## Модули над евклидовыми кольцами

В прошлой лекции мы обсудили связь задачи о приведении оператора к каноническому виду и задачи об описании конечнопорождённых модулей над кольцом многочленов. Мы сейчас решим вторую из этих задач.

Напомним, что определение модуля над кольцом совершенно аналогично определению векторного пространства над полем:

**Определение 1.** Пусть $R$ — ассоциативное коммутативное кольцо с единицей. *Модулем* над $R$ ($R$-модулем) называется абелева группа $M$, для которой есть отображение $R\times M \to M$, $(r,m)\mapsto rm$, такое что

- $\forall m_1, m_2 \in M, r \in R$ $r(m_1+m_2) = rm_1 + rm_2$;
- $\forall r_1, r_2 \in R, m \in M$ $(r_1+r_2)m = r_1m + r_2m$;
- $\forall r_1, r_2 \in R, m \in R$ $r_1(r_2m) = (r_1r_2)m$;
- $\forall m \in M$ $1m = m$.

**Пример 1.** Модуль над $\mathbb{Z}$ — это просто абелева группа, т. к. умножение на целые числа выражается через сложение; $nx = \underbrace{x+x+\ldots+x}_{n \text{ слагаемых}}$. Всякое кольцо есть модуль над собой: в качестве отображения $R\times R\to R$ надо взять умножение.

Начнём с нескольких общих определений.

**Определение 2.** *Подмодуль* $N$ модуля $M$ — это абелева подгруппа, замкнутая относительно умножения на элементы кольца, т. е. если $n\in N$, $r\in R$, то $rn\in N$.

**Пример 2.** Подмодуль кольца, рассматриваемого как модуль над собой (см. выше) — это идеал кольца.

**Определение 3.** Если $N$ — подмодуль модуля $M$, то можно определить на $M$ отношение эквивалентности: $m_1\sim m_2$, если $m_1-m_2\in N$. Тогда на множестве классов эквивалентности имеется естественная структура модуля. Этот модуль называется *фактормодулем $M$ по $N$* и обозначается $M/N$.

**Упражнение 1.** Введите на множестве классов эквивалентности структуру модуля. Проверьте корректность Вашего определения.

**Определение 4.** Отображение модулей (над одним и тем же кольцом $R$) $\varphi\colon M_1\to M_2$ называется *гомоморфизмом*, если оно является гомоморфизмом абелевых групп, и $\varphi(rm)=r\varphi(m)$ для $m\in M_1$, $r\in R$. Обратимый гомоморфизм называется *изоморфизмом.*

**Определение 5.** По гомоморфизму $\varphi$ канонически определены подмодули $\operatorname{Ker}\varphi\subset M_1$ (*ядро* $\varphi$) и $\operatorname{Im}\varphi\subset M_2$ (*образ* $\varphi$).

**Теорема 1.** (О гомоморфизме) Имеет место изоморфизм модулей $\operatorname{Im}\varphi\simeq M_1/\operatorname{Ker}\varphi$.

**Упражнение 2.** Докажите эту теорему.

**Определение 6.** Пусть $M_1$ и $M_2$ — модули над кольцом $R$. Их *прямая сумма* $M_1\oplus M_2$ — множество пар $(m_1,m_2)$, где $m_1\in M_1$, $m_2\in M_2$, с покомпонентным сложением и умножением на элементы кольца. Аналогично определяется прямая сумма нескольких модулей. Говорят, что *модуль разлагается в прямую сумму своих подмодулей* $M_1,\ldots,M_k$, если каждый его элемент представляется единственным образом в виде суммы $m_1+\ldots+m_k$, где $m_i\in M_i$. В этом случае модуль изоморфен прямой сумме $M_1\oplus\ldots\oplus M_k$.

**Определение 7.** Пусть $m_1,\ldots,m_k\in M$. Подмодуль всех элементов вида $r_1m_1+\ldots+r_km_k$, где $r_i\in R$, называется *подмодулем, порождённым* $m_1,\ldots,m_k$, и обозначается $(m_1,\ldots,m_k)$. Если $(m_1,\ldots,m_k)=M$, то говорят, что *модуль $M$ порождается* $m_1,\ldots,m_k$, и эти элементы называются *образующими* модуля $M$. Модуль, у которого существует конечная система порождающих, называется *конечнопорождённым.*

**Определение 8.** Система элементов $m_1,\ldots,m_k$ называется *линейно независимой*, если из $r_1m_1+\ldots+r_km_k=0$ ($r_i\in R$) следует $r_1=\ldots=r_k=0$. Линейно независимая система образующих называется *базисом* модуля.

**Определение 9.** Конечнопорождённый модуль, обладающий базисом, называется *свободным*. Модуль, порождённый одним элементом, называется *циклическим*.

**Пример 3.** Не всякий модуль обладает базисом; например, конечная абелева группа не обладает базисом как $\mathbb{Z}$-модуль.

**Теорема 2.** Всякий циклический модуль изоморфен факторкольцу по некоторому идеалу.

Действительно, пусть модуль $M$ порождён элементом $m$. Рассмотрим гомоморфизм из $R$ (рассматриваемого как модуль над собой) в $M$, переводящий единицу в $m$. Ясно, что образ есть всё, поэтому $M$ есть фактормодуль по кольца по некоторому подмодулю (ядру). Подмодуль в кольце есть идеал, поэтому требуемое доказано.

Оказывается, что если кольцо евклидово, то конечнопорождённые модули над ним можно эффективно описать. Идея описания содержится в доказательстве предыдущей теоремы. В самом деле, для конечнопорождённого модуля $M$ можно построить гомоморфизм из свободного модуля в $M$, образ которого есть $M$. Поэтому задачу описания конечнопорождённого модуля легко свести к описанию подмодулей свободного модуля. Поэтому будем временно изучать свободные модули.

**Теорема 3.** Во всех базисах свободного модуля $M$ над евклидовым кольцом $R$ одно и то же число элементов.

Действительно, возьмём какой-нибудь простой элемент $p$ кольца $R$ и рассмотрим модуль $M/pM$. Это векторное пространство над полем $R/(p)$ (если $[a] \in R/(p)$, $[f] \in M/pM$, то положим $[a][f] = [af]$; это определение корректно — проверьте!), и образ системы образующих при факторизации есть базис этого векторного пространства. (Пусть $f_1, \ldots, f_n$ — базис, но классы $[f_1], \ldots, [f_n]$ линейно зависимы, т. е. $[a_1][f_1] + \ldots + [a_n][f_n] = 0$. Тогда $[a_1 f_1 + \ldots + a_n f_n] = 0$, т. е. $a_1 f_1 + \ldots + a_n f_n = pm \in pM$. Отсюда видно, что для всех $i$ элемент $a_i$ делится на $p$ (разложим $m$ по базису $f_i$), поэтому над полем $R/(p)$ исходная зависимость была тривиальна.) Утверждение доказано. (Если простых элементов нет, то все элементы обратимы и кольцо само является полем, так что доказательство проходит.)

**Определение 10.** Число элементов базиса свободного модуля $M$ называется его *рангом* и обозначается $\operatorname{rk} M$.

**Теорема 4.** (О подмодулях свободного модуля) Всякий подмодуль $N$ свободного модуля $M$ над евклидовым кольцом является свободным модулем ранга не более $\operatorname{rk} M$, причём существует базис $e_1, \ldots, e_m$ модуля $M$ и такие элементы $u_1, \ldots, u_n$ кольца $R$, что $u_1 e_1, \ldots, u_n e_n$ — базис подмодуля $N$, причём $u_1 \mid u_2 \mid \ldots \mid u_n$.

Докажем сначала первое утверждение индукцией по $\operatorname{rk} M$. Если $\operatorname{rk} M = 1$, то модуль естественно отождествляется с $R$, а подмодуль — с некоторым идеалом. В евклидовом кольце все идеалы главные, поэтому утверждение верно.

Пусть теперь $\operatorname{rk} M = m > 1$ и $e_1, \ldots, e_m$ — какой-либо базис $M$. Положим $M_1 = (e_1, \ldots, e_{m-1})$, $N_1 = N \cap M_1$. По предположению индукции, $N_1$ — свободный модуль ранга не более $m-1$. Если $N = N_1$, то всё доказано. В противном случае рассмотрим канонический гомоморфизм $\pi\colon M \to M/M_1$. Поскольку $M/M_1$ — свободный циклический модуль, ясно, что $\pi(N)$ — тоже свободный циклический модуль. Пусть он порождён образом элемента $f$. Тогда ясно, что $N \simeq N_1 \oplus (f)$, поэтому $N$ — свободный модуль ранга не более $m$.

Докажем второе утверждение теоремы. Пусть $e_1, \ldots, e_m$ — базис модуля $M$. Выразим базис $f_1, \ldots, f_n$ модуля $N$ через $e_1, \ldots, e_m$:

$$f_i = \sum_{i=1}^{m} c_{ij} e_j \ (c_{ij} \in R).$$

Мы можем делать с системой образующих модуля следующие элементарные преобразования (получая из неё другую систему образующих):

- Перестановка двух базисных элементов.
- Прибавление к одному из элементов другого, умноженного на элемент кольца $R$.

Заметим, что элементарные преобразования базиса модуля $M$ приводят к преобразованиям столбцов матрицы $C$, а элементарные преобразования базиса модуля $N$ — к элементарным преобразованиям строк этой матрицы. Поэтому достаточно доказать, что всякая матрица преобразованиями строк и столбцов может быть приведена к диагональному виду с выполнением сформулированных в теореме условий делимости.

Докажем это утверждение индукцией по $n$ — числу строк матрицы — а при данном числе строк индукцией по минимуму нормы ненулевых элементов матрицы (если матрица нулевая, то утверждение очевидно).

Итак, пусть $C$ — матрица из $n$ строк. Перестановкой строк и столбцов добьёмся того, что наименьший по норме ненулевой элемент есть $c_{11}$. Если есть элемент $c_{i1}$, не делящийся на $c_{11}$, то его с помощью элементарных преобразований можно заменить на его остаток при делении на $c_{11}$, т. е. матрица сведена к матрице, в которой минимум нормы ненулевых элементов уменьшился. Поэтому можно считать, что все элементы первого столбца (и, аналогично, первой строки) делятся на $c_{11}$. Значит, с помощью элементарных преобразований можно добиться, чтобы все элементы первой строки и первого столбца, кроме $c_{11}$, были равны нулю.

Пусть теперь некоторый элемент $c_{ij}$ с $i, j \geqslant 2$ не делится на $c_{11}$: $c_{ij} = qc_{11} + r$. Прибавим к $j$-ому столбцу первый, после чего вычтем из $i$-ой строки первую, умноженную на $q$. Получим матрицу, в которой минимум ненулевых элементов меньше. Значит, можно считать, что все элементы матрицы делятся на $c_{11}$. Вычеркнем теперь из матрицы первую строку и первый столбец. Полученную матрицу можно по предположению индукции привести к диагональному виду, причём каждый следующий элемент на диагонали делится на предыдущий. Значит, можно привести к такому виду и исходную матрицу (ибо все элементы на диагонали, очевидно, делятся на $c_{11}$).

**Теорема 5.** Любой конечнопорождённый модуль над евклидовым кольцом изоморфен прямой сумме циклических модулей.

Действительно, пусть модуль $N$ порождается элементами $x_1, \ldots, x_n$. Рассмотрим отображение модулей $\pi\colon R^n \to N$, переводящее элемент $(a_1, \ldots, a_n)$ в элемент $\pi((a_1, \ldots, a_n)) = a_1x_1 + \ldots + a_nx_n$. Это, очевидно, гомоморфизм с образом $M$. Значит, $M \simeq R^n/\operatorname{Ker}\pi$. Согласно нашей теореме, найдётся такой базис $e_1, \ldots, e_n$ модуля $R^n$, что подмодуль $\operatorname{Ker}\pi$ порождён элементами $u_1e_1, \ldots, u_me_m$, где $u_i \in R$, причём $u_i \mid u_{i+1}$ при $1 \leqslant i \leqslant m-1$. Пусть $\pi_i$ — канонический гомоморфизм из $R$ в $R/(u_i)$. Будем считать для удобства $m = n$, положим, если нужно, $u_i = 0$ при $i > m$. Рассмотрим гомоморфизм $\varphi\colon R^n \to R/(u_1) \oplus \ldots \oplus R/(u_n)$, $\varphi(b_1e_1 + \ldots + b_ne_n) = (\pi_1(b_1), \ldots, \pi_n(b_n))$. Ясно, что этот гомоморфизм сюръективен, а его ядро изоморфно (и даже равно) ядру гомоморфизма $\pi$. Поэтому и образы изоморфны, что доказывает нашу теорему.

Более того, мы доказали, что можно выбрать циклические модули специальным образом: в соответствии с последовательностью $u_i$, в которой каждый член делит следующий. На практике есть куда более естественный способ выбора разложения в прямую сумму.

**Определение 11.** Циклический модуль называется *примарным*, если он изоморфен модулю $R/(p^k)$, где $p$ — простой элемент.

**Теорема 6.** Всякий конечнопорождённый модуль над кольцом главных идеалов изоморфен прямой сумме свободных модулей и циклических примарных модулей.

Действительно, для этого в силу доказанной теоремы проверить, что несвободный циклический модуль изоморфен прямой сумме примарных циклических модулей. Это следует из существования разложения на простые множители и того, что для взаимно простых элементов $r_1, r_2$ имеет место изоморфизм $R/(r_1r_2) \simeq R/(r_1) \oplus R/(r_2)$. Последнее можно доказать так: рассмотрим гомоморфизм $\pi\colon R \to R/(r_1) \oplus R/(r_2)$, $\pi(r) = (\pi_1(r), \pi_2(r))$, где $\pi_k$ — канонический гомоморфизм $R \to R/(r_k)$ $(k = 1, 2)$. Ясно, что его ядро есть идеал $(r_1r_2)$. Осталось проверить, что его образ есть всё. Это легко выводится из того, что существуют элементы $x, y \in R$: $xr_1 + yr_2 = 1$. Действительно, образ элемента $bxr_1 + ayr_2$ есть $(\pi_1(a), \pi_2(b))$.

**Упражнение 3.** Завершите доказательство теоремы.

**Теорема 7.** Набор циклических модулей из предыдущей теоремы определён однозначно с точностью изоморфизма.

Мы докажем эту теорему в следующей лекции.

**Упражнение 4.** Набор циклических модулей в разложении $M = R/(u_1) \oplus \ldots \oplus R/(u_m)$, где $u_1 \mid \ldots \mid u_m$, также определён однозначно с точностью до изоморфизма.