имеет корень a в K, то $a^{p^r}=c$ и

$$X^{p^r}-c=(X-a)^{p^r}.$$

Следовательно, наш многочлен имеет ровно один корень кратности p^r. Например, $(X-1)^{p^r}=X^{p^r}-1$.

§ 9. Симметрические многочлены

Пусть A — коммутативное кольцо и $t_1, \ldots, t_n$ — алгебраически независимые элементы над A. Пусть X — переменная над $A[t_1, \ldots, t_n]$. Образуем многочлен

$$\mathbf{F}(X)=(X-t_1)\ldots(X-t_n)=X^n-s_1X^{n-1}+\ldots+(-1)^n s_n,$$

где каждый элемент $s_i=s_i(t_1, \ldots, t_n)$ является многочленом от $t_1, \ldots, t_n$. Например,

$$s_1=t_1+\ldots+t_n \quad \text{и} \quad s_n=t_1\ldots t_n.$$

Многочлены $s_1, \ldots, s_n$ называются *элементарными симметрическими многочленами* от $t_1, \ldots, t_n$.

Мы предоставляем читателю в качестве упражнения проверку того, что s_i — однородный многочлен степени i от $t_1, \ldots, t_n$.

Пусть σ — некоторая перестановка целых чисел $(1, \ldots, n)$. Для данного многочлена $f(t)\in A[t]=A[t_1, \ldots, t_n]$ определим f^σ формулой

$$f^\sigma(t_1, \ldots, t_n)=f(t_{\sigma(1)}, \ldots, t_{\sigma(n)})\ ^{1)}.$$

Если σ, τ — две перестановки, то $f^{\sigma\tau}=(f^\sigma)^\tau$ и, следовательно, симметрическая группа G на n символах действует на кольце многочленов $A[t]$. Многочлен называется *симметрическим*, если $f^\sigma=f$ для всех $\sigma\in G$. Ясно, что множество симметрических многочленов есть подкольцо в $A[t]$, содержащее постоянные многочлены (т. е. само A), а также элементарные симметрические многочлены $s_1, \ldots, s_n$. Ниже мы увидим, что оно по существу ничего больше и не содержит.

Пусть $X_1, \ldots, X_n$ — переменные. Будем считать *весом* одночлена

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

целое число $\nu_1+2\nu_2+\ldots+n\nu_n$. Определим *вес* многочлена $g(X_1, \ldots, X_n)$ как максимум весов одночленов, встречающихся в g.

---

[1]) Имеется лишь внешнее сходство с обозначением f^σ из § 2 и 8. — *Прим. ред.*

Теорема 11. *Пусть $f(t) \in A[t_1, \ldots, t_n]$ — симметрический многочлен степени d. Тогда существует многочлен $g(X_1, \ldots, X_n)$ веса $\leqslant d$, такой, что*

$$f(t) = g(s_1, \ldots, s_n).$$

Доказательство. Индукция по n. Если $n = 1$, то теорема очевидна, так как $s_1 = t_1$.

Предположим, что теорема доказана для многочленов от $n-1$ переменной.

Если мы подставим $t_n = 0$ в выражение для $\mathbf{F}(X)$, то получим

$$(X - t_1) \ldots (X - t_{n-1}) X = X^n - (s_1)_0 X^{n-1} + \ldots$$
$$\ldots + (-1)^{n-1} (s_{n-1})_0 X,$$

где $(s_i)_0$ — выражение, полученное подстановкой $t_n = 0$ в s_i. Заметим, что $(s_1)_0, \ldots, (s_{n-1})_0$ — это как раз элементарные симметрические многочлены от $t_1, \ldots, t_{n-1}$.

Проведем теперь индукцию по d. Если $d = 0$, то наше утверждение тривиально. Предположим, что $d > 0$ и что наше утверждение доказано для многочленов степени $< d$. Пусть $f(t_1, \ldots, t_n)$ имеет степень $\leqslant d$. Существует многочлен $g_1(X_1, \ldots, X_{n-1})$ веса $\leqslant d$, такой, что

$$f(t_1, \ldots, t_{n-1}, 0) = g_1((s_1)_0, \ldots, (s_{n-1})_0).$$

Отметим, что $g_1(s_1, \ldots, s_{n-1})$ имеет степень $\leqslant d$ по $t_1, \ldots, t_n$. Многочлен

$$f_1(t_1, \ldots, t_n) = f(t_1, \ldots, t_n) - g_1(s_1, \ldots, s_{n-1})$$

имеет степень $\leqslant d$ (по $t_1, \ldots, t_n$) и является симметрическим. Имеем

$$f_1(t_1, \ldots, t_{n-1}, 0) = 0.$$

Следовательно, f_1 делится на t_n, т. е. содержит t_n множителем. Так как f_1 симметрический, то он содержит в качестве множителя $t_1 \ldots t_n$. Следовательно,

$$f_1 = s_n f_2(t_1, \ldots, t_n),$$

где f_2 — некоторый многочлен, который должен быть симметрическим и степень которого $\leqslant d - n < d$. По индукции существует многочлен g_2 от n переменных веса $\leqslant d - n$, для которого

$$f_2(t_1, \ldots, t_n) = g_2(s_1, \ldots, s_n).$$

Получаем

$$f(t) = g_1(s_1, \ldots, s_{n-1}) + s_n g_2(s_1, \ldots, s_n),$$

причем каждый член справа имеет вес $\leqslant d$. Это доказывает нашу теорему.

Покажем теперь, что элементарные симметрические многочлены $s_1, \ldots, s_n$ алгебраически независимы над A.

Если они зависимы, то возьмем не равный 0 многочлен $f(X_1, \ldots, X_n) \in A[X]$ наименьшей степени, для которого

$$f(s_1, \ldots, s_n) = 0.$$

Запишем f как многочлен от X_n с коэффициентами в $A[X_1, \ldots, X_{n-1}]$:

$$f(X_1, \ldots, X_n) = f_0(X_1, \ldots, X_{n-1}) + \ldots + f_d(X_1, \ldots, X_{n-1}) X_n^d.$$

Тогда $f_0 \neq 0$. Иначе

$$f(X) = X_n \psi(X),$$

где ψ — некоторый многочлен и, следовательно, $s_n \psi(s_1, \ldots, s_n) = 0$. Отсюда вытекало бы, что $\psi(s_1, \ldots, s_n) = 0$, причем ψ имеет степень, меньшую, чем степень f.

Подставляя s_i вместо X_i в предыдущее тождество, получаем

$$0 = f_0(s_1, \ldots, s_{n-1}) + \ldots + f_d(s_1, \ldots, s_{n-1}) s_n^d.$$

Это — соотношение в $A[t_1, \ldots, t_n]$; если мы подставим 0 вместо t_n в это соотношение, то все члены, кроме первого, обратятся в 0, что дает

$$0 = f_0((s_1)_0, \ldots, (s_{n-1})_0)$$

(мы используем те же обозначения, что и в доказательстве теоремы 1). Мы получили нетривиальное соотношение между элементарными симметрическими многочленами от $t_1, \ldots, t_{n-1}$ — противоречие.

Пример. Рассмотрим произведение

$$\delta(t) = \prod_{i<j} (t_i - t_j).$$

Мы тотчас видим, что какова бы ни была перестановка σ чисел $(1, \ldots, n)$,

$$\delta^\sigma(t) = \pm \delta(t).$$

Следовательно, $\delta(t)^2$ — симметрический многочлен; мы называем его *дискриминантом*

$$D(s_1, \ldots, s_n) = \prod_{i<j} (t_i - t_j)^2.$$

Таким образом, мы рассматриваем дискриминант как многочлен от элементарных симметрических функций.