

### 13. Тринадцатая лекция, 7 марта 2019 г.

**13.1. Модули над кольцами: определение.** Как известно, векторное пространство — это множество  $V$ , снабжённое двумя операциями: сложением (относительно которого оно является абелевой группой) и умножением на элементы фиксированного поля  $\mathbb{K}$ . Что будет, если попробовать заменить в этом определении поле  $\mathbb{K}$  на произвольное кольцо?

Например, всякая абелева группа является “векторным пространством над  $\mathbb{Z}$ ”: действительно: её элементы можно складывать между собой, а также умножать на целые числа по правилу  $n \cdot g = g + \dots + g$  (всего  $n$  слагаемых, с очевидными изменениями, если  $n < 0$ ). Это мотивирует следующее

**ОПРЕДЕЛЕНИЕ 13.1.** Пусть  $A$  — коммутативное ассоциативное кольцо с единицей. *Модуль* над кольцом  $A$  (или  *$A$ -модуль*) — это абелева группа, снабжённая действием кольца  $A$ , т.е. операцией  $A \times M \rightarrow M$ , удовлетворяющей следующим условиям:

- (M1):  $(ab)m = a(bm)$  для любых  $a, b \in A, m \in M$ ;
- (M2):  $1 \cdot m = m$  для любого  $m \in M$ ;
- (D1):  $(a + b)m = am + bm$  для любых  $a, b \in A, m \in M$ ;
- (D2):  $a(m + n) = am + an$  для любых  $a \in A, m, n \in M$ .

**ПРИМЕР 13.2.** Если  $A = \mathbb{K}$  — поле, то  $M$  есть не что иное, как векторное пространство над  $\mathbb{K}$ .

**ПРИМЕР 13.3.** Если  $A = \mathbb{Z}$ , то  $M$  — это просто абелева группа.

**ПРИМЕР 13.4** (очень важный!). Пусть  $A = \mathbb{K}[x]$ ,  $V$  — векторное пространство над  $\mathbb{K}$ ,  $\mathcal{A} \in \text{End}(V)$  — линейный оператор на  $V$ . Тогда  $V$  является  $\mathbb{K}[x]$ -модулем, на котором действие кольца многочленов задано так:

$$(a_n x^n + \dots + a_1 x + a_0) \cdot v = a_n \mathcal{A}^n v + \dots + a_1 \mathcal{A} v + a_0 v.$$

Иными словами,  $x$  действует на  $V$  при помощи оператора  $\mathcal{A}$ . Отметим, что разные линейные операторы задают *разные* структуры модуля на  $V$ .

**ПРИМЕР 13.5.** Всякое кольцо  $A$  является модулем над самим собой. Аксиомы (M1), (M2), (D1) и (D2) при этом следуют из определения кольца.

### 13.2. Подмодули, фактормодули, гомоморфизмы.

**ОПРЕДЕЛЕНИЕ 13.6.** Пусть  $M$  — модуль над  $A$ .  $N \subset M$  называется *подмодулем* в  $M$ , если  $n + n' \in N$  и  $an \in N$  для любых  $a \in A$  и  $n, n' \in N$ .

**ПРИМЕР 13.7.** Подмодули модулей из примеров 14.2 и 14.3 — это векторное подпространство и абелева подгруппа соответственно.

**ПРИМЕР 13.8.** Подмодуль модуля из примера 14.4 — это  $\mathcal{A}$ -инвариантное подпространство  $U \subset V$  (т.е. такое подпространство, для которого  $\mathcal{A}u \in U$  для любого  $u \in U$ ).

**ПРИМЕР 13.9.** Подмодуль модуля из примера 14.5 — это идеал  $I \subset A$ .

По подмодулям можно брать факторы.

**ОПРЕДЕЛЕНИЕ 13.10.** Пусть  $N \in M$  — подмодуль. Рассмотрим отношение эквивалентности на  $M$ :  $m \equiv m' \pmod{N}$ , если  $m - m' \in N$ . Множество классов эквивалентности  $m + N = [m]$  называется *фактормодулем* и обозначается через  $M/N$ . Операции на  $M/N$  задаются обычным образом:

$$(m + N) + (n + N) = (m + n) + N; \quad a(m + N) = am + N.$$

**УПРАЖНЕНИЕ 13.11.** Проведите сами все необходимые проверки корректности.

**ПРИМЕР 13.12.** Пусть  $A$  — кольцо,  $I \subset A$  — идеал. Тогда  $A/I$  тоже является  $A$ -модулем.

ОПРЕДЕЛЕНИЕ 13.13. Отображение  $A$ -модулей  $f: M \rightarrow N$  называется *гомоморфизмом*, если

$$f(x + y) = f(x) + f(y); \quad f(ax) = af(x)$$

для любых  $x, y \in M$ ,  $a \in A$ .

УПРАЖНЕНИЕ 13.14. Проверьте, что  $\text{Ker } f$  и  $\text{Im } f$  — подмодули в  $M$  и  $N$  соответственно.

ПРИМЕР 13.15. Пусть  $N \subset M$  — модуль и подмодуль. Отображение

$$\pi: M \rightarrow M/N, \quad m \mapsto m + N$$

является сюръективным гомоморфизмом (=эпиморфизмом). Оно называется *эпиморфизмом факторизации*.

Соответственно, имеется и теорема о гомоморфизме:

ТЕОРЕМА 13.16 (о гомоморфизме модулей). Пусть  $f: M \rightarrow N$  — гомоморфизм  $A$ -модулей. Тогда  $\text{Im } f \simeq M/\text{Ker } f$ . Более точно, отображение  $\varphi: \text{Im } f \rightarrow M/\text{Ker } f$ , при котором  $b = f(a) \in \text{Im } f$  отображается в  $\pi(a) = a + \text{Ker } f$ , есть изоморфизм.

ДОКАЗАТЕЛЬСТВО. Докажите эту теорему сами.  $\square$

**13.3. Системы порождающих. Конечно порождённые и циклические модули.** Пусть  $M$  —  $A$ -модуль,  $S \subset M$  — произвольное подмножество. Рассмотрим наименьший подмодуль в  $M$ , содержащий  $S$ . Это

$$\langle S \rangle = \{a_1x_1 + \dots + a_sx_s \mid x_i \in S, a_i \in A\}.$$

Если  $\langle S \rangle = M$ , то  $S$  называют *системой порождающих* модуля  $M$ . Если  $M$  допускает конечную систему порождающих, то он называется *конечно порождённым*.

ПРИМЕР 13.17.  $\mathbb{Q}$  как  $\mathbb{Z}$ -модуль не является конечно порождённым.

ПРИМЕР 13.18. Конечно порождённые  $\mathbb{K}$ -модули — это в точности конечномерные векторные пространства.

ОПРЕДЕЛЕНИЕ 13.19. Модуль, порождённый одним элементом, называется *циклическим*.

ПРИМЕР 13.20. Всякий циклический  $\mathbb{Z}$ -модуль изоморфен либо  $\mathbb{Z}$ , либо  $\mathbb{Z}/m\mathbb{Z}$ .

Пусть  $M$  — произвольный  $A$ -модуль. Рассмотрим множество

$$\text{Ann } M = \{a \in A \mid am = 0 \quad \forall m \in M\} \subset A.$$

Оно называется *аннулятором* модуля  $M$ . Ясно, что  $\text{Ann } M$  — идеал в  $A$ .

Нетрудно видеть, что имеется биекция между циклическими  $A$ -модулями и идеалами в  $A$ :

ТЕОРЕМА 13.21. Всякий циклический  $A$ -модуль  $M$  изоморфен  $A/I$ , где  $I$  — идеал в  $A$ , причем  $I = \text{Ann } M$ .

ДОКАЗАТЕЛЬСТВО. Ясно, что если  $I$  — идеал в  $A$ , то  $A/I$  — циклический модуль. Докажем обратное: пусть  $M = \langle x \rangle$  — циклический модуль. Рассмотрим гомоморфизм  $A$ -модулей

$$f: A \rightarrow M, \quad a \mapsto ax.$$

Ясно, что  $f$  сюръективен, и  $\text{Ker } f = \text{Ann } M$ . Но по теореме о гомоморфизме  $M \cong A/\text{Ker } f$ .  $\square$

**13.4. Базис. Свободные модули.** Как и в случае векторных пространств, для модулей имеют смысл понятия линейной зависимости и базиса.

**ОПРЕДЕЛЕНИЕ 13.22.** Элементы  $x_1, \dots, x_n \in M$  называются *линейно независимыми*, если для любых  $a_1, \dots, a_n \in A$ , не равных нулю одновременно,  $a_1x_1 + \dots + a_nx_n \neq 0$ . Линейно независимая система порождающих  $A$ -модуля  $M$  называется его *базисом*.

В отличие от векторных пространств, не у всякого модуля имеется базис. Так, например, в  $\mathbb{Z}/(m)$  базиса нет — поскольку даже всякая система из *одного* элемента оказывается линейно зависимой (поскольку  $mx = 0$  для любого  $x \in \mathbb{Z}/(m)$ ).

**ОПРЕДЕЛЕНИЕ 13.23.** Конечно порождённый модуль, обладающий базисом, называется *свободным*.

Скажем, всякий свободный циклический модуль изоморфен  $A$ .

Далее мы будем считать, что  $A$  — кольцо главных идеалов.

**ТЕОРЕМА 13.24.** Все базисы свободного  $A$ -модуля  $L$  содержат одинаковое число элементов.

**ДОКАЗАТЕЛЬСТВО.** Если  $A = \mathbb{K}$  — поле, то это просто теорема о размерности векторного пространства.

Пусть теперь  $A$  — не поле. Выберем в нём произвольный простой элемент  $p \in A$ . Мы знаем, что  $A/(p)$  — поле.

Рассмотрим в модуле  $L$  подмодуль  $pL$ , полученный как образ гомоморфизма  $\mu_p: x \mapsto px$ . В фактормодуле  $L/pL$  идеал  $(p) \subset A$  действует нулём, поэтому  $L/pL$  является векторным пространством над  $A/(p)$  (продумайте этот момент!).

Если  $e_1, \dots, e_n$  — базис в  $L$ , то классы базисных элементов  $[e_1], \dots, [e_n]$  будут образовывать базис в  $L/pL$  как в модуле над  $A/(p)$  — то есть как в векторном пространстве. А, как известно, все базисы векторного пространства состоят из одинакового числа элементов.  $\square$

**ОПРЕДЕЛЕНИЕ 13.25.** Число элементов в базисе свободного модуля называется его *рангом*.

**УПРАЖНЕНИЕ 13.26.** Докажите предыдущую теорему для произвольного целостного кольца  $A$  (не обязательно являющегося кольцом главных идеалов).

В силу предыдущей теоремы это определение корректно.

Всякий свободный модуль  $L$  изоморфен  $A^{\oplus r}$ , где  $r$  — ранг  $L$ . Изоморфизм, как и в случае векторных пространств, определяется выбором базиса в  $L$ .

Мы видели, что подгруппа свободной абелевой группы свободна. Для модулей над кольцами главных идеалов аналогичный факт тоже верен — причем доказательство его практически такое же, как для абелевых групп.

**ТЕОРЕМА 13.27.** Пусть  $N \subset A^{\oplus r}$  — подмодуль свободного модуля над кольцом главных идеалов  $A$ . Тогда  $N$  — свободный модуль, ранг которого не превосходит  $r$ .

**ДОКАЗАТЕЛЬСТВО.** Докажем эту теорему индукцией по  $r$ . База: если  $r = 1$ , то подмодуль  $N$  в  $A$  — это идеал. Но, поскольку все идеалы в  $A$  главные,  $N = (x) \cong A$ , если  $x \neq 0$ , или  $N = 0$ .

**Переход.** Пусть утверждение доказано для свободных модулей ранга меньше  $r$ . Рассмотрим множество всевозможных первых координат элементов из  $N$ :

$$I = \{x_1 \in A \mid (x_1, \dots, x_r) \in N\}.$$

Тогда  $I$  — идеал в  $A$ . Если  $I = 0$ , то  $N$  лежит в  $A^{\oplus r-1}$ , так что утверждение следует из предположения индукции. Если же этот идеал нетривиален, то он порожден некоторым элементом  $x \in A$ , и найдется такой элемент  $n \in N$ , у которого первая координата равна  $x$ .

Рассмотрим подмодуль  $N' \subset N$ , образованный всеми элементами из  $N$ , первая координата у которых равна нулю. По предположению индукции,  $N'$  свободен, и его ранг не превосходит  $r - 1$ . Но  $N = \langle x \rangle \oplus N' \cong A \oplus N'$ , откуда  $N$  также свободен ранга не выше  $(r - 1) + 1 = r$ .  $\square$

Здесь условие, что кольцо  $A$  является кольцом главных идеалов, уже оказывается существенным.

УПРАЖНЕНИЕ 13.28. Покажите, что идеал  $\mathbb{K}[x, y]_+ \subset \mathbb{K}[x, y]$ , образованный многочленами от двух переменных без свободного члена, не является свободным  $\mathbb{K}[x, y]$ -модулем.

*E-mail address:* `esmirnov@hse.ru`