

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

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

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 $A[t_1, \dots, t_n]$. 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 ≥ 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

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

$$g(X) = b_d X^d + \dots + b_0,$$

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 $\deg g \leq \deg f$ (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

$$f_1(X) = a_n b_d^{-1} X^{n-d} g(X) + q_1(X) g(X) + r(X)$$

и $\deg r < \deg g$. Положим

$$q(X) = a_n b_d^{-1} X^{n-d} + q_1(X),$$

чем доказательство существования q , r и закончено.

Что касается единственности, то предположим, что

$$f = q_1 g + r_1 = q_2 g + r_2,$$

где $\deg r_1 < \deg g$ и $\deg r_2 < \deg g$. Тогда

$$(q_1 - q_2)g = r_2 - r_1.$$

Так как по предположению старший коэффициент g есть единица, то

$$\deg(q_1 - q_2)g = \deg(q_1 - q_2) + \deg g.$$

Поскольку $\deg(r_2 - r_1) < \deg g$, то предыдущее соотношение может выполняться только при $q_1 - q_2 = 0$, т. е. $q_1 = q_2$ и, следовательно, $r_1 = r_2$, что и требовалось показать.

Теорема 3. Пусть k — поле. Тогда кольцо многочленов от одной переменной $k[X]$ является целостным кольцом главных идеалов.

Доказательство. Пусть a — идеал в $k[X]$, причем $a \neq 0$. Пусть g — элемент из a наименьшей степени ≥ 0 и f — любой отличный от нуля элемент из a . Согласно алгоритму Евклида (т. е. по теореме 2) мы можем найти $q, r \in k[X]$, такие, что

$$f = qg + r$$

и $\deg r < \deg g$. Но $r = f - qg$, следовательно, r лежит в a . Так как g имеет минимальную степень ≥ 0 , то $r = 0$; значит, a состоит из всех многочленов вида qg (где $q \in k[X]$). Это доказывает нашу теорему.

Следствие. Кольцо $k[X]$ факториально.

Если k — поле, то всякий ненулевой элемент из k будет единицей в k и непосредственно видно, что единицы в $k[X]$ — это просто единицы из k . (Никакой многочлен степени ≥ 1 не может быть единицей ввиду формулы сложения для степени произведения.)

Пусть A — коммутативное кольцо и $f(X)$ — многочлен из $A[X]$. Пусть A — подкольцо в B . Элемент $b \in B$ называется *корнем* или *нулем* f в B , если $f(b) = 0$. Аналогично, если (X) — набор из n переменных, то набор из n элементов (b) называется нулем f , если $f(b) = 0$.

Теорема 4. Пусть k — поле и f — многочлен степени $n \geq 0$ из $k[X]$ от одной переменной X . Тогда f имеет самое большее n корней в k , и если a — корень f в k , то $f(X)$ делится на $X - a$.

Доказательство. Предположим, что $f(a) = 0$. Найдем q, r , такие, что

$$f(X) = q(X)(X - a) + r(X)$$

и $\deg r < 1$. Тогда

$$0 = f(a) = r(a).$$

Поскольку r либо 0, либо ненулевая константа, то мы должны иметь $r = 0$, т. е. $X - a$ делит $f(X)$. Если a_1, \dots, a_m — различные корни f в k , то по индукции мы находим, что $f(X)$ делится на произведение

$$(X - a_1) \dots (X - a_m),$$

откуда $m \leq n$, как и утверждалось.

Следствие 1. Пусть k — поле, T — бесконечное подмножество в k и $f(X) \in k[X]$ — многочлен от одной переменной. Если $f(a) = 0$ для всех $a \in T$, то $f = 0$; иными словами, если f индуцирует нулевую функцию на T , то f — нулевой многочлен.

Следствие 2. Пусть k — поле, T_1, \dots, T_n — бесконечные подмножества в k и $f(X_1, \dots, X_n)$ — многочлен от n переменных над k . Если $f(a_1, \dots, a_n) = 0$ для всех $a_i \in T_i$ ($i = 1, \dots, n$), то $f = 0$.

Доказательство. По индукции. Мы только что убедились, что теорема справедлива для одной переменной. Пусть $n \geq 2$; запишем

$$f(X_1, \dots, X_n) = \sum_j f_j(X_1, \dots, X_{n-1}) X_n^j$$

как многочлен от X_n с коэффициентами в $k[X_1, \dots, X_{n-1}]$. Если существует набор

$$(b_1, \dots, b_{n-1}) \in T_1 \times \dots \times T_{n-1},$$

такой, что $f_j(b_1, \dots, b_{n-1}) \neq 0$ для некоторого j , то

$$f(b_1, \dots, b_{n-1}, X)$$

— ненулевой многочлен в $k[X_n]$, принимающий значение 0 на бесконечном множестве элементов T_n . Но это невозможно. Следовательно, f_j индуцирует нулевую функцию на $T_1 \times \dots \times T_{n-1}$ для всех j и по индукции мы имеем, что $f_j = 0$ для всех j . Следовательно, $f = 0$, что и требовалось показать.

Следствие 3. Пусть k — бесконечное поле и f — многочлен от n переменных над k . Если f индуцирует нулевую функцию на $k^{(n)}$, то $f = 0$.

Рассмотрим теперь случай конечных полей. Пусть k — конечное поле из q элементов и $f(X_1, \dots, X_n)$ — многочлен от n переменных над k . Запишем

$$f(X_1, \dots, X_n) = \sum a_{(v)} X_1^{v_1} \dots X_n^{v_n}.$$

Как мы условились говорить, одночлен $M_{(v)}(X)$ встречается в f , если $a_{(v)} \neq 0$. Предположим, что это имеет место и что в нашем одночлене $M_{(v)}(X)$ некоторая переменная X_i встречается с показателем $v_i \geq q$. Тогда мы можем написать

$$X_i^{v_i} = X_i^{q+\mu}, \quad \text{где } \mu \text{ — целое число } \geq 0.$$

Если мы теперь заменим в этом одночлене $X_i^{v_i}$ на $X_i^{\mu+1}$, то получим новый многочлен, определяющий ту же самую функцию, что и f . Степень этого нового многочлена не больше, чем степень f .

Выполняя предыдущую операцию конечное число раз для всех одночленов, встречающихся в f , и всех переменных X_1, \dots, X_n , мы получим некоторый новый многочлен f^* , который определяет ту же самую функцию, что и f , но степень которого по каждой переменной $< q$.

Теорема 5. Пусть k — конечное поле из q элементов и f — многочлен от n переменных над k , такой, что степень f по каждой переменной $< q$. Если f индуцирует нулевую функцию на $k^{(n)}$, то $f = 0$.

Доказательство. По индукции. Если $n = 1$, то $\deg f < q$ и, следовательно, f не может иметь q корней в случае $f \neq 0$. Индуктивный шаг проводится точно так же, как в доказательстве следствия 2.

Пусть f — многочлен от n переменных над конечным полем k . Многочлен g , степень которого по каждой переменной $< q$, будем называть *редуцированным*. Выше мы показали, что существует редуцированный многочлен f^* , который дает ту же самую функцию на $k^{(n)}$, что и f . Теорема 5 теперь показывает, что *этот редуцированный многочлен единственен*. Действительно, если g_1, g_2 — редуцированные многочлены, дающие одну и ту же функцию, то $g_1 - g_2$ — редуцирован и дает нулевую функцию. Следовательно, $g_1 - g_2 = 0$ и $g_1 = g_2$.

Дадим еще одно приложение теоремы 4. Пусть k — поле. Под мультиликативной подгруппой в k мы будем понимать подгруппу группы k^* (ненулевых элементов k).

Теорема 6. Пусть k — поле. Всякая конечная мультиликативная подгруппа U в k циклическая.

Доказательство. Запишем U в виде произведения подгрупп $U(p)$ для всех простых p , где $U(p)$ есть p -группа. В силу упражнения 22 из гл. I достаточно доказать, что $U(p)$ циклическая для каждого p . Пусть a — элемент из $U(p)$ максимального периода p^r , где r — некоторое целое число. Тогда $x^{p^r} = 1$ для всех элементов $x \in U(p)$ и, следовательно, все элементы из $U(p)$ являются корнями многочлена

$$X^{p^r} - 1.$$

Циклическая группа, порожденная a , содержит p^r элементов. Если эта циклическая группа не совпадает с $U(p)$, то наш многочлен имеет более чем p^r корней, что невозможно. Следовательно, a порождает $U(p)$, и наша теорема доказана.

Следствие. Если k — конечное поле, то группа k^* — циклическая,

Элемент ζ поля k , для которого существует такое целое число $n \geq 1$, что $\zeta^n = 1$, называется *корнем из единицы* или, более точно, *корнем n -й степени из единицы*. Таким образом, множество корней n -й степени из единицы — это множество корней многочлена $X^n - 1$. Существует самое большое n таких корней, и они, очевидно, образуют группу, которая, согласно теореме 6, является циклической. Позднее мы изучим корни из единицы более подробно. Образующая группы корней n -й степени из единицы (в том случае, если эта группа имеет порядок n) называется *примитивным* (или *первообразным*) корнем n -й степени из единицы. Например, в поле комплексных чисел $e^{2\pi i/n}$ — примитивный корень n -й степени из единицы, а все корни n -й степени из единицы имеют вид $e^{2\pi i v/n}$, где $1 \leq v \leq n$.

§ 5. Простейшие дроби

В этом параграфе мы займемся анализом поля частных кольца главных идеалов, используя факториальность такого кольца.

Теорема 7. Пусть A — целостное кольцо главных идеалов и P — множество представителей для его неприводимых элементов. Пусть K — поле частных кольца A и a — некоторый элемент из K . Тогда для каждого $p \in P$ найдутся элемент $a_p \in A$ и целое число $j(p) \geq 0$, такие, что $j(p) = 0$ для почти всех $p \in P$, a_p и $p^{j(p)}$ взаимно просты и

$$a = \sum_{p \in P} \frac{a_p}{p^{j(p)}}.$$