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 ν: $S \to \mathbf{N}$ — 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: $S \to \mathbf{N}\langle S\rangle$ (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

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

Как и в случае абелевых групп, имеет место свойство универсальности. Именно, пусть G — коммутативный моноид. Для всякого данного отображения $\lambda\colon S \to G$ существует единственный гомоморфизм моноидов $\mathbf{N}\langle S\rangle \to G$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} S & \xrightarrow{\lambda} & G \\ & {\scriptstyle j_S}\searrow \quad \nearrow & \\ & \mathbf{N}\langle S\rangle & \end{array}$$

В частности, для всякого данного отображения $\lambda\colon S \to S'$ одного множества в другое существует гомоморфизм моноидов $\lambda_*\colon \mathbf{N}\langle S\rangle \to \mathbf{N}\langle S'\rangle$, для которого коммутативна следующая диаграмма:

$$\begin{array}{ccc} S & \xrightarrow{j_S} & \mathbf{N}\langle S\rangle \\ {\scriptstyle\lambda}\downarrow & & \downarrow{\scriptstyle\lambda_*} \\ S' & \xrightarrow[j_{S'}]{} & \mathbf{N}\langle S'\rangle, \end{array}$$

иными словами,

$$\lambda_*\Big[\prod_{x\in S} x^{\nu(x)}\Big] = \prod_{x\in S} \lambda(x)^{\nu(x)}.$$

Доказательство этого утверждения тривиально, как и в случае абелевых групп. Можно рассматривать $\mathbf{N}\langle S\rangle$ как функтор из категории множеств в категорию коммутативных моноидов.

Пусть A — коммутативное кольцо. Тогда можно образовать моноидную алгебру $A[\mathbf{N}\langle S\rangle]$ над A, которую мы будем называть *кольцом (или алгеброй) многочленов от S над A*. Для простоты мы будем обозначать это кольцо через $A[S]$. По определению всякий элемент из $A[S]$ имеет единственное представление в виде линейной комбинации

$$\sum_{(\nu)} a_{(\nu)} M_{(\nu)}(S) = \sum_{(\nu)} a_{(\nu)} \prod_{x\in S} x^{\nu(x)},$$

где (ν) пробегает все отображения множества S в $\mathbf{N}$, обращающиеся в 0 для почти всех x, и $a_{(\nu)}$ равно 0 для почти всех (ν). *Примитивные одночлены образуют базис алгебры $A[S]$ над A*, как было отмечено выше для моноидных алгебр. Элементы из $A[S]$ называются *многочленами от S над A*. Элементы $a_{(\nu)}$ называются *коэффициентами* многочлена.

Замечание об обозначениях. Пусть T — подмножество коммутативного кольца B и $\nu\colon T \to \mathbf{N}$ — отображение, для которого $\nu(x) = 0$ при почти всех $x \in T$. Мы будем через $M_{(\nu)}(T)$ обозначать также элемент

$$M_{(\nu)}(T) = \prod_{x\in T} x^{\nu(x)},$$

причем подразумевается, что это произведение берется по тем x, для которых $\nu(x) \neq 0$, и что пустое произведение есть единичный элемент в B. Никакой путаницы с обозначениями для одночленов не возникнет, так как из контекста всегда будет ясно, что мы имеем в виду.

Если S есть множество из n символов $X_1, \ldots, X_n$, то

$$A[S] = A[X_1, \ldots, X_n],$$

и мы будем говорить о кольце (или алгебре) многочленов от $X_1, \ldots, X_n$ над A. Мы иногда будем использовать векторное обозначение и писать $A[X]$ вместо $A[X_1, \ldots, X_n]$.

Всякий многочлен из $A[X]$ может быть однозначно записан в виде

$$\sum a_{(\nu)} M_{(\nu)}(X) = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n},$$

где сумма берется по всем наборам из n целых чисел $\nu_1, \ldots, \nu_n \geqslant 0$, причем почти все коэффициенты $a_{(\nu)}$ равны 0.

Пусть снова S — произвольное множество. Отметим, что и S, и A обладают каноническими инъективными отображениями в $A[S]$, задаваемыми соответствиями

$$x \longmapsto 1 \cdot x^1 \text{ и } a \longmapsto a \cdot \prod_{x \in S} x^0.$$

В действительности каноническое отображение A в $A[S]$ является кольцевым гомоморфизмом, именно вложением. Можно безболезненно отождествлять S и A с соответствующими образами в $A[S]$. Одночлен $\prod_{x \in S} x^0$, служащий единичным элементом в моноиде $\mathbf{N}\langle S\rangle$, обозначается также через 1, поскольку это не приводит ни к какой путанице. Таким образом, если S состоит из одного символа X, то всякий многочлен может быть записан в виде

$$a_0 X^0 + a_1 X^1 + \ldots + a_n X^n = a_0 + a_1 X + \ldots + a_n X^n,$$

где $a_\nu \in A$ и n — некоторое целое число $\geqslant 0$.

Пусть A, B — коммутативные кольца и $f_0\colon A \to B$ — некоторая A-алгебра. Пусть S — подмножество в B. Если семейство одночленов

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

линейно независимо над A, то мы будем говорить, что S *алгебраически независимо* над A, или что элементы из S алгебраически независимы над A. Можно было бы также рассмотреть занумерованное множество $S = \{x_i\}_{i \in I}$, образовать одночлены

$$M_{(\nu)}(S) = \prod_{i \in I} x_i^{\nu_i}$$

и назвать семейство $\{x_i\}_{i\in I}$ алгебраически независимым, если одночлены $M_{(\nu)}(S)$ линейно независимы над A. В частности, когда множество S конечно, скажем $S=\{t_1, \ldots, t_n\}$, одночлены имеют вид

$$M_{(\nu)}(t_1, \ldots, t_n)=t_1^{\nu_1}\ldots t_n^{\nu_n},$$

где $(\nu_1, \ldots, \nu_n)$ пробегает все наборы из n целых чисел $\geqslant 0$.

Наша конструкция алгебры многочленов показывает, как при заданном коммутативном кольце A можно построить A-алгебру, имеющую сколь угодно много алгебраически независимых элементов.

Следующая теорема дает нам важное свойство универсальности для алгебраически независимых элементов.

Теорема 1. *Пусть A, B — коммутативные кольца, f_0: $A\to B$ — A-алгебра, S — подмножество в B, порождающее B. Предположим, что элементы из S алгебраически независимы над A. Пусть A' — коммутативное кольцо, f: $A\to A'$ — гомоморфизм колец и λ: $S\to A'$ — некоторое отображение. Тогда существует единственный гомоморфизм колец h: $B\to A'$, для которого диаграмма*

$$\begin{array}{ccc} B & \xrightarrow{h} & A' \\ {\scriptstyle f_0}\uparrow & \nearrow{\scriptstyle f} & \\ A & & \end{array}$$

коммутативна, и ограничение h на S равно λ.

Доказательство. Пусть G — мультипликативный моноид, состоящий из всех элементов $M_{(\nu)}(S)$ в B. Если $\nu\neq\mu$, то $M_{(\nu)}(S)\neq M_{(\mu)}(S)$, так как иначе мы имели бы соотношение линейной зависимости

$$M_{(\nu)}(S)-M_{(\mu)}(S)=0.$$

Следовательно, отображение φ: $G\to A'$, для которого

$$\varphi\Big(\prod_{x\in S}x^{\nu(x)}\Big)=\prod_{x\in S}\lambda(x)^{\nu(x)},$$

является гомоморфизмом моноидов. Для завершения доказательства применяем предложение 1.

Мы можем применить теорему 1 к алгебре многочленов $A[S]$, отождествив множество S с его каноническим образом в $A[S]$. Тогда, если $B=A[S]$ и

$$\alpha=\sum_{(\nu)}a_{(\nu)}\cdot\prod_{x\in S}x^{\nu(x)},$$

то гомоморфизм h записывается так:

$$h(\alpha)=\sum_{(\nu)}f(a_{(\nu)})\prod_{x\in S}\lambda(x)^{\nu(x)}.$$

Рассмотрим частный случай, когда S — конечное множество, состоящее из различных элементов $t_1, \ldots, t_n$, алгебраически независимых над A. Пусть $X_1, \ldots, X_n$ суть n различных символов. Тогда имеется гомоморфизм колец

$$A[X_1, \ldots, X_n] \to A[t_1, \ldots, t_n],$$

отображающий X_i в t_i и индуцирующий тождественное отображение на A. Из определений тотчас видно, что его ядро должно быть равно 0 и что поэтому мы имеем изоморфизм. В частности, любые два кольца, порожденные над A n алгебраически независимыми элементами, изоморфны.

Имеется еще несколько частных случаев теоремы 1, которые мы специально отметим.

Пусть сначала A фиксировано, и пусть S, S' — два множества с заданной биекцией λ: $S \to S'$. Рассматривая S' как подмножество в $A[S']$, получаем изоморфизм

$$A[S] \approx A[S'],$$

индуцирующий биекцию S на S'. В случае когда S состоит из n символов $X_1, \ldots, X_n$ и S' состоит из n символов $Y_1, \ldots, Y_n$, мы видим, что кольца многочленов изоморфны, причем этот изоморфизм для каждого i переводит X_i в Y_i.

Предположим, что S содержится в S'. Тогда $A[S]$ канонически вкладывается в $A[S']$. Если S есть множество $\{X_1, \ldots, X_n\}$ и S' есть множество

$$\{X_1, \ldots, X_n, X_{n+1}, \ldots, X_N\},$$

то мы можем считать кольцо многочленов $A[X_1, \ldots, X_n]$ содержащимся в $A[X_1, \ldots, X_N]$. Одночлен

$$X_1^{\nu_1} \ldots X_n^{\nu_n}$$

может рассматриваться как одночлен от $X_1, \ldots, X_N$, если продолжить функцию ν так, чтобы $\nu_i = 0$ для $i > n$.

Пусть теперь A — подкольцо кольца A' и S — некоторое множество. Тогда имеем естественное вложение $A[S]$ в $A'[S]$, а именно многочлен

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

с коэффициентами в A может рассматриваться как многочлен, имеющий коэффициенты в A'. Мы будем отождествлять $A[S]$ с соответствующим подкольцом в $A'[S]$.

Более общо, пусть σ: $A \to A'$ — гомоморфизм коммутативных колец. Тогда этот гомоморфизм единственным способом продолжается до гомоморфизма колец

$$\bar{\sigma}\colon A[S] \to A'[S],$$

индуцирующего тождественное отображение на S. Например, пусть S — множество из n символов $X_1, \ldots, X_n$. Тогда

$$\bar{\sigma}\colon A[X_1, \ldots, X_n] \to A'[X_1, \ldots, X_n]$$

есть гомоморфизм колец, задаваемый отображением

$$\sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n} \longmapsto \sum \sigma(a_{(\nu)}) X_1^{\nu_1} \ldots X_n^{\nu_n}.$$

Пусть α обозначает многочлен, стоящий слева от стрелки; мы часто будем обозначать многочлен, стоящий справа, символом α^σ.

Можно сказать, что α^σ получается из α применением σ к коэффициентам α.

Пусть A — целостное кольцо и $\mathfrak{p}$ — его простой идеал. Пусть $\sigma\colon A \to A'$ — канонический гомоморфизм A на $A/\mathfrak{p}$. Если $\alpha(X)$ — многочлен из $A[X]$, то α^σ будет иногда называться *редукцией* α *по модулю* $\mathfrak{p}$.

Например, взяв $A = \mathbf{Z}$ и $\mathfrak{p} = (p)$, где p — простое число, мы можем говорить о многочлене $3X^4 - X + 2$ как о многочлене mod 5, рассматривая коэффициенты 3, -1, 2 как целые числа mod 5, т. е. как элементы из $\mathbf{Z}/5\mathbf{Z}$.

§ 3. Элементарные свойства многочленов

Пусть A — коммутативное кольцо и S — множество из n символов $X_1, \ldots, X_n$. Отождествляя $X_1, \ldots, X_n$ с их каноническими образами в кольце многочленов $A[X_1, \ldots, X_n]$, мы называем $X_1, \ldots, X_n$ *независимыми переменными* над A, а $A[X]$—кольцом многочленов от n переменных. Всякий многочлен α из $A[X]$ допускает единственное представление в виде

$$\alpha = \sum a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n} = \sum a_{(\nu)} M_{(\nu)}(X).$$

Пусть $(b_1, \ldots, b_n)$ — элемент из $\prod_1^n A$ (прямого произведения A самого на себя n раз), которое мы будем обозначать через $A^{(n)}$. В силу теоремы 1 существует однозначно определенный гомоморфизм

$$h\colon A[X_1, \ldots, X_n] \to A,$$

для которого $h(X_i) = b_i$ при $i = 1, \ldots, n$ и который тождествен на A. Имеем

$$h(\alpha) = \sum \alpha_{(\nu)} b_1^{\nu_1} \ldots b_n^{\nu_n}.$$

Мы будем обозначать этот элемент из A через $\alpha(b_1, \ldots, b_n)$ и говорить, что это элемент, полученный *подстановкой* $(b_1, \ldots, b_n)$