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 1.

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

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

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 $d_1 | d_2 | \dots | d_k$ на диагонали.

Тогда $M \cong R^{n-k} \oplus R/(d_i) \oplus \dots \oplus R/(d_k)$ (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

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

Пусть $r \in R$, $r \neq 0$, $M[r] := \{m \in M : rm = 0\} \leq M$ - подмодуль, p - прrстой 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 $\mathrm{Tors}(M) \cong \bigoplus_{p-\text{простое}} M_p$.

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 $\bigoplus M_p \to \mathrm{Tors}(M)$, 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. $m \in \mathrm{Tors}(m)$, $rm = 0$, $r = \Pi_{i=1}^n p_i^{\alpha_i}$, 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.

□

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 $V = \mathrm{Tors}(V)$ (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 $\dim_F F[t]/(f_i) = \deg f_i < \infty$. $\square$

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

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

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 2.

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.

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

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:

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

Рассмотрим цепочку вложенных пространств:

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

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

Осталось найти тот самый базис, в котором матрица A имеет нужный вид. Рассмотрим фактор-пространство $V/\mathrm{Ker}(A^{k-1})$, и выберем в нём базис. Это даёт нам относительный базис V относительно $\mathrm{Ker}(A^{k-1})$ (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 $s = \dim V - \dim \mathrm{Ker}(A^{k-1})$.

Теперь рассмотрим $\mathrm{Ker}(A^{k-1})/(\mathrm{Ker}\, A^{k-2} + \mathrm{Im}\, A)$ - подпространство, порождённое $\mathrm{Ker}\, A^{k-2}$ и $\mathrm{Im}\, A$. 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 $k-i$: $\mathrm{Ker}(A^{k-i})/(\mathrm{Ker}(A^{k-i-1}) + \mathrm{Im}\, A^i)$, рассмотрим тут базис и проделаем аналогичные операции.