R-модули

Пусть R – кольцо, A – абелева группа. Тогда левым R-модулем назовем A, если $R \times A \to A :$ $(r, a) \to ra$

1. $1a = a$
2. $(r_1 r_2)a = r_1(r_2 a)$
3. $r(a_1 + a_2) = ra_1 + ra_2$
4. $(r_1 + r_2)a = r_1 a + r_2 a$

Вообще говоря *левым* здесь имеет значения, потому что ввести *правое* бесплатно ($(r, a) \mapsto$ (a, r)) нельзя, ведь кольцо необязательно коммутативно. В ином случае почему бы и нет.

G-модули

Введем понятие и для группы. G – группа, $\mathbb{Z}[G]$ – групповое кольцо (см. 2-ую лекцию). Тогда если A – абелева группа – $\mathbb{Z}[G]$-модуль, она G-модуль.

Утверждение. $G \times A \to A$ – действие, такое, что $(g, a) \mapsto ga \Leftrightarrow \mathbb{Z}[G] \times A \to A$, такое, что $(\sum n_i g_i, a) \mapsto \sum n_i (g_i a)$ – задает структуру $Z[G]$-модуля.

Упражнение. Если A – $\mathbb{Z}$-модуль, то умножение это либо $a + \ldots + a$ (n раз), либо $-(a + \ldots + a)$.

Локализации

Еще хорошим примером модулей являются модули локализаций. Локализация:

$$\mathbb{Z}[1/m] = \{a/m^n \mid a \in \mathbb{Z}, n \in \mathbb{Z}\}$$

операции все как с дробями. Ну и на самом деле $\mathbb{Z}[1/m] \subset \mathbb{Q}$.

Собственно, $\mathbb{Z}[1/m]$-модуль дает нам m-делимую абелеву группу (то есть $\forall a : \exists (a/m) :$ $m(a/m) = a$).

Свободные модули

A – R-модуль свободный, если существует ЛНЗ генераторы $\{e_i\}$ – базис.

Пример несвободного модуля: $\mathbb{Z}$ – $\mathbb{Z}_2$-модуль. Вообще говоря он либо тривиален, либо просто смена знака. Проверить, что смена знака не имеет базиса – упражнение.

Еще раз, формально, смена знака – это

$$\mathbb{Z}_2 = \{1, z\}, 1a = a, za = -a$$

Прямая сумма и тензорное умножение

Сначала зададим прямую сумму. Пусть A, B – левые R-модули.

$$A \oplus B = A \times B : r(a, b) = (ra, rb)$$

Кстати, если A – свободный, то он разбивается в прямую сумму $\mathbb{Z}$.

Теперь тензорное умножение. Если A – правый модуль, B – левый, то рассмотрим пары из $A \times B$:

$$\begin{cases} (m, n) + (m', n) \sim (m + m', n) \\ (m, n) + (m, n') \sim (m, n + n') \\ (mr, b) \sim (m, rb) \end{cases}$$

тогда $(a, b) \in A \times B \mapsto$ класс эквивалентности $\equiv a \otimes b$.

Примеры и упражнения

1. $R = \mathbb{Z}, A = B = \mathbb{Z}$ – что такое $\mathbb{Z} \otimes \mathbb{Z}$? Ну $\mathbb{Z} \times \mathbb{Z} \ni (m, n) \sim (mn, 1)$. Соответственно, проверить строго $\mathbb{Z} \otimes \mathbb{Z} \cong \mathbb{Z}$ – упражнение.

Вообще $\mathbb{Z}$ – довольно простая структура, но в теории чисел, в топологии – все очень сложно.

2. R – коммутативное кольцо, $A = B = \mathbb{Z} \Rightarrow R \otimes R \cong R$.

3. $R, A = R, B$ – R-модуль $\Rightarrow R \otimes B \cong B : (r, b) \sim (1, rb) \mapsto rb$.

Последний пункт особенно важен, ведь получается, что R – единица в кольце модулей с операциями прямой суммы и тензорного произведения (?).

Поля

Чем они особенны? Ну A – K-векторное пространство (модуль над полем), K – поле, тогда если A – конечно порождено (то есть существует конечный набор генераторов), то существует базис (оно свободно как K – модуль).

Индуктивное доказательство довольно несложно, приведем лишь базу:

$$\text{пусть } A \text{ – однопорождено: } \exists e : \forall x \in A : x = ce, c \in K \Rightarrow A \cong K$$

Конечная последовательность

Хороший пример бесконечнопорожденного модуля.

$$\ell_{\text{fin}} = \left\{ (a_i)_{\{i=1\}}^{\infty} \mid \exists k : \forall i \geq k : a_i = 0 \right\}$$

Очевидный базис: $(1, 0, 0, \ldots), (0, 1, 0, \ldots), (0, 0, 1, \ldots), \ldots$

Вспомнили дуальные пространства, упражнение:

$$(\ell_{\text{fin}})^* \cong \ell$$

Еще примеры бесконечнопорожденных:

1. $C_{A(\mathbb{R})}$ – Тейлоровы приближения (базис)
2. $L_2(\mathbb{R})$ – ряды Фурье (базис)

Дальше

- Рассмотрим утверждения
  1. В векторном пространстве есть базис
  2. Лемма Цорна (привет матлогу)
- Посчитаем порядок $GL_n(\mathbb{F})$ с помощью линейной алгебры
- Показать, что если порядок поля конечен, то он степень простого – уходит в упражнения