# 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).

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

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 $\psi$ 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

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

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

$N_i$ - 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).

тут надо дописать какую-то ебанину с кучей формул

## 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.