# 1. Поля и комплексные числа

1.1. **Введение.** $\mathbb{N} \subset \mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset$??
Пусть $i$ – "число" такое, что $i^2 = -1$ (т.е. $i = \sqrt{-1}$). Например,
$x^2 - 2x + 5 = 0 \Rightarrow x = 1 \pm \sqrt{1-5} = 1 \pm 2\sqrt{-1} = 1 \pm 2i$
"Проверка": $(1+2i) + (1-2i) = 2; (1+2i) \cdot (1-2i) = 1 - (2i)^2 = 5$.

Вообще, рассмотрим "числа" вида $a+bi$, где $a, b \in \mathbb{R}$ (это и "есть" комплексные числа!).
Действия:

$$(a+bi) \pm (c+di) = (a \pm c) + (b \pm d)i$$
$$(a+bi) \cdot (c+di) = ac + bci + adi + bdi^2 = (ac - bd) + (ad + bc)i$$
$$\frac{a+bi}{c+di} = \frac{(a+bi)(c-di)}{c^2+d^2} = \frac{(ac+bd) + (bc-ad)i}{c^2+d^2}$$

1.2. **Поля.**

*Определение.* Операция (точнее бинарная операция) на множестве $A$ – это отображение $A \times A \to A$.

*Примеры...*

*Определение.* Поле – это множество $F$ с заданными на нём операциями "$+$" (сложение) и "$\cdot$" (умножение), причем:

(1) $\forall a, b \in F : a + b = b + a$ (коммутативность сложения)
(2) $\forall a, b, c \in F : (a + b) + c = a + (b + c)$ (ассоциативность сложения)
(3) $\exists 0 \in F \ \forall a \in F : a + 0 = a$ (существование нуля)
(4) $\forall a \in F \ \exists (-a) \in F : a + (-a) = 0$ (существование противоположного)
(5) $\forall a, b \in F : ab = ba$ (коммутативность умножения)
(6) $\forall a, b, c \in F : (ab)c = a(bc)$ (ассоциативность умножения)
(7) $\exists 1 \in F \ \forall a \in F : a \cdot 1 = a$ (существование единицы)
(8) $\forall la \in F \diagdown \{0\} \ \exists a^{-1} \in F : a \cdot a^{-1} = 1$ (существование обратного)
(9) $\forall a, b, c \in F a(b + c) = ab + ac$ (дистрибутивность)
(10) $1 \neq 0$

*Примеры полей.* 1) $\mathbb{Q}$ 2) $\mathbb{R}$ 3) $\mathbb{Q}(\sqrt{2}) := \{a + b\sqrt{2} | a, b \in \mathbb{Q}\}$ 4) $\mathbb{F}_2 = 0, 1$, сложение и умножение по модулю 2.

*Упражнение.* Проверить, что множества из примеров 3 и 4 действительно являются полями.

*Предложение(следствия из аксиом поля).*
1) 0 единственен
2) 1 единственна

3) противоположный элемент к данному единственен
4) обратный элемент к данному (не равному нулю) единственен
5) если $a = b + c$, то $c = a + (-b) =: a - b$
6) если $a = bc$, и $b \neq 0$, то $c = ab^{-1} =: \frac{a}{b}$
7) $\forall a \in F : 0 \cdot a = 0$
8) $\forall a \in F : (-1) \cdot a = -a$
9) если $ab = 0$, то $a = 0$ или $b = 0$
10) если $ab = ac$, и $a \neq 0$, то $b = c$
*Доказательство.*
1) Пусть 0 и $0'$ – нули. Тогда $0 = 0 + 0' = 0'$
3) Пусть $a + b = a + c = 0$. Тогда $b = b + 0 = b + (a + c) = (b + a) + c = 0 + c = c$
7) Пусть $b = 0 \cdot a$. Тогда $a + b = 1 \cdot a + 0 \cdot a = (1 + 0)a = a \Rightarrow (-a) + a + b = (-a) + a \Rightarrow b = 0$. $\square$
*Упражнение.* Проверьте остальные пункты предложения.
*Определение.* $n$'ой степенью элемента $a$ поля называется выражение $\underbrace{a \cdot ... \cdot a}_{n} =: a^n$. Обозначим $a^0 := 1$ и при $a \neq 0$ $a^{-n} := (a^{-1})^n$.
*Упражнение.* В любом поле для любых $a, b \in F, m, n \in \mathbb{Z}$
1)$(a^m)^n = a^{mn}$
2)$a^{m+n} = a^m \cdot a^n$
3)$(ab)^n = a^n \cdot b^n$
*Замечание.* Пусть $F$ – удовлетворяет аксиомам (1)-(9). Тогда $1 \neq 0 \Leftrightarrow F \neq \{0\}$.
*Определение.* Подполе поля $F$ – это подмножество $G \subset F$ такое, что $1 \in G$ и для любых $a, b \in E :\ a + b, a \cdot b, -a, a^{-1} \in E$.
*Упражнение.*$E$ – подполе $F \Rightarrow\ 0 \in E$.
*Упражнение.* Подполе поля само является полем относительно "тех же"операций.
*Упражнение(транзитивность понятия подполя).* $K$ – подполе $E$,
$E$ – подполе $F \Rightarrow\ K$ подполе $F$.
*Пример.* $\mathbb{Q} \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$.
*Предложение.* Пересечение любой совокупности подполей поля – подполе.
*Доказательство.*
Единица лежит в каждом из подполей совокупности, следовательно лежит и в их пересечении. Произведение, сумма, противоположные и обратные к элементам пересечения лежат в каждом из подролей, следовательно и в их пересечении. $\square$
*Определение.* Пусть $F$ – поле, $A \subset F$. Подполе $F$ порожденное $A$ – это наименьшее среди всех полей в $F$, содержащих $A$ (то есть пересечение всех подполей в $F$ содержащих $A$).
*Примеры.*
1) $Q$ порождено $\varnothing$ (как подполе, скажем, в $\mathbb{R}$). В самом деле: 1) $\mathbb{Q}$ – подполе в $\mathbb{R}$; 2) если $E$ – подполе в $R$, то $E \ni 1 \Rightarrow E \ni 1 + 1 + ... + 1 \Rightarrow E \supset \mathbb{N}$,

тогда $E \supset \mathbb{Z} \Rightarrow E \supset \mathbb{Q}$. То есть $\mathbb{Q}$ – минимальное подполе в $\mathbb{R}$.
2) $Q(\sqrt{2})$ порождено $\{\sqrt{2}\}$. В самом деле: 1) это подполе; 2) если – подполе в $\mathbb{R}$ содержащее $\sqrt{2}$, то $E \supset \mathbb{Q}, E \ni \sqrt{2} \Rightarrow E \supset \mathbb{Q}(\sqrt{2})$. То есть $\mathbb{Q}(\sqrt{2})$ – наименьшее подполе содержащее $\sqrt{2}$.
*Задача.* Как могут быть устроены наименьшие подполя в поле (то есть порожденные $\varnothing$)?
*Определение.* Пусть $F$ – поле, $E$ – подполе в $F$, $a \in F$. Расширение $E$ с помощью $a$ – это подполе $E(a) \subset F$, порожденное множеством $E \cup \{a\}$.
*Примеры.*
1) $a \in E \Rightarrow E(a) = E$
2) $\mathbb{Q}(\sqrt{2})$ – действительно расширение $\mathbb{Q}$ с помощью $\sqrt{2}$
*Упражнение.* Как устроены $\mathbb{Q}(\sqrt[3]{2})$, $\mathbb{Q}(\sqrt{2}+\sqrt{3})$ (как подполя в $\mathbb{R}$)?

## 1.3. **Поле комплексных чисел.**

*Определение.* Поле комплексных чисел – это расширение поля $\mathbb{R}$ с помощью элемента $i$ такого, что $i^2 = -1$.
Будет показано, что такое поле существует и, по существу, единственно.
Как понимать единственность? *Определение.* Изоморфизм между полем $E$ и полем $F$ –это биективное отображение $\varphi : E \to F$ такое, что для любых
$a, b \in E : \varphi(a+b) = \varphi(a) + \varphi(b), \varphi(ab) = \varphi(a)\varphi(b)$.
Поле $E$ изоморфно полю $F$ (обозначается $E \cong F$), если между $E$ и $F$ существует изоморфизм.
*"Принцип изоморфизма":* В изоморфных полях операции "действуют одинаково". Поэтому изоморфные поля можно отождествить.
*Примеры.* $\mathbb{Q} \ncong \mathbb{R}$; $\mathbb{Q} \ncong \mathbb{Q}(\sqrt{2})$; $\mathbb{F}_2 \ncong \mathbb{Q}$.
*Упражнение.* Докажите, что приведенные выше поля неизоморфны.
"Труднее" привести пример изоморфных полей...(например, разные определения вещественных чисел приводят к изоморфным полям).
*Упражнение.* Если $\varphi$ – изоморфизм полей, то $\varphi(0) = 0, \varphi(1) = 1, \varphi(-a) = -\varphi(a), \varphi(a^{-1}) = (\varphi(a))^{-1}$.
*Упражнение.*
1) Тождественное отображение $id : F \to F$ – изоморфизм. В частности $F \cong F$.
2) Если $\varphi : E \to F$ – изоморфизм, то $\varphi^{-1} : F \to E$ – тоже изоморфизм. В частности, если $E \cong F$, то $F \cong E$.
3) Если $\varphi : E \to F$, $\psi : F \to K$ – изоморфизмы, то $\psi \circ \varphi : E \to K$ – изоморфизм. В частности, если $E \cong F, F \cong K$, то $E \cong K$.
(Резюме: отношение изоморфности есть отношение эквивалентности.)
*Определение.* Автоморфизм поля $F$ – это изоморфизм $F$ с собой.
*Упражнение.* 1) Любой автоморфизм поля $\mathbb{Q}$ – тождественен.

2*) Любой автоморфизм поля $\mathbb{R}$ – тождественен (в частности, если $F_1 \cong F_2 \cong \mathbb{R}$, то изоморфизм $\varphi : F_1 \to F_2$ единственен; то есть вещественные числа "имеют индивидуальности").

**Теорема.** Поле комплексных чисел существует и единственно с точностью до изоморфизма, тождественного на $\mathbb{R}$.

*Доказательство.*

Единственность: Пусть $E$ – поле комплексных чисел, то есть $E = \mathbb{R}(i)$, где $i^2 = -1$ (подразумевается, что $\mathbb{R}$ и $i$ лежат в некотором поле $F$).

*Лемма.* Элементы $E$ однозначно записываются в виде $a + bi$, где $a, b \in \mathbb{R}$.

*Доказательство леммы*: Пусть $\tilde{E} := \{a + bi | a, b \in \mathbb{R}\} \subset F$.

1)$\tilde{E}$ – подполе в $F$(*Упражнение*).

2) Любое подполе $F$ содержащее $\mathbb{R}$ и $i$, содержит $\tilde{E}$. То есть $\tilde{E} = E$.

3) $a + bi = c + di \Rightarrow a - c = (d - b)i \Rightarrow (a - c)^2 = -(d - b)^2 \Rightarrow a = c, b = d$.

Теперь пусть $E' = \mathbb{R}(i')$ – другое поле комплексных чисел; $(i')^2 = -1$. Определим $\varphi : E \to E', \varphi(a + bi) := a + bi'$. Тогда $\varphi$ – изоморфизм, причем $\varphi$ тождественен на $\mathbb{R}$.

Существование: Укажем одну из "реализаций"поля комплексных чисел. Рассмотрим множество $E := \mathbb{R} \times \mathbb{R} = \{(a, b) | a, b \in \mathbb{R}\}$. Введём в $E$ операции: $(a, b) + (c, d) := (a + c, b + d)$, $(a, b) \cdot (c, d) := (ac - bd, ad + bc)$. Пусть $K := \{(a, 0) | a \in \mathbb{R}\}$ .

*Упражнение.* $E$ – поле, $K$ – подполе в $E$, и отображение $\varphi : \mathbb{R} \to K$,
$\varphi(a) := (a, 0)$ – изоморфизм.

Отождествим $K$ с $\mathbb{R}$ с помощью $\varphi$. Положим $i := (0, 1)$; $i^2 = (-1, 0) = -1$; $(a, b) = a + bi$.

*Упражнение.* $K = \mathbb{R}(i)$.

□

*Обозначения:* $\mathbb{C}$ – поле комплексных чисел. Если $z \in \mathbb{C}$, то $z = a + bi$, где $a, b \in \mathbb{R}$ определены однозначно. $a$ называют вещественной частью $z$ ($a = Re(z)$), а $b$ – мнимой частью $z$ ($b = Im(z)$).($a + bi = c + di \Leftrightarrow a = c, b = d$)

*Комплексное сопряжение.* Пусть $z = a + bi \in \mathbb{C}$, где $a, b \in \mathbb{R}$. Число $\bar{z} := a - bi$ называется комплексно сопряженным к $z$. Ясно, что $\bar{\bar{z}} = z$ и $\bar{z} = z \Leftrightarrow z \in \mathbb{R}$. Так как $\mathbb{C} = \mathbb{R}(-i)$, где $(-i)^2 = -1$, то $z \to \bar{z}$ – автоморфизм поля $\mathbb{C}$ (то есть $\overline{z + w} = \bar{z} + \bar{w}, \overline{zw} = \bar{z} \cdot \bar{w}$). При этом $\mathbb{R}$ остаётся на месте.

*Упражнение.* Пусть $\varphi : \mathbb{C} \to \mathbb{C}$ – автоморфизм, тождественный на $\mathbb{R}$. Тогда либо $\varphi = id$, любо $\varphi$ – комплексное сопряжение (то есть комплексные числа имеют индивидуальность лишь с тосностью до сопряжения; нет принципиальной разницы между $i$ и $-i$).

PICTURE

1.4. **Геометрическая интерпретация.**
Сопоставим каждому комплексному $z = a + bi,\ a, b \in \mathbb{R}$ точку плоскости с координатами $(a, b)$.
*Замечание.* Сложению комплекных чисел соответствует сложение радиус-векторов.
Если $z \neq 0$, то можно рассмотреть полярные координаты $(r, \varphi)$. Ясно, что $a = rcos(\varphi), b = rsin(\varphi)$. Обратно, $r = \sqrt{a^2 + b^2}$; $\varphi$ определяется (mod $2\pi$) из формул $cos(\varphi) = \frac{a}{r}$, $sin(\varphi) = \frac{b}{r}$. Число $r$ называют модулем $z$ (обозначение: $r := |z|$), $\varphi$ – аргумент $z$.
Обычно пишут $arg(z)$ для какого-нибудь значения, $Arg(z)$ – для всех значений, то есть $Arg(z) = \{arg(z) + 2\pi n | n \in \mathbb{Z}\}$.
Итак, $z = r(cos(\varphi)+isin(\varphi))$ – тригонометрическая форма комплексного числа.
Заметим, что $r(cos(\varphi) + isin(\varphi)) = \rho(cos(\psi) + isin(\psi)) \Leftrightarrow r = \rho, \psi = \varphi + 2\pi n$, $n \in \mathbb{Z}$.
Тригонометрическая форма "приспособлена"к умножению:
*Предложение.* Пусть $z_1 r_1(cos(\varphi_1) + isin(\varphi_1)), z_2 = r_2(cos(\varphi_2) + isin(\varphi_2))$. Тогда $z_1 z_2 = r_1 r_2(cos(\varphi_1 + \varphi_2) + isin(\varphi_1 + \varphi_2))$.
*Упражнение.* Докажите предложение.
*Следствие.* В условиях предложения при $z_2 \neq 0$
$\frac{z_1}{z_1} = \frac{r_1}{r_2}(cos(\varphi_1 - \varphi_2) + isin(\varphi_1 - \varphi_2))$
*Следствие (формула Муавра).* Пусть $z = r(cos(\varphi) + isin(\varphi)),\ n \in \mathbb{Z}$. Тогда $z^n = r^n(cos(n\varphi) + isin(n\varphi))$.
*Доказательство:* Случай $n = 0$ тривиален. При $n \in \mathbb{N}$ применяем индукцию по $n$ и предложение, при $n < 0$ индукцию и предыдущее следствие.
*Замечание.* Для $\varphi \in \mathbb{R}$ положим по определению $e^{i\varphi} := cos(\varphi) + isin(\varphi)$.
Мотивировка: $e^{i\varphi_1 + i\varphi_2} = e^{i\varphi_1} e^{i\varphi_2}$.
Далее, положим $e^{a+bi} := e^a e^{bi} = e^a(cos(b) + isin(b))$. Тогда $e^{z_1+z_2} = e^{z_1} e^{z_2}$.
*Упражнение (ещё свойства модуля).*
1) $|z|^2 = z\tilde{z}$
2)$|z \pm w| \leq |z| + |w|$
3)$|z \pm w| \geq ||z| - |w||$
4)$|z - w|$ = расстояние от $z$ до $w$.

1.5. **Корни из комплексных чисел.**
Пусть $w \in \mathbb{C},\ n \in \mathbb{N}$. Что такое $\sqrt[n]{w}$?
*Определение.* Корни $n$-ой степени из $w$ это решения уравнения $z^n = w$.
*Упражнение.* $z^n = 0 \Rightarrow z = 0$.
*Предложение.* Пусть $w \in \mathbb{C}, w \neq 0$. Тогда существует ровно $n$ корней $n$-ой

степени из $w$. Если $w = r(cos(\varphi) + isin(\varphi))$, то эти корни имеют вид

$$z_k = \sqrt[k]{r}\left(cos\left(\frac{\varphi + 2\pi k}{n}\right) + isin\left(\frac{\varphi + 2\pi k}{n}\right)\right)\ ,\ k = 0,\ 1, ...,\ n-1$$

*Доказательство.* Ищем решения в виде $z = \rho(cos(\psi) + isin(\psi))$. Имеем $z^n = w \Leftrightarrow \rho^n = r,\ n\psi = \varphi + 2\pi k$, где $k \in \mathbb{Z}$. Пусть $z_k = \sqrt[k]{r}\left(cos\left(\frac{\varphi+2\pi k}{n}\right) + isin\left(\frac{\varphi+2\pi k}{n}\right)\right)$.
При каких $k$ решения одинаковы? $z_k = z_l \Leftrightarrow \frac{\varphi+2\pi l}{n} = \frac{\varphi+2\pi k}{n} + 2\pi m \Leftrightarrow l = k + mn$.
То есть достаточно брать $k = 0, 1, ..., n-1$.
Важный частный случай: корни из единицы. Важен, например, потому, что если $z_1^n = z_2^n \neq 0$, то $(\frac{z_1}{z_2})^n = 1$. То есть, если $z$ – один из корней степени $n$ из $w \neq 0$, то все прочие – это в точности $z \cdot \varepsilon$, где $\varepsilon$ – некоторый корень степени $n$ из единицы.
*Следствие.* Корни степени $n$ из единицы – это в точности
$\varepsilon_k = cos(\frac{2\pi k}{n}) + isin(\frac{2\pi k}{n}),\ k = 0, 1, ..., n-1$.
*Замечание.* Корни $n$-ой степени из 1 являются вершинами правильного $n$-угольника.
*Замечание.* $\varepsilon_0 = 1,\ \varepsilon_1 = cos(\frac{2\pi}{n}) + isin(\frac{2\pi}{n}),\ \varepsilon_k = \varepsilon_1^k$ (по формуле Муавра). То есть все корни из единицы степени $n$ – степени фиксированого. Этот "образующий"не обязательно (только) $\varepsilon_1$.
*Пример.* $n = 6$: Ту же роль играет $\varepsilon_5 = \varepsilon_1^{-1}$. Но не $\varepsilon_2, \varepsilon_3, ...$
Систематизируем:
Пусть $\varepsilon \in \mathbb{C}$ – корень из единицы (некоторой степени).
*Определение.* $\varepsilon$ – примитивный (=первообразный) корень из 1 степени $n$ (ещё синоним: $\varepsilon$ имеет порядок $n$), если $\varepsilon^n = 1$, и $\varepsilon^k \neq 1$, при $1 \leq k \leq n-1$.
Ясно, что каждый корень из единицы примитивный некоторой степени.
*Обозначение:* если $m, n \in \mathbb{Z}$, то $n|m \Leftrightarrow n$ делит $m$, то есть существует $k \in \mathbb{Z}$ : $m = nk$.
*Лемма* Пусть $\varepsilon$ – примитивный корень степени $n$ из единицы, $m \in \mathbb{Z}$. Тогда $\varepsilon^m = 1 \Leftrightarrow n|m$.
*Доказательство:* $\Leftarrow$: $n|m \Rightarrow \varepsilon^m = (\varepsilon^n)^k = 1$.
$\Rightarrow$: Поделим с остатком: $m = nl + r,\ 0 \leq r < n$. Тогда $1 = \varepsilon^m = \varepsilon^{nk+r} = \varepsilon^r$. Но $r < n$, значит $r = 0$. $\square$
*Предложение.* Пусть $\varepsilon$ – примитивный корень степени $n$ из единицы. Тогда все корни степени $n$ из единицы – это $1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}$.
*Доказательство.* 1) $(\varepsilon^k)^n = (\varepsilon^n)^k = 1$.
2) $\varepsilon^k = \varepsilon^l \Leftrightarrow \varepsilon^{k-l} = 1 \Leftrightarrow n|k-l$, то есть $k \equiv l\ mod\ n$. Если $0 \leq k, l \leq n-1$, то это возможно лишь при $k = l$.
Итак, имеем $n$ различных корней $n$-ой степени из $1 \Rightarrow$ это все корни. $\square$
*Замечание.* Обратно, если $\varepsilon$ – корень степени $n$ из единицы такой, что $1, \varepsilon, \varepsilon^2, ..., \varepsilon^{n-1}$ – все корни степени $n$ из единицы, то $\varepsilon$ – примитивный корень степени $n$.
Как явно описать все примитивные корни степени $n$?

**Теорема.** Пусть $\varepsilon$ – примитивный корень степени $n$ из единицы, $k \in \mathbb{N}$. Тогда $\varepsilon^k$ – примитивный корень степени $n$ из единицы $\Leftrightarrow n, k$ взаимно просты.
*Доказательство.* $\Rightarrow$: Пусть $d|n,\ d|k$, то есть $n = d\tilde{n},\ k = d\tilde{k}$.
Тогда $(\varepsilon^k)^{\tilde{n}} = (\varepsilon^n)^{\tilde{k}} = 1$. Если $d > 1$, то $\tilde{n} < n \Rightarrow \varepsilon^k$ не примитивный степени $n$.
$\Leftarrow$: Пусть $m \in \mathbb{N}$ таков, что $\varepsilon^{km} = (\varepsilon^k)^m = 1$. Тогда $n|km \Rightarrow n|m$. Среди таких $m$ наибольшее – это $n$. $\square$
*Следствие.* $cos\left(\frac{2\pi k}{n}\right) + isin\left(\frac{2\pi k}{n}\right)$ – примимитивный степени степени $n \Leftrightarrow n$ и $k$ – взаимно просты (то есть если получим несократимую дробь $\frac{k}{n}$, то в знаменателе – порядок).
*Замечание (о группах).* Группа – это множество с одной операцией, которая ассоциативна, имеет нейтральный элемент, и у любого элемента есть обратный (аксиомы 2,3,4 поля).
Например: 1) Если $F$ – поле, то $F$ – группа относительно "+" , $F^* := F \setminus \{0\}$ – группа относительно "$\cdot$".
2) $\sqrt[n]{1} \subset \mathbb{C}^*$– (под)группа (относительно "$\cdot$")
Эти группы "коммутативны"(то есть операции коммутативны).
Мы видели, что все элементы $\sqrt[n]{1}$ – степени некоторого элемента("образующего"). Это по определению означает, что $\sqrt[n]{1}$ – *циклическая* группа.
*Задача.* Дайте определение изоморфизма групп, и докажите любая циклическая группа из $n$ элементов изоморфна $\sqrt[n]{1}$. Как устроены бесконечные циклические группы?

## 1.6. **Уравнения малых степеней.**

### 1.6.1. *Квадратные уравнения.*

$ax^2 + bx + c = 0,\ a, b, c \in \mathbb{C},\ a \neq 0$

$$ax^2 + bx + c = a\left(x^2 + \frac{b}{a}x + \frac{c}{a}\right) = a\left(\left(x + \frac{b}{2a}\right)^2 - \frac{b^2}{4a^2} + \frac{c}{a}\right)$$

Значит корни имеют вид $-\frac{b}{2a} \pm \sqrt{\frac{b^2}{4a^2} - \frac{c}{a}} = \frac{-b \pm \sqrt{D}}{2a}$, где $D := b^2 - 4ac$.

При этом $D = 0 \Rightarrow$ корень один, $D \neq 0 \Rightarrow$ корней два.
Если $a, b, c \in \mathbb{R}$, то $D > 0 \Rightarrow$ два вещественных корня, $D < 0 \Rightarrow$ вещественных корней нет.
*Упражнение* Если корни уравнения обозначить $x_1$ и $x_2$, то $D = a^2(x_1 - x_2)^2$

1.6.2. *Кубические уравнения.*
$x^3 + ax^2 + bx + c = 0,\ a, b, c \in \mathbb{C}$
1) $y := x + \frac{a}{3} \Rightarrow$ уравнение принимает вид $y^3 + py + q = 0$
2) Далее считаем, что уравнение имеет вид $x^3 + px + q = 0(*)$. Подставим $x = \alpha + \beta$, т.е. $(\alpha+\beta)^3 + p(\alpha+\beta) + q = 0$ или $\alpha^3 + \beta^3 + (\alpha+\beta)(3\alpha\beta + p) + q = 0$. Потребуем дополнительно, чтобы $3\alpha\beta + p = 0$, тогда уравнение принимает вид $\alpha^3 + \beta^3 + q = 0$.

Точнее: $(*) \Leftrightarrow \exists \alpha, \beta : \begin{cases} \alpha + \beta = x \\ \alpha\beta = -\frac{p}{3} \\ \alpha^3 + \beta^3 = -q \end{cases}$ ($\Rightarrow$: нужно взять $\alpha, \beta$ корнями $t^2 - xt - \dfrac{p}{3} = 0$)

Итак нам нужно решить систему $(**)$ $\begin{cases} \alpha\beta = -\frac{p}{3} \\ \alpha^3 + \beta^3 = -q \end{cases}$ и вычислить $\alpha + \beta$.

$(**) \Rightarrow \begin{cases} \alpha^3\beta^3 = -\frac{p^3}{27} \\ \alpha^3 + \beta^3 = -q \end{cases} \Leftrightarrow \alpha^3,\ \beta^3$ $--$корни квадратного уравнения $t^2 + qt - \dfrac{p^3}{27}$

Итого получаем $x = \sqrt[3]{-\dfrac{q}{2} + \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}} + \sqrt[3]{-\dfrac{q}{2} - \sqrt{\dfrac{q^2}{4} + \dfrac{p^3}{27}}}$ (формула Кардано)

Уточнение: корней всего не более трех (а не 9...)
Надо не забывать о $\alpha\beta = -\frac{p}{3}$, то есть "согласовать" значения кубических корней.
Именно, если $\alpha, \beta$ таковы, что

$\begin{cases} \alpha^3 = -\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \\ \beta^3 = -\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}} \end{cases}$, причем $\alpha\beta = -\dfrac{p}{3}$, то $x = \alpha + \beta$ – решение уравнения (*).

Если $\alpha, \beta$ – одна такая пара, то другие – это $\varepsilon\alpha, \varepsilon^2\beta$ и $\varepsilon^2\alpha, \varepsilon\beta$, где $\varepsilon$ – корень кубический из единицы.
То есть $x_1 = \alpha + \beta$
$x_2 = \varepsilon\alpha + \varepsilon^2\beta = \varepsilon\alpha + \bar{\varepsilon}\beta$
$x_3 = \varepsilon^2\alpha + \varepsilon\beta = \bar{\varepsilon}\alpha + \beta$
Обозначим $D := -4p^3 - 27q^2 = -4 \cdot 27 \left(\frac{q^2}{4} + \frac{p^3}{27}\right)$ – дискриминант уравнения (*).
Заметим, что $D = -27(\alpha^3 - \beta^3)^2$
*Предложение.* Число корней уровнения (*) меньше трёх тогда и только тогда, когда $D = 0$.
*Доказательство.*Имеем $D = 0 \Leftrightarrow \alpha^3 = \beta^3$
1) $\beta = \alpha \Leftrightarrow x_2 = (\varepsilon + \bar{\varepsilon})\alpha = x_3$

2) $\beta = \varepsilon\alpha \Leftrightarrow x_1 = (\varepsilon + 1)\alpha = x_2$
2) $\beta = \varepsilon^2\alpha \Leftrightarrow x_1 = (\varepsilon^2 + 1)\alpha = x_3$ $\square$
*Упражнение.* $D = (x_1 - x_2)^2(x_2 - x_3)^2(x_3 - x_1)^2$
Пусть теперь $p, q \in \mathbb{R}$. Сколько вещественных корней имеет (*)? *Предложение.* 1) Если $D < 0$, то (*) имеет 1 вещественный корень (два другие – комплексно сопряжены)
2) Если $D > 0$, то (*) имеет 3 вещественных корня.
*Доказательство.* 1) $D < 0 \Rightarrow \alpha^3, \beta^3 \in \mathbb{R}$. Так как ещё и $\alpha\beta = -\frac{p}{3} \in \mathbb{R}$, то можно считать, что $\alpha, \beta \in \mathbb{R}$. Отсюда $x_1 = \alpha + \beta \in \mathbb{R}$, $x_2 = \overline{x_3} \notin \mathbb{R}$
2)$D < 0 \Rightarrow \beta^3 = \bar{alpha}^3 \notin \mathbb{R}$. Так как $\alpha\beta \in \mathbb{R}$, то $\beta = \bar{\alpha}$.
Тогда $x_1 = \alpha + \bar{\alpha} \in \mathbb{R},\ x_2 = \varepsilon\alpha + \overline{\varepsilon\alpha},\ x_3 = \varepsilon^2\alpha + \overline{\varepsilon^2\alpha}$. $\square$
*Упражнение.* Что если $D = 0$?
*Замечание.* Если $D > 0$, то для решения (*) (вычисления $\alpha, \beta$) нужно извлекать корни из комплексных чисел. В "общем" случае это нелегко сделать (ибо как вычислить аргумент?...).
*Пример.* $x^3 - 7x - 6 = 0$(корни: $-1; -2; -3$).
Нетрудно видеть, что $\alpha^3 = 3 + \frac{10}{3\sqrt{3}}i;\ \beta^3 = 3 - \frac{10}{3\sqrt{3}}i$. Пишем $\alpha = r(cos(\varphi) + isin(\varphi))$. Тогда $r = \sqrt{\frac{7}{3}}$ и $cos(3\varphi) = \frac{9}{7}\sqrt{\frac{3}{7}}$. Нужно найти $cos(\varphi)$. $cos(3\varphi) = 4cos^3(\varphi) - 3cos(\varphi)$. Обозначим $t := cos(\varphi)$. Тогда получаем уравнение: $4t^3 - 3t - \frac{9}{7}\sqrt{\frac{3}{7}} = 0$. Более того $\tau := 2\sqrt{\frac{7}{3}}t \Rightarrow \tau^3 - 7\tau - 6 = 0$!!!
На самом деле так получится в общем случае... То есть особой пользы в случае $D > 0$ не получим.

## 2. Кольца и многочлены

### 2.1. **Определение и примеры колец.**

*Определение.* Коммутативное кольцо с единицей – это множество $R$ с заданными

на нем операциями "+" и "$\cdot$" , причем выполняется

(11) $\forall a, b \in R: \ a + b = b + a$

(12) $\forall a, b, c \in R: \ (a + b) + c = a + (b + c)$

(13) $\exists 0 \in R \ \forall a \in R: \ a + 0 = a$

(14) $\forall a \in R \ \exists - a \in R: \ a + (-a) = 0$

(15) $\forall a, b \in R: \ a \cdot b = b \cdot a$

(16) $\forall a, b, c \in R: \ (a \cdot b) \cdot c = a \cdot (b \cdot c)$

(17) $\exists 1 \in R \ \forall a \in R: \ a \cdot 1 = a$

(18) $\forall a, b, c \in R: \ a \cdot (b + c) = a \cdot b + a \cdot c$

*Комментарий.* Имеются варианты этого определения. Аксиомы (1)-(4); (8) – всегда. Чаще всего и (6). Не выполняется (7) $\Leftrightarrow$ кольцо без 1. Не выполняется (5) $\Leftrightarrow$ кольцо некоммутативно (тогда нужны модификации (7) $\rightsquigarrow a \cdot 1 = 1 \cdot a = a$, к (8) добавить $(a + b) \cdot c = a \cdot c + b \cdot c$). У нас, (если не оговорено обратное) пока *кольцо* = коммутативное кольцо с 1.

*Упражнение* (следствия из аксиом кольца). В любом кольце 1) 0 – единственен; 2)1 – единственна; 3) противоположный элемент к данному единственен; 4) $a = b + c \Rightarrow c = a + (-b) =: a - b$; 5) $0 \cdot a = 0$; 6) $(-1) \cdot a = (-a)$.

*Упражнение.* Сформулировать понятие степени и проверить те же свойства, что для полей.

*Примеры колец.*1. Любое поле является кольцом.

2. $\{0\}$ – кольцо (но, по определению, не поле).

3. $\mathbb{Z}$ – кольцо.

4. Множество всех функций (скажем) $\mathbb{R} \to \mathbb{R}$ – кольцо (относительно каких операций?)

5) *Кольца вычетов.* Зафиксируем $n \in \mathbb{N}$. Напомним: $x, y \in \mathbb{Z}$; $x \equiv y \ mod \ n \overset{def}{\Leftrightarrow} n|(x - y)$.

*Упражнение.* Проверить рефлексивность, симметричность, транзитивность.

Идея: сделать отношение сравнения $mod \ n$ "настоящим" равенством. Где?

*Определение.* $x \in \mathbb{Z} \Rightarrow [x] = [x]_n := \{y \in \mathbb{Z} | x \equiv y \ mod \ n\}$ – класс вычетов $x \ mod \ n$ (иногда пишут $\bar{x}$, $x \ mod \ n$, *etc.*).

Отметим, что (по определению) $[x]_n = [y]_n \Leftrightarrow x \equiv y \ mod \ n$.

Очевидно, что $\mathbb{Z} = [0]_n \sqcup [1]_n \sqcup ... \sqcup [n-1]_n$.

*Замечание.* $0, 1, 2, ..., n-1$ – "стандартная" система представителей классов, однако "намертво" фиксировать не всегда удобно.

*Определение.* $\mathbb{Z}(n) \overset{def}{=} \{[x]_n | x \in \mathbb{Z}\}$. Очевидно, что $|\mathbb{Z}(n)| = n$.

Введём операции в $\mathbb{Z}(n)$ : $[x] + [y] := [x + y]$ $[x] \cdot [y] := [xy]$

*Пример.* $[2]_3[2]_3 = [4]_3 = [1]_3$; $[2]_4[2]_4 = [4]_4 = [0]_4$.

Проверка корректности определения: пусть $[x_1] = [x_2]$; $[y_1] = [y_2]$. Почему $[x_1 + y_1] = [x_2 + y_2]$; $[x_1 y_1] = [x_2 y_2]$?
Проверим для умножения: $x_1 y_1 - x_2 y_2 = (x_1 - x_2)y_1 + x_2(y_1 - y_2)$ – кратно $n$.
*Упражнение.* Проверьте корректность для сложения.
*Предложение.* $\mathbb{Z}(n)$ – кольцо (относительно введеных операций).
*Упражнение.* Докажите предложение.
Терминология: $\mathbb{Z}(n)$ – кольцо вычетов по модулю $n$.
*Задача (будет познее решена).* $\mathbb{Z}(n)$ – поле $\Leftrightarrow$ $n$ – простое число.
Например $\mathbb{Z}(2)$ – поле. $\mathbb{Z}_2 \cong \mathbb{F}_2 :\ [0]_2 \leftrightarrow 0;\ [1]_2 \leftrightarrow 1$.
Пусть $R, S$ – кольца.
*Определение.* Изоморфизм между $R$ и $S$ – это биективное отображение $\varphi : R \to S$ такое, что $\varphi(a+b) = \varphi(a) + \varphi(b),\ \varphi(ab) = \varphi(a)\varphi(b)$. $R$ изоморфно $S$ ($R \cong S$), если существует изоморфизм между $R$ и $S$.
*Упражнение.* $\varphi$ – изоморфизм колец $\Rightarrow\ \varphi(0) = 0,\ \varphi(-a) = -\varphi(a),\ \varphi(1) = 1$.
*Упражнение.* Отношение изоморфности рефлексивно, симметрично и транзитивно.
*Определение.* Подкольцо кольца $R$ – это подмножество $S \subset R$ такое, что $1 \in S$, и если $a, b \in S$, то $-a,\ a + b,\ ab \in S$. Подкольцо кольца– само кольцо относительно "тех же" операций.
*Пример.* $\mathbb{Z}$ – подкольцо в $\mathbb{Q}$ (но не подполе).
*Делители нуля.* Пусть $R$ – кольцо, $a \in \mathbb{R},\ a \neq 0$. *Определение.* $a$ – делитель нуля, если существует ненулевое $b$ такое, что $ab = 0$.
*Определение.* $R$ целостно, если в $R$ нет делителей нуля, и $R \neq \{0\}$ (то есть $1 \neq 0$).
*Примеры.* 1) $F$ – поле $\Rightarrow$ $F$ – целостно.
2)$\mathbb{Z}$ – целостно.
3)$\mathbb{Z}(4)$ не целостно. Вообще, если $n$ – составное число, то $Z(n)$ не целостное (и, в частности, не поле): если $n = n_1 n_2$, где $1 < n_1, n_2 < n$, то $a := [n_1],\ b := [n_2]$ таковы, что $a \neq 0, b \neq 0$, но $ab = 0$.
*Упражнение.* Докажите, что кольцо всех функций $\mathbb{R} \to \mathbb{R}$ не целостно и охарактерезуйте делители нуля.
*Упражнение.* Пусть $R$ – целостное кольцо, $a, b \in R,\ c \neq 0\ ac = bc$. Тогда $a = b$ (то есть в целостном кольце "можно сокращать").

## 2.2. **Кольцо многочленов одной переменной.**

*Введение (эвристические соображения).* Многочлен от $x$ – это "выражение" вида $a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$, где $a_i \in$ чему нибудь... Будем считать $a_i \in R$ – кольцо. Когда два многочлена равны?
Пусть $f = a_n x^n + \ldots + a_1 x + a_0$, $g = b_n x^n + \ldots + b_1 x + b_0$.
Вариант 1. Равенство "как формальных выражений" $f = g \Leftrightarrow \forall k a_k = b_k$.

Вариант 2. Равенство "как функций" $f = g \Leftrightarrow \ \forall t \in R\ a_n t^n + \ldots + a_1 t + a_0 = b_n t^n + \ldots + b_1 t + b_0$.
Вариант 1 $\Rightarrow$ Вариант 2; обратное (вообще говоря) не верно: например,
$R = F_2,\ f = x^2, g = x$.
Примем вариант 1: многочлен $\leftrightarrow$ последовательность (набор) его коэффициентов.
Перейдем к более точным определениям.
Пусть $R$ – кольцо. Хотим определить кольцо $R[x]$ – *кольцо многочленов от переменной $x$.*
*Определение.* Элемент $R[x]$ – это последовательность $(a_0, a_1, a_2, \ldots, a_n, \ldots)$, где $a_n \in R$, причем $a_n = 0$ для достаточно больших $n$ (т.е. $\exists N \forall n > N : a_n = 0$ ). (Часто пишут $a_n = 0$ при $n >> 0$).
Пусть $f, g \in R[x]$, $f = (a_0, a_1, \ldots)$, $g = (b_0, b_1, \ldots)$.
*Определение.* $f+g := (a_0+b_0, a_1+b_1, \ldots)$; $fg := (c_0, c_1, \ldots)$, где $c_n = \sum_{k+l=n} a_k b_l = \sum_{k=0}^{n} a_k b_{n-k} = a_0 b_n + a_1 b_{n-1} + \ldots + a_n b_0$.
*Комментарий.* 1). Эти формулы согласованы с условиями сложения и умножения "выражений": $\sum_k a_k x^k \cdot \sum_l b_l x^l = \sum_{k,l} a_k b_l x^{k+l} = \sum_n c_n x^n$, где $c_n = \sum_{k+l=n} a_k b_l$.
2). Если последовательности для $f, g$ "обрываются" (т.е. $f, g \in R[x]$ ), то и $f + g, f \cdot g \in R[x]$ : если $a_{m+1} = a_{m+2} = \ldots = 0$, $b_{n+1} = b_{n+2} = \ldots = 0$, то $c_{m+n+1} = c_{m+n+2} = \ldots = 0$.
3). Можно (и бывает полезно) рассматривать *все* последовательности $R[[x]]$ – те же определения операций. *Формальные степенные ряды.*
*Предложение.* $R[x]$ – кольцо.
Пусть $S = \{(a, 0, 0, \ldots) | a \in R\}$.
*Лемма.* $S$ – подкольцо в $R[x]$, причем $R \cong S$.
*Доказательство.* $(a, 0, 0, \ldots) \pm (b, 0, 0, \ldots) = (a \pm b, 0, 0, \ldots) \in S$;
$(a, 0, 0, \ldots) \cdot (b, 0, 0, \ldots) = (a \cdot b, 0, 0, \ldots) \in S$;
$1 = (1, 0, 0, \ldots) \in S$.
$\varphi : R \to S, \varphi(a) := (a, 0, 0, \ldots)$ – изоморфизм. $\square$
Отождествим $S$ с $R$ с помощью $\varphi$, т.е. $a = (a, 0, 0, \ldots)$, $R \subset R[x]$. Пусть $x = (0, 1, 0, 0, \ldots) \in R[x]$.
*Лемма.* Пусть $f \in R[x]$, $f = (a_0, a_1, a_2, \ldots, a_n, 0, 0, \ldots)$. Тогда $f = \sum_{k=0}^{n} a_k x^k - a_0 + a_1 x + \ldots + a_n x^n$
*Доказательство.* Сначала найдем $x^k = (\underbrace{0, 0, \ldots, 0}_{(k-1)\text{штука}}, \underbrace{1}_{k}, 0, 0, \ldots)$. Индукция по $k$ с тривиальной базой;
Далее, $a_k x^k = (a_k, 0, 0, ...) \cdot (0, 0, ..., \underset{k}{1}, 0, ...) = (0, 0, ..., \underset{k}{a_k}, 0, ...) \Rightarrow f = \sum_{k=0}^{n} a_k x^k$
$\square$
Отныне и присно будем писать многочлен в виде $f = \sum_{k=0}^{n} a_k x^k$.

Итак, по определению $\sum a_k x^k = \sum b_k x^k \Leftrightarrow \ \forall k : a_k = b_k$
*Терминология.* Пусть $f \in R[x],\ f \neq 0,\ = a_n x^n + ... + a_0$, где $a_k \in R$, причем $a_n \neq 0$. Тогда $n$ – степень $f$ (обозначение $n = deg\ f$) $a_n x^n$ – старший член $f$, $a_n$ – старший коэффициент, $a_0$ – свободный член.
Иногда считают, что $def\ 0 = -\infty$.
*Предложение.* Пусть $R$ – целостное кольцо. Тогда (1) $R[x]$ – целостно, (2) Если $f, g \in R[x]$, то $deg\ fg = deg\ f + deg\ g$.
*Доказательство.* Пусть $f, g \neq 0,\ f = a_m x^m +$ члены меньшей степени, $g = b_n x^n +$члены меньшей степени, $a_m, b_n \neq 0$. Тогда $fg = a_m b_n x^{m+n} +$члены меньшей степени
Поскольку $R$ целостно, то $a_m b_n \neq 0$, значит $deg\ fg = deg\ f + deg\ g$. $\square$
*Упражнение.* (1) $deg(f + g) \leq max(deg\ f,\ deg\ g)$
(2) Если $deg\ f \neq deg\ g$, то $deg\ (f \pm g) = max(deg\ f, deg\ g)$.

## 2.3. **Делимость в кольцах.**

Пусть $R$ – кольцо, $a, b \in R$.
*Определение.* $b$ делит $a$ ($a$ делится на $b$; обозначение $b|a$) если существует $c \in R :\ a = bc$.
*Пример.* $\forall b \in R :\ b|0$. С другой стороны, если $0|a$, то $a = 0$ (не путать с делителями нуля, то было более "тонкое"понятие).
*Замечание.* Если $b|a$, то не всегда можно говорить о “частном”. Например, в $\mathbb{Z}(4)$ $[2][1] = [2][3] = [2]$.
*Упражнение (простейшие свойства делимости).*
1) $a|a$
2) $a|b,\ b|c \Rightarrow\ a|c$
3)$a|b_1,\ a|b_2 \Leftrightarrow \forall c_1, c_2 :\ a|(c_1 b_1 + c_2 b_2)$
4)$a_1|b_1, a_2|b_2 \Rightarrow a_1 a_2 | b_1 b_2$
Проблема возникает из-за делителей нуля: именно, если $b|a$, причем $b$ – не делитель нуля (и $b \neq 0$) то “частное”, то есть $c \in R$ такое, что $a = bc$, определено однозначно (почему?).
Что такое “делители единицы”? $b|1 \Leftrightarrow \exists c \in R : bc = 1$. То есть делители единицы – это (по определению) обратимые элементы кольца.
*Упражнение* Если $b \in R$ обратим, то обратный элемент определен однозначно (обозначение $c = b^{-1}$).
*Упражнение.* Пусть $b \in R$. Тогда $b$ – обратим $\Leftrightarrow\ \forall a \in R :\ b|a$.
*Обозначение.* $R^* :=$ множество всех обратимых элементов в $R$.
*Упражнение.*
1) $a, b' in R^* \Rightarrow ab \in R^*$;
2)$1 \in R^*$;
3)$a \in R^* \Rightarrow a^{-1} \in R^*$.

(то есть $R^*$ – группа относительно умножения)
*Примеры.*1) $F$ – поле $\Rightarrow\ F^* = R \setminus \{0\}$;
2) $\mathbb{Z}^* = \{1, -1\}$;
3) Если $R$ – целостное кольцо, то $R[x]^* = R^*$. Проверка: очевидно, что $R^* \subset R[x]^*$. Обратно, пусть $f, g \in R[x],\ fg = 1$. Тогда степени $f, g$ не могут быть положителны.
Если $R$ – не целостно, то может быть $R^* \subsetneqq R[x]^*$: например при $R = \mathbb{Z}(4)$ : $(1 + 2x)^2 = 1$.
*Определение.* $a \sim b$ ($a$ ассоциировано с $b$) если $\exists u \in R^* :\ a = ub$.
Например: $R = \mathbb{Z}\ a \sim b \Leftrightarrow a = \pm b$
$R = F[x]\ f \sim g \Leftrightarrow f = ug,\ u \in F, u \neq 0$.
*Упражнение.* $\sim$ – отношение эквивалентности.
Ассоциированые элементы имеюь "одинаковые" свойства делимости:
*Упражнение.* Если $a \sim a',\ b \sim b'$, то $b|a \Leftrightarrow b'|a'$.
*Предложение.* Пусть $R$ – целостное кольцо, $a, b \in R$. Тогда $a \sim b \Leftrightarrow a|b, b|a$.
*Упражнение.* Докажите предложение.
*Упражнение.* Пусть $R$ целостное, $a, b, c \in R, c \neq 0$. Если $ac|bc$, то $a|b$.

## 2.4. **Деление с остатком.**

Напоминание: $R = \mathbb{Z}, a, b \in \mathbb{Z}, b \neq 0$. Тогда $\exists!\ q, r \in \mathbb{Z}$ ("неполное частное" и остаток), $0 \leq r < |b|$, $a = bq + r$. Например, $5 = (-3)\cdot(-1)+2$, $-5 = (-3)\cdot(2)+1$. Ясно, что $b|a \Leftrightarrow r = 0$.
Имеется прямой аналог для кольца $R = F[x]$, где $F$ – поле.
*Пример.* $f = x^3 - 2x + 1$, $g = 2x^2 - 3x$. Т.е. $f = gq + r$, где $q = \frac{1}{2}x + \frac{3}{4}$ $r = \frac{1}{4}x + 1$; $1 = \deg r < \deg q = 2$.
*Предложение* (деление с остатком в $F[x]$). Пусть $F$ – поле, $f, g \in F[x]$, $g \neq 0$. Тогда $\exists!\ q, r \in F[x] : f = gq + r, \deg r < \deg g$.
*Терминология:* $q$ – (неполное) частное от деления $f$ на $g$; $r$ – остаток от деления $f$ на $g$.
*Замечание:* $g|f \Leftrightarrow r = 0$ (ввиду единственности).
*Доказательство.* $\exists$ : Применим индукцию по $\deg f$ ($g$ фиксируется).
1). Если $\deg f < \deg g$, то берем $q = 0, r = f$ (в частности, имеется база индукции ...)
2) Пусть $\deg f = n \geq \deg g$. Предположение индукции: требуемое представление существует для всех многочленов степени $< n$. Пусть $f = a_n x^n + \ldots$, $g = b_m x^m + \ldots$, где $a_n \neq 0, b_m \neq 0$, т.е. $\deg g = m \leq n$. Положим $\widetilde{f} = f - \frac{a_n}{b_m} x^{n-m} g$. Тогда старший член $\left(\frac{a_n}{b_m} x^{n-m} \cdot g\right) = \frac{a_n}{b_m} x^{n-m} \cdot b_m x^m = a_n x^n =$ старший член $f$, т.е. $\deg \widetilde{f} < n$. По предположению индукции, $\exists \widetilde{q}, r \in F[x]$ такие, что $\widetilde{f} = g\widetilde{q} + r, \deg r < \deg g$. Тогда $f = gq + r$, где $q = \frac{a_n}{b_m} x^{n-m} + \widetilde{q}$.

! Пусть $f = gq_1 + r_1 = gq_2 + r_2$, где $\deg r_i < \deg g, i = 1, 2$. Тогда $g(q_1 - q_2) = r_2 - r_1$, причем $\deg(r_2 - r_1) \leq \max(\deg r_1, \deg r_2) < \deg g$. Если $q_1 \neq q_2$, то $\deg g(q_1 - q_2) = \deg g + \underbrace{\deg(q_1 - q_2)}_{\geq 0} \geq \deg g \Rightarrow$ противоречие. Т.е. $g_1 = g_2, r_1 = r_2$. $\square$

Аксиоматически обобщим понятие деления с остатком. Пусть $R$– целостное кольцо.

*Определение.* $R$ – *евклидово* кольцо, если $\exists$ функция $\delta : R \setminus \{0\} \to \mathbb{Z}_+ := \{m \mid m \in \mathbb{Z}, m \geq 0\}$ (выстота элемента ) со свойствами:

(1) Если $a|b$, то $\delta(a) \leq \delta(b)$, причем если $\delta(a) = \delta(b)$, то $a \cong b$;

(2) Если $a, b \in R, b \neq 0$, то $\exists q, r \in R : a = bq + r$, где $r = 0$ или $\delta(r) < \delta(b)$.

Отметим, что единственность в (2), вообще говоря, *не требуется.*

*Лемма.* В евклидовом кольце $R$ если $a \mid b, a \ncong b$ (т.е. $b \nmid a$), то $\delta(a) < \delta(b)$.

*Доказательство.* Делим с остатком $a = bq + r$, $r \neq 0$ (т.е. $\delta(r) < \delta(b)) \Rightarrow a \mid r \Rightarrow \delta(a) \leq \delta(r) < \delta(b)$. $\square$

Заметим, что если функция $\delta$ удовлетворяет условию (2), то $\delta'(a) := \min\{\delta(b) \mid b \cong a\}$ удовлетворяет (1) и (2).

*Примеры евклидовых колец.*

1. $R = \mathbb{Z}, \delta(a) = |a|$ (NB $5 = 3 \cdot 1 + 2 = 3 \cdot 2 - 1$)
2. $R = F[x], \delta(f) = \deg f$.
3. $R = \mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}\}$ – *целые гауссовы числа*, $\delta(a) = |a|^2$.

*Задача.* Проверьте, что $\mathbb{Z}[i]$ – подкольцо в $\mathbb{C}$, и докажите, что оно евклидово.

## 2.5. **Наибольший общий делитель.**

Пусть $R$ – целостное кольцо, $a, b \in R$.

*Определение. Наибольший общий делитель* $a$ и $b$ – это элемент $d \in R$ такой, что 1) $d \mid a, d \mid b$; 2) если $\widetilde{d} \mid a, \widetilde{d} \mid b$, то $\widetilde{d} \mid d$.

Обозначение: $d = \text{НОД}(a, b)$. Оно не вполне корректное из-за не полной однозначности НОД.

*Замечание.* Общие делители $a$ и $b$ = делители НОД$(a, b)$ ( $\Rightarrow$ по определению, $\Leftarrow$ упражнение).

*Пример.* НОД$(a, 0) = a$: т.к. 0 делится на все элементы, то общие делители $a$ и $0$ = делители $a$. В частности, НОД$(0, 0) = 0$.

Предположим, что НОД$(a, b)$ существует. Как они все устроены?

*Лемма.* Пусть $d = \text{НОД}(a, b)$. Тогда $\widetilde{d} = \text{НОД}(a, b) \Leftrightarrow \widetilde{d} \cong d$.

*Доказательство.* Если $d = 0$ – доказать самостоятельно (тогда $a = b = 0$).

$\Rightarrow \widetilde{d} \mid d, d \mid \widetilde{d}$ (по определению НОД) $\Rightarrow \widetilde{d} \cong d$.

$\Leftarrow$ доказать самостоятельно. $\square$

Всегда ли существует НОД, и как его вычислить?

*Задача.* $R =$ многочлены без члена первой степени – подкольцо в $F[x]$; в этом

кольце *не существует* НОД$(x^5, x^6)$.
Отметим также, что "школьный" способ для $\mathbb{Z}$ – разложение на простые – не работает на практике для "больших" чисел.
Мы докажем, что в евклидовом кольце НОД всегда существует, и есть "алгоритм" его вычисления: алгоритм Евклида.
Итак, пусть $R$ – евклидово кольцо, $a, b \in R$, $a \neq 0$, $b \neq 0$. Пусть для определенности $\delta(a) \geq \delta(b)$. Последовательно делим с остатком:

$$(1)\ a = bq_1 + r_1$$
$$(2)\ b = r_1q_2 + r_2$$
$$(3)\ r_1 = r_2q_3 + r_3$$
$$\dots$$
$$(n-1)\ r_{n-3} = r_{n-2}q_{n-1} + r_{n-1}$$
$$(n)\ r_{n-2} = r_{n-1}q_n + r_n$$
$$(n+1)\ r_{n-1} = r_nq_{n+1}.$$

При этом $\delta(b) > \delta(r_1) > \delta(r_2) > \dots$. Так как значения $\delta$ – целые неотрицательные числа, то процесс окончится, т.е. $\exists n : r_{n+1} = 0$. Пусть $d := r_n$ (последний остаток, который не равен нулю).
**Теорема** (алгоритм Евклида вычисления НОД).
1. $d =$ НОД$(a, b)$.
2. $\exists u, v \in R :\ d = ua + vb$ (*линейное представление* НОДа).
*Доказательство.*
а) Почему $d \mid a, d \mid b$ ? $(n+1) \Rightarrow d = r_n \mid r_{n-1}$. Далее, $d \mid r_n, d \mid r_{n-1} \overset{(n)}{\Rightarrow} d \mid r_{n-2}$ и так далее (по индукции).
б) Почему $d = ua + vb$ для подходящих $u, v$? Удобно доказать, что это так для любого $r_k$. Индукция по $k$. База: $r_1 = 1 \cdot a + (-q_1) \cdot b$; $r_2 = b - q_2 \cdot r_1 = a \cdot (-q_2) + (1 + q_1q_2) \cdot b$. Переход: если $r_{k-1} = u_{k-1}a + v_{k-1}b$, $r_{k-2} = u_{k-2}a + v_{k-2}b$, то, так как $r_{k-2} = r_{k-1} \cdot q_k + r_k$, то

$$r_k = (\underbrace{u_{k-2} - q_k \cdot u_{k-1}}_{=:u_k})a + (\underbrace{v_{k-2} - q_k \cdot v_{k-1}}_{=:v_k})b.$$

в) Пусть $\widetilde{d} \mid a, \widetilde{d} \mid b$ . Почему $\widetilde{d} \mid d$? Это так ввиду $d = u \cdot a + v \cdot b$. $\square$
*Замечание.* В тривиальном случае $a = 0$ или $b = 0$ все равно имеет место линейное представление НОД (упражнение: убедиться).
*Определение.* $a, b \in R$ взаимно просты, если НОД$(a, b) = 1$ (то есть общие делители $a$ и $b$ – это только "тривиальные"делители из $R^*$).
*Предложение.* $a, b \in R$ взаимно просты $\Leftrightarrow \exists u, v \in R : ua + vb = 1$.
*Доказательство.* $\Rightarrow$: следует из линейного представления НОД.

$\Leftarrow$: если $d|a,\ d|b$, то $d|1 = ua + vb$, т.е. НОД$(a, b)$=1.
*Упражнение.* Пусть НОД$(a, b) = d \neq 0,\ a = \tilde{a}d,\ b = \tilde{b}d$. Тогда $\tilde{a}$ и $\tilde{b}$ – взаимно просты.
*Предложение.* Пусть $a, b, c \in R,\ a|bc$ НОД$(a, b) = 1$. Тогда $a|c$.
*Доказательство.* $1 = ua + vb \Rightarrow c = cu \cdot a + v \cdot bc$ кратно $a$.

2.6. **Простые элементы кольца. Разложение на простые множители.**
Пусть $R$ – целостное кольцо, $p \in R,\ p \neq 0, p \notin R^*$.
*Определение.* $p$ – простой, если: $a|p \Leftrightarrow a \sim 1$ или $a \sim p$ (то есть, по существу, делители $p$ это лишь 1 и $p$).
*Замечание.* Пусть $p \sim q$. Тогда $p$ – прост $\Leftrightarrow q$ – прост.
*Примеры.* 1) $R = \mathbb{Z}$: простые элеметы – это $\pm p$, $p \in \mathbb{N}$ – простое число.
2) $R = F[x]$. Простые элементы – неприводимые (над $F$) *многочлены.* Например, если $deg\ f = 1$, то $f$ – неприводим (почему?)
*Предложение (свойства простых элементов).* Пусть $R$ – евклидово, $p \in R$, $p$ – простой. Тогда: 1) $p \nmid a \Rightarrow$ НОД$(a, p) = 1$.
2) $p|ab \Rightarrow p|a$ или $p|b$.
*Доказательство.*1) $d :=$НОД$(a, p) \Rightarrow d|p \Rightarrow d \sim 1$ или $d \sim p$. Если $d \sim p$, $p|a$ противоречие.
2) Пусть $p \nmid a$. Тогда НОД$(p, a) = 1 \Rightarrow p|b$.
*Упражнение.* В обозначениях предложения $p|a_1...a_n \Rightarrow \exists i : p|a_i$.
Применение к кольцам вычетов:
*Предложение.* Пусть $p$ – простое число. Тогда $\mathbb{Z}(p)$ – поле.(часто это поле обозначают $\mathbb{F}_p$ – поле из $p$ элементов)
*Доказательство* Пусть $a \in \mathbb{Z};\ [a] \neq 0 \Leftrightarrow p \nmid a$. Тогда НОД$(a, p) = 1 \Rightarrow \exists u, v :$ $1 = au + pv \Rightarrow [1] = [a][u]$, то есть $[a]$ обратим.
*Упражнение.* Пусть $n \in \mathbb{N},\ a \in \mathbb{Z}$. Тогда $[a] \in \mathbb{Z}(n)^* \Leftrightarrow$ НОД$(a, n) = 1$.
**Теорема (разложение на простые в евклидовом кольце).**
Пусть $R$ – евклидово кольцо, $a \in R,\ a \neq 0,\ a \notin R^*$. Тогда
1) $a$ разлагается в $R$ на простые множители (то есть $\exists p_1, .., p_n \in R$ – простые: $a = p_1 \cdot ...\cdot_n$).
2)Такое разложение единственно с точностью до порядка множителей и замены их на ассоциированые (то есть, если $a = p_1...p_n = q_1...q_m$, то $n = m$, и существует перестановка $i_1, ..., i_n$ чисел $1, ..., n$ такая, что $p_j \sim q_{i_j}$).
*Доказательство.*
1) От противного: пусть существуют элементы, не представимые ... Пусть $a$ такой элемент, с наименьшим $\delta(a)$. $a$ – не прост $\Rightarrow a = bc,\ b, c \notin R^*$. Тогда $b$ и $c$ – разложимы. противоречие. (NB использовона только часть (1) из определения евклидовости.)

2) Пусть $p_1...p_n = q_1...q_m$, где $n \leq m$. $p_1|q_1...q_m \Rightarrow \exists i_1 : p_1|q_{i_1}$. Переобозначение: $p_1|q_1$, то есть $p_1 \sim q_1$. Можно считать ("отдавая" множители из $R^*$ другим элементам) что $p_1 = q_1$. То есть (целостность) $p_2...p_n = q_2...q_m$ и так далее. В конце получим: если $n < m$, то $1 = q_{m-n}...q_n$, противоречит простоте $q_n$. (NB: здесь использована часть (2) определения евклидовости). $\square$

*Терминология.* Целостное кольцо удовлетворяющее условиям теоремы называется факториальным. То есть доказано, что евклидовы кольца (в частности $\mathbb{Z}, F[x]$) факториальны.

*Задача (пример нефакториальных – и тем более неевклидовых – колец).*

1) $R$ =кольцо многочленов без членов степени 1. Разложение на простые существует, но не единственно. $x^2, x^3$ – простые в $R$, $x^6 = x^3x^3 = x^2x^2x^2$. $R = \mathbb{Z}[\sqrt{-5}]$– аналогично $(6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5}))$

2) $R = \{\sum c_r x^r |\ r \in \mathbb{Q}, c_r \in F - -$поле, в сумме конечное число слагаемых$\}$. Здесь разложение на простые не существует. Аналогично в кольце целых алгебраических чисел.

*Упражнение.* Пусть $R$ – факториальное кольцо.

1) Пусть $a \in R, a = p_1^{k_1}...p_r^{k_r}$, где $p_i$ – простые, $p_i \nsim p_j$ при $i \neq j$, $k_i \in \mathbb{Z}_+$. Тогда $b|a \Leftrightarrow b \sim p_1^{l_1}...p_r^{l_r}$, где $l_i \in \mathbb{Z}_+,\ l_i \leq k_i$.

2) Пусть $a, b \in R,\ a = p_1^{k_1}...p_r^{k_r},\ b = p_1^{l_1}...p_r^{l_1}$, где $p_i$ такие же как в предыдущем пункте. Тогда НОД$(a, b) = p_1^{m_1}...p_r^{m_r}$, где $m_i = min(k_i, l_i)$ (в частности, НОД существует). Обобщите, на НОД$(a_1, ..., a_n)$.

*Определение.* Наименьшее общее кратное элементов $a, b$ целостного кольца $R$ – это элемент $c$ такой, что $a|c,\ b|c$, и если $a|\tilde{c}, b|\tilde{c}$, то $c|\tilde{c}$. Обозначение: НОК$(a, b)$.

*Упражнение.* Пусть $c =$НОК$(a, b)$. Тогда $\tilde{c} =$НОК$(a, b) \Leftrightarrow \tilde{c} \sim c$.

*Упражнение.* НОК$(a, 0) = 0$.

*Упражнение.* Пусть $R$ – факториальное кольцо, $a, b \in R, a, b \neq 0$. Тогда существует НОК$(a, b)$, причем НОК$(a, b) = \frac{ab}{\text{НОД}(a,b)}$. (NB: $R$ – целостно, значит с частным нет проблем).

В частности, если НОД$(a, b) = 1$, то НОК$(a, b) = ab$. Отсюда: если НОД$(a, b) = 1,\ a|c, b|c$, то $ab|c$.

*Упражнение.* Если в факториальном кольце $a = p_1^{k_1}...p_r^{k_r},\ b = p_1^{l_1}...p_r^{l_1}$ (обозначения из упражнения выше), то НОК$(a, b) = p_1^{n_1}...p_r^{n_r}$, где $m_i = max(k_i, l_i)$.

*Задача.* Сформулируйте определение НОК$(a_1, ..., a_n)$ и придумайте его свойства.

## 2.7. **Корни многочленов.**

Пусть $R$ - кольцо, $c \in R$. Если $f \in R[x]$, $f(x) = a_n x^n + \ldots + a_1 x + a_0$, то определим $f(c) := a_n c^n + \ldots + a_1 c + a_0 \in R$ – *значение* $f$ *при* $x = c$.

*Предложение.* $(f + g)(c) = f(c) + g(c)$; $(fg)(c) = f(c)g(c)$.

*Замечание.* В предложении важна *коммутативность* кольца!

*Замечание.* Это бывает полезно чуть обобщить: пусть $S$ – кольцо, $R \subset S$ – подкольцо, $f \in R[x], c \in S$. Тогда точно так же определяется $f(c) \in S$, и выполнено предложение.

*Пример.* $S = R[x], c = g \in R[x]$. Тогда $f(c) =: f \circ g \in R[x]$ (подстановка многочлена в многочлен). Например ($R = \mathbb{Z}$) $f = x^2 - x + 1, g = x + 1$ $\Rightarrow f \circ g = f(x+1) = (x+1)^2 - (x+1) + 1 = x^2 + x + 1$.

Далее будем рассматривать случай, когда $R = F$ – *поле.*

*Определение.* $c \in F$ – *корень* многочлена $f \in F[x]$, если $f(c) = 0$.

*Предложение.* Остаток от деления $f$ на $x - c$ равен $f(c)$.

*Доказательство.* $f = (x-c) \cdot q + r$, где $\deg r < \deg(x-c) = 1$, то есть $r \in F$ – "константа". Подставляем $x = c$, получаем $f(c) = r$. $\square$

*Следствие (теорема Безу).* $f(c) = 0 \Leftrightarrow (x-c) \mid f$. $\square$

*Упражнение.* Если $f \mid g, f(c) = 0$, то $g(c) = 0$.

*Следствие.* Пусть $f \in F[x], f \neq 0$. Тогда число корней $f$ не превосходит $\deg f$.

*Доказательство.* Индукция по $\deg f$. База: $\deg f = 0 \Rightarrow f$ – ненулевая константа $\Rightarrow f$ не имеет корней. Переход: пусть доказано для $\deg f \leq n$. Докажем для $\deg f = n + 1$. Если $f$ не имеет корней, то тривиально. Если $\exists c \in F : f(c) = 0$, то $f = (x-c)g$, где $\deg g = n$. $\{\text{Корни } f\} = \{\text{Корни } g\} \cup \{c\} \Rightarrow$ число корней $f$ $\leq$ (число корней $g$) $+ 1 \underset{\text{инд. пр-е}}{\leq} n + 1$. $\square$

*Предложение.* Пусть $|F| = \infty, \quad f, g \in F[x], \forall c \in F : f(c) = g(c)$. Тогда $f = g$.

*Доказательство.* Если $f \neq g$, то множество корней $f - g$ конечно $\Rightarrow \exists c \in F$ : $(f-g)(c) \neq 0$, то есть $f(c) \neq g(c)$. $\square$

*Замечание.* Для $|F| < \infty$ (например, $F = \mathbb{F}_p$) это неверно (???). Вообще, рассмотрим $f = \prod_{a \in F}(x - a)$. Тогда $f(c) = 0, \forall c \in F$, но $f \neq 0$.

Итак, над бесконечным полем можно не различать многочлены и представляемые ими функции; над конечным полем их необходимо различать.

*Замечание.* Пусть $R =$ кольцо всех функций $X \to \mathbb{F}_2$, где $|X| = \infty$. Тогда $|R| = \infty$, но $\forall a \in R : a = a^2$ (значения $a$ – это 0 или $1 \in \mathbb{F}_2 \ldots$). То есть многочлены $x^2, x \in R[x]$ задают равные функции (т.е. бесконечное поле нельзя заменить на бесконечное *кольцо*).

*Задача интерполяции.* Пусть $F$ – поле, $a_1, \ldots a_n \in F$, $a_i \neq a_j$ при $i \neq j$; $b_1, \ldots b_n \in F$. Задача: найти $f \in F[x], \deg f \leq n-1$ такой, что $f(a_i) = b_i, \ \forall i = 1, \ldots, n$.

Геометрическая интерпретация при $F = \mathbb{R}, n = 1, 2, 3$

**Теорема.** Решение задачи интерполяции существует и единственно.

*Доказательство.* Единственность: пусть $f, g \in F[x]$ – решения. Тогда $(f - g)(a_i) = 0 \quad \forall i = 1, \ldots, n$; $\deg(f-g) \leq \max(\deg f, \deg g) \leq n - 1 \Rightarrow f - g = 0$.

Существование: 1) Частный случай: $b_k = 1$ для некоторого $k$, $b_i = 0, \ \forall i \neq k$. То есть ищем $f_k \in F[x], \deg f_k \leq n - 1$,

$$f_k(a_i) = \begin{cases} 1, & i = k \\ 0, & i \neq k. \end{cases}$$

Вот ответ: $f_k = \alpha(x-a_1)\cdot\ldots\cdot(x-a_{k-1})(x-a_{k+1})\cdot\ldots\cdot(x-a_n)$ (NB: $\deg f_k = n-1$).

$$f_k(a_k) = 1 \Rightarrow \alpha = [(a_k - a_1)\cdot\ldots\cdot(a_k - a_{k-1})(a_k - a_{k+1})\cdot\ldots\cdot(a_k - a_n)]^{-1}.$$

2)Общий случай: $f = \sum_{k=1}^n b_k f_k$. Тогда $\deg f \leq n-1$, $f(a_i) = \sum_{k=1}^n b_k f_k(a_i) = b_i \quad \forall i$. $\square$

*Замечание.* Получена явная *формула Лагранжа* для решения задачи интерполяции

$$f = \sum_{k=1}^n b_k \frac{(x-a_1)\cdot\ldots\cdot(x-a_{k-1})(x-a_{k+1})\cdot\ldots\cdot(x-a_n)}{(a_k-a_1)\cdot\ldots\cdot(a_k-a_{k-1})(a_k-a_{k+1})\cdot\ldots\cdot(a_k-a_n)}.$$

*Следствие.* Пусть $f \in F[x],\ deg\ f \leq n-1,\ a_1, ..., a_n \in F, a_i \neq a_j$ при $i \neq j$.

$$\text{Тогда } f = \sum_{k=1}^n f(a_k) \frac{(x-a_1)\cdot\ldots\cdot(x-a_{k-1})(x-a_{k+1})\cdot\ldots\cdot(x-a_n)}{(a_k-a_1)\cdot\ldots\cdot(a_k-a_{k-1})(a_k-a_{k+1})\cdot\ldots\cdot(a_k-a_n)}.$$

*Замечание.* На практике часто удобнее так называемый метод Ньютона. Именно, ищем решение в виде $f = \lambda_1 + \lambda_2(x-a_1) + ... + \lambda_n(x-a_1)...(x-a_{n-1})$, и находим $\lambda_i$ из реккурентных соотношений $b_1 = \lambda_1,\ b_2 = \lambda_1 + \lambda_2(a_2 - a_1),\ ...,\ b_n = \lambda_1 + ... + \lambda_n(a_n - a_1)...(a_n - a_{n-1})$.

*Связь между корнями и НОД.* Пусть $f, g \in F[x]$

*Предложение.* Общие корни $f, g$ =корни НОД$(f, g)$.

*Доказательство.* Пусть $d :=$НОД$(f, g)$, тогда $f(c) = 0, g(c) = 0 \Leftrightarrow (x-c)|d \Leftrightarrow d(c) = 0 \square$.

*Следствие.* Если $f, g$ взаимно просты, то $f, g$ не имеюи общих корней.

*Замечание.* Это тривиально обобщается на любое конечное число многочленов.

## 2.8. **Кратность корня многочлена.**

Пусть $f \in F[x],\ f \neq 0,\ c \in F$.

*Определение.* Кратность корня $c$ многочлена $f$ – это наибольшее $k \in \mathbb{Z}_+$ такое, что $(x-c)^k | f$

Обозначение (необщепринятое): $k = \mathrm{Kp}_c f$.

Итак, по определению $k = \mathrm{Kp}_c f \Leftrightarrow (x-c)^k | f,\ (x-c)^{k+1} | f$.

*Замечание.* $\mathrm{Kp}_c f = 0 \Leftrightarrow (x-c) \nmid f \Leftrightarrow f(c) \neq 0$ (то есть $c$ не корень $f$).

*Терминология.* Корень $c$ многочлена $f$ – простой, если $\mathrm{Kp}_c f = 1$, кратный, если $\mathrm{Kp}_c f > 1$.

*Лемма (другое определение кратности).* Пусть $f \in F[x],\ f \neq 0,\ c \in F,\ k \in \mathbb{Z}_+$.

Тогда $k = \mathrm{Kp}_c f \Leftrightarrow f = (x-c)^k g$, где $g \in F[x],\ g(c) \neq 0$.
*Доказательство.* $\Rightarrow$: $k = \mathrm{Kp}_c f \Rightarrow f = (x-c)^k g$. Если $g(c) = 0$, то $(x-c)|g \Rightarrow (x-c)^{k+1}|f \Rightarrow$ противоречие.
$\Leftarrow$: $f = (x-c)^k g \Rightarrow (x-c)^k|f$. Если $(x-c)^{k+1}|f$, то $f = (x-c)^{k+1}h \Rightarrow g = (x-c)h \Rightarrow g(c) = 0$ противоречие $\square$.
*Предложение (свойства кратности)* Пусть $f, g \in F[x],\ f, g \neq 0\ c \in F$. Тогда
1)$\mathrm{Kp}_c fg = \mathrm{Kp}_c f + \mathrm{Kp}_c g$;
2) $\mathrm{Kp}_c(f+g) \geq min(\mathrm{Kp}_c f, \mathrm{Kp}_c g)$; если $\mathrm{Kp}_c f \neq \mathrm{Kp}_c g$, то "=";
3)$\mathrm{Kp}_c(\mathrm{НОД}(f,g)) = min(\mathrm{Kp}_c f, \mathrm{Kp}_c g)$
*Доказательство.* Пусть $m = \mathrm{Kp}_c f,\ n = \mathrm{Kp}_c g$, то есть $f = (x-c)^m \widetilde{f},\ g = (x-c)^n \widetilde{g},\ \widetilde{f}(c) \neq 0, \widetilde{g}(c) \neq 0$. 1) $fg = (x-c)^{m+n} \widetilde{f}\widetilde{g},\ \widetilde{f}\widetilde{g}(c) = \widetilde{f}(c)\widetilde{g}(c) \neq 0 \Rightarrow \mathrm{Kp}_c(fg) = \mathrm{Kp}_c(f) + \mathrm{Kp}_c(g)$.
2) Доказать самостоятельно.
3) $d = $ НОД $(f, g)$. Пусть $m \geq n$, тогда $(x-c)^n|f, (x-c)^n|g \Rightarrow (x-c)^n|d$. Если $(x-c)^{n+1}|d$, то $(x-c)^{n+1}|g$, получаем противоречие. $\square$
*Замечание.* Аналогично можно определить кратность вхождения простого элемента $p$ в элемент факториального кольца $R$: у нас $R = F[x]$, $p = x - c$. При этом выполняются свойства, аналогичные тем, что в предложении. (Задача: сделать это).
**Теорема.** Пусть $f \in F[x], f \neq 0$. Тогда $f = (x-c_1)^{k_1} \cdot \ldots \cdot (x-c_m)^{k_m} g$, где $c_i \in F$, $c_i \neq c_j$ при $i \neq j$, $k_i \in \mathbb{N}$, $g \in F[x]$, $g$ не имеет корней в $F$. При этом $c_1, \ldots, c_m$ – это в точности корни $f$ в поле $F$ (не исключается $m = 0$), $k_i = \mathrm{Kp}_{c_i} f$. Это представление единственно с точностью до нумерации $c_1, \ldots, c_m$.
*Доказательство.* Разложим $f$ на неприводимые множители. Множители степени 1 ассоциированы с $x - c$, где $c \in F$. Пусть $g$ – произведение остальных множителей (постоянные множители "отдадим" $g$). Получаем: $f = (x-c_1)^{k_1} \cdot \ldots \cdot (x-c_m)^{k_m} g$; $g$ не имеет корней (ибо если $g(c) = 0$, то $(x-c)|g$, что противоречит единственности разложения на неприводимые). Все остальное очевидно. (Упражнение: продумать). $\square$
*Следствие.* В условиях предыдущей теоремы $k_1 + \ldots + k_m$ (= число корней $f$ *с учетом кратности*) $\leq \deg f$.
*Замечание.* Если $f \in F[x], f \neq 0$, таково, что число корней $f$ с учетом кратности равно $\deg f$, то $f = \alpha(x-c_1)^{k_1} \cdot \ldots \cdot (x-c_m)^{k_m}$, где $\alpha \in F^*$. В самом деле, из теоремы: $\deg f = \sum_i k_i + \deg g \Rightarrow \deg g = 0 \Rightarrow g = \alpha \neq 0$ – константа. При этом $\alpha$ – это старший коэффициент $f$.
**Формулы Виета.** Пусть $f \in F[x], f \neq 0$, пусть число корней $f$ с учетом кратности равно $\deg f =: n$, то есть $f = a_n x^n + a_{n-1}x^{n-1} + \ldots + a_1 x + a_0$, $a_n \neq 0$. Пусть $x_1, \ldots, x_n \in F$ – все корни $f$ с учетом их кратности (то есть каждый написан столько раз, какова его кратность).

**Теорема** (формулы Виета).

$$\sum_{1\le i_1<\ldots<i_k\le n} x_{i_1}x_{i_2}\cdot\ldots\cdot x_{i_k} = (-1)^k\ \frac{a_{n-k}}{a_n}, k = 1, 2, \ldots, n.$$

*Примеры.* $n = 2 : f = a_2x^2 + a_1x + a_0;\quad x_1 + x_2 = -\frac{a_1}{a_2},\ x_1x_2 = \frac{a_0}{a_2}$
$n = 3 : f = a_3x^3 + a_2x^2 + a_1x + a_0;\quad x_1 + x_2 + x_3 = -\frac{a_2}{a_3},\ x_1x_2 + x_1x_3 + x_2x_3 = \frac{a_1}{a_3},$
$x_1x_2x_3 = -\frac{a_0}{a_3}$.
*Доказательство.* Имеем $f = a_n(x-x_1)...(x-x_n)$. Раскоем скобки, и посмотрим на слагаемые степени $n-k$. То есть нужно в $n-k$ скобках взять $x$, в оставшихся $k$ взять $x_i$. При перемножении получится $a_n(-x_{i_1})...(-x_{i_k})$. Итак

$$\sum_{1\le i_1<\ldots<i_k\le n} x_{i_1}x_{i_2}\cdot\ldots\cdot x_{i_k} = (-1)^k\frac{a_{n-k}}{a_n}$$

2.9. **Многочлены над полем $\mathbb{C}$.**
*"Основная теорема алгебры"(комплексных чисел).*
Пусть $f \in \mathbb{C}[x], deg\ f > 0$. Тогда существует $c \in \mathbb{C} :\ f(c) = 0$.
Доказательство см. в Курош пар.41,42 (4е издание 1955) или Кострикин гл. 6 пар. 3 (существует очень короткое доказательство из комплексного анализа – будет на 3 курсе)
*Замечание.* Если поле $F$ таково, что $\forall f \in F[x], deg\ f > 0,\ \exists c \in F :\ f(c) = 0$, то $F$ называется алгебраически замкнутым. Итак, $\mathbb{C}$ – алгебраически замкнуто, $\mathbb{R}, \mathbb{Q}$ – нет; $\mathbb{F}_p$ тоже не алгебраически замкнуто (почему?).
Можно доказать, что любое поле содержится в алгебраически замкнутом (причем это последнее можно выбрать минимальным, и тогда оно единственно с точностью до изоморфизма).
*Следствие.* Пусть $f \in \mathbb{C}[x]$. Тогда $f$ неприводим над $\mathbb{C} \Leftrightarrow deg\ f = 1$.
*Следствие.* Пусть $f \in \mathbb{C}[x],\ f \neq 0$. Тогда $f$ разлагается на множители степени 1 (точнее $f = \alpha(x - c_1)_1^k...(x - c_r)_r^k$, где $c_i$ – корни $f$, $c_i \neq c_j$ при $i \neq j$, $k_i$ – кратности корней, $\alpha$ – старший коэффициент $f$).
*Замечание.* Оба следствия верны для любых алгебраически замкнутых полей.

2.10. **Многочлены над полем $\mathbb{R}$.**
*Пример.* Квадратный трехчлен с отрицательным дискриминантом неприводим над $\mathbb{R}$.
Напомним: так как $\mathbb{R} \subset \mathbb{C}$, то $\mathbb{R}[x] \subset \mathbb{C}[x]$. Пусть $f \in \mathbb{C}[x]$, $f = a_nx^n + ... + a_0$. Положим $\bar{f} := \bar{a_n}x^n + ... + \bar{a_0}$.
*Упражнение.* $f, g \in \mathbb{C}[x]$:
1) $\overline{f \pm g} = \bar{f} \pm \bar{g}$, $\overline{fg} = \bar{f} \cdot \bar{g}$
2) $f \in \mathbb{R}[x] \Leftrightarrow f = \bar{f}$
3) Пусть $c \in \mathbb{C}$. Тогда $\overline{f(c)} = \bar{f}(\bar{c})$

*Предложение.* Пусть $f \in \mathbb{R}[x], f \neq 0$. Тогда, если $c$ – корень $f$, то $\bar{c}$ – тоже корень, причем кратности $c$ и $\bar{c}$ совпадают.
*Доказательство.* $f = (x-c)^k g,\ g(c) \neq 0$. Тогда $f = \bar{f} = (x-\bar{c})^k \bar{g},\ \bar{g}(\bar{c}) = \overline{g(c)} \neq 0$ □.
**Теорема.** Пусть $d \in \mathbb{R}[x], f \neq 0$. Тогда $f$ разлагается в произвдение множителей первой и второй степени с вещественными коэффициентами, причем множители второй степени имеют отрицательный дискриминант. Такое представление единственно.
*Доказательство.* Разложим $f$ на множители степени 1 над $c$, с учетом предыдущего предложения получим $f = \alpha(x-a_1)^{k_1}...(x-a_r)^{k_r}(x-c_1)^{l_1}(x-\bar{c_1})^{l_1}...(x-c_j)^{l_j}(x-\bar{c_j})^{l_j}$, гда $a_i$ – вещественный корни, $c_i$ – невещественные. Осталось сгруппировать сопряженный корни в вещественные квадратные трехчлены $g_j = (x-c_j)(x-\bar{c_j})$. Единственность следует из единственности разложения для комплексных многочленов.
*Следствие.* Пусть $f \in \mathbb{R}[x]$. Тогда $f$ неприводим $\Leftrightarrow$ либо $f$ первой степени, либо второй с отрицательным дискриминантом.

2.11. **Характеристика кольца.** Мотивировка: производная многочлена $(x^n)' = nx^{n-1}$. Если $x^n \in R[x]$, где $R$ – кольцо, то в каком смысле $n \in R$?

Напомним, $R$ – кольцо $c$ 1. Имеем отображение $\mathbb{N} \to R,\ n \to \underbrace{1+\ldots+1}_{n} \in R$. (NB: оно естественно продолжается до $\mathbb{Z} \to R,\ -n \to -(\underbrace{1+\ldots+1}_{n}) \in R$, $0 \to 0$).

*Определение.* Если в кольце $R$ для $\forall n \in \mathbb{N} : \underbrace{1+\ldots+1}_{n} \neq 0$, то $R$ – кольцо *характеристики* 0. В противном случае *характеристика* кольца $R$ – это $\min\{n \in \mathbb{N} \mid \underbrace{1+\ldots+1}_{n} = 0\}$. Обозначение: $char\ R$.

*Замечание.* $char\ R = 0 \Rightarrow R$ бесконечно (почему?)

*Примеры.* $char\ \mathbb{Z} = char\ \mathbb{Q} = char\ \mathbb{R} = char\ \mathbb{C} = 0$; $char\ \mathbb{Z}(n) = n$ (в частности, $char\ \mathbb{F}_p = p$).

**Теорема.** Пусть $R$ – целостное кольцо; $char\ R \neq 0$. Тогда $char\ R$ – простое число.

*Доказательство.* Пусть $n = n_1 n_2, n_i \in \mathbb{N}$. Тогда $(\underbrace{1+\ldots+1}_{n_1})(\underbrace{1+\ldots+1}_{n_2}) = (\underbrace{1+\ldots+1}_{n})$. Если $(\underbrace{1+\ldots+1}_{n}) = 0$, то (целостность!) или $(\underbrace{1+\ldots+1}_{n_1}) = 0$, или $(\underbrace{1+\ldots+1}_{n_2}) = 0$. Минимальность $n \Rightarrow$ или $n_1 = n$, или $n_2 = n$. Кроме того,

$1 \neq 0$ (часть определения целостности), то есть $n \neq 1$. Итого $n$ – простое число. $\square$

В частности, характеристика поля – это 0 или $p$ - простое.

*Задача.* $F$ – поле, $char\ F = 0 \Rightarrow F \supset \mathbb{Q}$; $char\ F = p \Rightarrow F \supset \mathbb{F}_p$.

Для колец: $R$ – кольцо, $char\ R = 0 \Rightarrow R \supset \mathbb{Z}$; $char\ R = n \Rightarrow R \supset \mathbb{Z}(n)$.

*Задача.* $char\ R = p$-простое $\Rightarrow \forall a, b \in R : (a+b)^p = a^p + b^p$.

2.12. **Производная и кратные корни.** Пусть $f = a_n x^n + \ldots + a_2 x^2 + a_1 x + a_0 \in F[x]$ (где $F$ – поле).

*Определение.* Производная $f$ – это $f' := na_n x^{n-1} + \ldots + 2a_2 x + a_1 \in F[x]$ (здесь $n = \underbrace{1 + \ldots + 1}_{n} \in F$.)

*Замечание.* $\deg f' \leq \deg f - 1$. Если $char\ F = 0$ (и $\deg f > 0$), то $\deg f' = \deg f - 1$. Если $char\ F = p$, то это не всегда так. Например, над $\mathbb{F}_2$: $(x^2)' = 0$.

*Предложение* (свойства производной).

(1) $(f \pm g)' = f' \pm g'$.

(2) $(fg)' = f'g + fg'$.

(3) $(f^n)' = nf^{n-1}f'$.

*Доказательство.* (1) – упражнение.

(2) *Частный случай*: $f, g$ – одночлены, то есть $f = ax^m, g = bx^n$, $a, b \in F$. Тогда $fg = abx^{m+n}$, $(fg)' = (m+n)abx^{m+n-1}$; $f' = max^{m-1}$; $f'g = mabx^{m+n-1}$; $g' = nbx^{n-1}$; $fg' = nabx^{m+n-1}$; откуда все следует.

*Общий случай*: $f = \sum_i f_i$, $g = \sum_j g_j$, где – $f_i, g_j$ одночлены; $fg = \sum_{i,j} f_i g_j$. Уже доказано, что $(f_i g_j)' = f_i' g_j + f_i g_j'$, $\forall i, j$. Тогда $(fg)' = \sum_{i,j} (f_i g_j)' = \sum_{i,j} f_i' g_j + \sum_{i,j} f_i g_j' = f'g + fg'$.

(3) Индукция по $n$. $\square$

*Упражнение.* $h = f \circ g \Rightarrow h' = (f' \circ g) \cdot g'$.

**Теорема.** Пусть $f \in F[x], f \neq 0$. Тогда кратные корни $f$ = общие корни $f$ и $f'$ (= корни НОД $(f, f')$).

*Доказательство.* Напоминание: $c$ – кратный корень $f \Leftrightarrow (x-c)^2 \mid f$.

1) Пусть $c$ – кратный корень $f$, то есть $f = (x-c)^2 h$. Тогда $f' = 2(x-c)h + (x-c)^2 h' \Rightarrow f'(c) = 0$.

2) Пусть $f(c) = f'(c) = 0$. Так как $f(c) = 0$, то $f = (x-c)g$. Тогда $f' = g + (x-c)g'$, то есть $f'(c) = 0 \Leftrightarrow g(c) = 0$. То есть $x - c \mid g \Rightarrow g = (x-c)h \Rightarrow f = (x-c)^2 h$ $\Rightarrow c$ – кратный корень $f$. $\square$

**Теорема.** Пусть $\mathrm{char}\ F = 0, f \in F[x]$, $f \neq 0, c \in F, f(c) = 0$. Тогда $\mathrm{Kp}_c f' = \mathrm{Kp}_c f - 1$.

*Доказательство.* $n := \mathrm{Kp}_c f \geq 1 \Rightarrow f = (x-c)^n g, g(c) \neq 0$. Тогда $f' = n(x-c)^{n-1}g + (x-c)^n g' = (x-c)^{n-1}h$, где $h = ng + (x-c)g'$; $h(c) = ng(c) \neq 0(\mathrm{char}\ F = 0)$. То есть $\mathrm{Kp}_c f' = \mathrm{Kp}_c f - 1$. $\square$

Определим индуктивно "высшие производные": $f^{(0)} = f, f^{(1)} = f'; f^{(n)} = \left(f^{(n-1)}\right)'$. Обычно пишут $f''$ вместо $f^{(2)}$ и тому подобное.

*Упражнение.* $\left(f^{(k)}\right)^{(l)} = f^{(k+l)}$.

*Следствие.* Пусть $\mathrm{char}\ F = 0, f \in F[x], f \neq 0, c \in f$. Тогда $\mathrm{Kp}_c f = n \Leftrightarrow f(c) = f'(c) = \ldots = f^{(n-1)}(c) = 0,\ f^{(n)}(c) \neq 0$ ( то есть $\mathrm{Kp}_c f = \min\{n \in \mathbb{Z}_+ \mid f^{(n)}(c) \neq 0\}$).

*Доказательство.* Индукция по $n$. База $n = 0 : \mathrm{Kp}_c f = 0 \Leftrightarrow f(c) \neq 0$ ($n = 1 : \mathrm{Kp}_c f = 1 \Leftrightarrow f(c) = 0, f'(c) \neq 0$). Переход $n \rightsquigarrow n+1$ ($n \geq 0, n+1 \geq 1$)

$\Rightarrow$: $\mathrm{Kp}_c f = n+1 \Rightarrow f(c) = 0$. Тогда (теорема) $\mathrm{Kp}_c f' = n \underset{\text{инд. пр.}}{\Rightarrow} f'(c) = f''(c) = \ldots = (f')^{(n-1)}(c) \left(= f^{(n)}(c)\right) = 0, (f')^{(n)}(c) \left(= f^{(n+1)}(c)\right) \neq 0$.

$\Leftarrow$: $f(c) = f'(c) = \ldots = f^{(n)}(c) = 0,\ f^{(n+1)}(c) \neq 0 \Rightarrow f'(c) = f''(c) = \ldots = \left(f'\right)^{(n-1)}(c) = 0, \left(f'\right)^{(n)}(c) \neq 0 \underset{\text{инд. пр.}}{\Rightarrow} \mathrm{Kp}_c f' = n \underset{\text{f(c)=0, теор.}}{\Rightarrow} \mathrm{Kp}_c f = n+1$. $\square$

*Предложение* ("отделение кратных корней"). Пусть $\mathrm{char}\ F = 0, f \in F[x], f \neq 0$. Положим $g := \frac{f}{\text{НОД}(f,f')}$. Тогда $g$ имеет в точности те же корни, что и $f$, но все они простые.

*Доказательство.*

1) Так как $g \mid f$, то $g(c) = 0 \Rightarrow f(c) = 0$.

2) Пусть $f(c) = 0$. Докажем, что $g(c) = 0$, причем $\mathrm{Kp}_c g = 1$. $d := \text{НОД}(f, f'), f = gd$. Тогда $\mathrm{Kp}_c f = \mathrm{Kp}_c g + \mathrm{Kp}_c d = \mathrm{Kp}_c g + \min(\mathrm{Kp}_c f, \mathrm{Kp}_c f') = \mathrm{Kp}_c g + \mathrm{Kp}_c f - 1 \Rightarrow \mathrm{Kp}_c g = 1$. $\square$

*Упражнение.* Пусть $\mathrm{char}\ F = 0, f \in F[x], \deg f = n, c \in F$. Тогда (*формула Тейлора*) $f = f(c) + \frac{f'(c)}{1!}(x-c) + \frac{f''(c)}{2!}(x-c)^2 + \ldots + \frac{f^{(n)}(c)}{n!}(x-c)^n$.

2.13. **Поле частных целостного кольца.** *Мотивировка* : построение $\mathbb{Q}$ по $\mathbb{Z}$: $a, b \in \mathbb{Z}, b \neq 0 \Rightarrow \frac{a}{b} \in \mathbb{Q}$. $\frac{a}{b} = \frac{c}{d} \Leftrightarrow ad = bc\ (\in \mathbb{Z})$. Операции: $\frac{a}{b} + \frac{c}{d} = \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$, $\mathbb{Z} \ni a = \frac{a}{1} \in \mathbb{Q}$ (то есть $\mathbb{Z} \subset \mathbb{Q}$).

Пусть $R$ – *целостное* кольцо. Рассмотрим $X = R \times (R \setminus \{0\}) = \{(a,b) \mid a, b \in R, b \neq 0\}$. Рассмотрим оттошение " $\sim$" на $X$ : $(a,b) \sim (c,d) \overset{\text{def}}{\Leftrightarrow} ad = bc$.

*Лемма.* $\sim$ – отношение эквивалентности на $X$.

*Доказательство.*

(1) $(a,b) \sim (a,b)$.

(2) Если $(a,b) \sim (c,d)$, то $(c,d) \sim (a,b)$ – тривиально.

(3) Пусть $(a,b) \sim (c,d), (c,d) \sim (e,f)$. Почему $(a,b) \sim (e,f)$? Дано: $ad = bc$ ($\Rightarrow adf = bcf$); $cf = de$ ($\Rightarrow bcf = bde$). Требуется доказать $af = be$. Имеем: $adf = bcf, bcf = bde \Rightarrow adf = bde \underset{R-\text{цел.},d\neq 0}{\Rightarrow} af = be$. $\square$

Пусть $F(R) :=$ множество классов эквивалентности на $X$. Обозначим $\frac{a}{b} :=$ класс$(a,b)$. Итак, по определению $\frac{a}{b} = \frac{c}{d} \Leftrightarrow (a,b) \sim (c,d) \Leftrightarrow ad = bc$. Операции в $F(R)$ : $\frac{a}{b} + \frac{c}{d} := \frac{ad+bc}{bd}$, $\frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$. (Заметим, что, так как $R$ – целостно, то $b \neq 0, d \neq 0 \Rightarrow bd \neq 0$).

*Замечание.* $\frac{ac}{bc} = \frac{a}{b}$ (при $b \neq 0, c \neq 0$).

*Корректность.* $\frac{a_1}{b_1} = \frac{a_2}{b_2}$, $\frac{c_1}{d_1} = \frac{c_2}{d_2} \overset{?}{\Rightarrow} \frac{a_1d_1+b_1c_1}{b_1d_1} = \frac{a_2d_2+b_2c_2}{b_2d_2}; \frac{a_1c_1}{b_1d_1} = \frac{a_2c_2}{b_2d_2}$.

Дано: $a_1b_2 = a_2b_1, c_1d_2 = c_2d_1$. Требуется доказать: $(a_1d_1 + b_1c_1)b_2d_2 = (a_2d_2 + b_2c_2)b_1d_1$, то есть $\underline{a_1d_1b_2d_2} + \underline{\underline{b_1c_1b_2d_2}} = \underline{a_2d_2b_1d_1} + \underline{\underline{b_2c_2b_1d_1}}$ – верно.

(*Упражнение*: доказать для умножения).

*Предложение.* $F(R)$ – поле.

*Доказательство.* Проверить: 1) ассоциативность сложения; 2) ноль: $\frac{0}{1}$; единица: $\frac{1}{1}$. Так как $0 \neq 1$, то $\frac{0}{1} \neq \frac{1}{1}$; 3) обращение: $\frac{a}{b} \in F(R), \frac{a}{b} \neq \frac{0}{1}$, то есть $a \neq 0$. Тогда $\frac{b}{a} \in F(R)$, и $\frac{a}{b} \cdot \frac{b}{a} = \frac{1}{1}$. Остальное – упражнение. $\square$

Пусть $S = \{\frac{a}{1} \mid a \in R\} \subset F(R)$. Имеем $\varphi : R \to S, \varphi(a) = \frac{a}{1}$.

*Лемма.* $S$ – подкольцо в $F(R)$, $\varphi$ – изоморфизм: $R \cong S$.

*Доказательство.* $\varphi$ – сюръективно по определению; $\varphi$ – инъективно: $\frac{a}{1} = \frac{b}{1} \Rightarrow a = b$. $\varphi(a+b) = \frac{a+b}{1} = \frac{a}{1} + \frac{b}{1} = \varphi(a) + \varphi(b)$, $\varphi(a \cdot b) = \frac{a \cdot b}{1} = \frac{a}{1} \cdot \frac{b}{1} = \varphi(a) \cdot \varphi(b)$. Кроме того, $\frac{1}{1} \in S, -\frac{a}{1} = \frac{-a}{1} \in S$, поэтому $S$ – подкольцо. $\square$

Отождествим $S$ с $R$ с помощью $\varphi$, то есть если $a \in R$, то $a = \frac{a}{1} \in F(R)$. То есть $R \subset F(R)$ – подкольцо.

*Терминология.* $F(R)$ – *поле частных* целостного кольца $R$.

*Замечание.* $\frac{a}{b} \cdot b = \frac{a}{b} \cdot \frac{b}{1} = \frac{ab}{b} = \frac{a}{1} = a \Rightarrow \frac{a}{b}$ – действительно частное от деления $a$ на $b$ (в поле $F(R)$)!

*Пример.* $F(\mathbb{Z}) = \mathbb{Q}$.

*Упражнение.* $E$ – поле $\Rightarrow F(E) \cong E$.

*Упражнение.* Опишите $F(\mathbb{Z}[i])(= \mathbb{Q}[i])$.

*Задача.* Пусть $R$ – целостное кольцо, $R \subset E$, где $E$ – поле. Тогда $\exists!$ подполе $R \subset F \subset E$, $F \cong F(R)$ (то есть в разумном смысле $F(R)$ – наименьшее поле, содержащее $R$).

## 2.14. **Поле рациональных функций.** (одной переменной)

Пусть $F$ – поле, $R = F[x]$ – целостное кольцо $\Rightarrow$ можно рассмотреть $F(x) := F(R)$ – "поле рациональных функций" от переменной $x$ с коэффициентами из $F$. Элементы $F(x)$ имеют вид $\frac{f}{g}$, где $f, g \in F[x], g \neq 0$; при этом $\frac{f_1}{g_1} = \frac{f_2}{g_2} \Leftrightarrow f_1g_2 = f_2g_1$; если $f \in F[x]$, то $f = \frac{f}{1} \in F(x)$.

*Замечание.* "Рациональные функции" – не функции, а "формальные выражения". Например, если $|F| < \infty$, $f = \prod_{a \in F}(x - a)$, то в $\frac{1}{f}$ ничего нельзя подставить.

Пусть $\varphi \in F(x), \varphi = \frac{f}{g}$. $\varphi$ – "правильная" дробь, если $\deg f < \deg g$.

*Корректность.* $\varphi = \frac{f}{g} = \frac{f_1}{g_1} \Rightarrow f g_1 = f_1 g \Rightarrow \deg f + \deg g_1 = \deg f_1 + \deg g \Rightarrow \deg f_1 = \underbrace{\deg f - \deg g}_{<0} + \deg g_1 < \deg g_1$.

*Лемма.* Пусть $\varphi_1, \varphi_2 \in F(x)$ – правильные. Тогда $\varphi_1 \pm \varphi_2, \varphi_1 \cdot \varphi_2$ – тоже правильные.

*Доказательство.* $\varphi_1 = \frac{f_1}{g_1}, \varphi_2 = \frac{f_2}{g_2} \in F(x)$, $\deg f_i < \deg g_i$. Тогда $\varphi_1 \pm \varphi_2 = \frac{f_1 g_2 \pm f_2 g_1}{g_1 g_2}$, $\deg(f_1 g_2 \pm f_2 g_1) \leq \max(\deg f_1 + \deg g_2; \deg f_2 + \deg g_1) < \deg g_1 + \deg g_2 = \deg(g_1 g_2)$. Для $\varphi_1 \cdot \varphi_2$ доказать самостоятельно. $\square$

*Замечание.* Для поля $\mathbb{Q}$ тоже есть понятие "правильная дробь", однако сумма правильных дробей – не обязательно правильная.

*Предложение.* Пусть $\varphi \in F(x)$. Тогда $\exists! q \in F[x], \psi \in F(x)$, $\psi$ – правильная, $\varphi = q + \psi$.

*Доказательство.* Существование: $\varphi = \frac{f}{g}$. С остатком: $f = gq + r, \deg r < \deg g \Rightarrow \varphi = \frac{f}{g} = q + \psi$, где $\psi = \frac{r}{g}$ – правильная.

Единственность: $q_1 + \psi_1 = q_2 + \psi_2$, где $q_i \in F[x], \psi_i$ – правильные дроби. Тогда $q_1 - q_2 = \underbrace{\psi_2 - \psi_1}_{\text{прав.}} = \frac{r}{g}, \deg r < \deg g$, $(q_1 - q_2)g = r$. Если $q_1 \neq q_2$, то $\deg((q_1 - q_2) \cdot g) \geq \deg g \Rightarrow$ противоречие. $\square$

*Замечание.* ??? считать, что знаменатель $\varphi$ = знаменатель $\psi$ (из доказательства).

*Определение.* $\psi \in F(x)$ – *простейшая дробь* , если $\psi = \frac{f}{p^n}$, где $f, p \in F[x], n \in \mathbb{N}$, $p$ неприводим над $F$, $\deg f < \deg p$ (простейшая $\Rightarrow$ правильная, но не наоборот).

*Примеры.* 1) $F = \mathbb{C}$ : $\frac{a}{(x-c)^n}$, где $a, c \in \mathbb{C}$

2) $F = \mathbb{R}$ : $\frac{a}{(x-c)^n}$, где $a, c \in \mathbb{R}$; $\frac{ax+b}{(x^2+qx+r)^n}$, $a, b, q, r \in \mathbb{R}, \mathrm{Discr}(x^2 + qx + r) = q^2 - 4r < 0$.

Докажем, что любая правильная дробь однозначно представляется в виде суммы простейших.

**Теорема 1.** Пусть $\varphi \in F(x)$ – правильная дробь. Запишем $\varphi = \frac{f}{p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}}$, где $p_i \in F[x]$ – неприводимы над $F$, $p_i \nsim p_j$ при $i \neq j$. Тогда $\varphi$ однозначно представима в виде $\sum_{i=1}^{r} \frac{g_i}{p_i^{n_i}}$, где все слагаемые – правильные дроби (то есть $\deg g_i < \deg p_i^{n_i} = n_i \deg p_i$).

*Доказательство.* Существование: $q_i = p_1^{n_1} \cdot \ldots \cdot p_{i-1}^{n_{i-1}} p_{i+1}^{n_{i+1}} \cdot \ldots \cdot p_r^{n_r}$ (то есть $p_1^{n_1} \cdot \ldots \cdot p_r^{n_r} = q_i p_i^{n_i}$). Заметим, что НОД$(q_1, q_2, \ldots, q_r) = 1$ (ибо если $p$ – неприводим, $p \mid q_1, \ldots, p \mid q_r$ то $p \nsim p_1, \ldots, p \nsim p_r$, что невозможно). Тогда $\exists u_i \in F[x] : 1 = \sum_{i=1}^r u_i q_i \Rightarrow f = \sum_{i=1}^r f u_i q_i =: \sum_{i=1}^r h_i q_i$, где $h_i = f u_i$. Тогда $\varphi = \sum_{i=1}^r \frac{h_i}{p_i^{n_i}}$; $\frac{h_i}{p_i^{n_i}} = f_i + \frac{g_i}{p_i^{n_i}}$, где $\deg g_i < \deg(p_i^{n_i})$. То есть $\varphi = \underbrace{\sum_i f_i}_{\text{многочл.}} + \underbrace{\sum_i \frac{g_i}{p_i^{n_i}}}_{\text{прав. др.}} \Rightarrow \sum_i f_i = 0$, что и требовалось доказать.

Единственность: $\sum_{i=1}^r \frac{g_i}{p_i^{n_i}} = \sum_{i=1}^r \frac{h_i}{p_i^{n_i}}$, дроби правильные $\Rightarrow \sum_{i=1}^r \frac{f_i}{p_i^{n_i}} = 0$ (где $f_i = g_i - h_i$). Требуется доказать: $f_i = 0 \ \forall i$. Покажем, что $f_1 = 0$ (остальное аналогично). Индукция по $n_1$. База $n_1 = 0 \overset{\text{прав.}}{\Rightarrow} f_1 = 0$. Переход: к общему знаменателю $\sum_i f_i q_i = 0 \Rightarrow f_1 g_1 = p_1 u$, где $u \in F[x]$ (ибо $p_1 \mid q_2, \ldots, p_1 \mid q_r$). То есть $p_1 \mid f_1 q_1, \text{НОД}(p_1, q_1) = 1 \Rightarrow p_1 \mid f_1$, То есть $f_1 = p_1 \widetilde{f_1}$. То есть $\frac{f_1}{p_1^{n_1}} = \frac{\widetilde{f_1}}{p_1^{n_1-1}} \underset{\text{инд. пр.}}{\Rightarrow} \widetilde{f_1} = 0 \Rightarrow f_1 = 0$. □

**Теорема 2.** Пусть $\varphi = \frac{g}{p^n}$ – правильная дробь, где $g, p \in F[x]$, $p$ – неприводим над $F$. Тогда $\varphi = \frac{f_1}{p} + \frac{f_2}{p^2} + \ldots + \frac{f_n}{p^n}$, где все слагаемые – простейшие дроби; такое представление однозначно.

*Доказательство.* Существование: индукция по $n$ с тривиальной базой $n = 1$. Переход: $g = pq + r, \deg r < \deg p \Rightarrow \frac{g}{p^n} = \frac{q}{p^{n-1}} + \frac{r}{p^n}$. Дробь $\frac{q}{p^{n-1}}$ – правильная как разность правильных дробей, применяем индуктивное предположение; $\frac{r}{p^n}$ – простейшая дробь.

Единственность: $\sum_{k=1}^n \frac{f_k}{p^k} = \sum_{k=1}^n \frac{g_k}{p^k} \Rightarrow \sum_{k=1}^n \underbrace{\frac{h_k}{p^k}}_{\text{простейш.}} = 0$, где $h_k = f_k - g_k$. Требуется доказать: $h_k = 0 \ \ \forall k$. Индукция по $n$ с тривиальной базой $n = 1$ (одно слагаемое). Переход: домножим на $p$ : $\underbrace{h_1}_{\text{многочл.}} + \underbrace{\frac{h_2}{p} + \ldots + \frac{h_n}{p^{n-1}}}_{\text{прав. дробь}} = 0$ $\Rightarrow h_1 = 0, \frac{h_2}{p} + \ldots + \frac{h_n}{p^{n-1}} = 0 \underset{\text{предп. инд.}}{\Rightarrow} h_2 = \ldots = h_n = 0$. □

Теорема 1 и теорема 2 дают

**Теорема.** (разложение на простейшие). Всякая правильная дробь $\varphi \in F(x)$ однозначно представляется в виде суммы простейших дробей. Если знаменатель $\varphi$ имеет вид $p_1^{n_1} \cdot \ldots \cdot p_r^{n_r}$, где $p_i \in F[x]$ неприводимы, $p_i \nsim p_j$ при $i \neq j$, то в разложение $\varphi$ на простейшие могут войти лишь слагаемые со знаменателями $p_1, p_1^2, \ldots, p_1^{n_1}, p_2, p_2^2, \ldots, p_2^{n_2}, \ldots, p_r, p_r^2, \ldots, p_r^{n_r}$.

*Замечание.* В случае поля $\mathbb{Q}$ любая правильная дробь (то есть $\frac{a}{b}$, где $|a| < b, b > 0$) разлагается на "простейшие" (что это?), но это разложение не всегда единственно.

2.15. **Многочлены над факториальным кольцом.** Цель: доказать, что, если $R$ факториально, то $R[x]$ тоже факториально. (Например, $\mathbb{Z}[x]$ – факториально).

Начнем с некоторых свойств делимости в факториальных кольцах.

Пусть $R$ – *факториальное* кольцо.

*Предложение.* Пусть $a, b \in R, a \sim p_1^{k_1} \cdot \ldots \cdot p_r^{k_r}$, $b \sim p_1^{l_1} \cdot \ldots \cdot p_r^{l_r}$, где $p_i \in R, p_i$ – простые, $p_i \nsim p_j$ при $i \neq j$, $k_i, l_i \in \mathbb{Z}_+$. Тогда

(1) $b \mid a \Leftrightarrow l_i \leq k_i \quad \forall i$;

(2) НОД$(a, b) = p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$, где $m_i = \min(k_i, l_i)$.

*Доказательство.* (1) $b \mid a \Leftrightarrow a = bc$, где $c = p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}, \alpha_i \in \mathbb{Z}_+$ (можно считать, что те же простые – иначе "фиктивно" добавим в степени 0), причем (единственность разложения!) $\forall i: \quad k_i = l_i + \alpha_i \Leftrightarrow \forall i: \quad k_i \geq l_i$.

(2) $d := p_1^{m_1} \cdot \ldots \cdot p_r^{m_r}$, где $m_i = \min(k_i, l_i)$. Согласно (1) $d \mid a, d \mid b$. Если $\widetilde{d} \mid a, \widetilde{d} \mid b$, то $\widetilde{d} \sim p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, где $\beta_i \leq k_i, \beta_i \leq l_i \quad \forall i \Rightarrow \beta_i \leq \min(k_i, l_i) \quad \forall i \Rightarrow \widetilde{d} \mid d$. $\square$

Итак, в факториальном кольце существует НОД.

*Упражнение.* Обобщить часть (2) на случай НОД$(a_1, \ldots, a_n)$.

*Следствие.* Пусть $a, b, p \in R$, $p$ – простой. Тогда $p \mid ab \Leftrightarrow p \mid a$ или $p \mid b$.

*Доказательство.*

$$a \sim p^k \cdot \underbrace{\ldots}_{\text{другие простые}}, \; b \sim p^l \cdot \underbrace{\ldots}_{\text{другие простые}} \Rightarrow ab \sim p^{k+l} \cdot \underbrace{\ldots}_{\text{другие простые}}.$$

Тогда $p \nmid ab \Leftrightarrow k + l = 0 \overset{k,l \in \mathbb{Z}_+}{\Leftrightarrow} k = 0, l = 0 \Leftrightarrow p \nmid a, p \nmid b$. $\square$

*Предложение.* Пусть $a_1, \ldots, a_n, b_1, \ldots, b_n, d \in R, \quad \forall i: a_i = db_i$. Тогда НОД$(a_1, \ldots, a_n) = d \Leftrightarrow$ НОД$(b_1, \ldots, b_n) = 1$.

*Доказательство.* Для простоты обозначений рассмотрим случай $n = 2$ (упражнение: общий случай). Запишем $d \sim p_1^{\gamma_1} \cdot \ldots \cdot p_r^{\gamma_r}$, $b_1 \sim p_1^{\alpha_1} \cdot \ldots \cdot p_r^{\alpha_r}$, $b_2 \sim p_1^{\beta_1} \cdot \ldots \cdot p_r^{\beta_r}$, здесь $p_i$ – простые, $p_i \nsim p_j$ при $i \neq j$, $\alpha_i, \beta_i, \gamma_i \in \mathbb{Z}_+$. Тогда $a_1 \sim p_1^{\alpha_1 + \gamma_1} \cdot \ldots \cdot p_r^{\alpha_r + \gamma_r}$, $a_2 \sim p_1^{\beta_1 + \gamma_1} \cdot \ldots \cdot p_r^{\beta_r + \gamma_r}$. При этом $d =$ НОД$(a_1, a_2) \Leftrightarrow \forall i: \quad \gamma_i = \min(\alpha_i + \gamma_i; \beta_i + \gamma_i)$ $\Leftrightarrow \forall i: \quad \min(\alpha_i; \beta_i) = 0 \Leftrightarrow$ НОД$(b_1, b_2) = 1$. $\square$

Перейдем к многочленам над $R$. Пусть $f \in R[x]$, $f = a_n x^n + \ldots + a_1 x + a_0, a_i \in R$. Определим $c(f) =$ НОД$(a_0, a_1, \ldots, a_n)$ – "содержание" $f$ ; $c(f)$ определено с точностью до $\sim$ .

$f$ – *примитивен* , если $c(f) = 1$, то есть его коэффициенты взаимно просты в совокупности.

*Пример.* $R = \mathbb{Z}$, $f = 2x^3 + 4x + 10, \quad c(f) = 2$; $g = 2x^3 + 3x + 10, \quad c(g) = 1$, то есть $g$ – примитивный.

*Замечание.* Если $c(f) = 1, a \in R$, то $c(af) = a$.

**Лемма Гаусса.** Пусть $f, g \in R[x]$. Если $f, g$ – примитивны, то $f \cdot g$ также примитивен.

*Доказательство.* Пусть $f = \sum_i a_i x^i, g = \sum_j b_j x^j$. Пусть $p \in R$, $p$ – простой. Так как $c(f) = 1$, то $p$ делит не все коэффициенты $f$, то же для $g$. Пусть $k$ – наименьшее такое, что $p \nmid a_k$ (то есть $p \mid a_0, \ldots, p \mid a_{k-1}$), $l$ – наименьшее такое, что $p \nmid b_l$ (то есть $p \mid b_0, \ldots, p \mid b_{l-1}$). Рассмотрим коэффициент $f \cdot g$ при $x^{k+l}$, он равен

$$A := a_k b_l + a_{k+1} b_{l-1} + \ldots + a_{k+l} b_0 + a_{k-1} b_{l+1} + \ldots + a_0 b_{k+l} =: a_k b_l + B.$$

По построению, $p \mid B$. С другой стороны, $p \nmid a_k b_l$, то есть $p \nmid A$. Вывод: для любого простого $p \in R$ найдется коэффициент $f \cdot g$, не делящий $p$. То есть коэффициенты $f \cdot g$ взаимно просты, то есть $c(f) = 1$. $\square$

*Замечание.* Обратно, если $f \cdot g$ – примитивный, то $f, g$ тем более примитивны (почему?).

*Упражнение* ("обобщенная" лемма Гаусса). Пусть $f, g \in R[x]$. Тогда $c(fg) \sim c(f)c(g)$. Указание: $f = c(f)\widetilde{f}, g = c(g)\widetilde{g}$, где $\widetilde{f}, \widetilde{g}$ примитивны. Примените лемму Гаусса.

Каковы простые элементы в $R[x]$? Во-первых, простые элементы из $R$ остаются простыми и в $R[x]$ (степень ...). Далее, пусть $f \in R[x], \deg f > 0$ (то есть $f \notin R$). Если $c(f) \neq 1$, то $f$ не простой. Пусть $c(f) = 1$, то есть $f$ – примитивный. В каком случае $f$ прост в $R[x]$?

Рассмотрим поле частных $F = F(R), R \subset F, R[x] \subset F[x]$.

*Предложение.* Пусть $f \in R[x], \deg f > 0, c(f) = 1$. Тогда $f$ – простой элемент в $R[x] \Leftrightarrow f$ – простой элемент в $F[x]$ (то есть $f$ неприводим над полем $F$).

*Доказательство.* $\Leftarrow$: если $f$ не прост в $R[x]$, то $f = gh$, где $g, h \in R[x], \deg g < \deg f, \deg h < \deg f$ в силу примитивности $f$ ("константа не выносится"). В частности, $f$ приводим над $F$.

$\Rightarrow$: $f = gh$, где $g, h \in F[x], \deg g < \deg f, \deg h < \deg f$. Запишем $g = \frac{a_1}{a_2}\widetilde{g}, h = \frac{b_1}{b_2}\widetilde{h}$, где $a_1, a_2, b_1, b_2 \in R$, $\widetilde{g}, \widetilde{h} \in R[x]$, $c(\widetilde{g}) = 1, c(\widetilde{h}) = 1$. Тогда $f = \frac{a_1 b_1}{a_2 b_2}\widetilde{g}\widetilde{h}$, то есть $a_2 b_2 f = a_1 b_1 \widetilde{g}\widetilde{h}$; $c(f) = 1 \Rightarrow c(a_2 b_2 f) = a_2 b_2$; (Лемма Гаусса) $c(\widetilde{g}\widetilde{h}) = 1 \Rightarrow c(a_1 b_1 \widetilde{g}\widetilde{h}) = a_1 b_1$. То есть $a_2 b_2 \sim a_1 b_1$ в кольце $R$, то есть $\exists u \in R^* : a_1 b_1 = u a_2 b_2$. Тогда $f = (u\widetilde{g})\widetilde{h}$ – это нетривиальное разложение на множители в кольце $R[x]$(ибо $\deg \widetilde{g} = \deg g < \deg f, \ldots$) $\Rightarrow$ противоречие. $\square$

*Следствие.* Простые элементы в $R[x]$ – это в точности: 1) простые элементы в $R$; 2) примитивные неприводимые над $F$.

**Теорема.** $R[x]$ – факториально.

*Доказательство.* Пусть $f \in R[x], f \neq 0, f \notin R[x]^* = R^*$. Надо доказать существование и единственность разложения $f$ на простые множители.

Существование: пишем $f = a\widetilde{f}$, где $a \in R$, $\widetilde{f}$ – примитивный. $a \in R$ разлагаем на простые ввиду факториальности кольца $R$. Далее, если $\widetilde{f}$ обратим (то есть $\widetilde{f} \in R^*$) или прост, то разложение получено. В противном случае $\widetilde{f} = gh$, где $\deg g < \deg f, \deg h < \deg f$, $g, h$ тоже примитивные. Повторяем те же рассуждения для $g$ и $h$, и тому подобное.

Единственность: $f = a_1 \cdot \ldots \cdot a_r \cdot p_1 \cdot \ldots \cdot p_m = b_1 \cdot \ldots \cdot b_s \cdot q_1 \cdot \ldots \cdot q_n$, где $a_i, b_j$ – простые в $R$, $p_i, q_j$ – примитивные многочлены в $R[x]$, неприводимые над $F$. Так как $F[x]$ – факториально (это для любого поля), то $m = n$, и (при подходящей нумерации) $q_i \sim p_i$ в $F[x]$, то есть $q_i = u_i p_i$, где $u_i \in F^*$ (NB: $a_i, b_j \in F^*$). Запишем $u_i = \frac{v_i}{w_i}$, где $v_i, w_i \in R, w_i \neq 0$. То есть $w_i q_i = v_i p_i, c(w_i q_i) = w_i, c(v_i p_i) = v_i \Rightarrow w_i \sim v_i$ в $R$, то есть $u_i \in R^* (= R[x]^*)$. Итак, $q_i \sim p_i$ также и в $R[x]$. Наконец, $a_1 \cdot \ldots \cdot a_r = u b_1 \cdot \ldots \cdot b_s$ (где $u = u_1 \cdot \ldots \cdot u_n \in R^*$) $\Rightarrow$ (факториальность $R$) $r = s$ и при подходящей нумерации $a_i \sim b_i$ в $R$. $\square$

*Предложение* (критерий Эйзенштейна). Пусть $f \in R[x]$ примитивен, $f = a_0 + a_1 x + \ldots + a_n x^n$. Пусть существует простой $p \in R$ такой, что $p \mid a_0, p \mid a_1, \ldots, p \mid a_{n-1}, (p \nmid a_n), p^2 \nmid a_0$. Тогда $f$ – простой элемент $R[x]$ (в частности, неприводим над $F$).

*Пример.* $f = x^n - 2$ прост в $\mathbb{Z}[x]$ по критерию Эйзенштейна при $p = 2$.

*Замечание.* Для неприводимости над $F$ примитивность не нужна (почему?).

*Доказательство критерия Эйзенштейна.* От противного: $f = gh$, где $m = \deg g < \deg f = n, \deg h < \deg f$. Запишем $g = \sum_i b_i x^i, h = \sum_j c_j x_j$. Так как $p \mid a_0 = b_0 c_0$, то $p \mid b_0$ или $p \mid c_0$. Так как $p^2 \nmid a_0$, то если $p \mid b_0$, то $p \nmid c_0$ (и наоборот). Для определенности предположим, что $p \mid b_0$, $p \nmid c_0$. Далее,

$$p \mid a_1 = b_0 c_1 + b_1 c_0, \quad p \mid b_0, p \nmid c_0 \Rightarrow p \mid b_1;$$

$$p \mid a_2 = b_0 c_2 + b_1 c_1 + b_2 c_0, \quad p \mid b_0, p \mid b_1, p \nmid c_0 \Rightarrow p \mid b_2;$$

$$\ldots$$

$$p \mid a_m = b_0 c_m + b_1 c_{m-1} + \ldots + b_m c_0, \quad p \mid b_0, p \mid b_1, \ldots, p \mid b_{m-1}, p \nmid c_0 \Rightarrow p \mid b_m.$$

То есть все коэффициенты $g$ кратны $p \Rightarrow$ все коэффициенты $f$ кратны $p \Rightarrow$ противоречие $(p \nmid a_n)$. $\square$

2.16. **Многочлены нескольких переменных.** Введение: Пример многочлена от двух переменных: $x^2 y + 2y^2 + 3x - 5y + 1$. "Общий вид": $\sum_{i,j \in \mathbb{Z}_+} a_{ij} x^i y^j$, где среди $a_{ij}$ лишь конечное число $\neq 0$.

Любой многочлен от $x, y$ – многочлен от $y$, коэффициенты которого – многочлены от $x$.

$$\sum_{i,j\in\mathbb{Z}_+} a_{ij}x^iy^j = \sum_{j\in\mathbb{Z}_+}\left(\sum_{i\in\mathbb{Z}_+} a_{ij}x^i\right)y^j$$

Например, $x^2y + 2y^2 + 3x - 5y + 1 = 2y^2 + (x^2 - 5)y + (3x + 1)$. "Аналогично" для $n$ переменных. К точным определениям.

Пусть $R$ – кольцо.

*Определение.* Кольцо многочленов от переменных $x_1, \ldots, x_n$ с коэффициентами в $R$ – это кольцо $R[x_1, \ldots, x_n] := R[x_1, \ldots, x_{n-1}][x_n]$.

*Комментарий.* 1) Это *индуктивное* определение. При $n = 1$ было. $n = 2$ : $R[x_1, x_2] = R[x_1][x_2] = S[x_2]$, где $S = R[x_1]$, и так далее.

2) Недостаток данного определения: нарушение "симметрии" между $x_1, \ldots, x_n$. Например, $x_1, x_2 \in R[x_1, x_2]$ имеют несколько разный смысл: $x_2$ – "переменная", $x_1$ – коэффициент (но он – переменная с точки зрения кольца коэффициентов). Можно дать "симметричное" определение (строго говоря, получится *другое* кольцо, хотя изоморфное этому).

*Лемма.* Пусть $f \in R[x_1, \ldots, x_n]$. Тогда

$$f = \sum_{i_1,\ldots,i_n\in\mathbb{Z}_+} a_{i_1,\ldots,i_n}x_1^{i_1}\cdot\ldots\cdot x_n^{i_n},$$

где $a_{i_1,\ldots,i_n} \in R$, лишь конечное множество $\neq 0$; такое представление единственно (то есть $\sum a_{i_1,\ldots,i_n}x_1^{i_1}\cdot\ldots\cdot x_n^{i_n} = \sum b_{i_1,\ldots,i_n}x_1^{i_1}\cdot\ldots\cdot x_n^{i_n} \Leftrightarrow a_{i_1,\ldots,i_n} = b_{i_1,\ldots,i_n} \quad \forall i_1, \ldots, i_n \in \mathbb{Z}_+$).

*Доказательство.* Индукция по $n$. База: $n = 1$ было ("определение"). Переход от $n - 1$ к $n$.

Существование: По определению, $f = \sum_k u_k x_n^k$, где $u_k \in R[x_1, \ldots, x_{n-1}]$. Предположение индукции:

$$u_k = \sum_{i_1,\ldots,i_{n-1}\in\mathbb{Z}_+} a_{i_1,\ldots,i_{n-1},k}x_1^{i_1}\cdot\ldots\cdot x_{n-1}^{i_{n-1}} \Rightarrow$$

$$f = \sum_{i_1,\ldots,i_{n-1},k\in\mathbb{Z}_+} a_{i_1,\ldots,i_{n-1},k}x_1^{i_1}\cdot\ldots\cdot x_{n-1}^{i_{n-1}}x_n^k,$$

что и требовалось доказать.

Единственность: упражнение. □

*Обозначения.* Пусть $\alpha \in \mathbb{Z}_+^n = \underbrace{\mathbb{Z}_+ \times \ldots \times \mathbb{Z}_+}_{n}$, $\alpha = (\alpha_1, \ldots, \alpha_n)$, $x^\alpha := x_1^{\alpha_1}\cdot\ldots\cdot x_n^{\alpha_n}$, здесь $\alpha$ – "мультииндекс" (или "мультистепень"). То есть $\sum_{i_1,\ldots,i_n\in\mathbb{Z}_+} a_{i_1,\ldots,i_n}x_1^{i_1}\cdot\ldots\cdot x_n^{i_n} = \sum_{\alpha\in\mathbb{Z}_+^n} a_\alpha x^\alpha$.

Итак, элементы $R[x_1, \ldots, x_n]$ однозначно записываются в виде $\sum_{\alpha\in\mathbb{Z}_+^n} a_\alpha x^\alpha$; при этом лишь конечное множество $a_\alpha \neq 0$.

Заметим, что если $f = \sum_{\alpha\in\mathbb{Z}_+^n} a_\alpha x^\alpha, g = \sum_{\alpha\in\mathbb{Z}_+^n} b_\alpha x^\alpha$, то $f+g = \sum_{\alpha\in\mathbb{Z}_+^n}(a_\alpha + b_\alpha)x^\alpha$. Как умножать? Если $\alpha = (i_1,\ldots,i_n), \beta = (j_1,\ldots,j_n) \in \mathbb{Z}_+^n$, то определим $\alpha+\beta := (i_1+j_1,\ldots,i_n+j_n)$ (*Упражнение*: изучите свойства этой операции в $\mathbb{Z}_+^n$). Тогда $x^\alpha \cdot x^\beta = x^{\alpha+\beta}$. То есть

$$f\cdot g = \left(\sum_\alpha a_\alpha x^\alpha\right)\cdot\left(\sum_\beta b_\beta x^\beta\right) = \left(\sum_{\alpha,\beta} a_\alpha b_\beta x^{\alpha+\beta}\right) = \sum_\gamma \left(\sum_{\alpha+\beta=\gamma} a_\alpha b_\beta\right) x^\gamma.$$

*Замечание.* Можно рассмотреть, скажем, $R[x_2][x_1]$. Из предыдущих формул видно, что элементы этого кольца записываются так же, как $R[x_1][x_2]$, и так же складываются и умножаются. То есть $R[x_2][x_1] \cong R[x_1][x_2]$. Аналогично для любого числа переменных. (Принято отождествлять все эти кольца с помощью этих изоморфизмов).

*Терминология.* Многочлен $x^\alpha = x_1^{i_1}\cdot\ldots\cdot x_n^{i_n}$ – *одночлен* (= *моном* ). Если $f = \sum_\alpha a_\alpha x^\alpha$, то $x^\alpha$ *входит* в $f$, если $a_\alpha \neq 0$. $a_\alpha x^\alpha$ –*член* многочлена $f$.

*Степень* одночлена $x^\alpha = x_1^{i_1}\cdot\ldots\cdot x_n^{i_n}$ – это $i_1+\ldots+i_n \in \mathbb{Z}_+$. Если $f \in R[x_1,\ldots,x_n], f\neq 0$, то *степень* $f$ – это наибольшая из степеней входящих в $f$ одночленов. Обозначение: $\deg f$.

Можно определить степень по каждой переменной (не понадобится ...)

*Пример.* $f = x^2y+2y^2+3x-5y+1$. Тогда $\deg f = 3$ (но $\deg_x f = 2, \deg_y f = 2$).

Пусть $f \in R[x_1,\ldots,x_n]$. $f$ – *однородный* многочлен *степени* $m$, если все одночлены, входящие в $f$, имеют степень $m$. (В частности, по определению, 0 – однородный любой степени!).

*Лемма.* Пусть $f \in R[x_1,\ldots,x_n], \deg f = m$. Тогда $f = f_0+f_1+\ldots+f_m$, где $f_k$ – однородный многочлен степени $k$ $\forall k = 0,1,\ldots,m$. Такое представление единственно.

*Доказательство.* $f_k :=$ сумма членов степени $k$, входящих в $f$. □

*Пример.* $f = x^2y+2y^2+3x-5y+1 = f_0+f_1+f_2+f_3$, где $f_0 = 1, f_1 = 3x-5y, f_2 = 2y^2, f_3 = x^2y$.

Многочлены $f_k$ из леммы выше называются *однородными компонентами* $f$.

*Упражнение.* $(f+g)_k = f_k+g_k$ (то есть при сложении многочленов однородные компоненты складываются).

**Теорема.** Пусть $R$ – целостное кольцо. Тогда

(1) $R[x_1,\ldots,x_n]$ – целостное кольцо;

(2) $\forall f,g \in R[x_1,\ldots,x_n], f\neq 0, g\neq 0 : \deg(fg) = \deg f + \deg g$.

*Доказательство.* (1) Индукция по $n$ с базой $n=1$: было раньше...

(2) а) Начнем с $f = ax^\alpha, g = bx^\beta$, где $a\neq 0, b\neq 0, \alpha = (i_1,\ldots,i_n), \beta = (j_1,\ldots,j_n)$. Тогда $fg = abx^{\alpha+\beta}$, причем $ab\neq 0$. То есть $\deg fg = i_1+j_1+i_2+j_2+\ldots+i_n+j_n = (i_1+\ldots+i_n)+(j_1+\ldots+j_n) = \deg f + \deg g$.

б) Пусть $f$ – однородный степени $l$, $g$ – однородный степени $m$, то есть $f$ – сумма членов степени $l$, $g$ –сумма членов степени $m$. Тогда $fg$ – сумма членов степени $l+m$ (согласно случаю а). То есть $fg$ – однородный степени $l+m$.

в) Общий случай: $f = f_0+f_1+\ldots+f_l, g = g_0+g_1+\ldots+g_m$; $f_i, g_j$ – однородные компоненты. Тогда $fg = \sum_{i,j} \underbrace{f_i \cdot g_j}_{\text{однор. ст. } i+j} = \underbrace{f_l \cdot g_m}_{\text{однор. ст. } l+m} +(\text{однор. ст.} < \text{l+m}).$
То есть $\deg fg = l+m = \deg f + \deg g$. □

*Замечание.* Из рассмотренного выше $fg = \sum_{i,j} f_i g_j = \sum_k \left(\sum_{i+j=k} f_i g_j\right)$, то есть $(fg)_k = \sum_{i+j=k} f_i g_j = f_0 g_k + f_1 g_{k-1} + \ldots + f_k g_0$.

**Теорема.** Пусть $R$ – факториальное кольцо. Тогда $R[x_1, \ldots, x_n]$ – факториальное кольцо.

*Доказательство.* Индукция по $n$ с базой $n = 1 \ldots$ □

*Следствие.* Пусть $F$ – поле. Тогда $F[x_1, \ldots, x_n]$ – факториальное кольцо.

*Замечание.* Если $n \geq 2$, то $F[x_1, \ldots, x_n]$ не является евклидовым. Почему? Рассмотрим случай $n = 2$ :

*Упражнение.* Не существуют $q, r \in F[x, y], \deg r < 1 = \deg x :\quad y = qx+r$ (то есть в $F[x, y]$ нет аналога деления с остатком в $F[x]$). Отсюда, строго говоря, еще *не* следует, что $F[x, y]$ не является евклидовым. Но:

*Упражнение.* НОД$(x, y) = 1$, но не существует $u, v \in F[x, y] :\ ux + vy = 1$ ( $\Rightarrow F[x, y]$ не является евклидовым).

Два последних упражнения легко обобщить на случай $\forall n \geq 2$.

*Замечание.* Если $f \in R[x_1, \ldots, x_n], c_1, \ldots, c_n \in R$, то можно определить $f(c_1, \ldots, c_n) \in R$ (сделайте!). Формальные свойства "те же": согласованы с операциями.

*Задача.* Если $F$ – бесконечное поле, $f, g \in F[x_1, \ldots, x_n]$, $\forall c_1, \ldots, c_n \in F :$ $f(c_1, \ldots, c_n) = g(c_1, \ldots, c_n)$, то $f = g$.

2.17. **Симметрические многочлены.** Пусть $R$ – кольцо. Многочлен $f \in R[x_1, \ldots, x_n]$ – симметрический, если $f$ не меняется при любых перестановках переменных. Что это означает?

2.17.1. *О перестановках. Перестановка* (*подстановка* ) ("степени $n$") – это биекция $\pi : \{1, \ldots, n\} \to \{1, \ldots, n\}$. Запись $\pi = \begin{pmatrix} 1 & 2 & \ldots & n \\ \pi(1) & \pi(2) & \ldots & \pi(n) \end{pmatrix}$.
$S_n :=$ множество всех перестановок степени $n$. $|S_n| = n!$ Если $\pi_1, \pi_2 \in S_n$, то $\pi_1 \circ \pi_2 \in S_n$, здесь $\circ$ – композиция ("произведение" перестановок). Ясно, что $(\pi_1 \circ \pi_2) \circ \pi_3 = \pi_1 \circ (\pi_2 \circ \pi_3)$. Кроме того $\mathrm{id} \in S_n$ и $\forall \pi \in S_n : \pi^{-1} \in S_n$, причем $\pi \circ \pi^{-1} = \pi^{-1} \circ \pi = \mathrm{id}$. (Это означает, что $S_n$ – группа. Эта группа *некоммутативна* при $n \geq 3$).

*Транспозиция* – это перестановка $\pi$ такая, что $\pi(i) = j, \pi(j) = i$ для некоторых $i \neq j$, и $\pi(k) = k \quad \forall k \neq i, k \neq j$. Обозначение: $(i, j)$. Ясно, что любая перестановка = произведение транспозиций; такое представление не единственно...

Вернемся к многочленам. Если $f \in R[x_1, \ldots, x_n], \pi \in S_n$, то определим $f^\pi \in R[x_1, \ldots, x_n], \quad f^\pi(x_1, \ldots, x_n) = f(x_{\pi(1)}, \ldots, x_{\pi(n)})$.

*Пример.* $f = x_1^2x_2 + x_2x_3 \in \mathbb{Z}[x_1, x_2, x_3]$, $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \Rightarrow f^\pi = x_2^2x_3 + x_3x_1 = x_2^2x_3 + x_1x_3$.

*Упражнение.* 1) $(f + g)^\pi = f^\pi + g^\pi$, $(fg)^\pi = f^\pi g^\pi$; 2) $(f^{\pi_1})^{\pi_2} = f^{\pi_1 \circ \pi_2}$

Итак, $f \in R[x_1, \ldots, x_n]$ – *симметрический* , если $\forall \pi \in S_n : \quad f^\pi = f$ (то есть $f(x_{\pi(1)}, \ldots, x_{\pi(n)}) = f(x_1, \ldots, x_n)$).

*Замечание.* $f$ симметрический $\Leftrightarrow$ для любой *транспозиции* $\pi : \quad f^\pi = f$ (в силу упражнения, пункт 2).

*Пример.* 1) $n = 1 \Rightarrow$ любой многочлен симметрический.

2)$n = 3 : x_1^4 + x_2^4 + x_3^4; x_1^2x_2 + x_2^2x_1 + x_1^2x_3 + x_3^2x_1 + x_2^2x_3 + x_3^2x_2$ – симметрические; $x_1^2x_2 + x_2^2x_3 + x_3^2x_1$ – *не* симметрический.

Внимание: $x_1^2 + x_2^2$ симметрический в $R[x_1, x_2]$, *не* симметрический в $R[x_1, x_2, x_3]$.

*Упражнение.* Симметрические многочлены – подкольцо в $R[x_1, \ldots, x_n]$.

*Замечания.* 1) Если $f \in R[x_1, \ldots, x_n]$ – однородный степени $m$, то $\forall \pi \in S_n$ $f^\pi$ тоже однородный степени $m$.

2) Пусть $f = \sum_k f_k$, где $f_k$ – однородный степени $k$. Тогда $f^\pi = \sum_k f_k^\pi$, где $f_k^\pi$ однородный степени $k$, то есть $(f^\pi)_k = f_k^\pi$. В частности, $f$ – симметричный $\Leftrightarrow \forall k : \quad f_k$ – симметричный.

*Элементарные симметрические многочлены* от $n$ переменных – это $\sigma_1, \sigma_2, \ldots, \sigma_n \in R[x_1, \ldots, x_n]$, определяемые формулами

$$\sigma_k = \sum_{1 \leq i_1 < i_2 < \ldots < i_k \leq n} x_{i_1}x_{i_2} \cdot \ldots \cdot x_{i_n}.$$

По определению, это – симметрические многочлены (Иногда: $\sigma_0 = 1$).

*Пример.* $n = 4 :$

$$\sigma_1 = x_1 + x_2 + x_3 + x_4;$$

$$\sigma_2 = x_1x_2 + x_1x_3 + x_1x_4 + x_2x_3 + x_2x_4 + x_3x_4;$$

$$\sigma_3 = x_1x_2x_3 + x_1x_2x_4 + x_1x_3x_4 + x_2x_3x_4;$$

$$\sigma_4 = x_1x_2x_3x_4.$$

*Упражнение.* Число одночленов, входящих в $\sigma_k \in R[x_1, \ldots, x_n]$, равно $C_n^k$.

**Основная теорема о симметрических многочленах.** Пусть $f \in R[x_1, \ldots, x_n]$, $f$ – симметрический. Тогда $\exists! g \in R[y_1, \ldots, y_n]$ такой, что $f = g(\sigma_1, \ldots, \sigma_n)$ (то

есть любой симметрический многочлен однозначно представим в виде многочлена от $\sigma_1, \sigma_2, \ldots, \sigma_n$).

*Замечание.* Обратно, $\forall g \in R[y_1, \ldots, y_n]$ многочлен $f = g(\sigma_1, \ldots, \sigma_n) \in R[x_1, \ldots, x_n]$ – симметрический (ибо сумма и произведение симметрических многочленов – симметрические).

*Примеры.* $n = 2 : \sigma_1 = x_1 + x_2,\ \sigma_2 = x_1 x_2$. $x_1^2 + x_2^2 = (x_1 + x_2)^2 - 2x_1 x_2 = \sigma_1^2 - 2\sigma_2$ (то есть при $f = x_1^2 + x_2^2$ имеем $g = y_1^2 - 2y_2$). $x_1^3 + x_2^3 = (x_1 + x_2)^3 - 3x_1 x_2 (x_1 + x_2) = \sigma_1^3 - 3\sigma_1\sigma_2$.

*Замечание* о формулах Виета: если $f \in F[x], f = a_0 + a_1 x + \ldots + a_n x^n$, $a_n \neq 0, c_1, c_2, \ldots, c_n \in F$ – корни $f$ с учетом кратности, то $\forall k = 1, 2, \ldots, n$ : $\sigma_k(c_1, \ldots, c_n) = (-1)^k \frac{a_{n-k}}{a_n}$.

Основная теорема $\Rightarrow$ значение любого симметрического многочлена на корнях $f$ можно выразить через коэффициенты $f$.

*Пример.* $f = a_2 x^2 + a_1 x + a_0; c_1, c_2$ – корни $f \Rightarrow \sigma_1(c_1, c_2) = c_1 + c_2 = -\frac{a_1}{a_2}$; $\sigma_2(c_1, c_2) = c_1 c_2 = \frac{a_0}{a_2}$. То есть, например, $c_1^3 + c_2^3 = \sigma_1(c_1, c_2)^3 - 3\sigma_1(c_1, c_2)\sigma_2(c_1, c_2) = \frac{3a_0 a_1 a_2 - a_1^3.}{a_2^3}$

Более общий пример: рассмотрим $D = \prod_{1 \leq i < j \leq n} (x_i - x_j)^2 \in R[x_1, \ldots, x_n]$ – симметрический многочлен.

Если $f \in F[x], f = a_n x^n + \ldots + a_1 x + a_0,\ a_n \neq 0,\ c_1, \ldots, c_n$ – корни $f$ с учетом кратности, то *дискриминант* $f$ – это

$$\mathrm{Discr}(f) := a_n^{2n-2} D(c_1, \ldots, c_n) = a_n^{2n-2} \prod_{1 \leq i < j \leq n} (c_i - c_j)^2.$$

Смысл: $f$ имеет кратные корни $\Leftrightarrow \mathrm{Discr}(f) = 0$.

Основная теорема $\Rightarrow$ $\mathrm{Discr}(f)$ можно выразить через коэффициенты $f$ ("независимо от того, какие корни").

*Упражнение.* $\mathrm{Discr}(f)$ – *многочлен* от $a_0, a_1, \ldots, a_n$ (для этого – множитель $a_n^{2n-2}$).

*Упражнение.* $f = x^3 + px + q \Rightarrow \mathrm{Discr}(f) = -4p^3 - 27q^2$.

*Подготовка к доказательству основной теоремы*

Рассмотрим $x^\alpha = x_1^{i_1} \cdot \ldots \cdot x_n^{i_n}$ и $x^\beta = x_1^{j_1} \cdot \ldots \cdot x_n^{j_n}$. Скажем, что $x^\alpha$ *выше* $x^\beta$ ($x^\alpha \succ x^\beta$), если $\exists r : i_1 = j_1, \ldots, i_{r-1} = j_{r-1}, i_r > j_r$ (не исключено, что $r = 1$), то есть первая из ненулевых разностей $i_k - j_k > 0$.

Это так называемый *лексикографический* (= словарный) порядок.

По определению, любые два одночлена связаны $\succ$ или $\prec$ .

*Пример.* $x_1^3 x_2^2 x_3 \succ x_1^3 x_2 x_3^5$ $(n = 3)$.

Внимание: порядок зависит от исходного упорядочения неизвестных. Например $(n = 2)$: $x \succ y \Rightarrow x^2 y \succ xy^2$ ("латинский алфавит"); $y \succ x \Rightarrow xy^2 \succ x^2 y$ ("кириллический алфавит").

*Предложение* (свойства лексикографического порядка).

(1) $x^\alpha \succ x^\beta, x^\beta \succ x^\gamma \Rightarrow x^\alpha \succ x^\gamma$;
(2) $x^\alpha \succ x^\beta \Rightarrow \quad \forall \gamma : \ x^{\alpha+\gamma} \succ x^{\beta+\gamma}$;
(3) $x^\alpha \succ x^\beta, x^\gamma \succ x^\delta \Rightarrow x^{\alpha+\gamma} \succ x^{\beta+\delta}$.

*Замечание.* (1) $\Rightarrow$ в любом конечном множестве одночленов есть наивысший.

*Доказательство.* $\alpha = (i_1, \ldots, i_n), \beta = (j_1, \ldots, j_n), \gamma = (k_1, \ldots, k_n)$.

(1) Дано: $i_1 = j_1, \ldots, i_{r-1} = j_{r-1}, i_r > j_r, \quad j_1 = k_1, \ldots, j_{s-1} = k_{s-1}, j_s > k_s$. Три варианта $r > s, r = s, r < s$. Пусть $r > s$. Тогда

$$\begin{array}{cccccc} i_1 & \ldots & i_{s-1} & i_s & \ldots & \\ \shortparallel & \ldots & \shortparallel & \shortparallel & \ldots & \\ j_1 & \ldots & j_{s-1} & j_s & \ldots & \Rightarrow \quad x^\alpha > x^\gamma. \\ \shortparallel & \ldots & \shortparallel & \vee & \ldots & \\ k_1 & \ldots & k_{s-1} & k_s & \ldots & \end{array}$$

Случаи $r = s, r < s$ – упражнение.

(2) Дано: $i_1 = j_1, \ldots, i_{r-1} = j_{r-1}, i_r > j_r$; $\alpha + \gamma = (i_1 + k_1, \ldots, i_n + k_n)$, $\beta + \gamma = (j_1 + k_1, \ldots, j_n + k_n)$. То есть $i_1 + k_1 = j_1 + k_1, \ldots, i_{r-1} + k_{r-1} = j_{r-1} + k_{r-1}, i_r + k_r > j_r + k_r \quad \Rightarrow \quad x^{\alpha+\gamma} \succ x^{\beta+\gamma}$.

(3) Согласно (2), $x^{\alpha+\gamma} \succ x^{\beta+\gamma}, \ x^{\beta+\gamma} \succ x^{\beta+\delta} \overset{(1)}{\Rightarrow} x^{\alpha+\gamma} \succ x^{\beta+\delta}$. $\square$

Пусть $f = \sum_\alpha a_\alpha x^\alpha \in R[x_1, \ldots, x_n], f \neq 0$. *Высший одночлен* $f$ – это наивысший среди одночленов, входящих в $f$. Если $x^\alpha$ – высший одночлен $f$, то $a_\alpha x^\alpha$ – *высший член* $f$. То есть $f = a_\alpha x^\alpha + \widetilde{f}$, где $a_\alpha \neq 0$, и все одночлены, входящие в $\widetilde{f}$, ниже, чем $x^\alpha$.

*Пример.* ($n = 3$): $f = x_1 x_2^2 + 2x_1^2 x_2 + 3x_1^2 x_3 \Rightarrow$ высший одночлен $f$ – это $x_1^2 x_2$; высший член $f$ – это $2x_1^2 x_2$.

*Лемма 1.* Пусть $x^\alpha$ – высший член $f$, $x^\beta$ – высший член $g$. Тогда $x^{\alpha+\beta}$ – высший член $fg$.

*Доказательство.* $f = x^\alpha + \widetilde{f}$, все одночлены, входящие в $\widetilde{f}$, ниже, чем $x^\alpha$; $g = x^\beta + \widetilde{g}$, все одночлены, входящие в $\widetilde{g}$, ниже, чем $x^\beta$. Тогда $fg = x^{\alpha+\beta} + x^\alpha \widetilde{g} + x^\beta \widetilde{f} + \widetilde{f}\widetilde{g} =: x^{\alpha+\beta} + h$. Проверим, что все одночлены, входящие в $h$, ниже, чем $x^{\alpha+\beta}$. В самом деле, пусть $x^\gamma$ входит в $\widetilde{g}$ (то есть $x^\beta \succ x^\gamma$), $x^\delta$ входит в $\widetilde{f}$ (то есть $x^\alpha \succ x^\delta$). Тогда в $h$ могут входить лишь одночлены вида $x^{\alpha+\gamma}, x^{\beta+\delta}, x^{\gamma+\delta}$. Но $x^{\alpha+\beta} \succ x^{\alpha+\gamma}, x^{\alpha+\beta} \succ x^{\delta+\beta}, x^{\alpha+\beta} \succ x^{\delta+\gamma}$ по свойствам лексикографического порядка. $\square$

*Упражнение.* Пусть $R$ – *целостно* , $x^\alpha$ – высший одночлен $f$, $x^\beta$ – высший одночлен $g$. Тогда $x^{\alpha+\beta}$ – высший одночлен $fg$.

*Упражнение.* Обобщить лемму 1 на случай нескольких множителей (индукция).

Пусть $\alpha = (i_1, i_2, \ldots, i_n)$. Говорят, что $x^\alpha$ – *невозрастающий,* если $i_1 \geq i_2 \geq \ldots \geq i_n$.

*Лемма 2.* Пусть $f \in R[x_1, \ldots, x_n]$ – симметрический многочлен, $f \neq 0$. Тогда высший член $f$ – невозрастающий.

*Доказательство.* Пусть $x^\alpha = x_1^{i_1} \cdot \ldots \cdot x_k^{i_k} x_{k+1}^{i_{k+1}} \cdot \ldots \cdot x_n^{i_n}$ – высший одночлен $f$, но существует $k: \quad i_k < i_{k+1}$. Рассмотрим транспозицию $\pi = (k, k+1)$. Так как $f = f^\pi$, то в $f$ входит одночлен $x_1^{i_1} \cdot \ldots \cdot x_k^{i_{k+1}} x_{k+1}^{i_k} \cdot \ldots \cdot x_n^{i_n}$, который выше, чем $x^\alpha$ – противоречие. □

*Пример.* Высший (одно)член $\sigma_k$ – это $x_1 x_2 \cdot \ldots \cdot x_k$.

*Лемма 3.* Каждый невозрастающий одночлен является высшим (одно)членом симметрического многочлена вида $\sigma_1^{k_1} \sigma_2^{k_2} \cdot \ldots \cdot \sigma_n^{k_n}$; такой симметрический многочлен определен однозначно. (То есть, пусть $x^\alpha$ – невозрастающий одночлен. Тогда $\exists!\ k_1, k_2, \ldots, k_n \in \mathbb{Z}_+$ такие, что $x^\alpha$ – высший (одно)член $\sigma_1^{k_1} \sigma_2^{k_2} \cdot \ldots \cdot \sigma_n^{k_n}$).

*Доказательство.* Лемма 1 $\Rightarrow$ высший член $\sigma_1^{k_1} \sigma_2^{k_2} \cdot \ldots \cdot \sigma_n^{k_n}$ равен $x_1^{k_1} (x_1 x_2)^{k_2} (x_1 x_2 x_3)^{k_3} \cdot \ldots \cdot (x_1 x_2 \cdot \ldots \cdot x_n)^{k_n} = x_1^{k_1+k_2+\ldots+k_n} x_2^{k_2+k_3+\ldots+k_n} \cdot \ldots \cdot x_{n-1}^{k_{n-1}+k_n} x_n^{k_n}$. С другой стороны, пусть $x^\alpha = x_1^{i_1} x_2^{i_2} \cdot \ldots \cdot x_n^{i_n}$, где $i_1 \geq i_2 \geq \ldots \geq i_n$. Тогда $x^\alpha$ – высший член $\sigma_1^{k_1} \sigma_2^{k_2} \cdot \ldots \cdot \sigma_n^{k_n} \Leftrightarrow$

$$\left\{\begin{array}{ccccccc} k_1+ & k_2+ & \ldots & +k_{n-1} & +k_n & = i_1 \\ & k_2+ & \ldots & +k_{n-1} & +k_n & = i_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ & & & k_{n-1} & +k_n & = i_{n-1} \\ & & & & k_n & = i_n \end{array}\right\} = \left\{\begin{array}{ccc} k_1 = & i_1 - i_2 & \in \mathbb{Z}_+ \\ k_2 = & i_2 - i_3 & \in \mathbb{Z}_+ \\ \ldots & \ldots & \ldots \\ k_{n-1} = & i_{n-1} - i_n & \in \mathbb{Z}_+ \\ k_n = & i_n & \in \mathbb{Z}_+. \end{array}\right.$$

□

*Лемма 4.* Для любого (фиксированного) одночлена $x^\alpha$ множество *невозрастающих* одночленов, которые ниже, чем $x^\alpha$, конечно.

*Доказательство.* Пусть $\alpha = (i_1, \ldots, i_n), \beta = (j_1, \ldots, j_n)$, $j_1 \geq \ldots \geq j_n$. Если $x^\alpha \succ x^\beta$, то $i_1 \geq j_1$. Таким образом, если $x^\alpha \succ x^\beta$, то $i_1 \geq j_1 \geq j_2 \geq \ldots \geq j_n$ $\Rightarrow \forall k$ есть лишь конечное число возможностей для $j_k$. □

*Доказательство основной теоремы: существование.* Укажем алгоритм. Пусть $f \in R[x_1, \ldots, x_n]$, $f$ – симметричный. Если $f = 0$, то нечего делать. Пусть $f \neq 0$, $ax^\alpha$ – высший член $f$, $a \neq 0$. Лемма 2 $\Rightarrow x^\alpha$ – невозрастающий. Лемма 3 $\Rightarrow x^\alpha$ – высший член некоторого симметрического многочлена $\sigma_1^{i_1} \sigma_2^{i_2} \cdot \ldots \cdot \sigma_n^{i_n}$. Рассмотрим $f_1 = f - a\sigma_1^{i_1} \sigma_2^{i_2} \cdot \ldots \cdot \sigma_n^{i_n}$. Тогда $f_1$ – симметрический. Если $f_1 = 0 \Rightarrow$ готово ($f = a\sigma_1^{i_1} \sigma_2^{i_2} \cdot \ldots \cdot \sigma_n^{i_n}$). В противном случае высший одночлен $f_1$ *ниже* , чем $x^\alpha$. Пусть $bx^\beta$ – высший член $f_1$. Повторяя предыдущее рассуждение, получаем симметрический $f_2 = f_1 - b\sigma_1^{j_1} \cdot \ldots \cdot \sigma_n^{j_n}$, причем высший одночлен $f_2$ ниже, чем

$x^\beta$. И так далее. Лемма 4 $\Rightarrow$ процесс остановится, то есть $\exists m:\ f_{m+1}=0$. Итого

$$\left.\begin{array}{rcl} f= & f_1+ & a\sigma_1^{i_1}\cdot\ldots\cdot\sigma_n^{i_n}\\ f_1= & f_2+ & b\sigma_1^{j_1}\cdot\ldots\cdot\sigma_n^{j_n}\\ f_2= & f_3+ & c\sigma_1^{k_1}\cdot\ldots\cdot\sigma_n^{k_n}\\ \ldots & \ldots & \ldots\\ f_{m-1}= & f_m+ & y\sigma_1^{s_1}\cdot\ldots\cdot\sigma_n^{s_n}\\ f_m= & & z\sigma_1^{t_1}\cdot\ldots\cdot\sigma_n^{t_n}\end{array}\right\}\underset{\sum}{\Rightarrow}$$

$$f=a\sigma_1^{i_1}\cdot\ldots\cdot\sigma_n^{i_n}+b\sigma_1^{j_1}\cdot\ldots\cdot\sigma_n^{j_n}+\ldots+z\sigma_1^{t_1}\cdot\ldots\cdot\sigma_n^{t_n}.$$

□

*Замечание.* Если $f$ – однородный, то в алгоритме выше все многочлены $f_1, f_2, \ldots$ – однородные той же степени.

*Пример.* ($n=3$) $f=x_1^3+x_2^3+x_3^3$, высший член $f$ равен $x_1^3=$ высший член $\sigma_1^3$. То есть $f_1=f-\sigma_1^3=x_1^3+x_2^3+x_3^3-(x_1+x_2+x_3)^3=-3(x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2)-6x_1x_2x_3$. Высший член$f_1$ равен $-3x_1^2x_2(=-3x_1(x_1x_2))=$ высший член $-3\sigma_1\sigma_2$. То есть $f_2=f_1+3\sigma_1\sigma_2=f_1+3(x_1+x_2+x_3)(x_1x_2+x_1x_3+x_2x_3)=f_1+3(x_1^2x_2+x_1x_2^2+x_1^2x_3+x_1x_3^2+x_2^2x_3+x_2x_3^2+3x_1x_2x_3)=3x_1x_2x_3=3\sigma_3$. Окончательно $f=\sigma_1^3-3\sigma_1\sigma_2+3\sigma_3$. (Громоздко...)

*Способ 2: неопределенные коэффициенты.* $f=x_1^3+x_2^3+x_3^3$. $f$ – однородный степени 3 (иначе – отдельно все однородные компоненты); высший (одно)член $f$ равен $x_1^3$. Перечислим все невозрастающие одночлены степени 3, которые ниже, чем $x_1^3$ (именно они могут быть высшими членами на следующих шагах): $x_1^3\succ x_1^2x_2\succ x_1x_2x_3$; это – высшие (одно)члены $\sigma_1^3,\sigma_1\sigma_2,\sigma_3$. То есть $f=\sigma_1^3+a\sigma_1\sigma_2+b\sigma_3$; $\quad a,b=?$ Подставим:

| $x_1$ | $x_2$ | $x_3$ | $\sigma_1$ | $\sigma_2$ | $\sigma_3$ | $f$ |
|---|---|---|---|---|---|---|
| 1 | 1 | 0 | 2 | 1 | 0 | $2=8+2a\Rightarrow a=-3$ |
| 1 | 1 | 1 | 3 | 3 | 1 | $3=27-27+b\Rightarrow b=3.$ |

*Доказательство основной теоремы: единственность.* Пусть $f=g(\sigma_1,\ldots,\sigma_n)-h(\sigma_1,\ldots,\sigma_n)$. Требуется доказать: $g=h$. Имеем $0=g(\sigma_1,\ldots,\sigma_n)-h(\sigma_1,\ldots,\sigma_n)=\sum_{i_1,\ldots,i_n\in\mathbb{Z}_+}a_{i_1,\ldots,i_n}\sigma_1^{i_1}\cdot\ldots\cdot\sigma_n^{i_n}$. Требуется доказать: $\forall i_1,\ldots,i_n: a_{i_1,\ldots,i_n}=0$. Лемма 3 $\Rightarrow$ все многочлены $\sigma_1^{i_1}\cdot\ldots\cdot\sigma_n^{i_n}$ имеют разные высшие члены. То есть самому высшему среди них (если они вообще есть) не с чем взаимно уничтожиться. □

2.18. **(Формальные) степенные ряды.** Пусть $R$ – кольцо. Определяем кольцо $R[[x]]$ формальных степенных рядов с коэффициентами из $R$. Именно, элемент $R[[x]]$ – это последовательность $(a_0,a_1,\ldots,a_n,\ldots)$, $a_i\in R$. Операции: $(a_0,a_1,\ldots,a_n,\ldots)+(b_0,b_1,\ldots,b_n,\ldots):=(a_0+b_0,a_1+b_1,\ldots,a_n+b_n,\ldots)$; $(a_0,a_1,\ldots,a_n,\ldots)\cdot(b_0,b_1,\ldots,b_n,\ldots):=(c_0,c_1,\ldots,c_n,\ldots)$, где $c_k=\sum_{i+j=k}a_ib_j=a_0b_k+a_1b_{k-1}+\ldots+a_kb_0$.

*Упражнение.* $R[[x]]$ – кольцо относительно этих операций.

По определению, $R[x]$ – подкольцо в $R[[x]]$.

Если $A = (a_0, a_1, \ldots, a_n, \ldots) \in R[[x]]$, то будем записывать $A(x) = \sum_{n=0}^{\infty} a_n x^n$ ("тонкость": сумма "формальная", – однако можно придать и "фактический" смысл (как предел)). В частности, $x = (0, 1, 0, \ldots, 0, \ldots)$ (как и для многочленов). Говорят еще, что $A(x)$ – это *"производящая функция"* последовательности $(a_0, a_1, \ldots, a_n, \ldots)$. Формулы сложения и умножения согласуются с "правилами действия" с такими суммами. Степень не определена: нет наибольшей! Скорее есть наименьшая...

*Предложение.* $R$ – целостно $\Rightarrow R[[x]]$ – целостно.

*Доказательство.* $A, B \in R[[x]], A \neq 0, B \neq 0$. $A = a_k x^k + a_{k+1}x^{k+1} + \ldots, a_k \neq 0$; $B = b_l x^l + b_{l+1}x^{l+1} + \ldots, b_l \neq 0 \Rightarrow AB = a_k b_l x^{k+l} +$ (члены степени $> k + l$), $a_k b_l \neq 0 \Rightarrow AB \neq 0$. $\square$

Каковы обратимые элементы в $R[[x]]$?

*Предложение.* Пусть $A \in R[[x]], A(x) = \sum_{n=0}^{\infty} a_n x^n$. Тогда $A \in R[[x]]^* \Leftrightarrow a_0 \in R^*$.

*Доказательство.* $\Rightarrow$: $B(x) = \sum_{n=0}^{\infty} b_n x^n$. $AB = 1 \Rightarrow a_0 b_0 = 1 \Rightarrow a_0 \in R^*$.

$\Leftarrow$: Пусть $a_0 \in R^*$.

$$a_0 b_0 = 1 \Rightarrow b_0 = a_0^{-1}$$

$$a_0 b_1 + a_1 b_0 = 0 \Rightarrow b_1 = -a_0^{-1}(a_1 b_0)$$

$$a_0 b_2 + a_1 b_1 + a_2 b_0 = 0 \Rightarrow b_2 = -a_0^{-1}(\ldots)$$

и так далее. $\square$

В частности, если $F$ – поле, то $A(x) = \sum_{n=0}^{\infty} a_n x^n \in F[[x]]^* \Leftrightarrow a_0 \neq 0$.

*Пример.* $\frac{1}{1-x} = \sum_{n=0}^{\infty} x^n = 1 + x + x^2 + \ldots + x^n + \ldots$. В самом деле $(1 - x) \cdot (1 + x + x^2 + \ldots) = (1 + x + x^2 + \ldots) - (x + x^2 + x^3 + \ldots) = 1$.

*Замечание.* ($F$ – поле) ??? Картинка

Что можно сказать о простых элементах в $R[[x]]$ (где $R$ – целостно)? Очевидно, $x \in R[[x]]$ – простой. Если $R = F$ – поле, то других и нет (с точностью до $\sim$). $A \in F[[x]], A(x) = a_k x^k + a_{k+1}x^{k+1} + \ldots$, $a_k \neq 0 \Rightarrow A(x) = x^k(\underbrace{a_k + a_{k+1}x + \ldots}_{\text{обратим}})$. В частности, видно, что $F[[x]]$ – факториально (и даже евклидово по тривиальной причине: для любых двух элементов один делится на другой!).

Если $R$ – кольцо (не поле), то ситуация сильно усложняется. Можно (не так просто) доказать, что если $R$ – евклидово, то $R[[x]]$ – факториально. Если $R$ – факториально, то $R[[x]]$ *не обязательно* факториально (примеры сложны).

Несколько примеров простых/составных:

*Задача.* Пусть $R$ – факториально, $A \in R[[x]], A(x) = \sum_{n=0}^{\infty} a_n x^n$.

1) Если $a_0 = p$ – простой, то $A$ – простой в $R[[x]]$.

2) Если $R$ – *евклидово* и $a_0 = bc$, где $b, c \in R, b, c \notin R^*, \text{НОД}(b, c) = 1$, то $A$ – составной в $R[[x]]$.

3) Если $a_0 = p^2$ (где $p$ – простой), $p \nmid a_1$, то $A$ – простой в $R[[x]]$.

*Задача.* Опишите поле частных $F((x))$ кольца $F[[x]]$.

Еще некоторые полезные "операции" над рядами:

*Композиция:* Пусть $A, B \in R[[x]], A(x) = \sum_{n=0}^{\infty} a_n x^n$, $B(x) = \sum_{n=1}^{\infty} b_n x^n$, то есть $b_0 = 0$.

$$A(B(x)) = \sum_{n=0}^{\infty} a_n B(x)^n = \sum_{n=0}^{\infty} a_n (b_1 x + b_2 x^2 + \ldots)^n = ?$$

Так как $B(x)^n = b_1^n x^n + (\text{члены степени} > n)$, то "вклад" в коэффициент при $x^n$ у $A(B(x))$ дают лишь $B(x)^k$ при $k = 0, 1, \ldots, n$. То есть формулы для коэффициентов $A(B(x))$ даются конечными суммами $\Rightarrow$ имеет смысл.

*Упражнение.* Напишите "явные" формулы для коэффициентов $A(B(x))$.

*Пример.* $\frac{1}{1-y} = \sum_{n=0}^{\infty} y^n$; $\quad y = -x \Rightarrow \frac{1}{1+x} = \sum_{n=0}^{\infty} (-x)^n = \sum_{n=0}^{\infty} (-1)^n x^n$. С другой стороны: $y = 1 - x \Rightarrow \sum_{n=0}^{\infty} (1-x)^n = ???$ Свободный член: $1+1+1+\ldots = \sum_{n=0}^{\infty} 1 = ???$ То есть $\frac{1}{1-(1-x)} = \frac{1}{x}$ не имеет смысла в $R[[x]]$ (что не удивительно ...).

*Замечание.* Если $c \in R$, то можно определить $R[[x-c]]$: элементы – это $\sum_{n=0}^{\infty} a_n (x-c)^n$. Конечно, $R[[x-c]] \cong R[[x]] \quad \forall c$. Для *многочленов* можно "переразложить" по степеням $x - c$. Для рядов это не получается (при $c \neq 0$). То есть разница между $R[[x-c]]$ для разных $c \in R$ в том, что кольцо многочленов вкладывается туда по-разному. И не только многочлены: скажем, $\frac{1}{x} \notin R[[x]]$ , но $\frac{1}{x} = \frac{1}{1-(1-x)} = \sum_{n=0}^{\infty} (-1)^n (x-1)^n \in R[[x-1]]$.

*Производная/интеграл.* Пусть $F$ – поле, $A \in F[[x]], A(x) = \sum_{n=0}^{\infty} a_n x^n$. Тогда $A'(x) := \sum_{n=0}^{\infty} n a_n x^{n-1} = a_1 + 2a_2 x + 3a_3 x^2 + \ldots$.

*Упражнение.* Проверьте: $(A+B)' = A' + B'$; $(A \cdot B)' = A'B + AB'$; если $A$ – обратим, то $\left(\frac{1}{A}\right)' = -\frac{A'}{A^2}$; $(A^n)' = nA^{n-1}A'$. Если $B$ без свободного члена, и $C(x) = A(B(x))$, то $C'(x) = A'(B(x)) \cdot B'(x)$.

$\int A(x)dx := c + \sum_{n=0}^{\infty} \frac{1}{n+1} a_n x^{n+1} = c + a_0 x + \frac{1}{2} a_1 x^2 + \ldots \leftarrow$ имеет смысл лишь в $\operatorname{char} F = 0$.

Ясно, что $\left(\int A(x)dx\right)' = A(x), \quad \int A'(x)dx = A(x) + c$.

Пусть снова $A \in F[[x]], A(x) = a_0 + a_1 x + a_2 x^2 + \ldots$. "Подставить" можно только $x = 0$. Далее:

$$A'(x) = a_1 + 2a_2 x + 3a_3 x^2 + \ldots \;\Rightarrow\; A'(0) = a_1;$$

$$A''(x) = 2a_2 + 3 \cdot 2 \cdot a_3 x + \ldots \;\Rightarrow\; A''(0) = 2a_2;$$

$$A'''(x) = 3 \cdot 2 \cdot 1 \cdot a_3 + \ldots \;\Rightarrow\; A'''(0) = 3! a_3$$

и так далее. Итак (упражнение) $A^{(n)}(0) = n! a_n$.

Если $\operatorname{char} F = 0$, то $a_n = \frac{A^{(n)}(0)}{n!}$, то есть получилась *формула Тейлора:* $A(x) = \sum_{n=0}^{\infty} \frac{A^{(n)}(0)}{n!} x^n$. Это важно, ибо помогает "назвать" некоторые важные и полезные ряды.

*Примеры* ($\operatorname{char} F = 0$).

1) $e^x := \sum_{n=0}^{\infty} \frac{1}{n!} x^n$. Это естественно, ибо если рассматривать вещественную функцию $F(x) = e^x$, то $F^{(n)}(0) = 1 \quad \forall n$.

2)

$$\sin x := \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n+1)!} x^{2n+1} = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \dots;$$

$$\cos x := \sum_{n=0}^{\infty} \frac{(-1)^n}{(2n)!} x^{2n} = 1 - \frac{x^2}{2!} + \frac{x^4}{4!} - \dots.$$

*Упражнение.* ($F = \mathbb{C}$) $e^{ix} = \cos x + i \sin x$

3)

$$\ln(1+x) := \sum_{n=1}^{\infty} \frac{(-1)^{n+1}}{n} x^n = x - \frac{x^2}{2} + \frac{x^3}{3} - \dots.$$

*Упражнение.* "Обоснуйте". 2 способа: 1) формула Тейлора; 2) $\frac{d}{dx} \ln(1+x) = \frac{1}{1+x} = \dots$

4) Бином: $(1+x)^m = \sum_{n=0}^{m} C_m^n x^n \quad (m \in \mathbb{Z}_+)$. Если $r \in F$ – любое, то $(1+x)^r := \sum_{n=0}^{\infty} C_r^n x^n$, где $C_r^n := \frac{r(r-1)\cdot\dots\cdot(r-n+1)}{n!}$.

*Упражнение.* "Обоснуйте" это определение, вычисляя производящие функции $(1+x)^r$ при $x = 0$.

2.18.1. *Применение к симметрическим многочленам.* Пусть $R$ – кольцо, $t$ – (дополнительная) переменная. Рассмотрим $\varphi = (1 - tx_1)(1 - tx_2) \cdot \dots \cdot (1 - tx_n)$. Тогда (вариант формул Виета) $\varphi = 1 - \sigma_1 t + \sigma_2 t^2 - \sigma_3 t^3 + \dots + (-1)^n \sigma_n t^n$, где $\sigma_k$ – элементарные симметрические многочлены от $x_1, \dots, x_n$. То есть $\varphi \in S[t]$, где $S$ – подкольцо симметрических многочленов в $R[x_1, \dots, x_n]$.

Пусть $h_k :=$ сумма *всех* одночленов степени $k$, то есть

$$h_k = \sum_{\substack{i_1,\dots,i_n \in \mathbb{Z}_+ \\ i_1+\dots+i_n = k}} x_1^{i_1} \cdot \dots \cdot x_n^{i_n},$$

$h_k$ – *полный* симметрический многочлен степени $k$. Например, $h_0 = 1, h_1 = \sigma_1, h_2 = \sum_{i=1}^{n} x_i^2 + \sum_{1 \le i < j \le n} x_i x_j, \dots$

**Теорема.** $h_k = h_{k-1}\sigma_1 - h_{k-2}\sigma_2 + \dots + (-1)^{k-1} h_0 \sigma_k, \ k \ge 1$.

*Доказательство.* Рассмотрим $\frac{1}{\varphi} \in S[[t]]$. Имеем

$$\frac{1}{\varphi} = \frac{1}{1 - tx_1} \cdot \frac{1}{1 - tx_2} \cdot \dots \cdot \frac{1}{1 - tx_n} =$$

$$= \sum_{i_1=0}^{\infty} x_1^{i_1} t^{i_1} \cdot \sum_{i_2=0}^{\infty} x_2^{i_2} t^{i_2} \cdot \ldots \cdot \sum_{i_n=0}^{\infty} x_n^{i_n} t^{i_n} = \sum_{k=0}^{\infty} h_k t_k.$$

С другой стороны, $\varphi = \sum_{k=0}^{\infty} (-1)^k \sigma_k t^k$, где $\sigma_0 = 1$, $\sigma_k = 0$ при $k > n$. Так как $\varphi \cdot \frac{1}{\varphi} = 1$, то при $k \geq 1$ : $\quad h_k\sigma_0 - h_{k-1}\sigma_1 + h_{k-2}\sigma_2 - \ldots + (-1)^k h_0 \sigma_k = 0$. □

Например, $h_2 = h_1\sigma_1 - h_0\sigma_2 = \sigma_1^2 - \sigma_2$, $h_3 = h_2\sigma_1 - h_1\sigma_2 + h_0\sigma_3 = (\sigma_1^2 - \sigma_2)\sigma_1 - \sigma_1\sigma_2 + \sigma_3 = \sigma_1^3 - 2\sigma_1\sigma_2 + \sigma_3$, и тому подобное.

*Следствие.* $\sigma_k = \sigma_{k-1}h_1 - \sigma_{k-2}h_2 + \ldots + (-1)^{k-1}\sigma_0 h_k, \quad k \geq 1.$

*Следствие.* Любой симметрический многочлен от $n$ переменных однозначно представим в виде многочлена от $h_1, h_2, \ldots, h_n$.

Пусть $p_k := x_1^k + x_2^k + \ldots + x_n^k$ – *степенная сумма* степени $k$.

**Теорема** (*формулы Ньютона.* ) $p_k = p_{k-1}\sigma_1 - p_{k-2}\sigma_2 + \ldots + (-1)^{k-2} p_1 \sigma_{k-1} + (-1)^{k-1} k\sigma_k,\ k \geq 1.$

*Доказательство.* $\sum_{k=1}^{\infty} p_k t^{k-1} = \sum_{k=0}^{\infty} p_{k+1} t^k = \sum_{k=0}^{\infty} \left(\sum_{i=1}^{n} x_i^{k+1}\right) t^k = \sum_{i=1}^{n} x_i \left(\sum_{k=0}^{\infty} x_i^k t^k\right) = \sum_{i=1}^{n} \frac{x_i}{1 - x_i t} = -\frac{\varphi'}{\varphi}$ (производная по $t$). С другой стороны, $\varphi' = \sum_{k=1}^{\infty} (-1)^k k \sigma_k t^{k-1}$.

Так как $\varphi' = \frac{\varphi'}{\varphi} \cdot \varphi$, то (приравниваем коэффициенты при $t^{k-1}$): $(-1)^k k\sigma_k = -(p_k\sigma_0 - p_{k-1}\sigma_1 + p_{k-2}\sigma_2 + \ldots + (-1)^{k-1} p_1 \sigma_{k-1})$. □

Например, $p_1 = \sigma_1, p_2 = p_1\sigma_1 - 2\sigma_2 = \sigma_1^2 - 2\sigma_2, p_3 = p_2\sigma_1 - p_1\sigma_2 + 3\sigma_3 = \sigma_1^3 - 3\sigma_1\sigma_2 + 3\sigma_3$, и тому подобное.

*Следствие.* Пусть $R = F$ – поле, char $F = 0$. Тогда

$$\sigma_k = \frac{1}{k}(\sigma_{k-1}p_1 - \sigma_{k-2}p_2 + \ldots + (-1)^{k-1}\sigma_0 p_k), \quad k \geq 1.$$

*Следствие.* Пусть $R = F$ – поле, char $F = 0$. Тогда любой симметрический многочлен от $n$ переменных однозначно представим в виде многочлена от $p_1, p_2, \ldots, p_n$.

*Упражнение.* Получите рекуррентную формулу, связывающую $p_k$ и $h_l$. (Указание: $\psi := \frac{1}{\varphi} \Rightarrow \frac{\psi'}{\psi} = -\frac{\varphi'}{\varphi}$).

*Задача.* ($F$ – поле, char $F = 0$). Получите "явную" (не рекуррентную) формулу, выражающую $\sigma_k$ и $h_k$ через степенные суммы.

## 3. Линейная алгебра

### 3.1. **Системы линейных уравнений.** $F$ – поле.

Система линейных уравнений (С.Л.У.) – это система уравнений вида

$$(*) \quad \begin{cases} a_{11}x_1 + & a_{12}x_2 + & \ldots & +a_{1n}x_n & = b_1 \\ a_{21}x_1 + & a_{22}x_2 + & \ldots & +a_{2n}x_n & = b_2 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ a_{m1}x_1 + & a_{m2}x_2 + & \ldots & +a_{mn}x_n & = b_m \end{cases}$$

Здесь $a_{ij} \in F, b_i \in F$. Решение $(*)$ – это $(x_1, \ldots, x_n) \in F^n$ такой , что все уравнения из $(*)$ обращаются в тождества.

Кратко $(*)$ : $\sum_{j=1}^{n} a_{ij}x_j = b_i, \quad i = 1, 2, \ldots, m$. Здесь $m$ – число уравнений, $n$ – число неизвестных (вообще говоря, $m \neq n$).

*Терминология.*

$(*)$ *совместна* $\Leftrightarrow$ существует решение.

$(*)$ *несовместна* $\Leftrightarrow$ не существует решения.

Совместная система *определенная* $\Leftrightarrow$ решение единственно.

Совместная система *неопределенная* $\Leftrightarrow$ решение не единственно.

?????

*Пример.* $ax = b$. Совместна $\Leftrightarrow a \neq 0$ или $a = b = 0$. (Несовместна $\Leftrightarrow a = 0$, но $b \neq 0$). Определенная $\Leftrightarrow a \neq 0$; неопределенная $\Leftrightarrow a = b = 0$.

$(*)$ *однородна* $\Leftrightarrow \forall i : \quad b_i = 0$.

$(*)$ *неоднородна* в противном случае.

Если $(*)$ : $\sum_{j=1}^{n} a_{ij}x_j = b_i, \quad i = 1, 2, \ldots, m,$ то С.Л.У. $\sum_{j=1}^{n} a_{ij}x_j = 0, \quad i = 1, 2, \ldots, m,$ – это так называемая *однородная система, ассоциированная с* $(*)$.

*Замечание.* Однородная система всегда совместна. Она определенная $\Leftrightarrow$ есть *лишь* нулевое решение.

Две С.Л.У. *эквивалентны* , если у них одинаковые множества решений.

Имея дело с С.Л.У., удобно использовать язык матриц.

*Матрица* (над $F$) – это прямоугольная таблица, заполненная элементами из $F$.

*Пример.* $\begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}$ – это $3 \times 4$-матрица (над, скажем, $F = \mathbb{Q}$).

*Терминология.* строки, столбцы; $m$ строк, $n$ столбцов $\Rightarrow m \times n$-матрица.

Запись: $A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix} \overset{\text{кратко}}{=} (a_{ij})$. $a_{ij}$ – *элемент* матрицы $A$ (точнее, (i,j)-элемент).

Вернемся к С.Л.У. *Матрица* системы $(*)$ – это

$$A = \begin{pmatrix} a_{11} & a_{12} & \ldots & a_{1n} \\ a_{21} & a_{22} & \ldots & a_{2n} \\ \ldots & \ldots & \ldots & \ldots \\ a_{m1} & a_{m2} & \ldots & a_{mn} \end{pmatrix}.$$

*Расширенная матрица* $(*)$ – это

$$\widetilde{A} = \begin{pmatrix} a_{11} & a_{12} & \dots & a_{1n} & b_1 \\ a_{21} & a_{22} & \dots & a_{2n} & b_2 \\ \dots & \dots & \dots & \dots & \dots \\ a_{m1} & a_{m2} & \dots & a_{mn} & b_m \end{pmatrix} = (A \mid B),$$

где $B = \begin{pmatrix} b_1 \\ b_2 \\ \vdots \\ b_m \end{pmatrix}$ – "столбец правых частей" $(*)$.

Ясно, что (коль скоро фиксирована нумерация неизвестных) задание $(*) \Leftrightarrow$ задание расширенной матрицы $\widetilde{A}$.

Как *решать* (то есть найти все решения) С.Л.У.? Обсудим так называемый *алгоритм Гаусса*.

*Элементарные преобразования* С.Л.У.:

1) перестановка уравнений.

2) умножение некоторого уравнения на $\lambda \in F, \lambda \neq 0$.

3) прибавление к некоторому уравнению другого, умноженного на $\lambda \in F$.

На языке (расширенных) матриц: те же преобразования со *строками* $\widetilde{A}$. При этом $\lambda(u_1, u_2, \dots, u_n) := (\lambda u_1, \lambda u_2, \dots, \lambda u_n)$; $(u_1, u_2, \dots, u_n) + (v_1, v_2, \dots, v_n) := (u_1 + v_1, u_2 + v_2, \dots, u_n + v_n)$.

*Лемма.* Если С.Л.У. $(**)$ получается из С.Л.У. $(*)$ элементарными преобразованиями, то $(*)$ и $(**)$ эквивалентны.

*Доказательство.* Очевидно, любое решение $(*)$ будет решением $(**)$. Наоборот тоже, ибо $(*)$ тоже получается из $(**)$ элементарными преобразованиями. Например, $u \rightsquigarrow \lambda u = v (\lambda \neq 0) \Rightarrow v \rightsquigarrow \frac{1}{\lambda} v = u$; $u \underset{(u' \rightsquigarrow u' = v')}{\rightsquigarrow} u + \lambda u' = v$ $\Rightarrow v \underset{(v' \rightsquigarrow v' = u')}{\rightsquigarrow} v - \lambda v' = u$. $\square$

Матрица называется *ступенчатой* , если она имеет следующий вид:

$$\begin{pmatrix} |\underline{a_{1,j_1}} & & & * & \\ & |\underline{a_{2,j_2}} & & & \\ & & |\underline{a_{3,j_3}} & & \\ & 0 & & \ddots & \\ & & & & |\underline{a_{r,j_r}} \end{pmatrix}$$

где $a_{i,j_i} \neq 0 \quad \forall i = 1, \dots, r$, $j_1 < j_2 < \dots < j_r$.

С.Л.У. – *ступенчатая* , если ее расширенная матрица – ступенчатая.

*Пример.* $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 0 & 4 \end{pmatrix}$ – ступенчатая; $\begin{pmatrix} 1 & 2 & 3 \\ 0 & 4 & 5 \\ 0 & 6 & 7 \end{pmatrix}$ – не ступенчатая.

Нулевую матрицу тоже удобно считать ступенчатой.

**Теорема.** Любую матрицу можно привести к ступенчатой элементарными преобразованиями строк матрицы.

*Доказательство:* Алгоритм: Пусть $A \neq 0$ (иначе тривиально). Выберем самый левый столбец содержащий ненулевой элемент ($j_1$ его номер). Переставляя строки добиваемся того, что $a_{1,j_1} \neq 0$. Тогда матрица примет вид

$$\begin{pmatrix} 0 & 0\dots & a_{1j_1} & \dots \\ 0 & 0\dots & a_{2j_1} & \dots \\ \dots & \dots & \dots & \dots \end{pmatrix}.$$

Далее, для всех $k \geq 2$ прибавим к $k$ой строке первую, умноженную на $-\frac{a_{kj_1}}{a_{1j_1}}$
Получим матрицу

$$\left(\begin{array}{cc|ccc} 0 & a_{1j_1} & * & \dots & * \\ 0 & 0 & & A_1 & \\ \dots & \dots & & & \end{array}\right)$$

Далее применяем те же рассуждения к матрице $A_1$ (индукция по числу строк).
*Следствие* Любая С.Л.У. эквивалентна ступенчатой.
*Пример.*

$$\begin{cases} x_1 + 2x_2 + x_3 = 2 \\ x_1 + 3x_2 + 2x_3 - x_4 = 4 \\ 2x_1 + x_2 - x_3 + 3x_4 = -2 \\ 2x_1 - 2x_3 + 3x_4 = 1 \end{cases} \quad \tilde{A} = \left(\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 2 \\ 1 & 3 & 2 & -1 & 4 \\ 2 & 1 & -1 & 3 & -2 \\ 2 & 0 & -2 & 3 & 1 \end{array}\right) \sim$$

$$\left(\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & -3 & -3 & 3 & -6 \\ 0 & -4 & -4 & 3 & -3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & 0 & 0 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

Как решить ступенчатую систему? У нас

$$\begin{cases} x_1 + 2x_2 + x_3 = 2 \\ x_2 + x_3 - x_4 = 2 \\ x_4 = -5 \end{cases}$$

То есть $x_4 = -5,\ x_2 = -3 - x_3,\ x_1 = 8 + x_3$. Придавая $x_3$ (любые) значения однозначно находим $x_1, x_2, x_4$. То есть исходная система неопределена.

Практически удобно совместить второй этап с первым:

$$\tilde{A} \sim \left(\begin{array}{cccc|c} 1 & 2 & 1 & 0 & 2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & -3 & -3 & 3 & -6 \\ 0 & -4 & -4 & 3 & -3 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & -1 & 2 & -2 \\ 0 & 1 & 1 & -1 & 2 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & -1 & 5 \end{array}\right) \sim \left(\begin{array}{cccc|c} 1 & 0 & -1 & 0 & 8 \\ 0 & 1 & 1 & 0 & -3 \\ 0 & 0 & 0 & 1 & -5 \\ 0 & 0 & 0 & 0 & 0 \end{array}\right)$$

То есть $x_1 = 8 + x_3,\ x_2 = -3 - x_3,\ x_4 = -5$.

Что в общем случае можно сказать о ступенчатой системе? Пусть $\tilde{A}(m \times (n+1))$ ступенчата. Тогда $A$ тоже ступенчата.

Пусть $r$ число ненулевых строк (то есть ступеней) в $A$, $\tilde{r}$ – число ступеней в $\tilde{A}$. Тогда $\tilde{r} = r$ или $\tilde{r} = r + 1$(почему?).

Случай 1: $\tilde{r} = r + 1 \Leftarrow$ система несовместна.

Случай 2: $\tilde{r} = r \leq n$. Пусть $j_1 < j_2 < ... < j_r$ – номера столбцов где "ступени".

Тогда можно выразить $x_{j_1}, x_{j_2}, ..., x_{j_r}$ через остальные $n - r$ переменных ("свободных")

Если остальных нет, то есть $r = n$ то система определена, если $r < n$, то неопределена, решение зависит от $n - r$ параметров.

*Замечание.* Оказывается, что $r$ не зависит от способа приведения к ступенчатому виду (далі буде).

Ещё пара полученых утверждений:

*Предложение.* Совместная С.Л.У. в которой число уравнений меньше числа неизвестных, является неопределенной.

*Следствие.* Однородная С.Л.У., в которой число уравнений меньше числа неизвестных, является неопределенной.

*Упражнение.* Пусть число переменных равно числу неизвестных. Тогда С.Л.У. определена $\Leftrightarrow$ соответсвующая однородная С.Л.У. определена.

## 3.2. **Линейные пространства.** (основной объект в линейной алгебре)

*Определение.* Линейное пространство над полем $F$ –это множество $V$ с заданной операцией сложения $V \times V \to V \quad ((v_1, v_2) \in V \times V \to v_1 + v_2 \in V)$ и отображением $F \times V \to V \quad ((\lambda, v) \in F \times V \to \lambda v \in V)$, причем:

(1) $\forall v_1, v_2 \in V: \quad v_1 + v_2 = v_2 + v_1$;

(2) $\forall v_1, v_2, v_3 \in V: \quad v_1 + (v_2 + v_3) = (v_1 + v_2) + v_3$;

(3) $\exists 0 \in V\ \forall v \in V: \quad v + 0 = v$;

(4) $\forall v \in V\ \exists -v \in V: \quad v + (-v) = 0$;

(5) $\forall \lambda_1, \lambda_2 \in F, \forall v \in V: \quad \lambda_1(\lambda_2 v) = (\lambda_1 \lambda_2)v$;

(6) $\forall \lambda_1, \lambda_2 \in F, \forall v \in V: \quad (\lambda_1 + \lambda_2)v = \lambda_1 v + \lambda_2 v$;

(7) $\forall \lambda \in F, \forall v_1, v_2 \in V: \quad \lambda(v_1 + v_2) = \lambda v_1 + \lambda v_2$;

(8) $\forall v \in V: \quad 1 \cdot v = v$.

*Терминология.* Линейное пространство = векторное пространство. Элементы $V$

– *векторы* , элементы $F$ – *скаляры* . То есть, есть сложение векторов и умножение вектора на скаляр.
*Упражнение.* 1) $0 \in V$ – единственен; 2) $\forall v \in V : -v$ – единственен; 3) $\forall v \in V : 0 \cdot v = 0$ (NB: "разные" нули!); 4) $\forall \lambda \in F : \lambda \cdot 0 = 0$; 5) $\lambda v = 0 \Rightarrow \lambda = 0$ или $v = 0$; 6) $\lambda v_1 = \lambda v_2, \lambda \neq 0 \Rightarrow v_1 = v_2$; 7) $\forall \lambda \in F, \forall v \in V : (-\lambda)v = \lambda(-v) = -(\lambda v)$.
Обычно поле $F$ фиксировано (и часто явно не указывается).
*Примеры линейных пространств.*
1) (Основной). $n \in \mathbb{N}; F^n := \{(x_1, \ldots, x_n) \mid x_i \in F\}$. Операции: $(x_1, \ldots, x_n) + (y_1, \ldots, y_n) := (x_1 + y_1, \ldots, x_n + y_n)$; $\lambda(x_1, \ldots, x_n) := (\lambda x_1, \ldots, \lambda x_n)$.
В частности, $F^1 = F$ (пропускаем скобки...), то есть $F$ – линейное пространство над собой.

NB: Часто удобнее записывать элементы $F^n$ в виде столбцов: $\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$.

Формально это другие пространства, однако...
2) Матрицы: $\mathrm{Mat}(m \times n, F)$, $\mathrm{Mat}(n, F) = \mathrm{Mat}(n \times n, F)$.
3) Последовательности с элементами из $F$ (то есть, по сути $F[[x]]$, умножение "забывается").
4) Конечные последовательности с элементами из $F$ (не фиксированной длины) (то есть, по сути $F[x]$, умножение "забывается").
5) $V$ – линейное пространство, $X$ – множество $\Rightarrow \mathrm{Fun}(X, V) = \{f : X \to V\}$ – линейное пространство. В частности, $\mathrm{Fun}(X, F)$ – линейное пространство.
6) $L$ – поле, $F \subset L$ – подполе $\Rightarrow L$ – линейное пространство над $F$.
7) О.
*Линейные отображения.* Пусть $V, W$ – линейные пространства над $F$.
*Определение.* Отображение $\varphi : V \to W$ *линейно* , если (1) $\forall v_1, v_2 \in V : \varphi(v_1 + v_2) = \varphi(v_1) + \varphi(v_2)$; (2) $\forall \lambda \in f, \forall v \in V : \varphi(\lambda v) = \lambda \varphi(v)$.
*Упражнение.* Если $\varphi$ линейно, то $\varphi(0) = 0$; $\varphi(\lambda_1 v_1 + \ldots + \lambda_n v_n) = \lambda_1 \varphi(v_1) + \ldots + \lambda_n \varphi(v_n)$.
*Пример.* $\varphi : F \to F, \varphi(x) = ax + b$ линеен $\Leftrightarrow b = 0$.
*Определение.* Отображение $\varphi : V \to W$ – *изоморфизм* , если $\varphi$ линейно и биективно. $V$ *изоморфно* $W$ ($V \cong W$), если существует изоморфизм $V \to W$.
*Примеры изоморфных линейных пространств.*
1) строки и столбцы;
2) $\mathrm{Mat}(m \times n, F) \cong F^{mn}$;
3) $|X| = n \Rightarrow \mathrm{Fun}(X, F) \cong F^n$ : если $X = \{x_1, \ldots, x_n\}$, то $f \to (f(x_1), \ldots, f(x_n))$ – изоморфизм.
*Операции над линейными отображениями:*
1. Пусть $\varphi_1, \varphi_2 : V \to W$– линейны. Определим $\varphi_1 + \varphi_2 : V \to W, (\varphi_1 + \varphi_2)(v) = \varphi_1(v) + \varphi_2(v)$. Тогда $\varphi_1 + \varphi_2$ – линеен: $(\varphi_1 + \varphi_2)(v_1 + v_2) = \varphi_1(v_1 + v_2) + \varphi_2(v_1 + v_2) =$

$\underline{\varphi_1(v_1)}+\underline{\varphi_1(v_2)}+\underline{\varphi_2(v_1)}+\underline{\underline{\varphi_2(v_2)}} = (\varphi_1+\varphi_2)(v_1)+(\varphi_1+\varphi_2)(v_2)$; $(\varphi_1+\varphi_2)(\lambda v) = \ldots$ – упражнение.

Пусть $\varphi : V \to W$ – линеен, $\lambda \in F$. Определим $\lambda\varphi : V \to W, (\lambda\varphi)(v) = \lambda\varphi(v)$.

*Упражнение.* $\lambda\varphi$ – линейно.

Обозначим через $\mathrm{Hom}(V, W)$ множество всех линейных отображений $V \to W$.

*Предложение.* $\mathrm{Hom}(V, W)$ – линейное пространство относительно введенных выше операций.

*Доказательство.* (Упражнение). Все же: например, $0 \in \mathrm{Hom}(V, W)$ – это тождественно нулевое отображение $V \to W$. □

2. Пусть $U \xrightarrow{\psi} V \xrightarrow{\varphi} W$ – линейные отображения. Тогда имеется композиция $\varphi \circ \psi : U \to W$. $\varphi \circ \psi$ линеен: $\varphi \circ \psi(u_1 + u_2) = \ldots$ и тому подобное. Композиция ассоциативна. Имеется $\mathrm{id} : V \to V$ – линейный, $\varphi \circ \mathrm{id} = \varphi, \mathrm{id} \circ \psi = \psi$.

*Упражнение.* $\lambda\varphi = (\lambda \cdot \mathrm{id}) \circ \varphi$ (NB: $\lambda \cdot \mathrm{id}$ – отображение умножения на $\lambda$).

*Упражнение.*

1. id – изоморфизм ($\Rightarrow V \cong V$).
2. $\varphi$ – изоморфизм $\Leftrightarrow \varphi^{-1}$ – изоморфизм ($\Rightarrow$ если $V \cong W$, то $W \cong V$).
3. $\varphi, \psi$ – изоморфизмы $\Leftrightarrow \varphi \circ \psi$ – изоморфизм ($\Rightarrow$ если $U \cong V$, $V \cong W$, то $U \cong W$).

*Лемма* (дистрибутивные законы для линейных отображений).

1). Если $U \overset{\psi_1}{\underset{\psi_2}{\rightrightarrows}} V \xrightarrow{\varphi} W$ – линейные, то $\varphi \circ (\psi_1 + \psi_2) = \varphi \circ \psi_1 + \varphi \circ \psi_2$.

2) Если $U \xrightarrow{\psi} V \overset{\varphi_1}{\underset{\varphi_2}{\rightrightarrows}} W$ – линейные, то $(\varphi_1 + \varphi_2) \circ \psi = \varphi_1 \circ \psi + \varphi_2 \circ \psi$.

*Доказательство.* Упражнение. □

*Замечание.* Рассмотрим $\mathrm{End}\ V := \mathrm{Hom}\ (V, V)$. В множестве $\mathrm{End}\ V$ имеются 1) структура линейного пространства (сложение и умножение на скаляр); 2) "умножение", то есть композиция. Умножение ассоциативно, есть единица (id), есть дистрибутивность. Однако (как правило) нет коммутативности (увидим...). То есть $\mathrm{End}\ V$ – вообще говоря, *некоммутативное* кольцо с единицей.

*Пример.* Строение $\mathrm{Hom}\ (F^n, F^m)$. Используем "столбцовую" запись. $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} \in F^n \Rightarrow$

$$x = x_1 \begin{pmatrix} 1 \\ 0 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_2 \begin{pmatrix} 0 \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + \ldots + x_n \begin{pmatrix} 0 \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} = \sum_{j=1}^{n} x_j e_j,$$

где

$$e_j = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j$$

– "орты". Пусть $\varphi \in \mathrm{Hom}\,(F^n, F^m)$. Тогда $\varphi(x) = \sum_{j=1}^n x_j \varphi(e_j)$, $\varphi(e_j) = ?$

Пусть $u_1, \ldots, u_m$ – "орты" в $F^m$. Запишем $\varphi(e_j) = \sum_{i=1}^m a_{ij} u_i = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{mj} \end{pmatrix}$ (это – определение $a_{ij}$ по $\varphi$). Тогда

$$\varphi(x) = \sum_{i=1}^m \left( \sum_{j=1}^n a_{ij} x_j \right) u_i = \begin{pmatrix} a_{11}x_1 + a_{12}x_2 + \ldots + a_{1n}x_n \\ a_{21}x_1 + a_{22}x_2 + \ldots + a_{2n}x_n \\ \ldots \quad \ldots \quad \ldots \\ a_{m1}x_1 + a_{m2}x_2 + \ldots + a_{mn}x_n \end{pmatrix} \qquad (*)$$

Рассмотрим $m \times n$-матрицу $A = (a_{ij})$. Итак, мы построили отображение $\mathcal{M} : \mathrm{Hom}\,(F^n, F^m) \to \mathrm{Mat}(m \times n, F), \varphi \in \mathrm{Hom}\,(F^n, F^m) \to A \in \mathrm{Mat}(m \times n, F)$.

*Предложение.* $\mathcal{M}$ – изоморфизм линейных пространств.

*Доказательство.* 1) Это биекция, ибо для любой матрицы $A$ можно рассмотреть отображение $\varphi : F^n \to F^m$, заданное $(*)$. Упражнение: $\varphi$ линейно.

2) Пусть $\varphi, \psi \in \mathrm{Hom}\,(F^n, F^m), \varphi \to A, \psi \to B$. $\varphi + \psi \to ?, \lambda\varphi \to ?$ Если $A = (a_{ij}), B = (b_{ij})$, то, по определению, $\varphi(e_j) = \sum_{i=1}^m a_{ij} u_i$, $\psi(e_j) = \sum_{i=1}^m b_{ij} u_i$, $\quad \forall i$. Тогда $(\varphi + \psi)(e_j) = \varphi(e_j) + \psi(e_j) = \sum_{i=1}^m (a_{ij} + b_{ij}) u_i$ то есть $\varphi + \psi \to A + B = (a_{ij} + b_{ij})$. Аналогично $\lambda\varphi \to \lambda A = (\lambda a_{ij})$. $\square$

То есть $\mathcal{M}$ согласовано с линейными операциями $\Rightarrow \mathcal{M}$ линейно.

Итак $\mathrm{Hom}\,(F^n, F^m) \simeq \mathrm{Mat}(m \times n, F)$.

Рассмотрим $F^n \overset{\psi}{\to} F^m \overset{\varphi}{\to} F^l$ – линейные. $\varphi \to A = (a_{ij}) \leftarrow l \times m$-матрица; $\psi \to B = (b_{jk}) \leftarrow m \times n$-матрица. Если $e_1, \ldots, e_n$ – "орты" $F^n$; $u_1, \ldots, u_m$ – "орты" $F^m$; $v_1, \ldots, v_l$ – "орты" $F^l$, то $\varphi(u_j) = \sum_{i=1}^l a_{ij} v_i; \psi(e_k) = \sum_{j=1}^m b_{jk} u_j$.

Рассмотрим $\varphi \circ \psi : \ F^n \to F^l$, $\varphi \circ \psi \to C = \leftarrow l \times n$-матрица. $C = ?$

По определению $(\varphi \circ \psi)(e_k) = \sum_{i=1}^l c_{ik} v_i$. С другой стороны $(\varphi \circ \psi)(e_k) = \varphi(\psi(e_k)) = \sum_{j=1}^m b_{jk} \varphi(u_j) = \sum_{i=1}^l \left( \sum_{j=1}^m a_{ij} b_{jk} \right) v_i$.

То есть,

$$c_{ik} = \sum_{j=1}^m a_{ij} b_{jk} \qquad (**)$$

Матрица $C$, чьи элементы определяются формулами $(**)$, называется произведением $A$ и $B$. Обозначение: $C = AB$.
Итак, если $\varphi \to A, \psi \to B$, то $\varphi \circ \psi \to AB$.
Из свойств операций над линейными отображениями теперь автоматически следует, что (для матриц "подходящего" размера):
1) $(AB)C = A(BC)$;
2) $(A_1 + A_2)B = A_1B + A_2B$;
3) $A(B_1 + B_2) = AB_1 + AB_2$.
Отметим, что $\mathrm{id} \to E := \begin{pmatrix} 1 & 0 & 0 & \dots & 0 \\ 0 & 1 & 0 & \dots & 0 \\ \dots & & \dots & & \dots \\ 0 & 0 & \dots & 0 & 1 \end{pmatrix}$, то есть (для матриц подходящего размера) $AE = A; EB = B$.
*Замечание.* Если даже $AB$ и $BA$ оба имеют смысл, то, как правило, $AB \neq BA$ :
1) $A$ – $m \times n$, $B$ – $n \times m \Rightarrow AB$ – $m \times m$, $BA$ – $n \times n$; несравнимы при $m \neq n$.
2) $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \Rightarrow AB \neq BA$.
*Замечание.* $\mathrm{Mat}(n, F)$ – кольцо с 1 (некоммутативное при $n \geq 2$, $\mathrm{Mat}(1, F) \simeq F$). $\mathrm{End}(F^n) \simeq \mathrm{Mat}(n, F)$ (не только как линейные пространства, но и как кольца).
Внимание: осторожно с некоммутативным умножением! Если $AB \neq BA$, то, скажем, $(AB)^2 \neq A^2B^2$, $(A + B)^2 \neq A^2 + 2AB + B^2$, и тому подобное.
Удобства матричного формализма:
1) $A$ – матрица $m \times n$, $x$ – матрица $n \times 1$ (то есть столбец) $\Rightarrow Ax$ – матрица $m \times 1$ (то же столбец). Если $\varphi \in \mathrm{Hom}(F^n, F^m),\ \varphi \to A$, то $\varphi(x) = Ax$.
2) С.Л.У. с расширеной матрицей $\tilde{A} = (A|b)$ записывается в виде $Ax = b$, где $x$ – столбец $x_i$.
Например:
*Предложение.* Все решения (совместной) С.Л.У. получаются так: к любому фиксированому решению добавляются решения соответствующей однородной С.Л.У.
*Доказательство:* $Ax_0 = b$. 1) $Ax = b, y = x - x_0 \Rightarrow Ay = 0$. 2) обратно $Ay = 0, x = x_0 + y \Rightarrow Ax = b$.□

3.3. **Определители.** Введение: рассмотрим

$$\begin{cases} a_{11}x_1 + a_{12}x_2 = b_1 \\ a21x_1 + a_{22}x_2 = b_2 \end{cases}$$

Умножим первое уравнение на $a_{22}$ второе на $a_{12}$ вычтем второе из первого. Получим, если $\Delta = a_{11}a_{22} - a_{12}a_{21} \neq 0$, то решение единственно.

Можно обобщить на случай любых квадратных матриц. Для этого:

3.3.1. *Дополнительные сведения о перестановках.* Пусть $\pi \in S_n$. Пара $i, j$, где $1 \leq i < j \leq n$ образует инверсию относительно $\pi$ если $\pi(i) > \pi(j)$. $Inv(\pi)$ –число инверсий $\pi$.
*Пример.*

$$\pi = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 1 & 3 & 2 & 6 & 5 \end{pmatrix} \in S_6.$$ "Правило ниточек"$Inv(\pi) = 5$.

$\pi$ – чётна (нечётна) если $Inv(\pi)$ – чётно (нечётно).
Знак $\pi$ – это $sgn\ \pi := (-1)^{Inv(\pi)}$. $\pi$ чётна $\Leftrightarrow sgn\ \pi = 1$, нечётна $\Leftrightarrow sgn\ \pi = -1$.
Очевидно, что $id$ – чётна.
*Предложение.* Любая транспозиция нечётна.
*Доказательство:* "ниточки".
**Теорема.** Если $\pi_1, \pi_2 \in S_n$, то $sgn(\pi_1\pi_2) = sgn(\pi_1)sgn(\pi_2)$
*Основная лемма.* $sgn\pi = \prod_{1\leq i<j\leq n} \frac{\pi(i)-\pi(j)}{i-j}$.
*Доказательство:* Правая часть – это

$$\frac{\prod_{1\leq i<j\leq n}(\pi(i) - \pi(j))}{\prod_{1\leq k<l\leq n}(l-k)}$$

Пусть $i < j,\ k = \pi(i), l = \pi(j)$. Тогда в числителе имеется множитель $l-k$. Если $k < l$, то инверсии нет, в знаменателе – множитель $l - k$, он же в числителе, отношение равно $+1$. Аналогично, при $k > l$ отношение равно $-1$.
*Вывод теоремы из основной леммы*

$$sgn(\pi_1\pi_2) = \prod_{1\leq i<j\leq n} \frac{\pi_1(\pi_2(j)) - \pi_1(\pi_2(i))}{j-i} = \prod_{1\leq i<j\leq n} \frac{\pi_1(\pi_2(j)) - \pi_1(\pi_2(i))}{\pi_2(j) - \pi(i)} \times$$

$$\times \prod_{1\leq i<j\leq n} \frac{\pi_2(j) - \pi_2(i)}{j-i} = (1) \times (2).\ (2) = sgn(\pi_2)$$

В (1) положим $k = \pi_2(i)$, $l = \pi_2(j)$, при $\pi_2(i) < \pi_2(j)$, в противном случае $k = \pi_2(j)$, $l = \pi_2(i)$. Тогда $(1) = \prod_{1\leq k<l\leq n} \frac{\pi_1(k)-\pi_1(l)}{k-l} = sgn(\pi_1)$.□
*Следствие.* Если $\pi \in S_n$,то $sgn(\pi^{-1}) = sgn(\pi)$.
*Следствие.* Если перестановка $\pi$ раскладывается в проиведение $m$ транспозиций, то $sgn\ \pi = (-1)^m$
К определителям. Пусть $A \in \mathrm{Mat}\ (n, F); A = (a_{ij})$. *Определитель* матрицы $A$ – это элемент $\det A \in F$, задаваемый формулой

$$\det A := \sum_{\pi\in S_n} \mathrm{sign}\pi \cdot a_{1,\pi(1)}a_{2,\pi(2)} \cdot \ldots \cdot a_{n,\pi(n)}$$

(Альтернативные обозначения: $|A|$, $\begin{vmatrix} a_{11} & a_{12} & \dots & a_{1n} \\ a_{21} & a_{22} & \dots & a_{2n} \\ \dots & \dots & \dots & \dots \\ a_{n1} & a_{n2} & \dots & a_{nn} \end{vmatrix}$).

*Примеры.* 1) $n = 1 : A = (a), \det A = a$.

2. $n = 2 : A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix}$; $S_2 = \{\mathrm{id}, \pi\}$, где $\pi = (1, 2)$, то есть $\det A = a_{11}a_{22} - a_{12}a_{21}$.

3. $n = 3 : A = \begin{pmatrix} a_{11} & a_{12} & a_{13} \\ a_{21} & a_{22} & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$;

$S_3 = \{ \quad \mathrm{id}; \quad \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}; \quad \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}; \quad (1,2); \quad (1,3); \quad (2,3)\}.$

sign: $\quad +1 \qquad +1 \qquad +1 \qquad -1 \qquad -1 \qquad -1$

То есть, $\det A = a_{11}a_{22}a_{33} + a_{12}a_{23}a_{31} + a_{13}a_{21}a_{32} - a_{12}a_{21}a_{33} - a_{13}a_{22}a_{31} - a_{11}a_{23}a_{32}$.
Правило: $+ : - :$

4. $n = 4 \Rightarrow |S_4| = 24$ – много... и дальше – больше... Нужны косвенные методы вычислений.

3.4. **Свойства определителей.** Пусть $A = (a_{ij}) \in \mathrm{Mat}(n, F)$. Матрица, *транспонированная* к $A$ – это матрица $A^T = (b_{ij})$, где $b_{ij} = a_{ji}$.
(NB: можно и для прямоугольных: $A \in \mathrm{Mat}(m \times n, F) \Rightarrow A^T \in \mathrm{Mat}(n \times m, F)$).
*Свойство 1.* $\det A^T = \det A$.
*Доказательство.* $\det A^T = \sum_{\pi \in S_n} \mathrm{sign}\pi \cdot a_{\pi(1),1}a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}$. Заметим, что $\pi \to \pi^{-1}$ – биекция $S_n$ на себя. Кроме того, если $\rho = \pi^{-1}$ и $i = \pi(j)$, то $j = \rho(i)$, то есть $a_{\pi(j),j} = a_{i,\rho(i)}$ Вспомним, что $\mathrm{sign}(\rho) = \mathrm{sign}(\pi^{-1}) = \mathrm{sign}(\pi)$. Поэтому $\det A^T = \sum_{\rho \in S_n} \mathrm{sign}\rho \cdot a_{1,\rho(1)}a_{2,\rho(2)} \cdot \ldots \cdot a_{n,\rho(n)} = \det A$. □
*Замечание.* Свойство 1 означает, что $\det A^T = \sum_{\pi \in S_n} \mathrm{sign}\pi \cdot a_{\pi(1),1}a_{\pi(2),2} \cdot \ldots \cdot a_{\pi(n),n}$. Если $A \in \mathrm{Mat}(n, F)$, то $A$ – строка, составленная из столбцов. То есть $A = (a_1, a_2, \ldots, a_n)$, где $a_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix}$. Мы изучим свойства $\det A$ как функции столбцов $A$. Аналогично, $A$ – столбец, составленный из строк. Так как $\det A^T = \det A$, то все свойства, относящиеся к столбцам, выполняются и для строк.
*Свойство 2.*

$$\det(a_1, \ldots, a_{j-1}, \lambda a_j, a_{j+1}, \ldots, a_n) = \lambda \det(a_1, \ldots, a_{j-1}, a_j, a_{j+1}, \ldots, a_n).$$

*Доказательство.* $\det(\ldots,\lambda a_j,\ldots)=\sum_{\pi\in S_n}\mathrm{sign}\pi\cdot a_{\pi(1),1}\cdot\ldots\cdot\lambda a_{\pi(j),j}\cdot\ldots\cdot a_{\pi(n),n}=\lambda\sum_{\pi\in S_n}\ldots=\lambda\det(\ldots,a_j,\ldots)$. □
*Свойство 3.* $\det(a_1,\ldots,a_{j-1},0,a_{j+1},\ldots,a_n)=0$.
*Доказательство.* Упражнение. □
*Свойство 4.* $\det(a_1,\ldots,a_{j-1},a_j^{'}+a_j^{''},a_{j+1},\ldots,a_n)=$
$\det(a_1,\ldots,a_{j-1},a_j^{'},a_{j+1},\ldots,a_n)+\det(a_1,\ldots,a_{j-1},a_j^{''},a_{j+1},\ldots,a_n)$.
*Доказательство.* $\det(\ldots,a_j^{'}+a_j^{''},\ldots)=\sum_{\pi\in S_n}\mathrm{sign}\pi\cdot a_{\pi(1),1}\cdot\ldots\cdot(a_{\pi(j),j}^{'}+a_{\pi(j),j}^{''})\cdot\ldots\cdot a_{\pi(n),n}=\sum_{\pi\in S_n}\ldots a_{\pi(j),j}^{'}\ldots+\sum_{\pi\in S_n}\ldots a_{\pi(j),j}^{''}\ldots=\det(\ldots a_j^{'}\ldots)+\det(\ldots a_j^{''}\ldots)$. □
*Замечание.* 1) Свойства 2)–4) означают, что det *линейная* функция (относительно *каждого* из столбцов матрицы). То есть det – "полилинейная" функция.
2) Выполнены аналогичные свойства $2)^{'},3)^{'},4)^{'}$ (упражнение: сформулировать) для строк. То есть det – полилинейная функция также и строк.
*Свойство 5.* Если $A=(a_1,\ldots,a_n)$ и $\exists i\neq j:\ a_i=a_j$, то $\det A=0$ (то есть если $A$ имеет два одинаковых столбца, то $\det A=0$).
*Доказательство.* Дано: $\forall k\ a_{ki}=a_{kj}$. Заметим следующее: для $\forall$ (фиксированного) $\rho\in S_n$ отображение $\pi\to\pi\circ\rho$ – биекция $S_n\to S_n$ (обратное отображение $\pi\to\pi\circ\rho^{-1}$). Возьмем $\rho=(i,j)$ ($\rho^{-1}=\rho$). Тогда $S_n$ разбивается на пары $\{\pi,\pi\circ\rho\}$. Найдем их "вклад" в $\det A$.

$$\mathrm{sign}(\pi\circ\rho)\cdot a_{(\pi\circ\rho)(1),1}\cdot\ldots\cdot a_{(\pi\circ\rho)(i),i}\cdot\ldots\cdot a_{(\pi\circ\rho)(j),j}\cdot\ldots\cdot a_{(\pi\circ\rho)(n),n}=$$

$$\mathrm{sign}(\pi)\cdot\mathrm{sign}(\rho)\cdot a_{\pi(1),1}\cdot\ldots\cdot a_{\pi(j),i}\cdot\ldots\cdot a_{\pi(i),j}\cdot\ldots\cdot a_{\pi(n),n}=$$

$$-\mathrm{sign}(\pi)\cdot a_{\pi(1),1}\cdot\ldots\cdot a_{\pi(i),i}\cdot\ldots\cdot a_{\pi(j),j}\cdot\ldots\cdot a_{\pi(n),n}$$

$\leftarrow$ взаимно уничтожается со слагаемым $\mathrm{sign}(\pi)\cdot a_{\pi(1),1}\cdot\ldots\cdot a_{\pi(i),i}\cdot\ldots\cdot a_{\pi(j),i}\cdot\ldots\cdot a_{\pi(n),n}$. То есть $\det A=0$. Схематично: ??? отличаются знаком! □
*Замечание (свойство 5').* если $A$ имеет две равные строки, то $\det A=0$
*Свойство 6.* $\det(...,a_i,..,a_j,...)=-\det(...,a_j,...,a_i,...)$.(то есть при транспозиции двух столбцов определитель меняет знак).
*Доказательство:* $0=\det(...,a_i+a_j,...,a_i+a_j,...)=\det(...,a_i,...,a_i,...)+\det(...,a_i,...,a_j,...)+\det(...,a_j,...,a_i,...)+\det(...,a_j,...,a_j,...)=$
$\det(...,a_j,...,a_i,...)+\det(...,a_i,...,a_j,...)$
*Замечание (свойство 6').* То же для строк...
*Свойство 7* $\forall\pi\in S_n:\det(a_{\pi(1)},...,a_{\pi(n)})=sgn\ \pi\det(a_1,..,a_n)$.
*Доказательство.* Запишем $\pi=\rho_1...\rho_m$, где $\rho_i$ – траспозиции. Итеируя свойство 6 получаем свойство 7.
*Замечание (свойство 7').* То же для строк...
Свойство 7 означает, что det – кососимметрическая функция столбцов.
*Свойство 8* $\det(...,a_i+\lambda a_j,...,a_j,...)=\det(...,a_i,..,a_j,...)$.

*Доказательство.* $\det(..., a_i+\lambda a_j, ..., a_j, ...) = \det(..., a_i, .., a_j, ...)+\lambda \det(..., a_j, .., a_j, ...) = \det(..., a_i, .., a_j, ...)$
*Замечание.* Свойтсва 2,7,8 контролируют поведение определителя при элементарных преобразованиях столбцов матрицы.

## 3.5. **Алгоритм Гаусса высичления определителя.** *Предложение.*

$$\begin{vmatrix} a_{11} & ... & a_{1,n-1} & a_{1n} \\ . & . & . & . \\ . & . & . & . \\ . & . & . & . \\ 0 & ... & 0 & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & ... & a_{1,n-1} \\ . & . & . \\ . & . & . \\ . & . & . \\ a_{n-1,1} & ... & a_{n-1,n-1} \end{vmatrix} a_{nn}$$

*Доказательство.*

$$\text{левая часть} = \sum_{\pi \in S_n} sgn\,\pi\, a_{1,\pi(1)}...a_{nn} = a_{nn} \sum_{\pi \in S_{n-1}} sgn\,\pi\, a_{1,\pi(1)}...a_{n-1.\pi(n-1)} = \text{правая часть}$$

Здесь была использована биекция $\{\pi \in S_n | \pi(n) = n\} \to S_{n-1}$
$\tilde{\pi} = \pi(\{1, .., n-1\})$. При этом $Inv(\tilde{\pi}) = Inv(\pi)$.
*Замечание.* Аналогичное верно и для столбцов.
*Следствие.*

$$\begin{vmatrix} a_{11} & & * \\ & a_{22} & \\ 0 & & a_{nn} \end{vmatrix} = \begin{vmatrix} a_{11} & & 0 \\ & a_{22} & \\ * & & a_{nn} \end{vmatrix} = a_{11}...a_{nn}$$

*Доказательство* Индукция по $n$.
Теперь сам алгоритм. Любую матрицу элементарными преобразованиями можно привести к ступенчатому виду. При этом определитель, вообще говоря, меняется, но контролируемо. Определитель треугольной матрицы можно вычислить.
*Пример.*

$$\begin{vmatrix} 1 & 2 & 3 \\ 4 & 5 & 6 \\ 7 & 8 & 9 \end{vmatrix} = \begin{vmatrix} 1 & 2 & 3 \\ 0 & -3 & -6 \\ 0 & -6 & -12 \end{vmatrix} = (-3)(-6) \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 1 & 2 \end{vmatrix} = (-3)(-6) \begin{vmatrix} 1 & 2 & 3 \\ 0 & 1 & 2 \\ 0 & 0 & 0 \end{vmatrix} = 0$$

*Геометрический смысл определителя:* $F = \mathbb{R}$.
$\det(a_1, a_2)$ = ориентированная площадь параллелограмма, натянутого на $a_1, a_2$. (Картинка...) Аналогично $\det(a_1, a_2, \ldots, a_n)\ldots$ *Разложение определителя по столбцу/строке*
Пусть $A \in \mathrm{Mat}(n, F), A = (a_{ij})$. Выкинем $i$-ю строку, $j$-й столбец, возьмем

определитель:

$$M_{ij} := \begin{vmatrix} a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} \\ \dots & & \dots & & & \dots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \dots & & \dots & & & \dots \\ a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} \end{vmatrix}$$

$M_{ij}$ – *миноры* матрицы $A$ (порядка $n-1$). Положим $A_{ij} = (-1)^{i+j} M_{ij}$ – алгебраическое дополнение к элементу $a_{ij}$ матрицы $A$. Правило знаков:

$$\begin{array}{cccccc} + & - & + & - & \dots \\ - & + & - & + & \dots \\ + & - & + & - & \dots \\ - & + & - & + & \dots \\ \dots & & \dots & & \dots \end{array}$$

**Теорема** (разложение определителя по $j$-му столбцу).

$$\det A = \sum_{i=1}^{n} a_{ij} A_{ij} = a_{1j} A_{1j} + a_{2j} A_{2j} + \ldots + a_{nj} A_{nj}.$$

*Доказательство.* $A = (a_1, \dots, a_n)$, где $a_j = \begin{pmatrix} a_{1j} \\ a_{2j} \\ \vdots \\ a_{nj} \end{pmatrix} = \sum_{i=1}^{n} a_{ij} e_i$, $e_i = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow i$ .

Линейность det по $j$-му столбцу $\Rightarrow$

$$\det A = \sum_{i=1}^{n} a_{ij} \begin{vmatrix} a_{11} & \dots & a_{1,j-1} & 0 & a_{1,j+1} & \dots & a_{1n} \\ \dots & & & \dots & & & \dots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & 0 & a_{i-1,j+1} & \dots & a_{i-1,n} \\ a_{i,1} & \dots & a_{i,j-1} & 1 & a_{i,j+1} & \dots & a_{i,n} \\ a_{i+1,1} & \dots & a_{i+1,j-1} & 0 & a_{i+1,j+1} & \dots & a_{i+1,n} \\ \dots & & & \dots & & & \dots \\ a_{n1} & \dots & a_{n,j-1} & 0 & a_{n,j+1} & \dots & a_{nn} \end{vmatrix}.$$

Переставим $j$-й столбец с каждым из последующих (которых $n-j$ штук).

$$\det A = \sum_{i=1}^{n} a_{ij}(-1)^{n-j} \begin{vmatrix} a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} & 0 \\ \dots & & & \dots & & & \dots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} & 0 \\ a_{i,1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{i,n} & 1 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} & 0 \\ \dots & & & \dots & & & \dots \\ a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} & 0 \end{vmatrix} =$$

(то же для $i-$ й строки) =

$$= \sum_{i=1}^{n} a_{ij}(-1)^{n-j+n-i} \begin{vmatrix} a_{11} & \dots & a_{1,j-1} & a_{1,j+1} & \dots & a_{1n} & 0 \\ \dots & & & \dots & & & \dots \\ a_{i-1,1} & \dots & a_{i-1,j-1} & a_{i-1,j+1} & \dots & a_{i-1,n} & 0 \\ a_{i+1,1} & \dots & a_{i+1,j-1} & a_{i+1,j+1} & \dots & a_{i+1,n} & 0 \\ \dots & & & \dots & & & \dots \\ a_{n1} & \dots & a_{n,j-1} & a_{n,j+1} & \dots & a_{nn} & 0 \\ a_{i,1} & \dots & a_{i,j-1} & a_{i,j+1} & \dots & a_{i,n} & 1 \end{vmatrix} =$$

$$= \sum_{i=1}^{n} a_{ij}(-1)^{i+j} M_{ij} = \sum_{i=1}^{n} a_{ij} A_{ij}.$$

□

*Следствие* (разложение определителя по $i$-й строке).

$$\det A = \sum_{j=1}^{n} a_{ij} A_{ij} = a_{i1}A_{i1} + a_{i2}A_{i2} + \ldots + a_{in}A_{in}.$$

*Замечание.* При $j \neq k$ имеем $\sum_{i=1}^{n} a_{ij}A_{ik} = 0$ (*разложение по "чужому" столбцу* ). Действительно, $0 = \det(\ldots, \underset{\uparrow}{a_j}, \ldots, \underset{\uparrow}{a_j}, \ldots) =$ (разложение по $j$-му столбцу) = $\sum_{i=1}^{n} a_{ij}A_{ik}$. Аналогично при $i \neq k$ имеем $\sum_{j=1}^{n} a_{ij}A_{kj} = 0$ (*разложение по "чужой" строке* ).

*Общее замечание.* Определение и все свойства определителей, указанные выше, выполняются для матриц с элементами в *некоммутативном* кольце (с 1).

*Определитель Вандермонда*

$$W(x_1, x_2, \ldots, x_n) = \begin{vmatrix} 1 & 1 & 1 & \dots & 1 & 1 \\ x_1 & x_2 & x_3 & \dots & x_{n-1} & x_n \\ x_1^2 & x_2^2 & x_3^2 & \dots & x_{n-1}^2 & x_n^2 \\ \dots & & & \dots & & \dots \\ x_1^{n-2} & x_2^{n-2} & x_3^{n-2} & \dots & x_{n-1}^{n-2} & x_n^{n-2} \\ x_1^{n-1} & x_2^{n-1} & x_3^{n-1} & \dots & x_{n-1}^{n-1} & x_n^{n-1} \end{vmatrix}$$

Это – определитель порядка $n$. Мы можем смотреть на $W$ как на многочлен от $x_1, \ldots, x_n$ (с коэффициентами в $\mathbb{Z}$). (А можем придать $x_i$ значения в некотором поле или кольце ...).

**Теорема.**

$$W(x_1, x_2, \ldots, x_n) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

*Доказательство.* Индукция по $n$. База $n = 1$: $W(x_1) = 1$; $n = 2$: $W(x_1, x_2) = \begin{vmatrix} 1 & 1 \\ x_1 & x_2 \end{vmatrix} = x_2 - x_1$. Переход $n-1 \rightsquigarrow n$. Рассмотрим $W$ как многочлен от $x_n$ (с коэффициентами, скажем, в поле частных $\mathbb{Q}(x_1, \ldots, x_{n-1})$ кольца $\mathbb{Z}[x_1, \ldots, x_{n-1}]$). Разложим по последнему столбцу: $W(x_1, \ldots, x_{n-1}, x_n) = W(x_1, \ldots, x_{n-1}) x_n^{n-1} +$ (члены степени $< n-1$ относительно $x_n$). Видим, что $W(x_1, \ldots, x_{n-1}, x_n) = 0$ при $x_n = x_1$, $x_n = x_2, \ldots, x_n = x_{n-1}$. То есть

$$W(x_1, \ldots, x_{n-1}, x_n) = W(x_1, \ldots, x_{n-1}) \prod_{i=1}^{n-1} (x_n - x_i) =$$

$$= \prod_{1 \le i < j \le n-1} (x_j - x_i) \prod_{i=1}^{n-1} (x_n - x_i) = \prod_{1 \le i < j \le n} (x_j - x_i).$$

□

*Определитель Якоби*

$$d_n := \begin{vmatrix} a & b & 0 & \ldots & 0 & 0 & 0 \\ c & a & b & \ldots & 0 & 0 & 0 \\ 0 & c & a & \ldots & 0 & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & a & b & 0 \\ 0 & 0 & 0 & \ldots & c & a & b \\ 0 & 0 & 0 & \ldots & 0 & c & a \end{vmatrix} \text{ (определитель порядка } n\text{, трехдиагональный)}$$

*Предложение.* $d_n = a d_{n-1} - bc d_{n-2}$

*Доказательство.*

$$d_n = a d_{n-1} - b \begin{vmatrix} a & b & 0 & \ldots & 0 & 0 \\ c & a & b & \ldots & 0 & 0 \\ 0 & c & a & \ldots & 0 & 0 \\ \ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\ 0 & 0 & 0 & \ldots & a & b \\ 0 & 0 & 0 & \ldots & 0 & c \end{vmatrix} = a d_{n-1} - bc d_{n-2} \text{ (разложение по } n'\text{ому столбцу)}$$

Отметим, что $d_1 = a$, $d_2 = a^2 - bc$; если $d_0 = 1$ то все ок.

Далее: например, производящая функция...

*Единственность определителя*
Точнее: аксиоматическое определение det.
Пусть $f : Mat(n,F) \to F$; $A = (a_1, ..., a_n) \Rightarrow f(A) = f(a_1, ..., a_n)$ функция столбцов $A$.
$f$ – полилинейна, если $f$ линейна по каждому столбцу.
$f$ – кососимметрична, если из $a_i = a_j, i \neq j$ следует, что $f(A) = 0$.
*Пример.* 1) det. 2) $c\det$, $c \in F$.
*Упражнение.* Пусть $f$ полилинейно.
1) Если $f$ кососимметрично, то $\forall \pi \in S_n :\ f(a_{\pi(1),...,a_{\pi(n)}}) = sgn\ \pi\ f(a_1, ..., a_n)$.
2) Если $charF \neq 2$, то и обратно.
**Теорема (единствеинность определителя).**
Пусть $f : Mat(n,F) \to F$ – полилинейна, кососимметрична. Тогда $f(A) = f(E)\det(A)$.
*Доказательство.*
$A = (a_1, ..., a_n)$, $a_j = \sum_{i=1}^{n} a_{ij}e_i$, $e_i$ – орты. $f(A) = \sum_{1 \leq i_1,...,i_n \leq n} a_{i_1,1}...a_{i_n,n}f(e_{i_1}, ..., e_{i_n})$
$= \sum_{\pi \in S_n} a_{\pi(1)}...a_{\pi(n)}sgn(\pi)f(E) = \det(A)f(E)$. □
Вот применения:
**Теорема (определитель блочно-диагональной матрицы).**
Пусть $A$ – матрица $k \times k$, $B$ – матрица $k \times l$, $C$ – матрица $l \times l$. Тогда

$$\det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix} = \det(A)\det(C).$$

*Доказательство.*

Зафиксируем $B$ и $C$ и рассмотрим $f : Mat(n,F) \to F, f(A) = \det \begin{pmatrix} A & B \\ 0 & C \end{pmatrix}$

Тогда $f$ полилинейно и кососимметрично, то есть $f(A) = f(E)\det(A) = \det(C)\det(A)$.
($f(E) = \det(C)$ из разложения левой части по первым $k$ столбцам)
*Следствие.* Пусть $A_1, ..., A_m$ – квадратные матрицы. тогда

$$\det \begin{pmatrix} A_1 & & & * \\ & A_2 & & \\ & & ... & \\ 0 & & & A_m \end{pmatrix} = \det(A_1)...\det(A_m)$$

*Упражнение.*

$$\det \begin{pmatrix} A & 0 \\ B & C \end{pmatrix} =?\ \det \begin{pmatrix} A & B \\ C & 0 \end{pmatrix} =?$$

**Теорема** (об определителе произведения матриц). Пусть $A, B \in \mathrm{Mat}(n,F)$. Тогда $\det AB = \det A \det B$.
*Доказательство.* Если $B = (b_1, b_2, \ldots, b_n)$, где $b_j$ – столбцы, то $AB = (Ab_1, Ab_2, \ldots, Ab_n)$.
Теперь зафиксируем $A$ и рассмотрим $f : \mathrm{Mat}(n,F) \to F, f(B) := \det AB =$

$\det(Ab_1, Ab_2, \ldots, Ab_n)$. Тогда $f$ полилинеен и кососимметричен по столбцам $B$. В самом деле:
1) $f(\ldots, \lambda b_j, \ldots) = \det(\ldots, A(\lambda b_j), \ldots) = \det(\ldots, \lambda A b_j, \ldots) = \lambda \det(\ldots, Ab_j, \ldots) = \lambda f(\ldots, b_j, \ldots)$.
$f(\ldots, b_j^{'} + b_j^{''}, \ldots) = \ldots$.
2) Если $\exists i \neq j : b_i = b_j$, то $Ab_i = Ab_j \Rightarrow f(b) = \det AB = 0$. То есть $f(B) = f(E) \det B$, но $f(E) = \det AE = \det A$. □
*Замечание.* В частности, $\det AB = \det BA$.
*Обратная матрица* Пусть $A \in \mathrm{Mat}(n, F)$. *$A$ обратима*, если $\exists B \in \mathrm{Mat}(n, F) : AB = BA = E$ (тогда $B$ – *обратная* к $A$, $B = A^{-1}$).
*Лемма.* Если $AB_1 = B_2 A = E$, то $B_1 = B_2$ (и $A$ обратима).
*Доказательство.* $B_1 = (B_2 A)B_1 = B_2(AB_1) = B_2$. □
*Следствие.* Обратная матрица к данной единственна.
*Упражнение.* 1) $E$ обратима; 2) $A$ обратима $\Rightarrow A^{-1}$ обратима; 3) $A, B$ обратимы $\Rightarrow AB$ обратима (и $(AB)^{-1} = B^{-1}A^{-1}$).
*Замечание.* Все вышесказанное дословно выполняется в любом кольце $R$ с 1 (*не обязательно коммутативном* ). У нас $R = \mathrm{Mat}(n, F)$.
Связь обратимости матриц и обратимости линейных отображений:
*Предложение.* Пусть $\varphi \in \mathrm{End}F^n (= \mathrm{Hom}(F^n, F^n)), \varphi \to A \in \mathrm{Mat}(n, F)$. Тогда $\varphi$ обратимо $\Leftrightarrow$ $A$ обратима.
*Доказательство.* $\varphi$ обратимо $\Leftrightarrow \exists \psi \in \mathrm{End}F^n : \varphi \circ \psi = \psi \circ \varphi = \mathrm{id}$. Тогда $\psi \to B \in \mathrm{Mat}(n, F); \varphi \circ \psi \to AB; \psi \circ \varphi \to BA; \mathrm{id} \to E$. То есть $\varphi$ обратимо $\Leftrightarrow \exists B \in \mathrm{Mat}(n, F) : AB = BA = E \Leftrightarrow A$ обратима. □
Когда $A$ обратима, как вычислить $A^{-1}$?
Пусть $A \in \mathrm{Mat}(n, F)$, $A = \begin{pmatrix} a_{11} & a_{12} & \ldots \\ a_{21} & a_{22} & \ldots \\ \ldots & \ldots & \ldots \end{pmatrix}$. Рассмотрим

$$\widehat{A} := \begin{pmatrix} A_{11} & A_{21} & \ldots & A_{n1} \\ A_{12} & A_{22} & \ldots & A_{n2} \\ \ldots & \ldots & \ldots & \ldots \\ A_{1n} & A_{2n} & \ldots & A_{nn} \end{pmatrix}$$

($\widehat{A}$ – матрица, *присоединенная* к $A$) – матрица из алгебраических дополнений $A_{ij}$, но *транспонированная* .
*Лемма.* $A\widehat{A} = \widehat{A}A = \det AE$.
*Доказательство.* $A\widehat{A} = (c_{ik})$, где $c_{ik} = \sum_{j=1}^{n} a_{ij}A_{kj} = \begin{cases} \det A & i = k \\ 0 & i \neq k \end{cases}$. $\widehat{A}A$ – упражнение. □
**Теорема.** Пусть $A \in \mathrm{Mat}(n, F)$. Тогда $A$ обратима $\Leftrightarrow \det A \neq 0$, при этом $A^{-1} = \frac{1}{\det A}\widehat{A}$.

*Доказательство.* $\Leftarrow$: $\det A \neq 0 \Rightarrow$ (лемма) $A \cdot \left(\frac{1}{\det A}\widehat{A}\right) = \left(\frac{1}{\det A}\widehat{A}\right) \cdot A = E$.
$\Rightarrow$: $A$ обратима $\Rightarrow \det A \cdot \det(A^{-1}) = 1 \Rightarrow \det A \neq 0$. $\square$
*Замечание.* $\det A^{-1} = \frac{1}{\det A}$.
Матрицы с $\det A \neq 0$ обычно называют *невырожденными* . То есть невырожденность $\Leftrightarrow$ обратимость.
*Предложение.* Пусть $A \in \mathrm{Mat}(n, F)$ такова, что $\exists B \in \mathrm{Mat}(n, F) : AB = E$. Тогда $A$ обратима и $A^{-1} = B$. (Смысл: ослабление условия обратимости).
*Доказательство.* $AB = E \Rightarrow \det A \cdot \det B = 1 \Rightarrow \det A \neq 0 \Rightarrow A$ – обратима $\Rightarrow$ $\exists B' : \begin{cases} B'A = E \\ AB = E \end{cases} \Rightarrow B' = B = A^{-1}$. $\square$
*Замечание.* Можно заменить $AB = E$ на $BA = E$ (тот же вывод ...).
Применим к С.Л.У. Рассмотрим

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots \\ a_{n1}x_1 + \ldots + a_{nn}x_n = b_n \end{cases} \quad (*),$$

где число уравнений = число неизвестных! Напомним: $A = \begin{pmatrix} a_{11} & \ldots & a_{1n} \\ \ldots & \ldots & \ldots \\ a_{n1} & \ldots & a_{nn} \end{pmatrix}$ – *матрица* $(*)$, $b = \begin{pmatrix} b_1 \\ \vdots \\ b_n \end{pmatrix}$; $\widetilde{A} = (A|b)$ – *расширенная* матрица $(*)$.

**Теорема.** $(*)$ определена (то есть решение $\exists!$) $\Leftrightarrow \det A \neq 0$.
(*Замечание.* То есть определенность $(*)$ не зависит от столбца в правой части).
*Доказательство.* $\Leftarrow$: $(*) \Leftrightarrow Ax = b$, где $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. Если $\det A \neq 0$, то $\exists A^{-1}$.
То есть если $Ax = b$, то $x = A^{-1}b$. И обратно: $A\left(A^{-1}b\right) = b$.
$\Rightarrow$: Элементарными преобразованиями приводим $\tilde{A}$ к ступенчатому виду: $\tilde{A} = (A|b) \to (A'|b') = \tilde{A}'$ – ступенчата; $A'$ – тем более ступенчата. Пусть $r$ – число ступенек $A'$, $\tilde{r}$ – число ступенек $\tilde{A}'$. Было: $(*)$ определена $\Leftrightarrow r = \tilde{r} = n$.

То есть, $A' = \begin{pmatrix} \lambda_1 & & & * \\ & \lambda_2 & & \\ & & \ldots & \\ 0 & & & \lambda_n \end{pmatrix}$ где $\forall i : \ \lambda_i \neq 0$. Тогда $\det A' = \lambda_1 \ldots \lambda_n \neq 0$.

С другой строны, $\det A'$ отличается от $\det A$ на ненулевой множитель (почему?), то есть $\det A \neq 0$.
*Замечание.* Можно доказать и "$\Leftarrow$" в стиле "$\Rightarrow$" (*Упражнение:* сделайте).

Напишем матрицу системы (*) в виде $A = (a_1, ..., a_n)$ю

**Теорема (формула Крамера).** Пусть $\det A \neq 0$. Тогда единственное решение

$$(*) \text{ даётся формулой } x_j = \frac{\det(a_1, ..., a_{j-1}, b, a_{j+1}, .., a_n)}{\det A} \text{ (словами...)}$$

*Доказательство:* Если $x$ – решение (*), то $x = A^{-1}b = \frac{1}{\det A}\hat{A}b$

$\hat{A}b = \begin{pmatrix} A_{11}b_1 + A_{21}b_2 + ... + A_{n1}b_n \\ ..... \\ A_{1n}b_1 + A_{2n}b_2 + ... + A_{nn}b_n \end{pmatrix}$ То есть, $x_j = \frac{1}{\det A}\sum_{i=1}^{n} A_{ij}b_i$. С другой стороны, $\det(a_1, ..., a_{j-1}, b, a_{j+1}, .., a_n) = \sum_{i=1}^{n} b_i A_{ij}$ $\square$.

Другой способ выисления $A^{-1}$: алгоритм Гаусса (это обычно удобнее)

Пусть $\det A \neq 0$. Ищем $X \in Mat(n, F)$ такую, что $AX = E$. Пишем $X = (x_1, ..., x_n)$, где $x_j$ – столбцы $X$. Тогда $Ax = (Ax_1, ..., Ax_n)$. То есть $Ax = E \Leftrightarrow \forall j: \ Ax_j = e_j$, где $e_j$ – орты (то есть решить $n$ систем с одинаковой матрицей). Гаусс: $(A|e_j) \to (E|x_j)$. Удобнее решать их все одновременно $(A|E) \to (E|A^{-1})$.

*Пример.* $A = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, $\det A = -2$.

Способ 1: $\hat{A} = \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \Leftarrow A^{-1} = \begin{pmatrix} -2 & 1 \\ \frac{3}{2} & -\frac{1}{2} \end{pmatrix}$

Способ 2: $\left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 3 & 4 & 0 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 2 & 1 & 0 \\ 0 & -2 & -3 & 1 \end{array}\right) \sim \left(\begin{array}{cc|cc} 1 & 0 & -2 & 1 \\ 0 & 1 & \frac{3}{2} & -\frac{1}{2} \end{array}\right)$

3.6. **Результант и дискриминант.** (приложения определителей к многочленам)

Пусть $f, g$ многочлены от $x$, $\deg f = n, \deg g = m$; $f = a_n x^n + a_{n-1}x^{n-1} + ... + a_0 = a_n(x - x_1) \cdot ... \cdot (x - x_n)$; $g = b_m x^m + b_{m-1}x^{m-1} + ... + b_0 = b_m(x - y_1) \cdot ... \cdot (x - y_m)$.

Напомним, что (формулы Виета) $a_{n-k} = a_n(-1)^k \sigma_k(x_1, ..., x_n)$; $b_{m-l} = b_m(-1)^l \sigma_l(y_1, ..., y$

Два возможных подхода:

1) $F$ – поле, $x_i, y_j \in F$, $a_n, b_m \in F$, то есть $f, g \in F[x]$.

2) $x_i, y_j$ (а также старшие коэффициенты $a_n, b_m$ и, конечно, $x$) – независимые переменные. То есть $f \in \mathbb{Z}[x_1, ..., x_n, a_n][x]$ и тому подобное.

*Определение. Результант* $f$ и $g$ – это $R(f, g) := a_n^m b_m^n \prod_{i,j}(x_i - y_j)$.

По определению, $R(f, g) = 0 \Leftrightarrow f, g$ имеют общий корень.

*Предложение* (элементарные свойства результанта).

1) $R(g, f) = (-1)^{mn} R(f, g)$.

2) $R(g, f) = a_n^m \prod_{i=1}^{n} g(x_i) = (-1)^{mn} b_m^n \prod_{j=1}^{m} f(y_j)$.

3) $R(f, g_1 g_2) = R(f, g_1) R(f, g_2)$.

*Доказательство.* 1) $\prod_{i,j}(y_j - x_i) = (-1)^{mn}\prod_{i,j}(x_i - y_j)$.
2) $g(x_i) = b_m\prod_{j=1}^{m}(x_i - y_j) \Rightarrow \dots$
3) Упражнение. $\square$

*Замечание.* По определению, $R(f,g)$ симметричен отдельно по $x_i$ и отдельно по $y_j$. То есть $R(f,g)$ выражается через $\sigma_k(x_1,\dots,x_n)$ и $\sigma_l(y_1,\dots,y_m)$, то есть через коэффициенты $f$ и $g$. Мы получим явную формулу:

**Теорема.**

$$R(f,g) = \begin{vmatrix} a_n & a_{n-1} & a_{n-2} & \dots & \dots & a_1 & a_0 & 0 & 0 & \dots & 0 & 0 \\ 0 & a_n & a_{n-1} & \dots & \dots & a_2 & a_1 & a_0 & 0 & \dots & 0 & 0 \\ 0 & 0 & a_n & a_{n-1} & \dots & a_3 & a_2 & a_1 & a_0 & 0 & \dots & 0 \\ \dots & & \dots & & \dots & & \dots & & \dots & & \dots & \dots \\ 0 & 0 & 0 & \dots & \dots & 0 & 0 & a_n & a_{n-1} & \dots & a_1 & a_0 \\ b_m & b_{m-1} & \dots & b_1 & b_0 & 0 & 0 & 0 & \dots & 0 & 0 & 0 \\ 0 & b_m & \dots & b_2 & b_1 & b_0 & 0 & 0 & \dots & 0 & 0 & 0 \\ \dots & & \dots & & \dots & & \dots & & \dots & & \dots & \dots \\ 0 & 0 & \dots & 0 & 0 & 0 & b_m & b_{m-1} & \dots & \dots & b_1 & b_0 \end{vmatrix}.$$

(матрица имеет размеры $(m+n)\times(m+n)$; строк, содержащих $a_i$, $m$ штук, строк, содержащих $b_j$, $n$ штук). Матрица, чей определитель выписан, – это так называемая *матрица Сильвестра* многочленов $f$ и $g$.

*Доказательство.* Сначала упражнение (модифицированный Вандермонд):

$$\begin{vmatrix} x_1^{n-1} & x_2^{n-1} & \dots & x_n^{n-1} \\ x_1^{n-2} & x_2^{n-2} & \dots & x_n^{n-2} \\ \dots & \dots & \dots & \dots \\ x_1 & x_2 & \dots & x_n \\ 1 & 1 & \dots & 1 \end{vmatrix} = \prod_{i<j}(x_i - x_j).$$

Рассмотрим

$$\Delta := \begin{vmatrix} y_1^{n+m-1} & \dots & y_m^{n+m-1} & x_1^{n+m-1} & \dots & x_n^{n+m-1} \\ \dots & \dots & \dots & \dots & \dots & \dots \\ y_1^2 & \dots & y_m^2 & x_1^2 & \dots & x_n^2 \\ y_1 & \dots & y_m & x_1 & \dots & x_n \\ 1 & \dots & 1 & 1 & \dots & 1 \end{vmatrix} =$$

$$= \prod_{1\le i<j\le m}(y_i - y_j)\prod_{i,j}(y_i - x_j)\prod_{1\le i<j\le n}(x_i - x_j),$$

то есть

$$a_n^m b_m^v \Delta = \prod_{1\le i<j\le m}(y_i - y_j)\prod_{1\le i<j\le n}(x_i - x_j)R(g,f). \qquad (*)$$

С другой стороны, пусть $S$ – определитель матрицы Сильвестра. Вычислим $S\Delta = \det$ произведения соответствующих матриц, то есть

$$S\Delta = \begin{vmatrix} y_1^{m-1}f(y_1) & y_2^{m-1}f(y_2) & \dots & y_m^{m-1}f(y_m) & 0 & 0 & \dots & 0 \\ \dots & \dots & \dots & \dots & 0 & 0 & \dots & 0 \\ y_1f(y_1) & y_2f(y_2) & \dots & y_mf(y_m) & 0 & 0 & \dots & 0 \\ f(y_1) & f(y_2) & \dots & f(y_m) & 0 & 0 & \dots & 0 \\ 0 & 0 & \dots & 0 & x_1^{n-1}g(x_1) & x_2^{n-1}g(x_2) & \dots & x_n^{n-1}g(x_n) \\ 0 & 0 & \dots & 0 & \dots & \dots & \dots & \dots \\ 0 & 0 & \dots & 0 & x_1g(x_1) & x_2g(x_2) & \dots & x_ng(x_n) \\ 0 & 0 & \dots & 0 & g(x_1) & g(x_2) & \dots & g(x_n) \end{vmatrix} =$$

(NB: (строка $m$) $\times$ (столбец 1) $= a_0 + a_1y_1 + \ldots + a_ny_1^n = f(y_1)$; $f(x_i) = 0$; (строка $m-1$) $\times$ (столбец 1) $= a_0y_1 + a_1y_1^2 + \ldots + a_ny_1^{n+1} = y_1f(y_1)$; $g(x_j) = 0$; и тому подобное).

$$= f(y_1)\cdot\ldots\cdot f(y_m)\begin{vmatrix} y_1^{m-1} & \dots & y_m^{m-1} \\ \dots & \dots & \dots \\ y_1 & \dots & y_m \\ 1 & \dots & 1 \end{vmatrix}\cdot g(x_1)\cdot\ldots\cdot g(x_n)\cdot\begin{vmatrix} x_1^{n-1} & \dots & x_n^{n-1} \\ \dots & \dots & \dots \\ x_1 & \dots & x_n \\ 1 & \dots & 1 \end{vmatrix} =$$

$$= \prod_{i=1}^{m} f(y_i)\cdot\prod_{i<j}(y_i - y_j)\cdot\prod_{i=1}^{n} g(x_i)\cdot\prod_{i<j}(x_i - x_j),$$

то есть

$$a_n^m b_m^n S\Delta = \prod_{i<j}(y_i - y_j)\cdot\prod_{i<j}(x_i - x_j)\cdot R(g,f)\cdot R(f,g). \qquad (**)$$

$(*)$ и $(**) \Rightarrow S = R(f,g)$. NB: Здесь $x_1,\ldots,x_n,y_1,\ldots,y_m$ – переменные. $\square$

*Замечание* Что если $f, g \in F[x]$ не разлагаются на множители степени 1 над $F$? Два способа выхода: 1) расширение основного поля (не обсуждали, но...) 2) можно определить результант $R(f,g)$ как det матрицы Сильвестра. Так и сделаем.

*Предложение.* $R(f,g) = 0 \Leftrightarrow f, g$ имеют нетривиальный общий множитель, то есть degНОД$(f,g) > 0$.

*Доказательство (не использующее расширения основного поля)* Пусть $n = \deg f$, $m = \deg g$.

1) degНОД$(f,g) > 0 \Leftrightarrow\ \exists u, v \in F[x],\ uv \neq 0,\ \deg u < m, \deg v < n : fu = gv$

В самом деле: $\Rightarrow$: если $f = vh,\ g = uh$ где $\deg h > 0$, то $fu = gv$.

$\Leftarrow$: если $fu = gv$, то, так как $f \not| v$, то $f$ и $g$ не взаимно просты.

NB: остаётся верным, если $n = \deg f, m \geq \deg g$ или наоборот, то есть $a_n \neq 0$ или $b_m \neq 0$.

2) Пусть $f = a_nx^n + ... + a_0,\ g = b_mx^n + ... + b_0$. Запишем $u = u_{m-1}x^{m-1} +$

$... + u_0,\ v = v_{n-1}x^{n-1} + ... + v_0$. Уравнение $fu = gv$ – это однородная С.Л.У. относительно неизвестных $u_{m-1}, ..., u_0, v_{n-1}, ..., v_0$ (всего $m+n$). Уравнений тоже $m+n$. условие существования нетривиального решения: определитель матрицы равен 0. Он сводиться к определителю Сильвестра.
Для простоты рассмотрим $n = 3,\ m = 2$ (в общем случае точно так же).
$(a_3x^3 + a_2x^2 + a_1x + a_0)(u_1x + u_0) = (b_2x^2 + b_1x + b_0)(v_2x^2 + v_1x + v_0)$
Пишем матрицу системы:

$$\begin{pmatrix} a_3 & 0 & -b_2 & 0 & 0 \\ a_2 & a_3 & -b_1 & -b_2 & 0 \\ a_1 & a_2 & -b_0 & -b_1 & -b_2 \\ a_0 & a_1 & 0 & -b_0 & -b_1 \\ 0 & a_0 & 0 & 0 & -b_0 \end{pmatrix}$$

Её определитель – $\pm\det$ матрицы Сильвестра (вынос знаков, транспонирование).
*Дискриминант* Пусть $\deg f = n,\ f = a_nx^n + ... + a_0 = a_n(x - x_1)...(x - x_n)$
Напомним, что $Discr(f) := a_n^{2n-2}\Pi_{i<j}(x_i - x_j)^2$.
То есть $Discr(f) = 0 \Leftrightarrow f$ имеет кратные корни.
Кроме того, $Discr(f)$ – многочлен от коэффициентов $f$.
*Упражнение.* $Discr(fg) = Discr(f)Discr(g)R(f, g)^2$
*Предложение.* Пусть $charF \not| n$. Тогда $R(f, f') = (-1)^{\frac{n(n-1)}{2}}a_nDiscr(f)$.
*Доказательство* При сделаных предположениях $degf' = (n-1)$. То есть $R(f, f') = a_n^{n-1}\Pi_{i=1}^n f'(x_i)$. Заметим, что $f' = a_n\sum_{j=1}^n \frac{f}{x-x_j} = a_n\sum_{j=1}^n f_j,\ f'(x_i) = a_nf_i(x_i) = a_n\Pi_{j:j\neq i}(x_i - x_j)$. То есть $R(f, f') = a_n^{2n-1}\Pi_{i\neq j}(x_i - x_j) = a_n(-1)^{n(n-1)/2}Discr(f)\square$.
*Замечание* Результат верен в любой характеристике, если интерпретировать $R(f, f')$ как det матрицы Сильвестра порядка $n + (n - 1)$ (то есть "притвориться", что $\deg f' = n - 1$).
*Пример.*

$$f = ax^2 + bx + c,\ f' = 2ax + b,\ R(f, f') = \begin{vmatrix} a & b & c \\ 2a & b & 0 \\ 0 & 2a & b \end{vmatrix} = a(-b^2 + 4ac) \Rightarrow$$

$$Discr(f) = -\frac{1}{a}R(f, f') = b^2 - 4ac.$$

*Упражнение.*

$$Discr(f) = a_n^{2n-2}\begin{vmatrix} p_0 & p_1 & ... & p_n - 1 \\ p_1 & p_2 & ... & p_n \\ ... & ... & ... & ... \\ p_{n-1} & p_n & ... & p_{2n-2} \end{vmatrix}$$

(Указание: $Discr(f) = a_n^{2n-2}W^2$, где $W$ – определитель Вандермонда. выпишите его как det произведения матрицы Вандермонда на её транспонированую).
*Пример* $f = a_2x^2 + a_1x + a_0,\ g = b_2x^2 + b_1x + b_0 \Rightarrow R(f,g) =$?(Упражнение). Если, скажем, $b_2 = 0$ (но $a_2 \neq 0$), то детерминант будет равен

$$a_2 \begin{vmatrix} a_2 & a_1 & a_0 \\ b_1 & b_0 & 0 \\ 0 & b_1 & b_0 \end{vmatrix}$$

С другой стороны $R(f,g)$ (уже как от многочленов степеней 2 и 1) равен

$$\begin{vmatrix} a_2 & a_1 & a_0 \\ b_1 & b_0 & 0 \\ 0 & b_1 & b_0 \end{vmatrix}$$

– отличается на множитель $a_2 \neq 0$.

3.7. **Линейная независимость и полнота.** Пусть $V$ – линейное пространство над $F$.
(Конечная) *система векторов* в $V$ – это семейство $v_1, \ldots, v_n \in V$; $n$ – число векторов системы. (Точнее: отображение $\{1, \ldots, n\} \to V, k \to v_k$).
Внимание: не путать с подмножеством: 1) важен порядок; 2) возможны повторения.
*Пример.* 1) $v_1 = (1,0), v_2 = (1,1)$.
2) $v_1 = (1,1), v_2 = (1,0)$.
3) $v_1 = (1,0), v_2 = (1,1), v_3 = (1,0)$.
Это три *различные* системы в $F^2$.
Мы будем систематически рассматривать лишь *конечные* системы.
Говорят, что $v \in V$ представим в виде *линейной комбинации* системы векторов $v_1, \ldots, v_n$, если $\exists\ \alpha_1, \ldots, \alpha_n \in F : v = \alpha_1v_1 + \ldots + \alpha_nv_n$.
Линейная комбинация *нетривиальна* , если $\exists i : \alpha_i \neq 0$; в противном случае *тривиальна.* Итак, тривиальная линейная комбинация представляет 0.
*Определение.* Система $v_1, \ldots, v_n \in V$ *линейно зависима*, если 0 представим в виде *нетривиальной* линейной комбинации $v_1, \ldots, v_n$ (то есть $\exists\ \alpha_1, \ldots, \alpha_n \in F : \sum \alpha_iv_i = 0$, причем $\exists i : \alpha_i \neq 0$).
В противном случае $v_1, \ldots, v_n$ *линейно независима* (то есть если $\alpha_1v_1 + \ldots + \alpha_nv_n = 0$, то $\forall i : \alpha_i = 0$).
*Примеры.* 1) $n = 1$ : система $v$ линейно независима $\Leftrightarrow\ v \neq 0$.
2) $n = 2$, $\alpha_1v_1 + \alpha_2v_2 = 0$. Если $\alpha_2 \neq 0$, то $v_2 = -\frac{\alpha_1}{\alpha_2}v_1$. Аналогично $\alpha_1 \neq 0$...
3) "Орты" – линейно независимая система в $F^n$.
*Замечание.* Линейная (не)зависимость не меняется при перенумерации векторов.

*Простейшие свойства линейной (не)зависимости:*
1) Подсистема линейно независимой системы – линейно независима.
2) Надсистема линейно зависимой системы – линейно зависима.
3) Система, содержащая 0, линейно зависима.
4) Система, содержащая два одинаковых вектора, линейно зависима.
5) Система линейно зависима $\Leftrightarrow$ один из векторов системы представим в виде линейной комбинации остальных.
*Доказательство.*
2) $v_1, \ldots, v_n$ линейно зависима $\Rightarrow \exists\ \alpha_1, \ldots, \alpha_n \in F : \alpha_1 v_1 + \ldots + \alpha_n v_n = 0$, $\exists i : \alpha_i \neq 0$. Рассмотрим $v_{n+1}, \ldots, v_N$ : $\alpha_1 v_1 + \ldots + \alpha_n v_n + 0 \cdot v_{n+1} + \ldots + 0 \cdot v_N = 0$ $\leftarrow$ нетривиальна $\Rightarrow v_1, \ldots, v_N$ линейно зависима.
3) Пусть $v_1 = 0 : 1 \cdot 0 + 0 \cdot v_2 + \ldots + 0 \cdot v_n = 0$; это – нетривиальная линейная комбинация.
Остальное – упражнение. $\square$
*Лемма.* Пусть $v_1, \ldots, v_n \in V$ линейно независимы, $v_1, \ldots, v_n, w \in V$ линейно зависимы. Тогда $w =$ линейная комбинация $v_1, \ldots, v_n$.
*Доказательство.* Пусть $\alpha_1 v_1 + \ldots + \alpha_n v_n + \beta w = 0$ – нетривиальная линейная комбинация. Тогда $\beta \neq 0$ (иначе $v_1, \ldots, v_n$ – линейно зависимы). То есть $w = -\frac{\alpha_1}{\beta} v_1 - \ldots - \frac{\alpha_n}{\beta} v_n$. $\square$
*Определение.* Система $v_1, \ldots, v_n \in V$ *полна* в пространстве $V$, если $\forall v \in V : v$ представим в виде линейной комбинации $v_1, \ldots, v_n$ (то есть $\exists\ \alpha_1, \ldots, \alpha_n \in F$ : $v = \alpha_1 v_1 + \ldots + \alpha_n v_n$). В противном случае – *неполна* в $V$.
*Примеры.* 1) "Орты" – полная система в $F^n$.
2) $(1,0), (0,1), (1,1)$ – полна в $F^2$.
*Замечание.* (Не)полнота не меняется при перенумерации.
*Упражнение.* Надсистема полной системы полна. Подсистема неполной системы неполна.
*Лемма* (о полноте). Пусть $v_1, \ldots, v_m$ полна в $V$; $w_1, \ldots, w_n \in V$; $\forall i = 1, \ldots, m$ : $v_i =$линейная комбинация $w_1, \ldots, w_n$. Тогда $w_1, \ldots, w_n$ полна в $V$.
*Доказательство.* Дано: $v_i = \sum_{j=1}^{n} \alpha_{ij} w_j$. Далее, $\forall v \in V\ \exists\ \lambda_1, \ldots, \lambda_m \in F$ : $v = \sum_{i=1}^{m} \lambda_i v_i$. То есть $v = \sum_{i=1}^{m} \lambda_i \sum_{j=1}^{n} \alpha_{ij} w_j = \sum_{j=1}^{n} \left(\sum_{i=1}^{m} \alpha_{ij} \lambda_i\right) w_j$. $\square$
*Следствие.* Пусть $v_1, \ldots, v_m$ полна в $V$; $v_m =$ линейная комбинация $v_1, \ldots, v_{m-1}$. Тогда $v_1, \ldots, v_{m-1}$ полна в $V$.
*Упражнение.* Линейная (не)зависимость и (не)полнота не меняются при изоморфизме.
*Базис и размерность линейного пространства*
*Определение.* Линейное пространство *конечномерно* , если в нем существует (конечная!) полная система векторов. (В противном случае – *бесконечномерно* ).
*Пример.* $F^n$ – конечномерно.

Будем систематически рассматривать лишь конечномерные пространства. Далее все линейные пространства конечномерны (если явно не оговорено обратное).

*Определение.* Система $v_1, \ldots, v_n \in V$ образует *базис* в $V$, если $\forall v \in V$ *однозначно* представим в виде линейной комбинации $v_1, \ldots, v_n$ (то есть $\forall v \in V$ $\exists! \alpha_1, \ldots, \alpha_n \in F : v = \alpha_1 v_1 + \ldots + \alpha_n v_n$).

Упорядоченный набор $(\alpha_1, \ldots, \alpha_n)$ – набор *координат* $v$ в этом базисе. По определению, вектор однозначно определяется своими координатами.

*Замечание.* При перенумерации базис переходит в (другой!) базис.

*Примеры.* 1) "орты" $e_1, ..., e_n$ – базис (так называемый "стандартный") в $F^n$

2) $(1,0); (1,1)$ – базис в $F^2$

3)$(1,0); (0,1); (1,1)$ – не базис в $F^2$

*Предложение(эквивалентные определения базиса).* Пусть $V \neq 0, v_1, ..., v_n \in V$. Следующие условия эквивалентны:

(1) $v_1, ..., v_n$ – базис в $V$

(2) $v_1, ..., v_n$ – линейно независима и полна

(3) $v_1, ..., v_n$ – максимальная линейно независимая система в $V$

(4) $v_1, ..., v_n$ – минимальная полная система в $V$

*Доказательство*

(1) $\Rightarrow$ (2): полнота по определению; линейна независима: 0 однозначно представим

(2) $\Rightarrow$ (3): Почему максимальная? Если $w \in V$, то (полнота) $w = \alpha_1 v_1 + ... + \alpha_n v_n \Rightarrow \alpha_1 v_1 + ... + \alpha_n v_n - 1w = 0$ – нетривиальная линейная комбинация $\Rightarrow$ $v_1, ..., v_n, w$ – линейно независимы.

(3) $\Rightarrow$ (4): Пусть $w \in V$. Так как $v_1, ..., v_n$ – максимальная линейно независимая, то $v_1, ..., v_n, w$ – линейно зависима $\Rightarrow$(лемма) $w$ есть линейная комбинация $v_i \Rightarrow$ $v_1, ..., v_n$ – полна в $V$. Почему минимальная полная? Пусть, скажем, $v_1, ..., v_{n-1}$ – тоже полна $\Rightarrow$ $v_1, ..., v_n$ – линейно зависима.

(3) $\Rightarrow$ (4): Пусть $v \in V$. Полнота $\Rightarrow$ $v$ – линейная комбинация $v_1, ..., v_n$. Почему однозначно? Пусть $v = \alpha_1 v_1 + ... + \alpha_n v_n = \beta_1 v_1 + ... + \beta_n v_n$, где, скажем $\alpha_n \neq \beta_n$. Тогда $0 = (\alpha_1 - \beta_1)v_1 + ... + (\alpha_n - \beta_n)v_n$, $(\alpha_n - \beta_n) \neq 0 \Rightarrow v_n$ – линейная комбинация $v_1, ..., v_{n-1} \Rightarrow$(лемма) $v_1, ..., v_{n-1}$ тоже полна $\Rightarrow$ противоречие.

(NB: что если $n = 1$? Тогда $0 = (\alpha - \beta)v_1 \Rightarrow v_1 = 0 \Rightarrow$ противоречие).

*Следствие* В любом (конечномерном, $\neq 0$) линейном пространстве существует базис.

*Доказательство* Возьмем любую (конечную!) полную систему и выкинем векторы так, чтобы она стала минимальной полной.

*Замечание* При $V = 0$ обычно считают, что базис – пустая система.

*Замечание* Из любой полной системы можно выделить базис. А как с линейно

независимыми системами? Может ли (в конечномерном пространстве) существовать сколь угодно большие линейно независимые системы?

**Теорема.** Пусть $v_1, ..., v_m$ – базис в $V$, $w_1, ..., w_n \in V$, $m < n$. Тогда $w_1, ..., w_n$ – линейно зависимы.

*Доказательство:* $w_j = \sum_{i=1}^{n} a_{ij} v_i,\ j = 1, ..., n,\ a_{ij} \in F$. Рассмотрим линейную комбинацию $\sum_{j=1}^{n} x_j w_j = 0$. Может ли она быть нетривиальной? Имеем $0 = \sum_{j=1}^{n} x_j w_j = \sum_{i=1}^{n} (\sum_{j=1}^{n} a_{ij} x_j) v_i \Rightarrow \sum_{j=1}^{n} a_{ij} x_j = 0,\ \forall i = 1, ..., m$. Это однородная С.Л.У., в которой число уравнений меньше числа неизвестных. Такая система имеет ненулевое решение $\Rightarrow w_1, ..., w_n$ – линейно зависимы $\square$.

То есть число векторов в любой линейно независимой системе ограничено сверху числом элементов любого базиса. То есть

*Замечание* Любую линейно независимую систему можно продолжить до базиса.

Кроме того: *Следствие* Число векторов во всех базисах пространства $V$ одинаково.

*Доказательство* Если $v_1, ..., v_m;\ w_1, ..., w_m$ – два базиса, и , скажем $m < n$, то теорема $\Rightarrow w_1, ..., w_n$ – линейно зависима $\square$.

Следствие отвечает за коректность следующего

*Определение* Размерность $V$ – это число векторов в базисе $V$. Обозанчение $\dim V = \dim_F V$. По определению, при $V = 0,\ \dim V = 0$.

*Пример.* $\dim F^n = n$

*Замечание.* 1) Пусть $v_1, ..., v_n \in V$. Если $v_1, ..., v_n$ – линейно независимы, то $\dim V \geq n$. Если $v_1, ..., v_n$ – полна в $V$, то $\dim V \leq n$.

2) Пусть $\dim V = n$. Тогда, если $v_1, ..., v_n$ – линейно независимы или полны в $V$, то $v_1, ..., v_n$ – базис.

*Замечание* $v_1, .., v_n$ – базис в $V$, $w_j = \sum a_{ij} v_i$, $A = (a_{ij})$. Тогда $w_1, ..., w_n$ – базис в $V \Leftrightarrow \det A \neq 0$.

*Доказательство.* базис $\Leftrightarrow Ax = 0$ имеет единственное решение $\Leftrightarrow \det A \neq 0$.

Несколько слов о бесконечномерных пространствах.

Можно определить базис, как (бесконечную) систему векторов, такую, что любой вектор есть конечная линейная комбинация....

Например, в $F[x]$ базис – $1, x, x^2, ...$

*Задача.* Докажите (с помощью леммы Цорна), что в любом пространстве есть базис.

*Классификация конечномерных пространств*

Напоминание: $V \simeq W$, если $\exists$ изоморфизм $\varphi : V \to W$.

**Теорема.** Пусть $V$ – линейное пространство над $F$, $\dim V = n$. Тогда $V \simeq F^n$.

*Доказательство.* Выберем базис $v_1, \ldots, v_n \in V$. Рассмотрим $\varphi : F^n \to V, \varphi(\alpha_1, \ldots, \alpha_n) = \sum_{i=1}^{n} \alpha_i v_i$. По определению базиса, $\varphi$ – биективен. Кроме того, $\varphi$ линеен. То есть $\varphi$ – изоморфизм. $\square$

*Замечание.* Построенный в доказательстве изоморфизм *зависит* от выбора

базиса в $V$.
*Следствие.* Если $\dim V = \dim W$, то $V \simeq W$.
Обратно, пусть $\varphi : V \to W$ – изоморфизм. Пусть $v_1, \dots, v_n$ – базис в $V$. Тогда (упражнение) $\varphi(v_1), \dots, \varphi(v_n)$ – базис в $W$. То есть $\dim W = \dim V = n$. Итого:
**Теорема.** $V \simeq W \Leftrightarrow \dim V = \dim W$.
*Замечание.* Обобщается на бесконечномерные в следующем смысле: $V \simeq W \Leftrightarrow$ базисы в $V$ и $W$ – равномощные.
*Упражнение.* Пусть $\varphi \in \mathrm{Hom}(V, W)$, $v_1, \dots, v_n$ – базис в $V$. Если $\varphi(v_1), \dots, \varphi(v_n)$ – *базис* в $W$, то $\varphi$ – изоморфизм. (То есть изоморфизм – это в точности линейное отображение, которое переводит базис в базис).
*Подпространство. Линейная оболочка.*
Пусть $V$ – линейное пространство над $F$.
*Определение. (Линейное) подпространство* в $V$ – это подмножество $L \subset V, L \neq \varnothing$, и такое, что 1) если $v_1, v_2 \in L$, то $v_1 + v_2 \in L$; 2) если $\alpha \in F, v \in L$, то $\alpha v \in L$.
*Замечание.* $L$ – подпространство $\Rightarrow 0 \in L$. Ибо $\exists v \in L \Rightarrow 0 = 0 \cdot v \in L$.
*Упражнение.* Если $L$ – подпространство в $V$, $v_1, \dots, v_n \in L$, $\alpha_1, \dots, \alpha_n \in F$, то $\sum \alpha_i v_i \in L$.
*Упражнение.* $L$ – подпространство в $U$, $U$ – подпространство в $V \Rightarrow L$ – подпространство в $V$.
*Замечание.* Подпространство – линейное пространство относительно "тех же" операций.
*Примеры.* 1) "Тривиальные" (= несобственные) подпространства 0 и $V$; 2) Прямая в $F^2$?
*Предложение.* Пусть $L$ – подпространство в $V$. Тогда 1) $\dim L \leq \dim V$; 2) если $\dim L = \dim V$, то $L = V$.
*Доказательство.* 1) Любая линейно независимая система в $L$, число векторов в ней ограничено сверху $\dim V$. Максимальная линейно независимая система – полная (и базис в $L$). То есть $L$ конечномерно, и $\dim L \leq \dim V$.
2) $\dim L = \dim V \Rightarrow \forall$ базис в $L$ – это *максимальная* линейно независимая система в $V \Rightarrow$ базис в $V$. То есть $L = V$. $\square$
Основной пример "конструкции" подпространств.
*Определение. Линейная оболочка* векторов $v_1, \dots, v_m \in V$ – это множество всех векторов из $V$, представимых в виде линейной комбинации $v_1, \dots, v_m$.
Обозначение: $\mathrm{Lin}\{v_1, \dots, v_m\}$. То есть $\mathrm{Lin}\{v_1, \dots, v_m\} = \{\sum \alpha_i v_i \mid \alpha_1, \dots, \alpha_m \in F\}$.
*Лемма.* $\mathrm{Lin}\{v_1, \dots, v_m\}$ подпространство в $V$.
*Доказательство. ...*
*Замечание.* 1) $\mathrm{Lin}\{v_1, \dots, v_m\}$ = подпространство в $V$, порожденное $v_1, \dots, v_m :=$ наименьшее подпространство в $V$, содержащее $v_1, \dots, v_m$ (то есть оно содержится в любом подпространстве в $V$, содержащем $v_1, \dots, v_m$).

2) Обобщение: $\forall A \subset V$ можно рассмотреть Lin $A :=$ наименьшее подпространство в $V$, содержащее $A$ (у нас $|A| < \infty$).
*Упражнение.* Покажите, что Lin $A = \{\sum_{i=1}^{n} \alpha_i v_i \mid v_1, \ldots, v_n \in A, \alpha_1, \ldots, \alpha_n \in F (n$ не фиксировано$)\}$. И обратно: если $v_1, \ldots, v_m$ полна в $L$, то $L =$ Lin $\{v_1, \ldots, v_m\}$.
*Замечание.* По определению, система $v_1, \ldots, v_m$ полна в Lin $\{v_1, \ldots, v_m\}$.
То есть $\dim$ Lin $\{v_1, \ldots, v_m\} \leq m$, причем $\dim$ Lin $\{v_1, \ldots, v_m\} = m \Leftrightarrow v_1, \ldots, v_m$ – линейно независимы (и тогда – базис в Lin $\{v_1, \ldots, v_m\}$).
Очевидно, что любое подпространство $L$ имеет вид Lin $\{v_1, \ldots, v_m\}$ для некоторой (конечно, *не* однозначно определенной) $v_1, \ldots, v_m$ (почему?).
*Упражнение.* Сформулировать необходимые и достаточные условия равенства Lin $\{v_1, \ldots, v_m\} =$ Lin $\{w_1, \ldots, w_n\}$.
Как "практически" находить базис в линейной оболочке? Способ 1: по индукции удалять "лишние векторы"; способ 2: алгоритм Гаусса.
$v_1, \ldots, v_m \in V$. Напомним: элементарные преобразования – это: 1) перестановка векторов; 2) $v_1, \ldots, v_i, \ldots, v_m \rightsquigarrow v_1, \ldots, \lambda v_i, \ldots, v_m, \lambda \in F, \lambda \neq 0$; 3) $v_1, \ldots, v_i, \ldots, v_j, \ldots v_m$ $v_1, \ldots, v_i + \lambda v_j, \ldots, v_j, \ldots v_m$, $\lambda \in F$. Удобно дополнить: 4) удаление/добавление 0.
*Лемма.* При элементарных преобразованиях системы векторов ее линейная оболочка не меняется.
*Доказательство.* Преобразования 1) и 4) – тривиально; 2) $v = \alpha_1 v_1 + \ldots + \alpha_i v_i + \ldots + \alpha_m v_m = \ldots + \frac{\alpha_i}{\lambda} v_i + \ldots$ (и обратно); 3) $v = \ldots + \alpha_i v_i + \ldots + \alpha_j v_j + \ldots = \ldots + \alpha_i (v_i + \lambda v_j) + \ldots + (\alpha_j - \lambda \alpha_i) v_j + \ldots$ (упражнение: обратно). $\square$
Пусть $\dim V = n$. Без ограничение общности считаем $V = F^n$.
Элементарные преобразования позволяют сделать матрицу, состоящюю из (строк) $v_1, ..., v_m$, ступенчатой (без нулевых строк). То есть $v_1, ..., v_m$ заменяется на $w_1, ..., w_r$, $(r \leq m)$ так, что

$$
\begin{gathered}
w_1 = (0, 0, ..., 0, \alpha_1, *, .....) \\
w_2 = (0, 0, ....., 0, \alpha_2, *, .....) \\
..... \\
w_r = (0, 0, ....., \alpha_r, *, ....) \\
.....j_1, .., j_2 ....j_r .....
\end{gathered}
$$

(здесь $\alpha_i \neq 0 \ \forall i$)
*Лемма.* $w_1, ..., w_r$ линейно независимы.
*Доказательство* Рассмотрим $x_1 w_1 + ... + x_r w_r = 0$, $x_i \in F$. Расмотрим $j_1$-ю координату.: $x_1 \alpha_1 = 0 \Rightarrow x_1 = 0$, рассмотрим $j_2$-ю: $x_2 = 0$ и так далее $\square$.
Итак $L := Lin\{v_1, ..., v_m\} = Lin\{w_1, ..., w_r\}$, $w_i$ – линейно независимы $\Rightarrow \dim L = r$.

## 3.8. **Ранг матрицы.**

Пусть $A \in Mat(m \times n, F)$. Запишем $A = \begin{pmatrix} a_1 \\ \cdot \\ \cdot \\ a_m \end{pmatrix}$, где $a_i \in F^n$ $--$строки $A$.

*Определение.* (Строковый) ранг $A$ – это $\dim Lin\{a_1, ..., a_m\}$. Обозначение: $rankA$
Аналогично можно определить столбцовый ранг $A$. Оказывается, что столбцовый ранг равен строковому. Оказывается, есть "симметричный" способ вычисления ранга – с помощью определителя
Напомним: минор матрицы $A$ порядка $p$ – это определитель $p \times p$ подматрицы $A$. Окаймляющий его минор (порядка $p+1$) получается добавлением ещё одной строки и столбца.
*Пример.*

$$A = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 5 & 6 & 7 & 8 \\ 9 & 10 & 11 & 12 \end{pmatrix}, \ \Delta = \begin{vmatrix} 1 & 3 \\ 5 & 7 \end{vmatrix} \text{ – минор второго порядка, } \begin{vmatrix} 1 & 2 & 3 \\ 5 & 6 & 7 \\ 9 & 10 & 11 \end{vmatrix}$$

окаймляет его.
**Теорема (о ранге)**. Пусть все миноры матрицы порядка $p+1$ равны нулю, и существует минор порядка $p$ отличный от нуля. Тогда $rankA = p$
*Замечания* 1) $A = 0 \Rightarrow$ считаем $p = 0$.
2) Если нулевых миноров нет, то $p = min\{m, n\}$
3) A priori таких $p$ может быть несколько. Теорема влечёт единственность такого $p$.
4) Знаем это в случае $m = n = p$ : $\det A \neq 0 \ \Leftrightarrow$ строки $A$ – базим в $F^n$.
*Доказательство* Пусть $r := rankA$. Требуется доказать $p = r$ (при $A = 0$ – верно).
1) $p$ не меняется при перестановке строк/столбцов $A$. $r$ не меняется при перестановке строк/столбцов $A$: строки по определению, стобцы – перестановки базисных векторов.

$$\text{То есть можем считать, что } \Delta := \begin{vmatrix} a_{11} & ... & a_{1p} \\ ... & ... & ... \\ a_{p1} & ... & a_{pp} \end{vmatrix} \neq 0, \text{ все миноры порядка } p+1 \ = 0$$

2) Почему $p \leq r$? Если $p > r$, то первые $p$ строк матрицы $A$ линейно зависимы $\Rightarrow$ первые $p$ строк матрицы $\Delta$ линейно зависимы. Противоречие.
3) Почему $p \geq r$? Проверим, что $a_{p+1}, ..., a_m \in Lin\{a_1, ..., a_p\}$. Зафиксируем

$i : p < r \leq n$. Для каждого $j$ рассмотрим

$$\Delta_j = \begin{vmatrix} a_{11} & ... & a_{1p} & a_{1j} \\ ... & ... & ... & ... \\ a_{p1} & ... & a_{pp} & a_{pj} \\ a_{i1} & ... & a_{ip} & a_{ij} \end{vmatrix}$$

$\Delta_j = 0\ \forall j$. Распишем $\Delta_j$ по последнему столбцу.$0 = A_1a_{1j} + ... + A_pa_{pj} + \Delta a_{ij}$. Здесь $a_1, ..., a_p$ не зависят от $j$. В "векторном виде" $0 = A_1a_1 + ...A_pa_p + \Delta a_i \Rightarrow a_i$ – линейная комбинация $a_1, ..., a_p\square$ . *Следствие.* Строковый ранг=столбцовому (то есть $rankA = rankA^T$).
*Упражнение* Выведите из теоремы о ранге, что если $rankA = p$, то все миноры $A$ порядка $> p$ равны нулю.

3.8.1. *Приложения к системам линейных уравнений.* 1. Рассмотрим

$$\begin{cases} a_{11}x_1 + \ldots + a_{1n}x_n = b_1 \\ \cdots\cdots\cdots \\ a_{m1}x_1 + \ldots + a_{mn}x_n = b_m \end{cases}, \qquad (*)$$

где $a_{ij}, b_i \in F$. Рассмотрим столбцы $a_j = \begin{pmatrix} a_{1j} \\ \vdots \\ a_{mj} \end{pmatrix}$ и $b = \begin{pmatrix} b_1 \\ \vdots \\ b_m \end{pmatrix}$ в пространстве $F^m$. Тогда $(*) \Leftrightarrow x_1a_1 + \ldots + x_na_n = b$, то есть $(*)$ совместна $\Leftrightarrow b \in \operatorname{Lin}\{a_1, \ldots, a_n\}$.
*Лемма.* $b \in \operatorname{Lin}\{a_1, \ldots, a_n\} \Leftrightarrow \operatorname{Lin}\{a_1, \ldots, a_n, b\} = \operatorname{Lin}\{a_1, \ldots, a_n\} \Leftrightarrow \dim \operatorname{Lin}\{a_1, \ldots, a_n$, $\dim \operatorname{Lin}\{a_1, \ldots, a_n\}$.
(a priori $\operatorname{Lin}\{a_1, \ldots, a_n, b\} \supset \operatorname{Lin}\{a_1, \ldots, a_n\}$)
*Доказательство.* $\Leftarrow$: тривиально; $\Rightarrow$: обратно, если $b =$ линейная комбинация $a_1, \ldots, a_n$, $v =$ линейная комбинация $a_1, \ldots, a_n, b$, то $v =$ линейная комбинация $a_1, \ldots, a_n$. $\square$
Напомним: $A = (a_1, \ldots, a_n)$ – матрица системы $(*)$, $\widetilde{A} = (A|b) = (a_1, \ldots, a_n, b)$ – расширенная матрица системы $(*)$. (Столбцевой) $\operatorname{rank} A = \dim \operatorname{Lin}\{a_1, \ldots, a_n\}, \operatorname{rank} \widetilde{A} = \dim \operatorname{Lin}\{a_1, \ldots, a_n, b\}$. То есть доказана
**Теорема** (Кронекера-Капелли). $(*)$ совместна $\Leftrightarrow \operatorname{rank} \widetilde{A} = \operatorname{rank} A$.
*Замечания.* 1) $(*)$ несовместна $\Leftrightarrow \operatorname{rank} \widetilde{A} = \operatorname{rank} A + 1$ (почему?)
2) На самом деле было раньше: (строковый) ранг = "число ступенек" эквивалентной ступенчатой матрицы. Только не знаем, что ранг – инвариант.
2. Рассмотрим случай однородной С.Л.У., то есть $b = 0$. Пусть $L$ – множество решений $(*)$ (рассматриваем как столбцы в $F^n$).
**Теорема.** $L$ – подпространство в $F^n$, причем $\dim L = n - \operatorname{rank} A$.

*Доказательство.* Матричный язык: $(*) \Leftrightarrow Ax = 0$, где $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$. То есть $L = \{x \in F^n \mid Ax = 0\}$. То есть $0 \in L$; $x, y \in L \Rightarrow x + y \in L, \lambda x \in L$. Итак, $L$ – подпространство.

Далее, $p := \operatorname{rank} A$. ( $p = 0 \Rightarrow L = F^n$ – верно). Переставим строки и столбцы (то есть переставим уравнения и перенумеруем неизвестные), считаем $\Delta = \begin{vmatrix} a_{11} & \dots & a_{1p} \\ \dots & \dots & \dots \\ a_{p1} & \dots & a_{pp} \end{vmatrix} \neq 0$. Тогда (из доказательства теоремы о ранге) любая строка $A =$ линейная комбинация первых $p$ строк. То есть

$$(*) \Leftrightarrow \begin{cases} a_{11}x_1 + \ldots + a_{1p}x_p = -(a_{1,p+1}x_{p+1} + \ldots + a_{1,n}x_n) \\ \cdots\cdots\cdots\cdots\cdots\cdots\cdots \\ a_{p1}x_1 + \ldots + a_{pp}x_p = -(a_{p,p+1}x_{p+1} + \ldots + a_{p,n}x_n) \end{cases}$$

То есть ($\Delta \neq 0$) $x_1, \ldots, x_p$ однозначно выражаются через $x_{p+1}, \ldots, x_n$ : $x_i = b_{i,p+1}x_{p+1} + \ldots + b_{in}x_n,\ i = 1, \ldots, n$. То есть

$$x = \begin{pmatrix} x_1 \\ \vdots \\ x_p \\ x_{p+1} \\ \vdots \\ x_n \end{pmatrix} = \ldots = x_{p+1} \begin{pmatrix} b_{1,p+1} \\ \vdots \\ b_{p,p+1} \\ 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix} + x_{p+2} \begin{pmatrix} b_{1,p+2} \\ \vdots \\ b_{p,p+2} \\ 0 \\ 1 \\ 0 \\ \vdots \end{pmatrix} + \ldots + x_n \begin{pmatrix} b_{1,n} \\ \vdots \\ b_{p,n} \\ 0 \\ \vdots \\ 0 \\ 1 \end{pmatrix} =:$$

$$=: x_{p+1}b_{p+1} + x_{p+2}b_{p+2} + \ldots + x_nb_n.$$

То есть $L = \operatorname{Lin} \{\underbrace{b_{p+1}, \ldots, b_n}_{n-p}\}$, причем $b_{p+1}, \ldots, b_n$ линейно независимы (почему?). То есть $\dim L = n - p$. □

*Терминология:* базис в $L$ = *фундаментальная система решений* $(*)$.

3.9. **Сумма и пересечение подпространств.** Пусть $V$ – линейное пространство над $F$, $L_1, L_2$ – подпространства в $V$.

*Лемма.* $L_1 \cap L_2$ – подпространство в $V$.

*Доказательство.* ... □

*Замечание.* $L_1 \cap L_2$ – наибольшее среди подпространств, содержащихся в $L_1$ и $L_2$.

*Упражнение.* (Обобщение) если $L_i$ ($i \in I$) – подпространства в $V$, то $\cap_i L_i$ – подпространство. Это – наибольшее среди подпространств, содержащихся в

$L_i\ \forall i \in I$.
Каково наименьшее среди подпространств, содержащих $L_1$ и $L_2$?
$L_1 \cup L_2$, как правило, не подпространство. (Упражнение: когда это все же подпространство?)
"Исправим": $L_1 + L_2 := \{v_1 + v_2 \mid v_1 \in L_1, v_2 \in L_2\}$ – сумма $L_1$ и $L_2$.
*Лемма.* $L_1 + L_2$ – подпространство в $V$.
*Доказательство.* ... $\square$
*Упражнение.* $L_1 + L_2$ – наименьшее среди подпространств, содержащих $L_1$ и $L_2$ (= пересечение всех подпространств, содержащих $L_1$ и $L_2$).
*Упражнение.* Если $L_1 = \text{Lin}\ \{v_1, \ldots, v_m\}$, $L_2 = \text{Lin}\ \{w_1, \ldots, w_n\}$, то $L_1 + L_2 = \text{Lin}\ \{v_1, \ldots, v_m, w_1, \ldots, w_n\}$.
**Теорема** (*формула Грассмана* ). $\dim(L_1 + L_2) = \dim L_1 + \dim L_2 - \dim(L_1 \cap L_2)$.
*Доказательство.* Пусть $p = \dim L_1, q = \dim L_2, r = \dim(L_1 \cap L_2)$. Выберем базис $u_1, \ldots, u_r$ в $L_1 \cap L_2$, дополним до базиса $u_1, \ldots, u_r, v_1, \ldots, v_{p-r}$ в $L_1$; дополним до базиса $u_1, \ldots, u_r, w_1, \ldots, w_{q-r}$ в $L_2$. Проверим, что $u_1, \ldots, u_r, v_1, \ldots, v_{p-r}, w_1, \ldots, w_{q-r}$ – базис в $L_1 + L_2$ (если это установлено, то $\dim(L_1 + L_2) = r + (p-r) + (q-r) = p + q - r$, что и требовалось доказать).
1) $\forall$ вектор из $L_1 + L_2$ = сумма вектора из $L_1$ и вектора из $L_2$ = (линейная комбинация $u_1, \ldots, u_r, v_1, \ldots, v_{p-r}$) + (линейная комбинация $u_1, \ldots, u_r, w_1, \ldots, w_{q-r}$) $\Rightarrow$ наша система полна в $L_1 + L_2$.
2) Линейная независимость: Рассмотрим $\sum_i \alpha_i u_i + \sum_j \beta_j v_j + \sum_k \gamma_k w_k = 0$. $x := \sum_i \alpha_i u_i + \sum_j \beta_j v_j = -\sum_k \gamma_k w_k \in L_1 \cap L_2 \Rightarrow x = \sum_l \delta_l u_l$. То есть $\sum_k \gamma_k w_k + \sum_l \delta_l u_l = 0 \Rightarrow$(базис в $L_2$ линейно независим) $\gamma_k = \delta_l = 0\ \forall k, l$. То есть $\sum_i \alpha_i u_i + \sum_j \beta_j v_j = 0 \Rightarrow \alpha_i = \beta_j = 0\ \forall i, j \square$.
*Пример.*($F = \mathbb{R}$) $\dim V = 3, \dim L_1 = \dim L_2 = 2,\ L_1 \neq L_2 \Rightarrow \dim L_1 \cap L_2 \leq 1$. $3 \geq \dim L_1 + L_2 = \dim L_1 + \dim L_2 - \dim L_1 \cap L_2 \geq 3 \Rightarrow \dim L_1 + L_2 = 3 \Rightarrow L_1 + L_2 = V \dim L_1 \cap L_2 = 1$. (то есть плоскости пересекаются по прямой).
*Замечание.* 1) Если $L_1, ..., L_m$ – подпространства в $V$, то $L_1 + ... + L_m = (L_1 + ... + L_{m-1}) + L_m = \{v_1 + ... + v_m | v_i \in L_i\}$ – подпространство в $V$. Это наименьшее подпространство содержащее все $L_i$.
2) Вообще, если $L_i (i \in I)$ – подпротсранства в $V$, то $\sum_i L_i :=$ наименьшее подпространство в $V$, содержащее $L_i, \forall i \in I$.
*Упражнение.* Из чего состоит $\sum_i L_i$?
*Прямая сумма*
Пусть $V$ – линейное пространство над $F$, $L_1, L_2$ – подпростанства в $V$.
*Определение.* Сумма $L_1$ и $L_2$ – прямая сумма, если $\forall v \in L_1 + L_2\ \exists! v_1 \in L_1, v_2 \in L_2 :\ v = v_1 + v_2$. (то есть $v_1, v_1' \in L_1 v_2, v_2' \in L_2, v_1 + v_2 = v_1' + v_2'$, то $v_1 = v_1',\ v_2 = v_2'$)
Обозначение: $L_1 \dot{+} L_2$(или $L_1 \bigoplus L_2$)
Если $v = v_1 + v_2$, где $v_i \in L_i$, то $v_i$ – проекция $v$ на $L_i$.
*Упражнение.* $\pi_i : L_1 \dot{+} L_2 \to L_i,\ \pi_i(v_1 + v_2) = v_i$ – линейное отображение.

*Пример.* Прямые на плоскости. РИСУНОК!
*Предложение.* $L_1 + L_2$ – прямая сумма $\Leftrightarrow L_1 \cap L_2 = 0$.
*Доказательство.* $\Rightarrow$: $v \in L_1 \cap L_2 \Rightarrow v = v + 0 = 0 + v \Rightarrow v = 0$.
$\Leftarrow$: $v_1 + v_2 = v_1' + v_2' \Rightarrow v_1 - v_1' = v_2 - v_2' \in L_1 \cap L_2 = 0 \Rightarrow v_1 = v_1', v_2 = v_2'$ $\square$.
Обобщение: $L_1, ..., L_m$ – подпространства в $V$. Сумма $L_1 + ... + L_m$ – прямая сумма, если $\forall v \in \sum L_i \exists! v_1 \in L_1, ..., v_m \in L_m : v = v_1 + ... + v_m$.
Обозначение: $L_1 \dot{+} ... \dot{+} L_m$ (или $\sum_{i=1}^{\cdot n} L_i$).
*Пример.* 1) три прямые на плоскости.
2) три прямые в пространстве
*Предложение.* Сумма $L_1 + ... + L_m$ – прямая сумма $\Leftrightarrow \forall i : L_i \cap (L_1 + ... + L_{i-1} + .L_{i+1}...L_m) = 0$.
*Доказательство:* Обозначим $U_i = L_i \cap (L_1 + ... + L_{i-1} + .L_{i+1}...L_m)$
$\Rightarrow$: $v \in U_i \Rightarrow v = 0 + ... + 0 + v + 0 + ... + 0 = v_1 + ...v_{i-1} + 0 + v_{i+1} + ... \Rightarrow v = 0$.
$\Leftarrow$: $v_1 + ... + v_m = v_1' + ... + v_m' \Rightarrow \forall i v_i - v_i' = \sum_{j \neq i}(v_j' - v_j) \in U_i = 0 \Rightarrow v_i = v_i' \square$.
*Упражнение.* Сумма $L_1 + ... + L_m$ – прямая $\Leftrightarrow \forall i : L_i \cap (L_1 + ... + L_{i-1}) = 0$. (по индукции...)
В каком случае $V = L_1 \dot{+} L_2$?
*Предложение.* Пусть $L_1, L_2$ – подпространства в $V$. Следующие условия эквивалентны:
(1) $V = L_1 \dot{+} L_2$
(2) $V = L_1 + L_2$ и $L_1 \cap L_2 = 0$
(3) $\dim V = \dim L_1 + \dim L_2$ и $L_1 \cap L_2 = 0$
(4) $V = L_1 + L_2$ и $\dim V = \dim L_1 + \dim L_2$
*Доказательство:* (1) $\Leftrightarrow$ (2): было; (2) $\Rightarrow$ (3) $\dim V = \dim L_1 + \dim L_2 - \dim L_1 \cap L_2 = \dim L_1 + \dim L_2$.
(3) $\Rightarrow$ (4) и (4) $\Rightarrow$ (2) – *Упражнение* $\square$.
Условие в терминах базисов:
*Предложение* (1) Если $V = L_1 \dot{+} L_2$, $e_1, ..., e_m$ – базис в $L_1$, $e_{m+1}, ..., e_n$ – базис в $L_2$, то $e_1, ..., e_n$ – базис в $V$.
(2) Пусть $L_1$ – подпространство в $V$, $e_1, ..., e_m$ – базис в $L_1$, $e_{m+1}, ..., e_n$ – таковы, что $e_1, ..., e_n$ – базис в $V$; $L_2 = Lin\{e_{m+1}, ..., e_n\}$. Тогда $V = L_1 \dot{+} L_2$.
*Доказательство:* (1) $v \in V \Rightarrow v = v_1 + v_2$....(единственно), $v_1 = ...$(единственно), $v_2 = ...$(единственно) $\Rightarrow v = ...$(единственно).
(2) $e_{m+1}, ..., e_n$ – линейно независимы $\Rightarrow$ это базис в $L_2$. Если $v \in V$, то $v = ...$(единственно)$= v_1 + v_2$, где $v_1 = ..., v_2 = ...\square$.
Пусть $L$ – подпространство в $V$.
*Определение* Подпространство дополнительное к $L$ – это подпространство $L' \subset V$ такое, что $V = L_1 \dot{+} L_2$.
*Следствие.* Дополнительное пространство существует.

*Замечание.* Дополнительное пространство не единственно (кроме... *Упражнение*): например $\dim V = 2,\ \dim L = 1$.
*Упражнение* (некоторые обобщения на несколько слагаемых). Пусть $L_1, \ldots, L_m$ – подпространства в $V$. Тогда $V = L_1 \dot{+} \ldots \dot{+} L_m \Leftrightarrow$ объединение (как-то упорядоченных) базисов в $L_1, \ldots, L_m$ является базисом в $V \Leftrightarrow \begin{cases} V = L_1 + \ldots + L_m \\ \dim V = \dim L_1 + \ldots + \dim L_m \end{cases}$
Мы рассмотрели так называемую "внутренюю" прямую сумму. Бывает и "внешняя", тесно связанная с "внутренней". Что это?
Пусть $V_1, V_2$ – линейные пространства над $F$. Рассмотрим $V = V_1 \times V_2 = \{(v_1, v_2) \mid v_1 \in V_1, v_2 \in V_2\}$. Операции в $V_1 \times V_2$: $(v_1, v_2) + (v_1', v_2') = (v_1 + v_1', v_2 + v_2')$, $\lambda(v_1, v_2) = (\lambda v_1, \lambda v_2)$.
*Упражнение.* Относительно этих операций $V_1 \times V_2$ – линейное пространство над $F$.
*Пример.* $F^2 = F \times F$ (и вообще, $F^k \times F^l = F^{k+l}$).
Рассмотрим $L_1 = \{(v_1, 0) \mid v_1 \in V_1\}, L_2 = \{(0, v_2) \mid v_2 \in V_2\}$.
*Упражнение.* $L_1, L_2$– подпространства в $V$.
Отметим, что
1) $(v_1, v_2) = \underset{\in L_1}{(v_1, 0)} + \underset{\in L_2}{(0, v_2)}$; $\quad L_1 \cap L_2 = 0$; то есть $V = L_1 \dot{+} L_2$;
2) Имеются изоморфизмы $V_1 \to L_1,\ v_1 \to (v_1, 0)$; $\quad V_2 \to L_2,\ v_2 \to (0, v_2)$.
Обычно отождествляют $V_i$ с $L_i$ с помощью этих изоморфизмов.
*Упражнение.* Обобщить на случай $V_1 \times \ldots \times V_m$.
*Замечание.* В случае *бесконечного* набора $V_i$ появляется разница!

3.10. **Ядро и образ линейного отображения.** Пусть $V, W$ – линейные пространства над $F$, $\varphi : V \to W$. Напомним: $\varphi$ –линейно, если ... $\mathrm{Hom}\,(V, W)$ – пространство всех линйейных отображений из $V$ в $W$.
"Измерим" отклонение $\varphi$ от изоморфизма (то есть биективности).
*Определение. Ядро* $\varphi$ – это $\mathrm{Ker}\ \varphi := \{v \in V \mid \varphi(v) = 0\}$. *Образ* $\varphi$ – это $\mathrm{Im}\ \varphi := \{w \in W \mid \exists v \in V : w = \varphi(v)\}$.
*Пример.* $V = V_1 \dot{+} V_2$; $\pi_i : V \to V$ – проекции. $\mathrm{Ker}\ \pi_i = ?$ $\mathrm{Im}\ \pi_i = ?$
*Лемма.* $\mathrm{Ker}\ \varphi$ – подпространство в $V$; $\mathrm{Im}\ \varphi$ – подпространство в $W$.
*Доказательство.* ... □
По определению, $\varphi$ сюръективно $\Leftrightarrow \mathrm{Im}\ \varphi = W$.
*Лемма.* $\varphi$ – инъективно $\Leftrightarrow \mathrm{Ker}\ \varphi = 0$.
*Доказательство.* ... □
Итого: $\varphi$ – изоморфмзм $\Leftrightarrow \mathrm{Ker}\ \varphi = 0, \mathrm{Im}\ \varphi = W$.
Как "исправить" не биективность $\varphi$?
Несюръективность: убрать "лишнее", то есть заменить $W$ на $\mathrm{Im}\ \varphi$.

Неинъективность: $\varphi(v_1) = \varphi(v_2) \Leftrightarrow v_1 - v_2 \in \mathrm{Ker}\ \varphi$; то есть надо "склеить" векторы, отличающиеся слагаемым из Ker $\varphi$. Для этого:

*Факторпространство*

Пусть $V$ – линейное пространство над $F$, $L$ – подпространство в $V$ (зафиксируем их).

Если $v_1, v_2 \in V$, то определим $v_1 \equiv v_2 \bmod L \overset{\text{def}}{\Leftrightarrow} v_1 - v_2 \in L$.

*Лемма.* 1) $\equiv \bmod L$ – отношение эквивалентности на $V$.

2) $\equiv \bmod L$ согласовано со сложением и умножением на скаляр (то есть $v_1 \equiv v_2 \bmod L, w_1 \equiv w_2 \bmod L \Rightarrow v_1 + w_1 \equiv v_2 + w_2 \bmod L, \lambda v_1 \equiv \lambda v_2 \bmod L$).

*Доказательство.* ... □

То есть $V$ – объединение попарно не пересекающихся классов эквивалентности. Класс эквивалентности $v \in V$ называется *смежным классом* $v$ по $L$ и равен $v + L = \{v + l \mid l \in L\}$. Итак $(v_1 + L) \cap (v_2 + L) \neq \emptyset \Leftrightarrow v_2 \in v_1 + L \Leftrightarrow v_1 + L = v_2 + L \Leftrightarrow v_1 \equiv v_2 \bmod L$.

*Пример.* 1) $\dim V = 2,\ \dim L = 1$: рисунок

2) $L$ – подпространство решений однородной С.Л.У. $\Rightarrow v + L$ – множество решений С.Л.У. ....

Обозначим $V/L$ – множество всех смежных классов векторов из $V$ по $L$.

Введём операции: $(v + L) + (w + L) = (v + w) + L,\ \lambda(v + L) = \lambda v + L$. Корректность этих операций следует из того, что $\equiv (mod L)$ согласовано ...

*Лемма* $V/L$ – линейное пространство относительно этих операций.

*Доказательство: Упражнение.*

**Теорема (базис в факторпространстве).** Пусть $L$ – подпространство в $V$, $L'$ – его (какое-нибудь) дополнительное пространство, $e_1, ..., e_m$ – базис в $L'$. Тогда $e_1 + L, ..., e_m + L$ – базис в $V/L$.

*Доказательство:* $V = L \dotplus L' \Rightarrow$: $v = l + l'$, где $l \in L, l' \in L'$. При этом $v = l'\ mod L$. $l' = \sum \alpha_i e_i \Rightarrow v + L = l' + L = \sum_i \alpha_i (e_i + L)$.

Единственность: $v + L = \sum \beta_i (e_i + L) \Rightarrow \sum (\alpha_i - \beta_i) e_i \in L \cap L' = 0 \Rightarrow \alpha_i = \beta_i$. □

Терминология: если $e_1, ..., e_m$ – таковы, что $e_1 + L, ..., e_m + L$ – базис в $V/L$, то $e_1, ..., e_m$ – базис в $V mod L$.

Итак, базис в $V mod L$ образуют векторы, дополняющие базис в $L$ до базиса в $V$.

*Следствие (размерность факторпространства).* $\dim V/L = \dim V - \dim L$.

Рассмотрим отображение $j : V \to V/L,\ j(v) = v + L$.

*Упражнение.* $j$ – линейно, сюръективно, $Ker j = L$.

*Каноническое разложение линейного отображения.*

Пусть $\varphi : V \to W$ линейно. Определим $\tilde{\varphi} : V/Ker\varphi \to Im\varphi, \tilde{\varphi}(v + Ker\varphi) := \varphi(v)$.

*Предложение.* Определение $\tilde{\varphi}$ корректно, причём $\tilde{\varphi}$ – изоморфизм.

*Доказательство.* 1) $v_1 + Ker\varphi = v_2 + Ker\varphi \Leftrightarrow v_1 - v_2 \in Ker\varphi \Leftrightarrow \varphi(v_1) = \varphi(v_2)$

$\Rightarrow$: корректность, $\Leftarrow$: инъективность.
2) сюръективность: по определению.
3) линейность: *Упражнение.* $\square$.
*Замечание.* Получено так называемое каноническое разложение $\varphi$:

$$\begin{array}{ccc} V & \xrightarrow{j} & V/Ker\varphi \\ {\scriptstyle\varphi}\downarrow & & \downarrow{\scriptstyle\tilde{\varphi}} \\ W & \xleftarrow{i} & Im\varphi \end{array}$$

Диаграма коммутативна, то есть $\varphi = i \circ \tilde{\varphi} \circ j$. Здесь $j$ – каноническая сюръекция, $i$ – каноническая инъекция.
*Следствие.* $\dim Ker\varphi + \dim Im\varphi = \dim V$.
*Замечание.* Рассмотрим однородную С.Л.У. $Ax = 0$, где $A \in Mat(m \times n, F)$. Пусть $V = F^n, W = F^m,\ \varphi \in Hom(V, W),\ \varphi(x) = Ax$
Пусть $L$ – пространство решений. Тогда $L = Ker\varphi$. С другой стороны, если $A = (a_1, ..., a_n)$(столбцы), то $Im\varphi = Lin\{a_1, ..., a_n\}$, то есть $\dim Im\varphi = rankA$. То есть получаем другое доказательство формулы $\dim L = n - rankA$.
*Следствие ("принцип Дирихле").* Пусть $n = \dim V = \dim W;\ \varphi \in Hom(V, W)$. Тогда $\varphi$ – биективно $\Leftrightarrow$ $\varphi$ инъективно $\Leftrightarrow$ $\varphi$ сюръективно.
*Замечание.* Аналогия со случаем $\varphi X \to Y$, где $|X| = |Y| < \infty$.
*Доказательство:* $\varphi$ инъективно $\Leftrightarrow$ $Ker\varphi = 0 \Leftrightarrow \dim Ker\varphi \Leftrightarrow \dim Im\varphi = n \Leftrightarrow Im\varphi = W \Leftrightarrow \varphi$ сюръективно.
*Упражнение.* Пусть $\varphi \in Hom(V, W)$
1) $\varphi$ инъективно $\Leftrightarrow$ $\forall$ линейного пространства $U$, $\forall X_1, X_2 \in Hom(U, V)$ : $\varphi \circ X_1 = \varphi \circ X_2 \Rightarrow X_1 = X_2 \Leftrightarrow \exists \psi \in Hom(W, V) : \psi \circ \varphi = id_V$.
1) $\varphi$ сюръективно $\Leftrightarrow$ $\forall$ линейного пространства $U$, $\forall X_1, X_2 \in Hom(W, U)$ : $X_1 \circ \varphi = X_2 \circ \varphi \Rightarrow X_1 = X_2 \Leftrightarrow \exists \psi \in Hom(W, V) : \varphi \circ \psi = id_W$.

3.11. **Линейные функционалы. Двойственность.** Пусть $V$ линейное пространство над $F$. *Линейный функционал* на $V$ – это линейное отображение $f : V \to F$. Обозначение: $V^* :=$ Hom $(V, F) =$ пространство линейных функционалов на $V =$ пространство, *двойственное* к $V$.
Пусть $\dim V = n$; $e_1, \ldots, e_n$ – базис в $V$. Рассмотрим $\varepsilon_j : V \to F$, $\varepsilon_j(\sum x_i e_i) = x_j$, то есть $\varepsilon_j(v) = j$-я координата $v$.
*Упражнение.* $\varepsilon_j \in V^*$.
$\varepsilon_j$ – это *координатные функционалы* в базисе $e_1, \ldots, e_n$. По определению $\varepsilon_j(e_i) = \delta_{ij} = \begin{cases} 1, & i = j \\ 0, & i \neq j \end{cases}$.
*Предложение.* $\varepsilon_1, \ldots, \varepsilon_n$ – базис в $V^*$.
*Доказательство.* Пусть $f \in V^*$. Тогда $f$ однозначно определяется по $f(e_1), \ldots, f(e_n)$,

ибо если $v \in V, v = \sum_i x_i e_i$, то $f(v) = \sum_i x_i f(e_i)$. Положим $\lambda_i = f(e_i)$. Рассмотрим $\widetilde{f} := \sum_j \lambda_j \varepsilon_j \in V^*$. Тогда $\widetilde{f}(e_i) = \sum_j \lambda_j \varepsilon_j(e_i) = \lambda_i = f(e_i) \quad \forall i \Rightarrow \widetilde{f} = f$. То есть $f = \sum_j \lambda_j \varepsilon_j$, где $\lambda_j = f(e_j)$ – однозначно определяются по $f$. $\square$

*Замечание.* Если $V = F^n$, $e_i$ – "орты", то $f \in V^*$ соответствует матрица $n \times 1$. Это строка $(f(e_1), \ldots, f(e_n))$. Конечно, в общем случае $V \simeq F^n$ (выбор базиса), то есть "то же самое". То есть результат, по сути, уже известен.

*Терминология.* $\varepsilon_1, \ldots, \varepsilon_n$ – базис в $V^*$, *двойственый* базису $e_1, \ldots, e_n$ в $V$.

*Следствие.* $\dim V^* = \dim V$, в частности, $V^* \simeq V$.

*Замечание.* 1) Изоморфизм $V^* \simeq V$ "неканонический", то есть он зависит от выбора исходного базиса в $V$. (Упражнение: докажите это!) 2) Если $\dim V = \infty$, то $\varepsilon_j$ линейно независимы, но *не* полны. (Упражнение: проверьте!) Более того, $\dim V^* > \dim V$ (в смысле мощности) (*Задача* : докажите это).

Далее, рассмотрим $V^{**} = (V^*)^*$. Конечно, в конечномерном случае $V^{**} \simeq V^* \simeq V$. Однако можно сделать более сильное утверждение.

Пусть $v \in V$. Рассмотрим $\varphi_v : V^* \to F, \varphi_v(f) := f(v)$.

*Лемма.* $\varphi_v \in V^{**}$.

*Доказательство.* ... $\square$

Таким образом, имеем отображение $\varphi : V \to V^{**},\ v \in V \to \varphi_v \in V^{**}$.

**Теорема.** $\varphi$ – изоморфизм.

*Доказательство.* 1) $\varphi$ – линеен: $\varphi_{v_1+v_2} \stackrel{?}{=} \varphi_{v_1} + \varphi_{v_2}; \varphi_{\lambda v} \stackrel{?}{=} \lambda \varphi_v$. Подставим $f \in V^* \ldots$.

2) $\operatorname{Ker} \varphi =? \ v \in \operatorname{Ker} \varphi \Leftrightarrow \varphi_v = 0 \Leftrightarrow \forall f \in V^* : f(v) = 0$. Если $v \neq 0$, то существует базис $v = e_1, \ldots, e_n$ в $V$. Тогда $\varepsilon_1(v) = \varepsilon_1(e_1) = 1 \neq 0$. То есть $\operatorname{Ker} \varphi = 0$, и $\varphi$ – инъективен.

3) Так как $\dim V^{**} = \dim V^* = \dim V$, то $\varphi$ и сюръективен тоже. $\square$

*Замечания.* 1) Изоморфизм $\varphi$ между $V$ и $V^{**}$ "канонический" в том смысле, что его конструкция не зависит ни от каких произвольных выборов. Обычно отождествляют $V^{**} = V$ с помощью $\varphi$, то есть не только функционалы из $V^*$ действуют на векторы из $V$, но и наоборот. Чтобы подчеркнуть эту двойственность, пишут $(f, v)$ вместо $f(v)$, где $f \in V^*, v \in V$. (То есть $(f, .)$ – линейный функционал на $V$, $(., v)$ – линейный функционал на $V^*$).

2) Если $\dim V = \infty$, то на этом пути получается инъективность (не сюръективность) линейного отображения $V \to V^{**}$. То есть можно считать $V \subset V^{**}$ (как подпространство).

*Аннулятор подпространства*

Пусть $L$ – подпространство в $V$. Определим его *аннулятор* $L^0 = \{f \in V^* \mid (f, v) = 0 \ \forall v \in L\}$.

*Лемма.* $L^0$ – подпространство в $V^*$.

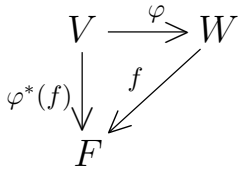
*Доказательство.* ... $\square$

*Предложение.* $\dim L^0 = \dim V - \dim L$.

*Доказательство.* Выберем базис $e_1, \dots, e_m$ в $L$ и дополним до базиса $e_1, \dots, e_m$, $e_{m+1}, \dots, e_n$ в $V$. Рассмотрим двойственный базис $\varepsilon_1, \dots, \varepsilon_n$ в $V^*$. Докажем, что $\varepsilon_{m+1}, \dots, \varepsilon_n$ – базис в $L^0$ (тогда $\dim L^0 = n - m$, что и требовалось доказать).
Пусть $f = \sum_{j=1}^{n} \lambda_j \varepsilon_j \in V^*$. Тогда $f \in L^0 \Leftrightarrow (f, e_i) = 0$ при $1 \le i \le m \underset{(f,e_i)=\lambda_i}{\Leftrightarrow}$ $\lambda_i = 0$ при $1 \le i \le m \Leftrightarrow f = \sum_{j=m+1}^{n} \lambda_j \varepsilon_j$, что и требовалось доказать. □
Аналогично, пусть $M$ – подпространство в $V^*$. Отождествим $V^{**} = V$, считаем $M^0 \subset V$, то есть $M^{)} = \{v \in V | (f, v) = 0 \ \forall f \in M\}$. По доказанному, $\dim M^0 = \dim V^* - \dim M$.
*Пример.* Рассмотрим С.Л.О.У.

$$(*) \begin{cases} a_{11}x_1 + ... + a_{1n}x_n = 0 \\ \qquad ..... \\ a_{m1}x_1 + ... + a_{mn}x_n = 0 \end{cases} \quad x_i \text{ – координаты } x \in V, \dim V = n \text{ в некотором базисе } e_i$$

Пусть $L$ – подпространство решений, $L \subset V$.
Рассмотрим $f_i \in V^*$. $(f_i, x) := a_{i1}x_1 + ... + a_{in}x_n$; то есть $(*) \Leftrightarrow (f_i, x) = 0, \ i = 1, ..., m$. Пусть $M = Lin\{f_1, ..., f_m\}$. Тогда $x \in L \Leftrightarrow \forall f \in M : (f, x) = 0$. То есть $L = M^0$. В частности $\dim L = \dim M_0 = \dim V^* - \dim M = n - rankA$ (ещё одно доказательство!).
Пусть снова $L \subset V$. Тогда $L^0 \subset V^*, \ L^0 \subset V^{**} = V$
*Предложение.* $L^{00} = L$.
*Доказательство:* 1) Пусть $v \in L$. Тогда $\forall f \in L^0 : (f, v) = 0$, то есть $v \in L^0 0$. Итак, $L \subset L^{00}$.
2) $\dim L^{00} = \dim V^* = \dim L^0 = \dim V - (\dim V - \dim L) = \dim L \to L = l^{00}$.
Другая формулировка: $M = L^0 \Leftrightarrow L = M^0$
*Пример (продолжение).* Так как $L = M^0$, то и $M = L^0$. В частности, любое подпространство в $V$ задается некоторой С.Л.О.У. А именно, если $L \subset V$, то рассмотрим $M := L^0$; и тогда $L = M^0$. Если $f_1, ..., f_m$ – базис в $M$, то $L$ задаётся С.Л.О.У. $(f_1, x) = ... = (f_m, x) = 0$.
*Упражнение.* 1) $L_1 \subset L_2 \Rightarrow L_1^0 \supset L_2^0$.
2) $(L_1 + L_2)^0 = L_1^0 \cap L_2^0$ ; $(L_1 \cap L_2)^0 = L_1^0 + L_2^0$
3) Если $V = L_1 \dot{+} L_2$, то $V^* = L_1^0 \dot{+} L_2^0$.
*Двойственное линейное отображение* Пусть $\varphi \in Hom(V, W)$. Определим $\varphi^* : W^* \to V^*$ так: пусть $f \in W^*$, тогда $\varphi * f \in V^*, (\varphi * (f), v) := (f, \varphi(v))$.




Отметим, что $\varphi^*(f) \in V^*$, ибо это композиция линейных отображений.
$\varphi^*$ – отображение двойственное к $\varphi$.

*Лемма.* $\varphi^* \in Hom(W^*, V^*)$.
*Доказательство:* $\varphi^*(f_1 + f_2) = \varphi^*(f_1) + \varphi^*(f_2)?,\ \varphi^*(\lambda f) = \lambda\varphi^*(f)?$. То есть $(f_1 + f_2)\varphi = f_1\varphi + f_2\varphi$; $(\lambda f)\varphi = \lambda(f\varphi)$ – было... $\square$
*Предложение (свойства двойственного линейного отображения).*
(1) $(\varphi_1 + \varphi_2)^* = \varphi_1^* + \varphi_2^*$
(2) $id^* = id,\ 0^* = 0$
(3) $(\varphi\psi)^* = \psi^*\varphi^*$
(4) $\varphi^** = \varphi$
*Доказательство:* (1), (2) – *Упражнение.*
(3) $U \to^{\psi} V \to^{\varphi} W$, $W^* \to^{\varphi^*} V \to^{\psi^*} U^*$. Если $f \in W^*$, то $((\varphi\psi)^*(f), u) = (f, \varphi(\psi(u))) = (\varphi^*\psi^*(f), u) \forall u \in U \Rightarrow (\varphi\psi)^*(f) - \varphi^*\psi^*(f) \in U^0 = 0$.
(4) $\varphi^{**} \in Hom(V^{**}, W^{**}) = Hom(V, W)$; $(f, \varphi^{**}(v)) = (\varphi^*(f), v) = (f, \varphi(v)) \Rightarrow$ $...\square$
*Замечание* Если $\dim V = \infty$, то $V \subset V^{**}$, и $\varphi^{**}|_V = \varphi$ .
*Предложение (двойственность ядро-образ)* $Ker\varphi^* = (Im\varphi)^0$, $Im\varphi^* = (Ker\varphi)^0$
*Доказательство:* $1) f \in Ker\varphi^* \Leftrightarrow \varphi^*(f) = 0 \Leftrightarrow \forall v \in V : (f, \varphi(v)) = 0 \Leftrightarrow f \in (Im\varphi)^0$ .
2) Применим 1) к $\varphi^* : Ker\varphi = Ker\varphi^{**} = (IM\varphi^*)^0 \Rightarrow ...\square$
*Задача.* Что в бесконечномерном случае?
*Пример.* Пусть $L$ – подпространство в $V$. Рассмотрим каноническую сюръекцию $j : V \to V/L$. Тогда $Kerj = L$. Рассмотрим $j^* : (V/L)^* \to V^*,\ j^*$ – инъективно $Imj^* = (Kerj)^0 = L^0$. То есть имеем канонический изоморфизм $(V/L)^* \cong L^0$.
Аналогично рассмотрим вложение $i : L \to V$. Тогда $i^* : V^* \to L^*$, $i^*$ – сюръекция, $Keri^* = (Imi)^0 = L^0$. То есть имеем канонический изоморфизм $V^*/L^0 \cong L^*$.

3.12. **Матрица линейного отображения.** Пусть $V, W$ – линейные пространства над $F$, $\dim V = n, \dim W = m$. Пусть $v_1, \ldots, v_n$ – базис в $V$, $w_1, \ldots, w_m$ – базис в $W$.
Пусть $\varphi \in \mathrm{Hom}\ (V, W)$. $\forall j :\ \varphi(v_j) \in W$, то есть $\varphi(v_j) = \sum_{i=1}^m a_{ij}w_i$, где $a_{ij} \in F$. Возникает матрица $A = (a_{ij}) \in \mathrm{Mat}\ (m \times n, F)$. Обозначение: $A =: \varphi_{w,v}$ – *матрица* $\varphi$ в *паре базисов* $v, w$.
*Замечание.* Это уже было в случае, когда $V = F^n, W = F^n$, базис – "орты". Общий случай, по сути, ничем не отличается, ибо выбор базиса в $V$ задает изоморфизм $V \simeq F^n$, при котором выбранный базис переходит в стандартный, то же для $W$. Но: преимущество (даже для $F^n$) – можно выбрать базис, удобный для конкретной ситуации.
Часто $W = V$, то есть $\varphi \in \mathrm{End}\ V$. Тогда обычно берут $w = v$ и пишут $\varphi_v := \varphi_{v,v}$. То есть $\varphi_v = (a_{ij})$, где $\varphi(v_j) = \sum_{i=1}^n a_{ij}v_i;\ \varphi_v \in \mathrm{Mat}\ (n, F)\ \leftarrow$ *квадратная.*
*Пример.* $\dim V = 2, V = L_1 \dot{+} L_2$, где $\dim L_i = 1 (i = 1, 2)$. $\varphi \in \mathrm{End}\ V$ – проекция

на $L_1$ вдоль $L_2$. Выберем базис $v_1 \in L_1, v_2 \in L_2$. Тогда $\varphi(v_1) = v_1 = 1 \cdot v_1 + 0 \cdot v_2$, $\varphi(v_2) = 0$. То есть $\varphi_v = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$.

Напомним свойства соответствия: линейные отображения $\to$ матрицы.

1) Линейность. Если $\varphi, \psi \in \mathrm{Hom}\,(V, W), \lambda \in F$, то $(\varphi+\psi)_{w,v} = \varphi_{w,v}+\psi_{w,v}$; $(\lambda\varphi)_{w,v} = \lambda\varphi_{w,v}$.

2) Согласованность с умножением. $U \overset{\psi}{\to} V \overset{\varphi}{\to} W, (U \overset{\varphi\circ\psi}{\to} W) \Rightarrow (\varphi \circ \psi)_{w,u} = \varphi_{w,v}\psi_{v,u}$.

NB: Если $\dim U = p, \dim V = n, \dim W = m$, то $\varphi_{w,v} \in \mathrm{Mat}\,(m \times n, F)$, $\psi_{v,u} \in \mathrm{Mat}\,(n \times p, F)$, $(\varphi \circ \psi)_{w,u} \in \mathrm{Mat}\,(m \times p, F)$. Кроме того: $\mathrm{id}_v = E$ $\forall$ базис $v$. Если $\varphi \in \mathrm{End}\, V$, то $\varphi$ – обратим $\Leftrightarrow$ ($\forall$ базис $v$) $\varphi_v$ – обратима.

В терминах матриц действие линейного отображения на вектор задается так. Пусть $\varphi \in \mathrm{Hom}\,(V, W), \varphi_{w,v} = (a_{ij}) \in \mathrm{Mat}\,(m \times n, F)$, то есть $\varphi(v_j) = \sum_i a_{ij} w_i$. Если $x \in V, x = \sum_j x_j v_j$, то $y = \varphi(x) = \ldots = \sum_i y_i w_i$ где $y_i = \sum_j a_{ij} x_j$. То есть если рассмотреть столбцы $x_v = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $y_w = \begin{pmatrix} y_1 \\ \vdots \\ y_m \end{pmatrix}$, то

$$y_w = \varphi(x)_w = \varphi_{w,v} \cdot x_v. \qquad (*)$$

*Замечание.* В частности, если $\varphi \in \mathrm{End}\, V$, то $\varphi(x)_v = \varphi_v \cdot x_v$.

*Замечание.* Матрица $\varphi$ в базисах $v, w$ *однозначно* определяется свойством $(*)$, то есть если $\forall x \in V: \ \varphi(x)_w = A \cdot x_v$, то $A = \varphi_{w,v}$. Именно, если взять $x = v_j$, то есть $x_v = \begin{pmatrix} 0 \\ \vdots \\ 1 \\ \vdots \\ 0 \end{pmatrix} \leftarrow j$ , то $Ax_v = j$-й столбец $A$. С другой стороны, $\varphi(x)_w = \varphi(v_j)_w =$ (по определению) $j$-й столбец $\varphi_{w,v}$.

*Матрица перехода*

Она нужна, чтобы ответить на вопрос, как преобразуется матрица линейного отображения при замене базиса.

Пусть $V$ – линейное пространство над $F$, $v_1, \ldots, v_n$ – базис в $V$, $v_1', \ldots, v_n'$ – (другой) базис в $V$.

Как связаны координаты вектора в этих базисах?

Имеем $v_j' = \sum_{i=1}^n t_{ij} v_i$, где $t_{ij} \in F$. $T_{v\to v'} := (t_{ij}) \in \mathrm{Mat}\,(n, F)$. $T_{v\to v'}$ – *матрица перехода* от базиса $v$ к базису $v'$.

Пусть $x \in V, x = \sum_i x_i v_i = \sum_j x_j' v_j'$. Рассмотрим $x_v = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, $x_{v'} = \begin{pmatrix} x_1' \\ \vdots \\ x_n' \end{pmatrix}$.

*Предложение.* $x_v = T_{v \to v'} \cdot x_{v'}$.

*Доказательство.* $x = \sum_j x_j' v_j' = \sum_j x_j' \sum_i t_{ij} v_i = \sum_i \left( \sum_j t_{ij} x_j' \right) v_i$. $\square$

*Замечание.* Матрица $T_{v \to v'}$ однозначно определяется этим свойством, то есть если $\forall x \in V : x_v = P \cdot x_{v'}$, то $P = T_{v \to v'}$. В самом деле, если $x := v_j'$, то $x_{v'} = j$-й орт, $P x_{v'} = j$-й столбец $P$; $x_v =$ (по определению) $j$-й столбец $T_{v \to v'}$.

*Замечание.* При желании можно интерпритировать матрицу перехода как матрицу линейного отображения, причем по-разному! Способ 1: $T_{v \to v'} = id_{v,v'}$ (что согласуется с формулой преобразования координат...). Способ 2: $T_{v \to v'} = \varphi_v (= \varphi_{v,v})$, где $\varphi(v_j) = v_j'$.

*Предложение (свойства матрицы перехода).*

(1) $T_{v \to v''} = T_{v \to v'} T_{v' \to v''}$;

(2) $T_{v,v} = E$

(3) $T_{v' \to v} = (T_{v \to v'})^{-1}$

*Доказательство:* (1) $\forall x \in V : (T_{v \to v'} T_{v' \to v''}) x_{v''} = T_{v \to v'} x_{v'} = x_v$. (2),(3) – *Упражнение.* $\square$

Пусть теперь $\varphi \in Hom(V, W)$. Пусть $v_1, ..., v_n, v_1' ... v_n'$ – базисы в $V$, $w_i, w_i'$ базисы в $W$.

*Предложение.* $\varphi_{w',v'} = T_{w' \to w} \varphi_{w,v} T_{v \to v'}$.

*Доказательство:* $\forall x \in V : \ T_{w' \to w} \varphi_{w,v} T_{v' \to v} x_{v'} = T_{w' \to w} \varphi_{w,v} x_v = T_{w' \to w} \varphi(x)_w = \varphi(x)_{w'}$.$\square$

Наиболее важный частный случай такой: $\varphi \in End(V)$(то есть $W = V$).

*Следствие.* Если $\varphi \in End(V), \ A = \varphi_v, A' = \varphi_{v'}, T = T_{v \to v'}$, то $A' = T^{-1} A T$.

*Следствие.* Если $\varphi \in End(V)$, то $\det \varphi$ – не зависит от выбора базиса.

*Доказательство:* $\det A' = \det(T^{-1} A T) = \det A$. $\square$

Если $\varphi \in End(V)$, то $\det \varphi = \det \varphi_v$ – определитель линейного оператора $\varphi$ (определение корректно в силу следствия above).

*Замечание.* Напомним, что если $A \in Mat(n, F)$, то след $A$: $TrA = \sum_i a_{ii}$. Мы проверяли, что $TrAB = TrBA$, то есть $TrT^{-1}AT = TrA$. Следовательно, если $\varphi \in End(V)$, то корректно определен $Tr\varphi = Tr\varphi_v$.

3.13. **Двойственность на языке матриц.** Пусть $V$ – линейное пространство над $F$, $\dim V = n$. Если $v_1, ..., v_n$ – базис в $V$, то имеется двойственный базис $f_i \in V^*, \ (f_i, v_j) = \delta_{ij}$. $x \in V \Rightarrow x = \sum_i x_i v_i; \ x_v = \begin{pmatrix} x_1 \\ ... \\ x_n \end{pmatrix} \xi \in V^*, \xi = \sum_j \lambda_j x_j, \lambda_j = (\xi, v_j), \xi_f = (\lambda_1, ..., \lambda_n)$ – это, кстати, матрица $\xi$ в базисах $v$ и

$1 \in F$.
Пусть $\varphi \in Hom(V,W)$, $v_i$ – базис в $V$, $w_j$ – базис в $W$. Рассмотрим $\varphi^* \in Hom(W^*,V^*)$ и двойственные базисы $f_i \in V^*$, $g_j \in W^*$.
*Предложение.* $(\varphi^*)_{f,g} = (\varphi_{w,v})^T$.
*Доказательство:* $\varphi_{w,v} = (a_{ij})$, где $\varphi(v_j) = \sum_i a_{ij}w_i$. $(\varphi^*)_{f,g} = (b_{kl})$, $\varphi^*(g_i) = \sum_j b_{ji}f_j$. Тогда $a_{ij} = (g_i, \varphi(v_j)) = (\varphi^*(g_i), v_j) = b_{ji}\square$.
С матрицей перехода та же история:
*Упражнение.* Пусть $v_i, v_i'$ – базис в $V$, $f_j, f_j'$ – базис в $V^*$. Тогда $T_{f'\to f} = (T_{v\to v'})^T$.
Резюме: на уровне матриц имеется двойственность стобцы $\leftrightarrow$ строки.

3.14. **Канонический вид матрицы линейного отображения между различными просранствами.** Пусть $V, W$ – линейные пространства над $F$, $\varphi \in Hom(V,W)$. $\varphi$ индуцирует изоморфизм $\tilde{\varphi} : V/Ker\varphi \to Im\varphi$. Пусть $v_1, ..., v_r$ – базис в $VmodKer\varphi$. Положим $w_j = \varphi(v_j)$. Тогда $w_1, ..., w_r$ – базис в $Im\varphi$. Дополним $v_1, ..., v_r$ до $v_1, ..., v_n \in V$, $w_1, ..., w_r$ до базиса $w_1, ..., w_m$, Тогда

$$\varphi_{w,v} = \begin{pmatrix} 1 & 0 & 0 & ... & 0 \\ 0 & 1 & 0 & ... & 0 \\ ... & & & & \\ 0 & 0 & 1 & ... & 0 \\ 0 & 0 & 0 & 0... & 0 \\ .... & & & & \\ 0 & 0 & 0 & ... & 0 \end{pmatrix}$$

Эта матрица зависит от $n = \dim V, m = \dim W, r = rank\varphi$. При этом $r \leq m, n$.
Далее рассмотрим случай $V = W, v = w$.
NB: имеем классификацию троек $(V, W, \varphi)$ (*Упражнение* продумать).
*Инвариантные подпространства*
Пусть $V$ – линейное пространство над $F$. Пусть $\varphi \in \mathrm{End}\, V$, то есть $\varphi$ – *линейный оператор* (употребляется для линейных $V \to V$). Пусть $L$ – подпространство в $V$.
*Определение.* $L$ – *инвариантно* для $\varphi$ (= относительно $\varphi$, $\varphi$-инвариантно), если $\varphi(L) \subset L$, то есть $\forall x \in L : \varphi(x) \in L$.
*Примеры.* 1) $0, V$ инвариантны относительно $\forall\varphi$.
2) $V = L \dot{+} L', \varphi$ – проекция на $L$ вдоль $L'$. Тогда $L, L'$ инвариантны для $\varphi$.
*Упражнение.* $L$ инвариантно относительно $\varphi \Rightarrow L^0$ инвариантно относительно $\varphi^*$.
На языке матриц (NB: теперь выбираем один и тот же базис в двух "копиях" $V$), пусть $v_1, \ldots, v_m$ – базис в $L$; дополним его до базиса $v_1, \ldots, v_m, v_{m+1}, \ldots, v_n$ в $V$. Пусть $\varphi \in \mathrm{End}\, V$.

*Предложение.* $L$ инвариантно относительно $\varphi \Leftrightarrow \varphi_v = \underbrace{\left(\begin{array}{c|c} * & * \\ \hline O & * \end{array}\right)}_{m \quad n-m} \begin{array}{l} \}m \\ \}n-m \end{array}$.

*Доказательство.* $\varphi_v = (a_{ij})$, где $\varphi(v_j) = \sum_{i=1}^n a_{ij} v_i = \underbrace{\sum_{i=1}^m \ldots}_{\in L} + \sum_{i=m+1}^n \ldots$.

Тогда $L$ инвариантно относительно $\varphi \underset{\text{упр.}:\Leftarrow}{\Leftrightarrow} \forall j \in \{1, \ldots, m\} : \ \varphi(v_j) \in L \Leftrightarrow \forall j \in \{1, \ldots, m\} \ \forall i \in \{m+1, \ldots, n\} : a_{ij} = 0$. $\square$

Каков смысл "блоков" блочно-треугольной матрицы $\varphi_v$ (при условии, что $L$ инвариантно относительно $\varphi$)? Итак, пусть $L$ – инвариантно относительно $\varphi$. Тогда можно рассмотреть ограничение $\varphi$ на $L$, то есть $\varphi_L : L \to L$, $\varphi_L(x) = \varphi(x)$ при $x \in L$ (другое обозначение $\varphi|_L$). Терминология: $\varphi_L$ – *подоператор* . По определению, $\varphi_L \in \operatorname{End} L$. Кроме того, матрица $\varphi_L$ в базисе $v_1, \ldots, v_m \in L$ – это верхний левый угол $\varphi_v$.

Далее, рассмотрим факторпространство $V/L$. Тогда $\varphi$ индуцирует отображение $\varphi_{V/L} : V/L \to V/L, \ \varphi_{V/L}(x + L) := \varphi(x) + L$. Это определение корректно: если $x + L = x' + L$, то есть $x - x' \in L$, то (инвариантность!) $\varphi(x) - \varphi(x') = \varphi(x - x') \in L$, то есть $\varphi(x) + L = \varphi(x') + L$. Терминология: $\varphi_{V/L}$ – *фактороператор* .

*Упражнение.* $\varphi_{V/L}$ – линейно.

Итак, $\varphi_{V/L} \in \operatorname{End} V/L$.

Напомним, что (в обозначениях, введенных выше) $v_{m+1} + L, \ldots, v_n + L$ – базис в $V/L$. Если $j \in \{m+1, \ldots, n\}$, то $\varphi_{V/L}(v_j + L) = \varphi(v_j) + L = \sum_{i=m+1}^n a_{ij} v_i + \underbrace{\sum_{i=1}^m a_{ij} v_i}_{\in L} + L = \sum_{i=m+1}^n a_{ij}(v_i + L)$. То есть матрица $\varphi_{V/L}$ в базисе $v_{m+1} + L, \ldots, v_n + L$ – это правый нижний угол матрицы $\varphi_v$.

Итого имеем: если $L$ – инвариантно относительно $\varphi$, то (допуская вольность обозначений) $\varphi_v = \left(\begin{array}{c|c} (\varphi_L)_v & * \\ \hline O & (\varphi_{V/L})_v \end{array}\right)$. Здесь правый верхний угол "отвечает" за "взаимодействие" $\varphi_L$ и $\varphi_{V/L}$, то есть как они "склеиваются" в $\varphi$. То есть $\varphi$ *не* восстанавливается однозначно по $\varphi_L$ и $\varphi_{V/L}$.

Ситуация, однако, упрощается, если есть два взаимно дополнительных инвариантных подпространства. Именно, пусть $V = L_1 \dotplus L_2$. Пусть $v_1, \ldots, v_m$ – базис в $L_1$, $v_{m+1}, \ldots, v_n$ – базис в $L_2$, тогда $v_1, \ldots, v_m, v_{m+1}, \ldots, v_n$ – базис в $V$. Пусть $\varphi \in \operatorname{End} V$.

*Предложение.* $L_1$ и $L_2$ – инвариантны относительно $\varphi \Leftrightarrow \varphi_v =$

$\left(\begin{array}{c|c} (\varphi_{L_1})_v & O \\ \hline O & (\varphi_{L_2})_v \end{array}\right)$, (то есть матрица $\varphi$ в указанном базисе блочно-диагональна).
*Доказательство.* Самостоятельно. □
*Терминология.* $\varphi$ – прямая сумма линейных операторов $\varphi_{L_1}$ и $\varphi_{L_2}$.
*Замечание.* Обратно, если $V = L_1 \dotplus L_2$ и $\varphi_{L_i} \in \mathrm{End}\, V$, то ...
*Упражнение.* Обобщить на случай $V = L_1 \dotplus \ldots \dotplus L_m$. В этом случае $\forall i : L_i$ – $\varphi$-инвариантно $\Leftrightarrow$ матрица $\varphi$ в базисе, "приспособленном" к $L_1, \ldots, L_m$, блочно-диагональная.

3.14.1. *Собственные векторы и собственные значения.* Пусть $\varphi \in \mathrm{End}\, V$. Как устроены одномерные $\varphi$-инвариантные подпространства? То есть $L = \mathrm{Lin}\,\{v\}$, где $v \in V, v \neq 0$, и $\varphi(v) \in L$, то есть $\varphi(v) = \lambda v$, где $\lambda \in F$.
*Определение. Собственный вектор* линейного оператора $\varphi$ – это $v \in V, v \neq 0$, такой что $\varphi(v) = \lambda v$, где $\lambda \in F$. Этот скаляр $\lambda$ – *собственное значение* , соответствующее $v$.
Вообще, *собственное значение* линейного оператора $\varphi$ – это $\lambda \in F$ такое, что существует собственные вектор, соответствующий $\lambda$.
Геометрический смысл: в направлении собственного вектора $\varphi$ действует умножением на собственное значение.
Как находить собственные векторы и собственные значения?
Пусть $\lambda \in F$ – произвольное. Рассмотрим $V_\lambda = V_\lambda(\varphi) := \mathrm{Ker}\,(\varphi - \lambda \cdot \mathrm{id})$.
*Лемма.* $\lambda$ – собственное значение $\varphi \Leftrightarrow V_\lambda \neq 0$; при этом $V_\lambda \setminus \{0\}$ – множество всех собственных векторов, соответствующих $\lambda$.
*Доказательство.* (по определению). □
*Терминология:* $V_\lambda(\varphi)$ – собственное подпространство линейного оператора $\varphi$ соответствующие $\lambda$. То есть, при фиксированом собственном значении $\lambda$ легко найти все собственные векторы: практически надо решить С.Л.О.У.
Как находить собственные значения?
Рассмотрим $\chi(\lambda) := \det(\varphi - \lambda id)$.
*Лемма.* $\chi$ – многочлен (относительно $\lambda$) с коэффициентами в $F$. $\deg \chi = \dim V$.
*Доказательство:* Пусть $v_1, ..., v_n$ – базис в $V$; $\varphi_v = A = (a_{ij}) \in Mat(n, F)$. Тогда $(\varphi - \lambda id)_v = A - \lambda E = \begin{pmatrix} a_{11} - \lambda & a_{12} & ... & a_{1n} \\ a_{21} & a_{22} - \lambda & ... & a_{2n} \\ ..... & & & \\ a_{n1} & a_{n2} & ... & a_{nn} - \lambda \end{pmatrix}$. Тогда все утверждения следуют и свойств det. □
*Замечание.* Старший коэффициент $\chi$ равен $(-1)^n$, где $n = \dim V$; свободный член $\chi$ – это $\det \varphi$.
*Упражнение.* Найдите коэффициент при $\lambda^{n-1}$.

Терминология: $\chi_\varphi$ – характеристический многочлен оператора $\varphi$.
*Предложение.* $\lambda$ – собственное значение $\varphi \Leftrightarrow \chi_\varphi(\lambda) = 0$.
*Доказательство* $\lambda$ – собственное значение $\Leftrightarrow V_\lambda = Ker(\varphi - \lambda id) \neq 0 \Leftrightarrow \varphi - \lambda id$ необратим $\leftrightarrow \chi(\lambda) = \det(\varphi - \lambda id) = 0$.$\square$
Это дает "практический" способ вычисления собственных значений...
*Пример.* $\varphi \to A = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$ Найти собственные значения и векторы.
*Замечания* 1) Пусть $F = \mathbb{C}$ (или $F$ – алгебраически замкнуто). Тогда при $n = \dim V > 0$ любой линейный оператор имеет $n$ собственных значений (с учетом кратности). Соответственно, существуют собственные векторы.
2) Пусть $F = \mathbb{R}$. Тогда это не так.
*Пример.* Поворот $\mathbb{R}^2$ на угол $\alpha \notin \pi\mathbb{Z}$ – нет собственных векторов.
*Предложение.* Пусть $v_1, ..., v_m$ – собственные векторы линейного оператора $\varphi$, $\lambda_1, ..., \lambda_m$ – соответсенные собственные значения, $\lambda_i \neq \lambda_j$ при $i \neq j$. Тогда $v_1, ..., v_m$ – линейно независимы.
*Доказательство:* От противного. Рассмотим соответсвующую линейную зависимость с наименьшим числом векторов, имеем $c_1\lambda_1 + ...c_l\lambda_l = 0,\ c_i \neq 0$. Можно заменить $v_i$ на $c_iv_i$ – тоже собственный вектор. Тогда $v_1 + ... + v_l = 0$. Применим $\varphi$: $\lambda_1v_1 + ... + \lambda_lv_l = 0 \Rightarrow (\lambda_1 - \lambda_l)v_1 + ... + (\lambda_{l-1} - \lambda_l)v_{l-1} = 0$ – меньше слагаемых. $\square$
*Следствие.* Пусть $\lambda_1, ..., \lambda_m$ – собственные значения $\varphi$ $\lambda_i \neq \lambda_j$ при $i \neq j$. Тогда сумма подпространств $V_{\lambda_1}, ..., V_{\lambda_m}$ – прямая.
*Определение.* $\varphi \in EndV$ диагонализуем (=полупрост), если существует базис $v_1, ..., v_n$ такой, что в нем $\varphi_v$ – диагональна. (то есть это базис собственных векторов).
Условия диагонализуемости? *Предложение.* Пусть $\lambda_1, ..., \lambda_m$ – все собственные значения $\varphi$ (без учета кратности). Тогда следующие условия эквивалентны:
(1) $\varphi$ – диагонализуем
(2) $V = V_{\lambda_1} \dot{+} ... \dot{+} V_{\lambda_m}$
(3) $\dim V = \dim V_{\lambda_1} + ... + \dim V_{\lambda_m}$
*Доказательство:*(1) $\Leftrightarrow$ (2): $V = V_{\lambda_1} \dot{+} ... \dot{+} V_{\lambda_m} \Leftrightarrow$ объединение базисов $V_{\lambda_i}$ дает базис $V$. Но такой базис автоматически состоит из собственных векторов. Обратно базис собственных векторов – объединение базисов $V_{\lambda_i}$
(2) $\Rightarrow$ (3): было
(3) $\Leftrightarrow$ (2): $\dim \sum_i V_{\lambda_i} = \sum_i \dim V_{\lambda_i}$, $\dim V = \sum_i \dim V_{\lambda_i} \Rightarrow V = \sum_i V_{\lambda_i}$. $\square$
*Предложение.* $\forall \mu \in F:\ \dim V_\mu \leq \mathrm{Kp}_\mu\chi$.
*Доказательство.* Если $\mu$ – не собственное значение $\varphi$, то тривиально: $0 \leq 0$. Далее $\mu$ – собственное значение $\varphi$. Выберем базис $v_1, \ldots, v_l$ в $V_\mu$ (то есть $l = \dim V_\mu$) и дополним до базиса $v_1, \ldots, v_l, v_{l+1}, \ldots, v_n$ в $V$. В этом базисе

$\varphi_v = \left(\begin{array}{ccc|c} \mu & & O & \\ & \ddots & & * \\ O & & \mu & \\ \hline & O & & * \end{array}\right)$, где левый верхний блок имеет размер $l \times l \Rightarrow \chi(\lambda) = (\mu - \lambda)^l \cdot f(\lambda)$, где $f$ – некий многочлен. Поэтому $\mathrm{Kp}_\mu \chi \geq l$, что и требовалось доказать. □

**Теорема.** $\varphi$ – диагонализуем $\Leftrightarrow$

$\begin{cases} (1)\ \chi_\varphi \text{ разлагается над } F \text{ на множители степени } 1 \\ (\text{то есть имеет } n = \dim V \text{ корней с учетом кратности}). \\ (2)\ \forall \text{ собственного значения } \mu: \ \dim V_\mu(\varphi) = \mathrm{Kp}_\mu \chi_\varphi. \end{cases}$

*Замечание.* Если $F$ алгебраически замкнуто (например, $F = \mathbb{C}$), то условие (1) выполняется автоматически.

*Доказательство.* Пусть $\lambda_1, \ldots, \lambda_m$ – все собственные значения $\varphi$ (без учета кратности), $k_i = \mathrm{Kp}_{\lambda_i} \chi$. То есть $\chi(\lambda) = (\lambda - \lambda_1)^{k_1} \cdot \ldots \cdot (\lambda - \lambda_m)^{k_m} f(\lambda)$, где $f$ не имеет корней в поле $F$. В частности, $\sum_i k_i \leq n := \dim V$, причем $\sum_i k_i = n$ $\Leftrightarrow \chi$ разлагается на множители степени 1.

Далее, пусть $l_i := \dim V_{\lambda_i}$. Тогда: 1) $\varphi$ – диагонализуем $\Leftrightarrow \sum_i l_i = n$; 2) $\forall i \ l_i \leq k_i$.

$\Leftarrow$: Дано: $\sum_i k_i = n$; $\quad \forall i \ l_i = k_i$. Тогда $\sum_i l_i = n$, то есть $\varphi$ диагонализуем.

$\Rightarrow$: Дано: $\sum_i l_i = n$. Тогда $n = \sum_i l_i \leq \sum_i k_i \leq n \Rightarrow \forall i: \ l_i = k_i$, и $\sum_i k_i = n$. □

*Следствие.* Пусть $\chi_\varphi$ имеет $n(= \dim V)$ *различных* корней в поле $F$. Тогда $\varphi$ диагонализуем.

*Доказательство.* В обозначениях предыдущего доказательства дано, что $\forall i$ : $k_i = 1$. Так как $\forall i: \ 0 < l_i \leq k_i$, то $l_i = 1$, то есть (2) выполнено. По условию, (1) тоже выполнено. □

3.14.2. *Жорданова форма линейного оператора.* ("суррогат" для недиагонализуемых операторов). *Определение. Жорданова клетка* – это матрица $J \in \mathrm{Mat}\ (n, F)$ вида $J = \begin{pmatrix} \lambda & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \lambda & 1 & 0 & \ldots & 0 \\ \ldots & & \ldots & & \ldots & & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \lambda & 1 \\ 0 & 0 & \ldots & 0 & 0 & 0 & \lambda \end{pmatrix}$, где $\lambda \in F$.

NB: 1) $n = 1 \Rightarrow \forall$ матрица – жорданова клетка; 2) иногда 1 под главной диагональю ("суть" не меняется).

*Жорданова матрица* – это блочно-диагональная матрица вида

$\begin{pmatrix} J_1 & & O \\ & J_2 & \\ & \ddots & \\ O & & J_m \end{pmatrix}$, где $J_1, \ldots, J_m$ –жордановы клетки (вообще говоря, у каждой – свое $\lambda$).

NB: То есть любая диагональная матрица – жорданова матрица.

*Примеры.* $\begin{pmatrix} 3 & 1 & 0 \\ 0 & 3 & 1 \\ 0 & 0 & 3 \end{pmatrix}$, $\left(\begin{array}{cc|c} 3 & 1 & 0 \\ 0 & 3 & 0 \\ \hline 0 & 0 & 3 \end{array}\right)$, $\left(\begin{array}{cc|c} 3 & 1 & 0 \\ 0 & 3 & 0 \\ \hline 0 & 0 & 2 \end{array}\right)$ – жордановы матрицы; $\begin{pmatrix} 3 & 1 & 0 \\ 0 & 2 & 0 \\ 0 & 0 & 2 \end{pmatrix}$ – нет.

**Теорема** (о жордановой форме линейного оператора). Пусть $V$ – линейное пространство над $F$, $\varphi \in \operatorname{End} V$. Пусть $\chi_\varphi$ разлагается на множители степени 1 над $F$. Тогда в $V$ существует базис $e_1, \ldots, e_n$ (так называемый *жорданов базис* для $\varphi$) такой, что матрица $\varphi_e$ – жорданова. При этом матрица $\varphi_e$ единственна с точностью до порядка жордановых клеток на диагонали.

NB: Жорданов *базис* не единствен!

*Замечание.* Если $\varphi$ – диагонализуем, то его базис диагонализуемости – жорданов базис.

Доказательство теоремы будет позже. Нужна подготовка. Как устроен жорданов базис?

*Пример* (одна жорданова клетка).

$$\varphi_e = \begin{pmatrix} \lambda & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & \ldots & 0 \\ 0 & 0 & \lambda & 1 & 0 & \ldots & 0 \\ \ldots & & \ldots & & \ldots & & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \lambda & 1 \\ 0 & 0 & \ldots & 0 & 0 & 0 & \lambda \end{pmatrix} \Leftrightarrow \begin{array}{c} \varphi(e_1) = \lambda e_1 \\ \varphi(e_2) = e_1 + \lambda e_2 \\ \varphi(e_3) = e_2 + \lambda e_3 \\ \ldots\ldots\ldots \\ \varphi(e_n) = e_{n-1} + \lambda e_n \end{array} \Leftrightarrow$$

$$\begin{array}{c} (\varphi - \lambda \cdot \mathrm{id})e_1 = 0 \\ (\varphi - \lambda \cdot \mathrm{id})e_2 = e_1 \\ (\varphi - \lambda \cdot \mathrm{id})e_3 = e_2 \\ \ldots\ldots\ldots \\ (\varphi - \lambda \cdot \mathrm{id})e_n = e_{n-1}. \end{array}$$

В частности, $(\varphi - \lambda \cdot \mathrm{id})^2(e_2) = 0, (\varphi - \lambda \cdot \mathrm{id})^3(e_3) = 0, \ldots, (\varphi - \lambda \cdot \mathrm{id})^n(e_n) = 0$.

*Определение. Корневой вектор* линейного оператора $\varphi$, соответствующий $\lambda \in F$ – это $v \in V$ такой, что $v \neq 0$ и $\exists k \in \mathbb{N}: \ (\varphi - \lambda \cdot \mathrm{id})^k(v) = 0$. Наименьшее $k$ с этим свойством – *высота* $v$.

*Замечания.* 1) Корневой вектор высоты 1 = собственный вектор.

2) Пусть $v$ – корневой вектор высоты $k$ соответствующий $\lambda$. Тогда вектор $w = (\varphi - \lambda id)^{k-1}v$ – это собственный вектор, ибо $w \neq 0$, $(\varphi - \lambda id)w = (\varphi - \lambda id)^k v = 0$.

То есть в определении корневого вектора можно без ограничения общности считать, что $\lambda$ – собственное значение $\varphi$.
Положим $V_\lambda^k = V_\lambda^k(\varphi) := Ker(\varphi - \lambda id)^k$ – корневое подпространство векторов высоты $\leq k$, соответствующее $\lambda \in F$.
По определению, $\forall k \in \mathbb{N} : V_\lambda^{k-1} \subset V_\lambda^k$. Ясно, что $V_\lambda^1 = V_\lambda$ – собственное подпространство. Кроме того, $V_\lambda^0 = 0$. $V_\lambda^k \neq 0 \Leftrightarrow \lambda$ – собственное значение.
*Предложение.* Пусть $\lambda$ – собственное значение $\varphi$. Тогда $\exists m = m(\lambda) \in \mathbb{N} : 0 = V_\lambda^0 \underset{\neq}{\subset} V_\lambda^1 \underset{\neq}{\subset} ... \underset{\neq}{\subset} V_{lambda}^m = V_\lambda^{m+1} = ....$
*Доказательство:* Так как $\dim V < \infty$, то $\exists m : V_\lambda^m = V_\lambda^{m+1}$. Что дальше? Пусть $s \in \mathbb{N}, v \in V_\lambda^{m+s}$, то есть $(\varphi - \lambda id)^{m+1}(\varphi - \lambda id)^{s-1}v = 0 \Rightarrow (\varphi - \lambda id)^{s-1} \in V_\lambda^{m+1} = V_\lambda^m \Rightarrow (\varphi - \lambda id)^m(\varphi - \lambda id)^{s-1}v = 0 \Rightarrow v \in V_\lambda^{m+s-1}$. То есть $V_\lambda^{m+s} = V_\lambda^{m+s-1} = ... = V_\lambda^m$. $\square$
Итак, высоты корневых векторов, соответствующих $\lambda$, ограничены сверху числом $m(\lambda)$. Удобно рассмотреть $V_\lambda^\infty := \cup_k V_\lambda^k$ – корневое подпространство соответствующее $\lambda$. По доказанному, $V_\lambda^\infty = V_\lambda^{m(\lambda)}$. Однако $m(\lambda)$ заранее не известно, и $V_\lambda^\infty$ "не конкретизирует" $m(\lambda)$.
(NB: В бесконечномерном случае, конечно, предложение не верно!)
*Лемма.* $\forall k : \ (\varphi - \lambda id)V_\lambda^k \subset V_\lambda^{k-1}$
*Доказательство:* $v \in V_\lambda^k \Leftrightarrow (\varphi - \lambda id)^k v = 0$. То есть, $(\varphi - \lambda id)^{k-1}(\varphi - \lambda id)v = 0 \Rightarrow (\varphi - \lambda id)v \in V_\lambda^{k-1}$. $\square$
*Замечание.* Так как $V_\lambda^{k-1} \subset V_\lambda^k$, то, в частности , $V_\lambda^k$ инвариантно относительно $\varphi - \lambda id$.
*Упражнение.* $V_\lambda^k$ – инвариантно относительно $\varphi$.
Обсудим подробнее, как $\varphi$ действует на свои корневые подпространства.
Зафиксируем $\lambda$. Выберем базис $e_1, ..., e_{n_1}$ в $V_\lambda^1$. Дополним его, до базиса $e_1, ..., e_{n_2} \in V_\lambda^2$ ... $e_1, ..., e_n \in V_\lambda^\infty$.
При этом, если $e_j \in V_\lambda^k$, то $(\varphi - \lambda id)e_j \in V_\lambda^{k-1}$, то есть $(\varphi - \lambda id)e_j$ – линейная комбинация $e_i, i < j$. Поэтому матрица $\varphi - \lambda id|_{V_\lambda^\infty}$ в этом базисе имеет вид $\begin{pmatrix} 0 & & * \\ & 0 & \\ ... & ... & .... \\ 0 & & 0 \end{pmatrix}$, а значит матрица $\varphi$ – $\begin{pmatrix} \lambda & & * \\ & \lambda & \\ ... & ... & .... \\ 0 & & \lambda \end{pmatrix}$. Отсюда: *Предложение* $\chi_\varphi(\mu) = (\lambda - \mu)^n$(здесь $\varphi = \varphi|_{V_\lambda^\infty}$). *Следствие.* $\lambda$ – единственное собственное значение $\varphi|_{V_\lambda^\infty}$, то есть $\forall \mu \in F, \mu \neq \lambda, (\varphi - \mu id)_{V_\lambda^\infty}$ – невырожденный. *Предложение.* $\dim V_\lambda^\infty = \mathrm{Kp}_\lambda \chi_\varphi$.
*Доказательство:* Пусть $L = V_\lambda^\infty, n = \dim L$. Пусть $e_1, ..., e_n$ – базис в $L$. Дополним его до базиса $e_1, ..., e_r$ в $V$. Тогда $\varphi_e = \left(\begin{array}{c|c} P & Q \\ \hline 0 & R \end{array}\right)$, где $P$ – матрица $\varphi_L$, $R$ – матрица $\varphi_{V/L}$. Отсюда $\chi_\varphi(\mu) = \det(P - \mu E)\det(R - \mu E) = (\lambda - \mu)^n \chi_{\varphi_{V/L}}(\mu)$.

Осталось: почему $\lambda$ – не корень $\chi_{\varphi_{V/L}}$, то есть не собственное значение $\varphi_{V/L}$? Пусть $\xi \in V/L,\ \varphi_{V/L}(\xi) = \lambda\xi$. То есть $\xi = x + L,\ \varphi(x) + L = \lambda x + L$, то есть $(\varphi - \lambda id)x =: y \in L = V_\lambda^\infty$, значит $\exists k \in \mathbb{N} : (\varphi - \lambda id)^k(y) = 0$. Тогда $(\varphi - \lambda id)^{k+1}(x) = 0 \Rightarrow x \in L \Rightarrow \xi = 0$.□

*Замечания.* 1) В частности, отсюда (снова) $\dim V_\lambda^1 \le \mathrm{Kp}_\lambda\chi$. Общее: $\forall k :\ \dim V_\lambda^k \le \mathrm{Kp}_\lambda\chi$.

2) Если $\mathrm{Kp}_\lambda\chi = 1$, то (было) $\dim V_\lambda^1 = 1$, то есть $V_\lambda^\infty = V_\lambda^1$. То есть $m(\lambda) = 1$, и все нетривиальные векторы – собственные.

3) $m(\lambda) \le \mathrm{Kp}_\lambda\chi$, ибо: $0 = V_\lambda^0 \subsetneqq V_\lambda^1 \subsetneqq \ldots \subsetneqq V_\lambda^{m(\lambda)}$ ($\dim : 0 < \ldots < \mathrm{Kp}_\lambda\chi$). Всего $m(\lambda)$ "шагов", на каждом шаге dim растет на $\ge 1$. Наибольшее число "шагов" – это $\mathrm{Kp}_\lambda\chi$ (тогда рост равен 1 на любом шаге).

Снова зафиксируем собственное значение $\lambda$ линейного оператора $\varphi \in \mathrm{End}\ V$ и рассмотрим $\psi := (\varphi - \lambda \cdot \mathrm{id})_{V_\lambda^\infty}$, $\psi \in \mathrm{End}\ V_\lambda^\infty$. По определению, $\psi$ – *нильпотентен* , то есть $\exists m \in \mathbb{N} :\ \psi^m = 0$ (например, $m = m(\lambda)$ подойдет, ибо $V_\lambda^\infty = V_\lambda^{m(\lambda)}$).

*Предложение.* $\forall k \in \mathbb{N}$ линейный оператор $\psi$ естественно индуцирует *инъективный* линейный оператор $\widetilde{\psi} :\ V_\lambda^{k+1}/V_\lambda^k \to V_\lambda^k/V_\lambda^{k-1}$.

*Доказательство.* Было: $x \in V_\lambda^{k+1} \Rightarrow \psi(x) = (\varphi - \lambda \cdot \mathrm{id})(x) \in V_\lambda^k$. Определим $\widetilde{\psi}$ формулой $\widetilde{\psi}(x + V_\lambda^k) := \psi(x) + V_\lambda^{k-1}$.

1) Корректность: $x_1 + V_\lambda^k = x_2 + V_\lambda^k \overset{?}{\Rightarrow} \psi(x_1) + V_\lambda^{k-1} = \psi(x_2) + V_\lambda^{k-1}$; $x := x_1 - x_2$, то есть $x \in V_\lambda^k \overset{?}{\Rightarrow} \psi(x) \in V_\lambda^{k-1}$ – верно, ибо $\psi(x) = (\varphi - \lambda \cdot \mathrm{id})(x)$.

2) Линейность $\widetilde{\psi}$: упражнение.

3) Инъективность $\widetilde{\psi}$. Требуется доказать: $\mathrm{Ker}\ \widetilde{\psi} = 0$.

Итак, пусть $x \in V_\lambda^{k+1}, x + V_\lambda^k \in \mathrm{Ker}\ \widetilde{\psi}$, то есть $\psi(x) = (\varphi - \lambda \cdot \mathrm{id})(x) \in V_\lambda^{k-1}$. Требуется доказать $x + V_\lambda^k = 0 + V_\lambda^k$, то есть $x \in V_\lambda^k$. Но $(\varphi - \lambda \cdot \mathrm{id})^k(x) = (\varphi - \lambda \cdot \mathrm{id})^{k-1}\underbrace{(\varphi - \lambda \cdot \mathrm{id})(x)}_{\in V_\lambda^{k-1}} = 0$ по определению. □

Напомним, что если $\widetilde{\psi} \in \mathrm{Hom}\ (W_1, W_2)$ *инъективен* , то $\dim W_1 \le \dim W_2$ (ибо $\dim W_1 = \dim\ W_1/\mathrm{Ker}\ \widetilde{\psi} = \dim \mathrm{Im}\ \widetilde{\psi} \le \dim W_2$). То есть:

*Следствие.* Последовательность $d_k = d_k(\lambda) := \dim V_\lambda^k/V_\lambda^{k-1} = \dim V_\lambda^k - \dim V_\lambda^{k-1}$ – невозрастающая.

*Доказательство.* $d_{k+1} = \dim V_\lambda^{k+1}/V_\lambda^k \le \dim V_\lambda^k/V_\lambda^{k-1} = d_k$. То есть $\dim V_\lambda^k$ с ростом $k$ растет "с замедлением". □

Как связаны корневые векторы с различными собственными значениями?

*Предложение.* Пусть $v_1, \ldots, v_m$ – корневые векторы $\varphi$, $\lambda_1, \ldots, \lambda_m$ – их собственные значения, $\lambda_i \ne \lambda_j$ при $i \ne j$. Тогда $v_1, \ldots, v_m$ – линейно независимы.

*Доказательство.* Рассмотрим $c_1v_1 + \ldots + c_mv_m = 0$. Требуется доказать: $\forall i : c_i = 0$. Замена $v_i := c_iv_i$, то есть $v_i \in V^\infty_{\lambda_i}$. То есть дано: $v_1 + \ldots + v_m = 0, v_i \in V^\infty_{\lambda_i}$. Требуется доказать: $\forall i : \ v_i = 0$.

Индукция по $m$ (с тривиальной базой $m = 1$). $\exists k : \ (\varphi - \lambda_m \cdot \mathrm{id})^k v_m = 0$. Применим $(\varphi - \lambda_m \cdot \mathrm{id})^k$ к равенству $v_1 + \ldots + v_m = 0$, получим $v_1' + \ldots + v_m' = 0$, где $v_i' = (\varphi - \lambda_m \cdot \mathrm{id})^k(v_i)$. Докажем, что $\forall i : \ v_i' \in V^\infty_{\lambda_i}$. Для этого: $V^\infty_{\lambda_i}$ инвариантно относительно $\varphi \Rightarrow$ инвариантно относительно $(\varphi - \lambda_m \cdot \mathrm{id})^k$, то есть $v_i' \in V^\infty_{\lambda_i}$.

По предположению индукции, из $v_1' + \ldots + v_{m-1}' = 0$ следует $v_i' = 0 \ \forall i = 1, \ldots, m-1$. То есть $\forall i = 1, \ldots, m-1 : \ (\varphi - \lambda_m \cdot \mathrm{id})^k v_i = 0$. Если $i \neq m$, то $\varphi - \lambda_m \cdot \mathrm{id}$ невырожден (то есть обратим) на $V^\infty_{\lambda_i}$, то есть $v_i = 0$ при $i = 1, \ldots, m-1$. Тогда и $v_m = 0$. $\square$

*Упражнение.* 1) $(\varphi - \lambda \cdot \mathrm{id}) \circ (\varphi - \mu \cdot \mathrm{id}) = (\varphi - \mu \cdot \mathrm{id}) \circ (\varphi - \lambda \cdot \mathrm{id})$.

2) Если $\varphi \circ \psi = \psi \circ \varphi$, то $\varphi^k \circ \psi^l = \psi^l \circ \varphi^k$.

*Следствие.* Пусть $\lambda_1, \ldots, \lambda_m$ – собственные значения $\varphi$, $\lambda_i \neq \lambda_j$ при $i \neq j$. Тогда сумма подпространств $V^\infty_{\lambda_1}, \ldots, V^\infty_{\lambda_m}$ является прямой суммой.

*Доказательство.* Упражнение (дословно как для собственных).

*Следствие.* Пусть $\chi_\varphi$ разлагается на множители степени 1 над $F$, $\lambda_1, \ldots, \lambda_m$ – все собственные значения для $\varphi$ (без учета кратности, то есть $\lambda_i \neq \lambda_j$ при $i \neq j$). Тогда $V = V^\infty_{\lambda_1} \dotplus \ldots \dotplus V^\infty_{\lambda_m}$.

*Доказательство.* Уже знаем, что сумма – прямая, то есть $\dim\left(\sum V^\infty_{\lambda_i}\right) = \sum \dim V^\infty_{\lambda_i} = \sum \mathrm{Kp}_{\lambda_i}\chi_\varphi \underset{\text{разл. на множ.}}{=} \deg \chi_\varphi = \dim V \Rightarrow \sum V^\infty_{\lambda_i} = V$. $\square$

*Замечание.* $\varphi$ диагонализуем $\Leftrightarrow V = V^1_{\lambda_1} \dotplus \ldots \dotplus V^1_{\lambda_m}$. Так как a priori $V^1_\lambda \subset V^\infty_\lambda$, то $\varphi$ диагонализуем $\Leftrightarrow \forall \lambda : \ V^\infty_\lambda = V^1_\lambda \Leftrightarrow \forall \lambda : \ m(\lambda) = 1$.

Промежуточные итоги: если $\chi_\varphi$ разлагается на множители степени 1 над $F$, то $V = V^\infty_{\lambda_1} \dotplus \ldots \dotplus V^\infty_{\lambda_m}$, где $\forall i : \ V^\infty_{\lambda_i}$ – инвариантно относительно $\varphi$. Выберем базис в каждом из $V^\infty_{\lambda_i}$ и объединим; в полученном базисе $\varphi_e = \begin{pmatrix} A_1 & & O \\ & A_2 & \\ & & \ddots \\ O & & & A_m \end{pmatrix}$, где $A_i =$ матрица $\varphi_{V^\infty_{\lambda_i}}$. Если $\forall i : \ A_i$ – жорданова, то и $A = \varphi_e$ – жорданова. То есть надо научиться строить жорданов базис отднльно в $\forall \ V^\infty_\lambda$.

Для построения жорданова базиса: напоминание о терминологии, связанной с факторпространствами. Пусть $V$ – линейное пространство, $L$ – подпространство в $V$, $v_1, \ldots, v_m \in V$. $v_1, \ldots, v_m$ – *линейно независимы (полны, базис)* $\mod L$, если $v_1 + L, \ldots, v_m + L$ линейно независимы в факторпространстве $V/L$. То есть по определению $v_1, \ldots, v_m$ линейно независимы $\mod L$, $\Leftrightarrow$ если $\sum \lambda_i v_i \in L$, то $\forall i : \ \lambda_i = 0 \Leftrightarrow$ если $e_1, \ldots, e_r$ – базис в $L$, то $e_1, \ldots, e_r, v_1, \ldots, v_m$ – линейно независимы. То есть линейно независимы $\Leftarrow$ линейно независимы $\mod L$.

3.14.3. *Доказательство существования жорданова базиса.* Пусть $\varphi \in \operatorname{End} V$ таков, что $\chi_\varphi$ разлагается на множители степени 1 над $F$. Достаточно построить жорданов базис в каждом $V_\lambda^\infty$, где $\lambda$ – собственное значение $\varphi$. Вот *алгоритм* :

Рассмотрим $0 = V_\lambda^0 \subsetneqq V_\lambda^1 \subsetneqq \ldots \subsetneqq V_\lambda^{m-2} \subsetneqq V_\lambda^{m-1} \subsetneqq V_\lambda^m = \ldots$, $V_\lambda^m = V_\lambda^\infty$, $m = m(\lambda)$.

Шаг 1. Выберем базис в $V_\lambda^m \mod V_\lambda^{m-1}$ (то есть возьмем дополнение к базису в $V_\lambda^{m-1}$ до базиса в $V_\lambda^m$).

Шаг 2. 1) Применим $\varphi - \lambda \cdot \mathrm{id}$ к векторам, построенным на шаге 1. Получим векторы в $V_\lambda^{m-1}$. Так как линейное отображение $V_\lambda^m / V_\lambda^{m-1} \to V_\lambda^{m-1} / V_\lambda^{m-2}$, индуцированное $\varphi - \lambda \cdot \mathrm{id}$, *инъективно,* то эти векторы из $V_\lambda^{m-1}$ линейно независимы $\mod V_\lambda^{m-2}$. (Упражнение: $\psi \in \operatorname{Hom}(W_1, W_2)$ – инъективно, $w_1, \ldots, w_m \in W_1$ линейно независимы $\Rightarrow \psi(w_1), \ldots, \psi(w_m)$ – линейно независимы в $W_2$).

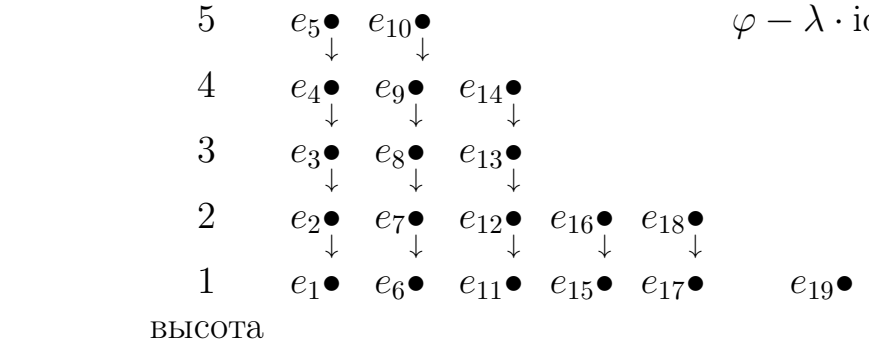
2) Дополним эти векторы до базиса в $V_\lambda^{m-1} \mod V_\lambda^{m-2}$.

Шаг 3. 1) Применим $\varphi - \lambda \cdot \mathrm{id}$ к векторам, построенным на шаге 2. Получим векторы в $V_\lambda^{m-2}$, линейно независимые $\mod V_\lambda^{m-3}$.

2) Дополним эти векторы до базиса в $V_\lambda^{m-2} \mod V_\lambda^{m-3}$. И так далее.

Последний шаг – это *Шаг m* : получаем базис в $V_\lambda^1 \mod V_\lambda^0 (= 0)$, то есть "просто" базис в $V_\lambda^1$.

*Пример.*




$0 = V_\lambda^0 \subsetneqq V_\lambda^1 \subsetneqq V_\lambda^2 \subsetneqq V_\lambda^3 \subsetneqq V_\lambda^4 \subsetneqq V_\lambda^5 = V_\lambda^6 = \ldots$

| dim | 0 | | 6 | | 11 | | 14 | | 17 | | 19 | | 19 | … |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| рост | | $\overbrace{\quad}$ | 6 | $\overbrace{\quad}$ | 5 | $\overbrace{\quad}$ | 3 | $\overbrace{\quad}$ | 3 | $\overbrace{\quad}$ | 2 | $\overbrace{\quad}$ | 0 | … |
| число жорд. кл. | | | $\underbrace{\quad}$ 1 | | $\underbrace{\quad}$ 2 | | $\underbrace{\quad}$ 0 | | $\underbrace{\quad}$ 1 | | $\underbrace{\quad}$ 2 | | | |

В каждой цепочке нумеруем векторы снизу вверх.

Построенные векторы образуют базис в $V_\lambda^m = V_\lambda^\infty$, ибо

1) векторы высоты 1 (построенные на шаге $m$) – базис в $V_\lambda^1$,

2) векторы высоты 2 (построенные на шаге $m-1$) – базис в $V_\lambda^2 \mod V_\lambda^1$.

Из 1) и 2) $\Rightarrow$ векторы высоты $1 \times 2$ – базис в $V_\lambda^2$;

3) векторы высоты 3 (построенные на шаге $m-2$) – базис в $V_\lambda^3 \mod V_\lambda^2$

$\Rightarrow$ векторы высоты $1 \times 2 \times 3$ – базис в $V_\lambda^3$, и так далее.

То есть векторы высоты $\leq k$ – базис в $V_\lambda^k$, $\quad \forall k = 1, 2, \ldots, m$.

Почему это *жорданов* базис? Рассмотрим одну из цепочек; пусть $k$ – ее высота.

| | По определению | То есть |
|---|---|---|
| $e_k \bullet$ | $(\varphi - \lambda \cdot \mathrm{id})(e_k) = e_{k-1}$ | $\varphi(e_k) = e_{k-1} + \lambda e_k$ |
| $\downarrow$ | | |
| $e_{k-1} \bullet$ | $(\varphi - \lambda \cdot \mathrm{id})(e_{k-1}) = e_{k-2}$ | $\varphi(e_{k-1}) = e_{k-2} + \lambda e_{k-1}$ |
| $\downarrow$ | | |
| $\ldots$ | $\ldots$ | $\ldots$ |
| $e_3 \bullet$ | $(\varphi - \lambda \cdot \mathrm{id})(e_3) = e_2$ | $\varphi(e_3) = e_2 + \lambda e_3$ |
| $\downarrow$ | | |
| $e_2 \bullet$ | $(\varphi - \lambda \cdot \mathrm{id})(e_2) = e_1$ | $\varphi(e_2) = e_1 + \lambda e_2$ |
| $\downarrow$ | | |
| $e_1$ | $(\varphi - \lambda \cdot \mathrm{id})(e_1) = 0$ | $\varphi(e_1) = \lambda e_1$ |

То есть матрица $\varphi$ на $\mathrm{Lin}\,\{e_1, \ldots, e_k\}$ в этом базисе – это жорданова клетка

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & 0 & \ldots & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & \ldots & 0 \\ \ldots & & \ldots & & \ldots & & \ldots \\ 0 & 0 & \ldots & 0 & 0 & \lambda & 1 \\ 0 & 0 & \ldots & 0 & 0 & 0 & \lambda \end{pmatrix} \text{ (размера } k \times k).$$

*Замечание.* Число жордановых клеток порядка $k$, соответствующих $\lambda$, равно числу цепочек высоты $k$, соответствующих $\lambda$, то есть равно $\dim V_\lambda^k / V_\lambda^{k-1} - \dim V_\lambda^{k+1} / V_\lambda^k = 2 \dim V_\lambda^k - \dim V_\lambda^{k-1} - \dim V_\lambda^{k+1}$.

*Пример* (конкретный). $\dim V = 5, e_1, e_2, e_3, e_4, e_5$ – базис в $V$.

$$\varphi_e = \begin{pmatrix} 2 & 0 & 3 & 4 & 5 \\ 0 & 2 & 0 & 3 & 4 \\ 0 & 0 & 2 & 0 & 3 \\ 0 & 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 0 & 2 \end{pmatrix}$$

Здесь $\lambda = 2, \mathrm{Kp}_\lambda \chi = 5$. Найдем корневые подпространства.

$$(\varphi - \lambda \cdot \mathrm{id})_e = \begin{pmatrix} 0 & 0 & 3 & 4 & 5 \\ 0 & 0 & 0 & 3 & 4 \\ 0 & 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow V_2^1 = \mathrm{Lin}\,\{e_1, e_2\}.$$

$$(\varphi - \lambda \cdot \mathrm{id})_e^2 = \begin{pmatrix} 0 & 0 & 0 & 0 & 9 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \end{pmatrix} \Rightarrow V_2^2 = \mathrm{Lin}\,\{e_1, e_2, e_3, e_4\}.$$

$(\varphi - \lambda \cdot \mathrm{id})_e^3 = 0 \Rightarrow V_2^3 = V.$
То есть имеем:

$$0 = \underset{0}{V_\lambda^0} \underset{2}{\subsetneq} \underset{\underset{0}{\smile}}{\underset{2}{V_\lambda^1}} \underset{2}{\subsetneq} \underset{\underset{1}{\smile}}{\underset{4}{V_\lambda^2}} \underset{1}{\subsetneq} \underset{\underset{1}{\smile}}{\underset{5}{V_\lambda^3}} = \underset{0}{V_\lambda^4} = \dots$$

То есть жорданова форма $\varphi$ – это $\varphi_u = \left(\begin{array}{ccc|cc} 2 & 1 & 0 & 0 & 0 \\ 0 & 2 & 1 & 0 & 0 \\ 0 & 0 & 2 & 0 & 0 \\ \hline 0 & 0 & 0 & 2 & 1 \\ 0 & 0 & 0 & 0 & 2 \end{array}\right)$.

Построим жорданов базис $u_1, u_2, u_3, u_4, u_5$.

$$\begin{array}{cc} \bullet u_3 & \\ \downarrow & \\ \bullet u_2 & \bullet u_5 \\ \downarrow & \downarrow \\ \bullet u_1 & \bullet u_4 \end{array}$$

Шаг 1. Выбираем $u_3$ – базис в $V_2^3 \mod V_2^2$.

Например, $u_3 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 0 \\ 1 \end{pmatrix} = e_5$

Шаг 2. 1) $u_2 = (\varphi - 2 \cdot \mathrm{id})u_3 = \begin{pmatrix} 5 \\ 4 \\ 3 \\ 0 \\ 0 \end{pmatrix} \in V_2^2$.

2) Выбираем $u_5$ так, чтобы $u_2, u_5$ – базис в $V_2^2 \mod V_2^1$.

То есть $u_5, u_2, \underbrace{e_1, e_2}_{\text{базис в } V_2^1}$ – базис в $V_2^2$. Например, $u_5 = \begin{pmatrix} 0 \\ 0 \\ 0 \\ 1 \\ 0 \end{pmatrix} = e_4$.

Шаг 3. $u_1 = (\varphi - 2 \cdot \mathrm{id})u_2 = \begin{pmatrix} 9 \\ 0 \\ 0 \\ 0 \\ 0 \end{pmatrix}$, $u_4 = (\varphi - 2 \cdot \mathrm{id})u_5 = \begin{pmatrix} 4 \\ 3 \\ 0 \\ 0 \\ 0 \end{pmatrix}$ – базис в $V_2^1$.

3.14.4. *Доказательство единственности жордановой формы.* Покажем, что если жордановы матрицы различны, то у соответствующих линейных операторов различные размерности корневых подпространств.

Для простоты обозначений отождествим линейные операторы и их матрицы (в фиксированном базисе).

1) Одна жорданова клетка: $J = \begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & \dots & 0 \\ \dots & & \dots & & \dots & & \dots \\ 0 & 0 & \dots & 0 & 0 & \lambda & 1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \lambda \end{pmatrix}$ порядка $s$. Тогда $\dim V_\lambda^k = k$ при $k = 1, \dots, s$; $\dim V_\lambda^k = s$ при $k > s$; кроме того, $V_\mu^k = 0\ \forall k$ при $\mu \neq \lambda$.

2) Пусть $A = \begin{pmatrix} J_1 & & & O \\ & J_2 & & \\ & & \ddots & \\ O & & & J_r \end{pmatrix}$, где $J_i$ – жордановы клетки. То есть $V = W_1 \dotplus \dots \dotplus W_r$, где $J_i : W_i \to W_i$. Тогда

$$A - \lambda E = \begin{pmatrix} J_1 - \lambda E & & & O \\ & J_2 - \lambda E & & \\ & & \ddots & \\ O & & & J_r - \lambda E \end{pmatrix},$$

$$(A - \lambda E)^k = \begin{pmatrix} (J_1 - \lambda E)^k & & & O \\ & (J_2 - \lambda E)^k & & \\ & & \ddots & \\ O & & & (J_r - \lambda E)^k \end{pmatrix}\ \forall k$$

(упражнение: проверить последнюю формулу). Если $x = \begin{pmatrix} x_1 \\ \vdots \\ x_r \end{pmatrix}$, где $x_i \in W_i$, то $(A - \lambda E)^k x = 0 \Leftrightarrow \forall i :\ (J_i - \lambda E)^k x_i = 0$. То есть $V_\lambda^k(A) = \operatorname{Ker}\,(A - \lambda E)^k = \operatorname{Ker}\,(J_1 - \lambda E)^k \dotplus \dots \dotplus \operatorname{Ker}\,(J_r - \lambda E)^k = V_\lambda^k(J_1) \dotplus \dots \dotplus V_\lambda^k(J_r)$; $\dim V_\lambda^k(A) = \sum_{i=1}^r \dim V_\lambda^k(J_i)$.

Пусть теперь $j_k = j_k(\lambda)$ – число жордановых клеток (среди $J_1, \dots, J_r$), соответствующих $\lambda$, и пусть $m = m(\lambda)$ – наибольший размер такой клетки. Тогда

$$\dim V_\lambda^1 = j_1 + j_2 + j_3 + \dots + j_m;$$
$$\dim V_\lambda^2 = j_1 + 2j_2 + 2j_3 + \dots + 2j_m;$$
$$\dim V_\lambda^3 = j_1 + 2j_2 + 3j_3 + \dots + 3j_m;$$
$$\dots \quad \dots \quad \dots$$

$$\dim V_\lambda^m = j_1 + 2j_2 + 3j_3 + \ldots + mj_m.$$

Отсюда $j_1, j_2, \ldots, j_m$ *однозначно* определяются по $\dim V_\lambda^k$, ибо

$$\begin{vmatrix} 1 & 1 & 1 & 1 & 1 & \ldots & 1 & 1 \\ 1 & 2 & 2 & 2 & 2 & \ldots & 2 & 2 \\ 1 & 2 & 3 & 3 & 3 & \ldots & 3 & 3 \\ 1 & 2 & 3 & 4 & 4 & \ldots & 4 & 4 \\ \ldots & & & \ldots & & \ldots & & \ldots \\ 1 & 2 & 3 & 4 & 5 & \ldots & m-1 & m \end{vmatrix} \neq 0$$

(упражнение: проверить это).

*Замечание.* Конечно, $j_k = 2\dim V_\lambda^k - \dim V_\lambda^{k-1} - \dim V_\lambda^{k+1}$; мы это извлекаем из конкретного алгоритма. Теперь знаем, что $j_k$ не зависит от способа построения жорданова базиса.

Что говорит наука о жордановой форме на языке матриц?

Пусть $A, B \in \mathrm{Mat}\,(n, F)$. Напомним, что $B$ *сопряжена* $A$, если $\exists T \in \mathrm{Mat}\,(n, F), \det T \neq 0 : B = T^{-1}AT$.

*Упражнение.* Отношение сопряженности является отношением эквивалентности.

Знаем, что $A, B$ сопряжены $\Leftrightarrow$ $A, B$ – матрицы одного линейного оператора в разных базисах.

Предположим, что поле $F$ *алгебраически замкнуто* (например, $F = \mathbb{C}$). Тогда основная теорема о жордановой форме означает:

**Теорема.** Любая матрица $A \in \mathrm{Mat}\,(n, F)$ сопряжена жордановой матрице (последняя единственна с точностью до порядка жордановых клеток).

*Следствие.* Пусть $A, B \in \mathrm{Mat}\,(n, F)$. Тогда $A, B$ сопряжены $\Leftrightarrow$ жордановы формы $A$ и $B$ (с точностью до порядка жордановых клеток) совпадают.

*Доказательство.* Упражнение. □

3.15. **Многочлены от линейного оператора (матрицы).** Пусть $V$ – линейное пространство над $F$, $\varphi \in \mathrm{End}\ V$.

Если $f \in F[t], f = a_m t^m + \ldots + a_2 t^2 + a_1 t + a_0$, то определим $f(\varphi) := a_m\varphi^m + \ldots + a_2\varphi^2 + a_1\varphi + a_0 \cdot \mathrm{id} \in \mathrm{End}\ V$.

Аналогично, если $A \in \mathrm{Mat}\,(n, F)$, то определим $f(A)$. Так как операции над линейными операторами и матрицами согласованы, то $f(\varphi)_e = f(\varphi_e)$ для любого базиса $e$.

*Упражнение.* $f_1, f_2 \in F[t] \Rightarrow (f_1 + f_2)(\varphi) = f_1(\varphi) + f_2(\varphi); (f_1 \cdot f_2)(\varphi) = f_1(\varphi) \cdot f_2(\varphi)$. То же для матриц.

Если $\dim V = n$, то $\dim \mathrm{End}\ V = n^2 < \infty$, то есть если $m \geq n^2$, то степени $\mathrm{id}, \varphi, \varphi^2, \ldots, \varphi^m$ линейно зависимы, то есть $\exists f \in F[t], f \neq 0 : f(\varphi) = 0$. Говорят, что $f$ – многочлен, аннулирующий $\varphi$.

Аннулирующий многочлен наименьшей степени – *минимальный* (аннулирующий) многочлен оператора $\varphi$. (Аналогично для матриц).

*Лемма.* Пусть $f \in F[t]$ – аннулирующий, $M$ – минимальный многочлен оператора $\varphi \in \operatorname{End} V$. Тогда $M \mid f$.

*Доказательство.* $f = M \cdot q + r,\ \deg r < \deg M;\ 0 = f(\varphi) = \underset{=0}{M(\varphi)} \cdot q(\varphi) + r(\varphi) \Rightarrow r(\varphi) = 0 \Rightarrow$ (минимальность $M$) $r = 0$. $\square$

В частности, минимальные многочлены делят друг друга $\Rightarrow$ минимальный иногочлен определен однозначно с точностью до постоянного множителя. Обозначим его $M_\varphi$. Обычно считают, что старший коэффициент $M_\varphi$ равен 1.

*Замечание* ("для умных"). Многочлены, аннулирующие $\varphi$ – это идеал в кольце $F[t]$. Так как $F[t]$ – кольцо главных идеалов, то этот идеал порождается некоторым многочленом. Это и есть $M_\varphi$.

Как находить минимальный многочлен? Для удобства изложения будем отождествлять линейные операторы с матрицами (то есть при фиксированном базисе $V \simeq F^n$, оператор действует умножением матрицы на столбец ...).

Начнем с жордановой клетки.

*Лемма 1.* Пусть $J = \begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & \dots & 0 \\ \dots & & \dots & & \dots & & \dots \\ 0 & 0 & \dots & 0 & 0 & \lambda & 1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \lambda \end{pmatrix} \in \operatorname{Mat}(n, F)$. Тогда $M_J = (t-\lambda)^n$.

*Доказательство.* Напомним: $J$ – матрица линейного оператора в базисе $\begin{matrix} \downarrow e_n \\ \vdots \\ \downarrow e_2 \\ e_1 \end{matrix}$, где $e_k$ – корневой вектор высоты $k$, соответствующий $\lambda$. В частности, $(J-\lambda E)^k e_k = 0,\ (J-\lambda E)^k e_l \neq 0$ при $k < l$. То есть $(J-\lambda E)^n = 0,\ (J-\lambda E)^k \neq 0$ при $k < n$. То есть $(t-\lambda)^n$ – аннулирующий, и все его (собственные) делители – не аннулирующие. То есть $M_J = (t-\lambda)^n$. $\square$

*Лемма 2.* Пусть матрица $A = \begin{pmatrix} J_1 & & & O \\ & J_2 & & \\ & & \ddots & \\ O & & & J_r \end{pmatrix}$ – блочно-диагональная. Тогда $M_A = \text{НОК}\ (M_{J_1}, M_{J_2}, \dots, M_{J_r})$.

*Доказательство.* Заметим, что $\forall f \in F[t]$ :

$f(A) = \begin{pmatrix} f(J_1) & & & O \\ & f(J_2) & & \\ & & \ddots & \\ O & & & f(J_r) \end{pmatrix}$ (сначала для степеней ...). То есть $f(A) = 0 \Leftrightarrow \forall i: \ f(J_i) = 0 \Leftrightarrow \forall i: \ M_{J_i} \mid f$. Многочлен наименьшей степени с этим свойством и есть НОК $(M_{J_1}, M_{J_2}, \ldots, M_{J_r})$. $\square$

С этого места будем считать, что $\chi_A$ *разлагается на множители степени* 1 *над полем* $F$ (например, $F$ – алгебраически замкнуто) – чтобы "работала" теорема о жордановой форме.

**Теорема.** Пусть $\lambda_1, \ldots, \lambda_m$ – все собственные значения $A$ (без учета кратности), $s_i$ – наибольший порядок жордановой клетки, соответствующей $\lambda_i$ в жордановой форме $A$. Тогда $M_A = \prod_i (t - \lambda_i)^{s_i}$.

*Доказательство.* Можно считать, что $A = \begin{pmatrix} J_1 & & & O \\ & J_2 & & \\ & & \ddots & \\ O & & & J_r \end{pmatrix}$, где все $J_i$ – жордановы клетки. Леммы 1 и 2 $\Rightarrow M_A = \text{НОК } (M_{J_1}, M_{J_2}, \ldots, M_{J_r}) = \prod_i (t - \lambda_i)^{s_i}$. $\square$

*Пример.* Если $A$ имеет жорданову форму $\begin{pmatrix} 2 & 1 & 0 & 0 \\ 0 & 2 & 0 & 0 \\ 0 & 0 & 2 & 0 \\ 0 & 0 & 0 & 3 \end{pmatrix}$, то $M_A = (t-2)^2(t-3))$.

*Пример.* Описание $A^3 = A^2$ : жорданова форма из $\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$, (0), (1).

*Следствие.* $A$ диагонализуем $\Leftrightarrow M_A$ не имеет кратных корней.

*Пример.* ($F$ – алгебраически замкнуто, char $F = 0$). Если $A^m = E$, то $A$ диагонализуем (почему?).

*Следствие* (**Теорема Гамильтона -Кэли** ). $\chi_A(A) = 0$.

*Доказательство.* В обозначениях предыдущей теоремы $\chi_A = \pm \prod_i (t - \lambda_i)^{k_i}$, где $k_i = \text{Кр}_{\lambda_i} \chi_A$ = сумма порядков жордановых клеток, соответствующих $\lambda_i$. То есть $s_i \leq k_i \ \forall i$. То есть $M_A \mid \chi_A$, что и требовалось доказать. $\square$

*Задача.* Докажите теорему Гамильтона-Кэли без предположения о том, что $\chi_A$ разлагается на линейные множители над $F$. Два способа: 1) расширение основного поля; 2) придать смысл "доказательству": $\chi_A(t) = \det(A - tE) \Rightarrow \chi_A(A) = \det(A - A) = 0$.

Как *практически* вычислить $f(A)$ (если $\deg f >> 0$)? Например, $A^m = ?$ ($m >> 0$). Для простоты предположим, что char $F = 0$ (+ пропуская предположения о $\chi_A$). Например, годится $F = \mathbb{C}$.

Способ 1: *использовать жорданову форму.* Именно, $B = T^{-1}AT$, где $B$ – жорданова (а $T$ – матрица перехода к жорданову базису), то есть $A = TBT^{-1}$. Тогда $A^m = TB^mT^{-1}$; более общо $f(A) = Tf(B)T^{-1}$ для любого многочлена $f$. Как найти $B^m$, и, более общо, $f(B)$?

Во-первых, $B = \begin{pmatrix} J_1 & & & O \\ & J_2 & & \\ & & \ddots & \\ O & & & J_r \end{pmatrix} \Rightarrow B^m = \begin{pmatrix} J_1^m & & & O \\ & J_2^m & & \\ & & \ddots & \\ O & & & J_r^m \end{pmatrix}$,

$f(B) = \begin{pmatrix} f(J_1) & & & O \\ & f(J_2) & & \\ & & \ddots & \\ O & & & f(J_r) \end{pmatrix}$, то есть все сводится к случаю одной жордановой клетки.

Итак, пусть $J = \begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 & 0 \\ 0 & \lambda & 1 & 0 & 0 & \dots & 0 \\ \dots & & \dots & & \dots & & \dots \\ 0 & 0 & \dots & 0 & 0 & \lambda & 1 \\ 0 & 0 & \dots & 0 & 0 & 0 & \lambda \end{pmatrix}$. Тогда

$$J^2 = \begin{pmatrix} \lambda^2 & 2\lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda^2 & 2\lambda & 1 & 0 & \dots & 0 \\ \dots & & \dots & & \dots & & \dots \\ 0 & 0 & \dots & 0 & \lambda^2 & 2\lambda & 1 \\ 0 & 0 & \dots & 0 & 0 & \lambda^2 & 2\lambda \\ 0 & 0 & \dots & 0 & 0 & 0 & \lambda^2 \end{pmatrix},$$

$$J^3 = \begin{pmatrix} \lambda^3 & 3\lambda^2 & 3\lambda & 1 & 0 & \dots & 0 & 0 \\ 0 & \lambda^3 & 3\lambda^2 & 3\lambda & 1 & 0 & \dots & 0 \\ \dots & & \dots & & \dots & & & \dots \\ 0 & 0 & \dots & 0 & \lambda^3 & 3\lambda^2 & 3\lambda & 1 \\ 0 & 0 & 0 & \dots & 0 & \lambda^3 & 3\lambda^2 & 3\lambda \\ 0 & 0 & \dots & 0 & 0 & 0 & \lambda^3 & 3\lambda^2 \\ 0 & 0 & \dots & 0 & 0 & 0 & 0 & \lambda^3 \end{pmatrix}, \text{ вообще}$$

$$J^m = \begin{pmatrix} \lambda^m & \binom{m}{1}\lambda^{m-1} & \binom{m}{2}\lambda^{m-2} & & \dots & \dots & \dots \\ & \lambda^m & \binom{m}{1}\lambda^{m-1} & \binom{m}{2}\lambda^{m-2} & & \dots & \dots \\ & & \lambda^m & \binom{m}{1}\lambda^{m-1} & \binom{m}{2}\lambda^{m-2} & \dots & \dots \\ \dots & & & & \dots & & \dots \\ O & & & & & \dots & \dots \end{pmatrix}$$ (упражнение: докажите индукцией по $m$).

Полезно заметить, что $\binom{m}{k}\lambda^{m-k} = \frac{m(m-1)\cdot\ldots\cdot(m-k+1)}{k!}\lambda^{m-k} = \frac{1}{k!}\left(\frac{d}{d\lambda}\right)^k \lambda^m$. Отсюда ($\forall$ многочлен $f$)

$f(J) = \begin{pmatrix} f(\lambda) & \frac{1}{1!}f'(\lambda) & \frac{1}{2!}f''(\lambda) & \dots & \frac{1}{(m-1)!}f^{(m-1)}(\lambda) \\ 0 & f(\lambda) & \frac{1}{1!}f'(\lambda) & \dots & \frac{1}{(m-2)!}f^{(m-2)}(\lambda) \\ \dots & & \dots & & \dots \\ \dots & & \dots & & \dots \end{pmatrix}$ (здесь $m$ – порядок матрицы $J$).

*Пример.* $A = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$. Собственное значение $\lambda = 2$ кратности 2. $A - 2E = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} \Rightarrow V_2^1$ – линейная оболочка $\begin{pmatrix} 1 \\ 1 \end{pmatrix}$, $V_2^2 = V$.

$\begin{matrix} \bullet e_2 \\ \downarrow \\ \bullet e_1 \end{matrix}$ $e_2 =$ (например) $\begin{pmatrix} 0 \\ 1 \end{pmatrix}$, $e_1 := (A - 2E)(e_2) = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. То есть, $T = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$, $T^{-1} = \begin{pmatrix} 1 & 0 \\ -1 & 1 \end{pmatrix}$, $B = \begin{pmatrix} 2 & 1 \\ 0 & 2 \end{pmatrix}$, $A = TBT^{-1}$.

$B^m = \begin{pmatrix} 2^m & m2^{m-1} \\ 0 & 2^m \end{pmatrix} \Rightarrow A^m = TB^mT^{-1} = 2^{m-1}\begin{pmatrix} -m+2 & m \\ -m & m+2 \end{pmatrix}$.

Способ 2: *использлвание аннулирующего многочлена + интерполяция.* Пусть $g$ – какой-либо аннулирующий многочлен для $A$, то есть $g(A) = 0, g \neq 0$. Хотим найти $f(A)$. Имеем $f = gq + r, \deg r < \deg g; f(A) = r(A)$. A priori годится $g = \chi_A$. Как найти $r$? (Прямое деление с остатком неудобно при $\deg f >> 0$).

Пусть $\lambda$ – корень $g$, $\mathrm{Kp}_\lambda g = k$. Тогда $\mathrm{Kp}_\lambda(f - r) \geq k$, то есть

$$f(\lambda) = r(\lambda),\ f'(\lambda) = r'(\lambda),\ \dots, f^{(k-1)}(\lambda) = r^{(k-1)}(\lambda) \quad (*)$$

(всего $k$ условий).

Если $g$ разлагается на множители степени 1, то $\sum \mathrm{Kp}_\lambda g = n = \deg g$. То есть для всех корней получаем $n$ условий.

**Теорема.** $\exists!$ многочлен $r, \deg r < n$, удовлетворяющий условиям $(*)$ для любого корня $g$. (Замечание: существенна единственность; существование ясно: $r =$ остаток от деления).

*Доказательство.* Рассмотрим $V = \{$многочлены степени $< n\}, \dim V = n$; $W = F^n, \dim W = n$. Рассмотрим отображение $\varphi : V \to W, \varphi : r \to$ упорядоченный набор $r(\lambda_1), r'(\lambda_1), \dots, r^{(k_1)}(\lambda_1), \dots$.

*Упражнение.* $\varphi$ – линейно.

Найдем $\mathrm{Ker}\ \varphi$. Если $r \in \mathrm{Ker}\ \varphi$, то $r(\lambda_1) = r'(\lambda_1) = \dots = r^{(k_1)}(\lambda_1) = \dots = 0$. То есть $r$ имеет $n$ корней с учетом кратности $\Rightarrow r = 0$. Итак, $\varphi$ – инъективно ($\Rightarrow$ единственность); $\dim W = \dim V \Rightarrow \varphi$ – биективно, то есть изоморфизм. $\square$

Многочлен $r$ решает *задачу интерполяции с кратными узлами.* Были частные случаи: 1) все кратности равны 1: "обычная" интерполяция; 2) единственное $\lambda$: формула Тейлора.

*Задача.* Придумайте "хороший" алгоритм поиска $r$.

*Пример.* $A = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$. Здесь $\lambda = 2$, кратность $= 2$. Берем $f(t) = t^m$. Ищем $r$ с условиями $r(2) = f(2) = 2^m,\ r'(2) = f'(2) = m2^{m-1}$. Ответ: $r = 2^m + m2^{m-1}(t-2) = m2^{m-1}t + (1-m)2^m$. Тогда $A^m = r(A) = m2^{m-1}A + (1-m)2^m E = 2^{m-1}\begin{pmatrix} -m+2 & m \\ -m & m+2 \end{pmatrix}$.

Обобщение:

3.16. **Функции от линейного оператора.** Пусть основное поле $F = \mathbb{R}$ или $\mathbb{C}$. Примем "матричную" точку зрения. Рассмотрим (для начала) так называемые *аналитические* функции, то есть $f(t) = \sum_{k=0}^{\infty} c_k t^k$. Точнее, $f(t) = \lim_{N\to\infty} \sum_{k=0}^{N} c_k t^k$ ("ряд сходится", то есть существует предел).

*Факт* о сходимости степенных рядов: рассмотрим $\sum_{k=0}^{\infty} c_k t^k$. Тогда $\exists R, 0 \le R \le \infty$, такое что если $|t| < R$, то ряд сходится; если $|t| > R$, то ряд расходится.

$R$ называется *радиусом сходимости* ряда; $|t| < R$ – интервал (над $\mathbb{R}$) или круг (над $\mathbb{C}$) сходимости.

Если $R > 0$, $f(t) := \sum_{k=0}^{\infty} c_k t^k$ при $|t| < R$, то функция $f$ (бесконечно) дифференцируема, причем $f'(t) = \sum_{k=1}^{\infty} k c_k t^{k-1}$ при $|t| < R$ (то есть тот же радиус сходимости для производной ряда).

*Задача* (из анализа). Докажите последний факт.

*Примеры.* 1) $e^t = \sum_{k=0}^{\infty} \frac{1}{k!} t^k;\ R = \infty$ (для доказательства можно использовать формулу Тейлора из анализа с оценкой остаточного члена).

2) $\frac{1}{1-t} = \sum_{k=0}^{\infty} t^k;\ R = 1$ ($\leftarrow$ Задача).

3) $\sum_{k=0}^{\infty} k! t^k;\ R = 0$.

Пусть $f(t) = \sum_{k=0}^{\infty} c_k t^k;\ A \in \mathrm{Mat}\ (n, F)$. Определим $f(A) := \sum_{k=0}^{\infty} c_k A^k = \lim_{N\to\infty} \sum_{k=0}^{N} c_k A^k$ (при условии, что предел существует; под пределом можно, например, понимать предел относительно каждого из матричных элементов).

*Замечание* (о сходимости). Пусть $A = (a_{ij}), a := \max_{ij} |a_{ij}|$.

*Упражнение.* Если $A^k = (b_{ij})$, то $|b_{ij}| \le n^{k-1} a^k \le (na)^k$.

Далее, если $R > 0$ – радиус сходимости ряда $f(t) = \sum_{k=0}^{\infty} c_k t^k$, то $f(A) := \sum_{k=0}^{\infty} c_k A^k$ гарантированно определена при $a < \frac{R}{n}$ (*Упражнение:* докажите). В частности, если $R = \infty$, то $f(A)$ определена для $\forall A$. Как вычислять $f(A)$? Оба способа обобщаются:

*Способ 1:* $A = TBT^{-1}$, где $B$ жорданова $\Rightarrow f(A) = Tf(B)T^{-1}$ (ибо умножение на матрицу непрерывно: проверьте, что если $B_N \to B$, то $TB_N T^{-1} \to TBT^{-1}$).

Далее, для жордановой клетки $J$ размера $m \times m$, соответствующей $\lambda$, имеем $f(J) = \begin{pmatrix} f(\lambda) & \frac{1}{1!}f'(\lambda) & \frac{1}{2!}f''(\lambda) & \dots & \frac{1}{(m-1)!}f^{(m-1)}(\lambda) \\ 0 & f(\lambda) & \frac{1}{1!}f'(\lambda) & \dots & \frac{1}{(m-2)!}f^{(m-2)}(\lambda) \\ \dots & & \dots & & \dots \\ \dots & & \dots & & \dots \end{pmatrix}$.

*Способ 2:* Берем *многочлен* $r, \deg r < n$, удовлетворяющий интерполяционным условиям $(*)$, и вычисляем $f(A) = r(A)$. (Для жордановой матрицы способ 2 = способ 1; в общем случае $A = TBT^{-1}$, и $f(A) = Tf(B)T^{-1} = Tr(B)T^{-1} = r(A)$).

*Замечание.* Эти формулы показывают, что можно определить $f(A)$ (любым из 2-х способов) для функции $f$, которая определена лишь (в окрестности) любого из собственных значений $\lambda$ матрицы $A$ и имеет там $k = \mathrm{Kp}\ _\lambda\chi$ производных.

*Пример.* $A = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}$. Найдем $e^{sA}$, где $s$ – (фиксированное) число. У нас $f(t) = e^{st}, f'(t) = se^{st}$, $\lambda = 2$, кратность $= 2$. То есть ищем многочлен $r(2) = f(2) = e^{2s}, r'(2) = f'(2) = se^{2s} \Rightarrow r(t) = e^{2s} + se^{2s}(t-2) = e^{2s}(st - 2s + 1)$. Отсюда $e^{sA} = r(A) = e^{2s}(sA + (1-2s)E) = e^{2s}\begin{pmatrix} -s+1 & s \\ -s & s+1 \end{pmatrix}$.

Зачем это? Например, вот зачем: функция $x(s) = e^{as}$ удовлетворяет $\frac{dx}{ds} = ax$; то же и для $x(s) = e^{as} \cdot C$, где $C$ – константа.

"Многомерный" аналог: пусть $x = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, где $x_i = x_i(s)$ – "вектор-функция"; $A \in \mathrm{Mat}\ (n, F)$. Тогда $x(s) = e^{sA} \cdot c$, где $c = \begin{pmatrix} c_1 \\ \vdots \\ c_n \end{pmatrix}$ – постоянная, удовлетворяет $\frac{dx}{ds} = Ax \leftarrow$ система линейных дифференциальных уравнений с постоянными коэффициентами.

*Пример.* $A = \begin{pmatrix} 1 & 1 \\ -1 & 3 \end{pmatrix}, x = \begin{pmatrix} x_1 \\ x_2 \end{pmatrix}, x_i = x_i(s)$. $\frac{dx}{ds} = Ax \Leftrightarrow \begin{cases} \frac{dx_1}{ds} = x_1 + x_2 \\ \frac{dx_2}{ds} = -x_1 + 3x_2 \end{cases}$.

Решим эту систему: $x = e^{sA} \cdot c = e^{2s}\begin{pmatrix} -s+1 & s \\ -s & s+1 \end{pmatrix}\begin{pmatrix} c_1 \\ c_2 \end{pmatrix} \Rightarrow \begin{matrix} x_1 = e^{2s}((c_2 - c_1)s + c_1) \\ x_2 = e^{2s}((c_2 - c_1)s + c_2) \end{matrix}$

Например, "начальное условие" $x(0) = \begin{pmatrix} 0 \\ 1 \end{pmatrix}$, то есть $x_1(0) = 0, x_2(0) = 1$. Тогда $c_1 = 0, c_2 = 1$, то есть $x_1 = se^{2s}, x_2 = (s+1)e^{2s}$.

3.17. **Билинейные функционалы.** Пусть $F$ – поле, $U, V, W$ – линейные пространства над $F$.

Отображение $B : U \times V \to W$ *билинейно* , если оно линейно относительно каждого из двух аргументов, то есть $B(\lambda_1 x_1 + \lambda_2 x_2, y) = \lambda_1 B(x_1, y) + \lambda_2 B(x_2, y)$; $B(x, \mu_1 y_1 + \mu_2 y_2) = \mu_1 B(x, y_1) + \mu_2 B(x, y_2)$.

*Билинейные функционалы (= билинейные формы)* на $V$ – это билинейные отображения $B : V \times V \to F$.

*Примеры.* 1) $B = 0$; 2) $V = \mathbb{R}^2$, $B =$ "стандартное" скалярное произведение; 3) $V = \mathbb{R}^2$, $B = \det$.

Координатная запись билинейных функционалов: пусть $e_1, \ldots, e_n$ – базис в $V$, $B$ – билинейный функционал на $V$. Рассмотрим $b_{ij} = B(e_i, e_j) \in F$. Получаем матрицу $B_e = (b_{ij}) \in \mathrm{Mat}\ (n, F)$. $B_e$ – *матрица билинейного функционала $B$ в базисе $e$.*

*Лемма.* Пусть $x, y \in V$, $x = \sum_i x_i e_i, y = \sum_j y_j e_j$. Тогда $B(x, y) = \sum_{i,j} b_{ij} x_i y_j$.

*Доказательство.* Упражнение. □

Заметим, что если рассмотреть $x_e = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}, y_e = \begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix}$, то $B(x, y) = x_e^T B_e y_e$ (здесь отождествляем $\mathrm{Mat}\ (1, F) = F$).

*Замечание.* Матрица $B_e$ однозначно определяется этим свойством. Ибо если $B(x, y) = x_e^T C y_e$, где $C = (c_{ij}) \in \mathrm{Mat}\ (n, F)$, то при $x = e_i, y = e_j$ получим $B(e_i, e_j) = c_{ij}$.

Пусть $\mathrm{Bilin}\ V =$ множество всех билинейных функционалов на $V$. Это – линейное пространство относительно естественных операций (упражнение). Тогда (при фиксированном базисе $e$) имеем $\mathrm{Bilin}\ V \to \mathrm{Mat}\ (n, F),\ B \to B_e$.

( $\mathrm{Bilin}\ (U \times V, W)$ –множество всех билинейных отображений $U \times V \to W$).

*Предложение.* Это изоморфизм линейных пространств.

*Доказательство.* Линейность: упражнение. Инъективность: из замечания выше. Сюръективность: $\forall C \in \mathrm{Mat}\ (n, F)$ рассмотрим $B(x, y) := x_e^T C y_e$. Упражнение: оно билинейно, $B_e = C$. □

*Замечание.* Умножение в $\mathrm{Mat}\ (n, F)$ не имеет естественной интерпретации в $\mathrm{Bilin}\ V$. Конечно, можно перемножать, но *зависит* от $e$!

Выясним зависимость $B_e$ от выбора базиса.

Пусть $e_1, \ldots, e_n$ и $e_1', \ldots, e_n'$ – базисы в $V$; пусть $P := T_{e \to e'}$ – матрица перехода. Пусть $B \in \mathrm{Bilin}\ V$.

*Предложение.* $B_{e'} = P^T B_e P$.

*Доказательство.* $B(x, y) = x_{e'}^T B_{e'} y_{e'}$; с другой стороны $x_{e'}^T P^T B_e P y_{e'} = x_e^T B_e y_e = B(x, y)$ (так как $y_e = P y_{e'}, x_e^T = (P x_{e'})^T = x_{e'}^T P^T$), что и требовалось доказать. □

*Замечание (связь с двойственностью).* Пусть $B \in \mathrm{Bilin}\ V$. Зафиксируем $y \in V$ и рассмотрим отображение $V \to F, x \to B(x, y)$. Это – линейный функционал

на $V$, то есть элемент $V^*$. То есть имеем отображение $\varphi : V \to V^*$, $\varphi(y) =$ этот линейный функционал, то есть $(x, \varphi(y)) := B(x, y)$.

*Упражнение.* $\varphi$ линейно, то есть $\varphi \in \mathrm{Hom}\,(V, V^*)$.

*Упражнение.* Этот функционал ($(x, \varphi(y)) = B(x, y)$) определяет изоморфизм между $\mathrm{Hom}\,(V, V^*)$ и $\mathrm{Bilin}\ V$.

Пусть теперь $e_1, \ldots, e_n$ – базис в $V$, $f_1, \ldots, f_n$ – *двойственный базис* в $V^*$. Пусть $\varphi_{f,\,e} = (a_{ij}) \in \mathrm{Mat}\,(n, F)$, то есть $\varphi(e_j) = \sum_i a_{ij} f_i$, откуда $a_{ij} = (e_i, \varphi(e_j)) = B(e_i, e_j)$. Итак, $B_e = \varphi_{f,\,e}$.

Отсюда еще раз получается формула преобразования $B_e$ при замене базиса, ибо $B_{e'} = \varphi_{f',\,e'} = T_{f' \to f} \varphi_{f,e}\, T_{e \to e'} =$ (было упражнение : $T_{f' \to f} = (T_{e \to e'})^T$) $= P^T \varphi_{f,\,e} P = P^T B_e P$.

Пусть $B \in \mathrm{Bilin}\ V$. Рассмотрим $B' : V \times V \to F$, $B'(x, y) = B(y, x)$. Очевидно, $B' \in \mathrm{Bilin}\ V$. При этом $(B')_e = (B_e)^T$.

Скажем, что $B$ *симметрично* , если $B' = B$, то есть $B(y, x) = B(x, y)$ $\forall x, y \in V$. Скажем, что $B$ *кососимметрично,* если $B' = -B$, то есть $B(y, x) = -B(x, y)$ $\forall x, y \in V$. На языке матриц это означает, что $B_e$ симметрична (или кососимметрична) (относительно главной диагонали).

*Упражнение* ($\mathrm{char}\ F \neq 2$). $\forall B \in \mathrm{Bilin}\ V$ $\exists!$ $B_1, B_2 \in \mathrm{Bilin}\ V$ : $B = B_1 + B_2$, $B_1$ – симметрично, $B_2$ – кососимметрично.

(Интерпретация: $\psi : \mathrm{Bilin}\ V \to \mathrm{Bilin}\ V, \psi : B \to B'$ – линейный оператор, $\psi^2 = \mathrm{id} \Rightarrow \ldots$).

Рассмотрим еще ранг матрицы билинейного функционала.

*Предложение.* $\mathrm{rank}\ B_e$ не зависит от выбора базиса $e$.

Обозначение: $\mathrm{rank}\ B := \mathrm{rank}\ B_e$.

*Доказательство.* Следует из формулы $B_{e'} = P^T B_e P$ и того, что ранг матрицы не меняется при умножении на невырожденную матрицу (с любой стороны). Упражнение: докажите.

Более "концептуальное" объяснение: пусть $\varphi : V \to V^*$ соответствует $B$. Тогда $\mathrm{rank}\ B_e = \mathrm{rank}\ \varphi_{f,e} = \dim \mathrm{Im}\ \varphi$ – не зависит от базиса. $\square$

3.17.1. *Квадратичные функционалы.* В этом разделе $\mathrm{char}\ F \neq 2$.

*Определение. Квадратичный функционал* (= квадратичная форма) на пространстве $V$ – это функция $Q : V \to F$ вида $Q(x) = B(x, x)$, где $B$ – некоторый билинейный функционал на $V$.

*Замечание.* Если $Q$ – квадратичный функционал, то $Q(\lambda x) = B(\lambda x, \lambda x) = \lambda^2 Q(x)$.

*Примеры.* $V = \mathbb{R}^2$ 1) $B =$"стандартное" скалярное произведение $\Rightarrow$ $Q(x) = x_1^2 + x_2^2$.

2) $B = \det \Rightarrow Q = 0$ (то же для любого кососимметричного) "Мораль": возможно, разные $B \rightsquigarrow$ одинаковым $Q$.

**Теорема.** Пусть $Q$ – квадратичный функционал на $V$. Тогда $\exists!$ *симметричный* билинейный функционал $B = B_Q$ такой, что $Q(x) = B_Q(x, x)$.

*Терминология.* $B_Q$ – *поляра* квадратичного функционала $Q$.

*Доказательство. Единственность:* Пусть $Q(x) = B(x, x)$, где $B$ – симметричный. Как восстановить $B$ по $Q$? $Q(x + y) = B(x + y, x + y) = \ldots \underset{\text{симм.}}{\Rightarrow} B(x, y) = \frac{1}{2}(Q(x + y) - Q(x) - Q(y))$.

*Существование:* Зададим $B(x, y) := \frac{1}{2}(Q(x+y)-Q(x)-Q(y))$. Тогда $B(y, x) = B(x, y)$, $B(x, x) = \frac{1}{2}(Q(2x) - 2Q(x)) = Q(x)$. Почему $B$ – билинейный? Нам дано, что $Q(x) = \widetilde{B}(x, x)$, где $\widetilde{B}$ – билинейный (не обязательно симметричный). Тогда $B(x, y) = \ldots = \frac{1}{2}(\widetilde{B}(x, y) + \widetilde{B}(y, x))$, то есть $B = \frac{1}{2}(\widetilde{B} + \widetilde{B}')$ – билинейный. $\square$

*Замечание.* Множество всех квадратичных функционалов на $V$ – линейное пространство (относительно естественных операций – проверьте!); теорема выше дает изоморфизм между этим пространством и подпространством симметрических билинейных форм в $\mathrm{Bilin}\, V$.
($\{$квадратичные функционалы на $V\} \simeq \{$симметрические билинейные функционалы на $V\}$).

Определим матрицу квадратичного функционала $Q$ (в базисе $e$) как матрицу его поляры, то есть $Q_e := (B_Q)_e$. Эта матрица автоматически симметрична. Если $B_Q(x, y) = x_e^T Q_e y_e = \sum_{i,j} b_{ij} x_i y_j$, то $Q(x) = x_e^T Q_e x_e = \sum_{i,j} b_{ij} x_i x_j \underset{b_{ij}=b_{ji}}{=} \sum_i b_{ii} x_i^2 + 2 \sum_{i<j} b_{ij} x_i x_j$.

*Пример.* $\dim V = 2$. $Q(x) = x_1^2 + 2x_1x_2 + 2x_2^2 \Rightarrow Q_e = \begin{pmatrix} 1 & 1 \\ 1 & 2 \end{pmatrix}$; $B_Q(x, y) = x_1y_1 + x_1y_2 + x_2y_1 + 2x_2y_2$.

Определим еще в любом базисе

**Теорема** (диагонализация квадратичного функционала). Пусть $Q$ – квадратичный функционал на линейном пространстве $V$. Тогда существует базис $e_1, \ldots, e_n$ в $V$ такой, что $Q_e = \begin{pmatrix} \lambda_1 & \ldots & 0 \\ & \ddots & \\ 0 & \ldots & \lambda_n \end{pmatrix}$ (в координатах: если $x = \sum_i x_i e_i$, то $Q(x) = \sum_i \lambda_i x_i^2$).

*Доказательство.* Используем координатный язык. Вот алгоритм (Лагранжа):

Имеем $Q = \sum_{i=1}^n q_{ii} x_i^2 + 2 \sum_{1 \le i < j \le n} q_{ij} x_i x_j$.

1) Пусть $q_{11} \neq 0$. Тогда $Q = q_{11}\left(x_1^2 + 2x_1\sum_{j=2}^n \frac{q_{1j}}{q_{11}}x_j + \left(\sum_{j=2}^n \frac{q_{1j}}{q_{11}}x_j\right)^2\right) - \underbrace{q_{11}\left(\sum_{j=2}^n \frac{q_{1j}}{q_{11}}x_j\right)^2 + \sum_{i=2}^n q_{ii}x_i^2 + 2\sum_{2\leq i<j\leq n} q_{ij}x_ix_j}_{=:Q_1}$.

Обозначим $a_{1j} := \frac{q_{1j}}{q_{11}}$, $y_1 := x_1 + \sum_{j=2}^n a_{1j}x_j$, $\lambda_1 = q_{11}$.

Тогда $Q = \lambda_1 y_1^2 + Q_1$, где $Q_1$ не содержит $x_1$ (то есть можно считать $Q_1$ определенным на $\mathrm{Lin}\,\{e_2, \ldots, e_n\}$, продолженным нулем на $\mathrm{Lin}\,\{e_1\}$). Далее индукция: $Q_1 = \lambda_2 y_2^2 + Q_2$, где $Q_2$ не содержит $x_1, x_2$, где $y_2 = x_2 + \sum_{j=3}^n a_{2j}x_j$, и так далее (это в предположении, что коэффициент у $Q_1$ при $x_2^2$ не равен нулю).

Итого: $Q = \lambda_1 y_1^2 + \ldots + \lambda_n y_n^2$, где

$$\begin{cases} y_1 = x_1 + a_{12}x_2 + a_{13}x_3 + \ldots + a_{1n}x_n \\ y_2 = \quad x_2 + a_{23}x_3 + \ldots + a_{2n}x_n \\ \ldots \quad \ldots \quad \ldots \quad \ldots \\ y_n = \quad x_n \end{cases},$$

то есть $\begin{pmatrix} y_1 \\ \vdots \\ y_n \end{pmatrix} = C\begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix}$, где $C = \begin{pmatrix} 1 & & * \\ & 1 & \\ & & \ddots \\ O & & 1 \end{pmatrix}$; $\det C = 1 \neq 0$. То есть $C = T_{u\to e}$, где $u_1, \ldots, u_n$ – базис с координатами $y_1, \ldots, y_n$.

2) Что, если $q_{11} = 0$? (более общо, нельзя применить случай 1) на каком-то шаге)?

а) $\exists i : q_{ii} \neq 0$. Перенумеруем $e_i \leftrightarrow e_1 \ldots$

б) $\forall i : q_{ii} = 0$, но $\exists i \neq j : q_{ij} \neq 0$. Переупорядочив, можно считать, что $q_{12} \neq 0$.

Вспомогательная замена $\begin{cases} x_1 = y_1 + y_2 \\ x_2 = y_1 - y_2 \\ x_3 = y_3 \\ \vdots \\ x_n = y_n \end{cases}$, при этом $\det\begin{pmatrix} 1 & 1 & & & \\ 1 & -1 & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \neq 0$. При этом $x_1x_2 = y_1^2 - y_2^2$ (больше $y_1^2$ не появится $\Rightarrow$ не уничтожится).

в) $q_{ij} = 0 \Rightarrow Q = 0 \Rightarrow$ тривиально. $\square$

*Следствие* (канонический вид квадратичной формы над полем $\mathbb{C}$). Пусть $V$ – линейное пространство над $\mathbb{C}, \dim V = n$, $Q$ – квадратичная форма в $V$. Тогда

существует базис $e_1, \ldots, e_n$ в $V$ такой, что

$$Q_e = \begin{pmatrix} 1 & & & & & O \\ & \ddots & & & & \\ & & 1 & & & \\ & & & 0 & & \\ & & & & \ddots & \\ O & & & & & 0 \end{pmatrix}, \quad \underbrace{\qquad\qquad}_{r}$$

где $r = \operatorname{rank} Q$ (то есть, если $x = \sum_{i=1}^{n} x_i e_i$, то $Q(x) = \sum_{i=1}^{r} x_i^2$).

*Доказательство.* Из теоремы следует, что $Q(x) = \sum_{i=1}^{r} \lambda_i y_i^2$, где $\lambda_i \in \mathbb{C}, \lambda_i \neq 0$ (при необходимости перенумеруем), $r \leq n$. $\exists \mu_i \in \mathbb{C} : \mu_i^2 = \lambda_i$. Тогда $x_i := \mu_i y_i$, и $Q = \sum_{i=1}^{r} x_i^2$ (то, что $r = \operatorname{rank} Q$, очевидно). $\square$

*Следствие* (канонический вид квадратичной формы над полем $\mathbb{R}$). Пусть $V$ – линейное пространство над $\mathbb{R}, \dim V = n$, $Q$ – квадратичная форма в $V$. Тогда существует базис $e_1, \ldots, e_n$ в $V$ такой, что

$$Q_e = \begin{pmatrix} 1 & & & & & & & O \\ & \ddots & & & & & & \\ & & 1 & & & & & \\ & & & -1 & & & & \\ & & & & \ddots & & & \\ & & & & & -1 & & \\ & & & & & & 0 & \\ & & & & & & & \ddots \\ O & & & & & & & 0 \end{pmatrix}, \quad \underbrace{\qquad}_{p} \underbrace{\qquad\qquad}_{q}$$

(то есть, если $x = \sum_{i=1}^{n} x_i e_i$, то $Q(x) = x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_{p+q}^2$).

*Доказательство.* $Q = \lambda_1 y_1^2 + \ldots + \lambda_p y_p^2 - \lambda_{p+1} y_{p+1}^2 - \ldots - \lambda_{p+q} y_{p+q}^2$, где $\lambda_i > 0$. $\mu_i = \sqrt{\lambda_i} \Rightarrow \ldots$ $\square$

*Задача.* 1) Тем самым получена классификация квадратичных функционалов над $\mathbb{C}$ (или симметрических билинейных), например, в следующем смысле: если $A_1, A_2$ – симметрические матрицы, то существует квадратичный функционал $Q$: $A_1$ и $A_2$ – матрицы $Q$ в различных базисах (или существует невырожденная $P : A_2 = P^T A_1 P$) $\Leftrightarrow \operatorname{rank} A_1 = \operatorname{rank} A_2$.

2) Можно (и бывает полезно) сменить точку зрения: выше *фиксирован* квадратичный функционал $Q$ и меняется базис; можно, наоборот, *фиксировать базис* и считать, что $A_1, A_2$ – матрицы различных $Q_1, Q_2$ в этом базисе. Если матрицы

$A_1, A_2$ связаны с помощью $A_2 = P^T A_1 P$, то $Q_1$ и $Q_2$ называются *эквивалентными* (или *изоморфными* ).

3) Еще полезнее сделать это в инвариантных терминах (ничего заранее не фиксируя): пусть $V_1, V_2$ – линейные пространства над $F$, $\varphi \in \mathrm{Hom}\,(V_1, V_2), B_2 \in \mathrm{Bilin}\ V_2$. Тогда возникает $B_1 \in \mathrm{Bilin}\ V_1, B_1(x,y) = B_2(\varphi(x), \varphi(y))$. Если $B_2$ – симметричный (кососимметричный), то $B_1$ тоже. Аналогично для квадратичных: $Q_1(x) = Q_2(\varphi(x))$.

Скажем, что $(V_1, B_1) \simeq (V_2, B_2)$, если существует изоморфизм $\varphi : V_1 \xrightarrow{\sim} V_2$ такой, что $B_1(x,y) = B_2(\varphi(x), \varphi(y))$. Аналогично для квадратичных функционалов.

Если $e_1, \ldots, e_n$ – базис в $V_1$, $u_1, \ldots, u_n$ – базис в $V_2$, то $B_1(x,y) = x_e^T (B_1)_e y_e$, $B_2(\varphi(x), \varphi(y)$ $(\varphi(x))_u^T (B_2)_u (\varphi(y))_u = x_e^T P^T (B_2)_u P y_e$, где $P = \varphi_{u,e}$. То есть ...

Что над $\mathbb{R}$? Очевидно, $p + q = \mathrm{rank}\ Q$ – инвариант $Q$ (не зависит от базиса). Оказывается, $p, q$ тоже не зависят (то есть получается *классификация* над $\mathbb{R}$). Сначала "назовем" крайние случаи.

*Определение.* Квадратичный функционал $Q$ на пространстве $V$ над полем $\mathbb{R}$ *положительно (отрицательно) определен* (обозначение: $Q > 0$ ($Q < 0$)), если для $\forall x \in V, x \neq 0 :\ \ Q(x) > 0$ ($Q(x) < 0$). (Иногда вводят понятие положительной/отрицательной *полуопределенности* $Q \geq 0$ ($Q \leq 0$)).

*Предложение* (закон инерции для квадратичных функционалов). В обозначениях предыдущего следствия $p, q$ – инварианты квадратичного функционала $Q$.

*Доказательство.* Так как $p+q = \mathrm{rank}\ Q$ – инвариант, то достаточно доказать для $p$. Покажем, что $p$ – наибольшая среди размерностей подпространств $L \subset V$ таких, что ограничение $Q_L > 0$ (то есть $Q(x) > 0\ \forall x \in L, x \neq 0$). Это определение $p$ не зависит от базиса.

Мы имеем $Q(x) = x_1^2 + \ldots + x_p^2 - x_{p+1}^2 - \ldots - x_{p+q}^2$, пусть $e_1, \ldots, e_p, e_{p+1}, \ldots, e_{p+q}, e_{p+q+1}, \ldots,$ – соответствующий базис в $V$.

1) Пусть $L := \mathrm{Lin}\ \{e_1, \ldots, e_p\}$. Тогда $Q_L > 0$.

2) Рассмотрим $M := \mathrm{Lin}\ \{e_{p+1}, \ldots, e_n\}$. Тогда $Q(x) \leq 0\ \forall x \in M$. С другой стороны, пусть $L' \subset V$ – какое-нибудь подпространство такое, что $Q_{L'} > 0$. Тогда $L' \cap M = 0$. То есть $n \geq \dim(L' + M) = \dim L' + \underbrace{\dim M}_{=n-p} \Rightarrow \dim L' \leq p$,

что и требовалось доказать. □

*Терминология.* $p$ – положительный индекс инерции $Q$, $q$ – отрицательный индекс инерции $Q$, $(p,q)$ – *сигнатура* $Q$.

Ясно, что $Q > 0 \Leftrightarrow$ сигнатура $Q$ есть $(n, 0)$ (где $n = \dim V$); $Q < 0 \Leftrightarrow$ сигнатура $Q$ есть $(0, n)$.

Имеются и условия , позволяющие проверить $Q > 0$ непосредственно по любой матрице $Q$.

**Теорема** (*критерий Сильвестра положительной определенности*). Пусть $V$ – линейное пространство над $\mathbb{R}$, $\dim V = n$, $Q$ – квадратичный функционал на $V$, $Q_e = \begin{pmatrix} q_{11} & q_{12} & \dots \\ \dots & \dots & \dots \\ & & \end{pmatrix}$ в некотором базисе $e$. Рассмотрим "главные диагональные миноры":

$$\Delta_1 := q_{11},\ \Delta_2 := \begin{vmatrix} q_{11} & q_{12} \\ q_{21} & q_{22} \end{vmatrix},\ \Delta_3 := \begin{vmatrix} q_{11} & q_{12} & q_{13} \\ q_{21} & q_{22} & q_{23} \\ q_{31} & q_{32} & q_{33} \end{vmatrix},\ \dots,\ \Delta_n := \det Q_e.$$

Тогда $Q > 0 \Leftrightarrow \forall k :\ \Delta_k > 0$.

*Замечание.* 1) На самом деле $Q > 0 \Leftrightarrow$ *все* диагональные миноры $Q_e$ положительны (надо переупорядочить базисные векторы).

2) $Q < 0 \Leftrightarrow \Delta_1 < 0, \Delta_2 > 0, \Delta_3 < 0, \dots$ (то есть $\forall k :\ (-1)^k \Delta_k > 0$). Та же оговорка про *все* диагональные миноры.

*Упражнение.* Проверьте $Q > 0 \Leftrightarrow -Q < 0$.

*Доказательство.* Индукция по $n$ с очевидной базой $n = 1$. Переход $n-1 \rightsquigarrow n$ : $Q = \sum q_{ij} x_i x_j = Q_1 + 2\sum_{i=1}^{n-1} q_{in} x_i x_n + q_{nn} x_n^2$, где $Q_1$ зависит лишь от $x_1, \dots, x_{n-1}$; $Q_1$ = ограничение $Q$ на подпространство $x_n = 0$ (то есть $\mathrm{Lin}\ \{e_1, \dots, e_{n-1}\}$). Отметим, что главные диагональные миноры $Q_1$ – это $\Delta_1, \Delta_2, \dots, \Delta_{n-1}$.

$\Rightarrow$: Если $Q > 0$, то тем более $Q_1 > 0$. Индуктивное предположение к $Q_1 \Rightarrow \Delta_k > 0\ \forall k < n$. Далее $\Delta_n = \det Q_e$. Так как $Q > 0$, то существует базис $u$ такой, что $Q_u = E = \begin{pmatrix} 1 & & O \\ & 1 & \\ & & \ddots \\ O & & 1 \end{pmatrix}$; $Q_e = P^T Q_u P = P^T P$, где $P = T_{u \to e}$ и $\det Q_e = (\det P)^2 > 0$.

$\Leftarrow$: Пусть $\forall k = 1, \dots, n :\ \Delta_k > 0$. Тогда по предположению индукции $Q_1 > 0$ $\Rightarrow$ в некотором (новом) базисе $Q_1 = \sum_{i=1}^{n-1} y_i^2$. Положим $y_n := x_n$, то есть $Q = Q_1 + 2\sum_{i=1}^{n-1} c_{in} y_i y_n + c_{nn} y_n^2$ (здесь $c_{nn} = q_{nn}$, $c_{in}$ линейно выражается через $q_{in}$).

Напишем $y_i^2 + 2c_{in} y_i y_n = (y_i + c_{in} y_n)^2 - c_{in}^2 y_n^2$ и положим $z_i = y_i + c_{in} y_n$ $(i = 1, \dots, n-1)$, $z_n = y_n$. Тогда $Q = \sum_{i=1}^{n-1} z_i^2 + c z_n^2$ для некоторого $c \in \mathbb{R}$. Почему $c > 0$? Пусть $v$ – базис с координатами $z_1, \dots, z_n$; $Q_v = \begin{pmatrix} 1 & & & O \\ & 1 & & \\ & & \ddots & \\ & & & 1 \\ O & & & c \end{pmatrix}$.

Тогда $c = \det Q_v = (\det P)^2 \cdot \det Q_e = (\det P)^2 \cdot \Delta_n > 0$. $\square$

*Замечание.* Если, в обозначениях из критерия Сильвестра, предположить, что $\Delta_k \neq 0\ \forall k$, то можно доказать, что в некотором базисе $Q = \Delta_1 y_1^2 + \frac{\Delta_2}{\Delta_1} y_2^2 + \frac{\Delta_3}{\Delta_2} y_3^2 + \ldots + \frac{\Delta_n}{\Delta_{n-1}} y_n^2$; имеется алгоритм (Якоби). Отсюда: 1) следует критерий Сильвестра; 2) можно обобщить : знаки $\Delta_k$ определяют сигнатуру $Q$ (как?). Доказательство: задача (или см., например, Гельфанд, Лекции по линейной алгебре, или Винберг, Курс алгебры).

3.18. **Полуторалинейные и эрмитовы квадратичные функционалы.** Пусть $F = \mathbb{C}$. Имеется версия рассказанного выше, использующая комплексное сопряжение. Пусть $V$ – линейное пространство над $\mathbb{C}$, $\dim V = n$.

*Определение. Полуторалинейный функционал (= полуторалинейная форма)* на $V$ – это функция $B : V \times V \to \mathbb{C}$, линейная по первой координате и *антилинейная* (или *полулинейная* ) по второй (NB: иногда наоборот), то есть

$$B(\lambda_1 x_1 + \lambda_2 x_2, y) = \lambda_1 B(x_1, y) + \lambda_2 B(x_2, y);$$

$$B(x, \mu_1 y_1 + \mu_2 y_2) = \bar{\mu_1} B(x, y_1) + \bar{\mu_2} B(x, y_2).$$

*Упражнение.* "Общий вид" полуторалинейного функционала: $B(x, y) = \sum_{i,j} b_{ij} x_i \bar{y}_j$, где $b_{ij} \in \mathbb{C}$, $x_i$ (соответственно $y_j$) – координаты $x$ (соответственно $y$) в некотором базисе (тогда $(b_{ij})$ – *матрица* $B$ ).

*Замечания.* 1) Подобно билинейному случаю, $B(x, y) = (x, \varphi(y))$, где $\varphi(y) \in V^*$. Получаем $\varphi : V \to V^*$ – *полулинейный* , то есть $\varphi(y_1 + y_2) = \varphi(y_1) + \varphi(y_2)$, $\varphi(\mu y) = \bar{\mu}\varphi(y)$. Так получена биекция (и даже изоморфизм) между пространствами полуторалинейных функционалов на $V$ и полулинейных отображений $V \to V^*$.

2) Рассмотрим в $V$ "новое" умножение на скаляр: $\lambda \circ x := \bar{\lambda} x$. Полученное линейное пространство обозначим $\overline{V}$ (*как множество* $V = \overline{V}$, но ...). Тогда полулинейное отображение $V \to V^*$ – это *линейное* $\overline{V} \to V^*$ (или $V \to \overline{V^*}$). Точно так же полуторалинейный функционал – это *билинейное* отображение $V \times \overline{V} \to \mathbb{C}$.

*Упражнение.* Убедитесь, что $\overline{V^*}$ и $\overline{V}^*$ – не одно и то же, но между этими пространствами существует канонический изоморфизм (ответ: $\overline{V}^*$ = полулинейные функционалы на $V$ (с обычным умножением на скаляр)); $\overline{V^*}$ = линейные функционалы на $V$ (с "сопряженным" умножением на скаляр); $\overline{V}^* \xrightarrow{\sim} \overline{V^*}$ задается комплексным сопряжением.

3) В том, что выше (и в большинстве ниже) можно заменить $\mathbb{C}$ на поле $F$ с заданным автоморфизмом ("инволюцией") $\sigma : \lambda \to \bar{\lambda}$ таким, что $\sigma^2 = \mathrm{id}$, $\sigma \neq \mathrm{id}$. При этом роль $\mathbb{R}$ играет подполе неподвижных элементов $\sigma$.

*Определение.* Полуторалинейный функционал $B$ – *эрмитов (=эрмитово-симметричный)*, если $B(y, x) = \overline{B(x, y)} \quad \forall x, y$.

*Упражнение.* $B$ – эрмитово-симметричен $\Leftrightarrow b_{ji} = \overline{b_{ij}} \quad \forall i, j$ (в частности $b_{ii} \in \mathbb{R}\ \forall i$).

*Замечание.* Можно определить "косоэрмитовы": $B(y,x) = -\overline{B(x,y)}$. Однако $B$ – эрмитов $\overset{\text{Упр.}}{\Leftrightarrow}$ $iB$ – косоэрмитов (вместо $i$ годится $\lambda$, $\bar{\lambda} = -\lambda$). То есть "ничего нового" (в отличие от билинейного случая, где такой связи нет).

*Определение.* Функция вида $Q(x) = B(x,x)$, где $B$ – *эрмитов* полуторалинейный функционал, называется *эрмитово квадратичным* функционалом (в частности, $Q(x) \in \mathbb{R} \quad \forall x \in V$, то есть $Q : V \to \mathbb{R}$).

*Задача.* Эрмитов функционал $B$ со свойством $Q(x) = B(x,x)$ определен по $Q$ *однозначно* (и называется полярой). (Как его найти? Аналог формулы поляризации?)

Итак, $Q(x) = \sum_{i,j} b_{ij} x_i \bar{x_j} = \sum_{i=1}^n b_{ii}|x_i|^2 + \sum_{i \neq j} b_{ij} x_i \bar{x_j} = \sum_{i=1}^n b_{ii}|x_i|^2 + 2\text{Re} \sum_{1 \leq i < j \leq n} b_{ij} x$ (так как $b_{ij} x_i \bar{x_j} + b_{ji} x_j \bar{x_i} = b_{ij} x_i \bar{x_j} + \overline{b_{ij} x_i \bar{x_j}} = 2\text{Re}\ b_{ij} x_i \bar{x_j}$).

*Задача.* Пусть $Q$ эрмитово квадратичный функционал. Тогда существует базис в $V$, в котором $Q(x) = |x_1|^2 + \ldots + |x_p|^2 - |x_{p+1}|^2 - \ldots - |x_{p+q}|^2$, причем $p, q$ - инварианты $Q$ ("эрмитов закон инерции"). (NB: здесь существенны $\mathbb{C}$ и $\mathbb{R}$). *Указание:* можно модифицировать алгоритм Лагранжа на основе $|a+b|^2 = |a|^2 + 2\text{Re}\ a\bar{b} + |b|^2$.

Точно так же, как и для квадратичных функцмоналов над $\mathbb{R}$; $Q > 0 \overset{def}{\Leftrightarrow} \forall x \in V \setminus \{0\} \quad Q(x) > 0$. При этом $Q > 0 \Leftrightarrow$ "сигнатура" $Q$ – это $(n, 0)$.

3.19. **Геометрия пространства с "метрикой".** Пусть $V$ – линейное пространство над $F$, $\text{char}\ F \neq 2, \dim V = n < \infty$. Под *"метрикой"* (смысл: $B(x,x)$ как "квадрат длины $x$" ) мы будем здесь понимать один из следующих вариантов:

(1) билинейный симметрический функционал;

(2) билинейный кососимметрический функционал;

(3) при $F = \mathbb{C}$ (или $F$ с инволюцией) полуторалинейный эрмитов функционал.

Коротко: (1) – симметрический случай; (2) – кососимметрический случай: (3) – эрмитов случай.

Итак, пусть $B$ – "метрика" в $V$. Все дальнейшее зависит от выбора $B$. (Но, как правило, $B$ будет фиксироваться, то есть не будет более одной "за раз").

Будем говорить, что $B$ – *невырождена,* если $\text{rank}\ B = n (= \dim V)$, то есть матрица $B$ невырождена. Напомним, что $B(x,y) = (x, \varphi(y))$, где $\varphi = \varphi_B : V \to V^*$ линейный (или полулинейный). Тогда $B$ невырождена $\Leftrightarrow$ $\varphi$ невырожден (то есть изоморфизм $V \to V^*$ (или $\overline{V^*}$)).

Пусть $x, y \in V$. Говорят, что $x, y$ – *ортогональны* относительно $B$, если $B(x,y) = 0$. Заметим, что, по условию, $B(x,y) = 0 \Leftrightarrow B(y,x) = 0$.

*Замечание.* Вообще говоря, не исключено, что $B(x,x)=0$ при $x\neq 0$ даже для невырожденной $B$. Такие $x$ – *изотропные векторы.* Например, так *всегда* в кососимметрическом случае! Примеры в симметрическом случае ($n=2$):

1) $F=\mathbb{C}$, $B(x,y)=x_1y_1+x_2y_2,\ x=(1,i)$.

2) $F=\mathbb{R}$, $B(x,y)=x_1y_1-x_2y_2,\ x=(1,1)$.

Пусть $L$ – подпространство в $V$. Обозначим $L^\perp=L^\perp_B:=\{x\in V\mid B(x,y)=0\quad\forall y\in L\}$ – *"ортогональное дополнение"* к $L$ относительно $B$.

*Замечание.* 1) $L^\perp=\{x\in V\mid (x,\varphi(y))=0\quad\forall y\in L\}=\varphi(L)^0$. В частности, $L^\perp$ – подпространство в $V$. Еще в частности $V^\perp=(\operatorname{Im}\varphi)^0$. То есть $V^\perp=0\Leftrightarrow\operatorname{Im}\varphi=V^*\Leftrightarrow B$ – невырождена. (*Упражнение:* "на самом деле" $V^\perp=\operatorname{Ker}\varphi$).

2) $\dim L^\perp=\dim\varphi(L)^0=n-\dim\varphi(L)\geq(\dim\varphi(L)\leq\dim L)\geq n-\dim L$, то есть $\dim L+\dim L^\perp\geq n(=\dim V)$.

*Предложение.* Пусть $B$ – невырождена. Тогда для любого подпространства $L\subset V:\dim L^\perp=n-\dim L$.

*Доказательство.* $B$ невырождена $\Leftrightarrow\varphi$ – изоморфизм, а тогда для любого $L:\dim\varphi(L)=\dim L$, то есть ... $\square$

Рассмотрим $L^{\perp\perp}=\left(L^\perp\right)^\perp$ (точнее, $\left(L^\perp_B\right)^\perp_B$). По определению $L^{\perp\perp}\supset L$.

*Предложение.* Если $B$ невырождена, то для любого подпространства $L\subset V$: $L^{\perp\perp}=L$.

*Доказательство.*

$$\left.\begin{array}{c}\dim L^{\perp\perp}=n-\dim L^\perp=n-(n-\dim L)=\dim L\\ L^{\perp\perp}\supset L\end{array}\right\}\Rightarrow L^{\perp\perp}=L.$$

$\square$

*Упражнение.* Пусть $B$ произвольная. При каком условии на $L:L^{\perp\perp}=L$?

Даже в невырожденном случае *не обязательно* $L\cap L^\perp=0$ (например, из-за изотропных векторов: если $L=\operatorname{Lin}\{x\}$, где $x$ изотропный, то $L\subset L^\perp$). То есть сумма $L$ и $L^\perp$ *не обязательно* прямая.

*Предложение.* Пусть $L$ – подпространство в $V$. Следующие условия эквивалентны: (1) $V=L\dot{+}L^\perp$; (2) $L\cap L^\perp=0$; (3) Ограничение $B$ на $L$ невырожденно.

*Доказательство.* (1) $\Rightarrow$ (2): было ($L^\perp$ не при чем: для любых подпространств...)

(2) $\Rightarrow$ (1): $L\cap L^\perp=0\Rightarrow$ сумма $L+L^\perp$ – прямая сумма. Далее, $\dim(L+L^\perp)=\dim L+\dim L^\perp\geq n\Rightarrow=n$, и $V=L\dot{+}L^\perp$.

(2) $\Leftrightarrow$ (3): $L\cap L^\perp=$ векторы из $L$, $B$-ортогональные для любого вектора из $L$. $\square$

*Замечание.* Если $L\subset V$ – подпространство, то невырожденность $B$ на всем $V$ и невырожденность $B$ на $L$, вообще говоря, непосредственно не связаны. Например:

1) $B=\begin{pmatrix}1&0\\0&0\end{pmatrix}$ вырожден на $V=F^2$, невырожден на $L=\operatorname{Lin}\{\begin{pmatrix}1\\0\end{pmatrix}\}$.

2) $B = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$ невырожден на $V = F^2$, вырожден на $L = \mathrm{Lin}\{\begin{pmatrix} 1 \\ -1 \end{pmatrix}\}$.

Если $B(x, y) = (x, \varphi(y))$, где $\varphi : V \to V^*$; $B_L$ – ограничение $B$ на $L \subset V$, то $B_L \leftrightarrow \varphi_L$, где (упражнение) $\varphi_L : L \xrightarrow{i} V \to V^* \xrightarrow{i^*} L^*$ (последнее отображение – ограничение на $L$). То есть то, что $\varphi$ – изоморфизм, не означает (вообще говоря), что $\varphi_L$ – изоморфизм (тем более наоборот).

*Замечание.* Пусть $V = L \dotplus L^\perp$, $e_1, \ldots, e_m$ – базис в $L$, $e_{m+1}, \ldots, e_n$ – в $L^\perp$. Тогда $B_e = \left(\begin{array}{c|c} (B_L)_e & O \\ \hline O & (B_{L^\perp})_e \end{array}\right)$, причем $\det(B_L)_e \neq 0$.

Вернемся к вопросам *классификации* с геометрической точки зрения.

Напомним, что $(V_1, B_1) \simeq (V_2, B_2) \Leftrightarrow$ существует изоморфизм $\psi : V_1 \xrightarrow{\sim} V_2$ такой, что $B_1(x, y) = B_2(\psi(x), \psi(y)) \quad \forall x, y \in V_1$. Терминология: $B_1$ и $B_2$ эквивалентны, или: $V_1, V_2$ *изометричны* ($\psi$ – "изометрия").

*Упражнение.* Пусть $B_i \leftrightarrow \varphi_i : \ V_i \to V_i^*$. Что означает изометричность "на языке $\varphi_1, \varphi_2$"? (Ответ: $\varphi_1 = \psi^* \varphi_2 \psi$).

На языке матриц: $A_1 = P^* A_2 P$, где $P^* = P^T$ в билинейном случае, $P^* = \overline{P^T}$ в полуторалинейном случае. (Упражнение: проверьте!)

Альтернативно (при $V_1 = V_2$) можно считать в формуле $A_1 = P^* A_2 P$, что $A_1, A_2$ – матрицы $B$ в разных базисах, $P$ – матрица перехода.

*Определение.* Базис $e_1, \ldots, e_n \in V$ *ортогонален* относительно $B$, если $B(e_i, e_j) = 0 \quad \forall i \neq j$ (то есть базисные векторы попарно ортогональны).

По определению, если базис $e$ ортогонален, то $B_e$ диагональна. То есть знаем, что в симметрическом случае ортогональный базис всегда существует (и в принципе есть алгоритм). Аналогично в эрмитовом случае (Задача).

Дальнейшая классификация зависит от основного поля $F$; (во многом – от структуры квадратов в $F$). Напомним, что в *симметрическом случае* :

1) $F = \mathbb{C} : (V_1, B_1) \simeq (V_2, B_2) \Leftrightarrow \dim V_1 = \dim V_2, \ \mathrm{rank}\ B_1 = \mathrm{rank}\ B_2$.

1) $F = \mathbb{R} : (V_1, B_1) \simeq (V_2, B_2) \Leftrightarrow \dim V_1 = \dim V_2,$ сигнатура $B_1 =$ сигнатура $B_2$.

В эрмитовом случае $F = \mathbb{C}$ $(V_1, B_1) \simeq (V_2, B_2) \Leftrightarrow \dim V_1 = \dim V_2,$ сигнатура $B_1 =$ сигнатура $B_2$. (Задача).

3.20. **Классификация кососимметрических (= симплектических) "метрик".** Оказывается, ответ *не зависит* от $F$ ($\mathrm{char}\ F \neq 2$)!

Надежды на ортогональный базис нет: *кососимметрический* $B$ обладает ортогональным базисом $\Leftrightarrow B \equiv 0$ (Упражнение).

**Теорема.** Пусть $B$ – кососимметрический билинейный функционал в $V$. Тогда существует базис $e_1, \ldots, e_n$ в $V$, такой что

$$B_e = \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & & & & O \\ & \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & & & \\ & & \ddots & & \\ & & & \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & \\ O & & & & 0 \\ & & & & & \ddots \\ & & & & & & 0 \end{pmatrix}.$$

То есть $B(e_1, e_2) = 1 = B(e_3, e_4) = \ldots = B(e_{2k-1}, e_{2k}), \quad (B(e_2, e_1) = -1 = \ldots)$ (остальное равно нулю).

*Терминология:* такой базис – *симплектический* .

*Следствие.* rank $B$ – четен.

*Доказательство теоремы.* 1) $B = 0$ – тривиально.

2) Индукция по $n = \dim V$. База $n = 1$ тривиальна (почему?). Переход: если $B \neq 0$, то $\exists x, y \in V : B(x, y) \neq 0$. $B$ – кососимметричен $\Rightarrow$ $x, y$ линейно независимы. Домножая на скаляр, можно считать, что $B(x, y) = 1$. (то есть если $B(x, y) = \lambda$, то $B(x, \frac{1}{\lambda} y) = 1 \ldots$).

Положим $e_1 = x, e_2 = y, L = \text{Lin}\,\{x, y\}$. Тогда $(B_L)_e = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$. В частности, $B$ невырожден на $L$, то есть $V = L + L^\perp$, и ($\forall$ дополнения $e_1, e_2$ до базиса $V$) $B_e = \left(\begin{array}{c|c} (B_L)_e & O \\ \hline O & (B_{L^\perp})_e \end{array}\right)$. К $L^\perp$ применяем индуктивное предположение. $\square$

*Замечание.* Вариант с другой нумерацией базиса:

$$\left(\begin{array}{ccc|c} & & 1 & \\ & \iddots & & \\ & 1 & & \\ \hline -1 & & & \\ & \iddots & & \\ -1 & & & \\ \hline & & & \end{array}\right).$$

*Следствие.* Пусть $B_i$ – кососимметрический билинейный функционал в $V_i$ ($i = 1, 2$). Тогда $(V_1, B_1) \simeq (V_2, B_2) \Leftrightarrow \dim V_1 = \dim V_2,\ \text{rank}\ B_1 = \text{rank}\ B_2$.

*Доказательство.* $\Rightarrow$: Упражнение.

$\Leftarrow$: Выбираем симплектические базисы $e_1^{(1)}, \ldots, e_n^{(1)}$ в $V_1$, $e_1^{(2)}, \ldots, e_n^{(2)}$ в $V_2$. Зададим $\psi : V_1 \to V_2$, $\psi(e_i^{(1)}) = e_i^{(2)}$. Тогда, по условию, $B_1(e_i^{(1)}, e_j^{(1)}) = B_2(e_i^{(2)}, e_j^{(2)}) = B_2(\psi(e_i^{(1)}), \psi(e_j^{(1)}))$, то есть (почему?) $\forall x, y \in V_1 :\ B_1(x, y) = B_2(\psi(x), \psi(y))$. $\square$

*Следствие.* Пусть $A \in \mathrm{Mat}\ (n, F)$ – кососимметрическая (то есть $A^T = -A$) матрица. Если $n$ нечетно, то $\det A = 0$. Если $n$ четно, то $\det A$ – квадрат в $F$.

*Доказательство.* Пусть $B$ – кососимметрический билинейный функционал с матрицей $A$. Тогда $A = P^T A_0 P$, где $A_0 = \begin{pmatrix} \boxed{\begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix}} & & \\ & \ddots & \\ & & \end{pmatrix}$. Тогда $\det A = (\det P)^2 \det A_0$. Если $n$ нечетно $\Rightarrow \det A_0 = 0 \Rightarrow \det A = 0$. Если $n$ четно $\Rightarrow \det A_0 = 0$ или $1 \Rightarrow \det A = 0$ или $(\det P)^2$. $\square$

Можно доказать и более сильное утверждение.

*Предложение.* Пусть $n$ четно. Тогда существует многочлен Pf с целыми коэффициентами от переменных $x_{ij}$, где $1 \le i < j \le n$, такой, что $\forall A \in \mathrm{Mat}\ (n, F)$, $A^T = -A$, имеем $\det A = (\mathrm{Pf}\ A)^2$. Многочлен Pf однозначно определяется дополнительным условием $\mathrm{Pf}\ A_0 = 1$ для $A_0 = \begin{pmatrix} \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} & & \\ & \ddots & \\ & & \begin{matrix} 0 & 1 \\ -1 & 0 \end{matrix} \end{pmatrix}$ и называется *пфаффианом.*

*Замечание.* Здесь $F$ – любое поле, $\mathrm{char}\ F \neq 2$.

*Пример.* $n = 2 : A = \begin{pmatrix} 0 & a \\ -a & 0 \end{pmatrix}$, $\det A = a^2 \Rightarrow \mathrm{Pf}\ A = a$.

*Упражнение.* Найдите Pf при $n = 4$.

*Доказательство предложения.* Рассмотрим кольцо многочленов $R_0 = \mathbb{Z}[x_{12}, x_{13}, \ldots, x_n$ и его поле частных $F_0 = \mathbb{Q}(x_{12}, x_{13}, \ldots, x_{n-1,n})$. Рассмотрим $X = (x_{ij}) \in \mathrm{Mat}\ (n, F_0)$, где $x_{ji} = -x_{ij}$. Тогда $\det X = f(X)^2$, где $f \in F_0$. Покажем, что $f \in R_0$. В самом деле, $f = \frac{g}{h}$, где $g, h \in R_0$, причем $f^2 = \frac{g^2}{h^2} = \det X \in R_0$. То есть $h^2 \mid g^2$ в кольце $R_0$, и так как $R_0$ факториально, то (Упражнение: рассмотреть простые делители) $h \mid g$ в кольце $R_0$, то есть $f \in R_0$. Равенство $\det X = f(X)^2$ определяет $f$ с точностью до знака. Знак – из условия $f(A_0) = 1$. Это определяет $f$ однозначно. То есть $f$ – это и есть Pf. $\square$

*Упражнение.* Докажите, что если $n$ четно, $A \in \mathrm{Mat}\ (n, F), A^T = -A, P \in \mathrm{Mat}\ (n, F), \det P \neq 0$, то $\mathrm{Pf}\ (P^T A P) = \det P \cdot \mathrm{Pf}\ A$.

Вернемся еще к линейным пространствам с кососимметрическим функционалом. Для приложений (к классической механике) важен невырожденный случай. То есть пусть $n = \dim V$ – четно, $B$ – невырожденный кососимметрический билинейный функционал на $V$ (= *"симплектическая форма"* ).

Подпространство $L \subset V$ называется *(вполне) изотропным,* если $B_L = 0$.

*Задача.* 1) Наибольшая размерность изотропного подпространства равна $\frac{n}{2}$.

2) Если $U$ – изотропное подпространство, то существует изотропное подпространство $L \subset V, \dim L = \frac{n}{2}, L \supset U$.

3) Если $L$ – изотропное подпространство, $\dim L = \frac{n}{2}$, то существует изотропное подпространство $L^{'}$, такое, что $V = L \dotplus L^{'}$.

4) Если $V = L_1 \dotplus L_1^{'} = L_2 \dotplus L_2^{'}$, где $L_i, L_i^{'}$ – (максимальные) изотропные, то существует изометрия (то есть сохраняющая $B$) $\psi : V \to V$ такая, что $\psi(L_1) = L_2,\ \psi(L_1^{'}) = L_2^{'}$.

(см. об этом: Кострикин, Манин, часть 2, §13, о приложениях: Арнольд, Математические меоды классической механики).

3.21. **Пространства со скалярным произведением.** В этом разделе $F = \mathbb{R}$ *или* $\mathbb{C}$ (два варианта), $V$ – линейное пространство над $F$.

*Определение.* $F = \mathbb{R}$ : *Скалярное произведение* в $V$ – это симметрический билинейный функцмонал в $V$ такой, что соответствующий квадратичный функционал положительно определен.

$F = \mathbb{C}$ : *Эрмитово скалярное произведение* в $V$ – это эрмитов полуторалинейный функцмонал в $V$ такой, что соответствующий эрмитов квадратичный функционал положительно определен.

*Обозначение:* $\langle \cdot, \cdot \rangle$.

(*Комментарий:* $\langle x, x \rangle \in \mathbb{R}; \langle x, x \rangle > 0 \quad \forall x \neq 0$.)

*Замечание.* $B(x, y) = \langle x, y \rangle$ – невырожденный. Более того, $B_L$ – невырожденный для любого подпространства $L$.

*Основной пример.* $V = F^n; \langle x, y \rangle = \sum x_i \bar{y}_i \leftarrow$ “стандартное” (эрмитово) скалярное произведение.

*Определение.* $F = \mathbb{R}$ : *Евклидово* пространство – это пара $(V, \langle \cdot, \cdot \rangle)$, где $\langle \cdot, \cdot \rangle$ – скалярное произведение в $V$.

$F = \mathbb{C}$ : *Унитарное ( = эрмитово)* пространство – это пара $(V, \langle \cdot, \cdot \rangle)$, где $\langle \cdot, \cdot \rangle$ – эрмитово скалярное произведение в $V$.

(“Вместе”: $(V, \langle \cdot, \cdot \rangle)$ – пространство со скалярным произведением).

*Предложение (неравенство Коши-Буняковского).* Пусть $(V, \langle \cdot, \cdot \rangle)$ – пространство со скалярным произведением, $x, y \in V$. Тогда $|\langle x, y \rangle| \leq \sqrt{\langle x, x \rangle \cdot \langle y, y \rangle}$. При этом “ $=$” $\Leftrightarrow x, y$ – линейно зависимы.

*Доказательство.* $x = 0$ – тривиально. Далее $x \neq 0$. Рассмотрим $t \in F$ и $tx + y \in V$. Тогда

$$0 \leq \langle tx + y, tx + y \rangle = |t|^2 \langle x, x \rangle + 2\mathrm{Re}\ t \langle x, y \rangle + \langle y, y \rangle =$$

$$\langle x, x \rangle \left( |t|^2 + 2\mathrm{Re}\ t \frac{\langle x, y \rangle}{\langle x, x \rangle} + \frac{\langle y, y \rangle}{\langle x, x \rangle} \right) =$$

$$\langle x,x\rangle \left( \left| t + \frac{\langle y,x\rangle}{\langle x,x\rangle} \right|^2 - \frac{|\langle x,y\rangle|^2}{\langle x,x\rangle^2} + \frac{\langle y,y\rangle}{\langle x,x\rangle} \right) =$$

$$\frac{1}{\langle x,x\rangle} \left( |\langle x,x\rangle t + \langle y,x\rangle|^2 - |\langle x,y\rangle|^2 + \langle x,x\rangle\langle y,y\rangle \right) \Rightarrow$$

$$\Rightarrow |\langle x,y\rangle|^2 \le \langle x,x\rangle\langle y,y\rangle + |\langle x,x\rangle t + \langle y,x\rangle|^2.$$

Если $t = -\frac{\langle y,x\rangle}{\langle x,x\rangle}$, то получаем требуемое.

Равенство $\Leftrightarrow \exists(!)t:\ \langle tx+y, tx+y\rangle = 0 \Leftrightarrow tx+y=0 \Leftrightarrow x, y$ линейно зависимы. $\square$

*Определение. Длина (= норма)* вектора $x \in V$ – это $\|x\| := \sqrt{\langle x,x\rangle}$.

В этих обозначениях неравенство Коши-Буняковского $\Leftrightarrow\ |\langle x,y\rangle| \le \|x\| \cdot \|y\|$.

*Предложение (свойства длины).* 1) $\|0\| = 0, \|x\| > 0 \quad \forall x \in V, x \ne 0$; 2) $\|\lambda x\| = |\lambda| \cdot \|x\|$; 3) (неравенство треугольника) $\|x+y\| \le \|x\| + \|y\|$.

*Доказательство.* 1), 2) – ясно; 3) $\|x+y\|^2 = \|x\|^2 + 2\mathrm{Re}\ \langle x,y\rangle + \|y\|^2 \le \|x\|^2 + 2|\langle x,y\rangle| + \|y\|^2 \underset{\text{К-Б}}{\le} \|x\|^2 + 2\|x\| \cdot \|y\| + \|y\|^2 = (\|x\| + \|y\|)^2$. $\square$

*Упражнение.* Когда в неравенстве треугольника имеет место равенство?

Пусть $V$ *евклидово* (то есть $F = \mathbb{R}$). Тогда *угол* между $x$ и $y$ – это $\varphi$ такое, что $0 \le \varphi \le \pi$, $\cos\varphi = \frac{\langle x,y\rangle}{\|x\|\cdot\|y\|}$ (корректность $\Leftarrow$ К-Б). В частности, $\varphi = \frac{\pi}{2} \Leftrightarrow \langle x,y\rangle = 0$.

В унитарном случае угол не определяют (*кроме* случая $\varphi = \frac{\pi}{2}$, то есть ортогональности).

*Упражнение ("теорема Пифагора").* Пусть $\langle x,y\rangle = 0$. Тогда $\|x+y\|^2 = \|x\|^2 + \|y\|^2$.

*Ортогональные и ортонормированные системы и базисы*

$(V, \langle\cdot,\cdot\rangle)$ – пространство со скалярным произведением.

Напомним: система векторов $e_1, \ldots, e_m$ *ортогональна,* если $\forall i \ne j\ \langle e_i, e_j\rangle = 0$. Далее считаем, что $\forall i\ e_i \ne 0$ ("невырожденность").

*Ортогональный базис* – ортогональная система, являющаяся базисом.

Система (базис) *ортонормирована* (проявляется специфика скалярного произведения) если 1) ортогональна; 2) $\forall i\ \|e_i\| = 1$ (то есть $\langle e_i, e_i\rangle = 1$).

*Пример.* $V = F^n, \langle\cdot,\cdot\rangle$ – стандартное $\Rightarrow$ стандартный базис ортонормированный. И обратно, если базис ортонормированный, то $\langle\cdot,\cdot\rangle$ в координатах в нем – стандартное.

*Замечание.* $e_1, \ldots, e_m$ – ортогональна $\Rightarrow \frac{e_1}{\|e_1\|}, \ldots, \frac{e_m}{\|e_m\|}$ – ортонормирована.

*Предложение.* Пусть $e_1, \ldots, e_m$ – ортогональная система в $V$, $L = \mathrm{Lin}\,\{e_1, \ldots, e_m\}$, $x \in L$, $x = \sum_i x_i e_i$. Тогда $x_i = \frac{\langle x,e_i\rangle}{\langle e_i,e_i\rangle} = \frac{\langle x,e_i\rangle}{\|e_i\|^2}$. (В частности, если *ортонормирована,* то $x = \langle x, e_i\rangle$).

*Доказательство.* $\langle x, e_i\rangle = \ldots \Rightarrow x_i = \ldots$ $\square$

Если $e_1, \ldots, e_n$ – ортогональный *базис* в $V$, то выполняется для $\forall x \in V$.

*Следствие.* Ортогональная система линейно независима (в частности, базис в своей линейной оболочке).

*Доказательство.* Применяем предложение к $x = 0$. $\square$

Мы видели, что ортогональный базис всегда существует (алгоритм Лагранжа). В случае скалярного произведения имеется уточненная и геометризованная версия (работает не с координатами, а с базисом).

*Предложение.* Пусть $a_1, \ldots, a_m \in V$ линейно независимы. Тогда существует ортогональная система $e_1, \ldots, e_m \in V$ такая, что $\forall r \in \{1, \ldots, m\} : \mathrm{Lin}\,\{e_1, \ldots, e_r\} = \mathrm{Lin}\,\{a_1, \ldots, a_r\}$ (в частности, $e_1, \ldots, e_r$ – ортогональный базис в $\mathrm{Lin}\,\{a_1, \ldots, a_r\}$).

*Доказательство.* Вот алгоритм (так называеиый алгоритм ортогонализации Грама-Шмидта (он же Якоби)).

1) $e_1 := a_1$ – годится.

2) $e_2 = a_2 + \lambda e_1$. Тогда $\mathrm{Lin}\,\{e_1, e_2\} = \mathrm{Lin}\,\{a_1, a_2\}$. Выбор $\lambda : 0 = \langle e_2, e_1\rangle = \langle a_2, e_1\rangle + \lambda\langle e_1, e_1\rangle \Rightarrow \lambda = \ldots$

3) $e_3 = a_3 + \lambda_1 e_1 + \lambda_2 e_2$. Тогда $\mathrm{Lin}\,\{e_1, e_2, e_3\} = \mathrm{Lin}\,\{a_1, a_2, a_3\}$. Выбор $\lambda_1, \lambda_2 \ldots$ И так далее. $\square$

Геометрический смысл: ???

*Упражнение.* Аналогично для любого (эрмитово) симметричного $B$ *в предположении,* что $B$ невырожден на $\mathrm{Lin}\,\{a_1, \ldots, a_r\}$ $\forall r$.

*Замечание (Упражнение).* Алгоритм Грама-Шмидта $\approx$ алгоритм Лагранжа $\ldots$

*Следствие.* Любую ортогональную систему можно дополнить до ортогонального базиса.

*Доказательство.* Упражнение.

*Упражнение.* Что дает алгоритм Грама-Шмидта для линейно зависимой системы?

*Ортогональное дополнение м ортогональная проекция*

Пусть $L \subset V$ – подпространство.

Напомним $L^\perp = \{x \in V \mid \forall y \in L : \langle x, y\rangle = 0\}$ – *ортогональное дополнение* к $L$. Так как $\langle\cdot,\cdot\rangle$ невырождено на любом $L$, то $V = L \dotplus L^\perp$ и $L^{\perp\perp} = L$ (всегда).

*Обозначение:* если $V = L_1 \dotplus L_2$, и $\langle x, y\rangle = 0$ $\forall x \in L_1, y \in L_2$, то пишут $V = L_1 \oplus L_2 \leftarrow$ ортогональная прямвя сумма.

Итак, $V = L \oplus L^\perp$.

*Упражнение.* Если $V = L_1 \oplus L_2$, то $L_1^\perp = L_2$, $L_2^\perp = L_1$.

Пусть $x \in V = L \oplus L^\perp \Rightarrow x = x_L + x_{L^\perp}$, где $x_L \in L$, $x_{L^\perp} \in L^\perp$.

Терминология: $x_L$ – *ортогональная проекция* $x$ на $L$, $x_{L^\perp}$ – *ортогональная составляющая* $x$ относительно $L$.

*Предложение.* Пусть $e_1, \ldots, e_m$ – ортогональный базис в $L, x \in V$. Тогда $x_L = \sum_{i=1}^m x_i e_i$, где $x_i = \frac{\langle x, e_i\rangle}{\langle e_i, e_i\rangle}$.

*Доказательство.* Дополним до ортогонального базиса $e_1, \dots, e_m, e_{m+1}, \dots, e_n$ ($e_{m+1}, \dots, e_n$ – ортогональный базис в $L^\perp$); $x = \underbrace{\sum_{i=1}^{m} x_i e_i}_{= x_L} + \underbrace{\sum_{i=m+1}^{n} x_i e_i}_{= x_{L^\perp}}$, где $x_i = \dots$

□

3.22. **Линейные операторы в пространствах со скалярным произведением.** Пусть $(V, \langle\cdot,\cdot\rangle)$ – евклидово (или унитарное) пространство.

Напомним, что $\langle\cdot,\cdot\rangle$ соответствует отображение $\psi : V \to V^* \quad \langle x, y\rangle = (x, \psi(y)) \quad \forall x, y \in V$. (NB: здесь чуть меняется отображение $\varphi \leftrightsquigarrow \psi$). При этом $\psi$ линейно (или полулинейно). Так как $\langle\cdot,\cdot\rangle$ невырожденно, то $\psi$ – изоморфизм $V \to V^*$ (или $V \to \overline{V^*}$). (То есть, в частности, $\forall f \in V^* \ \exists!\ y \in V \ \forall x \in V : \ (x, f) = \langle x, y\rangle$. Именно, $y = \psi^{-1}(f)$).

Далее, пусть $\varphi \in \operatorname{End} V$, то есть $\varphi : V \to V$ линеен. Тогда имеется линейный $\varphi^* : V^* \to V^* \quad (\varphi(x), f) = (x, \varphi^*(f)) \quad \forall x \in V, \forall f \in V^*$. С помощью биекции $\psi : V \to V^*$ можно "перенести" $\varphi^*$ в пространство $V$; именно, рассмотрим $V \xrightarrow{\psi} V^* \xrightarrow{\varphi^*} V^* \xrightarrow{\psi^{-1}} V$, откуда $V \xrightarrow{\varphi^*_{\text{new}}} V$. Отметим, что это *линейный* оператор (почему?).

Иными словами $\varphi^*_{\text{new}}(y) = (\psi^{-1} \circ \varphi^* \circ \psi)(y)$, то есть $\langle x, \varphi^*_{\text{new}}(y)\rangle = \langle x, (\psi^{-1} \circ \varphi^* \circ \psi)(y)\rangle = \langle x, \varphi^*(\psi(y))\rangle = \langle \varphi(x), \psi(y)\rangle = \langle \varphi(x), y\rangle \quad \forall x, y \in V$.

Далее в этом разделе мы будем понимать $\varphi^*$ как линейный оператор в $V$, то есть $\varphi^* := \varphi^*_{\text{new}}$. То есть, если $\varphi \in \operatorname{End} V$, то имеется *сопряженный* оператор $\varphi^* \in \operatorname{End} V$, однозначно определяемый соотношением $\langle \varphi(x), y\rangle = \langle x, \varphi^*(y)\rangle \quad \forall x, y \in V$.

*Замечание.* $\langle x, \varphi(y)\rangle = \langle \varphi^*(x), y\rangle$.

"Польза": можно сравнивать $\varphi$ и $\varphi^*$, ибо они действуют в одном пространстве.

*Замечание.* Если $\varphi : V \to W$, где $V, W$ – пространства со скалярным произведением, то можно определить $\varphi^*$ как линейное отображение $W \to V$. "Пользы", однако, в случае $W \neq V$ меньше.

*Предложение* (свойства сопряженного оператора).

(1) $(\varphi_1 + \varphi_2)^* = \varphi_1^* + \varphi_2^*$;

(2) $(\lambda\varphi)^* = \bar{\lambda}\varphi^*$;

(3) $\mathrm{id}^* = \mathrm{id}, \ 0^* = 0$;

(4) $(\varphi_1 \cdot \varphi_2)^* = \varphi_2^* \cdot \varphi_1^*$;

(5) Если $\varphi$ обратим, то $\varphi^*$ тоже обратим, причем $(\varphi^*)^{-1} = (\varphi^{-1})^*$;

(6) $\varphi^{**} = \varphi$.

*Доказательство.* (2): $(\lambda\varphi)^*(y) \stackrel{?}{=} \bar{\lambda}\varphi^*(y) \quad \forall y \in V$? Пусть $x \in V$ Рассмотрим $\langle x, (\lambda\varphi)^*(y)\rangle = \langle (\lambda\varphi)(x), y\rangle = \lambda\langle \varphi(x), y\rangle = \lambda\langle x, \varphi^*(y)\rangle = \langle x, \bar{\lambda}\varphi^*(y)\rangle$. Остальное – упражнение ((6) – замечание выше). □

Как связаны матрицы $\varphi$ и $\varphi^*$? Пусть $e_1, \dots, e_n$ – *ортонормированный* базис в $V$. Напомним, что $\varphi_e = (a_{ij})$, где $\varphi(e_j) = \sum_i a_{ij} e_i$. Виду ортонормированности базиса имеем $a_{ij} = \langle \varphi(e_j), e_i \rangle$. Аналогично $(\varphi^*)_e = (b_{ij})$, где $\varphi^*(e_j) = \sum_i b_{ij} e_i$, при этом $b_{ij} = \langle \varphi^*(e_j), e_i \rangle = \langle e_j, \varphi(e_i) \rangle = \overline{\langle \varphi(e_i), e_j \rangle} = \overline{a_{ji}}$.

Введем (напомним) обозначение: если $A = (a_{ij}) \in \mathrm{Mat}\ (n, F)$ (где $F = \mathbb{R}$ или $\mathbb{C}$), то $A^* = \overline{A^I}$, то есть $A^* = (\overline{a_{ji}})$ (матрица, *сопряженная* к $A$). ($F = \mathbb{R} \Rightarrow$ сопряжение "лишнее"). То есть мы доказали

*Предложение.* Пусть $(V, \langle \cdot, \cdot \rangle)$ – евклидово/унитарное пространство, $e_1, \dots, e_n$ – ортонормированный базис, $\varphi \in \mathrm{End}\ V$. Тогда $(\varphi^*)_e = (\varphi_e)^*$.

*Замечание.* Ортогональности базиса для выполнения последней формулы недостаточно!

( *Упражнение:* 1) что будет для ортогонального базиса? 2) формула $(\varphi^*)_e = (\varphi_e)^*$ верна для чуть более широкого, чем ортонормированные, класса базисов – какого?)

*Ортогональные/унитарные операторы и матрицы*

Пусть $(V, \langle \cdot, \cdot \rangle)$ – евклидово/унитарное пространство, $\varphi \in \mathrm{End}\ V$.

*Определение.* $\varphi$ *ортогонален/унитарен,* если $\varphi \circ \varphi^* = \varphi^* \circ \varphi = \mathrm{id}$ (то есть $\varphi$ обратим, причем $\varphi^{-1} = \varphi^*$).

С другой стороны, пусть $A \in \mathrm{Mat}\ (n, F)$, где $F = \mathbb{R}/\mathbb{C}$.

*Определение.* $A$ *ортогональна/унитарна,* если $AA^* = A^*A = E$ (то есть $A$ обратима и $A^{-1} = A^*$).

*Лемма.* Пусть $e_1, \dots, e_n$ – *ортонормированный* базис в $V$. Тогда $\varphi$ – ортогонален/унитарен $\Leftrightarrow$ $\varphi_e$ – ортогональна/унитарна.

*Доказательство.* Упражнение. $\square$

*Упражнение.* $\varphi$ – ортогонален/унитарен $\Rightarrow$ $|\det \varphi| = 1$; в частности, $\varphi$ – ортогонален $\Rightarrow \det \varphi = \pm 1$.

*Замечание.* Если $V$ – линейное пространство над $\mathbb{R}$, то имеется понятие *ориентации* $V$ – это класс базисов относительно отношения эквивалентности: матрица перехода имеет $\det > 0$. $\varphi \in \mathrm{End}\ V$ сохраняет/меняет ориентацию $\Leftrightarrow \det \varphi > 0 / \det \varphi < 0$.

То есть, если $\varphi$ ортогональный, то $\varphi$ сохраняет ориентацию $\Leftrightarrow \det \varphi = 1$.

*Предложение.* Пусть $\varphi \in \mathrm{End}\ V$. Тогда $\varphi$ ортогонален/унитарен $\Leftrightarrow \forall\ x, y \in V:\ \langle \varphi(x), \varphi(y) \rangle = \langle x, y \rangle$ (то есть $\varphi$ является "автоизометрией", то есть автоморфизмом пространства $V$ с $\langle \cdot, \cdot \rangle$).

*Доказательство.* $\Rightarrow$: Дано: $\forall x, z \in V \quad \langle \varphi(x), z \rangle = \langle x, \varphi^{-1}(z) \rangle$. Если $y \in V$, то $z := \varphi(y) \Rightarrow \dots$

$\Leftarrow$: 1) Почему $\varphi$ обратим? $x \in \mathrm{Ker}\ \varphi \Rightarrow\ 0 = \langle \varphi(x), \varphi(x) \rangle = \langle x, x \rangle \Rightarrow\ x = 0$.

2) Если $z \in V$, то $y := \varphi^{-1}(z) \Rightarrow\ \dots\ \square$

*Пример.* Повороты и отражения в $(\mathbb{R}^2, \langle \cdot, \cdot \rangle)$ – ортогональные (Упражнение: других и нет!).

*Упражнение.* $\varphi$ ортогонален/унитарен, $\lambda$ – собственное значение $\varphi \Rightarrow |\lambda| = 1$. В частности, если $\varphi$ ортогонален, то $\lambda = \pm 1$.

Вот несколько другой источник ортогональных/унитарных матриц:

*Предложение.* Пусть $e_1, \ldots, e_n; e_1^{'}, \ldots, e_n^{'}$ – ортонормированные базисы в $V$, $P = T_{e \to e'}$. Тогда $P$ ортогональна/унитарна.

*Доказательство. Способ 1:* "в лоб" (Упражнение). *Способ 2:* Рассмотрим $\varphi : V \to V$, $\varphi(e_i) = e_i^{'}$ $\forall i$, и продолжим по линейности. Тогда $\varphi$ ортогонален/унитарен (почему?). Заметим, что $P = \varphi_e$. То есть $P$ – ортогональна/унитарна. $\square$

*Замечание.* Если базисы $e$ и $e^{'}$ имеют одинаковые "матрицы Грама", то есть $\langle e_i, e_j \rangle = \langle e_i^{'}, e_j^{'} \rangle$ $\forall i, j$, то $P = T_{e \to e'}$ – ортогональна/унитарна. (Доказательство проходит в этом случае!).

*Замечание (о группах).* Рассмотрим $\mathrm{GL}\ (V) = \{\varphi \in \mathrm{End}\ (V) \mid \det \varphi \neq 0\}$ (то есть $\varphi$ обратим). Это – *группа* (относительно композиции). На "матричном" языке $\mathrm{GL}\ (n, F) = \{A \in \mathrm{Mat}\ (n, F) \mid \det A \neq 0\}$.

*Упражнение.* Проверьте, что ортогональные/унитарные операторы – *подгруппа* в $\mathrm{GL}\ (V)$, то есть:

1) $\varphi_1, \varphi_2$ – ортогональны/унитарны $\Rightarrow \varphi_1 \varphi_2$ – ортогонален/унитарен.

2) id – ортогонален/унитарен.

3) $\varphi$ – ортогонален/унитарен $\Rightarrow \varphi^{-1}$ ортогонален/унитарен.

То же верно для ортогональных/унитарных операторов с определителем $= 1$. Аналогично для матриц.

*Нормальные операторы*

Пусть $(V, \langle \cdot, \cdot \rangle)$ – евклидово/унитарное, $\varphi \in \mathrm{End}\ V$.

*Определение.* $\varphi$ – *нормален* , если $\varphi \circ \varphi^* = \varphi^* \circ \varphi$.

*Упражнение.* Если $e_1, \ldots, e_n$ – ортонормированный базис в $V$, $A = \varphi_e$, то $\varphi$ нормален $\Leftrightarrow AA^* = A^*A$.

По определению, если $\varphi$ ортогональный/унитарный, то $\varphi$ нормален.

Вот еще важный класс:

*Определение.* $\varphi$ – *самосопряжен,* если $\varphi^* = \varphi$.

Если $\varphi$ самосопряжен, то $\varphi \circ \varphi^* = \varphi^* \circ \varphi = \varphi^2$, то есть $\varphi$ нормален.

*Упражнение.* Если $e_1, \ldots, e_n$ – ортонормированный базис в $V$, $A = \varphi_e$, то $\varphi$ самосопряжен $\Leftrightarrow A^* = A$ (то есть $A$ эрмитова/симметричная).

**Теорема (спектральная теорема для нормальных операторов над $\mathbb{C}$).** Пусть $(V, \langle \cdot, \cdot \rangle)$ – *унитарное* пространство, $\varphi \in \mathrm{End}\ V, \varphi$ нормален. Тогда существует ортонормированный базис $e_1, \ldots, e_n$ в $V$ такой, что $\varphi_e = \begin{pmatrix} \lambda_1 & & O \\ & \ddots & \\ O & & \lambda_n \end{pmatrix}$, где $\lambda_i \in \mathbb{C}$.

(пояснение: спектр = множество собственных значений).

*Замечания.* 1) И обратно, если для некоторого ортонормированного базиса $e_1, \ldots, e_n$ матрица $\varphi_e = \begin{pmatrix} \lambda_1 & & O \\ & \ddots & \\ O & & \lambda_n \end{pmatrix}$, то $\varphi$ нормален (почему?).

2) На языке матриц теорема звучит так: если $A \in \mathrm{Mat}\,(n, \mathbb{C})$, $A^*A = AA^*$, то существует *унитарная* матрица $P \in \mathrm{Mat}\,(n, \mathbb{C})$ такая, что $P^*AP = \begin{pmatrix} \lambda_1 & & O \\ & \ddots & \\ O & & \lambda_n \end{pmatrix}$ (при этом $\lambda_i$ определены однозначно с точностью до порядка).

3) Теорема означает, что собственные подпространства нормального оператора попарно ортогональны.

*Лемма.* Пусть $(V, \langle \cdot, \cdot \rangle)$ евклидово/унитарное, $\varphi \in \mathrm{End}\ V, L$ – подпространство в $V$, инвариантное относительно $\varphi$. Тогда $L^\perp$ инвариантно относительно $\varphi^*$.

*Доказательство.* Пусть $y \in L^\perp$. Требуется доказать: $\varphi^*(y) \in L^\perp$. Пусть $x \in L$. Тогда $\langle x, \varphi^*(y) \rangle = \langle \underbrace{\varphi(x)}_{\in L}, \underbrace{y}_{\in L^\perp} \rangle = 0$, что и требовалось доказать. $\square$

*Доказательство теоремы.* Индукция по $\dim V$ с тривиальной базой ($\dim V = 1$). Выбираем собственное значение $\lambda$ оператора $\varphi$ (здесь важно, что $F = \mathbb{C}$!) и рассматриваем $L = V_\lambda(\varphi) = \{x \in V \mid \varphi(x) = \lambda x\} \neq 0$. Так как $L$ инвариантно относительно $\varphi$, то (лемма) $L^\perp$ инвариантно относительно $\varphi^*$. С другой стороны, $L$ инвариантно и относительно $\varphi^*$ : если $x \in L$, то есть $\varphi(x) = \lambda x$, то $\varphi\varphi^*(x) = \varphi^*\varphi(x) = \lambda\varphi^*(x) \Rightarrow \varphi^*(x) \in L$. Лемма $\Rightarrow L^\perp$ инвариантно относительно $\varphi^{**} = \varphi$.

Итак, $L^\perp$ инвариантно относительно $\varphi$ и $\varphi^*$.

*Упражнение.* $(\varphi_{L^\perp})^* = (\varphi^*)_{L^\perp}$; в частности, $\varphi_{L^\perp} \in \mathrm{End}\ L^\perp$ нормален.

Так как $\dim L^\perp < \dim V$, то применим индуктивное предположение: в $L^\perp$ существует ортонормированный базис из собственных векторов $\varphi$. Далее, любой ортонормированный базис в $L$ состоит из собственных векторов $\varphi$. Так как $V = L \oplus L^\perp$, то объединение этих базисов – искомый. $\square$

*Следствие 1 (спектральная теорема для самосопряженных операторов над $\mathbb{C}$).* Пусть $(V, \langle \cdot, \cdot \rangle)$ – *унитарное* пространство, $\varphi \in \mathrm{End}\ V, \varphi$ самосопряжен. Тогда существует ортонормированный базис $e_1, \ldots, e_n$ в $V$ такой, что $\varphi_e = \begin{pmatrix} \lambda_1 & & O \\ & \ddots & \\ O & & \lambda_n \end{pmatrix}$, где $\lambda_i \in \mathbb{R}$.

*Доказательство.* Осталось $\lambda_i \in \mathbb{R}$? То есть, почему собственные значения $\varphi$ вещественны? $\varphi(x) = \lambda x, x \neq 0 \Rightarrow \lambda\langle x, x \rangle = \langle \varphi(x), x \rangle = \langle x, \varphi(x) \rangle = \bar{\lambda}\langle x, x \rangle \Rightarrow \ldots$ $\square$ *Замечание.* И обратно...

*Следствие 2 (спектральная теорема для унитарных операторов).*

Пусть $(V, <, >)$ – унитарное пространство, $\varphi \in EndV$, $\varphi$ унитарен. Тогда существует ортогональный базис, в котором $\varphi$ диагонализуем и диогональные элементы $\lambda_i$ имеют модуль 1.
*Замечание.* И обратно...

3.23. **Комплексификация и овеществление.** Цель: "переходить" от линейной алгебры над $\mathbb{R}$ к линейной алгебре над $\mathbb{C}$ и наоборот.
(Обобщение: если $F \subset K$ – поля, то ... термин: подъём/спуск поля скаляров).
*Овеществление.* Пусть $V$ – линейное пространство над $\mathbb{C}$.
Рассмотрим $V_{\mathbb{R}}$ – линейное пространство над $\mathbb{R}$, определенное следующимобразом: $V_{\mathbb{R}} = V$ как множество, то же сложение и умножение на вещественные скаляры (то есть "забываем" про $\mathbb{C}$).
*Предложение.* Если $e_1, ..., e_n$ – базис в $V$, то $e_1, ..., e_n, ie_1, ..., ie_n$ – базис в $V_{\mathbb{R}}$.
*Доказательство:* $v \in V \Rightarrow v = \sum c_k e_k = \sum a_k e_k + \sum b_k i e_k$, где $c_k = a_k + ib_k$. Такое представление единственно.(почему?)
Если $V, W$ – линейные пространства над $\mathbb{C}$, $\varphi \in Hom(V, W)$, то можно рассмотреть $\varphi_{\mathbb{R}} \in Hom(V_{\mathbb{R}}, W_{\mathbb{R}})$, а именно $\varphi_{\mathbb{R}} = \varphi$.
*Упражнение.* Как связаны матрицы $\varphi$ и $\varphi_{\mathbb{R}}$? В частности, проверьте, что $\det \varphi_{\mathbb{R}} = |\det \varphi|^2 \geq 0$
*Задача.* 1) Пусть $\psi \in Hom(V_{\mathbb{R}}, W_{\mathbb{R}})$. В каком случае $\exists \varphi \in Hom(V, W)$ такой, что $\psi = \varphi_{\mathbb{R}}$.
2) Пусть $< \cdot, \cdot >$ – эрмитово скалярное произведение на $V$. Тогда $< \cdot, \cdot >_{\mathbb{R}} = Re < \cdot, \cdot >$ – скалярное произведение на $V_{\mathbb{R}}$.
*Замечание.* Более или менее, буквально обобщается на случай, когда $F \subset K$, $V$ – линейное пространство над $K \Rightarrow V_F$...
*Задача.* Как связаны $\dim_F V_F$ и $\dim_K V$?
*Комплексификация.* Пусть, наоборот, $V$ – линейное пространство над $\mathbb{R}$. Цель: построить $V^{\mathbb{C}}$ – линейное пространство над $\mathbb{C}$ такое, что $V \subset V^{\mathbb{C}}$, причем $V$ – подпространство в $(V^{\mathbb{C}})_{\mathbb{R}}$, кроме того $\forall v \in V^{\mathbb{C}} \exists! x, y \in V : v = x + iy$.
Именно, рассмотрим $V^{\mathbb{C}} = \{(x, y) | x, y \in V\}$. Определим $(x_1, y_1) + (x_2, y_2) = (x_1 + x_2, y_1 + y_2)$, $\alpha(x, y) = (\alpha x, \alpha y), \alpha \in \mathbb{R}$, $i(x, y) = (-y, x)$. Сразу заметим $(x, y) = (x, 0) + i(y, 0)$. Отождествим $x \in V$ с $(x, 0)$ (то есть $V \subset V^{\mathbb{C}}$), тогда $(x, y) = x + iy$. Так и будем далее писать.
*Упражнение.* $V^{\mathbb{C}}$ – линейное пространство над $\mathbb{C}$.
В $V^{\mathbb{C}}$ имеется сопряжение $(x + iy) \to x - iy$. "Те же свойства" (*Упражнение.* сформулируйте и докажите их)
*Предложение.* Всякий базис в $V$ является также базисом в $V^{\mathbb{C}}$. *Доказательство:* Пусть $e_1, ..., e_n$ – базис в $V$. Рассмотрим $v \in V^{\mathbb{C}}$; $v = x + iy$, где $x, y \in V$. Тогда $x = \sum \alpha_k e_k, y = \sum \beta_k e_k$. Тогда $v = \sum (\alpha_k + i\beta_k) e_k$. Представление единственно. $\square$

*Замечание.* Так получен базис в $V^{\mathbb{C}}$ из вещественных векторов.
Сравним подпространства в $V$ и $V^{\mathbb{C}}$. Если $L$ – подпространство в $V$, то имеется $L^{\mathbb{C}}$ – подпространство в $V^{\mathbb{C}}$, именно: $L^{\mathbb{C}} = \{x + iy | x, y \in L\}$. С другой стороны, пусть $U$ – подпространство в $V^{\mathbb{C}}$. Когда $U = L^{\mathbb{C}}$ для какого нибудь подпространства $L \subset V$?
Рассмотрим $\overline{U} = \{\bar{u} | u \in U\}$.
*Упражнение.* $\overline{U}$– тоже подпространство в $V^{\mathbb{C}}$..
*Предложение.* Существует подпространство $L \subset V$ такое, что $U = L^{\mathbb{C}} \Leftrightarrow U = \overline{U}$
.
*Доказательство:* $\Rightarrow$: ясно.
$\Leftarrow$: Рассмотрим $L = U \cap V$. $L$ – подпространство в $V$. Пусть $u = x + iy \in U$. Имеем $x - iy \in U$, то есть $x, y \in U$. Итак, $U = L + iL = L^{\mathbb{C}}$. $\square$
Пусть $\varphi \in Hom(V, W)$. Тогда возникает комплексификация $\varphi^{\mathbb{C}} \in Hom(V^{\mathbb{C}}, W^{\mathbb{C}})$; именно: $\varphi^{\mathbb{C}} := \varphi(x) + i\varphi(y)$.
*Упражнение.* $\varphi^{\mathbb{C}}$ – линейно.
*Упражнение.* 1) $(\varphi_1 + \varphi_2)^{\mathbb{C}} = \varphi_1^{\mathbb{C}} + \varphi_2^{\mathbb{C}}$.
2) $(\lambda\varphi)^{\mathbb{C}} = \lambda\varphi^{\mathbb{C}}, \lambda \in \mathbb{R}$.
3) $(\varphi_1\varphi_2)^{\mathbb{C}} = \varphi_1^{\mathbb{C}}\varphi_2^{\mathbb{C}}$.
Если $e_1, ..., e_n$ – базис в $V$, $u_1, ..., u_n$ – базис в $W$, то $(\varphi^{\mathbb{C}})_{u,e} = \varphi_{u,e}$.
*Упражнение.* $\varphi^{\mathbb{C}}(\bar{v}) = \overline{\varphi^{\mathbb{C}}(v)}$.
*Задача.* Охарактеризуйте линейные отображения $\psi \in Hom(V^{\mathbb{C}}, W^{\mathbb{C}})$ такие, что $\psi = \varphi^{\mathbb{C}}$, для некоторого $\varphi \in Hom(V, W)$.
*Комплексификация евклидовых пространств.*
Пусть $(V, <, >)$ – евклидово пространство. Определим эрмитово скалярное произведение $<, >^{\mathbb{C}}$ в $V^{\mathbb{C}}$ формулой $< x_1+iy_1, x_2+iy_2 >^{\mathbb{C}} := (< x_1, x_2 > + < y_1, y_2 > ) + i(< y_1, x_2 > - < x_1, y_2 >)$. Отметив сразу, что $< x_1, x_2 >^{\mathbb{C}} =< x_1, x_2 >$, при $x_1, x_2 \in V$.
*Упражнение.* $<, >^{\mathbb{C}}$ – эрмитово скалярное произведение.
*Лемма.* Пусть $\varphi \in EndV$. Тогда $(\varphi^{\mathbb{C}})^* = (\varphi^*)^{\mathbb{C}}$.
*Доказательство:* На “вещественных"векторах равенство выполняется. В частности, $(\varphi^{\mathbb{C}})^*$ переводит вещественые в вещественные $\Leftrightarrow$ определяется действием на вещественные весторы. Но на вещественных имеем равенство. $\square$
*Следствие.* $\varphi$ нормален $\Rightarrow \varphi^{\mathbb{C}}$ нормален, $\varphi$ ортогонален $\Rightarrow \varphi^{\mathbb{C}}$ унитарен, $\varphi$ самосопряжен $\Rightarrow \varphi^{\mathbb{C}}$ самосопряжен.

## 3.24. **Нормальные операторы в евклидовом пространстве. Спектральная теорема для операторов над $\mathbb{R}$**

Пусть $(V, <, >)$ евклидово, $\varphi \in End(V)$, $\varphi$ нормален. Тогда существует ортонормированый базис $e_1, ..., e_n$ такой, что

$$\varphi_e = \begin{pmatrix} \lambda_1 & & & & & & & \\ & ... & & & & & & \\ & & \lambda_p & & & & & \\ & & & \alpha_1 & \beta_1 & & & \\ & & & -\beta_1 & \alpha_1 & & & \\ & & & & & ... & & \\ & & & & & & \alpha_q & \beta_q \\ & & & & & & -\beta_q & \alpha_q \end{pmatrix}, \text{где } \alpha_i, \beta_i, \lambda_i \in \mathbb{R},\ \beta_i > 0$$

При этом матрица определена однозначно с точностью до порядка клеток на диагонали.

*Доказательство:* рассмотрим унитарное пространство $(V^{\mathbb{C}}, <, >^{\mathbb{C}})$ и оператор $\varphi^{\mathbb{C}} \in EndV^{\mathbb{C}}$. Так как в любом вещественном базисе матрица $\varphi^{\mathbb{C}}$ равна матрице $\varphi$, то их характеристические полиномы совпадают.

Пусть $\lambda_1, ..., \lambda_p, \alpha_1 \pm, i\beta_1, ..., \alpha_q \pm i\beta_q$ – собственные значения $\varphi^{\mathbb{C}}$ с учетом кратности (здесь все числа вещественны, $\beta_j > 0$). По спектральной теореме для нормальных операторов над $\mathbb{C}$ $V^{\mathbb{C}}$ есть ортогональная прямая сумма собственных подпространств $\varphi^{\mathbb{C}}$. Как они устроены?

1) вещественные собственные значения . Если $v \in (V^{\mathbb{C}})_\lambda$, то $\overline{v} \in (V^{\mathbb{C}})_\lambda$, значит в $(V^{\mathbb{C}})_\lambda$ есть базис из вещественных векторов. Его можно выбрать ортонормированым. Это бащис из собственных векторов $\varphi$ соответствующих собственному значению $\lambda$.

2) комплексное собственное значение $\lambda = \alpha + i\beta$. Снова берём $v \in (V^{\mathbb{C}})_\lambda, \varphi^{\mathbb{C}}(v) = \lambda v, \varphi^{\mathbb{C}}(\overline{v}) = \overline{\lambda}\overline{v} \Rightarrow < v, \overline{v} >= 0$. Пусть $v = x + iy$. Тогда $||x|| = ||y||, < x, y >= 0$ (ибо $< (x + iy), (x - iy) >= (< x, x > - < y, y >) + 2i < x, y >= 0$). Далее $\varphi^{\mathbb{C}}(v) = \varphi(x) + i\varphi(y) = (\alpha x - \beta y) + i(\beta x + \alpha y)$. То есть $Lin\{x, y\}$ инвариантна относительно $\varphi$, и матрица $\varphi$ имеет в базисе $(x, y)$ матрицу

$$\begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}$$

Сделаем это со всеми собственными векторами базиса для $\varphi^{\mathbb{C}}$. Почему полученные векторы попарно ортогональны?

Пусть $v_1 = x_1 + iy_1$ – собственный вектор значения $\lambda_1$, $v_2 = x_2 + iy_2$ – собственный вектор значения $\lambda_2$. Тогда $< v_1, v_2 >^{\mathbb{C}} = 0, < v_1, \overline{v_2} >^{\mathbb{C}} = 0$. Отсюда (открывая скобки) имеем $x_1, x_2, y_1, y_2$ – попарно ортогональны.

*Следствие 1.* Самосопряженный оператор в евклидовом пространстве диагонализуем.

*Следствие 2.* В некотором ортогональном базисе евклидова протранства ортогональный оператор принимает вид

$$\varphi_e = \begin{pmatrix} \epsilon_1 & & & & & & & \\ & \ldots & & & & & & \\ & & \epsilon_p & & & & & \\ & & & \cos\theta_1 & \sin\theta_1 & & & \\ & & & -\sin\theta_1 & \cos\theta_1 & & & \\ & & & & & \ldots & & \\ & & & & & & \cos\theta_q & \sin\theta_q \\ & & & & & & -\sin\theta_q & \cos\theta_q \end{pmatrix}, \text{где } \epsilon_i = \pm 1,\ 0 < \theta_j < \pi$$

*Примеры* 1) $\dim V = 2$. Любое ортогональное преобразование есть осевая симметрия, центральная симметрия или поворот.
2) $\dim V = 3$. Если $\det\varphi = 1$, то любое ортогональное преобразование есть вращение вокруг некоторой оси ("теорема Эйлера"). *Упражнение.* Разберите случай $\det\varphi < 0$.
*Билинейные (полуторолинейные) и (эрмитово) квадратичные функционалы в пространствах со скалярным произведением*
Пусть $(V, <,>)$ – евклидово (эрмитово) пространство. Если $\varphi \in End(V)$, то определим $B_\varphi : V \times V \to F, B(x,y) =< \varphi(y), x >= \overline{< x, \varphi(y) >}$. *Лемма.* Пусть $e_1, .., e_n$ – ортонормированый базис в $V$. Тогда $(B_\varphi)_e = \varphi_e$.
*Доказательство:* $(B_\varphi)_e = (b_{ij})$, где $b_{ij} = B_\varphi(e_i, e_j) =< \varphi(e_j), e_i >= (i)$'ая координата $\varphi(e_j)$. □
Пусть $B(x,y) =< \varphi(y), x >$. Тогда $B^*(x,y) := \overline{B(y,x)} =< \varphi^*(y), x >$. В частности, $B$ симметричен $\Leftrightarrow$ $\varphi$ самосопряжен. Ограничиваясь самосопряженными операторами, получаем изоморфизм (над $\mathbb{R}$!) между самосопряженными линейными операторами и эрмитовыми квадратичными функционалами, $Q(x) =< \varphi(x), x >$. При этом в ортонормированом базисе $Q_e = B_e = \varphi_e$.
**Теорема.(приведение (эрмитово)симметричной квадратичной формы к главным осям)**
Пусть $(V, <,>)$ – пространство со скалярным произведением, $Q$ – (эрмитово)квадратичный функционал в $V$. Тогда существует ортонормированый базис, в котором $Q$ диоганализуется.
*Доказательство.* применим спектральную теорему к самомопряженному оператору, порождающему $Q$. □
*Диоганализация пары (эрмитово) квадратичных функционалов*
**Теорема.** Пусть $(V, <,>)$ – пространство со скалярным произведением, $Q_1, Q_2$– (эрмитово)квадратичные формы в $V$, $Q_1 > 0$. Тогда существует базис $e_1, ..., e_n$ в $V$ такой, что $Q_1(x) = \sum_i |x_i|^2,\ Q_2(x) = \sum_i \lambda_i |x_i|^2$.
*Доказательство:* 1) $Q_1 > 0 \Rightarrow$ существует базис $u_1, ..., u_n$ такой, что $Q_1(y) =$

$\sum_i |y_i|^2$.
2) Поляра $Q_1$ есть (эрмитово) скалярное произведение на $V$. Обозначим его $<,>$.
3) В евклидовом(унитарном) пространстве $(V, <,>)$ приведём $Q_2$ к диагональному виду. $\square$

3.25. **Положительно определенные операторы.** Пусть $(V, <.,.>)$ – пространство со скалярным произведением, $\varphi \in EndV$ $\varphi$ – самосопряжен.
*Определение.* $\varphi$ – положительно определен($\varphi > 0$), если (эрмитово) квадратичный функционал $Q(x) =< \varphi(x), x >$ положительно определён, то есть, $< \varphi(x), x >> 0$ $\forall x \in V, x \neq 0$.
В базисе главных осей для $Q$ имеем $Q(x) = \sum \lambda_i |x_i|^2$, где $\lambda_i$ – собственные значение $\varphi$. То есть $\varphi > 0 \Leftrightarrow$ все собственные значения $\varphi$ неотрицательны.
*Предложение.* Пусть $\varphi \in EndV, \varphi > 0$. Тогда $\exists! \psi \in EndV \psi > 0 : \varphi = \psi^2$.
Обозначение: $\psi = \sqrt{\phi}$ ("арифметический квадратный корень")
*Доказательство:* $\exists$ : возьмем эрмитов базис $e_1, ..., e_n$ в котором $\varphi_e = \begin{pmatrix} \lambda_1 & & 0 \\ .... & ... & .. \\ 0 & & \lambda_n \end{pmatrix}$, и положим $\psi = \begin{pmatrix} \sqrt{\lambda_1} & & 0 \\ .... & ... & .. \\ 0 & & \sqrt{\lambda_n} \end{pmatrix}$. То же самое более инвариантно: пусть $\lambda_1, ..., \lambda_m$ – собственные значения $\varphi$, $V_i = V_{\lambda_i}(\varphi)$. Тогда $V = V_1 \oplus ... \oplus V_m$, причем $\varphi_{V_i}$ – умножение на $\lambda_i$. Определим $\psi$ так, что $\psi_{V_i}$ – уможение на $\sqrt{\lambda_i}$.
! : Пусть $\varphi = \psi^2, \psi > 0$ (в частности $\psi$ самосопряжен). Пусть $\mu_1, ..., \mu_l$ – собтвенные значения $\psi$, $V_i' = V_{\mu_i}(\psi)$. То есть $V = V_1' \oplus ... \oplus V_l'$. Тогда все $V_i'$ – $\varphi$-инвариантны, причем $\varphi_{V_i'}$ – умножение на $\mu_i^2$ ($\mu_i^2 \neq \mu_j^2$ при $i \neq j$). То есть $l = m$ и $\mu_i^2 = \lambda_i,\ V_i' = V_i$.$\square$
*Замечание.* Вообще говоря, уравнение $\varphi = \psi^2$ имеет много решений даже в случае самосопряженного оператора $\varphi$. (*Задача* Сколько, и от чего это число зависит.)
**Теорема (полярное разложение линейного оператора).**
Пусть $(V, <.,.>)$ – пространство со скалярным произведением, $\varphi \in EndV$, $\det \varphi \neq 0$. Тогда $\exists!$ $\psi, \theta \in EndV$ такие, что $\psi > 0, \theta$ – ортогональный (унитарный), и $\varphi = \psi\theta$.
*Комментарий:* Пусть $\dim V = 1,\ F = \mathbb{C}$. Тогда $\varphi =$ умножение на $z \in \mathbb{C},\ z \neq 0$. $\varphi =$ умножение на $r > 0$, $\theta$ – поворот на угол $\alpha$. То есть имеем тригонометрическую форму $z$.
*Доказательство:* ! : $\varphi^* = \theta^*\psi^* = \theta^{-1}\psi \Rightarrow \varphi\varphi^* = \psi^2 > 0 \Rightarrow \psi = \sqrt{\varphi\varphi^*}, \theta = \psi^{-1}\varphi$.
$\exists$ : Рассмотрим $\varphi\varphi^*$. Имеем $(\varphi\varphi^*)^* = \varphi\varphi^*$ самосопряжен; $< \varphi\varphi^*(x), x >=<$

$\varphi^*(x), \varphi^*(x) > > 0\ \forall x \neq 0$. Итак $\varphi\varphi^* > 0$. Положим $\psi := \sqrt{\varphi\varphi^*},\ \theta = \psi^{-1}\varphi$. По определению $\psi > 0$. Далее $\theta^* = \varphi^*\psi^{-1},\ \theta\theta^* = \psi^{-1}\psi^2\psi^{-1} = id.\square$
*Замечания* 1) Имеем "левосторонний" вариант $\varphi = \tilde{\theta}\tilde{\psi}$, где ...
2) Если $\varphi$ – нормален, то правосторонний и левосторонний вариант совпадают. Обратно, если совпадают, то нормален (почему?)

*Пример.* $\dim V = 2,\ F = \mathbb{R}$. $\varphi$ зажается матрицей $A = \begin{pmatrix} 1 & -2 \\ 2 & -1 \end{pmatrix}$. Тогда $AA^* = \begin{pmatrix} 5 & 4 \\ 4 & 5 \end{pmatrix}$, собственные значения $3, 1$, собственные векторы $1/\sqrt{2}(1,1), 1/\sqrt{2}(-1,1)$. Отсюда $B = \sqrt{AA^*} = \begin{pmatrix} 2 & 1 \\ 1 & 2 \end{pmatrix}$, $B^{-1}A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$.

## 4. Полилинейная алгебра

4.1. **Тензорное произведение линейных пространств.** Пусть $V_1, V_2$ – линейные пространства над $F$.
*Определение.* Тензорное произведение $V_1$ и $V_2$ – это пара $(W, \otimes)$, где $W$ – линейное пространство над $F$, $\otimes : V_1 \times V_2 \to W$ $((v_1, v_2) \to v_1 \otimes v_2)$ – билинейное отображение, причём (свойство универсальности) для любого билинейного отображения $V_1 \times^f V_2 \times W \exists!$ линейное отображение $\tilde{f} : W \to \tilde{W}$ такое, что $f(v_1, v_2) = \tilde{f}(v_1 \otimes v_2)$, то есть коммутативна диаграмма

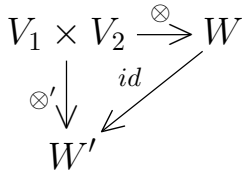
$$\begin{array}{ccc} V_1 \times V_2 & \xrightarrow{\otimes} & W \\ {\scriptstyle f}\downarrow & \swarrow{\scriptstyle \tilde{f}} & \\ \tilde{W} & & \end{array}$$

*Предложение* Тензорное произведение единственно в следующем смысле: если $(W, \otimes)$ и $(W', \otimes')$ – тензорные произведения $V_1$ и $V_2$, то существует и единственный изоморфизм $\varphi$ такой, что коммутативна диаграмма:

$$\begin{array}{ccc} V_1 \times V_2 & \xrightarrow{\otimes} & W \\ {\scriptstyle \otimes'}\downarrow & \swarrow{\scriptstyle \varphi} & \\ W' & & \end{array}$$

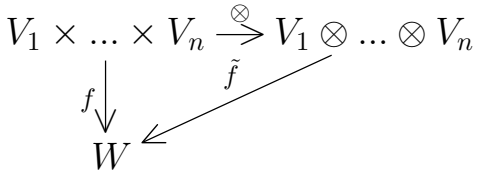
*Доказательство:* по определению, существуют и единственны линейные отображения $\varphi : W \to W'$ и $\psi W' \to W$ такие, что ...
Почему они взаимно обратны?

$$\begin{array}{ccc} V_1 \times V_2 & \xrightarrow{\otimes} & W \\ {\scriptstyle \otimes'}\downarrow & \swarrow{\scriptstyle \psi\circ\varphi} & \\ W' & & \end{array}$$




Значит $\psi \circ \varphi = id$. Аналогично $\varphi \circ \psi = id$.$\square$
*Замечание.* Это утверждение и доказательство – пример рассуждения из так называемой "теории категорий".
Обозначение тензорного произведения $V_1 \otimes V_2$, точнее $V_1 \times V_2 \to^{\otimes} V_1 \otimes V_2$ – билинейно.
**Теорема.** Тензорное произведение существует.
*Доказательство:* Пусть $V_1, V_2$ – линейные пространства над $F$. Построим $W = V_1 \otimes V_2$ и $\otimes : V_1 \times V_2 \to W$.
*Конструкция 1* Пусть $e_i (i \in I)$ – базис в $V_1$, $u_j$ – базис в $V_2$. Пусть $W$ – линейное пространство с базисом $e_i \otimes u_j$ (и любым упорядочиванием). То есть элементы $W$ – это $\sum \gamma_{ij} e_i \otimes u_j$. Определим $\otimes : V_1 \times V_2 \to W$ так: $(e_i, u_j) \to e_i \otimes u_j$ – продолжаем по билинейности, то есть если $v = \sum \alpha_i e_i, u = \sum \beta_j u_j$, то $\otimes(v_1, v_2) = \sum \alpha_i \beta_j e_i \otimes u_j$. Проверим свойство универсальности. Пусть $f : V_1 \times V_2 \to \tilde{W}$ какое-нибудь билинейное отображение. Определим $\tilde{f} : W \to \tilde{W} : \tilde{f}(e_i \otimes u_j) := f(e_i, u_j)$ и продолжаем по билинейности. Если $v_1 = \sum \alpha_i e_i, v_2 = \sum \beta_j v_j$, то $\tilde{f}(v_1 \otimes v_2) = \tilde{f}(\sum \alpha_i \beta_j e_i \otimes e_j) = \sum \alpha_i \beta_j f(e_i, u_j) = f(v_1, v_2)$.
*Конструкция 2:* Рассмотрим линейное пространство $M$ с базисом $V_1 \times V_2$. Далее рассмотрим $M_0 \subset M$, $M_0$ порождено элементами вида $(v_1' + v_1'', v_2) - (v_1', v_2) - (v_1'', v_2); (\lambda v_1, v_2) - \lambda(v_1, v_2); (v_1, v_2' + v_2'') - (v_1, v_2') - (v_1, v_2''); (v_1, \lambda v_2) - \lambda(v_1, v_2)$. Положим $W := M/M_0$ и $v_1 \otimes v_2 := (v_1, v_2) + M_0$. По построению, $\otimes : V_1 \times V_2 \to W$ билинейно. Свойство универсальности: пусть $f : V_1 \times V_2 \to \tilde{W}$ билинейно. Требуется $f : W \to \tilde{W} : \ \tilde{f}(v_1 \otimes v_2) = f(v_1, v_2)$. Так как $(v_1, v_2)$ – базис в $M$, то $v_1 \otimes v_2 = (v_1, v_2) + M_0, \ W = M/M_0 \Rightarrow$ единственность $\tilde{f}$.
Для доказательства существования $\tilde{f}$ рассмотрим $g : M \to W, g((v_1, v_2) := f(v_1, v_2))$ и продолжим по линейности. Заметим, что $M_0 \subset Kerg$. Отсюда имеем $\tilde{F} : m/m_0 \to W \ \tilde{f}((v_1, v_2) + M_0) = g((v_1, v_2)) = f(v_1, v_2)$.$\square$
*Следствие* $\dim(V_1 \otimes V_2) = \dim V_1 \dim V_2$ *Замечания* 1) если $e_i$ – базис в $V_1$, $u_j$ – базис в $V_2$, то $e_i \otimes u_j$ – базис в $V_1 \otimes V_2$. Такой базис будем называть тензорным базисом.
2) $v_1 \times v_2 = 0 \Leftrightarrow v_1 = 0$ или $v_1 = 0$
3) Вовсе не любой элемент $V_1 \otimes V_2$ имеет вид $v_1 \otimes v_2$. Общий вид: $\sum_i v_1^{(i)} \otimes v_2^{(i)}$.
*Замечание.* По определению, для любого линейного просранства $W$ есть естественная биекция между билинейными отображениями $V_1 \times V_1 \to W$ и $Hom(V_1 \otimes V_2, W)$. На самом деле эта биекция есть изоморфизм линейных пространств.

Обобщение: пусть $V_1, ..., V_n$ – линейные пространства над $F$. Их тензорное произведение – это линейное пространство $V_1 \otimes V_2 \otimes ... \otimes V_n$ вместе с полилинейным отображением $\otimes : V_1 \times ... \times V_n \to V_1 \otimes ... \otimes V_n$, причем выпоолнено свойство универсальности: для любого полилинейного отображения $f \exists! \tilde{f}$, такое, что коммутативна диаграмма:




Точно так же доказывается, что тензорное произведение существует и единственно...
В частности, если $e_j^(k)$ – базис в $V_k$, то $e^{(1)}_{i_1} \otimes ... \otimes e^{(1)}_{i_1}$ базис в $V_1 \otimes ... \otimes V_n$ и $\dim V_1 \otimes ... \otimes V_n = \dim V_1 ... \dim V_n$. Имеется изоморфизм между полилинейными отображениями $V_1 \times ... \times V_n \to W$ и $Hom(V_1 \otimes ... \otimes V_n, W)$.
*Пример.* Пусть $X$ – конечное множество. Рассмотрим пространство $Fun(X)$ – функции на $X$ со значениями в $F$. Базис в $Fun(X)$ образуют характеристические функции точек $\delta_x$, $\delta_x(y) = 0$ при $x \neq y$ и 1 в противном случае. Имее $f = \sum_x f(x)\delta_x$. В частности $\dim Fun(X) = |X|$.
Пусть $X, Y$ – конечные множества. имеется билинейное отображение $Fun(X) \times Fun(Y) \to Fun(X \times Y), (f, g) \to h, h(x, y) = f(x)g(y)$. По определению, ему соответсвует линейное отображение $Fun(X) \otimes Fun(Y) \to Fun(X \times Y)$. Это отображение – изоморфизм, ибо $\delta_x \otimes \delta_y \to \delta_{(x,y)}$. Итак, имеем изоморфизм $Fun(X) \otimes Fun(Y) \cong Fun(X \times Y)$.
*Замечание.* Для бесконечных множеств отображение $Fun(X) \otimes Fun(Y) \to Fun(X \times Y)$ не является изоморфизмом.
*Пример: подъем поля скаляров*
Пусть $F \subset K$ – расширение полей, $V$ – линейное пространство над $F$. Рассмотрим $K \otimes_F V$. Определим на нем структуру линейного пространства над $K$ так: если $\lambda \in K$, то $\lambda(a \otimes v) = (\lambda a) \otimes v$. Почему определение корректно? Рассмотрим отображение $K \times V \to K \times V \to K \otimes_F V$, $(a, v) \to (\lambda a, v) \to (\lambda a) \otimes v$. Это отображение билинейно над $F$, следовательно оно "проноситься" через тензорное произведение.
Говорят, что $V^K := K \otimes_F V$ получено из $V$ подъёмом поля скаляров. Как устроено $V^K$? Рассмотрим $V \to V^K$, $v \to 1 \otimes V$ – это отображение $F$ линейно и инъективно.
*Предложение.* Если $e_1, ..., e_n$ – базис в $V$ над $F$, то $1 \otimes e_1, ..., 1 \otimes e_n$ – базис в $V^K$ над $K$.
*Упражнение.* $F \otimes_F V = V$.
*Пример: Алгебры*

Алгебра над полем $F$ – это линейное пространство $A$ над $F$ с заданым билинейным отображением ("умножением") $A \times A \to A$. Используя тензорный формализм, можно считать, что задано отображение $A \otimes A \to A$.
Примеры алгебр: 1) $A = Mat(n, F)$
2) $A = Fun(X)$
3) $A = \mathbb{R}^3$, умножение – векторное произведение.
4) $A = Mat(n, F), [X, Y] = XY - YX$.
*Тензорное произведение линейных отображений*
Пусть $\varphi_i \in Hom(V_i, W_i),\ i = 1, 2$. Тогда имеем $V_1 \times V_2 \to W_1 \times W_2 \to W_1 \otimes W_2$, то есть имеем отображение $V_1 \otimes V_2 \to W_1 \times W_2$.

## 4.2. **Канонические изоморфизмы. I Ассоциативность:**

*Предложение.* $V_1 \otimes V_2 \otimes V_3 \cong (V_1 \otimes V_2) \otimes V_3$ (канонический изоморфизм)
*Доказательство:* Имеем билинейное отображение $V_1 \times V_2 \overset{\otimes}{\to} V_2 \otimes V_2,\ (V_1 \otimes V_2) \times V_3 \to^{\otimes} (V_1 \otimes V_2) \otimes V_3$.
Они дают $f : V_1 \times V_2 \times V_3 \to (V_1 \otimes V_2) \otimes V_3$ – трилинейно. То есть имеем отображение $\tilde{f} : V_1 \otimes V_2 \otimes V_3 \to (V_1 \otimes V_2) \otimes V_3,\ v_1 \otimes v_2 \otimes v_3 \to (v_1 \otimes v_2) \otimes v_3$. Оно переводит базис в базис то есть является изоморфизмом. □
Аналогично $V_1 \otimes V_2 \otimes V_3 = V_1 \otimes (V_2 \otimes V_3)$.
И вообще, $V_1 \otimes ... \otimes V_n =$ тому же с любой расстановкой скобок.
*Замечание.* Возникает, однако, вопрос о сочетании этих изоморфизмов. Мы построили изоморфизм $\Phi_{V_1,V_2,V_3} : (V_1 \otimes V_2) \otimes V_3 \to V_1 \otimes (V_2 \otimes V_3)$. Нетрудно проверить, что коммутативна следующая диаграмма:

$$\begin{array}{ccccc}
((V_1 \otimes V_2) \otimes V_3) \otimes V_4 & \xrightarrow{\Phi_{V_1,V_2,V_3} \otimes id} & (V_1 \otimes (V_2 \otimes V_3)) \otimes V_4 & \xrightarrow{\Phi_{V_1,V_2 \otimes V_3,V-4}} & V_1 \otimes ((V_2 \otimes V_3) \otimes V_4) \\
\Big\downarrow{\scriptstyle \Phi_{V_1 \otimes V_2,V_3,V_4}} & & & & \Big\downarrow{\scriptstyle id \otimes \Phi_{V_2,V_3.V_4}} \\
(V_1 \otimes V_2) \otimes (V_3 \otimes V_4) & & \xrightarrow{\qquad\qquad\Phi_{V_1,V_2,V_3 \otimes V_4}\qquad\qquad} & & V_1 \otimes (V_2 \otimes (V_3 \otimes V_4))
\end{array}$$

Соответствующее условие на систему изоморфизмов $\Phi$ называется "уравнение пятиугольника". Можно доказать, что совпадение любых "изоморфизмов ассоциативности" с общим началом и концом сводится к "уравнению пятиугольника".

**II Коммутативность:**

*Предложение.* $V_1 \otimes V_2 \cong V_2 \otimes V_1$ (естественный изоморфизм).
*Доказательство:* $V_1 \times V_2 \to^{\sigma} V_2 \times V_1 \to^{\otimes} V_2 \otimes V_1,\ \sigma(v_1, v_2) = (v_2, v_1)$ билинейно $\Rightarrow$ имеем отображение $V_1 \otimes V_2 \to V_2 \otimes V_1$. Это изоморфизм. □
*Замечание.* Отождествлять $V_1 \otimes V_2$ с $V_2 \otimes V_1$ нужно осторожно. Если $V_1 = V_2 = V$, то изоморфизм $V_1 \otimes V_2 = V_2 \otimes V_1 = V \otimes V$ не тождественный!
Обобщение: если $\pi \in S_n$, то возникает изоморфизм $f_\pi : V_1 \otimes ... \otimes V_n \to V_{\pi(1)} \otimes ... \otimes V_{\pi(n)}$. При этом $f_{\pi_1} f_{\pi_2} = f_{\pi_1 \pi_2}$ .

**III Двойственность:**
*Предложение.* $(V_1 \otimes V_2)^* = V_1^* \otimes V_2^*$ (естественный изоморфизм).
*Доказательство* Рассмотрим $V_1^* \times V_2^* \to \{$билинейные $V_1 \times V_2 \to F\} \to Hom(V_1 \otimes V_2, F) = (V_1 \otimes V_2)^*$. Это отображение билинейно $\Rightarrow$ получаем $V_1^* \otimes V_2^* \to (V_1 \otimes V_2) *\ \tilde{f}(v_1 \otimes v_2) = f_1(v_1)f_2(v_2)$. Это изоморфизм. $\square$
*Замечание.* 1) $\tilde{f}(v_1 \otimes v_2) = f_1(v_1)f_2(v_2)$. С другой стороны $f_1 \otimes f_2$ можно положить как $f_1 \otimes f_1 : V_1 \otimes V_2 \to F \otimes F$. Можно отождествить $F \otimes F$ с $F$, при этом все согласовано.
2) Аналогично $(V_1 \otimes ... \otimes V_n)^* = V_1^* \otimes ... \otimes V_n^*$.
3) Если $V_1$ или $V_2$ бесконечномерны, то имеется инъекция $V_1^* \otimes V_2^* \to (V_1 \otimes V_2)^*$. Оно не является изоморфизмом.
**IV**
*Предложение.* $Hom(V, W) = V^* \otimes W$ (естественный изоморфизм).
*Доказательство:* Рассмотрим $V^* \times W \to Hom(V, W),\ (f, v) \to \varphi,\ \varphi(v) = (f, v)w$. То есть имеем $V^* \otimes W \to Hom(V, W)$. На базисе $f^i w_j \to \phi^i_j$, где ... $\square$
*Замечание.* Если $\dim V = \infty$, то имеется вложение $V^* \otimes W \to Hom(V, W)$, не изоморфизм.
В частности, $EndV = V^* \otimes V$. $EndV$ – это алгебра. Что соответствует $id \to$? Чтобы выяснить это, рассмотрим следующее понятие
*Свертка*
Имеется естественный линейный функционал на $V^* \otimes V$, имеем $V^* \times V \to F\ (f, v) \to f(v)$ билинеен, значит линеен $V^* \otimes V \to F,\ f \otimes v \to f(v)$. Это и есть свёртка.
*Упражнения.*1) Конструкция $Hom(U, V) \times Hom(V, W) \to Hom(U, W)$, описывается так: $(U^* \otimes V) \otimes (V^* \otimes W) = U^* \otimes (V \otimes V^*) \otimes W \to^{\text{свертка}} U^* \otimes F \otimes V \to U^* \otimes W$
2) Свёртка $V^* \otimes V$ в $F$ соответствует следу $Tr : EndV \to F$.
3) Чему соответсвует свёртка $(V^* \otimes V)^* \to V^* \otimes V^*$.
Свёртка имеет обобщение $V_1 \otimes ... \otimes V_n \to ...,\ V_i = V,\ V_j = V^*$....
**V**
*Предложение.* $Hom(U \otimes V, W) = Hom(U, Hom(V, W))$ (естественное отображение).
*Доказательство:* $Hom(U \otimes V, W) \to \{$ билинейные $U \times V \to W$. С другой стороны, если $f : U \times V \to W$ билинеен, то имеем $u \to \varphi_u : V \to W,\ \varphi_u(v) = f(u, v)$. Имеем, $f \to \varphi \in Hom(U, Hom(V, W))$. Это изоморфизм. $\square$

4.3. **"Классические обозначения" и координатная запись.** Обозначим $T^q_p(V) := (V^*)^{\otimes p} \otimes V^{\otimes q}$ – пространство тензоров типа $(p, q)$. Соглашение: $T^0_0 = F$.
*Примеры:* 1) $T^1_0(V) = V$

2) $T_1^0 = V^*$ – ковекторы
3) $T_1^1 = V^* \otimes V = EndV$
4) $T_2^0 = V^* \otimes V^* = (V \otimes V)^* = \{\text{билинейные} V \times V \to F\}$
5) $T_2^1 = (V \otimes V)^* \otimes V = Hom(V \otimes V, V) = \{\text{струтуры алгебры на } V\}$ (то есть "структурный тензор алгебры" – элемент $T_2^1$)
*Координаты:*
Пусть $e_1, ..., e_n$ – базис в $V$. Если $x \in V$, то $x = \sum x^i e_i,\ x^i \in F$. "Правило Эйнштейна": пишут $x = x^i e_i$, подразумевается суммирование по повторяющимся индексам вверху-внизу.
Далее, пусть $e^1, ..., e^n$ – двойственный базис в $V^*$, то есть $e^i(e_j) = \delta_i^j$. Тогда ковекторы – это $y = y_i e^i$.
Далее, тензорный базис в $T_p^q(V)$ образуют тензоры $e^{i_1} \otimes e^{i_2} \otimes ... \otimes e^{i_p} \otimes e_{j_1} \otimes ... \otimes e_{j_q}$.
В координатах тензор $t \in T_p^q(V)$ записывается так:

$$t = t^{j_1,...,j_q}_{i_1,...,i_p} e^{i_1} \otimes ... \otimes e^{i_p} \otimes e_{j_1} \otimes ... \otimes e_{j_q}$$

*Примеры* 1) $\varphi \in T_1^1,\ \varphi = \varphi_j^i e^j e_i$. Имеем $\varphi(e_j) = \varphi_j^i e_i$, то есть $\varphi_j^i$ – матрица $\varphi$ в базисе $e$.
2) $b \in T_2^0(V),\ b = b_{ij} e^i \otimes e^j$, $b(e_i, e_j) = b_{ij}$...
*Замена базиса.*
Пусть $\tilde{e}_i$ – другой базис в $V$. Пусть $A = T_{e \to \tilde{e}}$ – матрица перехода.
*Лемма.* Матрица перехода от базиса $e^i$ к $\tilde{e^i}$ в пространстве $V^*$ – это матрица $(A^T)^{-1}$.
*Доказательство:* Рассмотрим $C = B^{-1} = (b_i^j)$, где $e^j = c_i^j \tilde{e^i}$. Тогда $A_j^i = e^i(a_j^k e_k) = c^i(\tilde{e_j}) = c_j^i \Rightarrow C = A^T$. □
Обозначение: $B = (b_i^j)$, $\tilde{e^j} = b_i^j e^i$.
*Предложение.* Пусть $t \in T_p^q(V),\ t = t^{j_1,..,j_q}_{i_1,...,i_p} e^{i_1} \otimes ... \otimes e^{i_p} \otimes e_{j_1} \otimes ... \otimes e_{j_q} = \tilde{t}^{l_1,..,l_q}_{k_1,...,k_p} \tilde{e^{k_1}} \otimes ... \otimes \tilde{e^{k_p}} \otimes \tilde{e_{l_1}} \otimes ... \otimes \tilde{e_{l_q}}$. Тогда $t^{j_1,..,j_q}_{i_1,...,i_p} = b^{k_1}_{i_1} ... b^{k_p}_{i_p} a^{j_1}_{l_1} ... a^{j_p}_{l_p} \tilde{t}^{l_1,..,l_q}_{k_1,...,k_p}$.
s *Доказательство:* $t = ...$ (выражаем $\tilde{e}$ через $e$) □
*Тензорное умножение*
Рассмотрим билинейное отображение $T_p^q \times T_p'^{q'} \to^{\otimes} T_{p+p'}^{q+q'}$. Задаётся так: $(V^* \otimes ... \otimes V^* \otimes V \otimes ... \otimes V) \times (V^* \otimes ... \otimes V^* \otimes V \otimes ... \otimes V) \to^{\otimes} V^* \otimes ... \otimes V^* \otimes V \otimes ... \otimes V \otimes V^* \otimes ... \otimes V^* \otimes V \otimes ... \otimes V \to V^* \otimes ... \otimes V^* \otimes V \otimes ... \otimes V$. $T_0^1 \times T_0^1 \to T_0^2$ – это "обычное" тензорное произведение. При этом отображении пары векторов из тензорного базиса переходят в тензорный базис. Поэтому в координатах $(t \otimes t')^{j_1,...,j_s,j'_1,...,j'_{s'}}_{i_1,...,i_p,i'_1,...,i'_{p'}} = t^{j_1,...,j_s}_{i_1,...,i_p} t'^{j'_1,...,j'_{s'}}_{i'_1,...,i'_p}$
В частности, отсюда видно, что $\otimes$ ассоциативно.
*Примеры.*1) $T_1^0 \times T_1^0 \to T_2^0$. Если $f_1, f_2 \in V^*$, то $f_1 \otimes f_2 \to b$, где $b(x_1, x_2) =$

$f_1(x_1)f_2(x_2)$
2) $T^1_1(V)\otimes T^1_1(V)\to^{\otimes} T^2_2(V)$, то есть имеем $EndV\times EndV\to^{\otimes} End(V\otimes V)$.
*Проверка 1:* $f\otimes V\to\varphi$, $\varphi(x)=f(x)v$. Тогда $(f_1\otimes v_1, f_2\otimes v_2)\to^{\otimes} f_1\otimes f_1\otimes v_1\otimes v_2\to\varphi$, где $\varphi(x_1\otimes v_2)=f(x_1)f(x_2)v_1\otimes v_2$.
*Проверка 2* В координатах (*Упражнение*).
*Упражнение.* Можно отождествить $T^q_p(V)=\{$полилинейные $V\otimes ...\otimes V\otimes V^*\otimes ...\otimes V^*\to F\}$. В этих терминах $\otimes$ задано так: $(t\otimes t')(v_1,...,v_{p+p'},f_1,...,f_{q+q'})=t(v_1,...,v_p,f_1,...,f_q)t'(v_{p+1},...,v_{p+p'},f_{q+1},...,f_{q+q'})$.
*Свертка в координатах*
1) $V^*\otimes V\to F, \varphi=\varphi^i_j e_i\otimes e^j$. $\varphi\to\varphi^i_j e_i(e_j)=e^i_i\ (=Tr\varphi)$
2) "Обобщенная свёртка" Рассмотрим $a=1,...,p$ $b=1,...,q$. Свертка по $(a,b)$ – это отображение $T^q_p\to T^{q-1}_{p-1}$, дейтсвующее как свёртка на $a$'ом множителе $V$ и $b$'ом множителе $V^*$ в разложении $V\otimes ...\otimes V\otimes V^*\otimes ...\otimes V^*$.
*Упражнение.* При свертке $t\to t'$

$$t'^{j_1,...,j_{b-1},j_{b+1},...,j_q}_{i_1,...,i_{a-1},i_{a+1},...,i_p}=t^{j_1,...,j_{b-1},k,j_{b+1},...,j_q}_{i_1,...,i_{a-1},k,i_{a+1},...,i_p}$$

4.4. **Симметрические и кососимметрические тензоры.** Пусть $V$ – линейное пространство над $F$. Будем предполагать, что $charF=0$. Рассмотрим $V^{\otimes q}$. Напомним, что для любой $\pi\in S_q$ имеем $f_\pi\in End(V^{\otimes q})$, $f_\pi(v_1\otimes ...\otimes v_q)=v_{\pi(1)}\otimes ...\otimes v_{\pi(q)}$.
*Определение.* Тензор $t\in V^{\otimes q}$ называется симметрическим (кососимметрическим), если $\forall\pi\in S_q$ $f_\pi(t)=t(=tsgn\ \pi)$.
Обозначение: $S^q(V)$ – множество симметрических тензоров, $\Lambda^q V$ – множество кососимметрических тензоров.
Так как $S^q(V)=\cap_{\pi\in S_q}Ker(f_\pi-id)$, $\Lambda^q V=\cup_{\pi\in S_q}(f_\pi-id\cdot sgn\ \pi)$, то $S^q,\Lambda^q$ – подпространства в $V^{\otimes q}$.
*Упражнение.* $V\otimes V=S^2(V)\dotplus\Lambda^2 V$.
*Упражнение.* $V^*\otimes V^*$ – билинейные функционалы; при этом $S^2$ – симметрические билинейные функционалы, $\Lambda^2$ – кососимметрическиею
Рассмотрим $Sym, Alt\in End(V^{\otimes q}, Sym:=1/q!\sum_{\pi\in S_q}f_\pi$ (симметризация), $Alt:=1/q!\sum_{\pi\in S_q}sgn\ \pi\cdot f_\pi$ (Альтернирование).
*Предложение.* 1) $Sym$ – проектор на $S^q$, то есть $Sym^2=Sym$, $ImSym=S^q$.
2) $Alt$ – проектор на $\Lambda^q$.
Пусть $e_1,...,e_n$ – базис в $V$. Обозначим $e_{i_1}\cdot ...\cdot e_{i_q}:=Sym(e_{i_1}\otimes ...\otimes e_{i_q})$. Заметим, что это "произведение" не зависит от порядка множителей, то есть достаточно рассмотреть $e_1^{a_1}\cdot ...\cdot e_n^{a_n}$, где $\sum_i a_i=q$.
*Предложение.* Тензоры $e_1^{a_1}...e_n^{a_n}$, где $\sum_i a_i=q$, образуют базис в $S^q(V)$. В частности, $\dim S^q(V)=\binom{n+q-1}{q}$.
*Доказательство:* $e_1^{a_1}...e_n^{a_n}$, как образ базиса в $V^{\otimes q}$ , порождает $ImSym$, то есть

$S^q(V)$. Осталось: они линейно независимы.
Пусть $\sum c_{a_1,...,a_n} e_1^{a_1}...e_n^{a_n} = 0$, то есть $\sum c_{a_1,...,a_n} Sym(e_1 \otimes ... \otimes e_1 \otimes e_2 \otimes ... \otimes e_n) = 0$. Коэффициент при $e_1 \otimes ... \otimes e_1 \otimes e_2 \otimes ... \otimes e_n (e_1 - a_1$ раз и т.д.) – это $c_{a_1,...,a_n} \cdot K/q!$, где $K$ – число перестановок, переставляющих только отдельно первые $a_1$ элементов, отдельно следующие $a_2$ и так далее. Значит (ибо это часть базиса) $c_{a_1,...,a_n} = 0$. $\square$
Перейдём к $\Lambda^q V$. Обозначим $e_{i_1} \wedge ... \wedge e_{i_q} = Alt(e_{i_1} \otimes ... \otimes e_{i_q})$. Заметим, что при перестановке индексов $\pi$ "произведение" умножается на знак $\pi$. Далее рассмотрим $e_{i_1} \wedge ... \wedge e_{i_q}$, где $1 \le i_1 < ... < i_q \le n$.
*Предложение.* 1) Если $q > n$, то $\Lambda^q V = 0$.
2) Если $q \le n$, то тензоры $e_{i_1} \wedge ... \wedge e_{i_q}$, где $1 \le i_1 < ... < i_q \le n$, образуют базис. В частности, $\dim \Lambda^q V = \binom{n}{q}$.
*Доказательство:* 2) Снова $e_{i_1} \wedge ... \wedge e_{i_q}$ порождают $\Lambda^q V$. Линейная независимость: есть $0 = \sum c_{i_1,...,i_q} e_{i_1} \wedge ... \wedge e_{i_q}$. Коэффициент при $e_{i_1} \otimes ... \otimes e_{i_q} - c_{i_1,...,i_q}/(q!) \Rightarrow$ все коэффициенты – нули. $\square$
*Упражнение.* $\dim \sum_{i=1}^{n} \Lambda^q V = 2^n$.
Пусть $\varphi \in End V$. Тогда имеется $\varphi^{\otimes q} \in End(V^{\otimes q})$. Отметив, что для любого $\pi \in S_q$ : $f_\pi \varphi^{\otimes q} = \varphi^{\otimes q} f_\pi$. Отсюда $Sym \varphi^{\otimes q} = \varphi^{\otimes q} Sym$, $Alt \varphi^{\otimes q} = \varphi^{\otimes q} Alt$, то есть $S^q$ и $\Lambda^q$ – пространства, инвариантные относительно $\varphi^{\otimes q}$. В частности, рассмотрим $\varphi^{\wedge q} = \varphi^{\otimes q}|_{\Lambda^q V}$.
*Предложение.* Если $\dim V = n$, то $\varphi^{\wedge n}$ – умножение на det.
*Замечание.* Это "научное" определение $\det \varphi$.
*Доказательство:* Пусть $e_1, ..., e_n$ – базис в $V$. Тогда $e_1 \wedge ... \wedge e_n$ – базис в $\Lambda^n V$. Пусть $\varphi(e_j) = \sum_i a_j^i e_i$, то есть $(a_i^j)$ – матрица $\varphi_e$. Тогда $\varphi^{\wedge n}(e_1 \wedge ... \wedge e_n) = Alt(\varphi(e_1) \otimes ... \otimes \varphi(e_n)) = \sum_{i_1,...,i_n} a_1^{i_1}...a_n^{i_n} e_{i_1} \wedge ... \wedge e_{i_n} = \sum_{\pi \in S_n} = a_1^{\pi(1)}...a_n^{\pi(n)} sgn\ \pi \cdot e_1 \wedge ... \wedge e_n = \det \varphi e_1 \wedge ... \wedge e_n$.$\square$
*Замечание.* $(\varphi\psi)^{\otimes q} = \varphi^{\otimes q}\psi^{\otimes q}$. В частности, $\det(\varphi\psi) = \det(\varphi)\det(\psi)$.
*Тензорная, симметрическая и внешняя алгебра*
Пусть $V$ – линейное пространство над $F$ $(char F = 0)$.
*Тензорная алгебра*
Рассмотрим $T_0(V) = \sum_{q \in \mathbb{Z}_+}^{\cdot} V^{\otimes q}$. Имеется тензорное произведение на $T_0$. Это ассоциативная алгебра с $1 \in F = V^{\otimes 0}$.
*Симметрическая алгебра*
Рассмотрим $S(V) := \sum_{q \in \mathbb{Z}_+}^{\cdot} S^q(V)$. Превратим $S(V)$ в алгебру, положив $t_1 t_2 = Sym(t_1 \otimes t_2)$.
**Теорема** $S(V)$ – ассоциативная, коммутативная алгебра с 1.
*Доказательство:* 1) Если $t_1 = v_1 \otimes ... \otimes v_p, t_2 = v_{p+1} \otimes ... \otimes v_{p+q}$, то $t_1 t_2 = t_2 t_1$. Отсюда $Sym(t_1 \otimes t_2) = Sym(t_2 \otimes t_1)$ для любых тензоров $t_1, t_2$.
2) Единица – это $1 \in F$

3) *Лемма.* $Sym(Sym(t_1)\otimes t_2) = Sym(t_1\otimes Sym(t_2)) = Sym(t_1\otimes t_2)$.
*Доказательство леммы:* $Sym(Sym(t_1)\otimes t_2) = 1/p!\sum_{\pi\in S_p} Sym(f_\pi(t_1)\otimes t_2) = 1/p!\sum_{\pi\in S_p} Sym(t_1\otimes t_2) = Sym(t_1\otimes t_2)$ Аналогично...
$(t_1t_2)t_3 = Sym(Sym(t_1\otimes t_2)\otimes t_3) = Sym(t_1\otimes t_2\otimes t_3) = t_1(t_2t_3)$. $\square$
*Замечание.* На базисе $(e_1^{a_1}...e_n^{a_n})(e_1^{b_1}...e_n^{b_n}) = e_1^{a_1+b_1}...e_n^{a_n+b_n}$.
*Внешняя алгебра (алгебра Грассмана)*
Рассмотрим $\Lambda V = \sum_{q\in\mathbb{Z}_+}^{\cdot} \Lambda^q V$. Отметим, что $\dim \Lambda V = 2^n$. Если $t_1\in\Lambda^p V, t_2\in\Lambda^q V$, то определим $t_1\wedge t_2 = Alt(t_1\otimes t_2)$, и продолжим $\wedge$ по билинейности на $\Lambda V$.
**Теорема.** $\Lambda V$ – ассоциативная алгебра с 1. Она кососкоммутативна (антикоммутативна) в следующем смысле: если $t_1\in\Lambda^p V, t_2\in\Lambda^q V$, то $t_1\wedge t_2 = (-1)^{pq} t_2\wedge t_1$.
*Доказательство:* Если $t_1\in V^{\otimes p}, t_2\in V^{\otimes q}$, то $t_2\otimes t_1 = f_\pi(t_1\otimes t_2)$, где $\pi\in S_{p+q}$ – произведение $pq$ транспозиций. Поэтому $Alt(t_2\otimes t_1) = (-1)^{pq}Alt(t_1\otimes t_2) \Rightarrow$ умножение кососимметрично. (*Упражнение* $Alt f_\pi = sgn\ \pi Alt$).
2)*Лемма* $Alt(Alt(t_1)\otimes t_2) = Alt(t_1\otimes Alt(t_2)) = Alt(t_1\otimes t_2)$
*Доказательство леммы:* $Alt(Alt(t_1)\otimes t_2 = 1/p!\sum_{\pi\in S_p} sgn\ \pi\cdot Alt(f_\pi(t_1)\otimes t_2) = 1/p!\sum_{\pi\in S_p} sgn\ \pi\cdot Alt(f_{\tilde\pi}t_1\otimes t_2) = 1/p!\sum_{\pi\in S_p} sgn\ \pi\cdot f_{\tilde\pi}Alt(t_1\otimes t_2) = 1/p!\sum_{\pi\in S_p}(sgn\ \pi)^2\cdot Alt(t_1\otimes t_2) = Alt(t_1\otimes t_2)$. Аналогично...
*Упражнение.* Выведите из леммы ассоциативность $\wedge$. $\square$
*Замечание.* Наше определение симметричной внешней алгебры содержит деление на $p!$, то есть использует то, что $charF = 0$. Это можно обойти с помощью другого определения. Именно, рассмотрим $I^q, J^q\subset V^{\otimes q}$, определенные так: $I^q$ – линейная оболочка тензоров вида $(t - f_{pi}(t)),\ t\in V^{\otimes q}$, $J^q$ – линейная оболочка тензоров вида $t - sgn\ \pi f_\pi(t)$.
Рассмотрим $\tilde S^q(V) := V^{\otimes q}/I^q$, $\tilde\Lambda^q V := V^{\otimes q}/J^q$. Далее $\tilde S(V) = \sum \tilde S^q(V)$, $\tilde\Lambda V = \sum \tilde\Lambda^q V$. Определим произведение классов, как класс тензорного произведения.
*Задача.* Эта операция корректна и задает на $\tilde S(V),\ \tilde{Lambda}V$ структуру алгебры. При этом $\tilde S(V)\cong S(V),\ \tilde\Lambda V\cong\Lambda V$.
На самом деле $\tilde S(V) = T_0(V)/I, \tilde\Lambda(V) = T_0(V)/J$, где $I := \sum^{\cdot} I^q,\ J := \sum^{\cdot} J^q$. Такое определение годится и при $charF > 0$.
*Поливекторы* Элементы $\Lambda^p V$ называются $p$-векторами. $p$-вектор разложим, если его можно представить в виде $v_1\wedge ...\wedge v_p$.
*Лемма.* Пусть $v_1, ..., v_p\in V$. Тогда $v_1\wedge ...\wedge v_p = 0 \Leftrightarrow v_1, ..., v_p$ – линейно зависимы.
*Доказательство:* $\Rightarrow$: Дополним $v_1, ..., v_p$ до базиса. Тогда $v_1\wedge ...\wedge v_p$ – один из чекторов базиса $\Lambda^p V$.
$\Leftarrow$: Пусть $v_p = \sum_i c^i v_i$. Тогда $v_1\wedge ...\wedge v_p = \sum c^i v_1\wedge ...\wedge v_{p-1}\wedge v_i = 0$.$\square$
"Геометрический смысл" разложимого $p$-вектора – "ориентированый" паралелотоп, натянутыц на $v_1, ..., v_p$.
Пусть $t\in\Lambda^p V$. Рассмотрим $Ann(t) = \{x\in V | x\wedge t = 0\}$ – аннулятор $t$.

**Теорема (критерий разложимости).** Пусть $0 \neq t \in \Lambda^p V$. Если $t$ разложим, то $\dim Ann(t) = p$. В противном случае $\dim Ann(t) < p$.

*Доказательство:*1) Пусть $t = e_1 \wedge ... \wedge e_n$. Дополним $e_i$ до базиса. Покажем, что $Ann(t) = Lin\{e_1, ..., e_p\}$. Для любого $i \leq p e_i \wedge t = 0 \Rightarrow V^{\otimes q}/I^q Ann(t) \supset Lin\{e_1, ..., e_p\}$. Обратно, если $x = \sum x^i e_i$, то $0 = x \wedge t = \sum x^i e_i \wedge e_1 \wedge ... \wedge e_p \Leftrightarrow x^i = 0, \forall i > p$.

2) Пусть $t$ произволен, $\dim Ann(t) = r$. Пусть $e_1, ..., e_r$ – базис в $Ann(t)$. Дополним его до базиса $e_1, ..., e_n$. Запишем $t = t^{i_1,...,i_p} e_{i_1} \wedge ... \wedge e_{i_p}$. Пусть $j \leq r$. Тогда $0 = e_j \wedge t = t^{i_1,...,i_p} e_j \wedge e_{i_1} \wedge ... \wedge e_{i_p} \Rightarrow t^{i_1,...,i_p} = 0$ при $j \notin \{i_1, ..., i_p\}$ . Значит $r \leq p$ и $t = e_1 \wedge ... \wedge e_r \wedge (\sum t^{1,...,r,i_1,...,i_{p-r}} e_{i_1} \wedge ... \wedge e_{i_{p-r}})$. Если $r = p$, то $t = \lambda e_1 \wedge ... \wedge e_p$ – разложим. $\square$

*Примеры.* 1) Любой 0-вектор и любой $n$-вектор разложим.

2) Любой 1-вектор разложим. Покажем, что любой $n-1$-вектор разложим. $\forall x \in V$ имеем линейное отображение $\Lambda^{n-1} V \to \Lambda^n V$, $t \to x \wedge t$. Но $\dim \Lambda^n V = 1$, то есть если $e_1, ..., e_n$ – базис в $V$, то $x \wedge t = f(x) e_1 \wedge ... \wedge e_n, f \in V^*$. $x \in Ann(t) \Leftrightarrow f(x) = 0$. Значит $Ann(t) = Ker f$. Если $t \neq 0$, то $f \neq 0$ и $\dim Ker f = n - 1 \to\sim Ann(t) = n - 1$.

*Упражнение.* "Разложите" $ae_1 \wedge e_2 + be_1 \wedge e_3 + ce_3 \wedge e_1$. Здесь $e_1, e_2, e_3$ – базис в $V$.

Как выглядят условия разлодимости в координатах? Пусть $e_1, ..., e_n$ – базис в $V$, $t \in \Lambda^p V,\ t = \sum t^{i_1,...,i_p} e_{i_1} \wedge ... \wedge e_{i_p}$.

*Предложение.* Существует система полиномиальных уравнений от $\binom{n}{p}$ переменных $t^{i_1,...,i_p}$, с целыми коэффициентами такая, что $t$ разложим $\Leftrightarrow$ его компоненты удовлетворяют системе. (Эти уравнения – уравнения Плюккера)

*Доказательство:* Пусть $x \in V$. Условие $x \in Ann(t)$, то есть $x \wedge t = 0$ – это система однородных линейных уравнений. Коэффициенты уравнения – это $\pm t^{i_1,...,i_p}$ или 0. Тогда $t$ – разложим $\Leftrightarrow \dim Ann(t) = p \Leftrightarrow \dim Ann(t) \geq p \Leftrightarrow$ ранг матрицы системы $\leq n - p \Leftrightarrow$ все миноры порядка $n - p + 1$ равны нулю. Это и есть искомая система полиномиальных уравнений. $\square$

*Пример.* $n = 4, p = 2$ $(x^1 e_1 + x^2 e_2 + x^3 e_3)(\sum t^{ij} e_i \wedge e_j) = 0$. Имеем систему

$$\begin{cases} t^{23}x_1 - t^{13}x_2 + t^{12}x_3 = 0 \\ t^{24}x_1 - t^{14}x_2 + t^{12}x_4 = 0 \\ t^{34}x_1 - t^{14}x_3 + t^{13}x_4 = 0 \\ t^{34}x_2 - t^{24}x_3 + t^{23}x_4 = 0 \end{cases}$$

*Упраженение.* Убедитесь, что миноры третьего порядка этой матрицы равны либо 0, либо $\pm t_{ij}(t^{12}t^{34} - t^{13}t^{24} + t^{14}t^{23})$. То есть $t$ – разложим $\Leftrightarrow t^{12}t^{34} - t^{13}t^{24} + t^{14}t^{23} = 0$.

Мы имеем отображение $Ann : \{\text{разложимые } p\text{-векторы}\} \to \{p\text{-мерные подпространства}\}$. Мы уже знаем его сюръективность. Насколько оно инъективно?

*Предложение.* Пусть $t, t' \in \Lambda^p V$ разложимы, и $Ann(t) = Ann(t')$. Тогда $t' = \lambda t, \lambda \in F^*$.
*Доказательство:* Пусть $L := Ann(t) = Ann(t')$. $t = e_1 \wedge ... \wedge e_p,\ t' = e'_1 \wedge ... \wedge e'_p$. Тогда $L = Lin\{e_1, ..., e_p\} = Lin\{e'_1, ..., e'_p\}$, то есть $t, t' \in \Lambda^p L$. Но $\dim \Lambda^p L = 1$.$\square$
*Следствие.* Пусть $t \in \Lambda^p V$ разложим$(\neq 0)$, $v \in Ann(t),\ v \neq 0$. Тогда $\exists$(разложимый)$t_1 \in \Lambda^{p-1} V : t = v \wedge t_1$.
*Упражнение.* Пусть $t_1 \in \Lambda^p V, t_2 \in \Lambda^q V$ – разложимы, $\neq 0$. Пусть $L_i := Ann(t_i)$. Тогда $L_1 \supset L_2 \Leftrightarrow t_1$ делится на $t_2$.
*Предложение* Пусть $t \in \Lambda^2 V,\ t \neq 0$. Тогда $t$ – разложим $\Leftrightarrow t \wedge t = 0$.
*Замечание.* Условие $t \wedge t = 0$ в координатах дают более простую ворму уравнений Плюккера.
*Пример.* $n = 4, p = 2. t = \sum t^{ij} e_i \wedge e_j$. $t \wedge t = (t^{12}t^{34} - t^{13}t^{24} + t^{14}t^{23}) e_1 \wedge e_2 \wedge e_3 \wedge e_4$.
*Доказательство:* $\Leftarrow$: индукция по $n = \dim V$. База, при $n = 2$. Переход $n \to n+1$ : Пусть $e_1, ..., e_n, e_{n+1}$ – базис в $V$. $V' = Lin\{e_1, ..., e_n\}$. Запишем $t = v \wedge e_{n+1} + t'$. Тогда $0 = t \wedge t = t' \wedge t' + t' \wedge e_{n+1} \wedge v + e_{n+1} \wedge v \wedge t' = t' \wedge t' + 2t' \wedge e_{n+1} \wedge v$. Так как $t' \wedge t'$ не содержит $e_{n+1}$, то $t' \wedge t' = 0$. Значит $t' \wedge v \wedge e_{n+1} = 0$. Предположение индукции влечёт разложимость $t'$. Тогда $v \wedge t' = 0$, то есть $v \in Ann(t') \Rightarrow t' = v \wedge v'$. То есть $t = v \wedge (v' + e_{n+1})$ – разложим.

4.5. **Геометрическая интерпритация: проективные пространства и грассманианы.** Пусть $V$ – линейное пространство над $F$.
*Определение.* Проективное пространство, ассоциированое с $V$, это пространство $\mathbb{P}(V)$, точки (элементы) которого есть одномерные подпространства в $V$.
Если $L \subset V,\ \dim L = 1$, то $L = Lin\{v\}, v \in V \setminus \{0\}$. При этом $Lin\{v\} = Lin\{w\} \Leftrightarrow \exists \lambda \in F, \lambda \neq 0 v = \lambda w$. То есть $\mathbb{P}V \leftrightarrow (V \setminus \{o\})/\sim, Lin\{v\} \leftrightarrow [v]$, где $v \sim w \Leftrightarrow w = \lambda v, \lambda \in F^*$.
Пусть $\dim V = n + 1$. Выберем базис в $V \Rightarrow V = F^{n+1}, v = (x_0, ..., x_n)$. Тогда $[v] =: (x_0 : x_1 : ... : x_n)$, где однородные координаты $x_0, ..., x_n$ определены с точностью до общего множителя их $F^*$.
Обозначают $\mathbb{P}^n = \mathbb{P}^n_F := \mathbb{P}(F^{n+1})$.
*Афинные покрытия проетивного пространства*: $\mathbb{P}^n = \bigcup_{i=0}^n A_i$, где $A_i = \{(x_0 : ... : x_n) | x_i \neq 0\}$.
NB: Если $x_i \neq 0$, то $(x_0 : ... : x_i : ... : x_n) = (x_0/x_i : ... : 1 : ... : \widehat{x_n/x_i})$.
Имеем биекции $f_i : A_i \to F^n,\ f_i(x_0 : ... : x_n) = (x_0)/x_i, ..., \widehat{x_i/x_i}, ..., x_n/x_i)$. Геометрический смысл: точки $A_i =$ прямые, которые пересекают "гиперплоскость" $x_i = 1$.
*Стратификация проетивного пространства:* Рассмотрим, скажем, $A_0$ и положим $B_0 := \mathbb{P}^n \setminus A_0$. То есть $\mathbb{P}^n = A_0 \sqcup B_0$. Имеется биекция $A_0 \leftrightarrow \mathbb{A}^n$, а таккже $B_0 \leftrightarrow \mathbb{P}^{n-1}$ . То есть, грубо говоря, $\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{P}^{n-1}$. По индукции

$\mathbb{P}^n = \mathbb{A}^n \sqcup \mathbb{A}^{n-1} \sqcup ... \sqcup \mathbb{A}^0$.

*Пример (с геометрической интерпритацией)* 1) $\mathbb{P}^1$. 2) $\mathbb{P}^2$

*Грассманианы.* $\mathbb{G}r(p, V)$ = множество $p$-мерных подпространств в $V$. Имеется биекция $Ann$ между разложимыми $p$-веторами, с точностью до умножения на константу ($\subset \mathbb{P}(\Lambda^p V)$) и $\mathbb{G}r(p, V)$. При этом $Ann(t_1 \wedge ... \wedge t_n = Lin\{v_1, ..., v_p\})$. То есть имеем вложение $Ann^{-1} : \mathbb{G}r(p, V) \to \mathbb{P}(\Lambda^p V)$.

Опишем его действие в координатах. Пусть $e_1, ..., e_n$ – базис в $V$. $L \in \mathbb{G}r(p, V)$, $L = Lin\{v_1, .., v_p\}$. Тогда $L \to [v_1 \wedge ... \wedge v_p] \in \mathbb{P}(\Lambda^p V)$. В $\mathbb{P}(\Lambda^p V)$ имеем координаты. Пусть $v = \sum_{i=1}^n a_i^j e_j$, $A = (a_i^j) \in Mat(p \times n, F)$.

*Предложение.* $t^{i_1,...,i^p}$ – минор $A$ порядка $p$ расположеный в столбцах $i_1, ..., i_p$.

*Доказательство:* $v_1 \wedge ... \wedge v_p = \sum a_1^{j_1} ... a_p^{j_p} e_{j_1} \wedge ... \wedge e_{j_p}$. Коэффициент при $e_{i_1} \wedge ... \wedge e_{i_p}$ равен $\sum a_1^{\pi(i_1)} ... a_p^{\pi(p)} sgn\ \pi$. Что и требовалось. $\square$

*Замечание.* Мы знаем, что образ $\mathbb{G}r(p, V)$ в $\mathbb{P}(\Lambda^p V)$ описывается уравнениями Плюккера. Эти уравнения однородны, то есть имеют смысл в $\mathbb{P}(\Lambda^p V)$.

*Внешнее умножение и двойственность*

*Задача.* Рассмотрим $\Lambda^p V \times \Lambda^{n-p} V \to \Lambda^n(V)$. Докажите, что если $t_1 \wedge t_2 = 0 \forall t_2 \in \Lambda^{n-p} V$, то $t_1 = 0$. Отсюда канонический изоморфизм $\Lambda^p V = (\Lambda^{n-p} V)^* \otimes \Lambda^n V$.

Рассмотрим $\Lambda(V^*)$ – алгебра внешних форм на $V$.

*Предложение.* $\Lambda^p(V^*) = (\Lambda^p(V))^* = \{$кососимметрические полилинейные функционалы на $V \times ... \times V\}$.

*Доказательство:* 1) $\Lambda^p(V^*) \subset (V^*)^{\otimes p} = (V^{\otimes p})^* \to (\Lambda^p V)^*$. Размерности совпадают. $e^1, ..., e^n$ – базис в $V^*$, то $e^{i_1} \wedge ... \wedge e^{i_p} \to f \in (\Lambda^p V)^*$, где $f(e_{j_1} \wedge ... \wedge e_{j_p}) = 0$, если $\{i_1, ..., i_p\} \neq \{j_1, ..., j_p\}$ и $1/p!$ в противном случае. То есть отображаем в базис $(\Lambda^p V)^*$.

2) $\Lambda^p(V^*) \subset (V^*)^{\otimes p} = (V^{\otimes p})^* = \{p$-линейные$V \times ... \times V \to F\}$.

*Упражнение.* Завершите доказательство.