Глава V

Многочлены

§ 1. *Свободные алгебры*

Пусть A — коммутативное кольцо. *A-алгебра* (или алгебра над A) — это модуль E вместе с билинейным отображением $E \times E \to E$. *Во всей этой книге мы, если не оговорено противное, будем иметь дело только со следующим специальным типом алгебр.* Пусть $f\colon A \to B$ — гомоморфизм колец, такой, что $f(A)$ содержится в центре B, т. е. $f(a)$ коммутирует с любым элементом из B для всякого $a \in A$. Тогда мы можем рассматривать B как A-модуль, определив действие A на B посредством отображения

$$(a, b) \longmapsto f(a) b$$

для всех $a \in A$ и $b \in B$. Аксиомы модуля тривиальным образом удовлетворяются, и мультипликативный закон композиции $B \times B \to B$, очевидно, билинеен (т. е. A-билинеен). Так вот, если не оговорено противное, то под алгеброй над A мы будем всегда понимать указанный выше гомоморфизм колец. Мы говорим, что алгебра является *конечно порожденной*, если B как кольцо над $f(A)$ конечно порождено.

Пусть G — *мультипликативный* моноид и A — коммутативное кольцо. Пусть $\mathscr{C}$ — категория, объектами которой являются тройки (φ, f, B), где $f\colon A \to B$ есть A-алгебра и $\varphi\colon G \to B$ — гомоморфизм мультипликативных моноидов. Если (φ', f', B') — другой объект в $\mathscr{C}$, то морфизм из (φ, f, B) в (φ', f', B') в категории $\mathscr{C}$ — это кольцевой гомоморфизм $h\colon B \to B'$, для которого коммутативна следующая диаграмма:

$$\begin{tikzcd}
G \arrow[d, "\varphi"'] \arrow[dr, "\varphi'"] & \\
B \arrow[r, "h"] & B' \\
A \arrow[u, "f"] \arrow[ur, "f'"'] &
\end{tikzcd}$$

Универсальный (отталкивающий) объект в $\mathscr{C}$ называется *свободной (A, G)-алгеброй*, или *свободной G-алгеброй над A*. Построим такую алгебру в явном виде.

Пусть $A[G]$ — множество всех отображений $\alpha\colon G \to A$, таких, что $\alpha(x)=0$ для почти всех $x \in G$. Определяем сложение в $A[G]$ как обычное сложение отображений в абелеву (аддитивную) группу. Если $\alpha,\ \beta \in A[G]$, то их произведение $\alpha\beta$ определяем формулой

$$(\alpha\beta)(t) = \sum_{xy=t} \alpha(x)\beta(y).$$

Сумма берется по всем таким парам (x, y) с $x, y \in G$, что $xy=t$. Эта сумма в действительности конечна, поскольку имеется лишь конечное число пар элементов $(x, y) \in G \times G$, для которых $\alpha(x)\beta(y) \neq 0$. Мы видим также, что $(\alpha\beta)(t)=0$ для почти всех t и, следовательно, $\alpha\beta$ принадлежит нашему множеству $A[G]$.

Аксиомы кольца тривиально проверяются. В качестве примера приведем доказательство ассоциативности. Пусть $\alpha, \beta, \gamma \in A[G]$. Тогда

$$((\alpha\beta)\gamma)(t) = \sum_{xy=t} (\alpha\beta)(x)\gamma(y) = \sum_{xy=t}\left[\sum_{uv=x}\alpha(u)\beta(v)\right]\gamma(y) =$$
$$= \sum_{xy=t}\left[\sum_{uv=x}\alpha(u)\beta(v)\gamma(y)\right] = \sum_{\substack{(u,\, v,\, y)\\ uvy=t}} \alpha(u)\beta(v)\gamma(y),$$

причем последняя сумма берется по всем тройкам (u, v, y), произведение которых равно t. Эта последняя сумма симметрична, и если бы мы вычислили $(\alpha(\beta\gamma))(t)$, то получили бы снова эту сумму. Это доказывает ассоциативность.

Единичным элементом в $A[G]$ служит функция δ, такая, что $\delta(e)=1$ и $\delta(x)=0$ для всех $x \in G$, $x \neq e$. Тривиально проверяется, что $\alpha = \delta\alpha = \alpha\delta$ для всех $\alpha \in A[G]$.

Введем теперь другие обозначения, которые сделают структуру $A[G]$ более ясной. Пусть $a \in A$ и $x \in G$. Мы будем обозначать через $a \cdot x$ (а иногда также через ax) функцию, значение которой в x равно a, а в y равно 0, если $y \neq x$. Тогда любой элемент $\alpha \in A[G]$ может быть записан в виде суммы

$$\alpha = \sum_{x \in G} \alpha(x) \cdot x.$$

Действительно, если $\{a_x\}_{x \in G}$ — семейство элементов из A, почти все из которых равны 0, и мы положим

$$\beta = \sum_{x \in G} a_x \cdot x,$$

то для любого $y \in G$ будем иметь $\beta(y) = a_y$ (непосредственно из определений). Это также показывает, что любой данный элемент α допускает единственное представление в виде суммы $\sum a_x \cdot x$.

Имеется естественный способ превратить $A[G]$ в A-модуль. Если $a \in A$ и элемент $\alpha \in A[G]$ записан в виде суммы $\sum a_x \cdot x$, то полагаем $a\alpha$ равным элементу $\sum (aa_x) \cdot x$. Ясно, что все аксиомы модуля удовлетворяются и что множество элементов $\{1 \cdot x\}_{x \in G}$ образует базис $A[G]$ над A.

В наших нынешних обозначениях умножение и сложение могут быть записаны соответственно следующим образом:

$$\left(\sum_{x \in G} a_x \cdot x\right)\left(\sum_{y \in G} b_y \cdot y\right) = \sum_{x,\, y} a_x b_y \cdot xy,$$

$$\sum_{x \in G} a_x \cdot x + \sum_{x \in G} b_x \cdot x = \sum_{x \in G} (a_x + b_x) \cdot x$$

— именно так, как нам хотелось бы. Отметим, что единичный элемент в $A[G]$ — это просто $1 \cdot e$.

Пусть φ_0: $G \to A[G]$ — отображение, задаваемое формулой $\varphi_0(x) = 1 \cdot x$. Непосредственно проверяется, что отображение φ_0 — гомоморфизм мультипликативных моноидов и что оно на самом деле инъективно, т. е. является вложением.

Пусть f_0: $A \to A[G]$ — отображение, задаваемое формулой

$$f_0(a) = a \cdot e.$$

Непосредственно проверяется, что f_0 — гомоморфизм колец, также являющийся вложением. Таким образом, мы превратили $A[G]$ в A-алгебру, и сразу видно, что структура A-модуля на $A[G]$, как на A-алгебре, совпадает с той, которая была описана выше.

Тройка $(\varphi_0, f_0, A[G])$ *есть свободная* (A, G)*-алгебра. Это утверждение является частным случаем следующего предложения.*

Предложение 1. *Пусть* f_0: $A \to B$ — *некоторая* A*-алгебра и* G — *мультипликативный подмоноид в* B. *Предположим, что* G *образует базис для* B *как модуля над* A. *Для всякой* A*-алгебры* f: $A \to C$ *и любого гомоморфизма моноидов* φ: $G \to C$ *существует единственный гомоморфизм колец* h: $B \to C$, *для которого диаграмма*

$$\begin{tikzcd} B \arrow[r, "h"] & C \\ A \arrow[u, "f_0"] \arrow[ur, "f"'] & \end{tikzcd}$$

коммутативна и ограничение h *на* G *равно* φ.

Доказательство. Для каждых $x \in G$ и $a \in A$ пишем $a \cdot x$ вместо $f_0(a)x$. Всякий элемент $\alpha \in A[G]$ имеет единственное представление в виде суммы

$$\alpha = \sum_{x \in G} a_x \cdot x$$

с $a_x \in A$, поскольку G — базис для B над A. Как мы видели при рассмотрении базисов модулей, существует единственный гомоморфизм модулей $h\colon B \to C$, ограничение которого на G равно φ, а именно такое отображение, для которого

$$h(\alpha) = \sum_{x \in G} f(a_x)\,\varphi(x).$$

Кроме того, если

$$\beta = \sum_{y \in G} b_y \cdot y,$$

то

$$\alpha\beta = \sum_{z \in G} \left(\sum_{xy = z} a_x b_y \right) \cdot z$$

и

$$h(\alpha\beta) = \sum_{z \in G} f\left(\sum_{xy = z} a_x b_y \right) \varphi(z) = \sum_{z \in G} \left(\sum_{xy = z} f(a_x) f(b_y) \right) \varphi(z) = h(\alpha)\,h(\beta).$$

Так как ограничение на G отображения h равно φ, то $h(1) = 1$. Следовательно, h является также гомоморфизмом колец. Отсюда вытекает коммутативность нашей диаграммы. Предложение доказано.

Чтобы вывести из предложения 1, что $(\varphi_0, f_0, A[G])$ — свободная (A, G)-алгебра, надо положить $B = A[G]$ и отождествить G с его образом в $A[G]$ при вложении φ_0.

Начиная с этого момента мы будем, не опасаясь путаницы, писать ax вместо $a \cdot x$. Мы будет называть $A[G]$ *моноидной алгеброй моноида G над A*. Отображения φ_0, f_0 называются *каноническими*.

В следующем параграфе мы в качестве частного случая получим алгебру многочленов. Для случая когда G — группа, групповая алгебра $A[G]$ будет более детально рассмотрена в этой книге позднее.

Наша моноидная алгебра обладает еще одним свойством универсальности.

Предложение 2. *Пусть $\varphi\colon G \to G'$ — гомоморфизм моноидов и $f\colon A \to A'$ — гомоморфизм колец, причем оба кольца A, A' коммутативны. Тогда существует единственный гомоморфизм колец*

$$h\colon A[G] \to A'[G'],$$

для которого коммутативна диаграмма

$$\begin{tikzcd}
G \arrow[r, "\varphi"] \arrow[d] & G' \arrow[d, "\varphi_0'"] \\
A[G] \arrow[r, "h"] & A'[G'] \\
A \arrow[r, "f"'] \arrow[u] & A' \arrow[u, "f_0'"']
\end{tikzcd}$$

(*Вертикальные отображения — канонические.*)

Доказательство. Это прямое следствие предложения 1: положим $C = A'[G']$, рассмотрим гомоморфизмы

$$\varphi_0' \circ \varphi \quad \text{и} \quad f_0' \circ f$$

и применим к ним предложение 1.

§ 2. *Определение многочленов*

Пусть S — некоторое множество и $\mathbf{N}$ — аддитивный моноид целых чисел $\geqslant 0$ (т. е. моноид натуральных чисел). Обозначим через

$$\mathbf{N}\langle S\rangle$$

множество функций $S \to \mathbf{N}$, которые равны 0 для почти всех элементов из S. (Это по существу та же самая конструкция, которую мы применяли для получения свободных абелевых групп; в настоящем случае мы получаем свободный абелев моноид. Однако мы будем записывать его мультипликативно.) Пусть $x \in S$ и $i \in \mathbf{N}$; мы обозначаем через x^i функцию, которая принимает значение i в x и 0 в $y \neq x$. Если φ, ψ — две функции из $\mathbf{N}\langle S\rangle$, то их произведение $\varphi\psi$ определяется формулой

$$(\varphi\psi)(x) = \varphi(x) + \psi(x).$$

Тогда $\mathbf{N}\langle S\rangle$ будет мультипликативным моноидом, единичным элементом которого служит нулевая функция. Всякий элемент $\varphi \in \mathbf{N}\langle S\rangle$ имеет единственное представление в виде произведения

$$\prod_{x \in S} x^{\nu(x)},$$

где $\nu\colon S \to \mathbf{N}$ — отображение, для которого $\nu(x) = 0$ при почти всех x. Такое произведение будет называться *примитивным одночленом* и будет иногда обозначаться символом $M_{(\nu)}(S)$ или просто $M_{(\nu)}$.

Имеем вложение $j_S\colon S \to \mathbf{N}\langle S\rangle$ (задаваемое правилом $x \mapsto x^1$), образ которого порождает $\mathbf{N}\langle S\rangle$ как моноид. Отметим, что если n — целое число $\geqslant 0$, то элемент

$$(x^1)^n = x^1 x^1 \ldots x^1$$

равен x^n, т. е. наше обозначение согласуется с обозначением, используемым для произведения функций.

Заметим, что если

$$\prod_{x \in S} x^{\nu(x)} \quad \text{и} \quad \prod_{x \in S} x^{\mu(x)}$$

— примитивные одночлены, то их произведение равно

$$\prod_{x \in S} x^{\nu(x)+\mu(x)}.$$