

## Глава II. Кольца многочленов

### 1. О СЛЕДСТВИЯХ КОММУТАТИВНОСТИ, АССОЦИАТИВНОСТИ И ДИСТРИБУТИВНОСТИ

*Суммы.* Пусть на множестве  $A$  задана бинарная алгебраическая операция сложения. Предположим, что эта операция ассоциативна, т.е.  $(a+b)+c = a+(b+c)$  для любых  $a, b, c \in A$ . Это значит, что сумма  $a+b+c$  не зависит от того, как мы расставим скобки. Нетрудно доказать по индукции, что то же самое верно и для любых конечных сумм. Например, при четырех слагаемых все 5 сумм

$$a+(b+(c+d)), \quad a+((b+c)+d), \quad (a+b)+(c+d), \quad ((a+b)+c)+d, \quad (a+(b+c))+d$$

равны. Поэтому конечные суммы  $a_1 + a_2 + \dots + a_n$  (если, конечно, сложение ассоциативно) обычно записываются без скобок; как бы мы ни группировали слагаемые так, чтобы каждый раз складывались два элемента, результат всегда будет один и тот же. Но, вообще говоря, порядок слагаемых в сумме менять нельзя.

Однако, если сложение не только ассоциативно, но и коммутативно, т.е.  $a+b = b+a$  для любых  $a, b \in A$ , то, как легко доказать по индукции, слагаемые в конечной сумме можно переставлять произвольным образом. Это позволяет нам записывать сумму нескольких элементов при помощи знака  $\sum$ . Выражения

$$\sum_{i=1}^n x_i, \quad \sum_{s \in S} s, \quad \sum_{i \in I} a_i$$

означают соответственно сумму элементов  $x_1, x_2, \dots, x_n \in A$ , сумму всех элементов из конечного множества  $S \subset A$  и сумму элементов  $a_i \in A$ , занумерованных элементами из конечного множества  $I$ . Часто бывает удобно рассматривать и сумму пустого множества слагаемых; ее естественно считать равной 0. Иногда аналогичные обозначения применяются и тогда, когда множество индексов бесконечно; например, нам придется рассматривать суммы вида

$$\sum_{i=1}^{\infty} a_i.$$

Такое выражение осмысленно, если все элементы  $a_i$ , кроме конечного числа, равны 0; в этом случае мы говорим, что почти все  $a_i$  равны 0.

Пусть теперь  $I, J$  – два конечных множества, и пусть  $I \times J$  – их декартово произведение. Далее, пусть  $a_{ij} \in A$  – набор элементов, занумерованных двумя индексами  $i \in I, j \in J$ . Тогда определена сумма

$$\sum_{(i,j) \in I \times J} a_{ij}.$$

Вместо того, чтобы считать сумму по декартову произведению двух множеств, можно поступить иначе: зафиксировав  $i$ , сосчитать сумму всех  $a_{ij}, j \in J$ , а затем сложить все получившиеся суммы. Еще один способ состоит в том, что, зафиксировав  $j$ , мы считаем сумму всех  $a_{ij}, i \in I$ , а затем складываем все получившиеся суммы. Ввиду независимости суммы от порядка и способа группировки слагаемых результат всегда будет один и тот же:

$$\sum_{(i,j) \in I \times J} a_{ij} = \sum_{i \in I} \sum_{j \in J} a_{ij} = \sum_{j \in J} \sum_{i \in I} a_{ij}.$$

**Произведения.** Все, что было сказано о сумме, остается справедливым и для произведения (если оно, конечно, ассоциативно и коммутативно). Для обозначения произведения нескольких сомножителей применяется знак  $\prod$ : выражения

$$\prod_{i=1}^n x_i, \quad \prod_{s \in S} s, \quad \prod_{i \in I} a_i, \quad \prod_{i=1}^{\infty} a_i$$

означают соответственно произведение элементов  $x_1, x_2, \dots, x_n \in A$ , произведение всех элементов из конечного множества  $S \subset A$ , произведение элементов  $a_i \in A$ , занумерованных элементами из конечного множества  $I$  и произведение элементов  $a_i$ ,  $1 \leq i < \infty$ , почти все из которых равны 1. Произведением пустого множества сомножителей удобно считать 1. Для двойных произведений справедливости соотношения, аналогичные соотношениям для двойных сумм:

$$\prod_{(i,j) \in I \times J} a_{ij} = \prod_{i \in I} \prod_{j \in J} a_{ij} = \prod_{j \in J} \prod_{i \in I} a_{ij}.$$

**Свойство 0.** Мы в самых различных ситуациях будем пользоваться тем, что умножение на 0 всегда дает нулевой результат. Чтобы не доказывать это каждый раз заново, приведем этот результат в достаточно общей форме.

**Предложение 1.** Пусть  $A, B, C$  – абелевы группы, и пусть для каждой элементов  $a \in A$ ,  $b \in B$  определено их произведение  $ab \in C$ , причем выполняется соотношение дистрибутивности:  $(a_1 + a_2)b = a_1b + a_2b$  для любых  $a_1, a_2 \in A$ ,  $b \in B$ . Тогда  $0_A \cdot b = 0_C$  для любого  $b \in B$ .

*Доказательство.* Мы имеем:

$$0_A \cdot b = (0_A + 0_A)b = 0_A \cdot b + 0_A \cdot b;$$

Прибавив к обеим частям этого равенства элемент  $-0_A \cdot b$  и воспользовавшись ассоциативностью сложения в группе  $C$ , получим:

$$\begin{aligned} 0_C &= 0_A \cdot b + (-0_A \cdot b) = (0_A \cdot b + 0_A \cdot b) + (-0_A \cdot b) = \\ &= 0_A \cdot b + (0_A \cdot b + (-0_A \cdot b)) = 0_A \cdot b + 0_C = 0_A \cdot b. \end{aligned}$$

В частности, это свойство выполняется, если  $A$  – любое кольцо, и  $B = C = A$ .

**Произведение сумм.** Укажем еще одно свойство, вытекающее из коммутативности и ассоциативности сложения, ассоциативности умножения и дистрибутивности. Сначала сформулируем его словесно. Для того, чтобы перемножить несколько сумм, надо в каждом сомножителе выбрать по одному слагаемому, перемножить выбранные слагаемые, а затем все так полученные произведения сложить. Запишем это теперь в виде точной формулы:

$$\left( \sum_{i_1 \in I_1} a_{1,i_1} \right) \left( \sum_{i_2 \in I_2} a_{2,i_2} \right) \cdots \left( \sum_{i_r \in I_r} a_{r,i_r} \right) = \sum_{(i_1, \dots, i_r) \in I_1 \times \cdots \times I_r} a_{1,i_1} a_{2,i_2} \cdots a_{r,i_r}.$$

## 2. ОПРЕДЕЛЕНИЕ И ПОСТРОЕНИЕ КОЛЕЦ МНОГОЧЛЕНОВ

**Определение кольца многочленов.** Пусть  $\Lambda$  – кольцо. Непустое подмножество  $A \subseteq \Lambda$  называется подкольцом  $\Lambda$ , если оно замкнуто относительно действий в  $\Lambda$ . Это значит, что для всяких  $a, b \in A$  их сумма  $a + b$ , разность  $a - b$  и произведение  $ab$  принадлежат  $A$ . Ясно, что любое подкольцо само является кольцом; если кольцо  $\Lambda$  коммутативно и ассоциативно, то и любое его подкольцо коммутативно и ассоциативно. Если кольцо  $\Lambda$  является кольцом с единицей 1, и 1 принадлежит подкольцу, то подкольцо – тоже кольцо с единицей.

Пусть  $\Lambda$  – ассоциативное кольцо с единицей 1. Для элемента  $t \in \Lambda$  определим по индукции его степени  $t^i$  с показателем  $i \in \mathbb{N}_0$ . Положим  $t^0 = 1$ ; если элемент

$t^i$  уже определен, то положим  $t^{i+1} = t^i t$ . Индукцией по  $j$  легко доказать, что  $t^i t^j = t^{i+j}$  для любых  $i, j \in \mathbb{N}_0$ . Действительно,  $t^i t^0 = t^i \cdot 1 = t^i = t^{i+0}$ . Если уже доказано, что  $t^i t^j = t^{i+j}$ , то

$$t^i t^{j+1} = t^i (t^j t) = (t^i t^j) t = t^{i+j} t = t^{(i+j)+1} = t^{i+(j+1)}.$$

Пусть  $\Lambda$  – коммутативное ассоциативное кольцо с единицей,  $A$  – подкольцо  $\Lambda$ , содержащее единицу 1 кольца  $\Lambda$ , а  $t$  – элемент из  $\Lambda$ . Мы говорим,  $\Lambda$  является кольцом многочленов от  $t$  над кольцом  $A$  и пишем  $\Lambda = A[t]$ , если любой элемент  $f \in \Lambda$  однозначно представляется в виде  $f = \sum_{i=0}^{\infty} a_i t^i$ , где  $a_i$  – элементы из  $A$ , почти все (т.е. все, кроме конечного числа) равные 0, так что на самом деле предыдущая сумма конечна. Однозначно определенные элементы  $a_i$  называются коэффициентами многочлена  $f$ .

Из этого определения не ясно, для всякого ли кольца существует кольцо многочленов над ним. Ниже мы докажем, что это так: для любого ассоциативного коммутативного кольца с единицей  $A$  существует кольцо  $\Lambda \supseteq A$  и элемент  $t \in \Lambda$ , такие что  $\Lambda = A[t]$ . Но сначала мы построим более широкое кольцо, а затем выберем в нем подкольцо, являющееся кольцом многочленов над  $A$ .

**Кольцо формальных степенных рядов.** Пусть  $A$  – коммутативное ассоциативное кольцо с единицей 1. Обозначим через  $A[[t]]$  множество всех бесконечных последовательностей  $(a_0, a_1, a_2, \dots)$  элементов из  $A$ . Если  $f = (a_0, a_1, a_2, \dots) \in A[[t]]$  – такая последовательность, то через  $f_{[i]}$  будем обозначать ее  $i$ -ю компоненту  $a_i$ ; это будет удобно, если элемент из  $A[[t]]$  обозначается не одной буквой  $f$ , а более сложным сочетанием знаков (например,  $f(g+h)$ ). Определим на  $A[[t]]$  две бинарных алгебраических операции – сложение и умножение, положив для любых  $f, g \in A[[t]]$  и любого  $i \in \mathbb{N}_0$

$$(f+g)_{[i]} = f_{[i]} + g_{[i]}, \quad (fg)_{[i]} = \sum_{s=0}^i f_{[s]} g_{[i-s]} = \sum_{\substack{p+q=i \\ p, q \geq 0}} f_{[p]} g_{[q]}.$$

Иными словами, если  $f = (a_0, a_1, a_2, \dots)$ ,  $g = (b_0, b_1, b_2, \dots)$ , то

$$f+g = (a_0+b_0, a_1+b_1, a_2+b_2, \dots), \quad fg = (c_0, c_1, c_2, \dots),$$

где для любого  $i \in \mathbb{N}_0$

$$c_i = \sum_{s=0}^i a_s b_{i-s} = \sum_{\substack{p+q=i \\ p, q \geq 0}} a_p b_q.$$

**Предложение 1.** *Относительно введенных операций  $A[[t]]$  является коммутативным ассоциативным кольцом с 1.*

*Доказательство.* Надо проверить, что выполняются следующие свойства:

- (1)  $f + (g + h) = (f + g) + h$  для любых  $f, g, h \in A[[t]]$  (ассоциативность сложения);
- (2)  $f + g = g + f$  для любых  $f, g \in A[[t]]$  (коммутативность сложения);
- (3) существует такой элемент  $0 \in A[[t]]$ , что  $0 + f = f$  для любого  $f \in A[[t]]$ ;
- (4) для любого  $f \in A[[t]]$  существует такой элемент  $-f \in A[[t]]$ , что  $f + (-f) = 0$ ;
- (5)  $f(gh) = (fg)h$  для любых  $f, g, h \in A[[t]]$  (ассоциативность умножения);
- (6)  $fg = gf$  для любых  $f, g \in A[[t]]$  (коммутативность умножения);
- (7) существует такой элемент  $1 \in A[[t]]$ , что  $1 \cdot f = f$  для любого  $f \in A[[t]]$ ;
- (8)  $f(g+h) = fg + fh$  для любых  $f, g, h \in A[[t]]$  (дистрибутивность умножения относительно сложения).

Действительно, в качестве 0 и 1 возьмем элементы  $(0, 0, 0, \dots)$  и  $(1, 0, 0, \dots)$  из  $A[[t]]$ , а для элемента  $f = (a_0, a_1, a_2, \dots)$  положим  $-f = (-a_0, -a_1, -a_2, \dots)$ . Пользуясь тем, что  $A$  – коммутативное ассоциативное кольцо с 1, для любого индекса  $i \in \mathbb{N}_0$  получаем:

$$\begin{aligned}
(1) \quad & (f + (g + h))_{[i]} = f_{[i]} + (g + h)_{[i]} = f_{[i]} + (g_{[i]} + h_{[i]}) = (f_{[i]} + g_{[i]}) + h_{[i]} = \\
& = (f + g)_{[i]} + h_{[i]} = ((f + g) + h)_{[i]}; \\
(2) \quad & (f + g)_{[i]} = f_{[i]} + g_{[i]} = g_{[i]} + f_{[i]} = (g + f)_{[i]}; \\
(3) \quad & (0 + f)_{[i]} = 0_{[i]} + f_{[i]} = 0 + f_{[i]} = f_{[i]}; \\
(4) \quad & (f + (-f))_{[i]} = f_{[i]} + (-f)_{[i]} = f_{[i]} + (-f_{[i]}) = 0 = 0_{[i]}; \\
(5) \quad & ((fg)h)_{[i]} = \sum_{s+r=i} (fg)_{[s]} h_{[r]} = \sum_{s+r=i} \left( \sum_{p+q=s} f_{[p]} g_{[q]} \right) h_{[r]} = \\
& = \sum_{s+r=i} \sum_{p+q=s} (f_{[p]} g_{[q]}) h_{[r]} = \sum_{p+q+r=i} f_{[p]} (g_{[q]} h_{[r]}) = \sum_{p+u=i} \sum_{q+r=u} f_{[p]} (g_{[q]} h_{[r]}) = \\
& = \sum_{p+u=i} f_{[p]} \sum_{q+r=u} (g_{[q]} h_{[r]}) = \sum_{p+u=i} f_{[p]} (gh)_{[u]} = (f(gh))_{[i]}; \\
(6) \quad & (fg)_{[i]} = \sum_{p+q=i} f_{[p]} g_{[q]} = \sum_{q+p=i} g_{[q]} f_{[p]} = (gf)_{[i]}; \\
(7) \quad & (1 \cdot f)_{[i]} = \sum_{p+q=i} 1_{[p]} f_{[q]} = f_{[i]}; \\
(8) \quad & ((f + g)h)_{[i]} = \sum_{p+q=i} (f + g)_{[p]} h_{[q]} = \sum_{p+q=i} (f_{[p]} h_{[q]} + g_{[p]} h_{[q]}) = \\
& = \sum_{p+q=i} f_{[p]} h_{[q]} + \sum_{p+q=i} g_{[p]} h_{[q]} = (fh)_{[i]} + (gh)_{[i]} = (fh + gh)_{[i]}
\end{aligned}$$

(все индексы  $p, q, r, s, t$ , участвующие в формулах, – целые неотрицательные числа).

Эти выкладки почти не нуждаются в комментариях; поясним только две из них. Поскольку  $1_{[0]} = 1$ ,  $1_{[p]} = 0$  при  $p \neq 0$ , в сумме из (7) остается только одно ненулевое слагаемое  $1_{[0]} f_{[i]} = f_{[i]}$ . Чуть больше надо сказать о выкладке (5). При переходе от третьего выражения к четвертому мы пользуемся дистрибутивностью умножения относительно сложения в кольце  $A$ : произведение суммы на элемент равно сумме произведений слагаемых на этот элемент. При следующем переходе мы делаем два преобразования. Каждое слагаемое двойной суммы зависит от индексов  $p, q, r$ , таких что  $p + q = s$ ,  $s + r = i$ ; исключая  $s$ , мы находим, что складываются выражения, отвечающие всем наборам индексов  $p, q, r$ , таким что  $p + q + r = i$ . Кроме того, в этом же преобразовании мы, пользуясь ассоциативностью умножения в  $A$ , заменяем произведение  $(f_{[p]} g_{[q]}) h_{[r]}$  на произведение  $f_{[p]} (g_{[q]} h_{[r]})$ . Дальнейшая выкладка – "обратный ход": мы делаем аналогичные преобразования в обратном порядке.

Обозначим через  $t$  элемент  $(0, 1, 0, \dots)$  построенного кольца  $A[[t]]$ . Это кольцо называется кольцом формальных степенных рядов над  $A$  от одной переменной  $t$ , и обычно его элементы  $f = (a_0, a_1, a_2, \dots)$  записываются в виде  $f = \sum_{i=0}^{\infty} a_i t^i$ . Подчеркнем, что это только другая форма записи элемента  $f$ : сумма бесконечного числа слагаемых не имеет смысла, и знак суммы в этом выражении является лишь графическим знаком, не несущим содержательного смысла.

Элементы из кольца  $A$  мы будем рассматривать как элементы из  $A[[t]]$ , отождествив  $a \in A$  с последовательностью  $(a, 0, 0, \dots) \in A[[t]]$  (мы уже сделали это выше для 0 и 1). Такое отождествление не приведет к противоречиям: действия над элементами  $a, b \in A$ , рассматриваемыми как элементы из  $A$  и как элементы из  $A[[t]]$ , приводят к одинаковым результатам:

$$\begin{aligned}
(a, 0, 0, \dots) + (b, 0, 0, \dots) &= (a + b, 0, 0, \dots), \\
(a, 0, 0, \dots)(b, 0, 0, \dots) &= (ab, 0, 0, \dots).
\end{aligned}$$

Кроме того, при таком отождествлении кольцо  $A$  не "сжимается": разные элементы  $A$  остаются различными и в  $A[[t]]$ . Таким образом, кольцо  $A$  является подкольцом кольца формальных степенных рядов  $A[[t]]$ .

**Построение кольца многочленов.** Выделим в кольце формальных степенных рядов  $A[[t]]$  подкольцо, которое окажется кольцом многочленов от  $t$  над кольцом  $A \subset A[[t]]$ . Пусть  $\Lambda \subset A[[t]]$  – множество всех элементов  $(a_0, a_1, a_2, \dots) \in A[[t]]$ , таких что  $a_i = 0$  почти для всех  $i$  (т.е. для всех  $i$ , кроме конечного числа). Легко проверить, что сумма разность и произведение элементов из  $\Lambda$  снова принадлежат  $\Lambda$ . Действительно, если  $f = (a_0, a_1, a_2, \dots)$  и  $g = (b_0, b_1, b_2, \dots)$  принадлежат  $\Lambda$ , то лишь конечное число элементов  $a_i, b_j$  отличны от 0, а поэтому отличаются от 0 лишь конечное число сумм  $a_i + b_i$ , разностей  $a_i - b_i$ , произведений  $a_p b_q$ , а вместе с последними – и сумм  $\sum_{p+q=i} a_p b_q$ . Но это и значит, что почти все компоненты  $(f \pm g)_{[i]}, (fg)_{[i]}$  суммы, разности и произведения элементов  $f$  и  $g$  равны 0, т.е.  $f \pm g, fg \in \Lambda$ . Таким образом,  $\Lambda$  – подкольцо  $A[[t]]$ .

**Лемма 1.** Пусть  $a_0, a_1, a_2, \dots$  – элементы из  $A$ , почти все равные 0. Тогда конечная сумма  $\sum_{i=0}^{\infty} a_i t^i$  равна элементу  $(a_0, a_1, a_2, \dots)$  кольца  $A[[t]]$ .

**Доказательство.** Сначала индукцией по  $i$  докажем, что  $(t^i)_{[i]} = 1$  и  $(t^i)_{[j]} = 0$  при  $j \neq i$ , т.е.

$$t^i = (0, 0, \dots, 0, 1, 0, \dots),$$

причем единственной единице в этой последовательности предшествуют  $i$  нулей. Действительно,  $t^0 = 1 = (1, 0, 0, \dots)$ . Если  $i > 0$  и для  $t^{i-1}$  утверждение уже доказано, то  $(t^i)_{[j]} = (t^{i-1}t)_{[j]} = \sum_{p+q=j} (t^{i-1})_{[p]} t_{[q]}$ . Но  $(t^{i-1})_{[p]} \neq 0$  и  $t_{[q]} \neq 0$  лишь при  $p = i - 1$  и  $q = 1$ , а значит, при  $j = p + q = (i - 1) + 1 = i$ . Итак,  $(t^i)_{[j]} = 0$  при  $j \neq i$ , а  $(t^i)_{[i]} = (t^{i-1})_{[i-1]} t_{[1]} = 1 \cdot 1 = 1$ .

Далее, покажем, что  $a_i t^i = (0, \dots, 0, a_i, 0, \dots)$ , где элементу  $a_i$  предшествуют  $i$  нулей. В самом деле,  $(a_i t^i)_{[j]} = \sum_{p+q=j} (a_i)_{[p]} (t^i)_{[q]}$ ; но  $(a_i)_{[p]}$  и  $(t^i)_{[q]}$  отличны от 0 лишь при  $p = 0, q = i$ , а значит, при  $j = p + q = 0 + i = i$ . Значит,  $(a_i t^i)_{[j]} = 0$  при  $j \neq i$ , а  $(a_i t^i)_{[i]} = (a_i)_{[0]} (t^i)_{[i]} = a_i \cdot 1 = a_i$ .

Теперь утверждение леммы становится очевидным: для любого  $j$  ненулевую  $j$ -ю компоненту имеет только слагаемое  $a_j t^j$  суммы  $\sum_{i=0}^{\infty} a_i t^i$ , и эта компонента равна  $a_j$ ; поэтому  $a_j$  является  $j$ -й компонентой суммы, и, таким образом,

$$\sum_{i=0}^{\infty} a_i t^i = (a_0, a_1, a_2, \dots).$$

**Теорема 1.** Кольцо  $\Lambda$  является кольцом многочленов от  $t$  над кольцом  $A$ .

**Доказательство.** Ясно, что  $A \subset \Lambda$ ; лемма 1 показывает, что всякий элемент  $f \in \Lambda$  представляется в виде  $f = \sum_{i=0}^{\infty} a_i t^i$ , где  $a_i$  – элементы из  $A$ , почти все равные 0, и это представление единственно, потому что коэффициенты  $a_i$  однозначно определяются элементом  $f$  (а именно,  $a_i = f_{[i]}$ ). Итак, построенное нами кольцо  $\Lambda$  – это кольцо многочленов от  $t$  над  $A$ .

**Старший член и степень многочлена.** Многочлен вида  $at^i$ , где  $a \in A, i \geq 0$ , называется одночленом; если  $a \neq 0$ , то число  $i$  называется степенью одночлена  $at^i$ . Легко видеть, что сумма одночленов одной и той же степени либо является одночленом той же степени, либо равна 0.

По определению, всякий ненулевой многочлен  $f(t) \in A[t]$  является суммой конечного числа одночленов попарно различных степеней; тот из них, который имеет наибольшую степень, называется старшим членом многочлена. Очевидно, что если к одночлену  $at^n$  прибавить сумму нескольких одночленов, степени которых строго меньше, чем степень одночлена  $at^n$ , но не обязательно попарно различны, то все равно  $at^n$  будет старшим членом получившегося многочлена.

Степенью ненулевого многочлена  $f(t)$  называется степень его старшего члена; она обозначается  $\deg f(t)$ . Таким образом, если  $f(t) \in A[t]$  – ненулевой многочлен, и его степень  $\deg f(t)$  равна  $n$ , то  $f(t) = a_0 + a_1t + \dots + a_nt^n$ , где  $a_0, a_1, \dots, a_n \in A$ ,  $a_n \neq 0$ ; при этом одночлен  $a_nt^n$  является старшим членом многочлена  $f(t)$ . Коэффициент  $a_n$  старшего члена  $a_nt^n$  многочлена  $f(t)$  называется старшим коэффициентом многочлена  $f(t)$ .

Дополним это определение, приписав нулевому многочлену степень  $-\infty$ . Мы будем считать, что символ  $-\infty$  обладает такими свойствами: для любого  $n \in \mathbb{N}_0$

$$-\infty < n, \quad -\infty + n = -\infty + (-\infty) = -\infty.$$

Следующее простое утверждение обычно называют теоремой о старшем члене произведения многочленов.

**Предложение 2.** Пусть  $f(t), g(t) \in A[t]$  – ненулевые многочлены, и пусть  $a_mt^m, b_nt^n$  – их старшие члены (здесь  $a_m, b_n$  – элементы из  $A$ ). Тогда произведение  $f(t)g(t)$  является суммой  $a_mb_nt^{m+n}$  и нескольких одночленов, степень каждого из которых меньше, чем  $m+n$ . Если  $a_mb_n \neq 0$ , то произведение  $a_mb_nt^{m+n} = (a_mt^m)(b_nt^n)$  старших членов многочленов  $f(t), g(t)$  является старшим членом произведения  $f(t)g(t)$ .

*Доказательство.* Пусть  $f(t) = a_0 + a_1t + \dots + a_mt^m, g(t) = b_0 + b_1t + \dots + b_nt^n$ . Для того, чтобы сосчитать их произведение, надо выбрать по одному слагаемому в каждом сомножителе, перемножить эти слагаемые и затем сложить все получившиеся произведения. Таким образом,  $f(t)g(t)$  является суммой произведений  $a_ib_jt^{i+j}$ , где  $0 \leq i \leq m, 0 \leq j \leq n$ . Если  $i < m$  или  $j < n$ , то произведение  $a_ib_jt^{i+j}$  или равно нулю, или является одночленом, степень  $i+j$  которого строго меньше, чем  $m+n$ . Поэтому  $f(t)g(t)$  является суммой  $a_mb_nt^{m+n}$  и нескольких одночленов, степень каждого из которых меньше, чем  $m+n$ . Последнее утверждение предложения очевидно.

**Предложение 3.** Пусть  $A$  – коммутативное ассоциативное кольцо с 1.

(1) Степень суммы и разности двух многочленов из  $A[t]$  не превосходит максимальной из степеней этих многочленов. Если степени многочленов различны, то степень их суммы и разности равна максимальной из степеней этих многочленов.

(2) Степень произведения двух многочленов из  $A[t]$  не превосходит суммы их степеней. Если  $A$  – область целостности (в частности, если  $A$  – поле), то степень произведения многочленов из  $A[t]$  равна сумме степеней сомножителей.

*Доказательство.* Утверждение (1) очевидно; докажем (2). Если хотя бы один из сомножителей является нулевым многочленом, то и произведение равно 0, и утверждение верно, так как  $-\infty + n = -\infty$  для любого  $n \in \mathbb{N}_0$  или  $n = -\infty$ . Если же оба многочлена отличны от 0, то утверждения пункта (2) непосредственно вытекают из предложения 2.

**Следствие.** Если  $A$  – область целостности, то  $A[t]$  – тоже область целостности.

*Доказательство.* Если  $f(t), g(t) \in A[t]$ ,  $f(t)g(t) = 0$ , то по предложению 3, (2)  $-\infty = \deg f(t)g(t) = \deg f(t) + \deg g(t)$ , а это возможно лишь если  $\deg f(t) = -\infty$  или  $\deg g(t) = -\infty$ , т.е. если  $f(t) = 0$  или  $g(t) = 0$ .

### 3. КОЛЬЦО МНОГОЧЛЕНОВ НАД ПОЛЕМ

*Деление с остатком для многочленов.* В этом параграфе мы увидим, что кольцо многочленов над полем во многом похоже на кольцо целых чисел. Всюду в нем  $k$  – некоторое поле, и мы не всегда будем напоминать об этом в формулировках утверждений. Одну общую черту колец  $\mathbb{Z}$  и  $k[t]$  мы уже знаем: в обоих случаях элементом сопоставляется некоторая "величина", являющаяся натуральным числом: для  $\mathbb{Z}$  это абсолютная величина числа, а для  $k[t]$  – степень многочлена. Наличие такой "величины" позволяет продолжить аналогию между этими кольцами.

**Теорема 1 (о делении с остатком для многочленов).** Пусть  $f(t), g(t)$  – многочлены над полем  $k$ , причем  $g(t) \neq 0$ . Тогда существуют единственные многочлены  $q(t), r(t) \in k[t]$ , такие что  $f(t) = g(t)q(t) + r(t)$  и  $\deg r(t) < \deg g(t)$ . Многочлен  $q(t)$  называется неполным частным, а многочлен  $r(t)$  – остатком от деления  $f(t)$  на  $g(t)$ .

*Доказательство.* Если  $\deg g(t) = 0$ , то  $g(t) = b \in k$ ,  $b \neq 0$ , и потому существует элемент  $b^{-1} \in k \subset k[t]$ ; тогда  $f(t) = b(b^{-1}f(t)) + 0$ , и многочлены  $b^{-1}f(t)$ ,  $0$  являются соответственно неполным частным и остатком от деления  $f(t)$  на  $g(t)$ .

Пусть теперь  $m = \deg g(t) > 0$ ; существование неполного частного и остатка будем доказывать индукцией по степени  $n$  многочлена  $f(t)$ . Если  $n < m$ , то  $f(t) = g(t) \cdot 0 + f(t)$ , и многочлены  $0, f(t)$  являются соответственно неполным частным и остатком от деления  $f(t)$  на  $g(t)$ . Пусть  $n \geq m$  и пусть существование неполного частного и остатка от деления на  $g(t)$  уже установлено для всех многочленов, степень которых меньше  $n$ .

Пусть  $a_n t^n$  и  $b_m t^m$  – старшие члены многочленов  $f(t)$  и  $g(t)$ ; разделив первый из них на второй, получим многочлен  $\frac{a_n}{b_m} t^{n-m}$ , который, как мы увидим, является старшим членом неполного частного. Степени всех одночленов, входящих в разности  $f(t) - a_n t^n$ ,  $\frac{a_n}{b_m} t^{n-m} g(t) - a_n t^n = \frac{a_n}{b_m} t^{n-m} (g(t) - b_m t^m)$ , строго меньше  $n$ , поэтому степень многочлена

$$f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} g(t) = (f(t) - a_n t^n) - \left( \frac{a_n}{b_m} t^{n-m} g(t) - a_n t^n \right)$$

тоже меньше  $n$ . По индукционному предположению, существуют многочлены  $q_1(t), r(t) \in k[t]$ , такие что  $f_1(t) = g(t)q_1(t) + r(t)$  и  $\deg r(t) < \deg g(t)$ ; при этом ясно, что степень многочлена  $q_1(t)$  меньше, чем  $n - m$ . Тогда получаем:

$$\begin{aligned} f(t) &= f_1(t) + \frac{a_n}{b_m} t^{n-m} g(t) = g(t)q_1(t) + r(t) + \frac{a_n}{b_m} t^{n-m} g(t) = \\ &= g(t) \left( \frac{a_n}{b_m} t^{n-m} + q_1(t) \right) + r(t), \end{aligned}$$

и мы видим, что многочлены  $q(t) = \frac{a_n}{b_m} t^{n-m} + q_1(t)$  и  $r(t)$  являются неполным частным и остатком от деления  $f(t)$  на  $g(t)$ .

Осталось доказать единственность неполного частного и остатка. Пусть  $q'(t), r'(t)$  – еще одна пара многочленов, обладающая свойствами  $f(t) = g(t)q'(t) + r'(t)$  и  $\deg r'(t) < \deg g(t)$ . Тогда  $r(t) - r'(t) = g(t)(q'(t) - q(t))$ , откуда следует, что

$$\deg g(t) > \deg(r(t) - r'(t)) = \deg g(t) + \deg(q'(t) - q(t)),$$

т.е.  $\deg(q'(t) - q(t)) < 0$ , а это возможно только если  $q'(t) - q(t) = 0$ . Итак,  $q'(t) = q(t)$ , а тогда  $r'(t) = f(t) - g(t)q'(t) = f(t) - g(t)q(t) = r(t)$ .

**Замечание.** Предыдущее доказательство теоремы о делении с остатком является конструктивным: оно указывает алгоритм, позволяющий найти неполное частное и остаток от деления  $f(t)$  на  $g(t)$ . В самом деле, из него следует, что старший член неполного частного равен отношению старших членов многочленов  $f(t)$  и  $g(t)$ . Вычитая из  $f(t)$  произведение полученного старшего члена неполного частного и  $g(t)$ , получаем многочлен  $f_1(t)$  меньшей, чем  $f(t)$  степени. Применяем к нему ту же процедуру, находим следующий по старшинству член неполного частного, который равен отношению старших членов многочленов  $f_1(t)$  и  $g(t)$ . Продолжая этот процесс до тех пор, пока не получим многочлен, степень которого меньше степени  $f(t)$ ; это и будет искомый остаток.

**Идеалы кольца многочленов.** При построении теории делимости в кольце целых чисел  $\mathbb{Z}$  важную роль сыграло то, что все идеалы кольца  $\mathbb{Z}$  главные. То же оказывается верным и для кольца многочленов над полем.

**Теорема 2.** Всякий идеал кольца многочленов  $k[t]$  над полем  $k$  является главным.

**Доказательство.** Пусть  $I$  – идеал кольца  $k[t]$ . Нулевой многочлен  $0$  всегда принадлежит идеалу. Если идеал  $I$  состоит только из  $0$ , то  $I = (0)$ , и все доказано. Пусть в  $I$  есть ненулевой элемент  $g(t)$ ; тогда множество чисел  $n \in \mathbb{N}_0$ , таких что в  $I$  есть многочлены степени  $n$ , непусто, и в нем есть наименьшее число  $m$ . Пусть  $g(t)$  – какой-то многочлен степени  $m$ , принадлежащий идеалу  $I$ . Покажем, что  $I = (g(t))$ , чем и завершим доказательство теоремы.

Любой элемент  $f(t) \in (g(t))$  имеет вид  $f(t) = g(t)h(t)$ , где  $h(t) \in k[t]$ ; но многочлен  $g(t)$  принадлежит  $(I)$ , и потому  $f(t) = g(t)h(t) \in I$ . Итак,  $(g(t)) \subseteq I$ . Обратно, пусть  $f(t) \in I$ ; разделим  $f(t)$  с остатком на  $g(t)$ :  $f(t) = g(t)q(t) + r(t)$ , где  $q(t), r(t) \in k[t]$  и  $\deg r(t) < \deg g(t)$ . Если  $r(t) \neq 0$ , то  $r(t) = f(t) - g(t)q(t)$  принадлежит идеалу  $I$ , так как  $f(t)$  и  $g(t)$  оба принадлежат  $I$ ; но  $\deg r(t) < \deg g(t) = m$ , а это противоречит тому, что  $m$  – наименьшая из степеней ненулевых многочленов, принадлежащих идеалу  $I$ . Итак,  $r(t) = 0$ , и  $f(t) = g(t)q(t) \in (g(t))$ . Таким образом, доказано и обратное включение  $I \subseteq (g(t))$ .

**Делители 1 и ассоциированные элементы в кольце многочленов.** Из сказанного выше следует, что к кольцу многочленов можно применить все утверждения теории делимости, доказанные в главе I для областей целостности, в которых все идеалы главные. Однако, некоторые понятия делимости имеют в кольце многочленов более наглядное описание.

**Предложение 1.** Для того, чтобы многочлен  $f(t)$  над полем  $k$  был делителем 1 в кольце  $k[t]$ , необходимо и достаточно, чтобы  $\deg f(t) = 0$ , т.е. чтобы  $f(t) = c$ , где  $c \in k \subset k[t]$ ,  $c \neq 0$ .

**Доказательство.** Если  $1 \div f(t)$ , то существует многочлен  $g(t) \in k[t]$ , такой что  $1 = f(t)g(t)$ ; тогда  $0 = \deg 1 = \deg f(t) + \deg g(t)$ . С другой стороны, ясно, что  $f(t) \neq 0$ ,  $g(t) \neq 0$ , поэтому  $\deg f(t) \geq 0$ ,  $\deg g(t) \geq 0$ . Следовательно,  $\deg f(t) = \deg g(t) = 0$ . Обратное утверждение очевидно: если  $f(t) = c \neq 0$ , то, поскольку  $k$  – поле, существует элемент  $c^{-1} \in k \subset k[t]$ , и  $1 = cc^{-1} = f(t)c^{-1} \div f(t)$ .

Прежде, чем сформулировать следующее утверждение, дадим определение, которое часто оказывается полезным при работе с многочленами. Ненулевой многочлен  $f(t)$  называется унитарным (по другой терминологии – нормализованным), если его старший коэффициент равен 1.

**Предложение 2.** Если ненулевые многочлены  $f(t)$ ,  $g(t)$  над полем  $k$  ассоциированы и унитарны, то они равны.



*Доказательство.* Поскольку  $f(t) \sim g(t)$ , существует ненулевой элемент  $c$  из поля  $k$ , такой что  $f(t) = cg(t)$ . По теореме о старшем члене произведения старший коэффициент 1 унитарного многочлена  $f(t)$  равен произведению  $c \cdot 1$  старших коэффициентов многочлена  $c$  и унитарного многочлена  $g(t)$ , и потому  $c = 1$ , т.е.  $f(t) = g(t)$ .

Отметим еще следующее утверждение, которое тоже немедленно следует из теоремы о старшем члене произведения многочленов.

**Предложение 3.** *Произведение унитарных многочленов – тоже унитарный многочлен.*

**Предложение 4.** *Для того, чтобы ненулевые многочлены  $f(t)$ ,  $g(t)$  над полем  $k$  были ассоциированы, необходимо и достаточно, чтобы существовал такой элемент  $c \in k$ ,  $c \neq 0$ , что  $g(t) = c(f(t))$ . Для каждого ненулевого многочлена  $f(t) \in k[t]$  существует единственный ассоциированный с ним унитарный многочлен.*

*Доказательство.* Мы знаем, что элементы из области целостности ассоциированы тогда и только тогда, когда они отличаются множителем, являющимся делителем 1; поэтому первое утверждение сразу следует из предложения 1. Если  $a_n$  – старший коэффициент ненулевого многочлена  $f(t)$ , то  $a_n \neq 0$ , и многочлен  $a_n^{-1}f(t)$  унитарен и ассоциирован с  $f(t)$ . Осталось заметить, что ассоциированные унитарные многочлены совпадают.

*Неприводимые многочлены.* Ненулевые простые элементы кольца многочленов  $k[t]$  называются неприводимыми над полем  $k$  многочленами. Таким образом, многочлен  $f(t) \in k[t]$  называется неприводимым над  $k$ , если  $f(t) \neq 0$ ,  $f(t)$  – не делитель 1, и во всяком его разложении  $f(t) = g(t)h(t)$  один из сомножителей является делителем 1, т.е. имеет степень 0. Поскольку мы исключаем 0 и делители 1 из числа неприводимых многочленов, степень любого неприводимого многочлена не меньше 1. Если  $f(t)$  – неприводимый многочлен, то всякий его делитель или является делителем 1, или ассоциирован с  $f(t)$ . Если же многочлен  $f(t)$  не равен 0, не является делителем 1 и не является неприводимым многочленом, то существует такое его разложение  $f(t) = g(t)h(t)$ , что степени обоих сомножителей не меньше 1.

**Предложение 5.** *Всякий многочлен степени 1 с коэффициентами из поля неприводим над этим полем.*

*Доказательство.* Пусть  $f(t) \in k[t]$ ,  $\deg f(t) = 1$ . Если  $f(t)$  не является неприводимым многочленом, то существует его разложение  $f(t) = g(t)h(t)$ , в котором оба сомножителя являются многочленами из  $k[t]$ , степени которых не меньше 1. Тогда  $1 = \deg f(t) = \deg g(t) + \deg h(t) \geq 2$ , что невозможно.

*Основная теорема арифметики для многочленов.*

**Теорема 3.** *Пусть  $k$  – поле. Всякий ненулевой многочлен  $f(t) \in k[t]$  может быть представлен в виде произведения  $f(t) = cp_1(t) \dots p_n(t)$ , где  $c \in k$ ,  $c \neq 0$ ,  $n \geq 0$ ,  $p_1(t), \dots, p_n(t)$  – унитарные неприводимые многочлены. Это представление единственно с точностью до порядка сомножителей: если есть другое представление  $f(t) = dq_1(t) \dots q_m(t)$ , где  $d \in k$ ,  $d \neq 0$ ,  $q_1(t), \dots, q_m(t)$  – унитарные неприводимые многочлены, то  $c = d$ ,  $m = n$  и существует подстановка  $\sigma \in S_n$ , такая что  $q_1(t) = p_{\sigma(1)}(t), \dots, q_n(t) = p_{\sigma(n)}(t)$ .*

*Доказательство.* Единственность по существу уже доказана. Если

$$f(t) = cp_1(t) \dots p_n(t) = dq_1(t) \dots q_m(t),$$

где  $c, d \in k$ ,  $c, d \neq 0$ , а  $p_i(t)$ ,  $q_j(t)$  – унитарные неприводимые многочлены, то  $p_1(t) \dots p_n(t) \sim q_1(t) \dots q_m(t)$ , и по предложению 5.1, (6) из главы I  $m = n$  и существует такая подстановка  $\sigma$  множества  $\{1, \dots, n\}$ , что

$$p_{\sigma(1)}(t) \sim q_1(t), \dots, p_{\sigma(n)}(t) \sim q_n(t).$$

Но унитарные многочлены ассоциированы лишь тогда, когда они совпадают, поэтому  $q_1(t) = p_{\sigma(1)}(t), \dots, q_n(t) = p_{\sigma(n)}(t)$ . Остается заметить, что по теореме о старшем члене произведения многочленов элементы  $c, d \in k$  оба равны старшему коэффициенту многочлена  $f(t)$ .

Существование разложения докажем индукцией по степени многочлена  $f(t)$ . Если  $\deg f(t) = 0$ , то  $f(t) = c \in k$ ,  $c \neq 0$ , а это и есть требуемое разложение (при  $n = 0$ ). Пусть  $\deg f(t) > 0$  и для всех многочленов меньших степеней существование разложения уже доказано. Если  $f(t)$  – неприводимый многочлен, а  $a$  – его старший коэффициент, то многочлен  $p(t) = a^{-1}f(t)$  унитарен и тоже неприводим, а тогда  $f(t) = ap(t)$  и есть нужное представление. Пусть теперь многочлен  $f(t)$  не является неприводимым; тогда существует разложение  $f(t) = g(t)h(t)$ , в котором степени обоих сомножителей больше 0. Тогда

$$\deg g(t) = \deg f(t) - \deg h(t) < \deg f(t),$$

и точно так же  $\deg h(t) < \deg f(t)$ . По предположению индукции, существуют ненулевые элементы  $d_1, d_2 \in k$  и неприводимые унитарные многочлены

$$p_1(t), \dots, p_m(t); \quad p_{m+1}(t), \dots, p_n(t),$$

такие что  $g(t) = d_1 p_1(t) \dots p_m(t)$ ,  $h(t) = d_2 p_{m+1}(t) \dots p_n(t)$ . Но тогда

$$f(t) = (d_1 d_2) p_1(t) \dots p_m(t) p_{m+1}(t) \dots p_n(t),$$

а это и есть нужное разложение.

Разложение, существование и единственность которого утверждаются только что доказанной теоремой, называется каноническим разложением многочлена в произведение унитарных неприводимых многочленов.

*Кольцо вычетов по модулю многочлена.* В предыдущей главе для любого коммутативного ассоциативного кольца с единицей  $A$  и любого элемента  $n \in A$  было построено кольцо вычетов  $A/(n)$  по модулю  $n$ . Напомним, что элементами этого кольца являются классы вычетов, т.е. такие подмножества  $\alpha$  множества  $A$ , в которых найдется элемент  $a$ , обладающий следующим свойством:  $\alpha$  совпадает с множеством  $[a]_n$  всех элементов кольца  $A$ , которые сравнимы с  $a$  по модулю  $n$ .

Опишем явно множество классов вычетов для случая  $A = k[t]$ . Пусть  $f(t) \in k[t]$  – многочлен степени  $n \geq 1$ . отождествим класс вычетов  $[a]_{f(t)}$ , определяемый элементом  $a \in k$ , с самим элементом  $a$ . Таким образом, поле  $k$  оказывается естественным образом вложенным в кольцо вычетов  $k[t]/(f(t))$ . Поскольку, очевидно,  $[a]_{f(t)} \pm [b]_{f(t)} = [a \pm b]_{f(t)}$ ,  $[a]_{f(t)}[b]_{f(t)} = [ab]_{f(t)}$  для любых  $a, b \in k$ , это вложение не нарушает действий: будем ли мы производить действия над элементами из  $k$  в самом поле  $k$  или в кольце вычетов  $k[t]/(f(t))$ , результат будет один и тот же.

**Предложение 6.** Пусть  $k$  поле, и пусть  $f(t)$  – многочлен степени  $n \geq 1$  с коэффициентами из  $k$ . Всякий класс из кольца вычетов  $k[t]$  по модулю  $f(t)$  единственным образом представим в виде

$$a_0 + a_1[t]_{f(t)} + a_2([t]_{f(t)})^2 + \dots + a_{n-1}([t]_{f(t)})^{n-1},$$

где  $a_0, a_1, a_2, \dots, a_{n-1}$  – элементы поля  $k$ .

*Доказательство.* В дальнейшем мы опускаем указание на модуль  $f(t)$  в обозначении класса вычетов по этому модулю и пишем  $[g(t)]$  вместо  $[g(t)]_{f(t)}$ . Пусть  $[h(t)]$  – произвольный класс вычетов из  $k[t]/(f(t))$  (здесь  $h(t)$  – многочлен из  $k[t]$ ), и пусть  $r(t) = a_0 + a_1 t + \dots + a_{n-1} t^{n-1}$  – остаток от деления  $h(t)$  на  $f(t)$ . Тогда

$h(t) - r(t) = f(t)q(t) \div f(t)$ , где  $q(t)$  – неполное частное, и потому  $h(t) \equiv r(t) \pmod{f(t)}$ . Следовательно,

$$\begin{aligned} [h(t)] &= [r(t)] = [a_0 + a_1t + \cdots + a_{n-1}t^{n-1}] = \\ &= [a_0] + [a_1][t] + \cdots + [a_{n-1}][t]^{n-1} = a_0 + a_1[t] + \cdots + a_{n-1}[t]^{n-1}. \end{aligned}$$

Докажем теперь единственность представления. Пусть

$$a_0 + a_1[t] + \cdots + a_{n-1}[t]^{n-1} = b_0 + b_1[t] + \cdots + b_{n-1}[t]^{n-1},$$

и пусть  $c_i = a_i - b_i$  ( $0 \leq i < n$ ); тогда

$$\begin{aligned} [0] &= c_0 + c_1[t] + \cdots + c_{n-1}[t]^{n-1} = [c_0] + [c_1][t] + \cdots + [c_{n-1}][t]^{n-1} = \\ &= [c_0 + c_1t + \cdots + c_{n-1}t^{n-1}], \end{aligned}$$

откуда следует, что многочлен  $c_0 + c_1t + \cdots + c_{n-1}t^{n-1}$  делится на многочлен  $f(t)$  степени  $n$ , а это возможно только если  $c_0 = c_1 = \cdots = c_{n-1} = 0$ , т.е.  $a_0 = b_0$ ,  $a_1 = b_1, \dots, a_{n-1} = b_{n-1}$ .

*Условие того, что кольцо вычетов по модулю многочлена – поле.* Хотя критерий того, что кольцо вычетов по модулю был сформулирован и доказан для произвольных областей целостности, в которых все идеалы главные, повторим его еще раз для случая кольца многочленов.

**Теорема 4.** Пусть  $k$  – поле, и пусть  $f(t)$  – ненулевой многочлен с коэффициентами из поля  $k$ . Кольцо вычетов  $k[t]/(f(t))$  тогда и только тогда является полем, когда многочлен  $f(t)$  неприводим.

#### 4. ПОЛЕ КОМПЛЕКСНЫХ ЧИСЕЛ

*Построение поля комплексных чисел.* Последняя теорема предыдущего параграфа позволяет конструировать новые поля, реализуемые как кольца вычетов кольца многочленов по неприводимому модулю. В этом параграфе мы строим и изучаем одно из таких полей, играющее важнейшую роль во всей математике.

**Лемма 1.** Многочлен  $t^2 + 1$  неприводим в кольце многочленов  $\mathbb{R}[t]$  над полем вещественных чисел  $\mathbb{R}$ .

*Доказательство.* Предположим, что это не так; тогда существует разложение  $t^2 + 1 = p(t)q(t)$ , где  $p(t), q(t) \in \mathbb{R}[t]$ , причем  $\deg p(t) \geq 1, \deg q(t) \geq 1$ . Поскольку  $\deg p(t) + \deg q(t) = \deg(p(t)q(t)) = \deg(t^2 + 1) = 2$ , получаем, что степени обоих многочленов  $p(t), q(t)$  равны 1. Следовательно, существуют такие вещественные числа  $a, b, c, d$ , что  $p(t) = at + b, q(t) = ct + d$ . Имеем равенство:

$$t^2 + 1 = p(t)q(t) = (at + b)(ct + d) = act^2 + (ad + bc)t + bd;$$

сравнивая коэффициенты при одинаковых степенях  $t$  в левой и правой частях этого равенства, получаем соотношения  $ac = bd = 1, ad = -bc$ . Но тогда оказывается, что  $1 = (ac)(bd) = (ad)(bc) = -(bc)^2 \leq 0$ , а это невозможно.

Из этой леммы и теоремы 3.4 следует, что кольцо вычетов  $\mathbb{R}[t]/(t^2 + 1)$  является полем; оно называется полем комплексных чисел и обычно обозначается через  $\mathbb{C}$ .

Обозначим через  $i$  класс вычетов  $[t]_{t^2+1} \in \mathbb{R}[t]/(t^2 + 1) = \mathbb{C}$ . Комплексное число  $i$  называется мнимой единицей; ее основным свойством является то, что ее квадрат равен  $-1$ . Действительно,

$$i^2 = ([t]_{t^2+1})^2 = [t^2]_{t^2+1} = [-1]_{t^2+1} = -1.$$

Далее, по предложению 3.6, любой элемент  $\alpha$  из поля  $\mathbb{C} = \mathbb{R}[t]/(t^2 + 1)$  однозначно представим в виде  $a[t]_{t^2+1} + b[t]_{t^2+1} = a + bi$ , где  $a, b$  – вещественные числа; они называются соответственно вещественной частью и коэффициентом мнимой части комплексного числа  $\alpha$  и обозначаются  $\operatorname{Re} \alpha$  и  $\operatorname{Im} \alpha$ .

Помня, что  $i^2 = -1$ , легко производить вычисления с комплексными числами; в частности, сумма и произведение комплексных чисел  $a+bi$  и  $c+di$  выражаются следующим образом:

$$(a+bi) + (c+di) = (a+c) + (b+d)i,$$

$$(a+bi)(c+di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.$$

**Замечание.** Если комплексное число записано в виде  $a+bi$ , это еще не значит, что  $a$  и  $b$  – вещественная часть и коэффициент при мнимой части, потому что ниоткуда не следует, что числа  $a, b$  вещественны. Поэтому нам каждый раз придется об этом говорить, и у нас постоянно будут встречаться надоедливые фразы вроде такой: пусть  $a+bi$  – комплексное число, где  $a, b \in \mathbb{R}$ .

**Тригонометрическая форма комплексного числа.** Модулем комплексного числа  $\alpha = a+bi$ , где  $a$  и  $b$  вещественны, называется число  $|\alpha| = \sqrt{a^2 + b^2}$ . Модуль всегда является неотрицательным вещественным числом; если  $|\alpha| = 0$ , то  $a^2 + b^2 = 0$ , и потому  $a = b = 0$ , т.е.  $\alpha = a+bi = 0$ .

Пусть  $\alpha = a+bi \in \mathbb{C}$ , причем  $a, b \in \mathbb{R}$ . Предположим, что модуль  $r = |\alpha|$  числа  $\alpha$  отличен от 0. Тогда  $(a/r)^2 + (b/r)^2 = 1$ , и поэтому существует такое вещественное число  $\varphi$ , что  $a/r = \cos \varphi$ ,  $b/r = \sin \varphi$ . Это число определено не однозначно, а с точностью до слагаемого вида  $2k\pi$ , где  $k$  – целое число; любое из таких чисел  $\varphi$  называется аргументом числа  $\alpha$ . Из самого определения следует, что если  $r$  – модуль, а  $\varphi$  – аргумент числа  $\alpha = a+bi$ , то

$$\alpha = a+bi = r\left(\frac{a}{r} + i\frac{b}{r}\right) = r(\cos \varphi + i \sin \varphi).$$

Если  $\alpha = 0$ , то мы разрешаем любому вещественному числу быть аргументом  $\alpha$ , и снова будет  $\alpha = r(\cos \varphi + i \sin \varphi)$ .

Такое выражение комплексного числа через его модуль и аргумент называется тригонометрической формой комплексного числа  $\alpha$ .

Отметим, что эта связь обратима: если комплексное число  $\alpha$  представлено в виде  $\alpha = r(\cos \varphi + i \sin \varphi)$ , где  $r \geq 0$  и  $\varphi$  – вещественные числа, то  $r = |\alpha|$ , а  $\varphi$  – одно из значений аргумента  $\alpha$ . Действительно, это очевидно. если  $r = 0$ , а при  $r > 0$  пусть  $a = r \cos \varphi$ ,  $b = r \sin \varphi$ , и тогда

$$\alpha = a+bi, |\alpha| = \sqrt{(r \cos \varphi)^2 + (r \sin \varphi)^2} = r, a/r = \cos \varphi, b/r = \sin \varphi,$$

а это и значит, что  $\varphi$  – одно из значений аргумента числа  $\alpha$ .

**Геометрическое изображение комплексных чисел.** Выберем на плоскости декартову систему координат. Поскольку каждое комплексное число  $\alpha$  однозначно представляется в виде  $\alpha = a+bi$ , где  $a, b \in \mathbb{R}$ , естественно сопоставить ему точку на плоскости с декартовыми координатами  $(a, b)$ . Эта точка называется геометрическим изображением комплексного числа  $\alpha$ . Каждая точка плоскости соответствует некоторому комплексному числу. Плоскость, состоящую из изображений всех комплексных чисел, называют комплексной плоскостью, а оси абсцисс и ординат на ней – вещественной и мнимой осями. Модуль и аргумент комплексного числа совпадают с полярными координатами его геометрического изображения в полярной системе координат, начало которой совпадает с началом  $O$  декартовой системой координат, а полярная ось – с положительным лучом вещественной оси.

*Неравенства для модулей суммы и разности комплексных чисел.*

**Теорема 1.** Пусть  $\alpha, \beta \in \mathbb{C}$ . Тогда

$$||\alpha| \pm |\beta|| \leq |\alpha \pm \beta| \leq |\alpha| + |\beta|.$$

*Доказательство.* В формулировке теоремы участвуют 6 неравенств; докажем сначала неравенство  $|\alpha + \beta| \leq |\alpha| + |\beta|$ , а остальные получатся из него в качестве простых следствий. Прежде, чем начать доказательство, сделаем одно простое замечание. Пусть  $x$  и  $y$  – два вещественных числа, причем число  $y$  неотрицательно; тогда из неравенства  $x^2 \leq y^2$  следует, что  $x \leq y$ . Действительно, если  $x < 0$ , то  $x < 0 \leq y$ ; если же число  $x$ , как и  $y$ , неотрицательно, то из неравенства  $y < x$  следовало бы, что  $y^2 < x^2 \leq y^2$ , а это невозможно, и потому  $x \leq y$ .

Поскольку число  $|\alpha| + |\beta|$  неотрицательно, из предыдущего замечания следует, что для доказательства неравенства  $|\alpha + \beta| \leq |\alpha| + |\beta|$  достаточно доказать, что

$$(*) \quad |\alpha + \beta|^2 \leq (|\alpha| + |\beta|)^2 = |\alpha|^2 + |\beta|^2 + 2|\alpha||\beta|.$$

Пусть  $\alpha = a + bi$ ,  $\beta = c + di$ , где  $a, b, c, d \in \mathbb{R}$ ; тогда  $\alpha + \beta = (a + c) + (b + d)i$  и

$$|\alpha + \beta|^2 = (a + c)^2 + (b + d)^2 = a^2 + b^2 + c^2 + d^2 + 2(ac + bd) = |\alpha|^2 + |\beta|^2 + 2(ac + bd),$$

и неравенство  $(*)$  превращается в неравенство  $ac + bd \leq |\alpha||\beta|$ . Но  $|\alpha||\beta| \geq 0$ , поэтому предыдущее неравенство следует из неравенства

$$(ac + bd)^2 \leq |\alpha|^2 |\beta|^2 = (a^2 + b^2)(c^2 + d^2),$$

которое тривиально, потому что

$$\begin{aligned} (a^2 + b^2)(c^2 + d^2) - (ac + bd)^2 &= (a^2 c^2 + a^2 d^2 + b^2 c^2 + b^2 d^2) - (a^2 c^2 + 2abcd + b^2 d^2) = \\ &= a^2 d^2 + b^2 c^2 - 2abcd = (ad - bc)^2 \geq 0. \end{aligned}$$

Для того, чтобы вывести остальные пять неравенств из уже доказанного неравенства  $|\alpha + \beta| \leq |\alpha| + |\beta|$ , заметим, что  $|\alpha| = \sqrt{(-a)^2 + (-b)^2} = \sqrt{a^2 + b^2} = |\alpha|$ , и точно так же  $|\beta| = |\beta|$ ; поэтому

$$\begin{aligned} |\alpha - \beta| &= |\alpha + (-\beta)| \leq |\alpha| + |-\beta| = |\alpha| + |\beta|; \\ |\alpha| &= |(\alpha \pm \beta) + (\mp \beta)| \leq |\alpha \pm \beta| + |\mp \beta| = |\alpha \pm \beta| + |\beta|; \\ |\beta| &= |(\alpha \pm \beta) + (\mp \alpha)| \leq |\alpha \pm \beta| + |\mp \alpha| = |\alpha \pm \beta| + |\alpha|, \end{aligned}$$

а это и суть те неравенства, которые мы хотели получить.

Доказанные соотношения допускают простую геометрическую интерпретацию. Если точки  $A, B, C$  являются геометрическими изображениями комплексных чисел  $\alpha, \beta$  и  $\alpha + \beta$ , то сумма векторов  $\vec{OA}$  и  $\vec{OB}$  равна вектору  $\vec{OC}$ , и потому сумма длин первых двух векторов не меньше, а разность длин – не больше длины третьего. Но это как раз и значит, что  $||\alpha| - |\beta|| \leq |\alpha + \beta| \leq |\alpha| + |\beta|$ .

*Сопряжение для комплексных чисел.* Пусть  $\alpha = a + bi \in \mathbb{C}$ , где  $a, b \in \mathbb{R}$ . Сопряженным к  $\alpha$  называется комплексное число  $a - bi$ ; оно обозначается  $\bar{\alpha}$ .

**Предложение 1.** Пусть  $\alpha, \beta \in \mathbb{C}$ . Тогда

- (1)  $\alpha = \bar{\alpha}$  тогда и только тогда, когда  $\alpha \in \mathbb{R}$ ;
- (2)  $\overline{(\bar{\alpha})} = \alpha$ ;
- (3)  $\alpha \bar{\alpha} = |\alpha|^2$ ;
- (4) если  $\alpha \neq 0$ , то  $\alpha^{-1} = \bar{\alpha}/|\alpha|^2$ ,  $\bar{\alpha}^{-1} = \alpha/|\alpha|^2$ ;
- (5)  $\overline{\alpha \pm \beta} = \bar{\alpha} \pm \bar{\beta}$ ;
- (6)  $\overline{\alpha \beta} = \bar{\alpha} \bar{\beta}$ ;
- (7) если  $\beta \neq 0$ , то  $\overline{\alpha/\beta} = \bar{\alpha}/\bar{\beta}$ .

*Доказательство.* Пусть  $\alpha = a + bi \in \mathbb{C}$ ,  $\beta = c + di$ , где  $a, b, c, d \in \mathbb{R}$ . Тогда

- (1)  $\alpha = \bar{\alpha}$  тогда и только тогда, когда  $0 = \alpha - \bar{\alpha} = (a + bi) - (a - bi) = 2bi$ , т.е.  $bi = 0$  и  $\alpha = a + bi = a \in \mathbb{R}$ ;
- (2)  $\overline{(\bar{\alpha})} = \overline{(a - bi)} = a + bi = \alpha$ ;
- (3)  $\alpha \bar{\alpha} = (a + bi)(a - bi) = a^2 + b^2 = |\alpha|^2$ ;
- (4) если  $\alpha \neq 0$ , то  $|\alpha| \neq 0$  и  $\alpha(\bar{\alpha}/|\alpha|^2) = \bar{\alpha}(\alpha/|\alpha|^2) = (\alpha \bar{\alpha})/|\alpha|^2 = |\alpha|^2/|\alpha|^2 = 1$ ;

$$\begin{aligned}
(5) \quad \overline{\alpha \pm \beta} &= \overline{(a + bi) \pm (c + di)} = \overline{(a \pm c) + (b \pm d)i} = (a \pm c) - (b \pm d)i = \\
&= (a - bi) \pm (c - di) = \overline{\alpha} \pm \overline{\beta}; \\
(6) \quad \overline{\alpha\beta} &= \overline{(a + bi)(c + di)} = \overline{(ac - bd) + (ad + bc)i} = (ac - bd) - (ad + bc)i = \\
&= (a - bi)(c - di) = \overline{\alpha}\overline{\beta}; \\
(7) \quad \overline{\alpha/\beta} &= \overline{\alpha\beta^{-1}} = \overline{\alpha}\overline{\beta^{-1}} = \overline{\alpha}(\overline{\beta}/|\beta|^2) = \overline{\alpha}(\beta/|\beta|^2) = \overline{\alpha}\overline{\beta}^{-1} = \overline{\alpha}/\overline{\beta}.
\end{aligned}$$

*Умножение и деление комплексных чисел в тригонометрической форме.* Пусть  $\alpha = r_1(\cos \varphi_1 + i \sin \varphi_1)$ ,  $\beta = r_2(\cos \varphi_2 + i \sin \varphi_2)$  – два комплексных числа, записанных в тригонометрической форме. Тогда

$$\begin{aligned}
\alpha\beta &= (r_1(\cos \varphi_1 + i \sin \varphi_1))(r_2(\cos \varphi_2 + i \sin \varphi_2)) = \\
&= r_1 r_2 (\cos \varphi_1 \cos \varphi_2 - \sin \varphi_1 \sin \varphi_2) + i(\sin \varphi_1 \cos \varphi_2 + \cos \varphi_1 \sin \varphi_2) = \\
&= r_1 r_2 (\cos(\varphi_1 + \varphi_2) + i \sin(\varphi_1 + \varphi_2)); \\
\frac{\alpha}{\beta} &= \alpha\beta^{-1} = \alpha\overline{\beta}/|\beta|^2 = (r_1(\cos \varphi_1 + i \sin \varphi_1))(r_2(\cos \varphi_2 - i \sin \varphi_2))/r_2^2 = \\
&= \frac{r_1}{r_2} (\cos \varphi_1 \cos \varphi_2 + \sin \varphi_1 \sin \varphi_2) + i(\sin \varphi_1 \cos \varphi_2 - \cos \varphi_1 \sin \varphi_2) = \\
&= \frac{r_1}{r_2} (\cos(\varphi_1 - \varphi_2) + i \sin(\varphi_1 - \varphi_2)).
\end{aligned}$$

Таким образом, при умножении двух комплексных чисел, заданных своими модулями и аргументами, получается комплексное число, для которого произведение модулей сомножителей и сумма их аргументов являются соответственно модулем и аргументом. Аналогично, отношение модулей и разность аргументов служат модулем и аргументом отношения этих комплексных чисел.

Формула для умножения легко переносится при помощи индукции на произведение любого числа сомножителей:

$$\prod_{s=1}^n r_s (\cos \varphi_s + i \sin \varphi_s) = \prod_{s=1}^n r_s (\cos \sum_{s=1}^n \varphi_s + i \sin \sum_{s=1}^n \varphi_s).$$

В частности, если все сомножители одинаковы и их модули равны 1, получаем формулу

$$(\cos \varphi + i \sin \varphi)^n = \cos n\varphi + i \sin n\varphi,$$

которая называется формулой Муавра. Она доказана для любого натурального показателя  $n$ , однако, ее легко обобщить и на случай произвольного целого показателя. Для комплексного числа  $\alpha \neq 0$  и  $n > 0$  положим  $\alpha^{-n} = (\alpha^n)^{-1}$ ; положим также  $\alpha^0 = 1$ . Мы получаем:

$$\begin{aligned}
(\cos \varphi + i \sin \varphi)^0 &= 1 = \cos(0 \cdot \varphi) + i \sin(0 \cdot \varphi), \\
(\cos \varphi + i \sin \varphi)^{-n} &= ((\cos \varphi + i \sin \varphi)^n)^{-1} = (\cos n\varphi + i \sin n\varphi)^{-1} = \\
&= \cos n\varphi - i \sin n\varphi = \cos(-n\varphi) + i \sin(-n\varphi).
\end{aligned}$$

*Экспонента комплексного числа и формулы Эйлера.* Пусть

$$e = \lim_{n \rightarrow \infty} (1 + 1/n)^n = 2,718281828459045...;$$

определим степени  $e$  с комплексными показателями. Для числа  $a + bi \in \mathbb{C}$ , где  $a, b \in \mathbb{R}$ , положим  $e^{a+bi} = e^a(\cos b + i \sin b)$ . Покажем, что так определенная экспонента комплексного числа обладает привычными свойствами показательной функции.

**Предложение 2.** Для любых  $\alpha, \beta \in \mathbb{C}$  и любого целого  $n$  выполняются равенства

$$e^\alpha e^\beta = e^{\alpha+\beta}, \quad (e^\alpha)^n = e^{n\alpha}.$$

*Доказательство.* Пусть  $\alpha = a + bi$ ,  $\beta = c + di$ , где  $a, b, c, d \in \mathbb{R}$ ; тогда, пользуясь правилом умножения комплексных чисел в тригонометрической форме и формулой Муавра, получаем, что

$$\begin{aligned} e^\alpha e^\beta &= (e^a(\cos b + i \sin b))(e^c(\cos d + i \sin d)) = e^{a+c}(\cos(b+d) + i \sin(b+d)) = \\ &= e^{(a+c)+(b+d)i} = e^{\alpha+\beta}, \\ (e^\alpha)^n &= (e^a(\cos b + i \sin b))^n = e^{na}(\cos nb + i \sin nb) = e^{na+nb i} = e^{n\alpha}. \end{aligned}$$

Любое ненулевое комплексное число  $\alpha$  может быть записано в виде экспоненты: если  $r$  и  $\varphi$  – модуль и аргумент  $\alpha$ , то  $\alpha = r(\cos \varphi + i \sin \varphi) = e^{\ln r + i\varphi}$ . Однако, чаще число  $\alpha$  записывается в форме  $\alpha = re^{i\varphi}$ . Такие формы записи комплексного числа "почти единственны" в смысле следующего утверждения

**Предложение 3.** Если  $\alpha, \beta \in \mathbb{C}$  и  $e^\alpha = e^\beta$ , то существует целое число  $k$ , такое что  $\alpha - \beta = 2k\pi i$ . Если  $r_1, r_2 > 0$  и  $\varphi_1, \varphi_2$  – вещественные числа, такие что  $r_1 e^{i\varphi_1} = r_2 e^{i\varphi_2}$ , то  $r_1 = r_2$ , и существует целое число  $k$ , такое что  $\varphi_1 - \varphi_2 = 2k\pi$ .

*Доказательство.* Пусть  $\alpha = a + bi$ ,  $\beta = c + di$ , где  $a, b, c, d \in \mathbb{R}$ ; если  $e^\alpha = e^\beta$ , то

$$e^a(\cos b + i \sin b) = e^\alpha = e^\beta = e^c(\cos d + i \sin d);$$

модули  $e^a$  и  $e^c$  левой и правой частей равны, поэтому  $a = c$ . Далее,  $e^a = e^c \neq 0$ , и мы получаем теперь, что  $\cos b + i \sin b = \cos d + i \sin d$ , т.е.

$$\cos b = \cos d, \quad \sin b = \sin d,$$

а это бывает только тогда, когда  $b - d = 2k\pi$  для некоторого целого  $k$ . Итак,

$$\alpha - \beta = (a + bi) - (c + di) = (b - d)i = 2k\pi i.$$

Второе утверждение – вариант первого; если первое утверждение применить к равенству  $e^{\ln r_1 + i\varphi_1} = e^{\ln r_2 + i\varphi_2}$ , то получим, что для некоторого  $k \in \mathbb{Z}$

$$2k\pi i = (\ln r_1 + i\varphi_1) - (\ln r_2 + i\varphi_2) = (\ln r_1 - \ln r_2) + (\varphi_1 - \varphi_2)i,$$

откуда следует, что  $\ln r_1 - \ln r_2 = 0$ , т.е.  $r_1 = r_2$ , и  $\varphi_1 - \varphi_2 = 2k\pi$ .

Используя экспоненту комплексных чисел, легко получить красивые формулы для синуса и косинуса, известные как формулы Эйлера. Пусть  $x$  – вещественное число; тогда  $e^{xi} = \cos x + i \sin x$ ,  $e^{-xi} = \cos x - i \sin x$ , откуда получаем:

$$\cos x = \frac{e^{xi} + e^{-xi}}{2}, \quad \sin x = \frac{e^{xi} - e^{-xi}}{2i}.$$

**Замечание.** Можно показать, что при нашем определении  $e^\alpha = \lim_{n \rightarrow \infty} (1 + \alpha/n)^n$  для любого комплексного числа  $\alpha$ , так что это определение вполне согласуется с известными из курса математического анализа фактами. Но нам это не понадобится.

*Некоторые применения формул Муавра и Эйлера.* Из школьного курса известны формулы  $\sin 2x = 2 \sin x \cos x$ ,  $\cos 2x = \cos^2 x - \sin^2 x$ . Они легко обобщаются при помощи формулы Муавра. Пусть  $n \geq 1$  – натуральное число; тогда

$$\cos nx + i \sin nx = (\cos x + i \sin x)^n.$$

Преобразуем правую часть этого равенства при помощи формулы бинома Ньютона, воспользовавшись еще тем, что  $i^{2s} = (-1)^s$ ,  $i^{2s+1} = (-1)^s i$  для любого целого  $s$ :

$$\cos nx + i \sin nx = (\cos x + i \sin x)^n = \sum_{j=0}^n C_n^j \cos^{n-j} x (i \sin x)^j =$$

$$\begin{aligned}
&= \sum_{s=0}^{[n/2]} C_n^{2s} \cos^{n-2s} x \sin^{2s} x i^{2s} + \sum_{s=0}^{[(n-1)/2]} C_n^{2s+1} \cos^{n-2s-1} x \sin^{2s+1} x i^{2s+1} = \\
&= \sum_{s=0}^{[n/2]} (-1)^s C_n^{2s} \cos^{n-2s} x \sin^{2s} x + i \sum_{s=0}^{[(n-1)/2]} (-1)^s C_n^{2s+1} \cos^{n-2s-1} x \sin^{2s+1} x
\end{aligned}$$

(переход от третьего выражения к четвертому состоит в том, что мы сумму по всем индексам  $j$  представляем как сумму сумм по четным и по нечетным индексам). Приравнявая вещественные части и коэффициенты мнимых частей правой и левой частей этого равенства, мы получаем формулы

$$\begin{aligned}
\cos nx &= \sum_{s=0}^{[n/2]} (-1)^s C_n^{2s} \cos^{n-2s} x \sin^{2s} x, \\
\sin nx &= \sum_{s=0}^{[(n-1)/2]} (-1)^s C_n^{2s+1} \cos^{n-2s-1} x \sin^{2s+1} x.
\end{aligned}$$

При  $n = 2$  эти формулы превращаются в приведенные выше формулы для синуса и косинуса двойного угла.

Используя формулы Эйлера и бином Ньютона, легко получить формулы, представляющие степени синуса и косинуса как линейные комбинации синусов и косинусов кратных углов; для  $n = 2$  такие формулы известны из школьного курса:

$$\sin^2 x = (1 - \cos 2x)/2, \quad \cos^2 x = (1 + \cos 2x)/2.$$

Мы не будем выписывать здесь общие формулы, а ограничимся разложением по синусам и косинусам кратных углов для пятой и шестой степеней синуса.

$$\begin{aligned}
\sin^5 x &= \left( \frac{e^{xi} - e^{-xi}}{2i} \right)^5 = \frac{e^{5xi} - 5e^{4xi}e^{-xi} + 10e^{3xi}e^{-2xi} - 10e^{2xi}e^{-3xi} + 5e^{xi}e^{-4xi} - e^{-5xi}}{32i} = \\
&= \frac{1}{16} \left( \frac{e^{5xi} - e^{-5xi}}{2i} - 5 \frac{e^{3xi} - e^{-3xi}}{2i} + 10 \frac{e^{xi} - e^{-xi}}{2i} \right) = \frac{1}{16} \sin 5x - \frac{5}{16} \sin 3x + \frac{5}{8} \sin x;
\end{aligned}$$

$$\begin{aligned}
\sin^6 x &= \left( \frac{e^{xi} - e^{-xi}}{2i} \right)^6 = \frac{e^{6xi} - 6e^{4xi} + 15e^{2xi} - 20 + 15e^{-2xi} - 6e^{-4xi} + e^{-6xi}}{-64} = \\
&= \frac{e^{6xi} + e^{-6xi}}{-64} - 6 \frac{e^{4xi} + e^{-4xi}}{-64} + 15 \frac{e^{2xi} + e^{-2xi}}{-64} - \frac{20}{64} = -\frac{1}{32} \cos 6x + \frac{3}{16} \cos 4x - \frac{15}{32} \cos 2x + \frac{5}{8}.
\end{aligned}$$

Приведем еще одну задачу, в решении которой помогают формулы Муавра и Эйлера. Мы хотим найти более компактное выражение для суммы

$$T = \sin x + \sin 2x + \dots + \sin nx.$$

Наряду с суммой  $T$  рассмотрим еще сумму  $S = 1 + \cos x + \cos 2x + \dots + \cos nx$ . Числа  $S$  и  $T$  вещественные; воспользовавшись формулой для суммы геометрической прогрессии, найдем, что

$$\begin{aligned}
S + iT &= (1 + \cos x + \cos 2x + \dots + \cos nx) + i(\sin x + \sin 2x + \dots + \sin nx) = \\
&= 1 + (\cos x + i \sin x) + (\cos 2x + i \sin 2x) + \dots + (\cos nx + i \sin nx) = \\
&= 1 + e^{ix} + e^{2ix} + \dots + e^{nix} = \frac{e^{(n+1)ix} - 1}{e^{ix} - 1} = \frac{e^{i(n+1)x/2}}{e^{ix/2}} \frac{e^{i(n+1)x/2} - e^{-i(n+1)x/2}}{e^{ix/2} - e^{-ix/2}} = \\
&= e^{inx/2} \frac{(e^{i(n+1)x/2} - e^{-i(n+1)x/2})/2i}{(e^{ix/2} - e^{-ix/2})/2i} = \left( \cos \frac{nx}{2} + i \sin \frac{nx}{2} \right) \frac{\sin \frac{(n+1)x}{2}}{\sin \frac{x}{2}}.
\end{aligned}$$



Сравнивая вещественные части и коэффициенты мнимых частей левой и правой частей этого равенства, находим, что

$$S = 1 + \cos x + \cos 2x + \dots + \cos nx = \frac{\cos \frac{nx}{2} \sin \frac{(n+1)x}{2}}{\sin \frac{x}{2}},$$

$$T = \sin x + \sin 2x + \dots + \sin nx = \frac{\sin \frac{nx}{2} \sin \frac{(n+1)x}{2}}{\sin \frac{x}{2}}.$$

*Извлечение квадратных корней из комплексных чисел.* Пусть  $\alpha \in \mathbb{C}$  и пусть  $n \geq 1$  – натуральное число. Комплексное число  $\beta$  называется корнем  $n$ -й степени из  $\alpha$ , если  $\beta^n = \alpha$ .

**Теорема 2.** У всякого ненулевого комплексного числа  $a+bi$ , где  $a, b \in \mathbb{R}$ , в поле  $\mathbb{C}$  есть ровно два квадратных корня (т.е. корня степени 2), которые следующим образом выражаются через  $a$  и  $b$ :

$$\pm \left( \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \frac{b}{2} \sqrt{\frac{2}{a + \sqrt{a^2 + b^2}}} i \right), \quad \text{если } b \neq 0;$$

$$\pm \sqrt{a}, \quad \text{если } b = 0, a > 0;$$

$$\pm i\sqrt{-a}, \quad \text{если } b = 0, a < 0.$$

*Доказательство.* Пусть  $x, y \in \mathbb{R}$  и  $a+bi = (x+yi)^2 = (x^2 - y^2) + 2xyi$ ; сравнивая вещественные части и коэффициенты мнимых частей левой и правой сторон равенства, получаем, что условие равносильно системе двух равенств  $x^2 - y^2 = a$ ,  $2xy = b$ .

Рассмотрим сначала простейший случай  $b = 0$ ; из равенства  $2xy = b = 0$  следует, что тогда  $x = 0$  или  $y = 0$ . В первом случае  $a = -y^2 < 0$ , и  $y = \pm\sqrt{-a}$ , а во втором  $a = x^2 > 0$ ,  $x = \pm\sqrt{a}$ . Итак, если  $(x+yi)^2 = a \neq 0$ , то  $x+yi = \pm\sqrt{a}$  или  $x+yi = \pm i\sqrt{-a}$  в зависимости от знака числа  $a$ . Очевидно, в обоих случаях полученные комплексные числа действительно являются квадратными корнями из  $a$ .

Пусть теперь  $b \neq 0$ ; из равенств  $x^2 - y^2 = a$ ,  $2xy = b$  следует, что

$$(x^2 + y^2)^2 = (x^2 - y^2)^2 + (2xy)^2 = a^2 + b^2.$$

Извлекая корень из обеих частей этого равенства и учитывая что  $x, y \in \mathbb{R}$  и потому  $x^2 + y^2 \geq 0$ , находим, что  $x^2 + y^2 = \sqrt{a^2 + b^2}$ , а значит,

$$x^2 = ((x^2 - y^2) + (x^2 + y^2))/2 = (a + \sqrt{a^2 + b^2})/2.$$

Покажем, что число  $a + \sqrt{a^2 + b^2}$  положительно: в противном случае мы имели бы  $-a \geq \sqrt{a^2 + b^2} \geq 0$ , откуда следовало бы, что  $a^2 = (-a)^2 \geq a^2 + b^2$ , а это невозможно, потому что  $b \neq 0$ . Мы находим теперь, что если  $x+yi$  – квадратный корень из  $a+bi$ , то  $x = \pm\sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}}$ , а соответствующее значение числа  $y$  получается из соотношения  $2xy = b$ . Итак, мы показали, что если  $x+yi$  – квадратный корень из  $a+bi$ , то

$$x+yi = \pm \left( \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \frac{b}{2} \sqrt{\frac{2}{a + \sqrt{a^2 + b^2}}} i \right).$$

Остается проверить, что найденные нами комплексные числа – действительно квадратные корни из  $a+bi$ :

$$\left( \pm \left( \sqrt{\frac{a + \sqrt{a^2 + b^2}}{2}} + \frac{b}{2} \sqrt{\frac{2}{a + \sqrt{a^2 + b^2}}} i \right) \right)^2 =$$

$$\begin{aligned}
&= \left( \frac{a + \sqrt{a^2 + b^2}}{2} - \frac{b^2}{2(a + \sqrt{a^2 + b^2})} \right) + bi = \\
&= \left( \frac{a + \sqrt{a^2 + b^2}}{2} - \frac{(\sqrt{a^2 + b^2})^2 - a^2}{2(a + \sqrt{a^2 + b^2})} \right) + bi = \\
&= \left( \frac{a + \sqrt{a^2 + b^2}}{2} - \frac{-a + \sqrt{a^2 + b^2}}{2} \right) + bi = a + bi.
\end{aligned}$$

*Извлечение корней произвольной степени из комплексных чисел.* Если мы попытаемся применить тот же подход, что и в предыдущем разделе, для извлечения корней третьей степени  $x + yi$  из числа  $a + bi \in \mathbb{C}$ , то получим для  $x$  и  $y$  систему уравнений третьей степени. Эта система сводится к одному уравнению третьей степени от одной неизвестной; такие уравнения умели решать еще в средние века. Однако, какой бы способ решения получившегося уравнения третьей степени мы ни применяли, всегда по ходу дела нам придется извлекать корень третьей как раз из числа  $a + bi$ , и у нас возникает замкнутый круг.

Поэтому для исследования корней степеней, больших 2, приходится использовать тригонометрическую форму комплексного числа.

**Теорема 3.** Пусть  $\alpha \neq 0$  – комплексное число,  $r$  и  $\varphi$  – его модуль и аргумент, и пусть  $n \geq 1$  – натуральное число. Существует ровно  $n$  корней степени  $n$  из  $\alpha$ , которые находятся по формуле

$$\beta_k = \sqrt[n]{r} e^{i(\varphi + 2k\pi)/n} = \sqrt[n]{r} \left( \cos \frac{\varphi + 2k\pi}{n} + i \sin \frac{\varphi + 2k\pi}{n} \right),$$

где  $k = 0, 1, \dots, n-1$ .

*Доказательство.* Комплексное число  $\beta = \rho e^{i\psi}$  (где  $\rho > 0$  и  $\psi$  вещественны) является корнем  $n$ -й степени из числа  $\alpha = r e^{i\varphi}$  тогда и только тогда, когда  $r e^{i\varphi} = \alpha = \beta^n = \rho^n e^{in\psi}$ ; по предложению 3 это значит, что  $r = \rho^n$ , т.е.  $\rho = \sqrt[n]{r}$ , и существует число  $k \in \mathbb{Z}$ , такое что  $n\psi = \varphi + 2k\pi$ . Таким образом, числа  $\beta_k = \sqrt[n]{r} e^{i(\varphi + 2k\pi)/n}$  – корни степени  $n$  из  $\alpha$ , и всякий корень совпадает с одним из  $\beta_k$ . Но среди чисел  $\beta_k$  много совпадающих; точнее, по предложению 3 числа  $\beta_s$  и  $\beta_t$  равны тогда и только тогда, когда существует целое число  $l$ , такое что

$$2l\pi = \frac{\varphi + 2s\pi}{n} - \frac{\varphi + 2t\pi}{n} = \frac{2(s-t)\pi}{n},$$

т.е. когда  $s - t = nl \div n$ . Поэтому числа  $\beta_0, \beta_1, \dots, \beta_{n-1}$  различны, и любое из чисел  $\beta_k$  совпадает с одним из перечисленных, потому что число  $k$  сравнимо по модулю  $n$  со своим остатком от деления на  $n$ .

*Корни из 1.* В частности, имеется  $n$  корней  $n$ -й степени из 1

$$\zeta_k = e^{i \cdot 2\pi k/n} = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n} \quad (k = 0, 1, \dots, n-1).$$

Знание корней из 1 позволяет вычислить все корни  $n$ -й степени из комплексного числа, если известен один из них.

**Предложение 4.** Пусть  $n \geq 1$  – натуральное число,  $0 \neq \alpha \in \mathbb{C}$  и  $\beta$  – один из корней степени  $n$  из  $\alpha$ . Тогда для любого корня  $\zeta$  степени  $n$  из 1 произведение  $\beta\zeta$  является корнем степени  $n$  из  $\alpha$ . Обратно, для любого корня  $\beta'$  степени  $n$  из  $\alpha$  найдется корень  $\zeta$  степени  $n$  из 1, такой что  $\beta' = \beta\zeta$ .

*Доказательство.* Если  $\beta^n = \alpha$ ,  $\zeta^n = 1$ , то  $(\beta\zeta)^n = \beta^n \zeta^n = \alpha \cdot 1 = \alpha$ . Обратно, если  $\beta'^n$  тоже равняется  $\alpha$  и  $\zeta = \beta'/\beta$ , то  $\zeta^n = \beta'^n/\beta^n = \alpha/\alpha = 1$  и  $\beta' = \beta\zeta$ .

**Предложение 5.** Пусть  $n \geq 1$  – натуральное число. Произведение корней  $n$ -й степени из 1 – снова корень  $n$ -й степени из 1. Комплексное число, обратное к

корню  $n$ -й степени из 1 – тоже корень  $n$ -й степени из 1. Число 1 – корень  $n$ -й степени из 1.

*Доказательство.* Ясно, что  $1^n = 1$ . Пусть  $\zeta, \eta$  – корни из 1 степени  $n$ ; тогда  $\zeta^n = \eta^n = 1$ , откуда следует, что

$$(\zeta\eta)^n = \zeta^n\eta^n = 1 \cdot 1 = 1, \quad (\zeta^{-1})^n = (1/\zeta)^n = 1/\zeta^n = 1/1 = 1.$$

Итак, числа  $\zeta\eta, \zeta^{-1}, 1$  – корни  $n$ -й степени из 1.

Поскольку умножение комплексных чисел коммутативно и ассоциативно, предложение 5 означает, что корни  $n$ -й степени из 1 образуют относительно умножения абелеву группу. Следующие утверждения проясняют структуру этой группы.

Пусть  $n \geq 1$  – натуральное число. Корень  $n$ -й степени из 1 называется первообразным корнем степени  $n$  из 1, если он не является корнем меньшей степени из 1.

**Предложение 6.** Пусть  $n \geq 1$  – натуральное число. Корень степени  $n$  из 1

$$\zeta_k = e^{i \cdot 2\pi k/n} = \cos \frac{2\pi k}{n} + i \sin \frac{2\pi k}{n}$$

является первообразным корнем степени  $n$  из 1 тогда и только тогда, когда числа  $k$  и  $n$  взаимно просты.

*Доказательство.* Пусть  $k$  и  $n$  не взаимно просты; тогда у них есть общий делитель  $d \geq 2$ , и существуют целые числа  $k_1, n_1$ , такие что  $k = dk_1, n = dn_1$ . Ясно, что  $0 < n_1 < n$ ; в то же время

$$\zeta_k^{n_1} = e^{i \cdot 2\pi k n_1/n} = e^{i \cdot 2\pi k_1 d n_1/n} = e^{i \cdot 2\pi k_1 n/n} = e^{2\pi k_1 i} = 1,$$

так что  $\zeta_k$  – не первообразный корень степени  $n$  из 1.

Пусть теперь  $k$  и  $n$  взаимно просты, и пусть  $\zeta_k$  – не первообразный корень степени  $n$  из 1. Тогда существует натуральное число  $m$ , такое что  $0 < m < n$  и  $\zeta_k^m = 1$ . Но  $\zeta_k^m = (e^{i \cdot 2\pi k/n})^m = e^{i \cdot 2\pi k m/n}$ , а это число равно 1 только тогда, когда число  $km/n$  целое, т.е.  $km$  делится на  $n$ . Поскольку  $k$  и  $n$  взаимно просты, это возможно только при  $m \div n$ , что противоречит неравенствам  $0 < m < n$ .

Доказанное предложение показывает, что первообразные корни степени  $n$  всегда существуют; например,  $\zeta_1 = e^{2\pi i/n}$  – первообразный корень степени  $n$  из 1. Более того, предложение показывает, что количество первообразных корней степени  $n$  из 1 равно  $\varphi(n)$ .

**Предложение 7.** Пусть  $n \geq 1$  – натуральное число, и пусть  $\theta$  – первообразный корень степени  $n$  из 1. Любой корень степени  $n$  из 1 является степенью  $\theta$ .

*Доказательство.* Все  $n$  чисел  $\theta^0, \theta^1, \theta^2, \dots, \theta^{n-1}$  являются корнями степени  $n$  из 1, и среди них нет одинаковых: иначе было бы  $\theta^s = \theta^t$  для некоторых показателей  $0 \leq s < t < n$ , и тогда мы бы имели  $\theta^{t-s} = 1$  для  $0 < t-s < n$ , что противоречит первообразности  $\theta$ . Значит, все  $n$  корней степени  $n$  из 1 принадлежат множеству  $\{\theta^0, \theta^1, \theta^2, \dots, \theta^{n-1}\}$ , состоящему из степеней  $\theta$ .

## 5. Многочлены как функции. Корни многочленов

*Значение многочлена.* До сих пор мы рассматривали многочлены формально, точнее, как элементы кольца многочленов. Теперь же мы начнем рассматривать их и с функциональной точки зрения.

Пусть  $A$  – коммутативное ассоциативное кольцо с единицей 1, и пусть  $\Lambda$  – ассоциативное кольцо но не обязательно коммутативное кольцо, содержащее  $A$  в качестве подкольца. Пусть, далее,  $f(t) = a_0 + a_1 t + \dots + a_n t^n \in A[t]$  и пусть  $\alpha$  – такой элемент из  $\Lambda$ , который перестановочен со всеми элементами из  $A$  (это

значит, что  $a\alpha = \alpha a$  для каждого  $a \in A$ ). Значением  $f(\alpha)$  многочлена  $f(t)$  при  $t = \alpha$  называется элемент

$$f(\alpha) = a_0 + a_1\alpha + \dots + a_n\alpha^n = \sum_{i=0}^n a_i\alpha^i \in \Lambda$$

(мы считаем, что  $\alpha^0 = 1$  даже если  $\alpha = 0$ ). Еще раз подчеркнем, что переменной  $t$  присваивается значение, которое принадлежит не обязательно самому кольцу  $A$ , но, быть может, его расширению.

**Замечание.** Значение многочлена  $t^n = 1 \cdot t^n$  при  $t = \alpha \in \Lambda$  равно  $1 \cdot \alpha^n$ , а не  $\alpha^n$ , потому что единица 1 кольца  $A$  не обязательно является единицей кольца  $\Lambda$ .

Основное свойство значения многочлена – его согласованность с действиями над многочленами.

**Предложение 1.** Пусть  $A$  – коммутативное ассоциативное кольцо с 1, и пусть  $\Lambda \supseteq A$  – ассоциативное кольцо, содержащее  $A$  в качестве подкольца. Пусть, далее,  $\alpha$  – элемент из  $\Lambda$ , перестановочный со всеми элементами из  $A$ ,  $f(t), g(t) \in A[t]$ ,  $s(t) = f(t) + g(t)$ ,  $p(t) = f(t)g(t)$ . Тогда  $s(\alpha) = f(\alpha) + g(\alpha)$ ,  $p(\alpha) = f(\alpha)g(\alpha)$ .

*Доказательство.* Утверждение труднее сформулировать, чем доказать. Пусть

$$f(t) = a_0 + a_1t + \dots + a_nt^n, \quad g(t) = b_0 + b_1t + \dots + b_nt^n,$$

где  $n$  максимальная из степеней многочленов  $f(t), g(t)$ , а  $a_i, b_j$  – элементы из  $A$ . Тогда  $s(t) = f(t) + g(t) = (a_0 + b_0) + (a_1 + b_1)t + \dots + (a_n + b_n)t^n$ , и потому

$$\begin{aligned} s(\alpha) &= (a_0 + b_0) + (a_1 + b_1)\alpha + \dots + (a_n + b_n)\alpha^n = \\ &= (a_0 + a_1\alpha + \dots + a_n\alpha^n) + (b_0 + b_1\alpha + \dots + b_n\alpha^n) = f(\alpha) + g(\alpha). \end{aligned}$$

Далее, значение многочлена  $a_ib_jt^{i+j}$  равно  $a_ib_j\alpha^{i+j}$ . Но  $p(t) = f(t)g(t) = \sum_{i,j} a_ib_jt^{i+j}$ , и по уже доказанному значение этой суммы равно сумме значений слагаемых, т.е.

$$p(\alpha) = \sum_{i,j} a_ib_j\alpha^{i+j} = \left( \sum_{i=0}^n a_i\alpha^i \right) \left( \sum_{j=0}^n b_j\alpha^j \right) = f(\alpha)g(\alpha).$$

**Теорема Безу.** Первым примером применения предыдущего предложения является следующее простое, но полезное утверждение.

**Предложение 2 (теорема Безу).** Пусть  $k$  – поле,  $f(t) \in k[t]$ ,  $a, c \in k$ . Следующие условия равносильны:

- (1)  $f(t) \equiv c \pmod{(t-a)}$ ;
- (2)  $f(a) = c$ .

*Доказательство.* (1)  $\Rightarrow$  (2). Если  $f(t) \equiv c \pmod{(t-a)}$ , то  $f(t) - c$  делится на  $(t-a)$ , и потому существует такой многочлен  $q(t) \in k[t]$ , что  $f(t) - c = q(t)(t-a)$ . По предложению 1,

$$f(a) - c = q(a)(a-a) = q(a) \cdot 0 = 0,$$

т.е.  $f(a) = c$ .

(2)  $\Rightarrow$  (1). Многочлен  $f(t)$  сравним по модулю  $t-a$  с остатком  $r(t)$  от деления  $f(t)$  на  $t-a$ . Но  $\deg r(t) < \deg(t-a) = 1$ , поэтому  $r(t) = d \in k$ . Таким образом,  $f(t) \equiv d \pmod{(t-a)}$ , и по уже доказанной части нашего утверждения  $d = f(a)$ . Если  $f(a) = c$ , то получаем, что  $d = f(a) = c$  и  $f(t) \equiv d = c \pmod{(t-a)}$ .

**Следствие.** Пусть  $k$  – поле, и пусть  $f(t) \in k[t]$ ,  $a \in k$ . Многочлен  $f(t)$  делится на  $(t-a)$  тогда и только тогда, когда  $f(a) = 0$ .

**Корни многочлена.** Пусть  $k$  – поле. Элемент  $a \in k$  называется корнем многочлена  $f(t) \in k[t]$ , если  $f(a) = 0$ . Предыдущее следствие может быть переформулировано так: элемент  $a \in k$  является корнем многочлена  $f(t) \in k[t]$  тогда и только тогда, когда  $f(t)$  делится на  $(t - a)$ .

**Теорема 1.** Пусть  $k$  – поле. Любой ненулевой многочлен  $f(t) \in k[t]$  имеет в  $k$  не больше корней, чем его степень  $\deg f(t)$ .

*Доказательство.* Пусть  $a_1, \dots, a_r \in k$  – различные корни  $f(t)$ ; по следствию из теоремы Безу многочлен  $f(t)$  делится на каждый из двучленов  $t - a_i$ ,  $1 \leq i \leq r$ . Но эти двучлены попарно взаимно просты, поэтому  $f(t)$  делится на их произведение  $(t - a_1) \cdots (t - a_r)$ ; отсюда и следует, что  $r = \deg((t - a_1) \cdots (t - a_r)) \leq \deg f(t)$ .

Напомним, что два многочлена равны, если равны их соответствующие коэффициенты. Однако, можно определить равенство многочленов  $f(t), g(t) \in k[t]$  и другим способом, а именно, считать что эти многочлены одинаковы, если  $f(a) = g(a)$  для всех  $a \in k$ . Такое равенство многочленов называется функциональным. Следующая теорема показывает, что понятия равенства и функционального равенства многочленов почти всегда совпадают.

**Теорема 2 (о формальном и функциональном равенстве многочленов).** Пусть  $k$  – бесконечное поле, и пусть  $f(t), g(t)$  – многочлены с коэффициентами из  $k$ . Если  $f(a) = g(a)$  для всех  $a \in k$  (т.е. если многочлены  $f(t)$  и  $g(t)$  функционально равны), то многочлены  $f(t), g(t)$  равны.

*Доказательство.* Пусть  $N$  – натуральное число, превосходящее степени обоих многочленов  $f(t), g(t)$ ; тогда степень разности  $h(t) = f(t) - g(t)$  строго меньше, чем  $N$ , но любой элемент  $a \in k$  является корнем  $h(t)$ , так как  $h(a) = f(a) - g(a) = 0$ . Если  $h(t) \neq 0$  и в поле  $k$  найдется не меньше  $N$  элементов, то получится, что ненулевой многочлен  $h(t)$  имеет больше корней, чем его степень, а это невозможно; поэтому  $h(t) = 0$  и  $f(t) = g(t)$ .

Отметим, что бесконечность поля  $k$  существенна: по малой теореме Ферма многочлены  $t^p$  и  $t$  над полем вычетов  $\mathbb{Z}/(p)$  по простому модулю  $p$  функционально равны, но, конечно, они не равны.

**Кратность корня.** Пусть  $f(t)$  – ненулевой многочлен над полем  $k$  и пусть  $a \in k$  – его корень. Тогда  $f(t)$  делится на  $(t - a)$ ; но может оказаться, что  $f(t)$  делится и на более высокую степень двучлена  $(t - a)$ . Натуральное число  $s \geq 1$  называется кратностью корня  $a$  многочлена  $f(t)$ , если многочлен  $f(t)$  делится на  $(t - a)^s$ , но не делится на  $(t - a)^{s+1}$ . Дополним это определение, приняв, что  $a \in k$  – корень многочлена  $f(t)$  кратности 0, если  $a$  не является корнем  $f(t)$ ,

**Предложение 3.** Пусть  $k$  – поле,  $f(t) \in k[t]$  – ненулевой многочлен, и пусть  $a_1, \dots, a_r \in k$  – все его попарно различные корни, а  $s_1, \dots, s_r \geq 1$  – их кратности. Тогда

$$f(t) = a(t - a_1)^{s_1} \cdots (t - a_r)^{s_r} p_1(t) \cdots p_q(t),$$

где  $a \in k$  – старший коэффициент многочлена  $f(t)$ , а  $p_1(t), \dots, p_q(t)$  – неприводимые унитарные многочлены, степень каждого из которых не меньше 2.

*Доказательство.* Многочлены  $(t - a_1)^{s_1}, \dots, (t - a_r)^{s_r}$  попарно взаимно просты, и многочлен  $f(t)$  делится на каждый из них. Поэтому  $f(t)$  делится на их произведение  $(t - a_1)^{s_1} \cdots (t - a_r)^{s_r}$ , и существует многочлен  $g(t) \in k[t]$ , такой что

$$f(t) = (t - a_1)^{s_1} \cdots (t - a_r)^{s_r} g(t).$$

Пусть  $g(t) = ap_1(t) \cdots p_q(t)$  – каноническое разложение  $g(t)$  в произведение старшего коэффициента  $a$  и неприводимых унитарных многочленов  $p_1(t), \dots, p_q(t)$

(такое разложение существует по основной теореме арифметики для многочленов). Тогда

$$f(t) = a(t - a_1)^{s_1} \cdots (t - a_r)^{s_r} p_1(t) \cdots p_q(t),$$

и нам остается доказать, что степень каждого из многочленов  $p_i(t)$  не меньше 2. Пусть  $\deg p_j(t) = 1$ ; тогда  $p_j(t) = t - a$  для некоторого  $a \in k$ . Поскольку  $f(t)$  делится на  $p_j(t) = t - a$ , элемент  $a$  является корнем  $f(t)$  и потому совпадает с каким-то из элементов  $a_i$ ,  $1 \leq i \leq r$ . Мы видим, что в этом случае  $f(t)$  делится на  $(t - a_i)^{s_i+1}$ , вопреки тому, что кратность корня  $a_i$  равна  $s_i$ . Значит, предположение  $\deg p_j(t) = 1$  было неверным, и  $\deg p_j(t) \geq 2$  для всех  $j$ ,  $1 \leq j \leq q$ .

**Следствие 1.** *Кратность корня  $a$  многочлена  $f(t) \neq 0$  совпадает со степенью, в которой двучлен  $(t - a)$  входит в каноническое разложение многочлена  $f(t)$  в произведение унитарных неприводимых многочленов (это верно и для нулевой кратности).*

**Следствие 2.** *Число корней ненулевого многочлена, считаемых каждый столько раз, какова его кратность, не больше степени этого многочлена.*

*Алгебраически замкнутые поля.* Поле  $k$  называется алгебраически замкнутым, если всякий многочлен  $f(t) \in k[t]$ , степень которого больше 0, имеет в  $k$  хотя бы один корень. Отметим, что многочлен 0, степень которого не больше 0, имеет в качестве корней все элементы поля  $k$ ; зато все остальные многочлены, степень которых не больше 0, являются ненулевыми константами и не имеют корней.

**Предложение 4.** *Пусть  $k$  – алгебраически замкнутое поле. Многочлен  $f(t)$  с коэффициентами из  $k$  неприводим в  $k[t]$  тогда и только тогда, когда его степень равна 1.*

*Доказательство.* Мы уже знаем, что многочлены степени 1 неприводимы над любым полем; докажем, что, если поле  $k$  алгебраически замкнуто, то верно и обратное утверждение. Пусть  $f(t) \in k[t]$  – неприводимый многочлен; по определению, неприводимый многочлен отличен от 0 и не является делителем 1, поэтому его степень больше 0. Поскольку поле  $k$  алгебраически замкнуто, у многочлена  $f(t)$  есть корень  $a \in k$ . По следствию из теоремы Безу  $(t - a)$  – делитель  $f(t)$ . Но мы знаем из предложения 5.1, (3) главы I, что если один неприводимый многочлен делится на другой то они ассоциированы, и поэтому  $f(t) = c(t - a)$ , где  $c \in k$ ,  $c \neq 0$ , и  $\deg f(t) = 1$ .

Из этого предложения следует, что всякий унитарный неприводимый многочлен над алгебраически замкнутым полем  $k$  имеет вид  $t - a$ , где  $a \in k$ . Поэтому по основной теореме арифметики для многочленов всякий ненулевой многочлен  $f(t) \in k[t]$  может быть представлен в виде произведения  $f(t) = c(t - b_1) \cdots (t - b_n)$ , где  $c \neq 0$ ,  $b_1, \dots, b_n$  – элементы из  $k$ . Собирая вместе одинаковые сомножители, представим  $f(t)$  в виде  $f(t) = c(t - a_1)^{s_1} \cdots (t - a_r)^{s_r}$ , где  $a_1, \dots, a_r$  – все различные из элементов  $b_1, \dots, b_n$ . Таким образом, основная теорема арифметики в случае алгебраически замкнутого поля принимает следующий вид.

**Теорема 3.** *Пусть  $k$  – алгебраически замкнутое поле. Всякий ненулевой многочлен  $f(t) \in k[t]$  может быть представлен в виде произведения*

$$f(t) = c(t - a_1)^{s_1} \cdots (t - a_r)^{s_r},$$

где  $c \neq 0$ ,  $a_1, \dots, a_r$  – элементы из  $k$ , а  $s_1, \dots, s_r \geq 1$  – натуральные числа. Это представление единственно с точностью до порядка сомножителей.

Впрочем, единственность канонического разложения многочлена в случае алгебраически замкнутого поля очевидна, ибо элементы  $a_1, \dots, a_r$  и числа  $s_1, \dots, s_r$

могут быть интерпретированы инвариантным образом, не зависящим от разложения: из предложения 2 следует, что  $a_1, \dots, a_r$  – все корни многочлена, а  $s_1, \dots, s_r$  – их кратности. Поскольку

$$\begin{aligned}\deg f(t) &= \deg(c(t - a_1)^{s_1} \cdots (t - a_r)^{s_r}) = \\ &= \deg c + \deg(t - a_1)^{s_1} + \dots + \deg(t - a_r)^{s_r} = s_1 + \dots + s_r,\end{aligned}$$

мы получаем следующее утверждение.

**Теорема 4.** *В алгебраически замкнутом поле число корней ненулевого многочлена, считаемых каждый столько раз, какова его кратность, равно степени этого многочлена.*

*Основная теорема высшей алгебры.* Так принято называть следующее утверждение.

**Теорема 5.** *Поле комплексных чисел  $\mathbb{C}$  алгебраически замкнуто.*

В названии "Основная теорема высшей алгебры" неверно все, кроме слова "теорема". Во-первых, эта теорема никак не может претендовать на титул основной для всей алгебры; во-вторых, она не является теоремой алгебры, так как по существу является утверждением о вещественных числах, а в поле вещественных чисел, помимо алгебраической структуры, важную роль играет топология, и оно является предметом изучения для математического анализа. Все доказательства основной теоремы высшей алгебры в той или иной форме используют соображения непрерывности, которая не является алгебраическим понятием. Несколько доказательств этой теоремы будут даны в курсах математического анализа и топологии. Здесь же мы ограничились только ее формулировкой.

Из основной теоремы высшей алгебры следует, что все то, что говорилось об алгебраически замкнутых полях, справедливо и для поля комплексных чисел.

**Теорема 6.** *Всякий неприводимый многочлен над полем комплексных чисел  $\mathbb{C}$  имеет степень 1. Всякий ненулевой многочлен  $f(t) \in \mathbb{C}[t]$  может быть представлен в виде произведения*

$$f(t) = c(t - a_1)^{s_1} \cdots (t - a_r)^{s_r},$$

где  $c \neq 0$ ,  $a_1, \dots, a_r$  – комплексные числа, а  $s_1, \dots, s_r \geq 1$  – натуральные числа. Это представление единственно с точностью до порядка сомножителей. Число комплексных корней ненулевого многочлена над полем  $\mathbb{C}$ , считаемых каждый столько раз, какова его кратность, равно степени этого многочлена.

*Каноническое разложение многочлена над полем вещественных чисел.* Воспользовавшись основной теоремой высшей алгебры, опишем неприводимые многочлены над полем вещественных чисел.

**Предложение 5.** *Если  $b, c \in \mathbb{R}$  и  $b^2 - 4c < 0$ , то многочлен второй степени  $t^2 + bt + c$  неприводим в кольце многочленов  $\mathbb{R}[t]$ . Кроме того, в  $\mathbb{R}[t]$  неприводимы многочлены первой степени  $t - a$ , где  $a \in \mathbb{R}$ . Обратно, если  $p(t) \in \mathbb{R}[t]$  – неприводимый унитарный многочлен, то или  $p(t) = t - a$ , где  $a \in \mathbb{R}$ , или  $p(t) = t^2 + bt + c$ , где  $b, c \in \mathbb{R}$ ,  $b^2 - 4c < 0$ .*

*Доказательство.* Неприводимость многочлена первой степени  $t - a$  уже доказана для любого поля, а не только для поля вещественных чисел. Рассмотрим теперь многочлен второй степени  $t^2 + bt + c$  с вещественными  $b, c$ . Если он не является неприводимым, то существует такое его разложение  $t^2 + bt + c = g(t)h(t)$ , что  $\deg g(t) \geq 1$ ,  $\deg h(t) \geq 1$ . Но  $\deg g(t) + \deg h(t) = \deg(t^2 + bt + c) = 2$ , поэтому  $\deg g(t) = \deg h(t) = 1$ , и существуют такие вещественные числа  $u, v, u', v'$ , что

$g(t) = ut + v$ ,  $h(t) = u't + v'$ . Значит,  $t^2 + bt + c = (ut + v)(u't + v')$ , откуда следует, что  $uu' = 1$ ,  $uv' + u'v = b$ ,  $vv' = c$ ; но тогда

$$b^2 - 4c = (uv' + u'v)^2 - 4vv' = (uv')^2 + 2uu'vv' + (vv')^2 - 4uu'vv' = (uv' - u'v)^2 \geq 0.$$

Следовательно, при  $b^2 - 4c < 0$  многочлен  $t^2 + bt + c$  неприводим.

Обратно, пусть многочлен  $p(t) \in \mathbb{R}[t]$  неприводим. Вещественный многочлен  $p(t)$  можно рассматривать как многочлен с комплексными коэффициентами; по основной теореме высшей алгебры, у него есть комплексный корень  $\alpha$ . Если  $\alpha = a \in \mathbb{R}$  то  $a$  – вещественный корень многочлена  $p(t)$ ; по теореме Безу неприводимый многочлен  $p(t)$  делится на неприводимый многочлен  $t - a$ . Тогда по предложению 5.1, (3) главы I, многочлены  $p(t)$  и  $t - a$  ассоциированы, а значит, равны, потому что оба этих многочлена унитарны.

Если же число  $\alpha$  не вещественно, то  $\bar{\alpha} \neq \alpha$ ; в то же время  $p(\bar{\alpha}) = \overline{p(\alpha)} = \bar{0} = 0$ , потому что коэффициенты многочлена  $p(t)$  вещественны, и значит, совпадают со своими сопряженными. Итак,  $\bar{\alpha}$  – тоже корень  $p(t)$ , а потому  $p(t)$  делится в  $\mathbb{C}[t]$  на различные, а потому взаимно простые унитарные неприводимые многочлены  $t - \alpha$  и  $t - \bar{\alpha}$ . Следовательно,  $p(t)$  делится в  $\mathbb{C}[t]$  на произведение  $g(t) = (t - \alpha)(t - \bar{\alpha})$ . Пусть  $\alpha = u + vi$ , где  $u$  и  $v$  вещественны; поскольку  $\alpha \notin \mathbb{R}$ , число  $v$  отлично от 0. Мы имеем:

$$g(t) = (t - (u + vi))(t - (u - vi)) = t^2 - 2ut + (u^2 + v^2) = t^2 + bt + c,$$

где  $b = -2u$ ,  $c = u^2 + v^2$  – вещественные числа, причем

$$b^2 - 4c = 4u^2 - 4(u^2 + v^2) = -4v^2 < 0,$$

т.е.  $g(t) = t^2 + bt + c$  – вещественный неприводимый многочлен степени 2. Многочлен  $p(t)$  делится на  $t^2 + bt + c$  в  $\mathbb{C}[t]$ ; вспоминая алгоритм деления с остатком и учитывая, что коэффициенты многочленов  $p(t)$  и  $t^2 + bt + c$  вещественны, находим, что частное  $q(t)$  от деления  $p(t)$  на  $t^2 + bt + c$  – тоже многочлен с вещественными коэффициентами. Поэтому неприводимый в  $\mathbb{R}[t]$  многочлен  $p(t)$  делится в  $\mathbb{R}[t]$  на другой неприводимый в  $\mathbb{R}[t]$  многочлен  $t^2 + bt + c$ ; по предложению 5.1, (3) главы I, многочлены  $p(t)$  и  $t^2 + bt + c$  ассоциированы, а значит, равны, потому что оба этих многочлена унитарны.

Теперь мы можем описать, как выглядит каноническое разложение многочленов в произведение неприводимых унитарных многочленов для многочленов над полем вещественных чисел.

**Теорема 7.** *Всякий ненулевой многочлен  $f(t) \in \mathbb{R}[t]$  может быть представлен в виде произведения*

$$f(t) = d(t - a_1) \cdots (t - a_r)(t^2 + b_1t + c_1) \cdots (t^2 + b_qt + c_q),$$

где  $d \neq 0$ ,  $a_1, \dots, a_r, b_1, c_1, \dots, b_q, c_q$  – вещественные числа, причем  $b_i^2 - 4c_i < 0$  для всех  $i$ ,  $1 \leq i \leq q$ . Это представление единственно с точностью до порядка сомножителей.

**Интерполяционная задача.** Если задан некоторый многочлен, то мы можем вычислить любое его значение. Интересна и обратная задача: по значениям многочлена в нескольких точках восстановить многочлен. Эта задача называется интерполяционной задачей.

**Теорема 8.** *Пусть  $k$  – поле, и пусть  $a_1, a_2, \dots, a_n; b_1, b_2, \dots, b_n$  – два набора элементов из  $k$ , причем элементы  $a_1, a_2, \dots, a_n$  попарно различны.*

- (1) *Существуют многочлены  $f(t) \in k[t]$ , такие что  $f(a_i) = b_i$  для всех  $i$ ,  $1 \leq i \leq n$ , и множество всех таких многочленов составляет класс вычетов по модулю  $(t - a_1)(t - a_2) \cdots (t - a_n)$ .*



- (2) Существует единственный многочлен  $f(t) \in k[t]$ , степень которого меньше  $n$ , такой что  $f(a_i) = b_i$  для всех  $i$ ,  $1 \leq i \leq n$ .

*Доказательство.* По теореме Безу (предложение 2) равенство  $f(a_i) = b_i$  и сравнение  $f(t) \equiv b_i \pmod{(t-a_i)}$  равносильны; поэтому (1) можно переформулировать так: существуют многочлены  $f(t) \in k[t]$ , такие что

$$f(t) \equiv b_1 \pmod{(t-a_1)}, \quad f(t) \equiv b_2 \pmod{(t-a_2)}, \dots, f(t) \equiv b_n \pmod{(t-a_n)},$$

и множество всех таких многочленов составляет класс вычетов по модулю произведения  $(t-a_1)(t-a_2) \cdots (t-a_n)$ . Но модули  $(t-a_i)$  попарно взаимно просты, поэтому наше утверждение является частным случаем китайской теоремы об остатках.

Утверждение (2) тривиально следует из (1): в каждом классе вычетов по модулю многочлена  $(t-a_1)(t-a_2) \cdots (t-a_n)$  степени  $n$  существует единственный многочлен, степень которого меньше  $n$ .

Единственный многочлен  $f(t) \in k[t]$ , степень которого меньше  $n$  и такой, что  $f(a_i) = b_i$  для всех  $i$ ,  $1 \leq i \leq n$ , называется интерполяционным многочленом для наборов  $a_1, a_2, \dots, a_n$ ;  $b_1, b_2, \dots, b_n$  элементов из поля  $k$ . Ясно, что интерполяционный многочлен имеет наименьшую степень среди всех многочленов, таких что  $f(a_i) = b_i$  для всех  $i$ ,  $1 \leq i \leq n$ .

Существует много способов построения интерполяционных многочленов. Один из них, называемый методом Ньютона, состоит в следующем. Мы последовательно строим многочлены  $f_1(t), f_2(t), \dots, f_n(t) = f(t)$ , которые являются интерполяционными многочленами не для целых наборов  $a_1, a_2, \dots, a_n$ ;  $b_1, b_2, \dots, b_n$ , а для их начальных отрезков. Таким образом, многочлен  $f_i(t)$  удовлетворяет условиям

$$f_i(a_1) = b_1, \quad f_i(a_2) = b_2, \quad \dots, \quad f_i(a_i) = b_i, \quad \deg f_i(t) < i.$$

Ясно, что  $f_1(t) = b_1$ . Если интерполяционный многочлен  $f_i(t)$  уже построен, то мы подправим его, добавив поправочное слагаемое так, чтобы получившийся многочлен принимал нужное значение и при  $t = a_{i+1}$ . Это поправочное слагаемое ищем в форме  $c_i(t-a_1)(t-a_2) \cdots (t-a_i)$ , где  $c_i \in k$ . Итак, мы хотим подобрать элемент  $c_i \in k$ , так, чтобы многочлен  $f_{i+1}(t) = f_i(t) + c_i(t-a_1)(t-a_2) \cdots (t-a_i)$  удовлетворял условиям

$$f_{i+1}(a_1) = b_1, \quad \dots, \quad f_{i+1}(a_i) = b_i, \quad f_{i+1}(a_{i+1}) = b_{i+1}.$$

Первые  $i$  из этих условий выполняются автоматически: если  $j \leq i$ , то

$$f_{i+1}(a_j) = f_i(a_j) + c_i(a_j - a_1) \cdots (a_j - a_j) \cdots (a_j - a_i) = f_i(a_j) = b_j;$$

поэтому остается лишь выбрать элемент  $c_i \in k$  так, чтобы выполнялось равенство

$$b_{i+1} = f_{i+1}(a_{i+1}) = f_i(a_{i+1}) + c_i(a_{i+1} - a_1)(a_{i+1} - a_2) \cdots (a_{i+1} - a_i).$$

Но элемент  $c_i = (b_{i+1} - f_i(a_{i+1})) / ((a_{i+1} - a_1)(a_{i+1} - a_2) \cdots (a_{i+1} - a_i))$  как раз и удовлетворяет этому требованию (знаменатель отличен от 0, потому что ни один из элементов  $a_1, a_2, \dots, a_i$  не равен  $a_{i+1}$ ).

Впоследствии мы найдем еще и явную формулу для интерполяционного многочлена.

## 6. ПОЛЕ РАЗЛОЖЕНИЯ МНОГОЧЛЕНА

*Существование расширения, в котором многочлен имеет корень.* По-видимому, алгебраисты придавали столь большое значение основной теореме алгебры потому, что она показывала, что любой многочлен с рациональными коэффициентами в каком-то большом поле полностью раскладывается в произведение линейных двучленов. Однако, для любого многочлена такое поле можно построить и чисто алгебраическим путем.

**Теорема 1.** Пусть  $k$  – поле, и пусть  $f(t)$  – неприводимый многочлен с коэффициентами из  $k$ . Тогда существует поле  $K \supseteq k$ , в котором у многочлена  $f(t)$  есть корень.

*Доказательство.* Поскольку многочлен  $f(t)$  неприводим, кольцо вычетов  $K = k[t]/(f(t))$  является полем, и поле  $k$  естественным образом вложено в  $K$ . Обозначим через  $\alpha$  класс вычетов  $[t]_{f(t)}$  элемента  $t$  по модулю  $f(t)$ , и покажем, что  $f(\alpha) = 0$ . Пусть  $f(t) = a_0 + a_1t + \dots + a_nt^n$ , где  $a_0, a_1, \dots, a_n \in k$ ; тогда

$$\begin{aligned} f(\alpha) &= a_0 + a_1\alpha + \dots + a_n\alpha^n = [a_0]_{f(t)} + [a_1]_{f(t)}[t]_{f(t)} + \dots + [a_n]_{f(t)}[t]_{f(t)}^n = \\ &= [a_0 + a_1t + \dots + a_nt^n]_{f(t)} = [f(t)]_{f(t)} = [0]_{f(t)} = 0. \end{aligned}$$

Итак,  $\alpha \in K$  – корень многочлена  $f(t) \in k[t] \subseteq K[t]$ .

Построенное в теореме расширение  $K$  поля  $k$  называют расширением, полученным присоединением к  $k$  корня неприводимого многочлена  $f(t)$ .

**Замечание.** Частный случай этой конструкции уже встречался нам: при построении поля комплексных чисел мы присоединяли к  $\mathbb{R}$  корень многочлена  $t^2 + 1$ .

**Следствие.** Пусть  $k$  – поле, и пусть  $f(t)$  – многочлен с коэффициентами из  $k$ , степень которого не меньше 1. Тогда существует поле  $K \supseteq k$ , в котором у многочлена  $f(t)$  есть корень.

*Доказательство.* По основной теореме арифметики для многочленов существует разложение  $f(t) = cp_1(t) \cdots p_r(t)$ , в котором  $p_1(t), \dots, p_r(t)$  – неприводимые унитарные многочлены, а  $c \in k$ ,  $c \neq 0$ . Поскольку  $\deg f(t) \geq 1$ , в разложении присутствует хотя бы один неприводимый множитель  $p_1(t)$ . По теореме 1 существует поле  $K \supseteq k$ , в котором у многочлена  $p_1(t)$ , а значит, и у многочлена  $f(t)$ , есть корень.

*Поле разложения многочлена.* Теперь мы построим расширение поля, в котором многочлен полностью раскладывается в произведение линейных множителей, и потому число его корней, сосчитанных каждый столько раз, какова его кратность, равно степени многочлена.

**Теорема 2.** Пусть  $k$  – поле, и пусть  $f(t)$  – ненулевой многочлен с коэффициентами из  $k$ . Тогда существует такое поле  $K \supseteq k$ , что  $f(t)$  раскладывается над  $K$  в произведение линейных множителей:  $f(t) = c(t - \alpha_1) \cdots (t - \alpha_n)$ , где  $\alpha_1, \dots, \alpha_n \in K$ , а  $c \in k$  – старший коэффициент многочлена  $f(t)$ .

*Доказательство.* Доказываем теорему индукцией по степени многочлена  $f(t)$ ; теорема тривиальна, если эта степень равна 0 или 1. Пусть  $\deg f(t) > 1$  и теорема уже доказана для всех многочленов меньших степеней. По следствию теоремы 1 существует поле  $k_1 \supseteq k$ , в котором многочлен  $f(t)$  имеет корень  $\alpha_1 \in k_1$ . Тогда  $f(t)$  делится в кольце  $k_1[t]$  на  $(t - \alpha_1)$ . Следовательно, существует многочлен  $g(t) \in k_1[t]$ , такой что  $f(t) = (t - \alpha_1)g(t)$ . Но  $\deg g(t) = \deg f(t) - 1 < \deg f(t)$ , поэтому по предположению индукции существует такое поле  $K \supseteq k_1$ , что  $g(t)$  раскладывается над  $K$  в произведение линейных множителей:  $g(t) = c(t - \alpha_2) \cdots (t - \alpha_n)$ , где  $\alpha_2, \dots, \alpha_n \in K$ , а  $c \in k$  – старший коэффициент многочленов  $f(t)$  и  $g(t)$ . Таким образом,  $f(t) = c(t - \alpha_1) \cdots (t - \alpha_n)$ , где  $\alpha_1, \dots, \alpha_n \in K$ , а  $c \in k$  – старший коэффициент многочлена  $f(t)$ .

*Новый пример конечного поля.* Мы уже использовали соображения теоремы 1 для построения поля комплексных чисел. Ту же конструкцию можно применить и в других ситуациях. Для примера возьмем в качестве  $k$  поле из двух элементов  $\mathbb{Z}/(2)$  и присоединим к нему корень неприводимого над ним многочлена  $f(t) = t^2 + t + [1]_2$ . Этот многочлен неприводим, потому что иначе у него был

бы делитель первой степени, и он имел бы корень в  $k$ ; но оба элемента  $[0]_2, [1]_2$  поля  $k$  не являются корнями этого многочлена. Поле  $K$ , полученное присоединением к  $k$  корня многочлена  $f(t)$  степени 2 состоит из классов вычетов по модулю  $f(t)$ , определяемых многочленами степени, меньшей 2. Итак, поле  $K$  состоит из 4 элементов – двух элементов  $[0]_2, [1]_2$  из поля  $k$  и двух классов, содержащих многочлены первой степени. Обозначим эти классы так:  $\alpha = [t]_{f(t)}$ ,  $\beta = [t + [1]_2]_{f(t)}$ . Вот все нетривиальные результаты сложения и умножения для этих элементов:

$$\begin{aligned} [1]_2 + [1]_2 &= \alpha + \alpha = \beta + \beta = [0]_2, & [1]_2 + \alpha &= \alpha + [1]_2 = \beta, \\ [1]_2 + \beta &= \beta + [1]_2 = \alpha, & \alpha + \beta &= \beta + \alpha = [1]_2, \\ \alpha^2 &= \beta, & \beta^2 &= \alpha, & \alpha\beta &= \beta\alpha = [1]_2. \end{aligned}$$

## 7. КОЛЬЦО МНОГОЧЛЕНОВ ОТ НЕСКОЛЬКИХ ПЕРЕМЕННЫХ

Пусть  $\Lambda$  – кольцо, и пусть  $S$  – подмножество  $\Lambda$ . Обозначим через  $\Pi \supseteq S$  множество элементов  $\pm\pi$ , где  $\pi$  пробегает множество всевозможных конечных произведений элементов из  $S$ , а через  $\Gamma$  – множество всевозможных конечных сумм элементов из  $\Pi$ . Ясно, что произведение элементов из  $\Pi$  – снова элемент из  $\Pi$ , а сумма и разность элементов из  $\Gamma$  – снова элемент из  $\Gamma$ . Покажем, что и произведение элементов из  $\Gamma$  принадлежит  $\Gamma$ , т.е.  $\Gamma$  – подкольцо  $\Lambda$ . Действительно, пусть  $\gamma_1 = \pi_1 + \dots + \pi_n$ ,  $\gamma_2 = \rho_1 + \dots + \rho_m$ , где  $\pi_1, \dots, \pi_n, \rho_1, \dots, \rho_m \in \Pi$ ; поскольку умножение в кольце  $\Lambda$  дистрибутивно относительно сложения, произведение  $\gamma_1\gamma_2$  равно сумме произведений  $\pi_i\rho_j$  ( $1 \leq i \leq n$ ,  $1 \leq j \leq m$ ), каждое из которых, как отмечено выше, принадлежит  $\Pi$ .

Построенное кольцо  $\Gamma$  называется подкольцом  $\Lambda$ , порожденным множеством  $S$ . Ясно, что оно содержится в любом подкольце кольца  $\Lambda$ , содержащем  $S$ .

Рассмотрим частный случай этого определения, который сейчас для нас особенно важен. Пусть  $\Lambda$  – коммутативное ассоциативное кольцо с 1, и пусть  $A$  – подкольцо  $\Lambda$ , содержащее 1, а  $t_1, \dots, t_r$  – какие-то элементы из  $\Lambda$ . В качестве  $S$  возьмем  $A \cup \{t_1, \dots, t_r\}$ . Тогда  $\Pi$  является множеством всех элементов вида  $at_1^{i_1} \dots t_r^{i_r}$ , где  $a \in A$ , а  $i_1, \dots, i_r$  – неотрицательные целые числа (мы, конечно, считаем, что нулевая степень любого элемента из  $\Lambda$  равна 1), а  $\Gamma$  – множество всевозможных конечных сумм элементов из  $\Pi$ .

Для того, чтобы иметь более удобную запись элементов из подкольца  $\Gamma$  кольца  $\Lambda$ , порожденного подкольцом  $A$  и элементами  $t_1, \dots, t_r$ , условимся о некоторых обозначениях. Через  $\mathbb{N}_0$  будем обозначать множество натуральных чисел с присоединенным 0, т.е. множество всех неотрицательных целых чисел. Для натурального  $r$  через  $\mathbb{N}_0^r$  обозначается декартово произведение  $r$  экземпляров множества  $\mathbb{N}_0$ . Иначе говоря,  $\mathbb{N}_0^r$  – это множество всех упорядоченных наборов  $(i_1, \dots, i_r)$ , состоящих из чисел  $i_1, \dots, i_r \in \mathbb{N}_0$ . Теперь мы можем охарактеризовать подкольцо, порожденное  $A$  и элементами  $t_1, \dots, t_r$  как множество всевозможных сумм вида

$$\sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} a_{i_1, \dots, i_r} t_1^{i_1} \dots t_r^{i_r},$$

где  $a_{i_1, \dots, i_r}$  – элементы из  $A$ , почти все (т.е. все, кроме конечного числа) равные 0, так что на самом деле предыдущая сумма конечна.

*Определение кольца многочленов от нескольких переменных.* Пусть  $\Lambda$  – коммутативное ассоциативное кольцо с единицей,  $A$  – подкольцо  $\Lambda$ , содержащее единицу 1 кольца  $\Lambda$ , а  $t_1, \dots, t_r$  – элементы из  $\Lambda$ . Мы говорим,  $\Lambda$  является кольцом многочленов от  $t_1, \dots, t_r$  над кольцом  $A$  и пишем  $\Lambda = A[t_1, \dots, t_r]$ , если любой

элемент  $f \in \Lambda$  однозначно представляется в виде

$$f = \sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} a_{i_1, \dots, i_r} t_1^{i_1} \dots t_r^{i_r},$$

где  $a_{i_1, \dots, i_r}$  – элементы из  $A$ , почти все равные 0. Однозначно определенные элементы  $a_{i_1, \dots, i_r}$  называются коэффициентами многочлена  $f$ .

**Предложение 1.** Пусть  $\Lambda$  – кольцо многочленов от  $t_1, \dots, t_r$  над кольцом  $A$ , и пусть  $1 \leq p < r$ . Подкольцо  $\Gamma$  кольца  $\Lambda$ , порожденное  $A$  и элементами  $t_1, \dots, t_p$  является кольцом многочленов от  $t_1, \dots, t_p$  над кольцом  $A$ , а  $\Lambda$  – кольцом многочленов от  $t_{p+1}, \dots, t_r$  над кольцом  $\Gamma$ . Обратно, если  $\Lambda$  – кольцо многочленов от  $t_{p+1}, \dots, t_r$  над кольцом  $A[t_1, \dots, t_p]$ , то  $\Lambda$  – кольцо многочленов от  $t_1, \dots, t_r$  над кольцом  $A$ .

*Доказательство.* По самому определению кольца  $\Gamma$  каждый его элемент представляется в виде

$$f = \sum_{(i_1, \dots, i_p) \in \mathbb{N}_0^p} a_{i_1, \dots, i_p} t_1^{i_1} \dots t_p^{i_p},$$

где  $a_{i_1, \dots, i_p}$  – элементы из  $A$ , почти все равные 0. Для того, чтобы доказать, что  $\Gamma$  – кольцо многочленов от  $t_1, \dots, t_p$  над  $A$ , остается убедиться в том, что такое представление единственно. Но

$$f = \sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} b_{i_1, \dots, i_r} t_1^{i_1} \dots t_r^{i_r},$$

где

$$b_{i_1, \dots, i_r} = \begin{cases} a_{i_1, \dots, i_p}, & \text{если } i_{p+1} = \dots = i_r = 0; \\ 0 & \text{в противном случае.} \end{cases}$$

Коэффициенты  $b_{i_1, \dots, i_r}$  многочлена  $f$ , рассматриваемого как многочлен от  $t_1, \dots, t_r$ , определены однозначно; поэтому и коэффициенты  $a_{i_1, \dots, i_p} = b_{i_1, \dots, i_p, 0, \dots, 0}$  определены однозначно.

Докажем теперь, что  $\Lambda = \Gamma[t_{p+1}, \dots, t_r]$ . Чтобы избежать растягивания формул на много строчек, рассмотрим лишь случай  $r = 2, p = 1$ ; ниже мы укажем, что надо изменить в общем случае.

**Лемма 1.** Пусть  $\Sigma = \Lambda$  или  $\Sigma = \Gamma[t_2]$ , и пусть  $a_{ij}, b_{ij}$  – элементы из  $\Sigma$ , заданные для всех натуральных  $i, j$  и почти все равные 0. Пусть, далее,

$$f = \sum_{(i,j) \in \mathbb{N}_0^2} a_{ij} t_1^i t_2^j, \quad f' = \sum_{(i,j) \in \mathbb{N}_0^2} b_{ij} t_1^i t_2^j \in \Sigma, \quad g_j = \sum_{i \in \mathbb{N}_0} a_{ij} t_1^i, \quad g'_j = \sum_{i \in \mathbb{N}_0} b_{ij} t_1^i \in \Gamma.$$

Тогда  $f = \sum_{j \in \mathbb{N}_0} g_j t_2^j$ . Кроме того,  $f = f'$  тогда и только тогда, когда  $\sum_{j \in \mathbb{N}_0} g_j t_2^j = \sum_{j \in \mathbb{N}_0} g'_j t_2^j$ .

*Доказательство.* Заменяя сумму по  $\mathbb{N}_0^2$  на двойную сумму и пользуясь дистрибутивностью умножения относительно сложения, получаем:

$$f = \sum_{(i,j) \in \mathbb{N}_0^2} a_{ij} t_1^i t_2^j = \sum_{j \in \mathbb{N}_0} \left( \sum_{i \in \mathbb{N}_0} a_{ij} t_1^i t_2^j \right) = \sum_{j \in \mathbb{N}_0} \left( \sum_{i \in \mathbb{N}_0} a_{ij} t_1^i \right) t_2^j = \sum_{j \in \mathbb{N}_0} g_j t_2^j.$$

Точно так же доказываем, что  $f' = \sum_{j \in \mathbb{N}_0} g'_j t_2^j$ , и потому равенство  $f = f'$  равносильно равенству  $\sum_{j \in \mathbb{N}_0} g_j t_2^j = \sum_{j \in \mathbb{N}_0} g'_j t_2^j$ .

Вернемся к доказательству предложения 1. Пусть сначала  $\Sigma = \Lambda$ . В обозначениях леммы 1 элемент  $f = \sum_{(i,j) \in \mathbb{N}_0^2} a_{ij} t_1^i t_2^j$  представляется в виде суммы  $f = \sum_{j \in \mathbb{N}_0} g_j t_2^j$ , в которой все  $g_j$  – многочлены из  $\Gamma$ , и почти все они равны 0. Из той же леммы следует, что если у  $f$  есть другое аналогичное представление  $f = \sum_{j \in \mathbb{N}_0} g'_j t_2^j$ , то  $f = f' = \sum_{(i,j) \in \mathbb{N}_0^2} a'_{ij} t_1^i t_2^j$ . Но коэффициенты  $f$  как многочлена

от  $t_1, t_2$  определены однозначно; поэтому  $a'_{ij} = a_{ij}$  для всех  $i, j$ , и, следовательно,  $g'_j = g_j$  для всех  $j$ . Таким образом, любой элемент  $f \in \Lambda$  представляется, и притом единственным образом, в виде  $f = \sum_{j \in \mathbb{N}_0} g_j t_2^j$ , где  $g_j \in \Gamma$  для всех  $j$ , причем  $g_j = 0$  почти для всех  $j$ ; но это и значит, что  $\Lambda$  – кольцо многочленов от  $t_2$  над кольцом  $\Gamma$ .

Пусть теперь  $\Sigma = \Gamma[t_2]$ . В обозначениях леммы 1 элемент  $f = \sum_{j \in \mathbb{N}_0} g_j t_2^j$  представляется в виде суммы  $\sum_{(i,j) \in \mathbb{N}_0^2} a_{ij} t_1^i t_2^j$ , где  $a_{ij}$  – элементы из  $A$ , почти все равные 0. Из той же леммы следует, что если у  $f$  есть другое аналогичное представление  $f = \sum_{(i,j) \in \mathbb{N}_0^2} a'_{ij} t_1^i t_2^j$ , то  $\sum_{j \in \mathbb{N}_0} g_j t_1^j = \sum_{j \in \mathbb{N}_0} g'_j t_1^j$ . Но  $\Sigma = \Gamma[t_2]$ , поэтому коэффициенты  $g_j \in \Gamma$  в разложении любого элемента из  $\Sigma$  по степеням  $t_2$  определены однозначно, и мы получаем, что  $g'_j = g_j$  для всех  $j$ . Вспоминая определения  $g_j$  и  $g'_j$ , мы видим, что  $\sum_{i \in \mathbb{N}_0} a_{ij} t_1^i = \sum_{i \in \mathbb{N}_0} a'_{ij} t_1^i$ ; поскольку  $\Gamma$  – кольцо многочленов от  $t_1$  над  $A$ , коэффициенты любого многочлена из  $\Gamma$  определены однозначно, и потому  $a_{ij} = a'_{ij}$  для всех  $i, j$ . Таким образом, любой элемент  $f \in \Sigma = \Gamma[t_2]$  представляется, и притом единственным образом, в виде  $f = \sum_{(i,j) \in \mathbb{N}_0^2} a_{ij} t_1^i t_2^j$ , где  $a_{ij}$  – элементы из  $A$ , почти все равные 0; но это и значит, что  $\Gamma[t_2] = (A[t_1])[t_2]$  – кольцо многочленов от  $t_1, t_2$  над кольцом  $A$ .

Как мы видим, по существу доказательство для случая  $r = 2, p = 1$  состояло в замене суммы по декартову произведению  $\mathbb{N}_0 \times \mathbb{N}_0$  на двойную сумму, и в обратной замене двойной суммы на сумму по декартову произведению. То же самое можно сделать и для произвольных  $r$  и  $p$ . Обозначим через  $q$  разность  $r - p$ . Декартова степень  $\mathbb{N}_0^r$  является декартовым произведением множеств  $\mathbb{N}_0^p$  и  $\mathbb{N}_0^q$ . Поэтому для любых  $X(i_1, \dots, i_r) \in A$ , почти везде равных 0, справедливо соотношение

$$\sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} X(i_1, \dots, i_r) = \sum_{(i_{p+1}, \dots, i_r) \in \mathbb{N}_0^q} \left( \sum_{(i_1, \dots, i_p) \in \mathbb{N}_0^p} X(i_1, \dots, i_r) \right).$$

В остальном доказательство последних двух утверждений предложения в общем случае полностью повторяет доказательство для  $r = 2, p = 1$ .

*Существование кольца многочленов от нескольких переменных.* Покажем, что для любого ассоциативного коммутативного кольца с единицей  $A$  и любого натурального числа  $r \geq 1$  существует кольцо  $\Lambda \supseteq A$  и элементы  $t_1, \dots, t_r \in \Lambda$ , такие что  $\Lambda$  является кольцом многочленов от  $t_1, \dots, t_r$  над кольцом  $A$ . Для  $r = 1$  мы построили такое кольцо в §2. Если  $r > 1$  и кольцо  $A[t_1, \dots, t_{r-1}]$  уже построено, то, опять используя конструкцию из §2, построим такое кольцо  $\Lambda \supseteq A[t_1, \dots, t_{r-1}]$  и выберем такой элемент  $t_r \in \Lambda$ , что  $\Lambda = (A[t_1, \dots, t_{r-1}])[t_r]$ . Тогда по предложению 1  $\Lambda$  является кольцом многочленов от  $t_1, \dots, t_r$  над кольцом  $A$ .

Мы видели выше, что кольцо многочленов от одной переменной над областью целостности само является областью целостности. Это утверждение легко переносится индукцией на многочлены от нескольких переменных: если  $A$  – область целостности, и уже доказано, что  $A[t_1, \dots, t_{r-1}]$  – область целостности, то и кольцо  $A[t_1, \dots, t_r]$ , которое является кольцом многочленов от одной переменной  $t_r$  над областью целостности  $A[t_1, \dots, t_{r-1}]$  – тоже область целостности.

*Степень многочлена от нескольких переменных.* Пусть  $f(t_1, \dots, t_r) \in A[t_1, \dots, t_r]$ , где  $A$  – коммутативное ассоциативное кольцо с 1. Тогда для любого  $i$ , такого что  $1 \leq i \leq r$ , кольцо  $A[t_1, \dots, t_r]$  является кольцом многочленов от  $t_i$  над кольцом  $A[t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_r]$ . Его степень как многочлена над  $A[t_1, \dots, t_{i-1}, t_{i+1}, \dots, t_r]$  называется степенью относительно  $t_i$ . Например, если  $n$  – степень  $f(t_1, t_2, \dots, t_r)$  относительно  $t_1$ , то

$$f(t_1, t_2, \dots, t_r) = g_0(t_2, \dots, t_r) + g_1(t_2, \dots, t_r)t_1 + \dots + g_n(t_2, \dots, t_r)t_1^n,$$

где  $g_i(t_2, \dots, t_r)$  – многочлены от  $t_2, \dots, t_r$  над  $A$ , причем  $g_n(t_2, \dots, t_r) \neq 0$ .

Помимо степени относительно каждой переменной, можно определить полную степень многочлена. Сначала определим полную степень одночлена  $at_1^{i_1} \cdots t_r^{i_r}$ ; если  $a \neq 0$ , то эта полная степень равна  $i_1 + \dots + i_r$ , а при  $a = 0$  мы полагаем равной  $-\infty$ . Полной степенью многочлена  $f(t_1, \dots, t_r) = \sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} a_{i_1, \dots, i_r} t_1^{i_1} \cdots t_r^{i_r}$ , где  $a_{i_1, \dots, i_r}$  – элементы из  $A$ , почти все равные 0, называется максимальная из полных степеней составляющих ее одночленов  $a_{i_1, \dots, i_r} t_1^{i_1} \cdots t_r^{i_r}$ . Отметим, что одночленов с одной и той же максимальной полной степенью среди одночленов  $a_{i_1, \dots, i_r} t_1^{i_1} \cdots t_r^{i_r}$  может быть несколько; если полная степень этого многочлена равна  $n \geq 0$ , то существуют такие  $i_1, \dots, i_r \geq 0$ , что  $i_1 + \dots + i_r = n$ ,  $a_{i_1, \dots, i_r} \neq 0$ , а при любых  $j_1, \dots, j_r \geq 0$ , таких что  $j_1 + \dots + j_r > n$ , соответствующий коэффициент  $a_{j_1, \dots, j_r}$  равен 0.

Многочлен называется однородным многочленом степени  $n$ , или формой степени  $n$ , если он является суммой (быть может, пустой) одночленов полной степени  $n$ . Поскольку нулевой многочлен – сумма пустого множества слагаемых, он является однородным многочленом любой степени. Линейные формы степени 0 – это элементы из  $A$ , формы степени 1 (они называются линейными формами) – это многочлены вида  $a_1 t_1 + \dots + a_r t_r$ , где  $a_1, \dots, a_r \in A$ , а формы степени 2, или квадратичные формы, имеют вид

$$\sum_{i=1}^r a_i t_i^2 + \sum_{1 \leq i < j \leq r} b_{ij} t_i t_j \quad (a_i, b_{ij} \in A).$$

*Значение многочлена от нескольких переменных.* Пусть  $A$  – коммутативное ассоциативное кольцо с единицей 1, и пусть  $\Lambda$  – ассоциативное кольцо, но не обязательно коммутативное, содержащее  $A$  в качестве подкольца. Пусть, далее,  $f(t_1, \dots, t_r) = \sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} a_{i_1, \dots, i_r} t_1^{i_1} \cdots t_r^{i_r} \in A[t_1, \dots, t_r]$ , где  $a_{i_1, \dots, i_r}$  – элементы из  $A$ , почти все равные 0, и пусть  $\alpha_1, \dots, \alpha_r$  – такие элементы из  $\Lambda$ , которые перестановочны друг с другом и со всеми элементами из  $A$  (это значит, что  $a\alpha_i = \alpha_i a$  и  $\alpha_i \alpha_j = \alpha_j \alpha_i$  для всех  $i, j$  и для всех  $a \in A$ ). Значением  $f(\alpha_1, \dots, \alpha_r)$  многочлена  $f(t_1, \dots, t_r)$  при  $t_1 = \alpha_1, \dots, t_r = \alpha_r$  называется элемент

$$f(\alpha_1, \dots, \alpha_r) = \sum_{(i_1, \dots, i_r) \in \mathbb{N}_0^r} a_{i_1, \dots, i_r} \alpha_1^{i_1} \cdots \alpha_r^{i_r} \in \Lambda$$

(сумма имеет смысл, потому что почти все слагаемые равны 0, и фактически складывается лишь конечное число слагаемых).

Как и для многочленов от одной переменной, значения многочленов от нескольких переменных согласованы с действиями: значения суммы, разности и произведения многочленов в некоторой точке равны соответственно сумме, разности и произведению значений многочленов в этих точках. Ввиду очевидности доказательства этого, мы опускаем не только доказательство, но и точную формулировку утверждения.

*Теорема о формальном и функционально равенстве для многочленов от нескольких переменных.* Выше мы доказали, что если два многочлена от одной переменной над бесконечным полем  $k$  принимают одинаковые значения при всех значениях аргумента  $\alpha \in k$ , то они совпадают. Этот результат остается верным и для многочленов от нескольких переменных.

**Теорема 1.** Пусть  $k$  – бесконечное поле, и пусть  $f(t_1, \dots, t_r), g(t_1, \dots, t_r)$  – многочлены от  $t_1, \dots, t_r$  с коэффициентами из  $k$ . Если  $f(a_1, \dots, a_r) = g(a_1, \dots, a_r)$  (т.е. если многочлены  $f(t_1, \dots, t_r)$  и  $g(t_1, \dots, t_r)$  функционально равны), то многочлены  $f(t_1, \dots, t_r)$ , равны.

*Доказательство.* Пусть  $h(t_1, \dots, t_r) = f(t_1, \dots, t_r) - g(t_1, \dots, t_r)$ ; тогда

$$h(a_1, \dots, a_r) = f(a_1, \dots, a_r) - g(a_1, \dots, a_r) = 0$$

для всех  $a_1, \dots, a_r \in k$ . Достаточно поэтому доказать следующее утверждение:

*Если  $h(t_1, \dots, t_r) \in k[t_1, \dots, t_r]$  – такой многочлен, что  $h(a_1, \dots, a_r) = 0$  для всех  $a_1, \dots, a_r \in k$ , то  $h(t_1, \dots, t_r) = 0$ .*

Доказывать это утверждение будем индукцией по  $r$ ; для  $r = 1$  оно является частным случаем теоремы о формальном и функциональном равенстве для многочленов от одной переменной. Пусть  $r > 1$ , и пусть утверждение уже доказано для многочленов от  $r - 1$  переменной. Представим  $h(t_1, \dots, t_r)$  как многочлен от  $t_1$  над  $k[t_2, \dots, t_r]$ :

$$h(t_1, \dots, t_r) = g_0(t_2, \dots, t_r) + g_1(t_2, \dots, t_r)t_1 + \dots + g_n(t_2, \dots, t_r)t_1^n,$$

где  $g_s(t_2, \dots, t_r) \in k[t_2, \dots, t_r]$  для всех  $s$ ,  $0 \leq s \leq n$ . Пусть  $h(t_1, \dots, t_r) \neq 0$ ; тогда для некоторого  $s$ ,  $0 \leq s \leq n$ , многочлен  $g_s(t_2, \dots, t_r)$  отличен от 0. По предположению индукции можно выбрать такие  $a_2, \dots, a_r \in k$ , что  $g_s(a_2, \dots, a_r) \neq 0$ . Тогда многочлен

$$u(t_1) = g_0(a_2, \dots, a_r) + g_1(a_2, \dots, a_r)t_1 + \dots + g_n(a_2, \dots, a_r)t_1^n \in k[t_1]$$

ненулевой, так как в нем коэффициент при  $t_1^s$  отличен от 0. Поэтому по теореме о формальном и функциональном равенстве многочленов от одной переменной существует такой элемент  $a_1 \in k$ , что  $u(a_1) \neq 0$ . Ясно, что  $g_i(a_2, \dots, a_r)$ ,  $a_1^i$  являются значениями многочленов  $g_i(t_2, \dots, t_r)$  и  $t_1^i$  из кольца  $k[t_1, \dots, t_r]$  при  $t_1 = a_1$ ,  $t_2 = a_2, \dots, t_r = a_r$ ; поэтому

$$0 \neq u(a_1) = g_0(a_2, \dots, a_r) + g_1(a_2, \dots, a_r)a_1 + \dots + g_n(a_2, \dots, a_r)a_1^n$$

является значением  $h(a_1, \dots, a_r)$  многочлена

$$h(t_1, \dots, t_r) = g_0(t_2, \dots, t_r) + g_1(t_2, \dots, t_r)t_1 + \dots + g_n(t_2, \dots, t_r)t_1^n,$$

а это противоречит тому, что все значения многочлена  $h(t_1, \dots, t_r)$  равны 0. Итак, предположение  $h(t_1, \dots, t_r) \neq 0$  привело к противоречию. Значит,  $h(t_1, \dots, t_r) = 0$ , что мы и хотели доказать.

## 8. Производная многочлена и ее применения

*Определение производной.* Понятие производной функции принадлежит математическому анализу; любое ее определение в той или иной мере использует пределы, непрерывность или что-либо подобное. Для "очень хороших" функций определение можно не вполне точно сформулировать следующим образом: функция  $f'(x)$  является производной для функции  $f(x)$ , если существует "хорошая" (т.е. непрерывная) функция двух аргументов  $\Phi(x, \varepsilon)$ , такая что  $f(x + \varepsilon) = f(x) + \varepsilon\Phi(x, \varepsilon)$  и  $f'(x) = \Phi(x, 0)$ .

Такое определение легко обобщить, если под "хорошей" функцией понимать не непрерывную функцию, а функцию из какого-то другого класса. Это позволяет определить производную и в таких ситуациях, когда никакой речи о пределах идти не может. Именно так мы и определим производную многочлена над произвольным полем, взяв в качестве класса "хороших" объектов класс всех многочленов.

Прежде, чем дать определение производной многочлена, напомним, что если  $f(t)$  – многочлен с коэффициентами из  $A$ , то мы можем считать его значения при значении  $t$ , не обязательно принадлежащем  $A$ , а какому-то его расширению. В частности, придавая  $t$  значение  $t + u \in A[t, u]$ , мы получим многочлен  $f(t + u) \in A[t, u]$ .

Теперь мы можем определить производную многочлена. Пусть  $A$  – область целостности, и пусть  $f(t) \in A[t]$  – многочлен с коэффициентами из  $A$ ; многочлен  $f'(t) \in A[t]$  называется производной многочлена  $f(t)$ , если существует многочлен

$\Phi(t, u) \in A[t, u]$  от двух переменных, такой что  $f(t+u) = f(t) + u\Phi(t, u)$ ,  $f'(t) = \Phi(t, 0)$ .

**Предложение 1.** Пусть  $A$  – область целостности. Для любого многочлена  $f(t) \in A[t]$  существует, и притом единственный многочлен  $f'(t) \in A[t]$ , являющийся производной многочлена  $f(t)$ .

*Доказательство.* Многочлен от двух переменных  $f(t+u)$  может быть записан как многочлен от  $u$  над  $A[t]$ :

$$f(t+u) = g_0(t) + g_1(t)u + g_2(t)u^2 + \dots + g_n(t)u^n.$$

Считая значения обеих частей равенства при  $u = 0$ , находим, что  $f(t) = g_0(t)$ , и потому предыдущее равенство принимает вид  $f(t+u) = f(t) + u\Phi(t, u)$ , где  $\Phi(t, u) = g_1(t) + g_2(t)u + \dots + g_n(t)u^{n-1}$ . Тогда многочлен  $g_1(t) = \Phi(t, 0)$  является производной многочлена  $f(t)$ .

Для доказательства единственности производной заметим, что не только свободный член  $g_1(t)$  многочлена  $\Phi(t, u)$ , но и сам многочлен  $\Phi(t, u)$  определен однозначно: если  $f(t+u) = f(t) + u\Phi(t, u) = f(t) + u\Phi_1(t, u)$ , то  $u\Phi(t, u) = u\Phi_1(t, u)$ , откуда следует, что  $\Phi(t, u) = \Phi_1(t, u)$ , потому что  $u \neq 0$ , а  $A[t, u]$  – область целостности.

Для изучения производной более удобна другая форма ее определения.

**Предложение 2.** Пусть  $A$  – область целостности, и пусть  $f(t) \in A[t]$ ; для того чтобы многочлен  $f'(t) \in A[t]$  был производной многочлена  $f(t)$  необходимо и достаточно, чтобы в  $A[t, u]$  выполнялось сравнение  $f(t+u) \equiv f(t) + f'(t)u \pmod{u^2}$ .

*Доказательство.* В обозначениях доказательства предложения 1 мы имеем:

$$f(t+u) = f(t) + g_1(t)u + g_2(t)u^2 + \dots + g_n(t)u^n \equiv f(t) + g_1(t)u = f(t) + f'(t)u \pmod{u^2}.$$

Обратно, пусть  $f(t+u) \equiv f(t) + g(t)u \pmod{u^2}$ , где  $g(t) \in A[t]$ ; тогда мы получаем, что  $g(t)u \equiv f'(t)u \pmod{u^2}$ , откуда следует, что существует такой многочлен  $\Psi(u) = h_0(t) + h_1(t)u + \dots + h_m(t)u^m \in A[t][u] = A[t, u]$ , что

$$g(t)u = f'(t)u + \Psi(u)u^2 = f'(t)u + h_0(t)u^2 + h_1(t)u^3 + \dots + h_m(t)u^{m+2}.$$

Сравнивая коэффициенты при  $u$  в левой и правой частях равенства, получаем, что  $g(t) = f'(t)$ .

*Свойства производной.* Покажем, что так определенная производная обладает обычными свойствами.

**Предложение 3.** Пусть  $A$  – область целостности, и пусть  $a \in A \subset A[t]$ ,  $f(t), g(t) \in A[t]$ ; тогда

- (1)  $a' = 0$ ,  $t' = 1$ ,  $(af(t))' = af'(t)$ ;
- (2)  $(f(t) \pm g(t))' = f'(t) \pm g'(t)$ ;
- (3)  $(f(t)g(t))' = f'(t)g(t) + f(t)g'(t)$ ;
- (4) если  $n \geq 0$  – целое число, то  $((t-a)^n)' = n(t-a)^{n-1}$  (в частности,  $(t^n)' = nt^{n-1}$ );
- (5)  $a_0 + a_1t + a_2t^2 + \dots + a_nt^n = a_1 + 2a_2t + \dots + na_nt^{n-1}$ .

*Доказательство.* Напомним, что по определению производной выполняются сравнения

$$f(t+u) \equiv f(t) + f'(t)u \pmod{u^2}, \quad g(t+u) \equiv g(t) + g'(t)u \pmod{u^2}.$$

Свойства (1)–(3) следуют из предложения 2 и следующих сравнений по модулю  $u^2$ :

$$a \equiv a + 0 \cdot u, \quad t + u \equiv t + 1 \cdot u, \quad af(t+u) \equiv a(f(t) + f'(t)u) = af(t) + (af'(t))u,$$



$$f(t+u) \pm g(t+u) \equiv (f(t)+f'(t)u) \pm (g(t)+g'(t)u) = (f(t) \pm g(t)) + (f'(t) \pm g'(t))u,$$

$$f(t+u)g(t+u) \equiv (f(t)+f'(t)u)(g(t)+g'(t)u) \equiv f(t)g(t) + (f'(t)g(t) + f(t)g'(t))u.$$

Свойство (4) доказывается индукцией по  $n$ : для  $n = 0$  и  $n = 1$  оно содержится в (1), и если уже доказано, что  $((t-a)^n)' = n(t-a)^{n-1}$ , то по свойству (3) получаем

$$\begin{aligned} ((t-a)^{n+1})' &= ((t-a)^n(t-a))' = ((t-a)^n)'(t-a) + (t-a)^n(t-a)' = \\ &= (n(t-a)^{n-1})(t-a) + (t-a)^n \cdot 1 = (n+1)(t-a)^n. \end{aligned}$$

Свойство (5) является непосредственным следствием свойств (2), (1) и (4).

**Критерий кратности корня многочлена.** Корень  $a$  многочлена  $f(t)$  с коэффициентами из поля называется простым, если его кратность равна 1, и кратным, если его кратность не меньше 2.

**Теорема 1.** Пусть  $k$  поле, и пусть  $f(t) \in k[t]$ . Для того, чтобы корень  $a$  многочлена  $f(t)$  был кратным, необходимо и достаточно, чтобы выполнялось равенство  $f'(a) = 0$ .

*Доказательство.* Пусть сначала  $f'(a) = 0$ . Поскольку  $a$  – корень  $f(t)$ , многочлен  $f(t)$  делится на  $(t-a)$ , и существует многочлен  $g(t) \in k[t]$ , такой что  $f(t) = (t-a)g(t)$ . Тогда  $f'(t) = (t-a)'g(t) + (t-a)g'(t)$ , и  $0 = f'(a) = 1 \cdot g(a) + (a-a)g'(a) = g(a)$ , и значит, по теореме Безу, многочлен  $g(t)$  делится на  $(t-a)$ . Следовательно, существует такой многочлен  $h(t) \in k[t]$ , что  $g(t) = (t-a)h(t)$ . Но тогда многочлен  $f(t) = (t-a)^2h(t)$  делится на  $(t-a)^2$ , а это значит, что кратность корня  $a$  многочлена  $f(t)$  не меньше 2.

Обратно, пусть  $a$  – кратный корень  $f(t)$ ; тогда многочлен  $f(t)$  делится на  $(t-a)^2$ , и существует такой многочлен  $h(t) \in k[t]$ , что  $f(t) = (t-a)^2h(t)$ . Значит,

$$f'(t) = ((t-a)((t-a)h(t)))' = (t-a)'((t-a)h(t)) + (t-a)((t-a)h(t))' \div ((t-a)),$$

и потому по теореме Безу  $f'(a) = 0$ .

**Следствие.** Для того, чтобы многочлен  $f(t) \in k[t]$  не имел кратных корней ни в каком поле  $K$ , содержащем  $k$ , необходимо и достаточно, чтобы он был взаимно прост со своей производной  $f'(t)$ .

*Доказательство.* Если многочлены  $f(t)$  и  $f'(t)$  не взаимно просты, то степень их наибольшего общего делителя  $d(t) \in k[t]$  больше 0, и потому существует поле  $K \supseteq k$ , в котором многочлен  $d(t)$  имеет корень  $\alpha$ . Поскольку  $f(t)$  и  $f'(t)$  делятся на  $d(t)$ , элемент  $\alpha \in K$  является общим корнем  $f(t)$  и  $f'(t)$ , а потому кратным корнем многочлена  $f(t)$ .

Если же многочлены  $f(t)$  и  $f'(t)$  взаимно просты, то существуют такие многочлены  $g(t), h(t) \in k[t]$ , что  $f(t)g(t) + f'(t)h(t) = 1$ ; если бы у многочлена  $f(t)$  в некотором поле  $K \supseteq k$  был кратный корень  $\alpha$ , то  $f(\alpha)$  и  $f'(\alpha)$  были бы равны 0, и мы получили бы, что  $1 = f(\alpha)g(\alpha) + f'(\alpha)h(\alpha) = 0 \cdot g(\alpha) + 0 \cdot h(\alpha) = 0$ , что невозможно.

**Интерполяционная формула Лагранжа.** Пусть  $k$  поле, и пусть  $a_1, \dots, a_i, \dots, a_n$  – различные элементы из  $k$ . Обозначим через  $g(t)$  произведение

$$(t-a_1) \cdots (t-a_i) \cdots (t-a_n)$$

всех двучленов  $(t-a_j)$ ,  $1 \leq j \leq n$ , а через  $g_i(t)$  – произведение всех этих двучленов, кроме  $(t-a_i)$ . Обычно многочлен  $g_i(t)$  записывается в форме  $g_i(t) = \frac{g(t)}{t-a_i}$ .

Ясно, что  $g_i(a_j) = 0$  при  $j \neq i$ ; найдем теперь, чему равняется  $g_i(a_i)$ . Для этого заметим, что, очевидно,  $g(t) = (t-a_i)g_i(t)$ , а потому  $g'(t) = (t-a_i)g'_i(t) + 1 \cdot g_i(t)$ , откуда следует, что  $g'(a_i) = (a_i-a_i)g'_i(a_i) + 1 \cdot g_i(a_i)$ . Таким образом,  $g_i(a_i) = g'(a_i)$ . Заметим, что  $a_i$  – простой корень многочлена  $g(t)$ , и потому  $g'(a_i) \neq 0$ .

Пусть теперь  $b_1, \dots, b_i, \dots, b_n$  – какие-то элементы из  $k$ ; положим

$$f(t) = \frac{b_1 g_1(t)}{g'(a_1)} + \dots + \frac{b_i g_i(t)}{g'(a_i)} + \dots + \frac{b_n g_n(t)}{g'(a_n)}.$$

Ясно, что степень многочлена  $f(t)$  не превосходит  $n-1$ ; кроме того, для любого  $i$ ,  $1 \leq i \leq n$  мы имеем:

$$f(a_i) = \frac{b_1 g_1(a_i)}{g'(a_1)} + \dots + \frac{b_i g_i(a_i)}{g'(a_i)} + \dots + \frac{b_n g_n(a_i)}{g'(a_n)} = \frac{b_i g'(a_i)}{g'(a_i)} = b_i.$$

Итак, мы доказали следующее утверждение.

**Теорема 2.** Пусть  $k$  – поле, и пусть  $a_1, a_2, \dots, a_n$ ;  $b_1, b_2, \dots, b_n$  – два набора элементов из  $k$ , причем элементы  $a_1, a_2, \dots, a_n$  попарно различны. Обозначим через  $g(t)$  многочлен  $(t-a_1) \cdots (t-a_i) \cdots (t-a_n)$ . Тогда многочлен

$$f(t) = \sum_{i=1}^n \frac{b_i g(t)}{g'(a_i)(t-a_i)}$$

является единственным многочленом, таким что  $\deg f(t) < n$ , и  $f(a_i) = b_i$  для всех  $i$ ,  $1 \leq i \leq n$ .

Полученная формула для интерполяционного многочлена называется интерполяционной формулой Лагранжа.

**Характеристика поля.** До сих пор все наши рассуждения были справедливы для произвольных полей; однако, в следующих пунктах нам придется накладывать на поля некоторые ограничения, о которых мы сейчас и будем говорить.

Пусть  $k$  – поле; рассмотрим в нем элементы

$$1, 1+1, 1+1+1, \dots, \underbrace{1+1+\dots+1}_n, \dots$$

Если все эти элементы не равны 0, то говорят, что характеристика поля  $k$  равна 0; если же среди них есть нули, то характеристикой поля  $k$  называется наименьшее число  $p > 0$ , такое что сумма  $p$  слагаемых, каждое из которых равно единице 1 поля  $k$ , равна 0. Для характеристики поля используется обозначение  $\text{char } k$ . Поскольку в любом поле  $0 \neq 1$ , характеристика поля не может быть равна 1.

**Предложение 4.** Характеристика любого поля или равна 0, или является простым числом.

**Доказательство.** Пусть  $k$  – поле, и пусть  $n = \text{char } k \neq 0$  – не простое число. Тогда  $n$  раскладывается в произведение натуральных чисел  $q > 1$  и  $r > 1$ . Обозначим через  $a, b \in k$  суммы соответственно  $q$  и  $r$  слагаемых, каждое из которых равно единице 1 поля  $k$ . Поскольку  $q, r < n = \text{char } k$ , оба элемента  $a, b$  отличны от 0, но

$$ab = \underbrace{(1+1+\dots+1)}_q \underbrace{(1+1+\dots+1)}_r = \underbrace{1+1+\dots+1}_{n=qr} = 0.$$

Это невозможно, потому что поле является областью целостности, и в нем нет делителей 0.

**Производные высших порядков.** Пусть  $A$  – коммутативное ассоциативное кольцо с 1, и пусть  $f(t) \in k[t]$ . Мы уже определили производную  $f'(t)$  многочлена  $f(t)$ . Второй производной  $f''(t)$  многочлена  $f(t)$  называется производная  $(f'(t))'$  его производной  $f'(t)$ . Продолжая этот процесс, определим по индукции  $n$ -ю производную многочлена  $f(t)$  как производную его  $(n-1)$ -й производной.  $n$ -ю производную многочлена  $f(t)$ , особенно при больших  $n$ , обозначают через  $f^{(n)}(t)$ ; таким образом,  $f^{(1)}(t) = f'(t)$ ,  $f^{(2)}(t) = f''(t)$ ,  $\dots$ ,  $f^{(n)}(t) = (f^{(n-1)}(t))'$ .

Поскольку степень производной меньше степени многочлена, все производные порядков больше  $n$  многочлена степени  $n$  являются нулевыми многочленами.

В следующем пункте нам окажется полезным такое утверждение.

**Лемма 1.** Пусть  $A$  – коммутативное ассоциативное кольцо с 1,  $n, m > 0$  – целые числа, и пусть  $f(t) = (t - a)^n$ . Тогда

$$f^{(m)}(t) = \begin{cases} n(n-1) \cdots (n-m+1)(t-a)^{n-m}, & \text{если } n > m; \\ n!, & \text{если } n = m; \\ 0, & \text{если } n < m. \end{cases}$$

Поэтому значение многочлена  $f^{(m)}(t) = ((t-a)^n)^{(m)}$  при  $n \neq m$  равно 0, а при  $n = m$  оно равно  $n!$ .

*Доказательство.* В последнем случае номер  $m$  производной больше степени многочлена  $(t-a)^n$ , поэтому его  $m$ -я производная равна 0. В первом и во втором случаях утверждение легко доказывается индукцией по  $m$  с использованием утверждения (4) предложения 3.

*Формула Тейлора.* Пусть  $k$  – поле, и пусть  $f(t) \in k[t]$ . Многочлен  $f(t+u)$  от двух переменных  $t, u$  можно представить как многочлен от  $u$  с коэффициентами из  $k[t]$ :

$$f(t+u) = g_0(t) + g_1(t)u + g_2(t)u^2 + \dots + g_n(t)u^n.$$

Мы уже знаем, что  $g_0(t) = f(t)$ ,  $g_1(t) = f'(t)$ . Выясним, чему равны остальные коэффициенты  $g_2(t), \dots, g_n(t)$ . Для этого возьмем значения обеих частей предыдущего равенства при  $t = u$ ,  $u = t - u$ ; мы получим соотношение

$$f(t) = g_0(u) + g_1(u)(t-u) + \dots + g_i(u)(t-u)^i + \dots + g_n(u)(t-u)^n.$$

Возьмем  $i$ -ю производную от обеих частей этого равенства, рассматриваемых как многочлены от  $t$  над  $k[u]$ , и сосчитаем ее значение при  $t = u$ ; по лемме из предыдущего пункта мы получим:

$$\begin{aligned} f^{(i)}(u) &= f^{(i)}(t)|_{t=u} = g_1(u)(t-u)^{(i)}|_{t=u} + \dots + g_i(u)((t-u)^i)^{(i)}|_{t=u} + \\ &+ \dots + g_n(u)((t-u)^n)^{(i)}|_{t=u} = g_i(u) \cdot i!. \end{aligned}$$

Полученное равенство является равенством многочленов от  $u$  над полем  $k$ . Взяв значения обеих частей равенства при  $u = t$ , мы получим, что  $i!g_i(t) = f^{(i)}(t)$ . Если  $\text{char } k = 0$  или  $\text{char } k > i$ , то  $i! = \underbrace{1_k + 1_k + \dots + 1_k}_{i!}$  – ненулевой элемент поля  $k$ , и на него можно делить; поэтому в этом случае мы находим выражение для коэффициента  $g_i(t)$ :

$$g_i(t) = \frac{f^{(i)}(t)}{i!}.$$

Подставив его в разложение многочлена  $f(t+u)$  по степеням  $u$ , мы получим следующий результат.

**Теорема 3 (формула Тейлора).** Пусть  $k$  – поле, и пусть  $f(t) \in k[t]$ . Если характеристика поля  $k$  равна 0 или больше степени  $n$  многочлена  $f(t)$ , то в кольце  $k[t, u]$  выполняется равенство

$$f(t+u) = f(t) + \frac{f'(t)}{1!}u + \dots + \frac{f^{(i)}(t)}{i!}u^i + \dots + \frac{f^{(n)}(t)}{n!}u^n.$$

Пусть теперь  $a \in k$ ; взяв значения обеих частей формулы Тейлора при  $t = a$ ,  $u = t - a$ , мы получим вариант формулы из теоремы 3, который обычно и называется формулой Тейлора:

$$f(t) = f(a) + \frac{f'(a)}{1!}(t-a) + \dots + \frac{f^{(i)}(a)}{i!}(t-a)^i + \dots + \frac{f^{(n)}(a)}{n!}(t-a)^n.$$

*Еще о кратных корнях.* Воспользуемся формулой Тейлора, чтобы уточнить наши результаты о кратных корнях. Сначала докажем простой, но удобный критерий того, что кратность корня равна числу  $s$ .

**Лемма 2.** Пусть  $k$  – поле,  $a \in k$ ,  $f(t) \in k[t]$ . Если  $f(t) = (t - a)^s g(t)$ , где  $s \geq 0$ ,  $g(t) \in k[t]$ , причем  $g(a) \neq 0$ , то кратность корня  $a$  многочлена  $f(t)$  равна  $s$ .

*Доказательство.* Если  $s = 0$ , то  $f(a) = g(a) \neq 0$ , т.е.  $a$  – корень многочлена  $f(t)$  кратности 0. Пусть  $s \geq 1$ ; многочлен  $f(t)$  делится на  $(t - a)^s$ , и надо показать только, что он не делится на  $(t - a)^{s+1}$ . Если бы это было не так, то существовал бы многочлен  $h(t) \in k[t]$ , такой что  $f(t) = (t - a)^{s+1}h(t)$ , и тогда получилось бы, что  $(t - a)^s g(t) = (t - a)^s((t - a)h(t))$ . Поскольку  $k[t]$  – область целостности, отсюда следовало бы, что  $g(t) = (t - a)h(t)$ , и потому  $g(a) = (a - a)h(a) = 0$ , что противоречит предположению леммы.

**Теорема 4.** Пусть  $k$  – поле,  $0 \neq f(t) \in k[t]$ , причем характеристика поля  $k$  равна 0 или больше степени многочлена  $f(t)$ . Элемент  $a \in k$  тогда и только тогда является корнем кратности  $s \geq 1$  многочлена  $f(t)$ , когда

$$f(a) = f'(a) = \dots = f^{(s-1)}(a) = 0, \quad f^{(s)}(a) \neq 0.$$

*Доказательство.* Пусть  $a \in k$ . Если  $n = \deg f(t)$  и  $a_n \neq 0$  – старший коэффициент  $f(t)$ , то  $f^{(n)}(a) = n!a_n$ , а этот элемент при наших предположениях о характеристике поля  $k$  отличен от 0. Однако, быть может, несколько первых производных функции  $f(t)$  обращаются в 0, но всегда найдется наименьший номер  $r$ , такой что  $f^{(r)}(a) \neq 0$ . Если  $f(a) = 0$ , то этот наименьший номер обозначим через  $r_f(a)$ ; если  $f(a) \neq 0$ , положим  $r_f(a) = 0$ .

Утверждение теоремы, очевидно, равносильно тому, что для любого  $a \in k$  число  $r_f(a)$  совпадает с кратностью корня  $a$  многочлена  $f(t)$  (напомним, что не являющийся корнем элемент является корнем кратности 0). Но это сразу следует из леммы 2 и формулы Тейлора. Действительно, пусть  $r = r_f(a)$ . Случай, когда  $r = 0$ , тривиален: тогда  $f(a) \neq 0$  и  $a$  – не корень  $f(t)$ , т.е. корень кратности 0. Пусть  $r \geq 1$ ; тогда  $f(a) = f'(a) = \dots = f^{(r-1)}(a) = 0$ ,  $f^{(r)}(a) \neq 0$ , и по формуле Тейлора имеем:

$$f(t) = f(a) + \frac{f'(a)}{1!}(t-a) + \dots + \frac{f^{(r-1)}(a)}{(r-1)!}(t-a)^{r-1} + \frac{f^{(r)}(a)}{r!}(t-a)^r + \dots + \frac{f^{(n)}(a)}{n!}(t-a)^n = (t-a)^r g(t),$$

где  $g(t) = \frac{f^{(r)}(a)}{r!} + \frac{f^{(r+1)}(a)}{(r+1)!}(t-a) + \dots + \frac{f^{(n)}(a)}{n!}(t-a)^{n-r}$ . Совершенно ясно, что

$g(a) = \frac{f^{(r)}(a)}{r!} \neq 0$ , и потому по лемме 2 число  $r$  является кратностью корня  $a$  многочлена  $f(t)$ .

Из этой теоремы очевидным образом вытекает

**Следствие.** В предположениях теоремы 4 корень кратности  $s \geq 1$  многочлена  $f(t)$  является корнем кратности  $(s-1)$  его производной  $f'(t)$ .

*Отделение кратных корней.* При численном нахождении корней многочлена наличие кратных корней часто осложняет работу. Поэтому было бы полезно освободиться от кратных корней, не потеряв при этом ни одного корня исходного многочлена. Предыдущие результаты показывают, как это сделать.

**Предложение 5.** Пусть  $k$  – поле,  $f(t)$  – ненулевой многочлен над  $k$ , причем характеристика поля  $k$  равна 0 или больше степени многочлена. Пусть, далее,

$d(t) \in k[t]$  – унитарный наибольший общий делитель многочлена  $f(t)$  и его производной  $f'(t)$ , и пусть  $f_1(t) \in k[t]$  – такой многочлен, что  $f(t) = d(t)f_1(t)$ . Тогда в любом поле, содержащем  $k$ , множества корней многочленов  $f(t)$  и  $f_1(t)$  совпадают, но у многочлена  $f_1(t)$  нет кратных корней.

**Доказательство.** Пусть  $K \supseteq k$  – такое поле, в котором многочлен  $f(t)$  раскладывается в произведение  $f(t) = c(t - \alpha_1)^{s_1} \cdots (t - \alpha_r)^{s_r}$ , где  $c \in k$ ,  $\alpha_1, \dots, \alpha_r$  – попарно различные элементы поля  $K$ ,  $s_1, \dots, s_r \geq 1$  (оно существует по теореме 6.2). Поскольку  $f(t) = d(t)f_1(t)$ , а разложение многочлена в произведение унитарных неприводимых многочленов единственно, канонические разложения многочленов  $d(t)$  и  $f_1(t)$  над полем  $K$  имеют аналогичный вид; в частности  $d(t) = (t - \alpha_1)^{p_1} \cdots (t - \alpha_r)^{p_r}$ , где некоторые (или все) из показателей  $p_1, \dots, p_r$  могут быть и равными 0 (тогда соответствующий множитель  $(t - \alpha_i)^{p_i}$  просто отсутствует в разложении). По следствию из теоремы 4  $\alpha_i$  является корнем кратности  $s_i - 1$  производной  $f'(t)$ , т.е.  $f'(t)$  делится на  $(t - \alpha_i)^{s_i-1}$ , но не делится на  $(t - \alpha_i)^{s_i}$ . Поскольку многочлен  $f(t)$  тоже делится на  $(t - \alpha_i)^{s_i-1}$ , на эту же степень  $(t - \alpha_i)$  делится и наибольший общий делитель  $d(t)$  многочленов  $f(t)$  и  $f'(t)$ . При этом  $d(t)$  не делится на  $(t - \alpha_i)^{s_i}$ , потому что иначе на  $(t - \alpha_i)^{s_i}$  делился бы и многочлен  $f'(t) \div d(t)$ . Итак,  $\alpha_i$  – корень  $d(t)$  кратности  $s_i - 1$ , и потому  $p_i = s_i - 1$ .

Таким образом,  $d(t) = (t - \alpha_1)^{s_1-1} \cdots (t - \alpha_r)^{s_r-1}$ , и потому  $f_1(t) = f(t)/d(t) = c(t - \alpha_1) \cdots (t - \alpha_r)$ , т.е. многочлен  $f_1(t) \in k[t]$  имеет в любом поле, содержащем  $k$ , те же корни, что и  $f(t)$ , но все они являются простыми корнями  $f_1(t)$ .

## 9. ДРОБНО-РАЦИОНАЛЬНЫЕ ФУНКЦИИ

**Поле отношений области целостности.** Пусть  $\Lambda$  – область целостности, т.е. коммутативное ассоциативное кольцо с 1. Поле  $K$  называется полем отношений области целостности  $\Lambda$ , если  $\Lambda$  – подкольцо  $K$ , и любой элемент  $\alpha \in K$  представляется в виде  $\alpha = ab^{-1}$ , где  $a, b \in \Lambda$ ,  $b \neq 0$ . Например, поле рациональных чисел  $\mathbb{Q}$  является полем отношений кольца целых чисел  $\mathbb{Z}$ , потому что всякое рациональное число представимо в виде  $a/b = ab^{-1}$ , где  $a, b$  – целые числа, причем  $b \neq 0$ . Это не только самый общеизвестный пример поля отношений; классическое построение рациональных чисел, исходя из целых чисел, как это почти строго делалось в школьных курсах арифметики, подсказывает, как погрузить в поле отношений произвольную область целостности.

**Теорема 1.** *Всякая область целостности может быть вложена в поле, которое является ее полем отношений.*

**Доказательство.** Пусть  $\Lambda$  – область целостности. Дробью над  $\Lambda$  назовем любую пару  $\frac{a}{b}$ , где  $a, b \in \Lambda$ ,  $b \neq 0$ . Здесь знак  $\frac{a}{b}$  не несет никакого содержательного смысла, а служит лишь "знаком препинания", разделяющим первую и вторую компоненту дроби. Введем на множестве всех дробей отношение эквивалентности, считая, что  $\frac{a}{b} \sim \frac{c}{d}$  тогда и только тогда, когда  $ad = bc$ . Кроме того, определим сложение и умножение дробей, положив  $\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd}$ ,  $\frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd}$ . Заметим, что мы снова получим дроби: произведение  $bd$ , являющееся второй компонентой суммы и произведения, не равно 0, потому что  $b \neq 0$ ,  $d \neq 0$ , а кольцо  $\Lambda$  – область целостности.

**Лемма 1.** *Пусть  $a, b, c, d, e, f, g, h \in \Lambda$ , причем  $b, d, f, h \neq 0$ . Тогда:*

- (1)  $\frac{a}{b} \sim \frac{a}{b}$  (рефлексивность);
- (2) если  $\frac{a}{b} \sim \frac{c}{d}$ , то  $\frac{c}{d} \sim \frac{a}{b}$  (симметричность);

- (3) если  $\frac{a}{b} \sim \frac{c}{d}$ ,  $\frac{c}{d} \sim \frac{e}{f}$ , то  $\frac{a}{b} \sim \frac{e}{f}$  (транзитивность);  
 (4) если  $\frac{a}{b} \sim \frac{e}{f}$ ,  $\frac{c}{d} \sim \frac{g}{h}$ , то  $\frac{a}{b} + \frac{c}{d} \sim \frac{e}{f} + \frac{g}{h}$ ,  $\frac{a}{b} \cdot \frac{c}{d} \sim \frac{e}{f} \cdot \frac{g}{h}$ .

*Доказательство.* (1)  $ab = ba$ , так как  $\Lambda$  – коммутативное кольцо.

(2) Если  $ad = bc$ , то  $cb = da$ , опять из-за коммутативности  $\Lambda$ .

(3) Если  $\frac{a}{b} \sim \frac{c}{d}$ ,  $\frac{c}{d} \sim \frac{e}{f}$ , то  $ad = bc$ ,  $cf = de$ . Тогда  $adf = bcf = bde$ . Поскольку  $\Lambda$  – область целостности, левую и правую части этого равенства можно сократить на  $d \neq 0$ ; мы получим, что  $af = be$ , т.е. что  $\frac{a}{b} \sim \frac{e}{f}$ .

(4) Если  $\frac{a}{b} \sim \frac{e}{f}$ ,  $\frac{c}{d} \sim \frac{g}{h}$ , то  $af = be$ ,  $ch = dg$ . Пользуясь этими равенствами, получаем

$$(ad + bc)fh = afdh + bfc h = bedh + bfdg = bd(eh + fg),$$

$$(ac)(fh) = (af)(ch) = (be)(dg) = (bd)(eg),$$

а это как раз и значит, что

$$\frac{a}{b} + \frac{c}{d} = \frac{ad + bc}{bd} \sim \frac{eh + fg}{fh} = \frac{e}{f} + \frac{g}{h}, \quad \frac{a}{b} \cdot \frac{c}{d} = \frac{ac}{bd} \sim \frac{eg}{fh} = \frac{e}{f} \cdot \frac{g}{h}.$$

Первые три утверждения доказанной леммы означают, что  $\sim$  действительно является отношением эквивалентности на множестве дробей, а последнее – что действия сложения и умножения устойчивы относительно этой эквивалентности; поэтому мы можем действовать далее так же, как в главе I при построении кольца вычетов. Поскольку мы еще не раз будем использовать подобные рассуждения, мы повторим формулировки и доказательства нескольких простых фактов из главы I в более общей ситуации, чем это было там и чем это надо сейчас.

*Об отношении эквивалентности.* Пусть  $X$  – множество, на котором задано отношение эквивалентности  $\sim$ , т.е. отношение  $x \sim y$  между элементами  $x, y \in X$ , обладающее свойствами:

- (1) рефлексивность:  $x \sim x$  для всякого  $x \in X$ ;
- (2) симметричность: если  $x, y \in X$  и  $x \sim y$ , то  $y \sim x$ ;
- (3) транзитивность: если  $x, y, z \in X$  и  $x \sim y$ ,  $y \sim z$ , то  $x \sim z$ .

Для элемента  $x \in X$  будем обозначать через  $[x]$  подмножество множества  $X$ , состоящее из всех таких элементов  $y \in X$ , что  $x \equiv y \pmod{n}$ . Это множество называется классом эквивалентности, определенным элементом  $x$ .

**Лемма.** (1) Элемент  $z \in X$  принадлежит классу эквивалентности  $[x]$  тогда и только тогда, когда  $[x] = [z]$ .

(2) Любые два класса эквивалентности или не пересекаются, или совпадают.

*Доказательство.* (1). Пусть  $[x] = [z]$ . Поскольку  $z \sim z$ , элемент  $z$  принадлежит классу  $[z] = [x]$ .

Обратно, пусть  $z \in [x]$ ; тогда, по определению,  $x \sim z$ . Если  $y \in [z]$ , то  $z \sim y$ , и по транзитивности  $x \sim y$ , т.е.  $y \in [x]$ ; таким образом,  $[z] \subseteq [x]$ . Если, наоборот,  $y \in [x]$ , то  $x \sim y$ ; кроме того, из соотношения  $x \sim z$  следует из-за симметричности эквивалентности, что  $z \sim x$ . Снова пользуясь транзитивностью, получаем:  $z \sim y$ , т.е.  $y \in [z]$ , и доказано включение  $[x] \subseteq [z]$ . Сопоставляя полученные включения  $[z] \subseteq [x]$ ,  $[x] \subseteq [z]$ , находим, что  $[x] = [z]$ .

(2). Если пересечение классов вычетов  $[x]$  и  $[y]$  непусто, то существует элемент  $z \in X$ , такой что  $z \in [x]$  и  $z \in [y]$ . Но тогда по (1)  $[x] = [z]$  и  $[y] = [z]$ , т.е.  $[x] = [y]$ .

Пусть теперь на множестве  $X$  задана алгебраическая операция, которая каждой паре элементов  $x, y \in X$  ставит в соответствие элемент  $x \circ y \in X$  (обычно

$\circ$  – это сложение или умножение); предположим, что эта операция устойчива относительно эквивалентности, т.е. выполняется условие

(4) если  $x, x_1, y, y_1 \in X$  и  $x \sim x_1, y \sim y_1$ , то  $x \circ y \sim x_1 \circ y_1$ .

В этом случае мы можем корректно определить операцию  $\circ$  над классами эквивалентности, положив  $[x] \circ [y] = [x \circ y]$ . Это определение не зависит от того, какие именно элементы  $x, y$  мы выбираем в классах: если  $[x] = [x_1], [y] = [y_1]$ , то  $x \sim x_1, y \sim y_1$ , и потому  $x \circ y \sim x_1 \circ y_1$ , а это значит, что  $[x \circ y] = [x_1 \circ y_1]$ .

*Окончание доказательства теоремы 1.* Применим соображения, изложенные в предыдущем пункте, к множеству дробей. Для дроби  $\frac{a}{b}$  обозначим через  $\left[\frac{a}{b}\right]$  множество всех дробей, эквивалентных этой дроби. Пусть  $K$  множество всех таких подмножеств  $\alpha$  множества всех дробей, которые являются классами эквивалентности дробей, т.е. таких, для которых найдется дробь  $\frac{a}{b}$ , такая что  $\alpha = \left[\frac{a}{b}\right]$ . Как мы отметили в предыдущем пункте, устойчивость сложения и умножения дробей относительно нашей эквивалентности позволяет определить сложение и умножение для классов эквивалентности:

$$\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{a}{b} + \frac{c}{d}\right], \quad \left[\frac{a}{b}\right] \cdot \left[\frac{c}{d}\right] = \left[\frac{a}{b} \cdot \frac{c}{d}\right].$$

**Лемма 2.** *Относительно введенных действий множество классов эквивалентности дробей  $K$  является полем.*

*Доказательство.* Надо проверить, что выполняются аксиомы поля:

- (1)  $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$  для любых  $\alpha, \beta, \gamma \in K$  (ассоциативность сложения);
- (2)  $\alpha + \beta = \beta + \alpha$  для любых  $\alpha, \beta \in K$  (коммутативность сложения);
- (3) существует такой элемент  $\bar{0} \in K$ , что  $\bar{0} + \alpha = \alpha$  для любого  $\alpha \in K$ ;
- (4) для любого  $\alpha \in K$  существует такой элемент  $-\alpha \in K$ , что  $\alpha + (-\alpha) = \bar{0}$ ;
- (5)  $\alpha(\beta\gamma) = (\alpha\beta)\gamma$  для любых  $\alpha, \beta, \gamma \in K$  (ассоциативность умножения);
- (6)  $\alpha\beta = \beta\alpha$  для любых  $\alpha, \beta \in K$  (коммутативность умножения);
- (7) существует такой элемент  $\bar{1} \in K$ , что  $\bar{1} \cdot \alpha = \alpha$  для любого  $\alpha \in K$ ;
- (8)  $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$  для любых  $\alpha, \beta, \gamma \in K$  (дистрибутивность умножения относительно сложения);
- (9) для любого  $\alpha \in K$ , не равного  $\bar{0}$ , существует такой элемент  $\alpha^{-1} \in K$ , что  $\alpha\alpha^{-1} = \bar{1}$ .

Пусть  $\alpha = \left[\frac{a}{b}\right], \beta = \left[\frac{c}{d}\right], \gamma = \left[\frac{e}{f}\right]$ ; в качестве  $\bar{0}, \bar{1}, -\alpha$  возьмем классы  $\left[\frac{0}{1}\right], \left[\frac{1}{1}\right], \left[\frac{-a}{b}\right]$ . Тогда соотношения (1)-(8) примут следующий вид.

- (1)  $\left[\frac{a}{b}\right] + \left(\left[\frac{c}{d}\right] + \left[\frac{e}{f}\right]\right) = \left(\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right]\right) + \left[\frac{e}{f}\right];$
- (2)  $\left[\frac{a}{b}\right] + \left[\frac{c}{d}\right] = \left[\frac{c}{d}\right] + \left[\frac{a}{b}\right];$
- (3)  $\left[\frac{0}{1}\right] + \left[\frac{a}{b}\right] = \left[\frac{a}{b}\right];$
- (4)  $\left[\frac{a}{b}\right] + \left[\frac{-a}{b}\right] = \left[\frac{0}{1}\right];$
- (5)  $\left[\frac{a}{b}\right] \left(\left[\frac{c}{d}\right] \left[\frac{e}{f}\right]\right) = \left(\left[\frac{a}{b}\right] \left[\frac{c}{d}\right]\right) \left[\frac{e}{f}\right];$
- (6)  $\left[\frac{a}{b}\right] \left[\frac{c}{d}\right] = \left[\frac{c}{d}\right] \left[\frac{a}{b}\right];$
- (7)  $\left[\frac{1}{1}\right] \cdot \left[\frac{a}{b}\right] = \left[\frac{a}{b}\right];$
- (8)  $\left[\frac{a}{b}\right] \left(\left[\frac{c}{d}\right] + \left[\frac{e}{f}\right]\right) = \left[\frac{a}{b}\right] \left[\frac{c}{d}\right] + \left[\frac{a}{b}\right] \left[\frac{e}{f}\right].$

Их проверка получается прямыми вычислениями с учетом того, что  $\Lambda$  – коммутативное ассоциативное кольцо с 1. В качестве примеров проверим соотношения

(1), (4) и (8); первое из них – "самое сложное", а два других являются единственными из соотношений (1)–(8), при проверке которых приходится заменять дробь на эквивалентную ей. Соотношение (1) вытекает из равенства

$$\frac{a}{b} + \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} + \frac{cf + de}{df} = \frac{a(df) + b(cf + de)}{b(df)} = \frac{(ad + bc) + (bd)e}{(bd)f} = \left(\frac{a}{b} + \frac{c}{d}\right) + \frac{e}{f}.$$

Далее,  $\frac{a}{b} + \frac{-a}{b} = \frac{ab + b(-a)}{b^2} = \frac{0}{b^2} \sim \frac{0}{1}$ , что означает справедливость соотношения (4). Наконец, из цепочки соотношений

$$\frac{a}{b} \left(\frac{c}{d} + \frac{e}{f}\right) = \frac{a}{b} \cdot \frac{cf + de}{df} = \frac{a(cf + de)}{b(df)} \sim \frac{(ac)(bf) + (bd)(ae)}{(bd)(bf)} = \frac{a}{b} \cdot \frac{c}{d} + \frac{a}{b} \cdot \frac{e}{f}$$

вытекает (8).

Проверим теперь, что аксиома (9), выделяющая поля в классе коммутативных ассоциативный колец с 1, тоже выполняется в  $K$ . Пусть  $\alpha = \left[\frac{a}{b}\right] \neq \bar{0} = \left[\frac{0}{1}\right]$ ; тогда неверно, что  $a \cdot 1 = b \cdot 0$ , и потому  $a = a \cdot 1 \neq b \cdot 0 = 0$ , а значит,  $\frac{b}{a}$  тоже является дробью. Теперь ясно, что в качестве  $\alpha^{-1}$  можно взять класс  $\left[\frac{b}{a}\right] \in K$ :

$$\alpha \left[\frac{b}{a}\right] = \left[\frac{a}{b}\right] \left[\frac{b}{a}\right] = \left[\frac{ab}{ba}\right] = \left[\frac{1}{1}\right] = \bar{1}.$$

Лемма полностью доказана.

Элементы из кольца  $\Lambda$  мы будем рассматривать как элементы из  $K$ , отождествив  $a \in \Lambda$  с классом дробей  $\left[\frac{a}{1}\right]$ . Такое отождествление не приведет к противоречиям: действия над элементами  $a, b \in \Lambda$ , рассматриваемыми как элементы из  $\Lambda$  и как элементы из  $K$ , приводят к одинаковым результатам:

$$\left[\frac{a}{1}\right] + \left[\frac{b}{1}\right] = \left[\frac{a+b}{1}\right], \quad \left[\frac{a}{1}\right] \cdot \left[\frac{b}{1}\right] = \left[\frac{ab}{1}\right].$$

Кроме того, при таком отождествлении кольцо  $\Lambda$  не "сжимается": разные элементы  $\Lambda$  остаются различными и в  $A[[t]]$ . Действительно, равенство  $\left[\frac{a}{1}\right] + \left[\frac{b}{1}\right]$  равносильно равенству  $a = a \cdot 1 = 1 \cdot b = b$ . Таким образом, кольцо  $\Lambda$  оказалось вложенным в поле  $K$ .

Осталось показать, что  $K$  является полем отношений кольца  $\Lambda$ , т.е. что каждый элемент из  $K$  представим в виде  $ab^{-1}$ , где  $a, b \in \Lambda, b \neq 0$ . Но это очевидно:

$$\left[\frac{a}{b}\right] = \left[\frac{a}{1}\right] \cdot \left[\frac{1}{b}\right] = \left[\frac{a}{1}\right] \cdot \left[\frac{b}{1}\right]^{-1} = ab^{-1}.$$

Теорема 1 доказана.

Мы увидели в конце доказательства, что если  $a, b \in \Lambda, b \neq 0$ , то  $\frac{a}{b} = ab^{-1} = \left[\frac{a}{b}\right]$ , где в левой части горизонтальная черта является знаком деления в поле  $K$  одного элемента из  $\Lambda$  на другой, а в правой – это "знак препинания", используемый для записи дробей. Таким образом, это равенство ни в коем случае не означает, что класс дробей равен своему представителю.

В дальнейшем элементы из поля отношений мы всегда будем записывать в виде отношения в  $K$  двух элементов из  $\Lambda$ , т.е. в виде  $\frac{a}{b}$ , где горизонтальная черта является знаком деления в  $K$ .



*Дробно-рациональные функции.* Пусть  $k$  – поле; поле отношений кольца многочленов  $k[t_1, \dots, t_n]$  называется полем дробно-рациональных функций от  $t_1, \dots, t_n$  над полем  $k$  и обозначается через  $k(t_1, \dots, t_n)$ . Элементы этого поля называются дробно-рациональными функциями, хотя как функции мы их рассматривать не будем, и каждый из них представим в виде  $\frac{f(t_1, \dots, t_n)}{g(t_1, \dots, t_n)}$ , где  $f(t_1, \dots, t_n)$ ,  $g(t_1, \dots, t_n)$  – многочлены, причем второй из них отличен от 0.

В дальнейшем мы будем заниматься только дробно-рациональными функциями от одной переменной. Дробно-рациональная функция  $\frac{f(t)}{g(t)} \in k(t)$  называется правильной, если  $\deg f(t) < \deg g(t)$ . Это определение не зависит от выбора представления дробно-рациональной функции в виде отношения двух многочленов: если  $\frac{f(t)}{g(t)} = \frac{f_1(t)}{g_1(t)}$  и  $\deg f(t) < \deg g(t)$ , то  $f(t)g_1(t) = g(t)f_1(t)$  и потому  $\deg f(t) + \deg g_1(t) = \deg g(t) + \deg f_1(t)$ , откуда следует, что

$$\deg f_1(t) = \deg g_1(t) + (\deg f(t) - \deg g(t)) < \deg g_1(t).$$

**Предложение 1.** *Сумма, разность и произведение правильных дробно-рациональных функций – снова правильные дробно-рациональные функции. Всякая дробно-рациональная функция однозначно представляется в виде суммы многочлена и правильной дробно-рациональной функции.*

*Доказательство.* Пусть  $\frac{f_1(t)}{g_1(t)}, \frac{f_2(t)}{g_2(t)}$  – правильные дробно-рациональные функции; это значит, что  $\deg f_1(t) < \deg g_1(t)$ ,  $\deg f_2(t) < \deg g_2(t)$ . Но тогда

$$\begin{aligned} \deg f_1(t)f_2(t) &= \deg f_1(t) + \deg f_2(t) < \deg g_1(t) + \deg g_2(t) = \deg g_1(t)g_2(t), \\ \deg f_1(t)g_2(t) &= \deg f_1(t) + \deg g_2(t) < \deg g_1(t) + \deg g_2(t) = \deg g_1(t)g_2(t), \\ \deg g_1(t)f_2(t) &= \deg g_1(t) + \deg f_2(t) < \deg g_1(t) + \deg g_2(t) = \deg g_1(t)g_2(t), \end{aligned}$$

а потому и  $\deg(f_1(t)g_2(t) + g_1(t)f_2(t)) < \deg g_1(t)g_2(t)$ . Следовательно,

$$\frac{f_1(t)}{g_1(t)} + \frac{f_2(t)}{g_2(t)} = \frac{f_1(t)g_2(t) + g_1(t)f_2(t)}{g_1(t)g_2(t)}, \quad \frac{f_1(t)}{g_1(t)} \cdot \frac{f_2(t)}{g_2(t)} = \frac{f_1(t)f_2(t)}{g_1(t)g_2(t)}$$

– правильные дробно-рациональные функции.

Пусть теперь  $\frac{f(t)}{g(t)}$  – произвольная дробно-рациональная функция. Поскольку  $g(t) \neq 0$ , по теореме о делении с остатком для многочленов существуют многочлены  $q(t), r(t)$ , такие что  $f(t) = q(t)g(t) + r(t)$ ,  $\deg r(t) < \deg g(t)$ . Тогда  $\frac{f(t)}{g(t)} = q(t) + \frac{r(t)}{g(t)}$  и есть представление  $\frac{f(t)}{g(t)}$  в виде суммы многочлена и правильной дробно-рациональной функции. Если  $\frac{f(t)}{g(t)} = q_1(t) + \frac{r_1(t)}{g_1(t)}$  было бы другим подобным представлением, то многочлен  $q_1(t) - q(t)$  был бы равен правильной дроби  $\frac{r(t)}{g(t)} - \frac{r_1(t)}{g_1(t)}$ , а это возможно только если  $q_1(t) - q(t) = 0$ . Таким образом,  $q_1(t) = q(t)$ , а потому и  $\frac{r_1(t)}{g_1(t)} = \frac{f(t)}{g(t)} - q_1(t) = \frac{f(t)}{g(t)} - q(t) = \frac{r(t)}{g(t)}$ .

*Простейшие дробно-рациональные функции.* Дробно-рациональная функция над полем  $k$  называется простейшей, если она представляется в виде  $\frac{g(t)}{(p(t))^s}$ , где

$p(t), g(t) \in k[t]$ ,  $s \geq 1$  – натуральное число, причем  $p(t)$  – унитарный неприводимый над  $k$  многочлен, и  $\deg g(t) < \deg p(t)$ . Таким образом, простейшими над алгебраически замкнутым полем  $k$  будут дробно-рациональные функции  $\frac{a}{(t-c)^s}$ , где  $a, c \in k$ . Над полем вещественных чисел  $\mathbb{R}$  простейшими будут дробно-рациональные функции видов

$$\frac{a}{(t-c)^s}, \quad \frac{at+b}{(t^2+pt+q)^s} \quad (s \geq 1, a, b, c, p, q \in \mathbb{R}, \text{ причем } p^2 < 4q).$$

**Теорема 2.** *Всякая правильная дробно-рациональная функция раскладывается в сумму нескольких простейших дробно-рациональных функций.*

*Доказательство.* Сначала докажем, что всякую правильную дробно-рациональную функцию можно разложить в сумму правильных дробно-рациональных функций, знаменатели которых – степени неприводимых многочленов.

**Лемма 3.** *Пусть  $k$  – поле,  $f(t) \in k[t]$ ,  $p_1(t), \dots, p_r(t) \in k[t]$  – попарно различные неприводимые унитарные многочлены,  $s_1, \dots, s_r \geq 1$  – натуральные числа, и пусть  $g(t) = (p_1(t))^{s_1} \dots (p_r(t))^{s_r}$ . Если  $\deg f(t) < \deg g(t)$ , то существуют такие многочлены  $f_1(t), \dots, f_r(t) \in k[t]$ , что  $\deg f_i(t) < \deg(p_i(t))^{s_i}$  при  $1 \leq i \leq r$  и*

$$\frac{f(t)}{g(t)} = \frac{f_1(t)}{(p_1(t))^{s_1}} + \dots + \frac{f_r(t)}{(p_r(t))^{s_r}}.$$

*Доказательство.* Обозначим через  $g_i(t)$  произведение всех многочленов  $(p_j(t))^{s_j}$ , кроме  $(p_i(t))^{s_i}$ , так что  $g(t) = (p_i(t))^{s_i} g_i(t)$ . Покажем, что  $g_1(t), \dots, g_r(t)$  – взаимно простые в совокупности многочлены. Действительно, пусть многочлен  $d(t) \in k[t]$  является их наибольшим общим делителем. Если неверно, что многочлены взаимно просты в совокупности, то  $\deg d(t) \geq 1$ , и существует неприводимый унитарный многочлен  $q(t)$ , на который делится  $d(t)$ , а значит, и все многочлены  $g_i(t)$ . В частности,  $g_1(t) = (p_2(t))^{s_2} \dots (p_r(t))^{s_r} \div q(t)$ ; поскольку все сомножители и многочлен  $q(t)$  неприводимые и унитарные, это возможно лишь тогда, когда  $q(t)$  совпадает с одним из многочленов  $p_j(t)$ ,  $2 \leq j \leq r$ . Но  $g_j(t)$  не делится на  $p_j(t) = q(t)$ ; мы пришли к противоречию, которое доказывает, что многочлены  $g_1(t), \dots, g_r(t)$  взаимно просты в совокупности.

По основному свойству взаимно простых в совокупности элементов, существуют такие многочлены  $F_1(t), \dots, F_r(t) \in k[t]$ , что

$$1 = F_1(t)g_1(t) + \dots + F_r(t)g_r(t).$$

Обозначим через  $f_i(t)$  и  $Q_i(t)$  остаток и неполное частное от деления многочлена  $f(t)F_i(t)$  на  $(p_i(t))^{s_i}$ , так что

$$f(t)F_i(t) = f_i(t) + Q_i(t)(p_i(t))^{s_i}, \quad \deg f_i(t) < \deg(p_i(t))^{s_i} \quad (1 \leq i \leq r).$$

Тогда получается:

$$\begin{aligned} f(t) &= f(t)F_1(t)g_1(t) + \dots + f(t)F_r(t)g_r(t) = \\ &= f_1(t)g_1(t) + Q_1(t)(p_1(t))^{s_1}g_1(t) + \dots + f_r(t)g_r(t) + Q_r(t)(p_r(t))^{s_r}g_r(t) = \\ &= f_1(t)g_1(t) + \dots + f_r(t)g_r(t) + (Q_1(t) + \dots + Q_r(t))g(t). \end{aligned}$$

Степень каждого из многочленов  $f_i(t)g_i(t)$  меньше степени многочлена  $g(t) = (p_i(t))^{s_i}g_i(t)$ , потому что  $\deg f_i(t) < \deg(p_i(t))^{s_i}$ . Степень многочлена  $f(t)$  тоже меньше степени многочлена  $g(t)$ . Поэтому

$$\begin{aligned} \deg g(t) &> \deg(f(t) - (f_1(t)g_1(t) + \dots + f_r(t)g_r(t))) = \deg(Q_1(t) + \dots + Q_r(t))g(t) = \\ &= \deg(Q_1(t) + \dots + Q_r(t)) + \deg g(t), \end{aligned}$$

а это возможно только если  $\deg(Q_1(t) + \dots + Q_r(t)) = -\infty$ , т.е. если многочлен  $Q_1(t) + \dots + Q_r(t)$  нулевой. Итак,  $f(t) = f_1(t)g_1(t) + \dots + f_r(t)g_r(t)$ , и

$$\frac{f(t)}{g(t)} = \frac{f_1(t)g_1(t)}{g(t)} + \dots + \frac{f_r(t)g_r(t)}{g(t)} = \frac{f_1(t)}{(p_1(t))^{s_1}} + \dots + \frac{f_r(t)}{(p_r(t))^{s_r}}.$$

**Лемма 4.** Пусть  $s \geq 1$  – натуральное число,  $h(t), p(t) \in k[t]$ , причем  $\deg p(t) \geq 1$ ,  $\deg h(t) < s \deg p(t)$ . Тогда существуют многочлены  $a_0(t), \dots, a_{s-1}(t)$ , такие что  $\deg a_i(t) < \deg p(t)$  для всех  $i$ ,  $0 \leq i \leq s-1$ , и

$$h(t) = a_0(t) + a_1(t)p(t) + \dots + a_{s-1}(t)(p(t))^{s-1}.$$

*Доказательство.* Индукция по  $s$  многочлена  $h(t)$ ; если  $s = 1$ , то достаточно положить  $a_0(t) = h(t)$ . Пусть  $s > 1$  и для  $s-1$  утверждение уже доказано. По теореме о делении с остатком существуют такие многочлены  $a_{s-1}(t), h_1(t)$ , что  $h(t) = a_{s-1}(t)(p(t))^{s-1} + h_1(t)$ , где  $\deg h_1(t) < \deg(p(t))^{s-1} = (s-1) \deg p(t)$ . Сравнивая степени, получаем:

$$\deg a_{s-1}(t) + (s-1) \deg p(t) = \deg(a_{s-1}(t)(p(t))^{s-1}) = \deg(h(t) - h_1(t)) < s \deg p(t),$$

поэтому  $\deg a_{s-1}(t) < \deg p(t)$ . По предположению индукции, существуют многочлены  $a_0(t), \dots, a_{s-2}(t)$ , такие что  $\deg a_i(t) < \deg p(t)$  для всех  $i$ ,  $0 \leq i \leq s-2$ , и  $h_1(t) = a_0(t) + a_1(t)p(t) + \dots + a_{s-2}(t)(p(t))^{s-2}$ . Тогда

$$h(t) = a_{s-1}(t)(p(t))^{s-1} + h_1(t) = a_0(t) + a_1(t)p(t) + \dots + a_{s-1}(t)(p(t))^{s-1}$$

и будет нужным представлением многочлена  $h(t)$ .

Теперь легко завершить доказательство теоремы 2. Пусть  $\frac{f(t)}{g(t)}$  – правильная дробно-рациональная функция над полем  $k$ ; домножая, если надо, числитель и знаменатель на ненулевую константу, добьемся того, чтобы многочлен  $g(t)$  был унитарным. Тогда  $g(t)$  раскладывается в произведение  $g(t) = (p_1(t))^{s_1} \dots (p_r(t))^{s_r}$ , где  $p_1(t), \dots, p_r(t) \in k[t]$  – попарно различные неприводимые унитарные многочлены,  $s_1, \dots, s_r \geq 1$  – натуральные числа. Поскольку наша дробно-рациональная функция правильная,  $\deg f(t) < \deg g(t)$ . Поэтому по лемме 3 найдутся такие многочлены  $f_1(t), \dots, f_r(t) \in k[t]$ , что

$$\frac{f(t)}{g(t)} = \frac{f_1(t)}{(p_1(t))^{s_1}} + \dots + \frac{f_r(t)}{(p_r(t))^{s_r}},$$

и все слагаемые в этой сумме – правильные дробно-рациональные функции. Докажем, что каждое из слагаемых раскладывается в сумму простейших дробно-рациональных функций. Пусть  $1 \leq i \leq r$ ; поскольку  $\deg f_i(t) < s_i \deg p_i(t)$ , по лемме 4 найдутся такие многочлены  $a_0(t), \dots, a_{s_i-1}(t)$ , что  $\deg a_j(t) < \deg p_i(t)$  для всех  $j$ ,  $0 \leq j \leq s_i-1$ , и  $f_i(t) = a_0(t) + a_1(t)p_i(t) + \dots + a_{s_i-1}(t)(p_i(t))^{s_i-1}$ . Тогда

$$\begin{aligned} \frac{f_i(t)}{(p_i(t))^{s_i}} &= \frac{a_0(t) + a_1(t)p_i(t) + \dots + a_{s_i-1}(t)(p_i(t))^{s_i-1}}{(p_i(t))^{s_i}} = \\ &= \frac{a_0(t)}{(p_i(t))^{s_i}} + \frac{a_1(t)}{(p_i(t))^{s_i-1}} + \dots + \frac{a_{s_i-1}(t)}{p_i(t)}, \end{aligned}$$

и все слагаемые в последней сумме – простейшие дробно-рациональные функции.

**Замечание.** Из доказательства теоремы видно, что в разложении в сумму простейших дробно-рациональной функции  $\frac{f(t)}{g(t)}$ , где  $g(t) = (p_1(t))^{s_1} \dots (p_r(t))^{s_r}$ , причем  $p_1(t), \dots, p_r(t) \in k[t]$  – попарно различные неприводимые унитарные многочлены, присутствуют лишь простейшие слагаемые, знаменатели которых имеют вид  $(p_i(t))^j$ , где  $1 \leq i \leq r$ ,  $1 \leq j \leq s_i$ .

*Формула Лагранжа для разложения в сумму простейших дробей.* В случае, когда знаменатель правильной дробно-рациональной функции не имеет кратных корней и полностью раскладывается над  $k$  в произведение линейных множителей, можно написать явную формулу для разложения дробно-рациональной функции в сумму простейших.

**Предложение 2.** Пусть  $k$  – поле, и пусть  $a_1, a_2, \dots, a_n$  – попарно различные элементы из  $k$ . Пусть, далее,  $g(t) = (t - a_1) \cdots (t - a_i) \cdots (t - a_n)$ , а  $f(t) \in k[t]$  – многочлен, степень которого меньше  $n$ . Тогда

$$\frac{f(t)}{g(t)} = \sum_{i=1}^n \frac{f(a_i)/g'(a_i)}{t - a_i}.$$

*Доказательство.* Согласно замечанию к доказательству теоремы 2, правильная дробно-рациональная функция  $\frac{f(t)}{g(t)}$  представляется в виде суммы простейших дробно-рациональных функций со знаменателями  $(t - a_i)$ ,  $1 \leq i \leq n$ , т.е.

$$\frac{f(t)}{g(t)} = \frac{b_1}{t - a_1} + \dots + \frac{b_i}{t - a_i} + \dots + \frac{b_n}{t - a_n},$$

где числители  $b_i$  – элементы из  $k$ . Для того, чтобы найти элементы  $b_i$ , умножим предыдущее равенство на  $g(t)$ , и мы получим соотношение

$$f(t) = b_1 g_1(t) + \dots + b_i g_i(t) + \dots + b_n g_n(t),$$

где  $g_i(t)$  – произведения всех биномов  $(t - a_j)$ , кроме  $(t - a_i)$ ; иначе говоря,  $g_i(t)$  – такие многочлены, что  $g(t) = g_i(t)(t - a_i)$ . Взяв значение обеих частей равенства при  $t = a_i$  и заметив, что  $g_j(a_i) = 0$  при  $j \neq i$ , найдем, что  $f(a_i) = b_i g_i(a_i)$ . Найдем  $g_i(a_i)$ , продифференцировав многочлен  $g(t) = g_i(t)(t - a_i)$  и взяв значение производной при  $t = a_i$ :

$$g'(t) = g'_i(t)(t - a_i) + g_i(t)(t - a_i)' = g'_i(t)(t - a_i) + g_i(t),$$

$$g'(a_i) = g'_i(a_i)(a_i - a_i) + g_i(a_i) = g_i(a_i).$$

Итак,  $g_i(a_i) = g'(a_i) \neq 0$ , потому что корень  $a_i$  многочлена  $g(t)$  не кратный, и значит,  $b_i = f(a_i)/g_i(a_i) = f(a_i)/g'(a_i)$ .