Алгебра 9
06.11.97

Часть 1. Основные свойства.

Модуль M над кольцом A называется конечнопорожденным, если имеется конечное подмножество (*образующие*) $\{m_1, \dots, m_k\} \subset M$ такое, что любой элемент $m \in M$ выражается в виде $a_1m_1 + \dots + a_km_k$, $a_i \in A$. Если модуль M порожден единственной образующей m, он называется *циклическим.* Например, циклические модули над $\mathbb{Z}$ — это в точности циклические абелевы группы. Всякий циклический модуль M изоморфен фактору A/I по некоторому идеалу: $I = \{a \in A \mid aM = 0\}$. Кстати, всякий идеал является подмодулем в A, рассматриваемом как модуль над собой.

Циклический модуль является аналогом одномерного векторного пространства над полем. Аналогом базиса является *система независимых образующих*: $\{m_1, \dots, m_k\} \subset M$ называются независимыми, если из равенства $a_1m_1 + \dots + a_km_k = 0$ вытекает $a_1m_1 = \dots = a_km_k = 0$. В этом случае подмодуль $(m_1, \dots, m_k) \subset M$, порожденный $m_1, \dots, m_k$, является прямой суммой циклических подмодулей, порожденных m_i, т.е. $(m_1, \dots, m_k) = (m_1) \oplus \dots \oplus (m_k)$.

Вообще говоря, не всякий модуль обладает системой независимых образующих. Например, в максимальном идеале $(x, y) \subset \mathbb{C}[x, y]$, рассматриваемом как модуль над $\mathbb{C}[x, y]$, нельзя выбрать независимые образующие (проверьте!). Модуль M имеет систему независимых образующих тогда и только тогда, когда он изоморфен прямой сумме циклических модулей: $M = A/I_1 \oplus \dots \oplus A/I_k$.

Модуль M называется *периодическим*, если $\exists a \in A$, $a \neq 0 \mid aM = 0$. Такой a называется *периодом* M. Множество всех периодов (и еще нуль) образует идеал $Ann(M) \subset A$, называемый *аннулятором* M. Обратно, для данного идеала $I \subset A$ его *аннулятор* $M_I \subset M$ — это подмодуль, аннулируемый всеми элементами I. Модуль M называется *конечным*, если он конечнопорожден и периодичен. Например, конечные $\mathbb{Z}$-модули — это в точности конечные абелевы группы, а конечный $\mathbb{C}[t]$-модуль — это то же самое, что конечномерное $\mathbb{C}$-векторное пространство V с действием линейного оператора $T: \ V \to V$.

Часть 2. Модули над кольцами главных идеалов.

Теорема. Пусть A — кольцо главных идеалов. Тогда любой конечный модуль M над A обладает системой независимых образующих, т.е. является прямой суммой циклических модулей.

Доказательство: Пусть $a \in A$ — период M, т.е. $M = M_{(a)}$. Мы будем для краткости писать M_a вместо $M_{(a)}$. Разложим a в произведение взаимно простых элементов: $a = bc$.

Лемма. $M = M_a = M_b \oplus M_c$.

Доказательство: Так как A — кольцо главных идеалов, найдутся $x, y \in A$ такие, что $bx+cy = 1$. Представим $m \in M$ в виде $m = 1 \cdot m = (bx+cy) \cdot m = bx \cdot m + cy \cdot m$. Первое слагаемое лежит в M_c (так как $c(bx \cdot m) = cbx \cdot m = ax \cdot m = a(x \cdot m) = 0$), а второе — в M_b. Значит, $M = M_b + M_c$. Но $M_b \cap M_c = 0$: если $bm = cm = 0$, то $m = xb \cdot m + yc \cdot m = 0$. Итак, $M = M_a = M_b \oplus M_c$. $\square$

Если теперь $a = p_1^{n_1} \cdot p_k^{n_k}$ — разложение a на простые множители, то применяя Лемму несколько раз, получаем $M = M_a = M_{p_1^{n_1}} \oplus \ldots \oplus M_{p_k^{n_k}}$. Будем обозначать $M(p) \subset M$ подмножество элементов, аннулируемых какой-нибудь степенью простого p. Очевидно, $M(p)$ является подмодулем M. Итак, мы получили разложение $M = M(p_1) \oplus \ldots \oplus M(p_k)$. Теперь осталось для простого p разложить $M(p)$ в прямую сумму циклических модулей. Иными словами, мы можем считать, что $M = M(p)$. Будем говорить, что $m \in M$ имеет *период* p^r, если $p^r \cdot m = 0$, а $p^{r-1} \cdot m \neq 0$.

Лемма. Пусть p^r — точный период M, т.е. $p^r M = 0$, а $p^{r-1} M \neq 0$. Возьмем $m \in M$ периода p^r и рассмотрим порожденный им подмодуль $(m) \subset M$. Обозначим соответствующий фактормодуль через $\overline{M} = M/(m)$. Пусть $\overline{y}_1, \ldots, \overline{y}_k \in \overline{M}$ независимы и имеют периоды, соответственно, $p^{n_1}, \ldots, p^{n_k}$. Тогда найдутся представители $y_1, \ldots, y_k \in M$, имеющие те же периоды, и такие что $m, y_1, \ldots, y_k$ независимы в M.

Доказательство: Пусть y_1' — какой-нибудь представитель $\overline{y}_1$ в M. Тогда $p^{n_1} \cdot y_1' \in (m)$, т.е. $p^{n_1} y_1' = a \cdot m$. Представим a в виде $a = p_1^s b$, где b не делится на p. Если $s = r$, то $p^{n_1} \cdot y_1' = 0$, но $p^{n_1 - 1} y_1' \neq 0$, так как даже его образ в $\overline{M}$ не равен нулю. Значит, y_1' имеет период n_1, и мы полагаем $y_1 := y_1'$. Если же $s < r$, то $p^{r-s}(p^{n_1} \cdot y_1') = 0$, а $p^{r-s-1}(p^{n_1} \cdot y_1') \neq 0$, откуда период y_1' равен $p^{r-s+n_1} \leqslant p^r \;\Rightarrow\; n_1 \leqslant s$. Положим $y_1 := y_1' - p_1^{s-n_1} b \cdot m$. Теперь $p^{n_1} y_1 = p^{n_1} \cdot y_1' - p^s b \cdot m = 0$. Аналогично выберем искомые подъемы y_i. Осталось проверить независимость. Пусть $am + a_1 y_1 + \ldots + a_k y_k = 0$. Тогда в модуле $\overline{M}$ имеем $a_1 \overline{y}_1 + \ldots + a_k \overline{y}_k = 0$, откуда $a_i y_i = 0 \;\Rightarrow\; a_i$ делится на $p^{n_i} \;\Rightarrow\; a_i y_i = 0 \;\Rightarrow\; am = 0$. $\square$

Закончим доказательство Теоремы. Заметим, что подмодуль $M_p \subset M$ является конечномерным векторным пространством над полем $A/(p)$. В условиях предыдущей Леммы $\dim M_p > \dim \overline{M}_p$: базис $\{\,\overline{z}_1, \ldots, \overline{z}_k\,\} \subset \overline{M}_p$ можно поднять до (линейно) независимых элементов $z_1, \ldots, z_k \in M_p$, но сверх того там содержится $p^{r-1} m$, который линейно независим от $z_1, \ldots, z_k$. Теперь можно воспользоваться индукцией по $\dim M_p$. Предположим, что $\overline{y}_1, \ldots, \overline{y}_k$ — система независимых образующих $\overline{M}$. Тогда $x, y_1, \ldots, y_k$ — система независимых образующих M. Доказательство Теоремы закончено.

Замечание. Итак, мы получили разложение в два этапа: сначала каноническое разложение $M = M_a = \bigoplus_{p_i | a} M(p_i)$, а потом какое-то разложение $M(p_i) \simeq \bigoplus_{j \geqslant 1} (A/(p_i^j))^{\oplus n_{ij}}$. Утверждается, что кратности n_{ij} определены однозначно. В самом деле, легко видеть, что $\dim M_{p_i} = \sum_{j \geqslant 1} n_{ij}$, $\dim (M/M_{p_i})_{p_i} = \sum_{j \geqslant 2} n_{ij}$, $\dim((M/M_{p_i})/(M/M_{p_i})_{p_i})_{p_i} = \sum_{j \geqslant 3} n_{ij}$ и так далее.

Часть 3. Приложения.

Пусть $A = \mathbb{Z}$. Тогда Теорема означает, что всякая конечная абелева группа разлагается в прямую сумму циклических групп вида $\mathbb{Z}/p^j\mathbb{Z}$. На самом деле примерно так же доказывается, что всякая *конечнопорожденная* абелева группа разлагается в прямую сумму конечных циклических групп и свободных циклических групп. С примером такого разложения мы уже сталкивались: всякий идеал кольца целых числового поля является прямой суммой свободных циклических групп.

Пусть $A = \mathbb{C}[t]$. Так как все неразложимые многочлены над $\mathbb{C}$ — линейные, Теорема означает, что всякий конечный $\mathbb{C}[t]$-модуль разлагается в прямую сумму циклических модулей вида $V_\lambda^j := \mathbb{C}[t]/(t-\lambda)^j$. Запишем матрицу оператора умножения на t в базисе $\overline{1}, \overline{t-\lambda}, \dots, \overline{(t-\lambda)^{j-1}}$ $\mathbb{C}$-векторного пространства V_λ^j. Получим *жорданов блок*

$$\begin{pmatrix} \lambda & 1 & 0 & 0 & \dots & 0 \\ 0 & \lambda & 1 & 0 & \dots & 0 \\ \vdots & \vdots & \ddots & \ddots & \vdots & \vdots \\ \\ 0 & 0 & \dots & 0 & \lambda & 1 \\ 0 & 0 & \dots & 0 & 0 & \lambda \end{pmatrix}$$

Значит, в подходящем базисе матрица всякого линейного оператора в $\mathbb{C}$-векторном пространстве состоит из жордановых блоков, т.е. имеет *жорданову нормальную форму.* В вещественном векторном пространстве такой базис не всегда можно найти (так как в $\mathbb{R}[t]$ есть нелинейные неприводимые многочлены). Например, матрица $\left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ не приводится к жордановой нормальной форме над $\mathbb{R}$ (а над $\mathbb{C}$ даже диагонализуется).

Как найти жорданову форму данной матрицы T? Числа λ_i, стоящие на диагонали — это корни характеристического многочлена $\chi(T,\lambda) = \det(T - \lambda \mathrm{Id})$, т.е. собственные значения T. Число λ_i встречается на диагонали столько раз, какова кратность корня λ_i многочлена $\chi(T,\lambda)$ — для доказательства надо посчитать $\chi(T,\lambda)$ в том базисе, в котором T имеет жорданов вид. Пусть блоков с λ_i на диагонали размера 1 — n_{i1} штук, размера 2 — n_{i2} штук и т.д. В соответствии с Замечанием после доказательства Теоремы, числа n_{ij} можно найти так: $\dim \operatorname{Ker}(T-\lambda_i) = \sum_{j\geqslant 1} n_{ij}$, $\dim \operatorname{Ker}(T-\lambda_i)^2 = \sum_{j\geqslant 1} n_{ij} + \sum_{j\geqslant 2} n_{ij}$ и т.д. Подчеркнем, что характеристическим многочленом жорданова нормальная форма *не определяется*: например, обе матрицы $\left(\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right)$ и $\left(\begin{smallmatrix} 0 & 1 \\ 0 & 0 \end{smallmatrix}\right)$ имеют характеристический многочлен λ^2.