Модули над кольцом

Если в определении векторного пространства заменить поле на произвольное кольцо, получится определение модуля.

Определение 1. *Модулем* над кольцом A (или A-модулем) называется абелева группа M вместе с операцией умножения $A \times M \to M$, удовлетворяющей свойствам:

1. $(a+b) \cdot m = a \cdot m + b \cdot m$;
2. $a \cdot (m_1 + m_2) = a \cdot m_1 + a \cdot m_2$;
3. $a \cdot (b \cdot m) = ab \cdot m$;
4. $1 \cdot m = m$.

Если A – поле, то модули обычно называются векторными пространствами. В этом случае в любом модуле есть базис и модуль задаётся с точностью до изоморфизма количеством элементов (мощностью) этого базиса. Для произвольных колец, однако, всё намного сложнее.

Для всякого модуля $0 \cdot m = 0$ и для образа натурального числа n в кольце A имеем $n \cdot m = m + \ldots + m$ (n слагаемых). Поэтому $\mathbb{Z}$-модуль – то же, что и просто абелева группа, произвола в выборе умножения нет.

Задача 1. Покажите, что $\mathbb{Z}/m\mathbb{Z}$-модули взаимно-однозначно соответствуют абелевым группам M, для которых $m \cdot M = 0$.

Пример 2.

1. A и 0 – A-модули.
2. Любой идеал в A – модуль над A.
3. Если $I \subset A$ – идеал, то A/I – A-модуль с умножением $a \cdot [b] = [ab]$.
4. Модуль над $\mathbb{Z}[x]$ – то же, что и абелева группа M с гомоморфизмом $x \colon M \to M$.
5. $\mathbb{C}[x_1, x_2, x_3]$-модуль – то же, что и векторное пространство над $\mathbb{C}$ с тремя коммутирующими линейными операторами.

Определение 3. *Подмодулем* модуля M назыается такая его подгруппа по сложению $M' \subset M$, что $a \cdot M' \subset M'$ для любого $a \in A$.

Очевидно, подмодули в A-модуле A – то же, что и идеалы.

Так же, как и идеалы, подмодули можно порождать семейством элементов модуля.

Определение 4. Пусть $X \subset M$ – подмножество в модуле. Подмодуль, *порождённый* множеством X, можно определить тремя равносильными способами:

1. как наименьший по вложению подмодуль M, содержащий X.
2. как пересечение всех подмодулей M, содержащих X.
3. как множество конечных сумм вида $\sum a_x x$, $a_x \in A$.

Подмодуль, порождённый множеством элементов $m_1, \ldots, m_n$, обозначают $\langle m_1, \ldots, m_n \rangle$.

Определение 5. Модуль, порождённый одним элементом, называется *циклическим*. Модуль, не имеющий нетривиальных подмодулей, называется *простым*.

Задача 2. Покажите, что a) A-модуль циклический $\iff$ имеет вид A/I, где I – идеал; b) A-модуль простой $\iff$ имеет вид A/I, где I – максимальный идеал.

Определение 6. Отображение A-модулей $f\colon M \to N$ называется *гомоморфизмом*, если $f(m_1+m_2) = f(m_1)+f(m_2)$ при всех $m_1, m_2 \in M$ и $f(am) = af(m)$ при всех $a \in A, m \in M$. Гомоморфизм называется *изоморфизмом*, если для него существует обратный гомоморфизм. Модули называются *изоморфными*, если между ними существует изоморфизм. Множество гомоморфизмов из M в N над A обозначается $\mathrm{Hom}_A(M, N)$.

Пример 7. Пусть в кольце A нет делителей нуля. Тогда любой главный идеал изоморфен A как модуль. Изоморфизм $A \to (a)$ задаётся формулой $x \mapsto xa$. Таким образом, разные идеалы (с неизоморфными факторкольцами) оказываются изоморфными как модули.

Задача 3. Приведите пример кольца A и идеалов I_1, I_2 таких, что кольца A/I_1 и A/I_2 изоморфны, а A-модули A/I_1 и A/I_2 не изоморфны.
Задача 4. Докажите, что a) $\mathrm{Hom}_A(A/I, A/I) \cong A/I$; b) $\mathrm{Hom}_A(A/I, A/J) \cong A/J$ при $I \subset J$; c) $\mathrm{Hom}_A(A/I, M) \cong \{m \in M \mid I \cdot m = 0\}$.

Замечание 8. Множество $\mathrm{Hom}_A(M, N)$ естественным образом является A-модулем: для $f, g \in \mathrm{Hom}_A(M, N)$ и $a \in A$ положим $(f + g)(m) = f(m) + g(m)$ и $(af)(m) = a \cdot f(m)$. Изоморфизмы из задачи 4 правильно понимать именно как изоморфизмы модулей, а не просто множеств.

Определение 9. *Прямой суммой* A-модулей M и N называется прямое произведение множеств $M \times N$, снабжённое покомпонентными операциями сложения и умножения на элементы A. Также оно называется прямым произведением. Обозначение: $M \oplus N, M \times N$.

Замечание 10. Заметим, что имеются естественные биекции

$$\mathrm{Hom}(T, M \times N) = \mathrm{Hom}(T, M) \times \mathrm{Hom}(T, N), \qquad \mathrm{Hom}(M \oplus N, T) = \mathrm{Hom}(M, T) \times \mathrm{Hom}(N, T)$$

для любого A-модуля T. Действительно, задать гомоморфизм из T во множество пар – всё равно, что задать по гомоморфизму в M и в N. А задать гомоморфизм из $M \oplus N$ в T – всё равно, что задать его на подмножествах $M \oplus 0$ и $0 \oplus N \subset M \oplus N$.

Эти свойства однозначно характеризуют прямую сумму и прямое произведение, в том числе, для произвольного семейства модулей.

Определение 11. *Прямым произведением* семейства A-модулей $M_i, i \in I$, называется множество $\prod_i M_i$ с покомпонентыми операциями. *Прямой суммой* семейства A-модулей $M_i, i \in I$, называется подмножество $\oplus_i M_i$ прямого произведения, состоящее из конечных наборов.

Замечание 12. Имеются естественные биекции

$$\mathrm{Hom}(T, \prod M_i) = \prod \mathrm{Hom}(T, M_i), \qquad \mathrm{Hom}(\oplus M_i, T) = \prod \mathrm{Hom}(M_i, T)$$

для любого A-модуля T.

Полезно убедиться, что замена прямых произведения и суммы модулей друг на друга в этих свойствах приводит к их нарушению.

Определение 13. *Свободным модулем* над A называется любая прямая сумма модулей, изоморфных A. Если эта сумма конечна, то число слагаемых называется *рангом* свободного модуля.

Пример 14. Модуль $\mathbb{Z}/m\mathbb{Z}$ над $\mathbb{Z}$, очевидно, не свободный: в нём есть делители нуля, а в свободном модуле их нет. Приведём также пример несвободного модуля без делителей нуля. Это идеал (x, y) в $\mathbb{C}[x, y]$. Он не может быть порождён одним многочленом, так как x и y не имеют общих нетривиальных делителей. С другой стороны, на любые два многочлена из (x, y) есть соотношение линейной зависимости с коэффициентами из $\mathbb{C}[x, y]$, поэтому идеал (x, y) не может быть свободным модулем ранга более одного.

Определение 15. *Суммой* двух подмодулей $M_1, M_2 \subset M$ называется наименьший подмодуль M, содержащий M_1 и M_2. Это множество всевозможных сумм $m_1 + m_2$, где $m_i \in M_i$.

Также подмодули фиксированного модуля можно пересекать – очевидно, пересечение снова будет подмодулем.

Задача 5. Пусть $M_1, M_2 \subset M$ – подмодули. Проверьте, что гомоморфизм $M_1 \oplus M_2 \to M$, заданный формулой $(m_1, m_2) \mapsto m_1 + m_2$, является изоморфизмом $\iff$ $M_1 \cap M_2 = 0$, $M_1 + M_2 = M$.

Если это так, говорят, что M *раскладывается в прямую сумму* своих подмодулей M_1 и M_2.

Определение 16. *Ядром* гомоморфизма модулей $f\colon M \to N$ называется множество $\ker f = \{m \in M \mid f(m) = 0\}$.

Несложно видеть, что ядро гомоморфизма – подмодуль в M. Также подмодулем в N будет образ гомоморфизма, обозначаемый $\operatorname{im} f$. Как и в случае гомоморфизмов колец, гомоморфизм f инъективный $\iff$ $\ker f = 0$.

Определение 17. Пусть $M' \subset M$ – подмодуль. *Фактормодулем* M по M' называется множество M/M' классов эквивалентности M по отношению эквивалентности: $m_1 \equiv m_2 \iff m_1 - m_2 \in M'$. На M/M' вводятся сложение и умножение по правилам $[m_1] + [m_2] = [m_1 + m_2]$, $a \cdot [m] = [am]$. Это превращает M/M' в A-модуль. Естественное отображение $\pi\colon M \to M/M'$ – гомоморфизм, его ядро – M'.

Предложение 18. *Если $M' \subset M$ – подмодуль, то имеется биекция между подмодулями в M, содержащими M', и подмодулями в M/M'.*

Доказательство. Биекция из правой части в левую задаётся формулой $N \mapsto \pi^{-1}(N)$, где $N \subset M/M'$, $M' \subset \pi^{-1}(N) \subset M$. □

Основное свойство фактормодулей – следующее

Предложение 19. *Пусть $M' \subset M$ – подмодуль, а $f\colon M \to N$ – гомоморфизм такой, что $f(M') = 0$. Тогда существует единственный гомоморфизм $f'\colon M/M' \to N$, для которого $f = f'\pi$.*

Доказательство. Если f' существует, то $f(m) = f'\pi(m) = f'([m])$ при всех m, и это однозначно определяет f'. Обратно, определим f' формулой $f'([m]) = f(m)$. Это корректное определение: если классы $[m_1]$ и $[m_2]$ равны, то $m_1 - m_2 \in M'$ и поэтому $f(m_1) - f(m_2) = f(m_1 - m_2) = 0$ по условию. Ясно, что такой f' будет искомым гомоморфизмом. □

Следствие 20 (теорема о гомоморфизме)**.** *Если $f\colon M \to N$ – гомоморфизм модулей, то $\operatorname{im} f \cong M/\ker f$.*

При помощи теоремы о гомоморфизме удобно доказывать свойства, подобные приведённым ниже.

Предложение 21. *Пусть $M_1, M_2 \subset M$ – подмодули. Тогда*

$$(M_1 + M_2)/M_2 \cong M_1/(M_1 \cap M_2).$$

Доказательство. Рассмотрим композицию гомоморфизмов

$$M_1 \to M_1 + M_2 \xrightarrow{\pi} (M_1 + M_2)/M_2$$

(первая стрелка обозначает вложение). Она сюръективна, а её ядро – пересечение $M_1 \cap M_2$. Применяя теорему о гомоморфизме, получаем требуемое. □

Задача 6. Покажите, что для $K \subset L \subset M$ верно $M/L \cong (M/K)/(L/K)$.

Определение 22. *Аннулятором* модуля M над A называется множество элементов $a \in A$ таких, что $a \cdot M = 0$.

Как нетрудно видеть, аннулятор модуля – это идеал.

Для подмодулей $K, L \subset M$ обозначим

$$(K : L) = \{a \in A \mid a \cdot L \subset K\}.$$

Задача 7. a) Покажите, что $(K : L)$ – идеал; b) Найдите $(K : L)$ для $K = (k), L = (l)$ – идеалов в $\mathbb{Z}$.

Задача 8. Проверьте, что a) $\operatorname{Ann}(M_1 + M_2) = \operatorname{Ann}(M_1) \cap \operatorname{Ann}(M_2)$; b) $\operatorname{Ann}((M_1 + M_2)/M_2) = (M_2 : M_1)$.

Наконец, определим тензорное произведение модулей. Пусть A – коммутативное кольцо с единицей, M и N – модули над A.

Определение 23. Рассмотрим свободный A-модуль F с базисом $e_{m,n}$, где m и n пробегают все элементы M и N соответственно. Рассмотрим подмодуль

$$F' = \left\langle \begin{matrix} e_{m_1+m_2,n} - e_{m_1,n} - e_{m_2,n} \\ e_{m,n_1+n_2} - e_{m,n_1} - e_{m,n_2} \\ e_{am,n} - ae_{m,n} \\ e_{m,an} - ae_{m,n} \end{matrix} \right\rangle \subset F,$$

порождённый указанными выражениями, где $m_1, m_2 \in M, n_1, n_2 \in N, a \in A$ – всевозможные элементы. Определим $M \otimes_A N$ как фактормодуль F/F'.

Образ элемента $e_{m,n}$ при канонической проекции $F \to M \otimes_A N$ обозначается $m \otimes n$. Элементы вида $m \otimes n$ порождают тензорное произведение как модуль. Для них выполнены следующие соотношения

$$\begin{gathered} (m_1 + m_2) \otimes n = m_1 \otimes n + m_2 \otimes n \\ m \otimes (n_1 + n_2) = m \otimes n_1 + m \otimes n_2 \\ (am) \otimes n = a \cdot m \otimes n \\ m \otimes (an) = a \cdot m \otimes n \end{gathered}$$

Используя эти соотношения при раскрытии скобок, можно показать следующее:

Предложение 24. *Если элементы $m_1, m_2, \ldots$ порождают M, а $n_1, n_2, \ldots$ порождают N, то произведения $m_i \otimes n_j$ порождают $M \otimes N$.*

С данным выше определением никогда не работают напрямую. Вместо этого используют свойство универсальности тензорного произведения,

Пусть M, N, K – модули над A. Отображение $f\colon M \times N \to K$ называется *билинейным*, если $\forall m \in M$ отображение $f(m, -)\colon N \to K$ – гомоморфизм и $\forall n \in N$ отображение $f(-, n)\colon M \to K$ – гомоморфизм.

Примеры:

1. умножение $A \times A \to A$;

2. отображение $\tau\colon M \times N \to M \otimes_A N$, переводящее пару (m, n) в $m \otimes n$.

Любое билинейное отображение единственным образом пропускается через тензорное произведение:

Предложение 25. *Билинейное отображение $\tau\colon M \times N \to M \otimes N$ является* универсальным*, то есть для любого билинейного отображения $f\colon M \times N \to K$ существует и единственен гомоморфизм $\widetilde{f}\colon M \otimes N \to K$ такой, что $\widetilde{f}\tau = f$.*

Доказательство. Если $\widetilde{f}$ существует, то он единствен. Действительно, $\widetilde{f}(m \otimes n) = \widetilde{f}\tau(m, n) = f(m, n)$, а элементы $m \otimes n$ порождают $M \otimes N$. Чтобы доказать существование, рассмотрим гомоморфизм $f'\colon F \to K$, переводящий $e_{m,n}$ в $f(m, n)$. Так как $e_{m,n}$ образуют базис свободного модуля A, такой гомоморфизм существует. Заметим, что $f' = 0$ на всех элементах, порождающих подмодуль F'. Например, $f'(e_{m_1+m_2,n} - e_{m_1,n} - e_{m_2,n}) = f(m_1 + m_2, n) - f(m_1, n) - f(m_2, n) = 0$ по билинейности f. Значит, $f' = 0$ на F' и по предложению 19 гомоморфизм f' пропускается через гомоморфизм $\widetilde{f}\colon F/F' = M \otimes N \to K$. Имеем $\widetilde{f}(m \otimes n) = f'(e_{m,n}) = f(m, n)$, значит $\widetilde{f}$ искомый. □