Алгебра. Конспект 2 сем.

Мастера Конспектов

(по материалам лекций В. А. Петрова,
а также других источников)

12 февраля 2021 г.

Некоторые записи по алгебре.

Содержание

1 Лекция 30.

Пусть R - кольцо главных идеалов, а M - конечно порождённый R-модуль (левый).

$$m_1, \ldots, m_n \in M, \ \ M = \{\sum r_i m_i | r_i \in R\}$$

Пусть $\varphi : R^n \to M$ - функция, которая действует по правилу $e_i \mapsto m_i$ (базисные элементы R^n (именно тривиального базиса) в элементы m_i).

Тогдя ядро $\operatorname{Ker}\varphi \leq R^n$ - подмодуль. Причём равен он $\{(r_i) | \sum r_i m_i = 0\}$ - *соотношения* (линейные) между m_i. А также он есть *свободный* модуль R^k, $k \leq n$.

$$\operatorname{Ker}\varphi = R^k, \ \ R^k \leq R^n$$
$$\psi : R^k \to R^n$$

Подходящей заменой базиса в R^k и R^n можно добиться того, чтобы ψ стала диагональной матрицей (с нижними нулевыми строками, естественно) и числами $d_1 | d_2 | \ldots | d_k$ на диагонали.

Тогда $M \cong R^{n-k} \oplus R/(d_i) \oplus \ldots \oplus R/(d_k)$ (это планируется доказывать, но перед этим нужно ввести несколько определений).

Определение 1. Пусть R кольцо (не обязательно коммутативное), тогда M - *циклический*, если он порождён одним элементом ($M = \{rm | r \in R\}$).

Пусть $\theta : R \to M$ - гомоморфизм R-модулей, действующий по правилу $r \mapsto rm$, он сюръективен и $M \simeq R/\operatorname{Ker}\theta$ по теореме о гоморфизме.

$$\operatorname{Ker}\theta = \{r \in R | rm = 0\} \leq R,$$

что также является левым идеалом.

А если R - область главных идеалов, то циклический модуль выглядит как $R/(d)$. Если $d = 0$, то R - свободный модуль ранга 1, а если он не равен нулю, то это есть *модуль кручения* $\forall x \in M \ dx = 0$.

Теорема 1. *Конечнопорождённый модуль над областью главных идеалов - конечная прямая сумма циклических модулей.*

Была доказана в прошлом семестре (не у нас). Однаком мы можем сформулировать следствие:

Следствие 1. Конечнопорождённая абелева группа - конечная прямая сумма циклических групп.

Пусть R - область, M - R-модуль, тогда подмодуль кручения -

$$\operatorname{Tors}(M) = \{m \in M | \exists r \neq 0, \ rm = 0\}$$

Утверждение 1. $\operatorname{Tors}(M)$ - модмодуль в M.

Нужно выполнить проверку этого утверждения, но для этого достаточно проверить, что всё хорошо с нулём (он там лежит и $1 \cdot 0 = 0$), а затем несколько свойств:

$$m_1, m_2 \in \operatorname{Tors}(M), \ r_1, r_2 \neq 0, \ r_1 m_1 = r_2 m_2 = 0,$$

тогда

$$r_1 r_2 (m_1 + m_2) = 0, \ r_1 r_2 \neq 0,$$

а также, если

$$m \in \text{Tors}(M),\ s \in R,\ rm = 0 \Rightarrow r(sm) = rsm = s(rm) = 0.$$

Пусть $r \in R$, $r \neq 0$, $M[r] := \{m \in M : rm = 0\} \leq M$ - подмодуль, p - пргстой элемент R. Рассмотрим $M[p] \leq M[p^2] \leq M[p^3] \leq \ldots$ - получили цепочку вложенных модулей.

$M_p := \bigcup_{i \geq 1} M[p^i]$ - подмодуль, p-кручение в M.

Сейчас начнётся пиздец. Наша цель: доказать, что $\text{Tors}(M) \cong \bigoplus_{p-\text{простое}} M_p$.

N_i - модули $i \in I$, $\bigoplus := \{(n_i)_{i \in I} | n_i \in N_i,$ почти все $n_i = 0\}$, операции покомпонентные. Это, получается, (бесконечная) прямая сумма модулей.

Теорема 2. *(О примарном разложении). Пусть R - область главных идеалов, M - R-модуль. Тогда $\bigoplus M_p \to \text{Tors}(M)$, дествующий по правилу $(m_p) \mapsto \sum m_p$ (конечная сумма) - изоморфизм модулей.*

Доказательство. Докажем всё по порядку:

- Докажем, что это гомоморфизм. $(m_p + n_p) \mapsto \sum m_p + n_p = \sum m_p + \sum n_p$, а также $(rm_p) \mapsto \sum rm_p = r(\sum m_p)$.
- Теперь нужно доказать сюръективность. $m \in \text{Tors}(m)$, $rm = 0$, $r = \Pi_{i=1}^n p_i^{\alpha_i}$, где p_i - простое. Рассмотрим линейное разложение НОД:

  $$r_1 p_2^{\alpha_2} \ldots p_n^{\alpha_n} + \ldots + r_n p_1^{\alpha_1} \ldots p_{n-1}^{\alpha_{n-1}} = 1.$$

  Тогда если мы домножим равенство на m, получим, что $r_i = \frac{rm}{p_i^{\alpha_i}} \in M_{p_i}$, тогда получили, что $(r_1 p_2^{\alpha_2} \ldots p_n^{\alpha_n} m, \ldots, r_n p_1^{\alpha_1} \ldots p_{n-1}^{\alpha_{n-1}} m) \mapsto m$.
- Осталась инъективность. Пусть $0 \neq (m_p) \mapsto 0$, возьмём наименьшее число индексов, что $\sum m_p = 0$. А теперь начнём его уменьшать. Пусть у нас есть $p_1, \ldots, p_n$, $p_i^{\alpha_i} m_{p_i} = 0$. Всё домножим на $p_n^{\alpha_n}$, получим $\sum p_n^{\alpha_n} m_p = 0$. Тогда раньше было $m_{p_n} \neq 0$, а теперь $p_n^{\alpha_n} m_{p_m} = 0$. Докажем, что ничего, кроме последнего не обнулилось. Предположим противное, $p_1^{\alpha_1} m_1 = 0$, $p_n^{\alpha_n} m_1 = 0$, но $p_1^{\alpha_1}$, $p_n^{\alpha_n}$ - взаимно просты, тогда есть линейное разложение $r_1 p_1^{\alpha_1} + r_n p_n^{\alpha_n} = 1$, домножим на m, получим $r_1 p_1^{\alpha_1} m_1 + r_n p_n^{\alpha_n} m_1 = m_1$, но оба они не могут быть равны нулю.

$\square$

Сейчас будем заниматься в основном кольцом многочленов. Пусть $R = F[t]$, F - поле, V - R-модуль. В частности, V - F-модуль, то векторное пространство $A : v \to tv$ - F-линейное отображение $V \to V$ *оператор.* Линейные операторы образуют кольцо (сумма - поточечно, умножение - композиция). $A(v)$ или Av.

$$(a_0 + a_1 t + \ldots + a_n t^n)V = a_0 v + a_1 Av + \ldots + a_n A^n v$$

V - векторное порстранство с оператором, значит, $F[t]$ - модуль.

Пусть a - матрица $n \times n$ $F^n \to F^n$, $F[t]$ - модуль на F^n. $F[t]$ - как модуль над собой векторное пространство со счётным базисом.

Утверждение 2. Пусть V возьмём конечнопорождённый модуль над $F[t]$, тогда V - конечномерное векторное пространство над F тогда и только тогда, когда $V = \text{Tors}(V)$ (как $F[t]$-модуль).

Доказательство. $F[t]^n \oplus F[t]/(f_i) \oplus \ldots \oplus F[t]/(f_k)$, где $f_i \neq 0$. Если $n \neq 0$, то в V есть бесконечномерное подпространство $F[t]$. Если $n = 0$, то $\dim_F F[t]/(f_i) = \deg f_i < \infty$. □

Теперь рассмотрим матрицы. Пусть $\dim V = n$, $A : V \to V$. Если зафиксировать базис в V, получается матрица a $n \times n$. Взали другой базис, получим матрицу перехода c. $V \to V$ посредством A, причём стороны соответственно изоморфны вот таким вещам (по центру, я не умею так круто чертить, загляните в лекцию) $F^n \xrightarrow{c^{-1}} F^n \xrightarrow{a} F^n \xrightarrow{c} F^n$. И, кстати, $a \sim c^{-1}ac$ (сопряжённая матрица).

Рассмотрим модуль $F[t]/(f)$, что также есть V, A. Поймём, что такое f. Он обладает таким свойством: $(f) = \mathrm{Ker}(F[t \to F[t/(f)]]) = \{g(t) |\, g(t) \cdot v = 0\, \forall v \in V\}$. Однако последнее равенство неочевидно. По определению там может быть написано $\{g(t) |\, g(t) \cdot [1] = 0\}$, но $[h(t)] = h(t) \cdot 1$, поэтому он обнуляется $g(t)$: $g(t) \cdot [h(t)] = h(t) \cdot g(t) \cdot [1] = 0$, откуда и получаем искомое.

Давайте теперь запишем это в терминах оператора. Если

$$g(t) = a_0 + a_1 t + \ldots + a_k t^k,$$

тогда

$$g(t) \cdot v = a_0 v + a_1 A v + \ldots + a_k A^k v.$$

Каждый раз писать такие длинные вещи неудобно, поэтому введём следующее обозначение:

$$g(A) := a_0 v + a_1 A + \ldots + a_k A^k.$$

В силу того, что A коммутирует с собой, то такая запись корректна. Тогда мы можем переписать:

$$\{g(t) |\, g(t) \cdot v = 0\, \forall v \in V\} = \{g(t) |\, g(A) v = 0\, \forall v \in V\},$$

но если последнее выполнено для любого $v \in V$, то получаем, что оператор - тождественный нуль, получаем $\{g(t) |\, g(A) = 0\}$.

Также можно пойти и в обратныую сторону, то есть, пусть мы знаем A, рассмотрим $\{g(t) |\, g(A) = 0\}$. Это - идеал в $F[t]$, скажем, что это $(f(t))$, тогда $f(t)$ мы будем называть *минимальным многочленом* оператора A. Можно заметить, что минимальный многочлен не равен нулю, если у нас имеется конечномерное пространство, не может быть такого, что никакой многочлен A не обнуляет. Покажем это.

Найдём некую линейную зависимость между степенями A. Рассмотрим $\mathrm{Id}, A, A^2, \ldots$ - элементы кольца операторов. Рассмотрим это кольцо как векторное пространство над F. Если $\dim V =$ т, то у полученного пространства размерность есть n^2, то есть, конечна. Потому бесконечной линейно независимой системы быть не может, тогда когда-то мы получим линейную зависимость:

$$a_0 + a_1 A + \ldots + a_k A^k = 0,$$

тогда отсюда мы и нашли требуемый многочлен.

2 Лекция 31.

Начинаем опять с оператора. Рассматриваем векторной пространство V над каким-то полем F и мы действуем на него оператором $A : V \to V$. Мы его также рассматривали как $F[t]$-модуль, $t \cdot v = Av$. Мы определили минимальный многочлен A такой, что $\{g(t) \in F[t] | g(a) = 0\} \triangleleft F[t]$, причём $F[t] = (f(t))$ - идеал унитарного (нуо) многочлена. Такой $f(t)$ и называется минимальным многочленом.

Теперь немного понятнее на языке модулей. Рассмотрим V - $F[t]$-модуль, а также $\mathrm{Ann}(V) := \{r \in V | rv = 0,\ \forall v \in V\}$. Это - идеал в R, причём даже двусторонний (можно будет потом записать проверку). Причём получаем, что $\mathrm{Ann}(V) = (f(t))$, легко заметить, что они совпадают.

$g(A)v = 0$, но тогда

$$g = a_0 + a_1 t + \ldots + a_k t^k$$

$$g = a_0 + a_1 Av + \ldots + a_k A^t v = 0,$$

что также и равно $g(t) \cdot v$. Тогда $f(A)v = g(t) \cdot v$ как оператор и из структуры модуля соответственно. Тогда $g(A) = 0 \Leftrightarrow g(A) \cdot v = 0$ для любого $v \in V \Leftrightarrow g(t) \cdot v = 0\ \forall v \in V \Leftrightarrow g(t) \in \mathrm{Ann}(v)$.

Мы уже начинали рассматривать такой модуль: $F[t]/(f(t))$ - $F[t]$-модуль, имеем также V, $Av = t \cdot v$. Мы хотим придумать базис V, в которм матрица A имеет простой вид. Возьмём такой базис: $[1], [t], \ldots, [t^{k-1}]$, тогда $[t^k] = -a_0[1] - \ldots - a_{k-1}[t^{k-1}]$. Как выглядит матрица A в этом базисе?

$$\begin{pmatrix} 0 & 0 & \ldots & 0 & -a_0 \\ 1 & 0 & \ldots & 0 & -a_1 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ \vdots & \vdots & \ldots & 0 & -a_{k-2} \\ 0 & 0 & \ldots & 1 & -a_{k-1} \end{pmatrix}$$

Такая матрица называется *фробениусовой клеткой.* А вообще, в итоге мы получили, что если V - циклический $F[t]$-модуль, то A в некотором базисе записывается фробениусовой клеткой, причём последним столбцом будут коэффициенты минимального многочлена, только со знаком "минус".

А если модуль не циклический (произвольный и с конечномерным V), то мы можем его разложить в прямую сумма циклических:

$$F[t]/(f_1(t)) \oplus F[t]/(f_2(t)) \oplus \ldots \oplus F[t]/(f_m(t)),$$

причём мы можем даже потребовать, чтобы $f_1 | f_2 | \ldots | f_n$.

Умножение на t будет действовать поккординатно.

Для каждого слагаемого мы умеем выписывать матрицу оператора A в подходящем базисе. Матрица A тогда выглядит на всём пространстве как цепочка фробениусовых клеток, расставленных по порядку по диагонали.

Зададимся теперь вопросом: чему же в таком случае равен минимальный многочлен? Ответ таков:

$$A = f_m(t),$$

причём принципиально условие цепочки делений.

Как считать инвариантные факторы (то есть, $f_1(t), \ldots, f_n(t)$)? Рассмотрим V и $F[t]$. $e_1, \ldots, e_n$ - базис V как векторное пространство над F, а тем более, это система образующих V как $F[t]$-модуля. Какими соотношениями обладает этот набор? $t \cdot e_i = Ae_i$ - линейная комбинация $e_1, \ldots, e_n$. Это соотношение между e_i с коэффициентами из $f(t)$, получаем $(t \cdot I - A)e_i = 0$.

Мы имеем n образующих и n таких последних соотношений. Рассмотрим матрицу $(t \cdot I - A)$, она имеет размер $n \times n$ над $F[t]$ и выглядит так:

$$\begin{pmatrix} t - a_{11} & -a_{12} & \ldots & -a_{1n} \\ -a_{21} & t - a_{22} & \ldots & -a_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ -a_{n1} & -a_{n2} & \ldots & -a_{nn} \end{pmatrix}$$

Домножим её слева и справа на обратимые над $F[t]$ матрица и приведём её к диагональному виду, а на диагонали будут расставлены $f_1, \ldots, f_m$ (перед которыми $n - m$ единиц). Последний многочлен будет минимальным многочленом A.

Сравним определители этих матриц. Определитель обратимой матрицы лежит в $F[t]^* = F^*$. Идеал, порождённый в $F[t]$ определителем, не поменяется, тогда

$$(\det(t \cdot I - A)) = (f_1(t) \ldots f_n(t)),$$

тогда $\det(t \cdot I - A)) \in F[t]$ мы будем называть *характеристическим многочленом* матрицы A (обозначаем $\chi_A(t)$). Имеет он степень n, причём он ещё и унитарный в силу того, что максимальная степень будет содержаться в $(t - a_{11})(t - a_{22}) \ldots (t - a_{nn})$.

Причём тогда мы можем получить такое равенство из того, что и характеристический многочлен, и призведение f_i унитарно:

$$\chi_a(t) = f_1(t) \cdot \ldots \cdot f_n(t),$$

откуда минимальный многочлен делит характеристический многочлен, а характеристический делит минимальный в степени n.

Наборы неприводимых делителей у минимаьлного и характеристического многочленов совпадают. В частности, наборы корней без учёта кратности совпадают.

Теорема 3. *(Теорема Гамильтона-Кэли). Минимальный многочлен делит характеристичесий, имеет такие же корни [и у них совпадают неприводимые делители].*

Приступим теперь к рассмотрению *нильпотентным* операторам.

Определение 2. $A : V \to V$ - *нильпотентный*, если $A^k = 0$ для некоторого k.

Нужно теперь научиться понимать, когда это выполнено. Берём $k : A^k = 0, A^{k-1} \neq 0$ (наименьшее возможное?). Минимальный многочлен у A - t^k, потому что он подходит, и никакой его делитель не подходит. Какой же характеристический многочлен у A? Это есть t^n, где $n = \dim V$ из теоремы Гамильтона-Кэли.

Пусть $A^k = 0$ - минимальная такая степень. Рассмотрим V как $F[t]$-модуль.

$$F[t]/(t^{k_1}) \oplus F[t]/(t^{k_2}) \oplus \ldots \oplus F[t]/(t^{k_m}),\ k_1 \le k_2 \le \ldots \le k_m = k,$$

а само k мы называем *степенью нильпотентности.* Кстати, фробениусова клетка нильпотентного оператора теперь выглядит ещё лучше, весь правый столбец теперь состоит из нулей (в подходящем базисе). В общем случае, она составлена из квадратиков такого вида. Получили мы матрицу строгонижнетреугольного вида.

Определение 3. *Нижнетреугольная матрица* - всё, выше главной диагонали - нули. *Строгонижнетреугольная матрица* - ещё и диагональ - нули.

Как найти такой базис (без формы Смита)? Запишем по индукции:

$$\begin{aligned}
V[t] &= \{v \in V | tv = 0\} = \operatorname{Ker}(A),\\
V[t^2] &= \{v \in V | t^2 v = 0\} = \operatorname{Ker}(A^2),\\
&\dots\\
V[t^{k-1}] &= \operatorname{Ker}(A^{k-1}),\\
V[t^k] &= \operatorname{Ker}(A^k) = V.
\end{aligned}$$

Рассмотрим цепочку вложенных пространств:

$$0 < \operatorname{Ker}(A) \leq \operatorname{Ker}(A^2) \leq \ldots \leq \operatorname{Ker}(A^{k-1}) < V.$$

Посмотрим на образ A (то есть, $\operatorname{Im} A$), он попадёт в $\operatorname{Ker}(A^{k-1})$, а вот $A(\operatorname{Ker}(A^{k-2})) \leq \operatorname{Ker}(A^{k-2})$.

Осталось найти тот самый базис, в котором матрица A имеет нужный вид. Рассмотрим фактор-пространство $V/\operatorname{Ker}(A^{k-1})$, и выберем в нём базис. Это даёт нам относительный базис V относительно $\operatorname{Ker}(A^{k-1})$ (скажем, это $e_1, \ldots, e_s$). Тогда что с ними происходит: $e_1.Ae_1, \ldots, A^{k-1}e_1$, причём получается, что все они не равны нулю, так как они не лежат в классе нуля.

Рассмотрим $\langle e_1.Ae_1, \ldots, A^{k-1}e_1\rangle$ - A переводит его в себя. Рассмотрим матрицу A в данном базисе, это как раз будет фробениусова клетка размера k. Так проделаем для каждого элемента базиса и получим s фробениусовых клеток размера k, где s также было размерностью отфакторизованного пространства, тогда $s = \dim V - \dim \operatorname{Ker}(A^{k-1})$.

Теперь рассмотрим $\operatorname{Ker}(A^{k-1})/(\operatorname{Ker} A^{k-2} + \operatorname{Im} A)$ - подпространство, порождённое $\operatorname{Ker} A^{k-2}$ и $\operatorname{Im} A$. Возьмём относительный базис $e_{1,1}, \ldots, e_{s_1,1}$, опять перейдём к $\langle e_{1,1}.Ae_{1,1}, \ldots, A^{k-1}e_{1,1}\rangle$ - тут A имеет матрицу в виде фробениусовой клетки размера $k-1$ (если фробениусовых клеток такого размера нет, это пространство равно нулю). s_1 - количество таких клеток.

И, наконец, клетки размера $k-i$: $\operatorname{Ker}(A^{k-i})/(\operatorname{Ker}(A^{k-i-1}) + \operatorname{Im} A^i)$, рассмотрим тут базис и проделаем аналогичные операции.

3 Лекция 32.

Примечание 1. В предыдущей лекции была допущены небольшая ошибка, в месте, где записано $\operatorname{Ker} A^i/(\operatorname{Ker} A^{i-1} + \operatorname{Im} A^{n-i})$, нужно записать $\operatorname{Ker} A^i/(\operatorname{Ker} A^{i-1} + (\operatorname{Im} A \cap \operatorname{Ker} A^i))$.

Допустим, у нас есть два разных поля: пусть раньше мы рассуждали над полем K, а сейчас есть ещё $L \geq K$. Над K было векторное пространство V с базисом $e_1, \ldots, e_n$. Мы можем рассмотреть такое же пространство над L, размерности тоже n. Рассмотрим V_L - пространство, натянутое на $e_1, \ldots, e_n$ над L, то есть, все линейные комбинации вида $\{\alpha_1 e_1 + \ldots + \alpha_n e_n\}$. То есть, $\dim V = \dim V_L = n$. Тогда понятно, если у нас есть оператор $A : V \to V$, то мы можем его продолжить до оператора $A_L : V_L \to V_L$.

Представить себе это можно по-разному. Представим себе матрицу изначального оператора в этом базисе, это какая-то матрица $M_n(K) \subseteq M_n(L)$ - можем "расширить", и получим, что первое - подкольцо второго. И тогда можно написать оператор с точно такой же матрицей на L. Можно также сказать, что мы рассматриваем $A(\alpha_1 e_1 + \ldots + \alpha_n e_n)$, тогда раскроем по линейности $\alpha_1 A(e_1) + \ldots + \alpha_n A(e_n)$, и посчитаем необходимые элементы внутри первого кольца.

Что же меняется при переходе от ожного поля к другому? У нас есть инвариантные факторы, например, если у нас есть оператор A, то для него есть многочлены $f_1, \ldots, f_m \in K[t]$ (последний - минимальный). Тогда для A_L они также инвариантны, причём даже минимальный многочлен такой же. Давайте вспомним, как они строятся в терминах оператора A.

Пусть у нас имеется матрица a (перехода A), рассмотрим матрицу $a - t \cdot I$, тогда инвариантные факторы - $\frac{\text{НОД(все миноры порядка } i-1)}{\text{НОД(все миноры порядка } i)}$. А наибольший общий нелитель не зависит от того, в каком поле ме его рассматривали. Значит, инвариантные факторы не изменятся.

Мы знаем, что в каком-то базисе матрицу A можно привести к фробениусовой форме (на диагонали - квадратики, последняя клетка - соответствующая f_m).

Определение 4. $\mathrm{End}(V) = \{A : V \to V\}$ - множество всех линейных операторов (эндоморфизмы V). Кстати, это кольцо (поточечное сложение и композиция), которое изоморфно $M_n(K)$, посредством выбора базиса.

Пусть c - матрица перехода при изменении базиса и A - операотр с матрицей a, тогда в новом базисе у него будет матрица $c^{-1}ac$ - *сопряжённая* к a матрица.

Определение 5. A, B - *сопряжённые*, если существует C - обратимый $B = C^{-1}AC$.

Сформулируем такую теорему, которую мы уже по сути доказали:

Теорема 4. *A, B сопряжены тогда и только тогда, когда у них одинаковые инвариантные факторы.*

Доказательство. Найдём базис, в котором матрица A записывается в фробениусовой нормальной форме. Существует какой-то другой базис, в котором матрица B записывается точно также. Тогда нужно взять просто матрицу, которая переведёт один базис в другой. В обратную сторону - если A известно в какой фробениусовой форме, то легко определить, что f_j - инвариантные факторы. □

Следствие 2. A, B сопряжены тогда и только тогда, когда A_L, B_L сопряжены. Анаолгично можно записать и для матриц из изоморфности колец.

Приведём другое доказательство второго пункта в случае бесконечного K. Мы хотим найти такую обратимую матрицу, что $ac = cb$. Пусть c - матрица с неизвестными коэффициентами. Тогда у нас имеется система однородных линейных уравнений на $x_{i,j}$, где $c = (x_{i,j})$. Она имеет нетривиальное решение над L, причём набор решений образует подпространство L^{n^2} размерности K. Тогда над базовым полем K размерность подпространства будет точно такая же, поскольку метод Гаусса не зависит от поля, над которым мы работаем, поэтому он выдаст одинаковые ответы для K и для L.

Возьмём базис в этом подпространстве: $c_1, \ldots, c_k$. Рассмотрим всевозможные комбинации $\{\lambda_1 c_1 + \ldots + \lambda_k c_k\}$, и будме искать такую линейную комбинацию, определитель которой не равен нулю. Мы знаем, что над L такие существуют, потому что над L у нас есть решение. Но определитель - суть многочлен от λ_i, причём ненулевой, поскольку над L можно найти такие λ_i, значение при которые не нуль. А поскольку поле K бесконечное, то можно такие коэффициенты найти и над K (индукция по k). Доказательство завершили.

Рассмотрим теперь за место L алгебраическое замыкание K, $K \leq \overline{K}$. Мы уже знаем, что есть фробениусова нормальная форма, но она не очень удобна. Рассмотрим оператор

$A_{\overline{K}}$. Применим для кольца $\overline{K}[t]$ теорему о строении модулей над кольцами главных идеалов, но сначала применим примарное разложение. То есть, возьмём какой-то неприводимый многочлен над алгебраически замкнутым полем, он линейный $(t-\lambda)$. И начинаем теперь образовывать блоки. У нас есть $V_{\overline{K}}[t-\lambda] = \{v : (t-\lambda)v = 0\} = \{v : Av = \lambda V\}$ - собственное подпространство, соответствующее собственному числу λ. $v \neq 0$ из этого множества - собственные векторы, соответствующие собственному числу λ.

Нас интересуют в качестве λ - корни минимального многослена (корни характеристического) (чтобы мы получали ненулевые множества), но можно и проще, преобразуем к $(A - \lambda I)v = 0$, но это раносильно тому, что $\det(A - \lambda I) = 0$, что и равносильно первому. Далее мы смотрим на степени $V_{\overline{K}}[(t-\lambda)^2] = \{v : (t-\lambda)^2 v = 0\}$, и так далее, а затем берём объединенение $V_\lambda = \bigcup_{i \geq 1} V_{\overline{K}}[(t-\lambda)^i]$, это - корневое подпространство, отвечающее собственному числу λ. Не стоит путать это с собственным подпространством (по сути, первый и последний член цепи).

Из общей теории мы теперь знаем, что $V_{\overline{K}} = \oplus V_\lambda$, где суммируем по λ - собственным числам. Мы получили корневре разложение. Посмотрим теперь, что происходит на каком-то корневом подпространстве. Ограничим $A|_{V_\lambda}$, тогда минимальный многочлен этого ограничения - $(t-\lambda)^k$. А если рассмотреть оператор $A - \lambda I$, то его минимальный многочлен будет t^k, то есть, ограничение такой вещи нильпотентное, то есть, матрица будет состоять из квадратиков по диагонали, на диагонали которых нули, а под ними - диагональ из единиц. А вот если мы вернёмся к изначальному сужению, то мы получим матрицу, состоящую из *жордановых блоков*, это то же самое, что и предыдущая матрица, только на главной диагонали везде λ.

Сама матрица A тогда будет состоять из кучи таких блоков для всех λ по диагонали, и целиком такое представление A будет называться *жордановой нормальной формой*. Таким образом, для любого ооператора существует базис, в котором матрица выглядит в такой форме.

Рассмотрим такой важный частный случай. Пусть имеется характеристический многочлен $\chi_A(t)$ (по сути, $\det(\lambda I - A)$), и степень его тогда есть размерность пространства (n). Предположим, что он раскладывается в произведение линейных $(t-\lambda_1)\dots(t-\lambda_n)$ (это какое-то условие на характеристический многочлен (НОД$(\chi_A(t), \chi'_A(t)) = 1$)). Но всё же, если они все различны, то жорданова форма просто диагональная, так как на диагонали под ними просто ничего не поместится, квадратики единичные. В каком же базисе матрица имеет такой вид? Для того, чтобы это понять, достаточно решить $Av_i = \lambda_i v_i$, $v_i =\neq 0$. Такой базис, который мы найдём, *диагонализирует* матрицу. Пока что всё это происходило над алгебраическим замыканием.

Перейдём к случаю $K = \mathbb{R}$, $\overline{K} = \mathbb{C}$ и придумаем вещественную жорданову форму (именно её, а не фробениусову, потому что она удобнее). Для этого, нам нужно разобрать немного подробнее процедуру переходу из поля в замыкание с одним и тем же базисом $(V \to V_\mathbb{C})$. Как нам тогда восстановить $V_\mathbb{C}$? Вообще, никак, но если ввести некую дополнительную структуру это можно сделать. Хочется ввести на $V_\mathbb{C}$ какую-то инволюцию - аналог комплексного сопряжения. Если у нас уже есть базис, то пусть $\overline{z_1 e_1 + \ldots + z_n e_n} = \overline{z_1} e_1 + \ldots + \overline{z_n} e_n$, это операция из $V_\mathbb{C}$ в $V_\mathbb{C}$, которая не будет линейной, а будет *полулинейной*, то есть, выполнено $\overline{zv} = \bar{z}\bar{v}$, а не $\overline{zv} = z\bar{v}$. С суммой же всё нормально. Получили мы *полулинейный оператор*, который является инволюцией.

А само V тогда восстанавливается: $V = \{v \in V_\mathbb{C} : \bar{v} = v\}$. Это уже пространство над $\mathbb{R}$ такой же размерности.

Итого, вещественные векторные пространства по сути есть комплексные векторные пространства такой же размерности с полулинейной инволюцией. Придумаем теперь вещественный аналог жордановой формы. Пусть есть V, $A : V \to V$, тогда $V_\mathbb{C}$ назовём *комплек-*

сификацией V, а наоборот - *овеществлением.* Также мы можем рассмотреть и комплексификацию $A_{\mathbb{C}} : V_{\mathbb{C}} \to V_{\mathbb{C}}$. Есть базис, в котором он представляется жордановой начальной формой. У A есть характеристический многочлен $f(t) \in \mathbb{R}[t]$, у которого есть вещественные корни α_i и мнимые λ_j вместе со своими сопряжёнными парами. Пусть λ - комплексный корень этого многочлена, тогда у нас сеть корневые пространства V_λ и $V_{\bar{\lambda}}$, тогда их сумма устойчива относительно нашей полулинейной инволюции. Потому что, допустим, $Av = \lambda v$, тогда $\overline{AV} = \bar{\lambda}\bar{v}$, но про A мы знаем, что у его матрицы коэффициенты вещественные, поэтому $\overline{Av} = A\bar{v}$ (можно расписать умножение матрицы на столбец для наглядности).

Таким образом, если v - собственный вектор, отвечающий λ, то $\bar{v}$ - собственный вектор, отвечающий $\bar{\lambda}$, и со степенью, конечно, то же самое: $(A - \lambda I)^i v = 0$, тогда $\overline{(A - \lambda I)^i}\bar{v} = 0 = (A - \bar{\lambda} I)^i v$. То есть, вся эта прямая сумма относительно λ и его сопряжённого, будет устойчивой относительно нашей полуинволюции. Мы знаем, что вещественное векторное пространство это то же самое, что и комплексное с полуинволюцией, тогда все пары λ_i и их сопряжённый будут объединяться в пары и давать вещественные подпространства.

4 Лекция 33.

В прошлый раз мы рассматривали V - векторное пространство над полем вещественных чисел и какой-то оператор $A : V \to V$, а также его комплексификацию $V_{\mathbb{C}}$ и переход от одного к другому брагодаря полулинейному отображению.

V над вещественными разбивается в сумму пространств, часть из них соответствует вещественным корням, а часть - мнимым.

$$V = \oplus_{\lambda=\bar{\lambda}} V_{\lambda}^{\mathbb{R}} \oplus_{\lambda \neq \bar{\lambda}} V_{\lambda,\bar{\lambda}}^{\mathbb{R}}.$$

Как выглядит ограничение оператора A на эти подпространства? Давайте начнём с какого-то жорданового блока (для начала, случай $\lambda \neq \bar{\lambda}$). Обозначим базис данной жордановой формы $v_1, \dots, v_k$, тогда

$$\begin{aligned} A_{\mathbb{C}} v_1 &= \lambda v_1 + v_2, \\ A_{\mathbb{C}} v_2 &= \lambda v_2 + v_3, \\ &\vdots \\ A_{\mathbb{C}} v_{k-1} &= \lambda v_{k-1} + v_k, \\ A_{\mathbb{C}} v_k &= \lambda v_k. \end{aligned}$$

Что плохо в эитх векторах, почему их нельзя спустить до нашего пространства над вещественными? Они могут быть не инвариантны относительно инволюции. Применим ко всему, кроме $A_{\mathbb{C}}$ черту. Это означает, что в пару к данному жордановому блоку идёт другой жорданов блок, базис которого соответственно сопряжён изначальному, а на диагонали стоят $\bar{\lambda}$. Пусть теперь у нас есть v_1 и $\overline{v_1}$. Чтобы получить вектор, инвариантный относительно инволюции, надо их сложить. Также можно вычесть и умножить на i, нетрудно проверить, что эта вещь также будет инвариантна относительно инволюции.

И теперь возьмём прямую сумму тех самых парных пространств, но сделаем замену базиса на $v_j + \bar{v}_j, i(v_j - \bar{v}_j)$ по всем j. Несложно просерить, что это также базис, однако теперь все его элементы инвариантны относительно инволюции, а значит, просто "живут" в самом V. Осталось переписать матрицу A в новом базисе. Тут какая-то муть с вычислениями, в итоге получается

$$\begin{pmatrix} \operatorname{Re}(\lambda) & -\operatorname{Im}(\lambda) \\ \operatorname{Im}(\lambda) & \operatorname{Re}\lambda \end{pmatrix}$$

- расставлены по диагонали квадратиками 2×2, а под каждым из них - единичные матрички 2×2.

Кстати, $\mathbb{C} \leq M_2(\mathbb{R})$ посредством перехода λ в такие матрицы. Теперь пора перейти к случаю вещественного λ.

Возможны два варианта: v_1 и $\bar{v_1}$ могут быть либо линейно зависимы, либо линейно независимы (раньше-то они лежали в разных пространствах, а сейчас такое утверждать нельзя). В первом случае скажем, что $\bar{v_1} = \alpha v_1$. Тогда α может равняться чему-то на единичной окружности, так как из инволюции $\alpha\bar{\alpha} = 1$.

Лемма 1. *(Простейший случай теоремы Гильберта 90). Если $\alpha\bar{\alpha} = 1$, то существует β такой, что $\alpha = \frac{\beta}{\bar{\beta}}$ (всё в $\mathbb{C}$).*

Эта лемма была к рассуждению о том, что если $v_1 \to \beta v_1$, то $\overline{\beta v_1} = \bar{\beta}\alpha v_1 = \bar{\beta}\frac{\alpha}{\beta}(\beta v_1)$, тогда мы и выбираем $\frac{\beta}{\bar{\beta}} = \alpha$. То есть, можем считать, что $v_1 = \bar{v_1}$.

Но тогда v_1 лежит в нашем вещественном пространстве, и то, что им порождено, также лежит в этом пространстве ($v_1 \in V$, $v_2 = Av_1 - \lambda v_1 \in V$, и так далее). То есть, в этом случае, жорданов блок так и остаётся жордановым блоком в том же самом базисе.

Ну и, наконец, если $\langle v_1 \rangle \neq \langle \bar{v_1} \rangle$ - сделаем то же, что и раньше, от того, комплексное λ или вещественное, зависело только то, будет ли система базисом или нет. То есть, матрица состоит из блоков 2×2 с λ по диагонали, под которыми, опять-таки, единичные 2×2. А если перенумеровать базис (сначала идут нечётные, а потом чётные), то просто получатся два жордановых блока одинакового размера. Окончательно, теорема такая:

Теорема 5. *Есть V, A, $\chi_A(t)$, корни которого есть λ_i - мнимые и α_j - вещественные (причём, суммарно количество корней - размерность пространства, конечно же). Тогда в некотором базисе A имеет вид блочный, состоящий из жордановых блоков, каждый из соответствующих комплексным $\lambda_i, \bar{\lambda_i}$ выглядит как квадратик 2×2, вид которого был показан выше, под каждым из которых единичная матричка 2×2, а что касается вещественных, они просто выглядят без изменений, обычная жорданова форма.*

Вернёмся опять к ситуации алгебраически замкнутого поля. Мы говорили, что если $\chi_A(t)$ имеет различные корни λ_i, то A диагонализируема и принимает вид - n её корней по диагонали по порядку. Давайте поймём, когда все корни $f(t) \in K[t]$ в $\overline{K}$ различны. Мы уже знаем, что можно сказать, что требуемо соотношение НОД$(f(t), f'(t)) = 1$, но мы хотим переписать это в каком-то более явном виде многочлена от коэффициентов. Пусть у нас есть $f(t)$ и $g(t)$, $\deg(t) = n$, $\deg(g) = m$. Как узнать по коэффициентам f и g, когда их НОД есть единица. Так мы перешли к теме *результанты*.

Для начала, немного в общих чертах. Если НОД $= 1$, то существуют p, q: $pf + qg = 1$. Давайте расссмотрим гомоморфизм $F[t] \times F[t] \to F[t]$, действующий по правилу $(p, q) \to pf + qg$. Это F-линейное отображение (не гомоморфизм колец), причём единица представляется тогда и только тогда, когда оно сюръективно. Критерий хороший, плохо только то, что трудно проверить сюръективность.

Рассмотрим $F[t]/(g) \oplus F[t]/(f) \to F[t]/(fg)$ по формуле $([p], [q]) \mapsto ([pf + qg])$. Необходимо, конечно, проверить корректность этого отображения (но это - в запись, если интересно). Размерность пространств из отобажения - $m+n$ у обоих. Тогда матрица отображения квадратная, и сюръективность отображения контроллируется определителем. Осталось выписать матрицу отображения в каком-то базисе. Пусть $f = a_n t^n + \ldots + a_0$, $g = b_m t^m + \ldots + b_0$. Тогда в базисах - степенях t от нулевой до n-ой, m-ой и $n+m$-ой соответственно, матрица так и выглядит:

$$\begin{pmatrix} a_0 & 0 & 0 & \ldots & 0 & b_0 & 0 & \ldots & 0 \\ a_1 & a_0 & 0 & \ldots & 0 & b_1 & b_0 & \ldots & 0 \\ a_2 & a_1 & a_0 & \ldots & 0 & b_2 & b_1 & \ldots & 0 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ a_n & a_{n-1} & a_{n-2} & \ldots & a_i & \vdots & \vdots & \ddots & \vdots \\ 0 & a_n & a_{n-1} & \ldots & a_{i+1} & b_m & b_{m-1} & \ldots & b_j \\ 0 & 0 & a_n & \ldots & a_{i+2} & 0 & b_m & \ldots & b_{j+1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & 0 & \ldots & a_n & 0 & 0 & \ldots & b_m \end{pmatrix}$$

И чуть менее легко, чем её написание, мы можем найти её определитель, который и называется *результантом* f и g (как многочлен). Таким образом, сформулируем теорему:

Теорема 6. $\text{НОД}(f, g) = 1 \Leftrightarrow \text{Res}(f, g) \neq 0$

Следствие 3. f не имеет кратных корней в $\bar{F}$ тогда и только тогда, когда $\text{Res}(f, f') \neq 0$. И, кстати, если определить *дискриминант* в общем случае: $\text{disc}(f) = \frac{\text{Res}(f,f')}{a_n}$, то можно говорить, что дискриминант не равен нулю.

Таким образом, мы узнали, что кратность еорней контроллируется каким-то многочленом, которых зависит от коэффициентов изначальных многочленов. Благодаря принципу продолжения алгебраических тождеств можно перейти к *плотности диагонализируемых матриц*. Каков принцип? Пусть, имеются матрицы $n \times n$, хотим проверить, что какой-то многочлен от коэффициентов равен нулю $P(a_{ij}) = 0$ - хотим проверить (например, мы хотим доказать теорему Гамильтона-Кэли: $\chi_A(A) = 0$). Мы хотим, чтобы многочлен принимал значение нуль также и при коэффициентах сопряжённой матрицы. Тогда достаточно это проверять только для диагональных матриц - если это выполнено для диагональных, то выполнено и для всех.

(сюда можно пару чертежей пояснения перенести)

Почему этот принцип верен? Перейдём сначала к $\bar{K}$, затем рассмотрим $\text{disc}(\chi_A(t))$. Тогда если дискриминант не равен нулю, то матрица диагонализуема, то есть, сопряжена с диагональной, а тогда многочлен P на ней обнуляется. То есть, если дискриминант не равен нулю, то $P = 0$, применяем принцип продолжения и получим, что P тождественно равен нулю. Сам принцип - по сути тавтология, просто надо умножить P на дискриминант, это всегда нуль, тогда и получаем, что требовалось.