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* $(b_1, \ldots, b_n)$

вместо $(X_1, \ldots, X_n)$ в α. Таким образом, мы видим, что α определяет функцию на $A^{(n)}$ со значениями в A.

Аналогично, если A — подкольцо (коммутативного) кольца B и $(b) = (b_1, \ldots, b_n)$ — элемент из $B^{(n)}$, то мы можем тем же путем, что и выше, образовать элемент $\alpha(b)$ и получить функцию из $B^{(n)}$ в B, задаваемую соответствием $(b) \longmapsto \alpha(b)$.

Записывая α, как и выше, мы видим, что

$$\alpha(b_1, \ldots, b_n) = \sum a_{(\nu)} M_{(\nu)}(b_1, \ldots, b_n),$$

или в векторных обозначениях

$$\alpha(b) = \sum a_{(\nu)} M_{(\nu)}(b).$$

В этих обозначениях

$$\alpha = \alpha(X) = \alpha(X_1, \ldots, X_n).$$

Мы увидим ниже, что в том случае, когда A — целостное кольцо, $A[X_1, \ldots, X_n]$ также целостное. Если K — поле частных кольца A, то поле частных кольца $A[X_1, \ldots, X_n]$ обозначается через $K(X_1, \ldots, X_n)$. Элементы поля $K(X_1, \ldots, X_n)$ называются *рациональными функциями*. Всякая рациональная функция может быть записана в виде дроби $f(X)/g(X)$, где f, g — многочлены. Если $(b_1, \ldots, b_n)$ — элемент из $K^{(n)}$ и рациональная функция допускает представление в виде такой дроби f/g, что $g(b) \neq 0$, то мы говорим, что эта рациональная функция *определена* в (b). Из общих свойств локализации вытекает, что в этом случае мы можем подставить (b) в рациональную функцию и получить значение $f(b)/g(b)$.

Может случиться, что многочлен не является нулевым многочленом, но определяет нулевую функцию.

Пример. Пусть $A = \mathbf{Z}/p\mathbf{Z}$ для некоторого простого p. Если $a \in A$ и $a = 0$, то $a^p = 0$. Если $a \neq 0$, то a — элемент мультипликативной группы ненулевых элементов из A, имеющей порядок $p - 1$. Значит, $a^{p-1} = 1$, и мы получаем

$$a^p = a.$$

Это справедливо для всех $a \in A$. Поэтому многочлен $X^p - X$ определяет нулевое отображение A в себя, а многочлены X^p и X определяют одну и ту же функцию, а именно тождественное отображение на A.

Вообще пусть F — конечное поле и q — число элементов в F. Тогда как X^q, так и X определяют тождественное отображение F в себя. Можно показать, что любое отображение F в себя задается некоторым многочленом (от одной переменной) и аналогично любая функция на $F^{(n)}$ со значениями в F задается некоторым многочленом от n переменных (см. упражнения).

Пусть снова A — подкольцо в B, и пусть $b_1, \ldots, b_n$ — элементы из B. Напомним, что если гомоморфизм

$$A[X_1, \ldots, X_n] \to B,$$

задаваемый соответствием $\alpha(X) \mapsto \alpha(b)$, имеет тривиальное ядро, т. е. если он является вложением, то $b_1, \ldots, b_n$ *алгебраически независимы над* A. Если $n = 1$ и элемент $b = b_1$ алгебраически независим над A, то мы также говорим, что b *трансцендентен* над A.

Пример. Известно (хотя и не тривиально доказывается), что числа $e = 2{,}71\ldots$ и $\pi = 3{,}14\ldots$ трансцендентны над полем рациональных чисел $\mathbf{Q}$. Не известно, являются ли они алгебраически независимыми (или даже, рационально ли число $e + \pi$). Для конкретных комплексных чисел обычно бывает чрезвычайно трудно выяснить, являются ли они трансцендентными или же алгебраически независимыми над полем рациональных чисел.

Пусть A обозначает, как и прежде, коммутативное кольцо, и пусть $S = \{X_1, \ldots, X_n\}$. Под *степенью* примитивного одночлена

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

мы будем понимать целое число $\nu_1 + \ldots + \nu_n$ (которое $\geqslant 0$).

Многочлен

$$aX_1^{\nu_1} \ldots X_n^{\nu_n} \quad (a \in A)$$

будет называться *одночленом* (не обязательно примитивным).

Если $\alpha(X)$ — многочлен из $A[X]$, записываемый в виде

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

то либо $\alpha = 0$, и в этом случае мы говорим, что его степень равна $-\infty$, либо $\alpha \neq 0$, и тогда мы определяем *степень* α как максимум степеней одночленов $M_{(\nu)}(X)$, для которых $a_{(\nu)} \neq 0$. (О таких одночленах говорят, что они *встречаются* в многочлене.) Отметим, что степень многочлена α равна 0 в том и только в том случае, если

$$\alpha(X) = a_0 X_1^0 \ldots X_n^0$$

для некоторого $a_0 \in A$, $a_0 \neq 0$. Этот многочлен мы также записываем просто как $\alpha(X) = a_0$, т. е. пишем 1 вместо

$$X_1^0 \ldots X_n^0,$$

отождествляя тем самым этот многочлен с константой a_0.

Отметим, что многочлен $\alpha(X_1, \ldots, X_n)$ от n переменных можно рассматривать как многочлен от X_n с коэффициентами в $A[X_1, \ldots, X_{n-1}]$ (если $n \geqslant 2$). Действительно, имеет место гомоморфизм

$$A[X_1, \ldots, X_n] \to A[X_1, \ldots, X_{n-1}][X_n],$$

получаемый подстановкой, и этот гомоморфизм, очевидно, является изоморфизмом. Таким образом,

$$\alpha(X_1, \ldots, X_n) = \sum_{j=0}^{\infty} \alpha_j(X_1, \ldots, X_{n-1}) X_n^j,$$

где α_j — элементы из $A[X_1, \ldots, X_{n-1}]$. Под *степенью многочлена* α *относительно* X_n мы будем понимать его степень как многочлена от X_n с коэффициентами в $A[X_1, \ldots, X_{n-1}]$. Легко видеть, что если эта степень равна d, то d — наибольшее целое число, встречающееся в качестве показателя при X_n в одночленах

$$a_{(\nu)} X_1^{\nu_1} \ldots X_n^{\nu_n}$$

с $a_{(\nu)} \neq 0$. Аналогичным образом определяем степень по каждой переменной X_i $(i = 1, \ldots, n)$.

Степень многочлена α по каждой отдельной переменной, как правило, отличается, конечно, от его степени (которую называют иногда *полной* степенью, если хотят избежать двусмысленности). Например,

$$X_1^3 X_2 + X_2^2$$

имеет полную степень 4, степень 3 по X_1 и 2 по X_2.

Мы будем часто слово „степень" сокращенно обозначать символом deg.

Пусть $f(X)$ — многочлен от одной переменной из $A[X]$

$$f(X) = a_0 + \ldots + a_n X^n,$$

где $a_i \in A$ и n — некоторое целое число $\geqslant 0$. Если $f \neq 0$ и $\deg f = n$, то по определению $a_n \neq 0$; мы называем a_n *старшим коэффициентом* многочлена f, а a_0 — его *постоянным членом*. Заметим, что $a_0 = f(0)$.

Пусть

$$g(X) = b_0 + \ldots + b_m X^m$$

— некоторый многочлен из $A[X]$ степени m, причем $g \neq 0$. Тогда

$$f(X)\, g(X) = a_0 b_0 + \ldots + a_n b_m X^{m+n}.$$

Если предположить, что по крайней мере один из старших коэффициентов a_n *или* b_m *не является делителем* 0 *в* A, *то*

$$\deg(fg) = \deg f + \deg g$$

и старший коэффициент fg *равен* $a_n b_m$. *Это выполняется, в частности, в тех случаях, когда* a_n *или* b_m *есть единица в* A, *или*

когда кольцо A — целостное. Следовательно, если A — целостное кольцо, то $A[X]$ также целостное.

Если f или $g = 0$, то мы по-прежнему имеем

$$\deg(fg) = \deg f + \deg g,$$

если считать, что $-\infty + m = -\infty$ для любого целого m.

Тривиально проверяется, что для любых многочленов $f, g \in A[X]$ имеет место неравенство

$$\deg(f+g) \leqslant \max(\deg f, \deg g),$$

опять-таки при соглашении, что $-\infty < m$ для всякого целого m.

Мы предоставляем читателю в качестве упражнения доказать, что в том случае, когда A — целостное кольцо и f, g — многочлены *от нескольких переменных*, имеют место те же правила:

$$\deg(fg) = \deg f + \deg g,$$

$$\deg(f+g) \leqslant \max(\deg f, \deg g).$$

Здесь степень может пониматься либо как полная степень, либо как степень по одной из переменных. Мы заключаем отсюда, что кольцо $A[X_1 \ldots, X_n]$ — целостное.

Пусть снова A — произвольное коммутативное кольцо и d — целое число $\geqslant 0$. Пусть

$$f(X_1, \ldots, X_n) \neq 0$$

— многочлен от n переменных над A. Мы будем говорить, что f — *однородный* многочлен степени d, или *форма* степени d, если все одночлены, встречающиеся в f, имеют степень d, т. е. если в записи

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

для всякого $a_{(\nu)} \neq 0$ имеем

$$\nu_1 + \ldots + \nu_n = d.$$

Мы предоставим читателю в качестве упражнения доказать, что *ненулевой многочлен f от n переменных над A является однородным степени d тогда и только тогда, когда для всякого множества из $n+1$ алгебраически независимых элементов $u, t_1, \ldots, t_n$ над A имеет место равенство*

$$f(ut_1, \ldots, ut_n) = u^d f(t_1, \ldots, t_n).$$

Пусть f — однородный многочлен степени d. В силу теоремы 1 аналогичное соотношение выполняется, если подставить вместо u, $t_1, \ldots, t_n$ произвольные элементы $b_0, b_1, \ldots, b_n$ (при этом b_i берутся из некоторого коммутативного кольца B, содержащего A в качестве подкольца).

Отметим, что если f и g — однородные многочлены степеней d и e соответственно и $fg \neq 0$, то fg — однородный многочлен степени de. Если $d = e$ и $f + g \neq 0$, то $f + g$ — однородный многочлен степени d.

Наконец, сделаем одно замечание относительно терминологии. Ввиду изоморфизма

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

между кольцом многочленов от n переменных и кольцом, порожденным над A n алгебраически независимыми элементами, мы можем применять всю терминологию, введенную нами для многочленов, к элементам из $A[t_1, \ldots, t_n]$. Таким образом, мы можем говорить о степени элемента из $A[t]$, и правила для степени произведения и суммы будут выполняться. Фактически мы будем элементы из $A[t]$ называть также многочленами от (t). Алгебраически независимые элементы будут также называться переменными (или независимыми переменными); любое различие, которое мы делаем между $A[X]$ и $A[t]$, является скорее психологическим, чем математическим.

§ 4. Алгоритм Евклида

Теорема 2. *Пусть A — коммутативное кольцо, f, $g \in A[X]$ — многочлены от одной переменной степени $\geqslant 0$. Предположим, что старший коэффициент многочлена g является единицей в A. Тогда существуют однозначно определенные многочлены q, $r \in A[X]$, такие, что*

$$f = gq + r$$

и $\deg r < \deg g$.

Доказательство. Пусть

$$f(X) = a_n X^n + \ldots + a_0,$$
$$g(X) = b_d X^d + \ldots + b_0,$$

где $n = \deg f$, $d = \deg g$, так что a_n, $b_d \neq 0$ и b_d — единица в A. Применим индукцию по n.

Если $n = 0$ и $\deg g > \deg f$, то положим $q = 0$, $r = f$. Если $\deg g = \deg f = 0$, то положим $r = 0$ и $q = a_n b_d^{-1}$.

Предположим, что теорема доказана для многочленов степени $< n$ (где $n > 0$). Мы можем предполагать, что $\deg g \leqslant \deg f$ (иначе возьмем $q = 0$ и $r = f$). Тогда

$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + f_1(X),$$

где $f_1(X)$ имеет степень $< n$. По индукции мы можем найти q_1, r, такие, что

$$f(X) = a_n b_d^{-1} X^{n-d} g(X) + q_1(X) g(X) + r(X)$$