НМУ Алгебра I, Константин Логинов

Глава 1

Векторные пространства

1.1 Жорданова нормальная форма

Матрица называется жордановым блоком, если она имеет вид

$$J_k(\lambda) = \begin{pmatrix} \lambda & 1 & 0 & \cdots & 0 \\ 0 & \lambda & 1 & \ddots & \vdots \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda & 1 \\ 0 & \cdots & \cdots & 0 & \lambda \end{pmatrix}$$

Болок размера $k \times k$ с λ на диагонали и с 1 над диагональю. В прошлый раз мы доказали, что для любого линейного эндоморфизма векторных конечномерных пространств над алгебраически замкнутым полем есть базис, в котором матрица имеет болочно диагональный вид, с жордановыми блоками.

Поле называется алгебраически замкнутым, если каждый многочлен над этим полем положительной степени имеет корень.

$$\begin{pmatrix} J_{k_1}(\lambda_1) & & & 0 \\ & J_{k_2}(\lambda_2) & & \\ & & \ddots & \\ 0 & & & J_{k_n}(\lambda_n) \end{pmatrix}$$

Стоит отметить, что λ_i и k_i

Пример: Пусть полем будет $\Bbbk = \mathbb{R}$, а пространством $V = \mathbb{R}^2$. Зметим, что $x^2 + 1$ неприводим в этом поле. Тогда возьмём оператор поворота на 90 градусов.

$$A = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

Для неё нет жордановой нормальной формы над $\mathbb{R}$, так как у неё нет собственных значений. Если бы они были, то были бы корнем характеристического многочлена $\chi_A(t) = t^2 + 1$, а у него корней нет. Над $\mathbb{C}$, наш оператор приводим, так как $\pm\sqrt{-1}$ его собственные значения, а тогда

$$A = \begin{pmatrix} \sqrt{-1} & 0 \\ 0 & -\sqrt{-1} \end{pmatrix}$$

Заметим, что по жордановой нормальной форме легко вычислять инварианты, так как след – сумма диагональных элементов, $\operatorname{tr}(A) = \sum k_i \lambda_i$.

Замечание: базис, в котором оператор имеет жорданову нормальную форму, вообще говоря не единственен, например тривиальный оператор I.

Тем не менее кое-что определено канонически. Давайте бозначим за $n_{\lambda,k}$ – количество клеток вида $J_k(\lambda)$ в нашей матрице.

Утверждение:

$$\sum_{p=1}^{k} pn_{\lambda,p} + \sum_{p=k+1}^{\inf} kn_{\lambda,p} = \operatorname{dimKer}(A - \lambda \operatorname{Id})^k, \ \forall \lambda, k$$

Следовательно, $n_{\lambda,k}$ – инвариаенты A.

Для доказательства, давайте запишем матрицу в жордановой нормальной форме и посчитаем ядро $\operatorname{dimKer}(A - \operatorname{Id})^{\lambda}$. В таком виде нас будут интересовать только клетки, в которых стоит λ. Тогда можно предполагать, что оператор состоит только из клеток с λ. Если посмотреть на то, что происходит с клетками, то мы увидем

$$J_k(\lambda) - \lambda \operatorname{Id} = \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

И если мы возведем в степень такие клетки, то равенство станет очевидным.

Замечание: Пусть $A \in \operatorname{End}(V)$. Заметим, что задать оператор A, равносильно заданию на V структуры $\Bbbk[t]$-модуля. Структура $\Bbbk[t]$-модуля это в точности $\Bbbk$-модуль с действием t. Зададим это действие следующим образом $t^l \cdot v = A^l(v)$, $v \in V$ и продолжим его по линейности. В обратную сторону, мы зададим оператор через действие t, то есть $A(v) = t \cdot v$. И это также эквивалентно заданию гомоморфизма (колец?) $\phi : \Bbbk[t] \to \operatorname{End}(V)$, где образ t будет оператором A. (Скорее всего это работает только в коммутативном случае, когда на $\operatorname{End}(V)$ Есть структура модуля и я бы брал гомоморфизмы модулей!).

Например если $A = J_k(\lambda)$, то $V \cong \Bbbk[t]/(t-\lambda)^k$. Давайте поймём почему этот изоморфизм имеет место. Нам нужно вопервых убедится, что они изоморфны как $\Bbbk$-векторные пространства, а во вторых, что A действует в V также как t умножением в $\Bbbk[t]/(t-\lambda)^k$. Первое верно из наблюдения размерности, в обоих случаях она k. Для второго, нужно понять как $A - \lambda\mathrm{Id}$ дей ствует на базисные вектора, а именно $e_1 \mapsto 0$ и $e_{i+1} \mapsto e_i$ для $1 \leq i \leq k$. Заметим, что $\{(t-\lambda)^i\}_{0\leq i\leq k}$ $\Bbbk$-базис фактор кольца, и в нём $t-\lambda$ умножением действует точно также на элементы кольца, а значит у нас есть изоморфизм $\Bbbk[t]$-модулей.

Следситвие (из теоремы о существовании ЖНФ) Для $A \in \mathrm{End}(V)$, V – $\Bbbk[t]$-модуль. То $V \cong_{\Bbbk[t]} \bigoplus_{i=1}^N \Bbbk[t]/(t-\lambda_i)^{k_i}$, где действие A соответствует действию t, а сумма идёт по жордановым блокам. Это верно, так как матрица оператора блочно диагональная, а значит пространство раскладывается в прямую сумму подпространств, так, что на каждом подпространстве наш оператор деуствует как жорданов блок, а тогда применив предыдущий результат, мы получаем искомое. Такая формулировка теоремы о жордановой нормальной форме более правильная, так как она имеет обобщения, то есть на классификацию конечно порожденных модулей. В частности классификация конечных и конечно порожденных абелевых групп.

Определение: $A \in \mathrm{End}(V)$ называется полупростым, если существует базис, в котором матрица A диагональна. A называется нильпотентом, если $A^m = 0$ для $m > 1$.

Следствие (из ЖНФ): $A \in \mathrm{End}(V)$, то $A = A_{ss} + A_n$, где A_{ss} – полупрост, а A_n – нильпотент. И эти два оператора коммутируют.

$$J_k(\lambda) = \lambda\mathrm{Id} + \begin{pmatrix} 0 & 1 & & 0 \\ & \ddots & \ddots & \\ & & \ddots & 1 \\ 0 & & & 0 \end{pmatrix}$$

Теорема (Гамильтона-Кэли): $A \in \mathrm{End}(V) \Rightarrow \chi_A(A) = 0$. Поле не обязательно алгебраически замкнуто. $\chi_{J_k(\lambda)}(t)|_{t=a} = (t-\lambda)^k|_{t=A} = (A-\lambda)^k = 0$. А значит в каждом блоке будет 0, теорему доказали, но жульничество в том, что нам необходима алгебраическая замкнутость поля, но жульничество можно обойти, показав, что каждое поле вложено в алгебраически замкнутое.

Доказательство:
$(tE-A)(\widehat{tE-A}) = (\widehat{tE-A})(tE-A) = \chi_A(t)\mathrm{Id}$ в кольце $\mathcal{M}at_{n\times n}(\Bbbk[t]) = (\mathcal{M}at_{n\times n}(\Bbbk))[t]$. Определим отображение

$$\phi : R \to \mathcal{M}at_{n\times n}(\Bbbk),$$

где $R = Z_A(\mathcal{Mat}_{n\times n}(K)[t])$, а устроено оно вычислением в A, то есть $\phi(\sum B_i t^i) = \sum B_i A^i$, где $B_i \in \mathcal{Mat}_{n\times n}(\Bbbk)$. Заметим, что ϕ является гомоморфизмом.

$\chi_A(A) = \phi(\chi_A(t)E) = \phi((t\widehat{E - A})(tE - A)) = \phi(t\widehat{E - A}\phi(tE - A) = \phi(t\widehat{E - A})(A - A) = 0$.

Замечание: $A \in \mathrm{End}(V)$ задание эндоморфизма эквивалентно заданию гомоморфизма $\phi : \Bbbk[t] \to \mathrm{End}(V)$. По теореме Гамильтона-Кэли мы знаем, что $\chi_A(t) \in \mathrm{Ker}(\phi)$. С другой стороны $\mathrm{Ker}(\phi) = (m_A(t))$, тогда можно определить m_A минимальный многочлен оператора A, минимальный многочлен оператора A, он определен однозначно, если страший коэффициент брать за 1. Заметим, что минимальны многочлен делит характеристичесий.

Упражнение: Существует N, что $\chi_a(t) \mid m_a(t)^N$.

Пример:

- $m_A(t) = t - \lambda$, для $A = \lambda E$. Тогда $\chi_A(t) = (t - \lambda)^k$.
- $m_A(t) = t^k$, тогда $A -$ и $\chi_A(t) = t^n$. Можно взять нулевой жордановый блок и нулевуюматрицу и соединить их в блочно диагональной маньере.
- Если $m_A(t) = (t - 1)^k$, то A называется унипотентом.
- Если $m_A(t) = t(t - 1)$, то A – проектор. Идемпотентен

Глава 2

Поля и их расширения

Пусть $\Bbbk$ – поле. Тогда можно рассмотреть гомоморфизм $\varkappa : \mathbb{Z} \to \Bbbk, 1 \mapsto 1$, у него есть ядро $\mathrm{Ker}(\varkappa) \subseteq \mathbb{Z}$, это идеал в $\mathbb{Z}$, он главный, так как идеал кольца главных идеалов, пусть он равен (d).

Утверждение: d – простое число или 0.

Доказательство: Ядро – прообраз простого идеала, а значит ядро просто.

Определение: d – характериситка $\Bbbk$, её мы обозначаем $\mathrm{char}(\Bbbk) = d$, то есть простое число или 0, которое однозначно определяется по полю.

- $\mathrm{char}(\mathbb{Q}) = 0$
- $\mathrm{char}(\mathbb{Z}/p\mathbb{Z}) = p$

Напоминание: Если $f : \mathbb{K} \to \mathbb{L}$ гомоморфиз полей, то он инъективен. Так как несобственный идеал только 0.

$A = \mathrm{Im}(\varkappa)$ – область целостности. Тогда можно рассмотреть поле частных $\mathrm{Frac}(A) \leq \Bbbk$, подполе в $\Bbbk$, оно назаватеся простым подполем.

$$\mathrm{Frac}(A) \cong \begin{cases} \mathbb{Q} & \mathrm{char}(\Bbbk) = 0 \\ \mathbb{Z}/p\mathbb{Z} & \mathrm{char}(\Bbbk) = p \end{cases}$$

Простое подполе определено однозначно, так как гомоморфизм $\varkappa$ определен однозначно, канонически. Оно называется простым, так как в нём нет собственных подполей.

Утверждение: Пусть $f : \mathbb{K} \to \mathbb{L}$ – гомоморфизм полей. Тогда $\mathrm{char}(\mathbb{K}) = \mathrm{char}(\mathbb{L})$ и f индуцирует изоморфизм простых подполей в $\mathbb{K}$ и $\mathbb{L}$.

Доказательство:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "\varkappa_K"] \arrow[rr, bend right, "\varkappa_L"'] & \mathbb{K} \arrow[r, "f"] & \mathbb{L} \end{tikzcd}$$

Давайте тогда заметим, что композиция является гомоморфизмом $\varkappa$ для $\mathbb{L}$, так как композиция перводит единицу в единицу. Отсюда следует, что ядро $\varkappa_L$ равно ядру $\varkappa_K$, так как f вложение. Более того $\mathrm{Im}(\varkappa_K) \cong_f \mathrm{Im}(\varkappa_L)$, а значит простые подполя изоморфны, а характеристики равны.

Определение: $K \leq L$ называется расширением полей, если $K \hookrightarrow L$, то есть следующий набор данных, поле K, поле L и вложение. Иногда это обозначается (L/K) и черта читается как "над".

Если $K \leq L$, то L является векторным пространством над K. Тогда можно говорить о размерности L над K и если $\dim_K L \leq \infty$, то расширение мы называем конечным, а размерность мы будем писать чуть иначе $\dim_K L = [L : K]$.

$K_1 \leq K_2 \leq \ldots \leq K_s$ мы называем башней полей, а расширение $K_i \leq K_{i+1}$ – этаж этой башни.

Пример: $\mathbb{Q} \leq \mathbb{R} \leq \mathbb{C}$ в этой башне только второй этаж конечен.

Утверждение: Если $F \leq K \leq L$, то $[L : F] = [L : K][K : L]$

Доказательство: Пусть $K = \langle x_i \rangle_F$, $x_i \in K$, где $\{x_i\}$ базис K над L и пусть $L = \langle y_j \rangle_K$, $y_j \in L$, где $\{y_j\}$ базис L над F. Тогда мы можем построить базис L над F, а именно $L = \langle x_i y_j \rangle_F$ поверим это. Пусть $a \in L$, тогда его можно разложить над $\{y_j\}$, то есть $a = \sum a_j y_j$, $a_j \in K$. Но тогда a_j можно разложить над $\{x_i\}$, то есть $a_j = \sum a_{i,j} x_i$, $a_{i,j} \in F$, а тогда $a = \sum a_{i,j} x_i y_j$, что означает $\{x_i y_j\}$ порождает L над F.

Пусть теперь