Конечнопорождённые модули

Определение 1. *Подмодуль* $M' \subset M$ — подмножество, замкнутое относительно сложения, вычитания и действия.

Определение 2. Модуль называется *простым*, если у него нет нетривиальных (кроме нулевого и всего модуля) подмодулей.

Модули устроены проще колец и групп — любой подмодуль может быть получен как ядро отображения в определённый ниже модуль.

Определение 3. Пусть $M' \subset M$ — подмодуль. Определим *фактормодуль* M/M' как множество классов эквивалентности элементов M по отношению $m_1 \sim m_2$, если $m_2 - m_1 \in M'$.

Предложение 1 *Сложение, вычитание и действие корректно определены на множестве* M/M' *и задают на нём структуру модуля.*

Пример. Для кольца K и левого идеала $I \subset K$ левый модуль K/I является фактормодулем K по подмодулю I.

Определение 4. Подмодуль M, *порождённый (generated by)* подмножеством $X \subset M$ — минимальный по вложению подмодуль M, содержащий X. Для векторных пространств он также называется *линейной оболочкой.*

Будем говорить, что модуль M порождён подмножеством X, если подмодуль, порождённый X совпадает со всем M. В этом случае будем называть элементы X *образующими (generators)* модуля M.

Легко увидеть, что для левого модуля такой подмодуль будет состоять из элементов вида $x_1 m_1 + \cdots + x_k m_k$, где $x_i \in K$, $m_i \in X$.

Определение 5. *Конечнопорождённый модуль* — модуль, порождённый некоторым своим конечным подмножеством. Такие векторные пространства также называются *конечномерными.*

Пример. $\mathbb{C}$ является конечнопорождённым как модуль над $\mathbb{R}$ и $\mathbb{C}$, но не как модуль над $\mathbb{Q}$ и $\mathbb{Z}$.

Теорема 1 *(i) Всякий конечнопорождённый модуль над евклидовым кольцом* K *изоморфен прямой сумме модулей вида* K *и* K/p^iK, *где* $p \in K$ *прост,* $i \in \mathbb{N}$.

(ii) Такое разложение единственно.

Пример. В случае $K = \mathbb{Z}$ получаем известную теорему о классификации конечнопорождённых абелевых групп.

Пример. В поле не бывает нетривиальных идеалов, тем самым, всякое конечномерное векторное пространство над F изоморфно F^n для некоторого натурального числа n, называемого *размерностью.* При этом $F^m \cong F^n$ только при $m = n$.

Цель этой лекции — доказательство Теоремы 1. На самом деле, задача о классификации модулей и задача о решении системы линейных уравнений опираются на один и тот же метод — классификацию матриц с точностью до умножению на обратимую, другими словами, классификацию отображений свободных модулей $\phi : K^n \to K^m$ с точностью до композиции с изоморфизмами $\psi_1 : K^n \to K^n$ и $\psi_2 : K^m \to K^m$.

Заметим, что если $m_1, \ldots, m_n$ — образующие модуля M, то отображение $\mathrm{gen} : K^n \to M$, $\mathrm{gen}((x_1, \ldots, x_n)) = x_1 m_1 + \cdots + x_n m_n$, является наложением. Тогда $M \cong K^n/\mathrm{Ker}(\mathrm{gen})$, и осталось описать ядро отображения gen.

Определение 6. *Соотношения* в модуле M — образующие ядра отображения gen.

Если соотношений конечное число r, то M определяется отображением $K^r \to K^n$, переводящим образующие K^r в соотношения. При этом композиция с обратимым отображением $K^r \to K^r$ заменяет набор соотношений на эквивалентный им, а композиция с обратимым отображением $K^n \to K^n$ записывает те же соотношения в другом наборе образующих M. Фактически, из коэффициентов соотношений вида $a_{11}m_1 + \cdots + a_{1n}m_n = 0$ изготовляется матрица, которую можно в условиях Теоремы 1 привести к диагональному виду (нормальной форме Смита).

Пусть теперь соотношений бесконечно много, докажем, что из них можно выбрать конечный набор. Проведём индукцию по числу образующих. Базой можно считать нулевой модуль с нулём образующих. Вспомним, что первый диагональный элемент в нормальной форме Смита — наибольший общий делитель элементов матрицы. Пусть a — наибольший общий делитель всех коэффициентов соотношений, его можно получить как наибольший общий делитель конечного набора соотношений. Составим из коэффициентов этих соотношений матрицу и приведём к нормальной форме Смита. Тогда в новых образующих возникнет соотношение $am_1 = 0$, используя которое запишем все остальные соотношения без m_1. Теперь рассмотрим подмодуль, порождённый $m_2, \ldots, m_n$, и применим к нему предположение индукции. Этот набор соотношений вместе с соотношением $am_1 = 0$ определит модуль.

Таким образом, в новых образующих соотношения будут иметь вид $a_i m_i = 0$, $i = 1 \ldots s$, которые соответствуют модулю $K^{n-s} \oplus K/a_1K \oplus K/a_2K \oplus \cdots \oplus K/a_sK$. Теперь разложим a_i на взаимно-простые множители вида $p_j^{l_j}$ и воспользуемся китайской теоремой об остатках, получив $K/a_iK = K/p_1^{l_1}K \oplus K/p_2^{l_2}K \oplus \ldots$, и, тем самым, требуемое в Теореме 1 разложение. Существование доказано, перейдём к единственности.

Лемма 1 *Пусть K евклидово. Тогда $K^m \cong K^n$ тогда и только тогда, когда $m = n$.*

Доказательство: Мы знаем, что отображение $K^m \to K^n$ однозначно задаётся матрицей $m \times n$, приведём её к нормальной форме Смита. Тогда нулевые столбцы укажут нам на наличие ядра отображения, или нулевые строки покажут, что отображение не является наложением.

Заметим, что для $x \in K$ и K-модуля M подмножество xM является подмодулем. Для евклидового K и простого $p \in K$ рассмотрим фактормодуль $p^nM/p^{n+1}M$. Так как pK действует на нём нулём, он автоматически является модулем над полем K/pK, и по Лемме 1 его размерность является инвариантом M по отношению к изоморфизмам.

Теперь если разложить M на слагаемые указанного в Теореме 1 вида, то размерность $p^nM/p^{n+1}M$ — количество слагаемых вида K и K/p^mK при $m > n$. Варьируя p и n, восстановим структуру разложения. Теорема 1 доказана.

Следствие 1 *Всякий конечнопорождённый модуль над евклидовым кольцом K изоморфен прямой сумме $K/a_1K \oplus \cdots \oplus K/a_nK$, где $a_i \in K$ — необратимые элементы, такие что $a_i | a_{i+1}$, причём такое разложение единственно.*

Доказательство: Используя китайскую теорему об остатках и разлагая ненулевые a_i на простые множители, сопоставим такому разложению разложение Теоремы 1. Чтобы доказать взаимную однозначность такого сопоставления, построим обратное отображение. Упорядочим степени простых чисел в разложении Теоремы 1, получим последовательности вида $p_i^{k_{i1}}, p_i^{k_{i2}}, \ldots$, где $0 < k_{i1} \leqslant k_{i2} \leqslant \ldots$. Добавляя при необходимости в начало этих последовательностей p_i^0, сделаем их все одной длины. Теперь положим a_j равным произведению $p_i^{k_{ij}}$, а слагаемым вида K будут соответствовать $a_j = 0$.

Следствие 2 *В случае евклидового кольца нормальная форма Смита однозначно определяется матрицей.*

Доказательство: Рассмотрим модуль, в котором соотношения заданы нашей матрицей. Тогда, умножая матрицу на обратимые, получим изоморфные модули. Но модули, соответствующие разным нормальным формам Смита, не изоморфны по Следствию 1.