. $\psi : R_1 \mapsto R_2$ гомоморфизм колец.

$g(x) \in R_1[x]$ - многочлен. $\lambda \in R_1$ - корень $g(x)$

Построим многочлен $\psi(g) = \psi(a_0) + \psi(a_1)x + \ldots \psi(a_n)x^n$

Тогда $\psi(\lambda) \in \mathbb{R}_2$ - корень $\psi(g)$

Доказательство.
$$a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda^n = 0.$$
$$\psi(a_1\lambda + a_2\lambda + \ldots + a_n\lambda^n) = \psi(0) = 0.$$
$$\psi(a_1\lambda + a_2\lambda^2 + \ldots + a_n\lambda) = \psi(a_1)\psi(\lambda) + \psi(a_2)\psi(\lambda)^2 + \ldots + \psi(a_n)\psi(\lambda)^n = \psi(g)(\psi(\lambda)) = 0.$$
□

Утверждение 1.4. Любой изоморфизм $\varphi : \mathbb{C} \mapsto \mathbb{C}$ такой, что $\varphi|_{\mathbb{R}} = \mathrm{id}$ либо $\varphi = \mathrm{id}$, либо φ - комплексное сопряжение.

Доказательство. $\varphi(a+bi) = \varphi(a) + \varphi(b)\varphi(i) = a + b\varphi(i)$.

$\varphi(x^2+1) = x^2+1$.

Значит $\varphi(i)$ тоже корень x^2+1. Значит, либо $\varphi(i) = i$, либо $\varphi(i) = -i$. □

Утверждение 1.5. $|z| = \sqrt{z\overline{z}}$

Доказательство. $z\overline{z} = (a+bi)(a-bi) = a^2+b^2$. □

Утверждение 1.6. $|z_1z_2| = |z_1||z_2|$

Доказательство. $|z_1z_2|^2 = z_1z_2 \cdot \overline{z_1z_2} = z_1\overline{z_1}z_2\overline{z_2} = |z_1|^2|z_2|^2$. □

***Определение* 1.5.** Аргументом $z = a+bi \neq 0$ называется угол между вещественной прямой и радиус-вектором точки задаваемой этим числом на комплексной плоскости. И обозначается $\operatorname{Arg} z \in \mathbb{R}/(2\pi\mathbb{Z})$.

Утверждение 1.7. $z_1, z_2 \neq 0$. $\operatorname{Arg} z_1z_2 = \operatorname{Arg} z_1 + \operatorname{Arg} z_2$.

Доказательство. $\operatorname{Arg} \frac{z_1}{|z_1|} = z_1$, значит можно доказывать только для элементов с $|z| = 1$.

$|z_1| = |z_2| = 1$. Пусть $\varphi = \operatorname{Arg} z_1$, $\psi = \operatorname{Arg} z_2$.

Тогда $z_1 = \cos\varphi + i\sin\varphi$, $z_2 = \cos\psi + i\sin\psi$.

$$z_1z_2 = (\cos\varphi\cos\psi - \sin\varphi\sin\psi) + i(\cos\varphi\sin\psi + \cos\psi\sin\varphi) = \cos(\varphi+\psi) + i\sin(\varphi+\psi).$$
□

Доказательство. Факт: Пусть есть изометрия плоскости у которой ести единственная неподвижная точка, то эта изометрия - поворот.

Введём расстояние между комплексными числами - $\rho(z_1, z_2) = |z_1 - z_2|$. Оно соответсвует обычному расстоянию на плоскости.

$|z_1| = |z_2| = 1$.

При $z_1 = 1$ тривиально, предположим что $z_1 \neq 1$.

Рассмотрим отображения $x \mapsto z_1 x$.

Докажем что это изометрия: $|z_1 x - z_1 y| = |z_1(x-y)| = |z_1||x-y| = |x-y|$.

Заметим, что $z_1 x = x \iff x(z_1 - 1) = 0 \iff x = 0$.

Значит, заданное отображение - поворот вокруг начала координат. При этом, так-как $z_1 \cdot 1 = z_1$, то это поворот на угол $\operatorname{Arg} z_1$. Значит, $\operatorname{Arg} z_1 x = \operatorname{Arg} z_1 + \operatorname{Arg} x \implies \operatorname{Arg} z_1 z_2 = \operatorname{Arg} z_1 + \operatorname{Arg} z_2$. □

***Определение* 1.6.** Тригонометрическая форма записи комплексного числа $z \neq 0$ с аргументом $\varphi = \operatorname{Arg} z$:

$$a + bi = z = |z|\frac{z}{|z|} = |z|\left(\cos\varphi + i\sin\varphi\right) = |z|e^{i\varphi}.$$

Свойства. $z_1 = r_1 e^{i\varphi_1}$, $z_2 = r_2 e^{i\varphi_2}$.

$z_1 z_2 = r_1 r_2 e^{i\varphi_1} e^{i\varphi_2} = r_1 r_2 e^{i(\varphi_1 + \varphi_2)}$

Замечание.

$$e^x = 1 + x + \frac{x^2}{2!} + \dots \frac{x^j}{j!} + \dots.$$

$$e^{ix} = 1 + ix + \frac{-x}{2!} + \frac{-ix}{3!} + \frac{x}{4!} + \dots.$$

При чётных степенях:

$$1 - \frac{x^2}{2} + \frac{x^4}{4!} + \dots + (-1)^k \frac{x^{2k}}{2k!} = \cos x.$$

При нечётных:

$$ix - \frac{ix^3}{3!} + \dots + (-1)^k \frac{ix^{2k+1}}{(2k+1)!} = i\sin x.$$

$$e^{ix} = \cos x + i\sin x.$$

Теорема 1.8. В комплексных числах есть корни уравнения вида $x^n = a$

Доказательство. Если $a = 0$, то сущетсвует единственный корень кратности n - $x = 0$.

Предположим что $a \neq 0$.

$$a = re^{i\varphi}$$

$$x = se^{i\varphi}.$$

$$x^n = s^n e^{in\alpha}.$$

$$s^n = r \implies s = \sqrt[n]{r}.$$

$$n\alpha = \varphi + 2\pi k \implies \alpha = \frac{\varphi}{n} + \frac{2\pi}{n}k.$$

$$x_k = \sqrt[n]{r} e^{i\left(\frac{\varphi}{n} + \frac{2\pi}{n}k\right)}.$$

Таких решений n штук, значит это все решения уравнения. □

Пример. Рассмотрим уравнение $x^n = 1 = 1 \cdot e^0$.

Тогда $\varepsilon_k = e^{i \cdot \frac{2\pi k}{n}}$.

***Определение* 1.7.** R - кольцо, $x \in R$ удовлетворяющий $x^n = 1$. Тогда x - корнеь степени n из единицы.

***Определение* 1.8.** K - поле, тогда $\varepsilon \in K$ называется первообразным корнем степени n из единицы, если $\operatorname{ord} \varepsilon = n$.

Замечание. Все первообразные корни степени n из единицы в $\mathbb{C}$ имеют вид ε_k, где k взаимно-просто с n.

Теорема 1.9 (Основная теорема алгебры)**.** Любой многочлен $p(x) \in \mathbb{C}[x]$ степени хотя-бы один, имеет хотя-бы один корень в $\mathbb{C}$.

Без доказательства.

***Определение* 1.9.** Поле K называется алгебраически замкнутым, если у любього многочлена $p(x) \in K[x]$ степени хотя-бы один есть корень в K.

Лемма. K - алгебраически замкнутое поле. Тогда многочлен $p(x) \in K[x]$ имеет ровно $\deg p(x) \geqslant 1$ корней с учётом кратности.

Доказательство. Пусть $n = \deg p$.

Если $n = 1$, то есть ровно один корень.

Пусть $n > 1$, так-как K замкнуто, то существует корень λ.

Тогда $p(x) = p'(x)(x - \lambda)$.

По индукции у $p'(x)$ ровно $n - 1$ корень с учётом кратности, и один корень у $x - \lambda$. Итого, n корней. □

Замечание. Любой многочлен $f(x) \in \mathbb{C}[x]$ представляется в виде

$$f(x) = c(x - \lambda_1) \dots (x - \lambda_n) \, .$$

Лемма. Если $\lambda \in \mathbb{C}$ - корень $p(x) \in \mathbb{R}[x]$, то $\overline{\lambda}$ - тоже корень.

Доказательство. Заметим, что $p(x) = \overline{p}(x)$. Значит, их корни совпадают. Но $\overline{\lambda}$ - корень $\overline{p}(x)$. □

Утверждение 1.10. Если $p(x) \in \mathbb{R}[x]$ неприводимый, то либо $p(x) = c(x - \lambda)$, либо $p(x) = x^2 + bx + c$ и $b^2 - 4c < 0$.

Доказательство. То, что эти многочлены неприводимы тривиально.

Предположим что p неприводимо и $\deg p > 2$.

Заметим, что p имеет комплексный корень λ. Тогда $p \, \vdots \, (x - \lambda)$ и $p \, \vdots \, (x - \overline{\lambda})$.

$\lambda \neq \overline{\lambda}$, так-как p неприводим.

Тогда $p(x) = p'(x)((x - \lambda)(x - \overline{\lambda})) = p'(x) \left(x^2 - \lambda x - \overline{\lambda} x + \lambda\overline{\lambda}\right) = p' \left(x^2 - 2 \operatorname{Re} \lambda x + |\lambda|^2\right)$.

Предположим что $p(x) \not\vdots \, (x - \lambda)(x - \lambda')$ в вещественных.

Тогда они взаимно простые. Тогда

$$a(x)p(x) + b(x)(x - \lambda)(x - \overline{\lambda}) = 1.$$

Но $p(\lambda) = 0$ и второе слагаемое тоже равно нулю. Противоречие.

Значит, $p' \in \mathbb{R}[x]$, и p приводим. Противоречие, значит неприводимых многочленов степени больше 2 не существует. $\square$

2. Лекция 2

Пример Гомоморфизмы колец.

1. $\overline{z} : \mathbb{C} \mapsto \mathbb{C}$
2. $\mathrm{id} : R \mapsto R$
3. $\mathbb{Z} \mapsto \mathbb{Z}/n$
4. $\mathbb{Z}/nm \mapsto \mathbb{Z}/n$
5. $a \in R$, $\varphi : R[x] \mapsto R$, $\varphi(f) = f(a)$
6. $g(x) \in R[x]$, $\varphi : R[x] \mapsto R[x]$. $\varphi(f) = f(g(x))$
7. $g \in C[0,1]$, $\varphi : C[0,1] \mapsto C[0,1]$, $\varphi(f) = f(g(x))$.

Утверждение 2.1.

R, S - кольца.

Тогда,

$$\forall \psi : R \mapsto S \quad \forall \lambda \in S \quad \exists! \varphi : R[x] \mapsto S \quad \begin{cases} \forall r \in R \quad \varphi(r) = \psi(r) \\ \varphi(x) = \lambda \end{cases} .$$

Доказательство. Пусть есть $\psi : R \mapsto S$. Построим $\varphi : R[x] \mapsto S$, такое, что $\varphi|_R = \psi$ и $\varphi(x) = \lambda$.

$$\varphi(a_0 + a_1 x + \ldots + a_n x^n = \varphi(a_0) + \varphi(a_0)\varphi(x) + \ldots + \varphi(a_n)\varphi(x). = \psi(a_0) + \psi(a_1)\lambda + \ldots + \psi(a_n)\lambda^n$$

Значит, такой гомоморфизм единственнен. Существование доказывается проверкой, что это формула - гомоморфизм. Заметим, что формула эквивалентна гомоморфизму подстановки (из примеров). □

Утверждение 2.2.

S - кольцо.

$$\exists! \varphi : Z \mapsto S \quad .$$

Доказательство.

$$\varphi(1) = 1_S.$$

$$\varphi(n) = \varphi(\underbrace{1 + 1 + \ldots + 1}_{n}) = n \cdot 1_S.$$

Существование проверяется тривиально. □

***Определение* 2.1.**

Пусть R - кольцо. Тогда $\exists! \varphi : \mathbb{Z} \mapsto R$

Тогда $\exists n \in \mathbb{N} \cup \{0\} \quad \mathrm{Ker}\, \varphi = n\mathbb{Z}$.

Число $\mathrm{char}\, R := n$ называется характеристикой кольца R.

Пример.

1. $\mathrm{char}\, \mathbb{Z} = 0$

2. $\forall R \quad \mathbb{Z} \subset R \implies \operatorname{char} R = 0$

3. $\operatorname{char} \mathbb{Z}/n = n$

4. $\operatorname{char} \mathbb{Z}/n[x] = n$

Теорема 2.3.
R - область целостности.

Тогда, либо $\operatorname{char} R = 0$, либо $\operatorname{char} R$ - простое.

Доказательство. Пусть $\operatorname{char} R = n_1 n_2$.

Тогда $\varphi(n_1)\varphi(n_2) = \varphi(n) = 0$, но $n_1 \not\vdots\, n$ и $n_2 \not\vdots\, n$, значит n_1, n_2 - делители нуля. □

***Определение* 2.2.**
R - кольцо.

Производной $\frac{d}{dx} : R[x] \mapsto R[x]$ называется

$$\frac{d}{dx}(a_0 + a_1 x + \ldots + a_n x^n) = a_1 + 2a_2 x + \ldots + n a_n x^n.$$

Свойства.

- $(\lambda \in R)' = 0$
- $(f + g)' = f' + g'$
- $(fg)' = f'g + fg'$
- $(f^n)' = nf'f^{n-1}$
- $(f \circ g)' = g'(f' \circ g)$

Доказательство. Сидим и раскрываем скобки. **МНЕ ЛЕНЬ**. □

Теорема 2.4.
Пусть K - поле. $f, q \in K[x]$, $\deg q \geqslant 1$, при этом q неприводим. Пусть $q^\ell | f$, $\ell \geqslant 1$. Тогда $q^{\ell-1} | f'$.

Если $\operatorname{char} K = 0$ ил $\operatorname{char} K > \deg f$, то если $q^{\ell+1} \nmid f$ то $q^\ell \nmid f'$.

Доказательство.

$$f = q^\ell \cdot g(x).$$

$$f' = \ell q' g^{\ell-1} g + g' q^\ell = q^{\ell-1} \left(\ell q' g + g' q\right).$$

Для второго утверждения надо доказать что $(\ell q' g + g' q) \not\vdots\, q \iff q' g \not\vdots\, q$.

Заметим, что $\deg q' < \deg q$, так-что если $\ell q' \vdots\, q$, то $\ell q' = 0$.

Если $\operatorname{char} K = 0$, то $\ell_K \neq 0$. Аналогично, мы знаем что $\ell \leqslant \deg f$, иначе f не могло-бы делиться на q^ℓ. Значит $\ell_K \neq 0$.

Мы знаем что q не константа, значит $q' \neq 0$ если $\operatorname{char} K = 0$.

Знаем, что $\deg q \leqslant \deg f < \operatorname{char} K$, значит доп-множители в производной не 0 в K, значит сущесвует ненулвой коэффициент. **TODO:** Почему $s \cdot a_s \neq 0_K$? □

Следствие.

Если $\operatorname{char} K = 0$ или $\operatorname{char} k > \deg f$, то λ корень f кратности $\ell \geqslant 1$ тогда и только тогда, когда λ - корень f' кратности ℓ.

Следствие.

Если $\operatorname{char} K = 0$ или $\operatorname{char} k > \deg f$, то есть простой алгоритм переводящий $f = p_1^{\alpha_1} \dots p_k^{\alpha_k}$ в $\hat{f} = p_1 \dots p_k$.

Доказательство. Заметим, что $(f, f') = p_k^{\alpha_1 - 1} \dots p_k^{\alpha_k - 1}$, значит $\frac{f}{(f,f')} = p_1 \dots p_k$. □

Теорема 2.5 (Метод Ньютона)**.**

Есть $f \in \mathbb{R}[x]$, хотим найти корень x_0.

Возьмём произвольную точку x_1, проверим является-ли она корнем. Если нет, то рассмотрим значение аппроксимации многочлена в окретсности x_1: $\hat{f}(x) = f(x_1) + f'(x_1)(x - x_1)$.

Найдём корень $\hat{f}$:

$$f(x_1) + f'(x_1)(x - x_1) = 0 \iff x_1 - \frac{f(x_1)}{f'(x_1)}.$$

Возьмём этот корень как новую точку x_2.

$$x_i = x_{i-1} = -\frac{f(x_{i-1})}{f'(x_{i-1})}.$$

Теорема 2.6.

Пусть $f \in \mathbb{R}[x]$ не имеет кратных корней.

Тогда $\exists \delta > 0 \quad \forall x_1 \quad |x_1 - x_0| < \delta \implies \lim\limits_{i \to \infty} x_i = x_0$

Утверждение 2.7.

Пусть $x_0 \in K$, тогда $\forall f \in K[X] \quad f = a_0 + a_1(x - x_0) + \ldots + a_n(x - x_0)^n$.

Если $\operatorname{char} K = 0$ или $\operatorname{char} K > i$, то $a_i = \frac{f^{(i)}(x_0)}{i!}$ (условие на хар-ку нужно для обратимости факториала).

3. Лекция 3

Прастите. Я задалбался.

4. Лекция 4

***Определение* 4.1.**

Поле рациональных функций: $K(x) = Q(K[x])$.

Утверждение 4.1.

$\frac{f}{g} \in K(x)$. $\exists! u, v \in K[x]$ т. ч:

1. $(u, v) = 1$
2. старший коэффициент v - 1
3. $\frac{f}{g} = \frac{u}{v}$

Доказательство. Существование:

Пусть $d = (f, g)$.

Пусть $\hat{u} = \frac{f}{d}$, $\hat{v} = \frac{g}{d}$.

Тогда $(\hat{u}, \hat{v}) = 1$ и $\frac{f}{g} = \frac{\hat{u}}{\hat{v}}$.

Пусть c - старшний коэффицент $\hat{v}$.

Тогда $v = c^{-1}\hat{v}$, $u = c^{-1}\hat{u}$.

Единственность:

Пусть $\frac{u_1}{v_1} = \frac{u_2}{v_2}$, при этом $(u_1, v_1) = 1$ и $(u_2, v_2) = 1$.

Тогда $v_2 u_1 = u_2 v_1$. Заметим, что $v_1 \vdots v_2$ и $v_2 \vdots v_1$.

Значит, $v_1 = c v_2$.

Так-как старшие коэффициенты равны 1, $c = 1$ и $v_1 = v_2$, а значит и $u_1 = u_2$. □

Лемма.

$\frac{r_1}{g_1}$, $\frac{r_2}{g_2}$ - правильные дробе ($\deg r < \deg g$).

Тогда $\frac{r_1}{g_1} + \frac{r_2}{g_2}$ - правильная дробь.

Доказательство.

$$\frac{r_1 g_2 + r_2 g_1}{g_1 g_2} = \frac{r_3}{g_3}.$$

$$\deg r_3 \leqslant \max(\deg r_1 g_2, \deg r_2 g_1) < \deg g_1 g_2 = \deg g_3.$$

□

Утверждение 4.2.

$\forall \frac{f}{g} \in K(x) \quad \exists! h \in K[x], \frac{r}{g_1} \in K(x) \quad \frac{f}{g} = h(x) + \frac{r}{g_1}, \deg r < \deg g_1$

Доказательство. Существование:

$$f = gh + r.$$

$$\frac{f}{g} = h + \frac{r}{g}.$$

Единственность:

Пусть $h_1 + \frac{r_1}{g_1} + h_2 + \frac{r_2}{g_2}$.

Тогда $h_1 - h_2 = \frac{r_2}{g_2} - \frac{r_1}{g_1}$. Значит, $h_1 - h_2$ - правильная дробь. Но единственная прваильная дробь из оригинального кольца многочленов - 0. □

.

***Определение* 4.2** (Простейшая дробь)**.**
Пусть $p \in K[x]$, p - неприводимый.

Простейшей дробью называется $\frac{r}{p^\alpha}$, где $\deg r < \deg p$, $\alpha \in \mathbb{N}$.

Лемма (О разложении по основанию)**.**
Пусть $r, p \in K[x]$, $\deg p \geqslant 1$.

Тогда существует разложение $r(x) = a_0(x) + a_1(x)p + \ldots + a_k(x)p^k$, где $\deg a_i < \deg p$.

Доказательство. Заметим, что $r = g \cdot p + a_0$.

Остальные коэффициенты можно получить разложив g:

$$g = a_1 + a_2 p + \ldots + a_k p^{k-1}.$$
$$r = a_0 + a_1 p + \ldots + a_k p^k.$$
□

Утверждение 4.3.
Пусть $\frac{f}{p^\alpha}$ - правильная дробь.

Тогда существует разложение $\frac{f}{p^\alpha} = \sum\limits_{j=1}^{k} \frac{r_j}{p^j}$, $\forall j \quad \deg r_j < \deg p$.

Доказательство.

$$\frac{f}{p^\alpha} = \frac{\sum\limits_{j=1}^{k} p^{k-j} r_j}{p^k}.$$

Существование:

Пусть $k = \alpha$.

Тогда r_j - коэффициенты из разложения f по основанию p. □

Лемма.
$\frac{f}{g}$ - правильная дробь, $g = g_1 g_2$, $(g_1, g_2) = 1$.

Тогда существует единственное разложение $\frac{f}{g} = \frac{h_1}{g_1} + \frac{h_2}{g_2}$ (все дроби правильные).

Доказательство.

$$f = h_1 g_2 + h_2 g_1.$$

Такие уравнения решаются аналогично диофантовым в целых числах.

Пусть нашли какое-то решение $\tilde{h_1}, \tilde{h_2}$. Тогда можем найти другое решение h_2 как остаток от деления $\tilde{h_2}$ на g. Тогда $\deg h_2 < \deg g$.

Найдём соответствующие h_1:

$$h_1 g_2 = h_2 g_1 - f.$$

$$\deg h_1 + \deg g_2 < \deg g_1 + \deg g_2 \implies \deg h_1 < \deg g_1.$$

Все отсальные решения уравнения имеют слишком большую степень. □

Теорема 4.4 (О разложении на простейшие)**.**
Пусть $\frac{f}{g} \in K(x)$. Тогда $\exists! h, p_1, \ldots, p_k, r_{ij} \in K[x] \quad \exists! \alpha_1, \ldots, \alpha_n \quad 1 \leqslant i \leqslant k, 1 \leqslant j \leqslant \alpha_i, \frac{f}{g} = h(x) + \sum \frac{r_{ij}}{p_i^j}, \deg r_{ij} < \deg p_i, p_i$ - неприводимые, старший коэффицент p_i - 1, $r_{i\alpha_i} \neq 0$,

Доказательство.

$$\frac{f}{g} = h(x) + \frac{r}{g}.$$

$$g = p_1^{\alpha_1} \dots p_k^{\alpha_k}.$$

Возьмём $g_1 = p^\alpha$

Предположим, что g имеет старший коэффициент 1, как и все p_i (несложно сделать).

Тогда

$$\frac{r}{g} = \frac{h_1}{p_1^{\alpha_1}} + \frac{h_2}{p_2^{\alpha_2} \dots p_k^{\alpha_k}}.$$

По индукции, всё разложится на дроби.

Разложим дробь по основанию:

$$\frac{r}{g} = \sum_{j=1}^{\alpha_1'} \frac{r_{1j}}{p_1^j} + \frac{h_2}{p_2^{\alpha_2} \dots p_k^{\alpha_k}}.$$

Где α_1' - максимальное число, такое что $r_{1\alpha_1'} \neq 0$.

Раскладывая по индукции, получим нужное разложение.

Единственность h следует из правильности суммы.

Без ограничения общности, пусть $\frac{f}{g}$ - неприводимая дробь, и старший коэффицент g - 1.

Тогда $g = p_1^{\alpha_1'} \dots p_k^{\alpha_k'}$.

TODO: я запутался □

Пример.

Простейшие дроби в $\mathbb{C}$ - $\frac{c}{(x-\lambda)^\alpha}$, $c, \lambda \in \mathbb{C}$

Простейшие дроби в $\mathbb{R}$ - $\frac{c}{x-\lambda}$, $c, \lambda \in \mathbb{R}$, $\frac{Ax+B}{(x^2+ax+b)}$, $A, B, a, b \in \mathbb{R}$, $b^2 < 4a$.

Разложим $\frac{1}{x^n-1}$:

$$1 = \sum_{i=1}^{n} \frac{x^n - 1}{n\varepsilon_i^{n-1}(x - \varepsilon_i)}.$$

$$\frac{1}{x^n - 1} = \sum_{i=1}^{n} \frac{1}{n\varepsilon^{n-1}(x - \varepsilon_i)} = \sum_{i=1}^{n} \frac{\varepsilon_i}{n(x - \varepsilon_i)}.$$

5. Лекция 5

***Определение* 5.1.**

Система линейных (алгебраичех) уравнений - сисетма условий вида

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ a_{21}x_1 + \ldots + a_{2n}x_n = b_2 \\ \vdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_n \end{cases}$$

Где $a_{ij}, b_i \in R$, где R - кольцо.

x_i называются переменными.

Решение системы: $\{(x_1, \ldots, x_n) \mid x_i \in R$ и выполнены все условия системы$\}$.

Если у нас есть система, можем взять два любых уравнения E_i, E_j из неё, взять два коэффициента $\lambda, \mu \in R$, и получить новое уравнение $\lambda E_i + \mu E_j$. Каждый элемент из решения системы так-же удовлетворяет этому уравнению.

***Определение* 5.2.**

Две системы называются равносильными, если равны (как множества) их решения.

Лемма.

Пусть есть два уравнения из системы E_i, E_j, тогда если заменить E_j на $E_j + \lambda E_i$, $\lambda \in R$, то новая система будет равносильна.

Доказательство. Добавим в систему уравнение $E_j + \lambda E_i$. Любое решение E_i, E_j является решением этого уравнения. Удалим уравнение E_j, могли появиться новые решениея. Но исчезунть не могли.

Повторим процесс в обратную сторону, заменив $E_j + \lambda E_i$ на $E_j + \lambda E_i - \lambda E_i = E_j$, так-как исчезнуть решения не могли, системы равносильны. □

Лемма.

Заменой строк местами можно получить равносильную систему

Лемма.

Если уравнение E_i домножить на $\lambda \in R^*$, получиться равносильная система.

***Определение* 5.3.**

Матрицей с коэффициентами в R размерности $m \times n$ называется таблица из $m \times n$ из элементов R. Их можество обозначается $M_{m\times n}(R)$.

***Определение* 5.4.**

Матрица $m \times n$

$$\begin{bmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ a_{m1} & a_{m2} & \ldots, a_{mn} & \end{bmatrix}$$

Называется матрицей системы

TODO: расширенная

5.1. Метод Гаусса

Если $a_{11} \neq 0$ (в поле), прибавив первую строку системы к $i > 1$-й с коэффициентом $-\frac{a_{i1}}{a_{11}}$ можно убрать вхождение x_1 в строку i.

Если $\exists i \quad a_{i1} \neq 0$, можно поменять её местами с первой строкой, и применить предыдущее преобразование.

Если $\forall i \quad a_{i1} = 0$, то можно «забыть» про первый столбец матрицы.

***Определение* 5.5.**

Элемент a_{ij} называется главным элементом строки i матрицы A, если он первый ненулевой элемент в этой строке.

***Определение* 5.6.**

Матрица A имеет ступенчатый вид, если $\forall i \quad$ строка i состоит из нулей, либо позиция главного элемента строки i строго больше позиции главного элемента строки $i-1$.

Теорема 5.1.

Любую матрицу над полем K можно при помощи элементарных преобразований привести к равносильной ей ступенчатой, такой, что главный коэффициент в каждой не нулевой строке равен 1 а над каждым главным элементом стоят нули.

Рассмотрим расширеную матрицу системы $(A|b)$. Привдём её к равносильной ступенчатой методом Гаусса.

Рассмотрим последнее ненулевое уравнение в такой системе. Пусть оно имеет вид $x_s + a_{s+1}x_{s+1} + \ldots + a_m x_m = b \implies x_s = b - \sum\limits_{i=s+1}^{m} a_i x_i$.

Может быть ситуация, когда главный элемент является частью подматрицы b. Тогда у системы нет решений. В остальных случаях есть.

***Определение* 5.7.**

Зависимые переменные - переменные, которые в приведённой матрице соответствуют главным элементам.

Остальные переменные называются независимыми.

Лемма.

Зависимые переменные однозначно выражается через независимые.

Пример Задача интерполяции.

Хотим найти $f(x) = \lambda_0 + \ldots + \lambda_{n-1}x^{n-1}$, такой, что $f(x_i) = a_i$, $\lambda_i, x_i, a_i \in K$, $x_i \neq x_j$.

$$\lambda_0 + \lambda_1 x_1 + \lambda_2 x_1^2 + \ldots + \lambda_{n-1}x_1^{n-1} = a_1$$
$$\vdots$$

Её матрица:

$$\begin{bmatrix} 1 & x_1 & x_1^2 & \ldots & x_1^{n-1} \\ \vdots & \vdots & \vdots & \vdots & \vdots \\ 1 & x_n & x_n^2 & \ldots & x_n^{n-1} \end{bmatrix}$$

Решение методом Гаусса - $\mathcal{O}(n^3)$, формулой интерполяции - $\mathcal{O}(n^2)$.

Пример Pagerank.

Пусть есть орграф G символизирующий набор страниц ссылающихся друг на друга.

Хотим каждой вершине сопоставить $w_i = \sum\limits_{j \to i} \frac{1}{\text{outdeg}(j)} w_j$.

$\forall i \quad w_i = 0$ - точно решение. Есть-ли другие?

5.2. Операции над матрицами

***Определение* 5.8.**
Пусть $A, B \in M_{m\times n}(R)$, то $\exists C \in M_{m\times n}(R) \quad C = A + B$. При этом, $C_{ij} = A_{ij} + B_{ij}$.

***Определение* 5.9.**
Пусть $A \in M_{m\times n}(R)$, $\lambda \in R$. Тогда $\exists \lambda A \in M_{m\times n}(R) \quad (\lambda A)_{ij} = \lambda A_{ij}$.

Свойства.

1. $M_{m\times n}(R)$ - абелева группа по сложению
2. $A, B \in M_{m\times n}(R)$, $\lambda \in R$. $\lambda(A + B) = \lambda A + \lambda B$.
3. $A \in M_{m\times n}(R)$, $\lambda, \mu \in R$, $(\lambda + \mu)A = \lambda A + \mu A$.
4. $A \in M_{m\times n}(R)$, $\lambda, \mu \in R$, $(\lambda\mu)A = \lambda(\mu A)$.
5. $1A = A$.

Замечание.

$$\begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} \in R^n = M_{n\times 1}(R)$$

$$(a_1, \dots, a_n) \in M_{1\times n}(R)$$

***Определение* 5.10.**

$$(a_1, \dots, a_n) \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix} = a_1 x_1 + \ldots + a_n x_n$$

***Определение* 5.11.**

$$\begin{bmatrix} a_{11} & \dots & a_{1m} \\ \vdots & \vdots & \vdots \\ a_{n1} & \dots & a_{nm} \end{bmatrix} \begin{bmatrix} x_1 \\ \vdots \\ x_n \end{bmatrix}$$

$$(Ax)_i = \sum_{j=1}^{n} A_{ij} x_j$$

***Определение* 5.12.**
Произведение матриц: $\cdot : M_{m\times n}(R) \times M_{n\times k}(R) \mapsto M_{m\times k}(R)$

$$(AB)_{ij} = \sum_{s=1}^{k} A_{is} B_{sj}.$$

Свойства.

$A, B, C \in M_{*\times*}(R)$ (размеры любые, но такие, чтобы произведения были определены). $\lambda \in R$

1. $(AB)C = A(BC)$
2. $\lambda(AB) = (\lambda A) = A(\lambda B)$
3. $C(A+B) = CA + CB$
4. $0_M = \begin{bmatrix} 0 & \dots & 0 \\ \vdots & \vdots & \vdots \\ 0 & \dots & 0 \end{bmatrix}$. $0_M A = A$.
5. $I = \begin{bmatrix} 1 & 0 & \dots & 0 \\ 0 & 1 & \dots & 0 \\ \vdots & \vdots & \vdots & \vdots \\ 0 & 0 & \dots & 1 \end{bmatrix}$. $IA = AI = A$.

Следствие.

$R^n \mapsto R^m$ заданное матрицей $A \in M_{m\times n}(R)$, такое, что $x \to Ax$ является гомоморфизмом групп.

***Определение* 5.13.**

$\operatorname{Ker} A = \{x \in R^n \mid Ax = 0\}$.

Ядро матрицы - множество решений однородной системы уравнений соответствующей этой матрице.

Следствие.

Если система уравнений $Ax = b$ имеет решение, то есть биекция между множеством её решений и $\operatorname{Ker} A$.

Доказательство. Возьмём такое x_0, что $Ax_0 = b$.

Пусть x^* такое, что $Ax^* = b$, тогда $x^* - x_0 \in \operatorname{Ker} A$.

Пусть $y \in \operatorname{Ker} A$, тогда $A(y + x_0) = b$. □

Лемма.

Пусть $x \in \operatorname{Ker} A$, $\lambda \in R$. Тогда $\lambda x \in \operatorname{Ker} A$.

***Определение* 5.14 (Векторное пространство).**

Векторным пространством называется четвёрка $\langle V, K, +, \cdot\rangle$, где V называется множеством векторов, K - полем скаляров, $+ : V \times V \mapsto V$, $\cdot : K \times V \mapsto V$. При этом, операции удовлетворяют следующим свойствам:

1. $\langle V, +\rangle$ - абелева группа
2. $\lambda(u + v) = \lambda u + \lambda v$
3. $(\lambda + \mu)\, u = \lambda u + \mu u$
4. $\lambda(\mu u) = (\lambda\mu) u$
5. $1u = u$

Пример.

0 $\{0\}$

1. $\langle K, K, +, \cdot \rangle$
2. $\langle K^n, K, +, \cdot \rangle$, $\langle M_{m \times n}(K), K, +, \cdot \rangle$
3. X - множество. K^X - множество функций из X в K.
4. $\langle C\left[0,1\right], \mathbb{R}, +, \cdot \rangle$

***Определение* 5.15.**
Векторным подпространством U пространства $\langle V, K, +, \cdot \rangle$, $U \subset V$.
$u_1, u_2 \in U$, $\lambda \in K$.

$$u_1 + u_2 \in U.$$

$$\lambda u_1 \in U.$$

$$0 \in U.$$

Пример.
$\operatorname{Ker} A$ - подпространство в K^n $(A \in M_{m \times n}(K))$.

$C^1[0,1] \leqslant C[0,1]$

$C[0,1] \geqslant \{f \in C[0,1] \mid f(\frac{1}{2}) = 0\}$

$K[x] \geqslant K_{\leqslant n}[x] = \{f \in K[x] \mid \deg f \leqslant n\}$

***Определение* 5.16 (Линейная комбинация).**
Пусть $v_1, \ldots, v_n \in V$, $\lambda_1, \ldots, \lambda_n \in K$.

Их линейной комбинацией называется $\lambda_1 v_1 + \ldots + \lambda_n v_n$

***Определение* 5.17.**
Пусть $X \subset V$ (подмножество).

Пространством, порождённым X (линейной оболочкой X) называется:

1. наименьшее по включению подпространство содержащие X
2. $\langle X \rangle = \{\lambda_1 x_1 + \ldots \lambda_n x_n \mid x_i \in X\}$

***Определение* 5.18.**
Если $\langle X \rangle = V$, то X пораждает V. (элементы X - образующие V)

***Определение* 5.19.**
Пусть есть набор векторов $v_1, \ldots, v_n \in V$.

Набор линейное зависим, если

$$\exists \lambda_1, \ldots, \lambda_n \text{ хотя-бы один из которых не } 0 \quad \lambda_1 v_1 + \ldots + \lambda_n v_n = 0.$$

***Определение* 5.20.**
Набор векторов $v_1, \ldots, v_n \in V$ называется базисом V, если он образует V и при этом линейно независим.

6. Лекция 6

Утверждение 6.1 (Эквивалентные переформулировки понятия базиса)**.**

Пусть V - векторное пространство над полем K, и набор векторов $e_1, \dots, e_n$. Следующие утверждения эквивалентны:

1. $e_1, \dots, e_n$ - базис
2. $e_1, \dots, e_n$ - минимальная по включению порождающая система V
3. $\forall v \in V \quad \exists! \lambda_1, \dots, \lambda_n \quad v = \lambda_1 e_1 + \ldots + \lambda_n e_n$
4. $e_1, \dots, e_n$ - максимальная по включению независимая система векторов

Доказательство.

$1 \implies 2$: Предположим что можно выкинуть вектор e_n. Значит, $V = \langle e_1, \dots, e_{n-1} \rangle$. Значит, $\exists \mu_i \quad \mu_1 e_1 + \ldots + \mu_{n-1} e_{n-1} = e_n \implies \mu_1 e_1 + \ldots + \mu_{n-1} e_{n-1} - e_n = 0$, значит, начальная система была линейно зависима.

$2 \implies 3$: $e_1, \dots, e_n$ - порождающая система, значит такие λ точно существуют. Пусть $\exists v \in V \quad \lambda_1 e_1 + \ldots + \lambda_n e_n = v = \mu_1 e_1 + \ldots + \mu_n e_n$. Пусть $\lambda_1 \neq \mu_1$. Тогда

$$0 = (\lambda_1 - \mu_1)e_1 + \ldots + (\lambda_n - \mu_n)e_n.$$

$$e_1 = \frac{1}{-(\lambda_1 - \mu_1)} \sum_{i=2}^{n} (\lambda_i - \mu_i)e_i.$$

Значит, e_1 можно выкинуть из системы. Противоречие с минимальностью.

$3 \implies 4$: Пусть $\lambda_1 e_1 + \ldots + \lambda_n e_n = 0$. Так-как разложение вектора 0 единственно, то $\lambda_1 = \ldots = \lambda_n = 0$. Возьмём вектор $v \in V$. Тогда $v = \mu_1 e_1 + \ldots + \mu_n e_n$, значит $\mu_1 e_1 + \ldots + \mu_n e_n - v = 0$, значит эта система максимальная.

$4 \implies 1$: Построим разложение вектора $v \in V \setminus \{0\}$.
Знаем, что система максимальна, значит $\lambda_1 e_1 + \ldots \lambda_n e_n + \lambda_v v = 0$.
Если $\lambda_v \neq 0$, перенесём v направо и разделим на λ_v.
Если $\lambda_v = 0$, то придём к противоречию с независимостью. □

***Определение* 6.1** (Координатная запись)**.**

Пусть $e = \{e_1, \dots, e_n\}$ - базис V, $v \in V$. Тогда координатной записью v в базисе e называется

$$[v]_e = \begin{bmatrix} \lambda_1 \\ \lambda_2 \\ \vdots \\ \lambda_n \end{bmatrix}.$$

При том, что $v = \lambda_1 e_1 + \lambda_2 e_2 + \ldots + \lambda_n e_n$.

***Определение* 6.2.**

Пространство V называется конечномерным, если $\exists v_1, \dots, v_n \quad \langle v_1, \dots, v_n \rangle = V$.

Все последующие теоремы доказываются только для конечномерных пространств.

Теорема 6.2 (О существовании базиса)**.**

Пусть V - конечномерное пространство над K. И $v_1, \ldots, v_m$ - порождающая система.

Возьмём линейно независимый набыор $e_1, \ldots, e_k$. Тогда $e_1, \ldots, e_k$ можно дополнить до базиса, при помощи $v_1, \ldots, v_n$.

Доказательство.

Индукция по количеству векторов из набора $v_1, \ldots, v_n$, которые не лежат в $\langle e_1, \ldots, e_k \rangle$:

Если $V = \langle e_1, \ldots, e_k \rangle$, то утверждение тривиально.

Пусть $v_i \notin \langle e_1, \ldots, e_k \rangle$. Рассмотрим систему $e_1, \ldots, e_k, v_i$.

Проверим, что она независима: Пусть зависима, тогда

$$\lambda_1 e_1 + \ldots + \lambda_k e_k + \lambda_v v = 0.$$

Тогда, либо $\lambda_v = 0$, и все $\lambda_i = 0$, либо

$$v = \frac{1}{\lambda_v} \left(\lambda_1 e_1 + \ldots + \lambda_n e_n \right).$$

Что противоречит тому, как мы брали v. □

Замечание.

Теорема верна и для бесконечномерных пространств, но доказательство сложнее.

Следствие.

Пусть V - конечномерное пространство. Тогда в нём существует базис.

Доказательство. Возьмём пустое множество как начало для предыдущей теоремы. □

Лемма (О линейной зависимости линейных комбинаций)**.**

Пусть есть наборы векторов $v_1, \ldots, v_m$ и $e_1, \ldots, e_n$. При этом, $v_i \in \langle e_1, \ldots, e_n \rangle$. Если $m > n$, то v_i линейно зависимые.

Доказательство.

Выпишем разложения для v_i:

$$v_i = \lambda_{i1} e_1 + \ldots \lambda_{in} e_n.$$

Индукция по n:

База: $n = 1$. $\langle e_1 \rangle = k e_1$. $k_1 e_1 + k_2 e_1 = 0 \iff k_1 - k_2 = 0$.

Предположим, что $\lambda_{11} \neq 0$ (можно добиться перенумеровкой, и выкидыванием бесполезных e_i). Тогда $u_i = v_i - \frac{\lambda_{i1}}{\lambda_{11}} v_1$, $i \in \{2, \ldots, m\}$.

Тогда $u_i \in \langle e_2, \ldots, e_n \rangle$.

По индукции, u_i линейно зависимы.

$$\mu_2 u_2 + \ldots \mu_m u_m = 0.$$

$$C v_1 + \mu_2 v_2 + \ldots \mu_m v_m = 0.$$

Значит, v_i линейно зависимы. □

Теорема 6.3 (О равномощности базиса)**.**

Пусть V - конечномерное пространство. И e, f - базисы V. Тогда $|e| = |f|$.

Доказательство. Пусть e конечно.

Предположим что f - бесконечный или $|f| > |e|$. Тогда там есть хотя-бы $n+1$ линейно независимый элемент.

То $\forall i \quad f_i \in \langle e \rangle$, значит любой набор из $n+1$ элементов f линейно зависим. Противоречие.

Если $|e| > |f|$, то анологичным образом приходим к противоречию. □

Замечание.

Теорема верна для произвольного пространства.

Определение 6.3.

Пусть V - векторное пространство. Тогда размерность $\dim V = n$, если в V есть базис мощности n, либо $\dim V = \infty$ если конечного базиса не существует.

Лемма.

Пусть $v_1, \ldots, v_k$ линейно независимо в V, при этом, $\dim V = n$. Тогда $k \leqslant n$, и если $k = n$, то $v_1, \ldots, v_k$ - базис.

Доказательство. Возьмём наш набор, и дополним до базиса векторами $v_{k+1}, \ldots, v_n$. Значит, изначально было $k \leqslant n$, и если $k = n$, то ничего не добавилось, значит и так базис. □

Лемма.

Пусть $v_1, \ldots, v_k$ - пораждающая система V, и $\dim V = n$. Тогда $k \geqslant n$, и если $k = n$, то $v_1, \ldots, v_k$ - базис.

Доказательство. Возьмём $\varnothing$, дополним до базиса векторами v_i. Выбрали n штук векторов. Значит, было хотя-бы n, и если было ровно n, то взяли все. □

Следствие.

Если $U \leqslant V$, и $\dim V = n$, то $\dim U \leqslant n$ и если $\dim U = n$, то $U = V$.

Доказательство. Возьмём базис U: $e_1, \ldots, e_k$. Он линейно независим в U, значит линейно независим V. Значит, $\dim U = k \leqslant n = \dim V$. Если $k = n$, то e - базис V, и $U = \langle e \rangle = V$. □

Утверждение 6.4.

Пусть $U_1, U_2 \leqslant V$. Тогда $U_1 \cap U_2 \leqslant V$. И $U_1 + U_2 = \{u_1 + u_2 \mid u_1 \in U_1, u_2 \in U_2\} \leqslant V$.

Доказательство.

Пересечение: **TODO:**

Сумма: $(u_1 + u_2) + (u_1' + u_2') = (u_1 + u_1') + (u_2 + u_2')$. $\lambda(u_1 + u_2) = \lambda u_1 + \lambda u_2$. $0 = 0 + 0$. □

Утверждение 6.5.

Пусть $U_1, U_2 \leqslant V$. $\dim U_1 = \ell$, $\dim U_2 = k$.

Тогда $\dim U_1 + \dim U_2 = \dim(U_1 + U_2) + \dim(U_1 \cap U_2)$.

Доказательство. Выберем $e_1, \ldots, e_k$ - базис $U_1 \cap U_2$.

Дополним до базиса в U_1 и U_2: $e_1, \ldots, e_k, f_1, \ldots, f_n$ - базис U_1, $e_1, \ldots, e_n, g_1, \ldots, g_m$ - базис U_2.

Тогда $e_1, \ldots, e_k, f_1 \ldots . f_n, g_1, \ldots, g_n$ - порождает $U_1 + U_2$.

Покажем что оно базис:

$$\lambda_1 e_1 + \ldots \lambda_k e_k + \mu_1 f_1 + \ldots + \mu_n f_n = \eta g_1 + \ldots + \eta_m g_m.$$

Слева вектор из U_1, справа из U_2. Значит, он лежит в пересечении. Тогда

$$\eta_1 g_1 + \ldots \eta_m g_m + c_1 e_1 + \ldots + c_n e_n = 0.$$

А это базис U_2, противоречие.

Тогда $(k+n)+(k+m) = (k+n+m)+k$, что соответствует утверждениям о размерностях. $\square$

***Определение* 6.4.**
$U \leqslant V$, $\dim V = n$, $\dim U = k$, $\operatorname{codim} U = n - k$.

7. Лекция 7

***Определение* 7.1.**

Пусть $U_1, U_2 \leqslant V$, то V раскладывается в прямую сумму ($V = U_1 \oplus U_2$), если

$$\forall v \in V \quad \exists! u_1, u_2 \in U_1, U_2 \quad v = u_1 + u_2.$$

Утверждение 7.1.

Пусть $U_1, U_2 \leqslant V$. Тогда следующие утверждения эквивалентны:

1. $V = U_1 \oplus U_2$
2. $U_1 \cap U_2 = \{0\}$, $\dim U_1 + \dim U_2 = \dim V$
3. $\forall e_1, \ldots, e_k \in U_1 \quad \forall f_1, \ldots f_\ell \in U_2$ (базисы), $e_1, \ldots, e_k, f_1, \ldots, f_\ell$ - базис V
4. $\forall \to \exists$

Доказательство.

$1 \implies 2$:

Пусть $v \in U_1 \cap U_2$. Тогда $v = 0 + v = v + 0$. Если $v \neq 0$, то получили два разложения v. Значит, $U_1 \cap U_2 = \{0\}$.

Имеем $V = U_1 + U_2$. По формуле Грассмана, $\dim V = \dim U_1 + \dim U_2 - \dim U_1 \cap U_2 = \dim U_1 + \dim U_2$.

$2 \implies 3$:

Взяли базисы e_i, f_i.

Покажем независимость в V: $\lambda_1 e_1 + \ldots + \lambda_k e_k = -(\mu f_1 + \ldots \mu_\ell f_\ell)$. Это элемент из пересечения, но пересечение тривиально. Значит по обе стороны нули. Значит, все коэффициенты - 0.

$k + \ell = \dim V$, $e_i, f_i \in V$, значит, $\langle e, f \rangle = V$.

$3 \implies 4$ тривиально.

$4 \implies 1$:

Взяли $v \in V$. Возьмём базисы U_1, U_2, которые дают базис v. Получили представление.

При этом, v разложился по базису V. А такое разложение единственно. □

***Определение* 7.2** (Линейное отображение)**.**

Пусть V_1, V_2 - векторные пространства над K. Тогда $f : V_1 \mapsto V_2$ называется линейным отображением, если

1. $\forall v, u \in V_1 \quad f(v + u) = f(v) + f(u)$
2. $\forall \lambda \in K \quad \forall v \in V_1 \quad f(\lambda v) = \lambda f(v)$.

Замечание.

Линейные отображения - гомоморфизмы групп

Пример.

1 id

1' $v \to \lambda v$.

2 $V_1 = K^n$, $V_2 = K^m$. $A \in M_{m\times n}(K)$. $v \to Av$.

3 $V_1 = V_2 = K[x]$, $f \to f'$.

4 $V_1 = C^1[a,b]$, $V_2 = C[a,b]$, $f \to f'$.

5 $f \to \int\limits_0^1 f(x)dx$

6 $f \to \int\limits_0^x f(x)dx$.

7 $V_1 = K[x]$, $V_2 = K$. $\lambda \in K$. $f \to f(\lambda)$.

8 $K[x] \mapsto K[x]$, $f \to f(g(x))$.

9 $f(x) \mapsto g(x)f(x)$

Утверждение 7.2.

Пусть $f, g : V_1 \mapsto V_2$, $k, h : V_2 \mapsto V_3$ - линейные отображение.

Тогда

1. $\lambda_1 f + \lambda_2 g$ - линейное отображение.
2. $k \circ f : V_1 \mapsto V_3$ - линейное отображение
3. $\mathrm{Hom}_K(V_1, V_2)$ - множество всех линейных отображений $V_1 \mapsto V_2$. $\mathrm{Hom}_K(V_1, V_2)$ - векторное пространство относительно поточечного сложения и домножения на скаляр.
4. $(k + h) \circ f = k \circ f + h \circ f$
5. $k \circ (f + g) = k \circ f + k \circ g$
6. f - инъективно $\iff \operatorname{Ker} f = \{0\}$.

Теорема 7.3.

Пусть V_1, V_2 - конечномерные векторные пространства. $e_1, \ldots, e_n$ - базис V_1. $u_1, \ldots, u_n$ - набор элементов (не обязательно базис) V_2.

Тогда $\exists! f : V_1 \mapsto V_2 \quad f(e_i) = u_i$.

Доказательство.

Пусть $v \in V_1$. $v = \lambda_1 e_1 + \ldots + \lambda_n e_n$.

Тогда $f(v) = f(\lambda_1 e_1 + \ldots + \lambda_n e_n) = \lambda_1 f(e_1) + \ldots + \lambda_n f(e_n) = \lambda_1 u_1 + \ldots + \lambda_n u_n$.

Покажем линейность: v_1, v_2 раскладываются по e с координатами λ_i, μ_i.

Тогда $f(v_1 + v_2)$ раскладывается по $f(e)$ с координатами $(\lambda_i + \mu_i)$. Аналогично $f(v_1) + f(v_2)$. Домножение на скаляр анологично. □

Следствие.

Возьмём $f : K^n \mapsto K^m$. Тогда $\exists! A \in M_{m\times n}(K) \quad f(x) = Ax$.

Доказательство.

Возьмём канонический базис K^n, назовём его e_i.

Возьмём $u_i = f(e_i)$.

Тогда, подходящая матрица -

$$\begin{bmatrix} u_1 & \dots & u_n \end{bmatrix} = \begin{bmatrix} u_{11} & \dots & u_{m1} \\ u_{m2} & \dots & u_{m2} \\ \vdots & \vdots & \vdots \\ u_{1n} & \dots & u_{mn} \end{bmatrix}.$$

□

Определение 7.3.

Векторные пространства V_1 и V_2 называются изоморфными, если $\exists f : V_1 \mapsto V_2$, такое, что f - линейное и биекция. f называется изоморфизмом.

Замечание.

f - изоморфизм $\iff$ f^{-1} - изоморфизм

Следствие.

Пусть $f : V_1 \mapsto V_2$ - линейное отображение. Следующие утверждения эквивалентны:

1. L - изоморфзим
2. $\forall e_1, \dots, e_n$ - базис V_1, тогда $L(e)$ - базис V_2
3. $\forall \to \exists$

Доказательство.

$1 \implies 2$:

Заметим, что $\operatorname{Im} f = \langle f(e) \rangle = V_2$. Пусть $f(e)$ линейно зависима. Тогда существуеют два разложения 0. Тогда есть два элемента, которые f переводит в 0, но f биекция. Значит, $f(e)$ линейно независимо.

$2 \implies 3$ тривиально.

$3 \implies 1$:

Пусть g - отображение, переводящие базис $f(e)$ в базис e. Тогда $(g \circ f)(e_i) = e_i$ $(f \circ g)(f(e_i) = f(e_i)$. Построили обратное $\implies$ биекция. □

Следствие.

Пусть V, W - векторные пространства, и $\dim V = \dim W = n$.

Доказательство.

Возьмём базисы, построим по ним. □

Следствие.

Пусть V - векторное пространство. $\dim V = n$. Тогда выбор базиса в V задаёт изоморфизм в K^n.

Определение 7.4.

Изоморфизм $V \mapsto K^n$ называется линейное системой координат. Каждая компонента называется координатной функцией.

Теорема 7.4 (О подходящем выборе базиса)**.**

Пусть $f : V_1 \mapsto V_2$ - линейное отображение, $\dim V_1 = n$.

Тогда $\exists$базис $e \quad V_1$, такой, что $f(e_i)$, $i \leqslant k$ - базис $\operatorname{Im} f$, $e_{k+1}, \ldots, e_n$ - базис $\operatorname{Ker} f$.

Доказательство.

TODO: □

Следствие Связь размерностей.

Пусть $f : V_1 \mapsto V_2$ - линейное.

$\dim V_1 = \dim \operatorname{Im} f + \dim \operatorname{Ker} f$.

Следствие Принцип Дирихле.

Пусть V, W - векторные пространства, такие, что $\dim V = \dim W$ - конечные.

Тогда, любое линейное отображение $f : V \mapsto W$ сюрьективно тогда и только тогда когда оно инъективно

Доказательство.

$$\dim W = \dim V = \dim \operatorname{Im} f \iff \dim \operatorname{Ker} f = 0.$$

□

Следствие.

Пусть $A \in M_{n\times n}(K)$. Тогда $\exists! x \in K^n \quad Ax = 0 \iff \forall b \in K^n \quad \exists x \in K^n \quad Ax = b$

Следствие.

Пусть $A \in M_{m\times n}(K)$. Тогда

$$\forall b \in K^m \quad \exists x \in K^n \quad Ax = b \iff \dim\{x \in K^n \mid Ax = 0\} = n - m.$$

8. Лекция 8

Утверждение 8.1.

Пусть $A \in M_{m\times n}(K)$ и ситема уравнений $Ax = b$.

Если у этой системы есть хоть одно решение, то все её решения описываются $\dim \operatorname{Ker} A$ независимыми переменными.

Доказательство.

Заметим, что приведение матрицы к ступенчатому виду не изменяет множество решений.

Множество решений системы - $\{x_0 + y \mid Ay = 0\} = \{x_0 + y \mid y \in \operatorname{Ker} A\}$

Заметим, что если взять матрицу системы $Ax = 0$, то получиться такое-же количество независимых переменных. Пусть $x_{i_1}, \dots, x_{i_s}$ - независимых переменных. Тогда $x_k = \sum\limits_{j=1}^{s} C_{kj} x_{i_j}$.

Значит, матрица $C \in M_{n\times s}(K)$ переводит столбец независимых переменных переменных в столбец решений. Причём, это отображение - биекция. Значит, отображение, задаваемое C - изоморфизм. Значит, размерности сохраняются. □

***Определение* 8.1.**

Пусть есть $L : V_1 \mapsto V_2$ - линейное отображение. e_i - базис V_1, f_i - базис V_2.

Тогда матрица линейного отображения $[L]_e^f$ - матрица, в которой i-й столбец равен $[L(e_i)]_f$.

Пример.

1. $V_1 = V_2 = K[x]_{\leqslant n}$, $f(x) \to f(x + a)$. Базисы стандартные. Матрица отображения:

$$\begin{bmatrix} 1 & a & \dots & a^n \\ 0 & 1 & \dots & na^{n-1} \\ 0 & 0 & \dots & n(n-1)a^{n-2} \\ \vdots & \vdots & \vdots & \binom{n}{i} a^{n-i} \\ 0 & 0 & \dots & 1 \end{bmatrix}$$

2. $V_1 = V_2 = K[x]_{\leqslant n}$, $f(x) \to f(x + a)$. Базис V_1 - стандартный. Базис V_2 - $1, (x + a), (x + a)^2, \dots, (x + a)^n$. Матрица отображения - E_{n+1}.

Утверждение 8.2.

Пусть $L : V_1 \mapsto V_2$ - линейное отображение, e_i - базис V_1, f_i - базис V_2.

Тогда $A = [L]_e^f$ - единственная матрица, такая, что $A[v]_e = [u]_f \iff L(v) = u$.

Утверждение 8.3.

Пусть $L_1, L_2 : V_1 \mapsto V_2$ - линейные отображения, e_i - базис V_1, f_i - базис V_2.

Тогда $[L_1 + L_2]_e^f = [L_1]_e^f + [L_2]_e^f$

Пусть $\lambda \in K$. Тогда $[\lambda L_1]_e^f = \lambda [L_1]_e^f$

Доказательство.

Без ограничения общности, докажем совпадение первого столбца.

Заметим, что $(L_1 + L_2)(e_1) = L_1(e_1) + L_2(e_1)$, значит, $[(L_1 + L_2)(e_1)]_f = [L_1(e_1) + L_2(e_2)]_f = [L_1(e_1)]_f + [L_2(e_1)]_f$. Значит, столбец соответствующий e_1 совпадает.

Второе утверждение аналогично. □

Утверждение 8.4.

Пусть есть $L_1 : V_1 \mapsto V_2$, $L_2 : V_2 \mapsto V_3$, e_i, f_i, g_i - базисы V_1, V_2, V_3 соответственно.

Тогда
$$[L_2 \circ L_1]_e^g = [L_2]_f^g \, [L_1]_e^f \, .$$

Доказательство.

Обозначим $A = [L_1]_e^f$, $B = [L_2]_f^g$

Рассмотрим вектор $u \in V_1$. $x = [u]_e$.

Тогда $u \to L_1(u)$, $x \to Ax$.

Потом $L_1(u) \to L_2(L_1(u))$. $Ax \to B(Ax) = (BA)x$.

По теореме о единственности матрицы линейного отображения, получили что $[L_2 \circ L_1]_e^g = BA = [L_2]_f^g [L_1]_e^f$. □

Утверждение 8.5.

Пусть $L : V_1 \mapsto V_2$ - изоморфизм. e, f - базисы V_1, V_2

Тогда $[L^{-1}]_f^e [L]_e^f = E_n = [L]_e^f \, [L^{-1}]_f^e$

***Определение* 8.2.**

Матрица $A \in M_n(K)$ называется обратимой, если $\exists A^{-1} \in M_n(K) \quad AA^{-1} = E_n = A^{-1}A$.

Замечание.

Пусть $A = [L]_e^f$. Тогда $\exists L^{-1} \iff \exists A^{-1}$

Утверждение 8.6.

Пусть $A, B \in M_n(K)$, и $AB = E_n$. Тогда $BA = E_n$.

Доказательство.

Перейдём к отображениям, задаваемым этими матрицами. Пусть A задаёт L_1, B задаёт L_2.

Знаем, что $L_1 \circ L_2 = \mathrm{id}$. Из этого следует, что L_1 сюръективна. Значит, оно инъективно по принципу Дирихле. Значит, матрица A обратима. Домножим равенство $AB = E_n$ а A^{-1} слева, получим $B = A^{-1}$ □

***Определение* 8.3.**

Пусть в V выбраны два базиса: e_i, e'_i.

Матрица замены координат из базиса e в базис e' - такая матрица, которая переводит $[u]_e$ в $[u]_{e'}$.

Утверждение 8.7.

Матрица $[\mathrm{id}]_e^{e'}$ - матрица замины координат.

Утверждение 8.8.

Матрица замены координат - матрица состоящая из столбцов $[e_i]_{e'}$

***Определение* 8.4.**

Матрица перехода из базиса e в базис e' - такая матрица, что столбцы этой матрицы - $[e'_i]_e$.

Утверждение 8.9.

Матрица замены координат и матрица перехода взаимно обратны.

Доказательство.

Пусть C - матрица замены координат, D - матрица перехода.

Тогда

$$D = [\mathrm{id}]^e_{e'} = \left([\mathrm{id}]^{e'}_e\right)^{-1} = C^{-1}.$$

□

Пример.

Пусть есть пространство K^n. e - стандартный базис, e' - какой-то базис.

Тогда матрица перехода:

$$\begin{bmatrix} e'_1 & e'_2 & \dots & e'_n \end{bmatrix}.$$

Замечание.

Пусть e, e' - базисы V. Тогда матрица перехода - $D^{e'}_e$.

Свойства.

Пусть e, f, g - базисы V.

Тогда

$$D^g_e = D^g_f D^f_e.$$

$$D^e_f = (D^f_e)^{-1}.$$

$$D^e_e = E_n.$$

Теорема 8.10.

Пусть $L : V_1 \mapsto V_2$ - линейное отображение. e, e' - базисы V_1, f, f' - базисы V_2.

Тогда $[L]^f_e = D^{f'}_f [L]^{f'}_{e'} \left(D^{e'}_e\right)^{-1}$

***Определение* 8.5.**

Пусть $L : V_1 \mapsto V_2$. Тогда ранг $\operatorname{rk} L = \dim \operatorname{Im} L$

Теорема 8.11.

Пусть $L : V_1 \mapsto V_2$. Тогда $\exists e$ - базис V_1 $\quad \exists f$ - базис V_2 $\quad$, такие, что

$$[L]^f_e = \begin{bmatrix} E_r & 0 \\ 0 & 0 \end{bmatrix}$$

Где $r = \operatorname{rk} L$.

Доказательство.

Выберем такой базис e, такой, что первые r векторов - базис образа, остальные - базис ядра. Такой базис существует по теореме о выборе базиса.

Первые r векторов f - $L(e_i)$. Остальные можно выбрать как угодно. □

Следствие.

Пусть выбрали такой базис. Тогда $L(e_{r+1}) = \ldots = L(e_n) = 0$. $i \leqslant r \implies L(e_i) = f_i$.

9. Лекция 9

Теорема 9.1.

Пусть $U \leqslant K^n$, такое, что $\operatorname{codim} U = d \iff \dim U = n - d$.

Тогда U можно задать d уравнениями.

$$\exists A \in M_{d\times n}(K) \quad U = \{x \in K^n \mid Ax = 0\} = \operatorname{Ker} A$$

$$\exists f : K^n \mapsto K^d \quad U = \operatorname{Ker} f$$

Доказательство.

Выберем базис U - $e_{d+1}, \ldots, e_n$.

Дополним до базиса K^n с помощью $e_1, \ldots, e_d$.

Тогда $\forall i > d \quad f(e_i) = 0$. $\forall i \leqslant d \quad f(e_i) = k_i$, где k - стандартный базис K^d.

Включение $U \subset \operatorname{Ker} f$ очевидно.

При этом, $\dim \operatorname{Im} f = d \implies \dim \operatorname{Ker} f = n - d \implies U = \operatorname{Ker} f$. □

Теорема 9.2.

Пусть $A \in M_{m\times n}(K)$, то $\exists D \in M_{m\times m}, C \in M_{n\times n}$ - обратимые $\quad A = D \begin{bmatrix} E_r & 0 \\ 0 & 0 \end{bmatrix} C$.

Доказательство.

Пусть e, f - стандартные базисы K^n, K^m.

Пусть $L : K^n \mapsto K^m$ - такое, что $[L]_e^f = A$.

Возьмём базисы $e' \in K^n, f' \in K^m$, такие, что $[L]_{e'}^{f'} = \begin{bmatrix} E_r & 0 \\ 0 & 0 \end{bmatrix}$

Тогда $C = (D_{e'}^{e})^{-1}$, $D = D_{f'}^{f}$

□

Теорема 9.3 (Ранговое разложение)**.**

Пусть $A \in M_{m\times n}(K)$. $\operatorname{rk} A = r$.

Тогда $\exists B \in M_{m\times r}, C \in M_{r\times m} \quad A = BC$

Доказательство.

Возьмём $V = \operatorname{Im} A$. Возьмём v - базис $\operatorname{Im} A$. Возьмём e, f - стандартные базисы K^n, K^m.

Пусть возмьём такие L_1, L_2, такие, что $(x \to Ax) = L_2 \circ L_1$. Тогда $A = [L_2]_v^f [L_1]_e^v$. □

Доказательство.

Предствим A как $D \begin{bmatrix} E_r & 0 \\ 0 & 0 \end{bmatrix} C$.

Заметим, что $\begin{bmatrix} E_r & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix} \cdot \begin{bmatrix} 1 & \ldots & 1 & 0 & \ldots & 0 \end{bmatrix}$.

Тогда $A = \left(D \begin{bmatrix} 1 \\ \vdots \\ 1 \\ 0 \\ \vdots \\ 0 \end{bmatrix}\right) \left(\begin{bmatrix} 1 & \dots & 1 & 0 & \dots & 0 \end{bmatrix} C\right)$ □

Утверждение 9.4.

Пусть $L_1 : U \mapsto V$, $L_2 V \mapsto W$.

Тогда $\operatorname{rk} L_2 \circ L_1 \leqslant \min(\operatorname{rk} L_1, \operatorname{rk} L_2)$.

Доказательство.

$$\operatorname{rk} L_2 \circ L_1 = \dim \operatorname{Im} L_1 \circ L_2 \subset \operatorname{Im} L_2 \implies \operatorname{rk} L_2 \circ L_1 \leqslant \operatorname{rk} L_2.$$
$$\dim \operatorname{Im} L_1 = \operatorname{rk} L_1 \implies \dim L_2(\operatorname{Im} L_1) \leqslant \dim \operatorname{Im} L_1 \implies \operatorname{rk} L_2 \circ L_1 \leqslant \operatorname{rk} L_1.$$
□

Следствие.

Пусть $T : U' \mapsto U$, $L : U \mapsto V$, $S :\mapsto V'$.

Тогда $\operatorname{rk} S \circ L \circ T = \operatorname{rk} L$.

Доказательство.

$$L = S^{-1} \circ S \circ L \circ T \circ T^{-1} \implies \operatorname{rk} L \leqslant \operatorname{rk} S \circ L \circ T.$$

□

Теорема 9.5.

$$\operatorname{rk} A + B \leqslant \operatorname{rk} A + \operatorname{rk} B.$$

Доказательство.

$$\operatorname{Im} A + B \subset \operatorname{Im} A + \operatorname{Im} B.$$

□

Утверждение 9.6.

$$\operatorname{rk} A + B \geqslant |\operatorname{rk} A - \operatorname{rk} B|.$$

Доказательство.

Пусть $\mathbb{E}^r_{m\times n} \in M_{m\times n}(K) = \begin{bmatrix} E_r & 0 \\ 0 & 0 \end{bmatrix}$

Без обграничения общности, $\operatorname{rk} A \geqslant \operatorname{rk} B$. . Выберем такую систему координат, что $B = \mathbb{E}^r_{m\times n}$.

В A есть $\operatorname{rk} A$ независимых столбцов. В результате прибавления B изменилось не более $\operatorname{rk} B$ столбцов. Уберём их из рассмотрения, точно осталось $\operatorname{rk} A - \operatorname{rk} B$ независимых столбцов. □

***Определение* 9.1.**

Пусть $A \in M_{m\times n}$. Тогда $\operatorname{rk}_{\text{row}} A = \dim \langle \text{строки } A \rangle$

***Определение* 9.2.**

Пусть $A \in M_{m\times n}$. Тогда транпонированная матрица $A^T \in M_{n\times m}$ - такая матрица, что $A^T_{ij} = A_{ji}$.

Утверждение 9.7.

$$\operatorname{rk}_{\text{row}} A = \operatorname{rk} A^T.$$

Свойства.

1. $(A+B)^T = A^T + B^T$
2. $(\lambda A)^T = \lambda A^T$
3. $(AB)^T = B^T A^T$
4. A - обратимая. Тогда $(A^T)^{-1} = (A^{-1})^T$

Утверждение 9.8.

$$\operatorname{rk}_{\text{row}} A = \operatorname{rk} A.$$

Доказательство.

Пусть $A = C\mathbb{E}^r_{m\times n}D$.

Тогда $A^T = D^T \mathbb{E}^r_{n\times m} C^T$.

Заметим, что $\operatorname{rk} A^T = \operatorname{rk} A$. □

Утверждение 9.9.
Каждое элементарное преобразование можно представить как домножение на матрицу.

Доказательство.

$E_{ij}(\lambda) = E_n + \lambda e_{ij}$ - к i-й строке прибавить j-ю строку домноженную на λ

$P_{(ij)} = E_n - e_{ii} - e_{jj} + e_{ij} + e_{ji}$ - поменять местами i-ю и j-ю строки.

$D_i(\lambda) = E_n - e_{ii} + \lambda e_{ii}$ - Домножение i-й строки на $\lambda \in K^*$

$E_{ij}(\lambda)^{-1} = E_{ij}(-\lambda)$, $P^{-1}_{(ij)} = P_{(ij)}$, $D_i(\lambda)^{-1} = D_i\left(\lambda^{-1}\right)$ □

Замечание.

$AP_{(ij)}$ - поменять i-й и j-й столбец местами.

$AD_i(\lambda)$ - домножить i-й столбец на λ.

$AE_{ij}(\lambda)$ - добавить в j-му столбцу i-й столбец умноженный на λ.

***Определение* 9.3.**

Пусть $\sigma \in S_n$. Тогда $(P_\sigma)_{ij} = \begin{cases} 0 & \sigma(j) \neq i \\ 1 & \end{cases}$

***Определение* 9.4.**

Матрица A называется нижнетреугольной и обозначается $A \in LT_n(K)$, если $\forall i < j \quad A_{ij} = 0$.

Матрица A называется верхнетреугольной, $A \in UT_n(K)$, если $\forall i > j \quad A_{ij} = 0$.

Утверждение 9.10.

Пусть $A, B \in LT_n(K)$.

Тогда

1. $A + B \in LT_n$
2. $\lambda A \in LT_n(K)$

3. $AB \in LT_n(K)$

Доказательство.

$$(AB)_{ij} = \sum_{k=1}^{n} A_{ik}B_{kj} = \sum_{k=j}^{i} A_{ik}B_{kj} \implies (j > i \implies (AB)_{ij} = 0).$$

$\square$

4. $A^{-1} \in LT_n(K)$

Доказательство.

Лемма.
$\forall A \in LT_n$, такая, что A обратима, A раскладывается в виде произведения F_i - элементарные преобразования вида $E_{st}(\lambda)$, $s > t$ и $D_s(\lambda)$

Доказательство.
Если матрица обратима, то все элементы на главной диагонали не 0, и переставлять сточки не надо.

Применим метод Гаусса, сначала поскладываем строки, получиться диагональная матрица. Потом можем домножить i-ю строку на $\frac{1}{A_{ii}}$, получим единичную. Все матрицы которые применяли обратимы, значит, разложили в произведение. $\square$

Если A обратима, то A - произведение матриц элементарных проеобразований, тогда A^{-1} - произвдение обратных к ним, а они тоже нижнетреугольные. $\square$

Доказательство.
Без ограничения общности, на главной диагонали A стоят единицы.

Представим $A = E_n + N$. У N на диагонали и выше нули.

Тогда $N^n = 0$ (заметим, что $N(e_1) \in \langle e_2, \dots, e_n \rangle$, $N(e_2) \in \langle e_3, \dots, e_n \rangle, \dots, N(e_n) = 0$). Тогда, на кадой итерации мы теряем хотя-бы один вектор. После n шагов везде нули.

Тогда

$$A^{-1} = (E_n + N)^{-1} = E_n - N + N^2 - N^3 + \ldots + (-1)^{n-1}N^{n-1}.$$ $\square$

Теорема 9.11.
Любую обратимую матрицу $A \in M_{n\times n}(K)$ можно разложить как $PA = LU$, $L \in LT_n(K)$, $M \in UT_n(K)$, P - матрица перестановки.

Доказательство.
TODO: $\square$

Следствие.
Обратимая матрица $A \in M_{n\times n}(K)$ имеет LU разложение, когда подматрицы вида

$$A_i = \begin{bmatrix} A_{11} & A_{12} & \dots & A_{1i} \\ A_{21} & A_{22} & \dots & A_{2i} \\ \vdots & \vdots & \vdots & \vdots \\ A_{i1} & A_{i2} & \dots & A_{ii} \end{bmatrix}.$$

обратимы. Причём, если зафиксировать элементы диагонали L, то такое разложение единственно.

Доказательство.

TODO: $\square$

10. Лекция 10

***Определение* 10.1.**

Объём парралелелепипида натянутого на вектора $v = v_1, \ldots, v_n$: функция $\mathrm{Vol}(v) \in \mathbb{R}$, удовлетворяющая следующим свойствам:

0 $\mathrm{Vol}(e) = 1$, где e - стандартный базис $\mathbb{R}^n$

1. $\mathrm{Vol}(v_1, \ldots, \lambda v_i, \ldots, v_n) = |\lambda| \mathrm{Vol}(v_1, \ldots, v_n)$.
2. $\mathrm{Vol}(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_n) = 0$.
3. $\mathrm{Vol}(v_1, \ldots, v_i, \ldots, v_j + \lambda v_i, \ldots, v_n) = \mathrm{Vol}(v_1, \ldots, v_n)$.

***Определение* 10.2.**

Пусть задан набор пространств $U_1, \ldots, U_n$ и W, надо полем K.

Отображение $\omega : U_1 \times \ldots \times U_n \mapsto W$ называется полилинейным, если оно линейнок по каждому входному вектору.

Множество всех полилинейных отображение отображается $\mathrm{Hom}_K(U_1, \ldots, U_n; W)$.

***Определение* 10.3.**

Отображение $\omega \in \mathrm{Hom}_K(U_1, \ldots, U_n; K)$ называется полилинейной формой.

***Определение* 10.4.**

Отображение $\omega \in \mathrm{Hom}_K(\underbrace{V \times \ldots \times V}; K)$ называется полилинейной формой степени ℓ на V.

***Определение* 10.5.**

Полилинейная форма степени ℓ ω называется симметричной, если $\omega(v_1, \ldots, v_\ell) = \omega(v_{\sigma(1)}, \ldots, v_{\sigma(\ell)}$, $\sigma \in S_\ell$.

ω называется кососимметричной, если $\omega(v_1, \ldots, v_i, \ldots, v_i, \ldots, v_\ell) = 0$.

Утверждение 10.1.

Пусть $\omega : V^{\times \ell} \mapsto K$, e - базис V.

Тогда

$$\omega(v_1, \ldots, v_\ell) = \sum_{i_1, \ldots, i_\ell} \omega(e_{i_1}, \ldots, e_{i_\ell}) \prod_{j=1}^{\ell} \lambda_{j i_j}.$$

Где $\lambda_{j i_j}$ - i_j-я координата v_j в базисе e.

Доказательство.

Разложим по базису, воспользуемся линейностью. □

Утверждение 10.2.

Пусть ω - полилинейная форма.

1. Если ω - кососимметричная, то $\omega(\ldots, v_i, \ldots, v_j, \ldots) = (-1)\omega(\ldots, v_j, \ldots, v_i, \ldots)$.
2. Если выполнено условие 1 и $\mathrm{char}\, K \neq 2$, то ω кососимметричная.
3. Если ω - кососимметричная, то $\omega(v_1, \ldots, v_\ell) = \mathrm{sgn}(\sigma)\omega(v_{\sigma(1)}, \ldots, v_{\sigma(\ell)})$.

4. Если ω - кососимметричная, то $\omega\left(v_1, \ldots, v_\ell\right) = \sum\limits_{i_1<\ldots<i_\ell} w(e_{i_1}, \ldots e_{i_\ell}) \sum\limits_{\sigma \in S_\ell} \operatorname{sgn}(\sigma) \prod\limits_{j=1}^{\ell} \lambda_{j\sigma(i_j)}$

Доказательство.
TODO: □

***Определение* 10.6.**
Пусть V - векторное пространство размерности n, Тогда $\omega : V^{\times n} \mapsto K$ называется формой объёма, если она является кососимметричной полилинейной формы.

Замечание.
ω называется невырожденной если $\omega \neq 0$.

***Определение* 10.7.**
Пусть $A \in M_n(K)$. тогда $\det A = \sum\limits_{\sigma \in S_n} \operatorname{sgn}(\sigma) \prod\limits_{j=1}^{n} A_{\sigma(j)j}$.

Теорема 10.3.

1. Определитель - форма объёма на пространстве столбцов.
2. V - пространство размерности n, e - базис V. Тогда $\operatorname{Vol}_e : V^{\times n} \mapsto K$, $\operatorname{Vol}_e(v_1, \ldots, v_n) = \det\left[[v_1]_e, \ldots, [v_n]_e\right]$ - форма объёма.
3. Форма объёма единственна с точностью до константы. Если ω - форма объёма, то $\omega = \omega(e_1, \ldots, e_n) \operatorname{Vol}_e$.
4. Для любой ω - невырожденной формы объёма $\omega(v_1, \ldots, v_n) \neq 0 \iff v_1, \ldots, v_n$ - линейно независимы.

Доказательство.
TODO: □

11. Лекция 11

Свойства.

Если $A, B, C \in M_n(K)$.

0 $\det(A) = \det(A^T)$

1 Определитель не меняется при элементарных преобразованих первого типа (лин. комбинация) для строк/столбцов, меняет знак при свопе строк/столбцов, домножается на λ при домножении строки/столбца на λ.

Доказательство.

Для столбцов прямо следует из свойств определителя, для строк рассмотрим определитель A^T. $\square$

2 $\det(AB) = \det(A)\det(B)$

Доказательство.

Возьмём форму $B \to \det AB$. Она линейна по столбцам B. Чтобы показать это, заметим, что $A(B+X) = AB + AX \implies (B+X) \to \det A(B+X) = \det AB + \det AX$ (альтернативно: определитель линеен по столбцам произведения, произведение линейно по столбцам B (i-й столбец произведения зависит только от i-го столбца B, и зависит линейно).

Если у матрицы B есть одинаковые столбцы, то они есть и у матрицы AB.

Значит, $B \to \det AB$ - форма объёма. Все формы объёма пропорциональны, подставим $B = E_n$, получим, что $B \to \det A \det B \implies \det AB = \det A \det B$.

Альтернативно - найдём комбинацию элементарных преобразований L, такую, что $LA = E_n$ такая комбинация существует, если A невырождена.

Если A вырождена, то $\det A = 0$, AB - вырождена, $\det AB = 0 = 0 \det B$.

Тогда $LAB = B$.

Тогда $L^{-1}B = AB$.

Если $B = E_n$, то получаем $\det A = \det L^{-1}1 = k$.

По пункту 1, применение этих элементарных преобразований всегда домножает определитель на k, значит $\det L^{-1}B = k \det B = \det A \det B$. $\square$

3 $\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det(A)\det(C)$

Доказательство.

Сначала рассмотрим $\det \begin{bmatrix} E_n & B \\ 0 & E_m \end{bmatrix}$. Элементарными преобразованиями первого типа можно получить из неё E_{n+m}, значит определитель 1.

Заметим, что форма $A \to \det \begin{bmatrix} A & B \\ 0 & E_m \end{bmatrix}$ - форма объёма, значит она пропорциональна $\det A$, причём с коэффициентом 1.

Теперь, рассмотрим форму $C \to \det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$ - это форма объёма по строчкам C. Получаем, что оно пропорционально $\det C$ с коэффициентом $\det A$.

Значит, $\det \begin{bmatrix} A & B \\ 0 & C \end{bmatrix} = \det A \det B$. $\square$

4 Определитель верхнетреугольной или нижнетреугольной матрицы равен произведению диогональных элементов.

Доказательство.
Индукция по размеру.

Пусть $X \in LT_n$.

Разобьём на блоки вида $\begin{bmatrix} A & B \\ 0 & C \end{bmatrix}$. $A = X_{11}$, остальные выводятся из этого. $\det X = \det A \det C = X_{11} \det C = \prod\limits_{i=1}^{n} X_{ii}$. $C \in LT_{n-1}$.

Если получили матрицу из LT_1, то определитель равен единственному её элементу. □

5 $\det(A^{-1}) = (\det A)^{-1}$

Доказательство.
Заметим, что $\det A^{-1}A = 1 = \det A^{-1} \det A \implies \det A^{-1} = \frac{1}{\det A}$. □

6 $\det : GL_n(K) \to K^*$ - гомоморфизм групп

Доказательство.
Произведение сохраняется по свойству 2, результат обратим по свойству 5. □

Определитель можно вычислить методом Гаусса, привдя матрицы к ступенчатом виду, перемножив элементы на диоганали, и скорректировавшись на эффект преобразований.

Теорема 11.1.
Если есть отображение $\mathrm{Vol} : M_n(\mathbb{R}) \to \mathbb{R}$, удовлетворяющие свойствам

1. $\mathrm{Vol}(E_n) = 1$
2. $\mathrm{Vol}(\ldots, u + \lambda v, \ldots, v) = \mathrm{Vol}(\ldots, u, \ldots, v, \ldots)$
3. $\mathrm{Vol}(\ldots, \lambda v, \ldots) = |\lambda| \mathrm{Vol}(\ldots, v, \ldots)$

То $\mathrm{Vol} = |\det|$

Доказательство.
Рассмотрим случай, когда матрица вырождена.

Тогда существует элемент, который можно выразить как линейную комбинацию других, и можно получить $\mathrm{Vol}(\ldots, 0, \ldots) = 0\,\mathrm{Vol}(\ldots, v, \ldots) = 0$.

Если матрица невырождена, то можно привести её к единчному виду. Обе функции меняются одинаокого при элементарных преобразованиях, занчит они совпадут. □

12. Лекция 12

***Определение* 12.1.**

Пусть V - векторное пространство над $\mathbb{R}$. Базисы e_i и f_i называются одинаково ориентированными, если $\det C_{e\to f} > 0$.

Одинакованння ориентированность - отношение эквивалентности.

***Определение* 12.2.**

Ориентация пространства - задание класса эквивалентности базисов.

Пример.

Пространство - $\mathbb{R}^n$, $e_1, \ldots, e_n$ - стандарнтный базис. Он задаёт стандартную ориентацию.

Нестандартная ориентация: $\mathbb{R}^2$, $\begin{bmatrix} -1 \\ 0 \end{bmatrix}, \begin{bmatrix} 0 \\ 1 \end{bmatrix}$

Утверждение 12.1.

Пусть e, f - разноориентированные базисы $\mathbb{R}^n$, то

$$\nexists \quad g : C[0,1] \mapsto GL_n(\mathbb{R}) \quad \begin{cases} g(0) = (e_1, \ldots, e_n) \\ g(1) = (f_1, \ldots, f_n) \end{cases} .$$

($GL_n(\mathbb{R})$ - множество обратимых матриц $n \times n$)

Доказательство.

Предположим, что такое g существует.

Заметим, что $\det : GL_n(\mathbb{R}) \mapsto \mathbb{R}$ непрерывен, как многочлен от компонентов.

Рассмотрим $\det \circ g : [0,1] \mapsto \mathbb{R}$. Заметим, что $\det(g(0)) > 0, \det(g(0)) < 0$, значит, $\exists t \in [0,1] \quad \det(g(t))$ $0 \implies g(t) \notin GL_n(\mathbb{R})$. Противоречие. □

***Определение* 12.3.**

Пусть V - векторное пространство над K. Тогда, линейный оператор (эндоморфизм) над V - линейное отображение $L : V \mapsto V$.

***Определение* 12.4.**

Матрица линейного оператора в базисе e - $[L]_e = [L]_e^e = \big[L(e_1), L(e_2), \ldots, L(e_n)\big]$.

***Определение* 12.5.**

Определитель оператора L - $\det L = \det[L]_e$ для произвольного базиса e.

Доказательство.

Корректность:

Пусть e, f - базисы v.

Тогда

$$\exists C \in GL_n(K) \quad [L]_e = C[L]_f C^{-1}.$$

$$\det[L]_e = \det C[L]_f C^{-1} = \det C \det[L]_f \det C^{-1} = \det C \det[L]_f (\det C)^{-1} = \det[L]_f.$$ □

***Определение* 12.6.**

Пусть L - линейный оператор на V. Тогда L сохраянет ориентацию, если $\det L > 0$, и меняет ориентацию, если $\det L < 0$.

***Определение* 12.7.**

Пусть $A \in M_n(K)$, $I, J \subset \{1, \dots, n\}$. Тогда, A_{IJ} - матрица составленная из элементов, которые стоят на позициях с номерами строк из I и столбцов из J.

Замечание.

Если $I \subset \{1, \dots, n\}$, то $\overline{I} = \{x \in \{1, \dots, n\} \mid x \notin I\}$

***Определение* 12.8.**

Пусть $A \in M_n(K)$, $|I| = |J| = k$, тогда $\det A_{IJ} = M_{IJ}$ - минор матрицы A размера k.

***Определение* 12.9.**

Пусть $A \in M_n(K)$. Тогда алгебраическим дополнением элемента a_{ij} называется $A^{ij} = (-1)^{i+j} M_{\overline{ij}}$.

Лемма (О разложении определителя по столцу)**.**

Пусть $A \in M_n(K)$, задан j столбец.

Тогда существуют такие коэффициенты c_i, такие, что

$$\det A = \sum_{i=1}^{n} c_i a_{ij}.$$

При этом, $c_i = A^{ij}$.

Доказательство.

Существование коэффициентов следует из полилинейности определителя.

Рассмотрим матрицу A'_i, такую, что

$$a'_{i'j'} = \begin{cases} a_{i'j'} & j' \neq j \\ 0 & j' = j, i' \neq i \\ 1 & j' = j, i' = i \end{cases}.$$

□

Тогда $\det A'_i = c_i$.

Передвинем j-й столбец по циклу в начало, знак определителя изменится на $(-1)^{j-1}$.

Передвинем i-ю строку в начало, знак определителя изменится на $(-1)^{i-1}$, вместе с предыдущеим поменялся на $(-1)^{i-1+j-1} = (-1)^{i+j-2} = (-1)^{i+j}$.

Матрица получилась блочной, с блоками 1 и $A_{\overline{ij}}$, значит, $c_i = \det A'_i = (-1)^{i+j} \det A_{\overline{ij}} = (-1)^{i+j} M_{ij} = A^{ij}$.

Лемма (О разложении по строке)**.**

$$\det A = \sum_{j=1}^{n} a_{ij} A^{ij}.$$

Лемма (Формула Крамера)**.**

Если $A \in GL_n(K)$, то решение уравнения $Ax = b$ можно выписать в явном виде:

$$x_i = \frac{\Delta_i}{\Delta}.$$

$$\Delta = \det A.$$

Δ_i - определитель матрицы A с i-м столбцом заменённым на b

Доказательство.

Пусть v_i - i-й столбец A

Пусть $b = c_1 v_1 + \ldots +_n v_n$.

Тогда $\Delta_i = \det(v_1, \ldots, v_{i-1}, b, v_{i+1}, v_n)$.

По линейности, $\Delta_i = c_i \Delta$. **TODO:** ? □

Пример.

Найдём обратную матрицу через Крамера:

Для j-го столбца обратной мартицы верно $Ax_j = e_j$.

i-я координата такого вектора равна $x_{ij} = \frac{A^{ji}}{\Delta}$. (в i-м столбце единица на j-й позиции).

***Определение* 12.10.**

Присоеденённой к A матрицей называется матрица $\operatorname{Adj} A$, такая, что $(\operatorname{Adj} A)_{ij} = A^{ji}$

Теорема 12.2.

$$A \in M_n(K).$$

$$\operatorname{Adj} A \cdot A = A \cdot \operatorname{Adj} A = \det A E_n.$$

Доказательство.

Если A обратима, то знаем что $A^{-1} = \operatorname{Adj} A$, $AA^{-1} = A^{-1}A = E_n \implies \operatorname{Adj} A \cdot A = A \cdot \operatorname{Adj} A = \Delta E_n$.

Рассмотрим кольца R и S, причём есть гомоморфизм $\varphi : R \mapsto S$.

Заметим, что если тождетсво верно для $A \in M_n(R)$, то верно для $\varphi(A) \in M_n(S)$, так-как можно переписать тождество через многочлены.

Рассмотрим кольцо многочленов $\mathbb{Z}[a_{11}, a_{12}, \ldots, a_{nn}]$.

Тогда существует гомоморфизм в произвольное кольцо, такой, что $\varphi(a_{ij}) = b_{ij}$: подстановка.

Тогда, любая матрица является образом матрицы с коэффициентами a_{ij}.

Построим поле частных $Q(\mathbb{Z}[a_{11}, a_{12}, \ldots, a_{nn}])$, вложим наше кольцо в него.

Заметим, что в этом поле $\det A = \det A$ как многочлену, а он не 0. Для обратимых матриц в поле знаем что верно, значит верно для всех. □

***Определение* 12.11** (Алгебра)**.**

Алгеброй над полем K называется набор $\langle A, K, +, \cdot, \times \rangle$, удовлетворяющий следующим аксиомам:

1. K - поле
2. $\langle A, +, \times \rangle$ - кольцо (абсолютно произвольное).
3. $\langle A, K, +, \cdot \rangle$ - векторное пространство
4. $\lambda(a \times b) = (\lambda a) \times b = a \times (\lambda b)$, $a, b \in A$, $\lambda \in K$.

Пример.

Поле K - алгебра над собой.

Кольцо матриц $M_n(K)$ и кольцо эндоморфизмов векторных пространств $\operatorname{End}(V)$

Кольцо многочленов $K[x_1, \ldots, x_n]$.

Кольцо верхнетреугольных матриц $LT_n(K)$.

Если поле K - подполе L, то L - алгебра над K.

***Определение* 12.12.**

Пусть R, S - две K-алгебры, то $\varphi : R \mapsto S$ называется гомоморфизм алгебр, если он является линейным гомоморфизмом колец:

$$\varphi(a+b) = \varphi(a) + \varphi(b).$$
$$\varphi(\lambda a) = \lambda\varphi(a).$$
$$\varphi(a \times b) = \varphi(a) \times \varphi(b).$$

С текущего момента, все кольца и алгебры ассоциативны и с единицей, но не обязательно коммутативны.

Пример.

$$M_{\dim V}(K) \cong \mathrm{End}_K(V).$$

Пусть $y \in A$, где A - K-алгебра. Тогда можем посчитать выражение $a_0 + a_1 \cdot y + \ldots + a_n \cdot y^n$, $a_i \in K$. Назовём это многочленом от элемента алгебры.

Утверждение 12.3.

Пусть A - K-алгебра. Тогда

$$\forall y \in A \quad \exists! \varphi : K[x] \mapsto A \text{ - гомоморфизм} \quad \varphi(x) = y.$$

Прчём, этот гомоморфизм имеет вид $\varphi(p(x)) = p(y)$.

Следствие.

Если $A \in M_n(K)$, $p, q \in K[x]$, то $(pq)(A) = p(A)q(A)$.

Теорема 12.4 (Теорема типа-Кэли)**.**

Пусть A - конечномерная алгебра над K, и $\dim_K A = n$.

Тогда A вкладывается в $M_n(K)$.

Доказательство.

Будем доказывать что вкладывается в $\mathrm{End}_K(A)$.

Сопоставим каждому элементу $a \in A$ отображение $x \to a \times x$.

Покажем, что оно гомоморфизм:

$$a \times b \to (x \to (a \times b) \times x) = (x \to a \times (b \times x)).$$

Отображение будет эндоморфзимом, через дистрибутивность и спец. аксиому для алгебр.

Инъективность: $a \to (1 \to a \times 1) = a$. □

Пример.

Вложим алгебру $\mathbb{C}$ в $M_2(\mathbb{R})$:

Возьмём базис $e_1 = 1$, $e_2 = i$.

Пусть $L_z = a + bi$. Тогда $L_z(1) = a + bi$, $L_z(i) = -b + ai$.

Тогда, матрица выглядит как $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$.

Лемма.

Пусть A - конечномерная K-алгебра.

Тогда

$$\forall y \in A \quad \exists p \in K[x] \setminus \{0\} \quad p(y) = 0.$$

Доказательство.

Возьмём $1, y, \ldots, y^n$, $n = \dim A$. Получили $n+1$ элемент из A.

Значит, они линейно зависимы, значит $\exists a_i \quad a_0 \cdot 1 + \ldots + a_n y^n = 0$, причём есть ненулевой a_i. Получился многочлен. □

***Определение* 12.13.**

Пусть $y \in A$, тогда μ_y - многочлен минимальной степени, со старшим коэффициентом 1, такой, что $\mu_y(y) = 0 \in A$ называется минимальным многочленом элемента y.

***Определение* 12.14.**

Аннулятор $y \in A$, где A - конечномерная алгебра - $\operatorname{Ann}_y = \{p(y) = 0 \mid p \in K[x]\}$.

Свойство.

Ann_y - нетривиальный идеал в кольце многочленов.

Доказательство.

$$(p+g)(y) = p(y) + g(y) = 0 + 0 = 0.$$

$$(pg)(y) = p(y)g(y) = 0 \cdot 0 = 0.$$

$$0 \in \operatorname{Ann}_y.$$

Ann_y нетривиальен, по предыдущей теореме. □

Следствие.

Так-как любой идеал в $K[x]$ главный, то $\exists! \mu_y \quad \operatorname{Ann}_y = (\mu_y)$.

Лемма.

Пусть $y \in A$, A - конечномерная алгебра над K.

Тогда либо y - делитель нуля, либо y обратим.

Доказательство.

Возьмём μ_y,

$$\mu_y(y) = 0 \implies a_n y^n + \ldots + a_0 = 0.$$

Если $a_0 \neq 0$, то $y(a_n y^{n-1} + \ldots + a_1) = -a_0 \implies y^{-1} = \frac{a_n y^{n-1} + \ldots + a_1}{-a_0}$.

Если $a_0 = 0$, то $y(a_n y^{n-1} + \ldots + a_1) = 0$. Так-как μ_y - минимальный многочлен, то правый множитель не 0, значит y - делитель нуля. □

***Определение* 12.15.**

Пусть $L \in \operatorname{End}_K(V)$. Тогда, собственным вектором оператора L называется такой вектор $v \neq 0$, что $\exists \lambda \in K \quad L(v) = \lambda k$. Такое λ называется собственным числом.

Лемма.

λ является собственным чилслом L тогда и только тогда, когда $\det(L - \lambda \operatorname{id}) = 0$.

Доказательство.

v - собственный вектор L тогда и только тогда $(L - \lambda\,\mathrm{id})(v) = L(v) - \lambda v = 0$. Ненулевой вектор может перейти в 0, тогда и только тогда ядро нетривиально, а ядро нетривиально тогда и только тогда, когда определитель 0. □

***Определение* 12.16.**

Характерестический многочлен оператора L - $\chi_L(\lambda) = \det(L - \lambda\,\mathrm{id})$.