Модули над областями главных идеалов

Определение 1. Пусть R — ассоциативное кольцо с единицей. Абелева группа M вместе с операцией $\cdot R \times M \to M$ называется левым R-модулем , если Ассоциативность для умножения
1) $\forall a \in M$, $\forall r, s \in R$ выполнено $r \cdot (s \cdot a) = (rs) \cdot a$
Дистрибутивность
2) $\forall a, b \in M$, $\forall r \in R$ выполнено $r \cdot (a + b) = r \cdot a + r \cdot b$
3) $\forall a \in M$, $\forall r, s \in R$ выполнено $(r + s) \cdot b = r \cdot b + s \cdot b$ очень хочется, чтобы единичка действовала как тождественное отображение
4) $\forall a \in M$ выполнено $1 \cdot a = a$.

Определение 2. Пусть R — ассоциативное кольцо с единицей, а M, N — левые R-модули. Гомоморфизмом левых R-модулей называется гомоморфизм абелевых групп $f\colon M \to N$ удовлетворяющий свойству $f(ra) = rf(a)$ для любого $r \in R$ и любого $a \in M$.

Определение 3. Пусть R — ассоциативное кольцо с единицей, а M, – левый R-модули. Подгруппа $N \leq M$ называется подмодулем, если $\forall r \in R$ $\forall n \in N$ верно, что $rn \in N$.

В случае коммутативных колец принято говорить просто про модули, так как по левому модулю автоматически можно получить правый модуль ($m * r := r \cdot m$).

Примеры:

1) Абелева группа M единственным образом снабжается структурой $\mathbb{Z}$ модуля.
2) Пусть R — коммутативное кольцо. Задать структуру $R[t]$-модуля на M эквивалентно заданию структуры R-модуля и гомоморфизма модулей $L\colon M \to M$. В частности, если $R = K$ — поле, то $K[t]$ модули это операторы на векторных пространствах над K.
3) Над произвольным ассоциативным кольцом с единицей R есть левый модуль R. Такой модуль иногда называют регулярным или свободным модулем ранга 1.
4) Пусть N и M — левые R-модули, тогда $N \oplus M$ снабжается естественной структурой левого R-модуля.
5) Пусть задано множество индексов I и для каждого $i \in I$ задан левый модуль M_i. Тогда прямой суммой семейства M_i называется подмодуль в прямом произведении $\prod_{i \in I} M_i$ (домножение покомпонентное)

$$\bigoplus_{i \in I} M_i = \{\{u_i\}_{i \in I} \,|\, u_i \in M_i, \text{ где все кроме конечного числа } u_i \text{ равны } 0\ \}\,.$$

6) Пусть I — множество индексов. Модуль $R^{\oplus I} = \bigoplus_{i \in I} R$ называется свободным модулем ранга $|I|$ (все изоморфные таким тоже называют свободными). Для конечного множества индексов это определение совпадает с прямым произведением.
7) Пусть $N \leq M$ подмодуль. Тогда фактор M/N единственным образом снабжается структурой левого R-модуля.
8) Левые идеалы внутри кольца R однозначно соответствуют подмодулям R, как левого модуля над собой.
9) Пусть $I \leq R$ — левый идеал. Тогда модуль R/I называется циклическим.

В дальнейшем все модули будут левыми.

Определение 4. Пусть M — R-модуль. Будем говорить, что подмножество $X \subseteq M$ порождает подмодуль $\langle X \rangle = \{u \in M \,|\, u = \sum r_i x_i\}$.

Теорема 1. *Пусть M модуль над R. Тогда для всякого множества I имеет место соответствие:*

$$\mathrm{Hom}(R^I, M) \cong \{\{u_i\}_{i \in I} \,|\, u_i \in M\}$$

Иными словами гомоморфизм однозначно задаётся образами стандартных базисных.

Следствие 1. *Любой модуль есть фактор какого-то свободного (надо воспользоваться первой теоремой о гомоморфизме).*

Определение 5. Базисом модуля M называется набор $\{v_i\}_{i\in I}$, что для любого $v \in M$ $\exists r_i \in R$, что $v = \sum r_i v_i$, причём все, кроме конечного числа $v_i = 0$ (т.е. сумма конечная).

Следствие 2. *Выбор базиса задаёт изоморфизм со свободным модулем и наоборот, изоморфизм со свободным модулем задаёт базис. Модули довольно редко имеют базис и бывают свободными...*

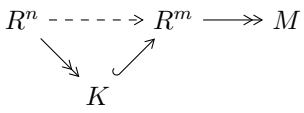
Определение 6. Модуль M называется конечно порождённым, если существует конечное $X \subseteq M$ $\langle X\rangle = M$. Эквивалентно, если существует сюръективный гомоморфизм $R^n \to M$

Определение 7. Кольцо R называется нётеровым, если любой подмодуль конечно порождённого модуля конечно порождён.

Для коммутативных колец верно следующее:

Теорема 2. *Область главных идеалов нётерова. Кольцо многочленов от n переменных над нётеровым кольцом нётерово. Фактор нётерого кольца по любому идеалу — нётерово кольцо.*

Рассмотрим конечно порождённый модуль M над кольцом R. Тогда есть сюръективное отображение $f\colon R^m \to M$. Пусть K – ядро f (этот подмодуль R^m называется модулем соотношений, подумайте почему). Тогда, если кольцо R нётерово, то K — конечно порожден и есть отображение $R^n \to K$. Имеем:



Таким образом классификация модулей с точностью до изоморфизма приводит к классификации отображений из $R^n \to R^m$, то есть матриц. Теперь докажем основную лемму.

Лемма 1. Пусть R — область главных идеалов. Тогда для любой матрицы $A \in M_{n\times m}(R)$ существуют матрицы $B \in GL_n(R)$ и $C \in GL_m(R)$, что

$$BAC = \begin{pmatrix} \varepsilon_1 & & & & & \\ & \ddots & & & & \\ & & \varepsilon_l & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

При этом можно добиться, чтобы $\varepsilon_{i+1} \vdots \varepsilon_i$.

Доказательство. Найдём такие матрицы B и C, что у матрицы BAC в левом верхнем углу будет стоять наибольший общий делитель всех элементов из первой строки и первого столбца. Рассмотрим первые два элемента $a = a_{11}$ $b = a_{21}$. Пусть $d = \text{НОД}(a, b)$. Тогда существуют x и y из R, что $ax + by = d$. Тогда матрица

$$B = \begin{pmatrix} x & y & & & \\ -\frac{b}{d} & \frac{a}{d} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix}$$

обратима и

$$BA = \begin{pmatrix} x & y & & & \\ -\frac{b}{d} & \frac{a}{d} & & & \\ & & 1 & & \\ & & & \ddots & \\ & & & & 1 \end{pmatrix} \begin{pmatrix} a & * & \dots & * \\ b & * & \dots & * \\ * & & & * \\ \vdots & & & \vdots \\ * & * & \dots & * \end{pmatrix} = \begin{pmatrix} \text{НОД}(a,b) & * & \dots & * \\ * & * & \dots & * \\ * & & & * \\ \vdots & & & \vdots \\ * & * & \dots & * \end{pmatrix}.$$

Домножая на аналогичные матрицы справа и слева получим требуемое. Дальше — вычтем все из всех строк первую строку, так чтобы коэффициент в столбце был равен нулю. Аналогично по столбцу. Далее — индукция. □

Теорема. Пусть R — кольцо главных идеалов. Тогда для любого гомоморфизма $f\colon R^m \to R^n$ существует базисы $v_1, \dots, v_n$ $u_1, \dots, u_m$, что матрица отображения в этом базисе имеет вид

$$\begin{pmatrix} \varepsilon_1 & & & & & \\ & \ddots & & & & \\ & & \varepsilon_l & & & \\ & & & 0 & & \\ & & & & \ddots & \\ & & & & & 0 \end{pmatrix}.$$

В частности, так как любой подмодуль свободного модуля есть образ какого-то такого отображения, то подмодуль свободного модуля свободен.

Теорема. Пусть R — кольцо главных идеалов, а M — конечно порождённый модуль над R. Тогда модуль M имеет вид

$$M = \bigoplus_{i=1}^{r} R/(\varepsilon_i) \oplus R^l$$

для некоторых $r, l \in \mathbb{N}$ и $\varepsilon_i \in R$, ε_i — степень какого-то неприводимого элемента.

Следствие 3. *Если $R = K[t]$, то получаем теорию про жорданову (или фробениусову, см. предыдущие ДЗ) форму. Если $R = \mathbb{Z}$, то получается теорема о классификации конечно порождённых абелевых групп.*

Задачи

Задача 1. Представьте в виде суммы циклических абелевых групп:

$$\mathbb{Z}^3/\langle v_1, v_2, v_3\rangle, \text{ где } v_1 = \begin{pmatrix}1\\4\\7\end{pmatrix}, v_2 = \begin{pmatrix}2\\5\\8\end{pmatrix}, v_3 = \begin{pmatrix}3\\6\\9\end{pmatrix}.$$

Задача 2. Пусть $L\colon \mathbb{Z}^n \to \mathbb{Z}^n$ — гомоморфизм абелевых групп. Пусть $A \in M_n(\mathbb{Z})$ — матрица L в стандартном базисе . Покажите, что

$$|\det A| = |\mathbb{Z}^n / L(\mathbb{Z}^n)|.$$

(Покажите, что модуль определителя не меняется при замене базиса с каждой стороны).

Задача 3. Представьте в виде суммы циклических, а так же найдите образующие (в виде классов смежности векторов в стандартном базисе) у абелевой группы.

$$\mathbb{Z}^3/\langle v_1, v_2, v_3\rangle, \text{ где } v_1 = \begin{pmatrix}7\\21\\5\end{pmatrix}, v_2 = \begin{pmatrix}2\\8\\4\end{pmatrix}, v_3 = \begin{pmatrix}3\\9\\3\end{pmatrix}.$$

Задача 4. Покажите, что любой вектор из $x \in \mathbb{Z}^n$, такой, что наибольший общий делитель его координат равен 1, может быть дополнен до базиса в $\mathbb{Z}^n$.

Задача 5. Пусть K — поле. Что такое модуль над $K[t_1, t_2]$ в терминах векторных пространств?