Алгебра. Глава 3. Многочлены.

Д. В. Карпов

2022

Определение

Пусть K — коммутативное кольцо.

1) *Кольцо многочленов* над K состоит из бесконечных последовательностей $(a_0, \dots, a_n, \dots)$ с коэффициентами из K, в которых лишь конечное число ненулевых коэффициентов.

2) *Сложение* многочленов покоэффициентное:

$$(a_0, \dots, a_n, \dots) + (b_0, \dots, b_n, \dots) := (a_0 + b_0, \dots, a_n + b_n, \dots).$$

3) Определим *умножение* многочленов:

$(a_0, \dots, a_n, \dots) \cdot (b_0, \dots, b_n, \dots) = (c_0, \dots, c_n, \dots)$, где

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

4) *Степень* многочлена $f = (a_0, \dots, a_n, \dots)$ — это максимальный номер ненулевого коэффициента (обозначение: $\deg(f)$). Отдельно определим степень многочлена $0 := (0, \dots, 0, \dots)$: положим $\deg(0) := -\infty$. Если $\deg(f) = n \in \mathbb{N}_0$, то a_n называется *старшим коэффициентом* f.

• Если $f = (a_0, \dots, a_n, \dots)$ и $\deg(f) \le n$, часто применяется запись $f(t) = a_n t^n + \dots + a_1 t + a_0$, где t — *формальная переменная*. Кольцо многочленов над кольцом K обозначается через $K[t]$, где t — переменная.

• Пусть K — коммутативное кольцо, $f, g \in K[t]$.

Свойство 1

$\deg(fg) \le \deg(f) + \deg(g)$. *Если K — кольцо без делителей 0, то* $\deg(fg) = \deg(f) + \deg(g)$.

Доказательство. • Если один из многочленов f и g равен 0, то несложно проверить, что произведение также равно 0. Тогда $\deg(fg) = -\infty = \deg(f) + \deg(g)$ (так как $-\infty$ при сложении с любой возможной степенью даст $-\infty$.

• Пусть $\deg(f) = n$, $\deg(g) = m$, где $m, n \in \mathbb{N}_0$, $f = (a_1, \dots, a_s, \dots)$, $g = (b_1, \dots, b_s, \dots)$ и $fg = (c_1, \dots, c_s, \dots)$.

• При $k > n + m$ имеем $c_k = (\sum\limits_{i=0}^{n-1} a_i b_{k-i}) + (\sum\limits_{i=n}^{k} a_i b_{k-i}) = 0$.

(В первой сумме $k - i > m$, поэтому $b_{k-i} = 0$. Во второй сумме $i > n$, поэтому $a_i = 0$.)

• Значит, $\deg(fg) \le \deg(f) + \deg(g)$.

• $c_{n+m} = (\sum\limits_{i=0}^{n-1} a_i b_{n+m-i}) + a_n b_m + (\sum\limits_{i=n+1}^{n+m} a_i b_{n+m-i}) = a_n b_m \ne 0$,

если K — без делителей 0. В этом случае $\deg(fg) = m + n$.

• (В первой сумме $n + m - i > m$, поэтому $b_{n+m-i} = 0$. Во второй сумме $i > n$, поэтому $a_i = 0$.) $\square$

Свойство 2

$\deg(f+g) \le \max(\deg(f), \deg(g))$. Если $\deg(f) \ne \deg(g)$, то $\deg(f+g) = \max(\deg(f), \deg(g))$.

Доказательство. • $f = (a_1, \dots, a_n, \dots)$, $g = (b_1, \dots, b_n, \dots)$.

• При $k > \max(\deg(f), \deg(g))$ имеем $a_k = b_k = 0$, а значит и $a_k + b_k = 0$. Следовательно, $\deg(f+g) \le \max(\deg(f), \deg(g))$.

• Пусть НУО $\deg(f) = n > \deg(g)$. Тогда $a_n + b_n = a_n + 0 \ne 0$, а значит, в этом случае $\deg(f+g) = n$. □

Теорема 1

Пусть K — коммутативное кольцо. Тогда $K[t]$ — тоже коммутативное кольцо. Если при этом K — кольцо с 1, то $K[t]$ — тоже с 1.

Доказательство. Ассоциативность и коммутативность сложения в $K[t]$ следуют из ассоциативности и коммутативности сложения в K (так как сложение покоэффициентное).

Ноль. Несложно проверить, что многочлен 0 будет нолем в $K[t]$.

Обратный элемент по сложению. Для $f = (a_0, \dots, a_n, \dots)$ положим $-f := (-a_0, \dots, -a_n, \dots)$.

Коммутативность умножения. Пусть $f = (a_0, \dots, a_n, \dots,)$ и $g = (b_0, \dots, b_n, \dots,)$, $fg = (d_0, \dots, d_n, \dots)$ и $gf = (d'_0, \dots, d'_n, \dots)$. Тогда $d_n = \sum\limits_{i=0}^{n} a_i b_{n-i} = \sum\limits_{j=0}^{n} b_j a_{n-j} = d'_n$.

Дистрибутивность. Пусть $h = (c_0, \dots, c_n, \dots,)$, $(f+g)h = (d_o, \dots, d_n, \dots,)$, $fh = (p_0, \dots, p_n, \dots,)$ и $gh = (q_0, \dots, q_n, \dots,)$. Тогда $d_n = \sum\limits_{i=0}^{n}(a_i + b_i)c_{n-i} = (\sum\limits_{i=0}^{n} a_i c_{n-i}) + (\sum\limits_{i=0}^{n} b_i c_{n-i}) = p_n + q_n$, а это коэффициент многочлена $fh + gh$.

Ассоциативность умножения. Пусть $fg = (d_0, \dots, d_n, \dots)$ и $(fg)h = (p_0, \dots, p_n, \dots)$. Тогда

$$p_n = \sum_{k=0}^{n} d_k c_{n-k} = \sum_{k=0}^{n}(\sum_{i=0}^{k} a_i b_{k-i})c_{n-k} = \sum_{i,j,\ell\in\mathbb{N}_0,\ i+j+\ell=n} a_i b_j c_\ell.$$

При другом порядке скобок, очевидно, получится то же самое.

Единица. Если существует $1 \in K$, то несложно проверить, что $1 := (1, 0, \dots, 0, \dots)$ — единица в $K[t]$. $\square$

Константы

Лемма 1

Пусть K — коммутативное кольцо, $\varphi : K \to K[t]$ задано формулой $\varphi(c) := (c, 0, 0, \dots)$. Тогда φ — мономорфизм колец.

Доказательство. • Пусть $a, b \in K$. Тогда $\varphi(a+b) = (a+b, 0, \dots, 0, \dots) = (a, 0, \dots, 0, \dots) + (b, 0, \dots, 0, \dots) = \varphi(a) + \varphi(b)$.

• $\varphi(ab) = (ab, 0, \dots, 0, \dots)$, а $\varphi(a)\varphi(b) = (a, 0, \dots, 0, \dots) \cdot (b, 0, \dots, 0, \dots) =: (c_0, c_1, \dots)$.

Тогда $c_0 = a_0 b_0$, а при $n > 0$ имеем $c_n = \sum\limits_{i=0}^{n} a_i b_{n-i} = 0$, так как каждое слагаемое равно 0 (если $i > 0$, то $a_i = 0$, иначе $b_{n-i} = 0$). Значит, $\varphi(ab) = \varphi(a)\varphi(b)$.

• Таким образом, φ — гомоморфизм.

• Пусть $a \in \mathrm{Ker}(\varphi)$, Тогда $(a, 0, \dots) = \varphi(a) = (0, 0, \dots)$, значит, $a = 0$.

Определение

Многочлен вида $(a, 0, 0, \dots)$ называется константой. Мы будем отождествлять такой многочлен с числом $a \in K$ и считать, что $K \subset K[t]$.

• Нетрудно проверить, что для $a \in K$ и $f = (b_0, b_1, \dots)$ выполнено $(a, 0, 0 \dots) \cdot (b_0, b_1, \dots) = (ab_0, ab_1, \dots)$. Мы будем обозначать такой многочлен af и говорить, что он получен из f умножением на константу.

• Далее будем рассматривать случай, когда K — поле (то есть, многочлены с коэффициентами из поля).

Лемма 2

Если K — поле, то обратимые элементы $K[t]$ — это в точности ненулевые константы.

Доказательство. • Пусть $f, g \in K[t]$, $fg = 1$. Тогда $0 = \deg(1) = \deg(f) + \deg(g)$, откуда следует $\deg(f) = \deg(g) = 0$, то есть, f и g — ненулевые константы.

• Наоборот, если $a \in K$, $a \neq 0$, то существует $a^{-1} \in K$. Числам a и a^{-1} соответствуют взаимно обратные многочлены-константы в $K[t]$. $\square$

Ассоциированные многочлены

Определение

Пусть $f, g \in K[t]$, K — поле. Будем говорить, что f и g *ассоциированы*, если $f = cg$, где $c \in K$, $c \neq 0$ (обозначение: $f \sim g$).

Лемма 3

Ассоциированность — отношение эквивалентности.

Доказательство. Рефлексивность. $f = 1 \cdot f$, значит, $f \sim f$.

Симметричность. Пусть $f \sim g$, тогда $\exists a \in K$, $a \neq 0$, такое, что $f = ag$. Тогда $g = a^{-1}f$, а значит, $g \sim f$.

Транзитивность. Пусть $f \sim g$ и $g \sim h$, тогда $\exists a, b \in K$ такие, что $f = ag$ и $g = bh$. Тогда $f = ag = (ab)h$, а значит, $f \sim h$. $\square$

- Если $f, g \in K[t]$ и $f \sim g$, то $\deg(f) = \deg(g)$.
- $-f = (-1) \cdot f$, следовательно, $(-f) \sim f$.

Теорема о делении с остатком в кольце многочленов над полем.

Теорема 2

Пусть K — поле, $f, g \in K[t]$, причем $g \neq 0$. Тогда существуют единственные такие $q, r \in K[t]$, что $f = gq + r$ и $\deg(r) < \deg(g)$.

• Многочлен r из этого представления называется остатком от деления f на g.

Доказательство. Пусть $\deg(f) = n$, $\deg(g) = m$, $f(t) = a_n t^n + \dots + a_0$ и $g(t) = b_m t^m + \dots + b_0$.
$\exists$. • Индукция по $\deg(f)$. База для случая $n < m$: тогда подходит $q = 0$ и $r = f$.

Переход. • Пусть $n \geq m$ и для многочленов степени менее n утверждение доказано.

• Так как $f_1(t) = f(t) - \frac{a_n}{b_m} t^{n-m} \cdot g(t)$ имеет степень $\deg(f_1) < n$, по индукционному предположению, $f_1 = q_1 g + r$, где $\deg(r) < m$.

• Тогда $f(t) = (q_1(t) + \frac{a_n}{b_m} t^{n-m}) \cdot g(t) + r(t)$ — искомое представление для f.

! Пусть $f = q_1g + r_1 = q_2g + r_2$, где $\deg(r_1) < m$ и $\deg(r_2) < m$. Тогда $r_1 - r_2 = g(q_2 - q_1)$.

- Пусть $q_1 \neq q_2$. Тогда $\deg(q_2 - q_1) \in \mathbb{N}_0$ и $\deg((q_2 - q_1)g) = \deg(q_2 - q_1) + \deg(g) \geq m$. С другой стороны, $\deg(r_1 - r_2) \leq \max(\deg(r_1), \deg(r_2)) < m$, противоречие.
- Значит, $q_1 = q_2$, тогда и $r_1 = r_2$. $\square$

Делимость многочленов

Определение

Пусть K — поле, $f, g \in K[t]$, $g \neq 0$. Говорят, что f **делится** на g (обозначение $f \,\vdots\, g$), если существует такой $h \in K[t]$, что $f = gh$.

Свойство 1

Если $f \,\vdots\, g$ и $g \,\vdots\, h$, то $f \,\vdots\, h$.

Доказательство. Тогда $f = pg$ и $g = qh$, где $p, q \in K[t]$, откуда следует $f = (pq)h$. $\square$

Свойство 2

Пусть $f, g \vdots h$, *a* $p, q \in K[t]$. *Тогда* $fp + gq \vdots h$.

Доказательство. Тогда $f = ah$ и $g = bh$, где $a, b \in K[t]$, откуда следует $fp + gq = (ap + bq)h$. □

Свойство 3

Пусть $f, g \in K[t]$, $f \neq 0$, $f \vdots g$. *Тогда* $\deg(f) \geq \deg(g)$.

Доказательство. Тогда $f = gh$, где $h \in K[t]$, причем понятно, что $h \neq 0$. Следовательно,
$\deg(f) = \deg(g) + \deg(h) \geq \deg(g)$. □

Свойство 4

Пусть $f, g \in K[t]$, $f, g \neq 0$, $f \vdots g$ *и* $\deg(f) = \deg(g)$. *Тогда* $f \sim g$.

Доказательство. • Тогда $f = gh$, где $h \in K[t]$, и $\deg(g) = \deg(f) = \deg(g) + \deg(h)$.

• Следовательно, $\deg(h) = 0$, значит, $h \in K$, $h \neq 0$, то есть, $f \sim g$. □

Свойство 5

Пусть $f, g \in K[t]$, $f, g \neq 0$, $f \vdots g$ *и* $g \vdots f$. *Тогда* $f \sim g$.

Доказательство. Тогда $\deg(f) \geq \deg(g)$ и $\deg(g) \geq \deg(f)$. Следовательно, $\deg(f) = \deg(g)$. По Свойству 4, $f \sim g$. □

Идеалы в кольце многочленов над полем.

Теорема 3

Пусть K *— поле, а* I *— Идеал в* $K[t]$. *Тогда* $I = dK[t]$ *для некоторого* $d \in K[t]$.

Доказательство. • Если $I = \{0\}$, то подойдет $d = 0$.

• Пусть $I \neq \{0\}$. Тогда рассмотрим все ненулевые многочлены из I и найдем из них многочлен наименьшей степени d.

• Докажем, что все многочлены из I делятся на d (тогда $I = dK[t]$).

• Пусть $f \not\vdots d$, тогда поделим f на d с остатком: $f = qd + r$, $\deg(r) < \deg(d)$, $r \neq 0$.

• Так как $f, d \in I$, мы имеем $r = f - dq \in I$. Противоречие с минимальностью $\deg(d)$. □

НОД в кольце многочленов над полем.

Определение

Пусть K — поле, $f_1, \dots, f_n \in K[t]$. Тогда $\mathrm{OD}(f_1, \dots, f_n)$ — это множество всех многочленов, являющихся общими делителями $f_1, \dots, f_n$, а их НОД $(f_1, \dots, f_n))$ — это любой многочлен наибольшей степени из $\mathrm{OD}(f_1, \dots, f_n)$.

• Мы докажем, что многочлены наибольшей степени в $\mathrm{OD}(f_1, \dots, f_n)$ — это в точности множество попарно ассоциированных многочленов.

• В таком случае нам все равно, какой из них считать НОДом, для удобства будем считать НОДом любой из них. Запись $(f_1, \dots, f_n) = d$ в этом случае следует понимать так: НОД — любой из многочленов, ассоциированных с d.

Определение

Линейное представление НОД — это представление вида $(f_1, \dots, f_n) = p_1 f_1 + p_2 f_2 + \dots + p_n f_n$, где $p_1, \dots, p_n \in K[t]$.

• Если найти линейное представление любого НОД, то найдутся и линейные представления всех остальных (мы докажем, что все НОД попарно ассоциированы).

Теорема 4

Пусть K — поле, $f_1, \dots, f_n \in K[t]$.

1) *Существует линейное представление* $(f_1, \dots, f_n)$.

2) $\mathrm{OD}(f_1, \dots, f_n)$ *состоит из всех делителей* $(f_1, \dots, f_n)$.

3) *Все НОД* $f_1, \dots, f_n$ *попарно ассоциированы.*

Доказательство. 1) • Пусть $I = \langle f_1, \dots, f_n \rangle$ (напомним, что это идеал, состоящий из всех линейных комбинаций $f_1, \dots, f_n$).

• По Теореме 3, $I = dK[t]$ для некоторого многочлена $d \in K[t]$.

• Так как $f_1, \dots, f_n \in I$, все они делятся на d. Значит, $d \in \mathrm{OD}(f_1, \dots, f_n)$.

• Так как $d \in I$, существует представление $d = p_1 f_1 + \dots + p_n f_n$.

• Пусть $g \in \mathrm{OD}(f_1, \dots, f_n)$. Тогда $d \,\vdots\, g$, следовательно, $\deg(d) \geq \deg(g)$.

• Следовательно, d — многочлен наибольшей степени в $\mathrm{OD}(f_1, \dots, f_n)$, то есть, НОД этих многочленов.

2) Выше доказано, что d делится на все ненулевые многочлены из $\mathrm{OD}(f_1, \dots, f_n)$.

3) • Пусть $g \in \mathrm{OD}(f_1, \dots, f_n)$ и $\deg(g) = \deg(d)$. Тогда по Свойству 4 делимости многочленов $d \sim g$.

• Наоборот, если $g \sim d$, то, очевидно, $g \in I$. Множество кратных d совпадает с множеством кратных g, поэтому, $I = gK[t]$ и все доказанное выше для d верно и для g.

• Следовательно, НОДы $f_1, \dots, f_n$ — это в точности все многочлены, ассоциированные с d. $\square$

Свойство 1

Если $f, g, h \in K[t]$, то $(fh, gh) \sim (f, g)h$.

Доказательство. • Пусть $I = \langle f, g \rangle$ и $I_h = \langle fh, gh \rangle$. Первый идеал состоит из линейных комбинаций f и g, а второй — из линейных комбинаций fh и gh.

• Следовательно, $p \in I \iff p = qf + rg \iff ph = q(fh) + r(gh) \iff ph \in I_h$ (здесь $q, r \in K[t]$).

• Поэтому, если $I = dK[t]$, то $I_h = (dh)K[t]$. Остается заметить, что $(f, g) = d$ и $(fh, gh) = dh$. $\square$

Свойство 2

Если $f, g \in K[t]$ *и* $f \,\vdots\, g$, *то* $(f, g) \sim g$.

Доказательство. Пусть $I = \langle f, g \rangle$. Так как $f \,\vdots\, g$, то все линейные комбинации f и g — это в точности все кратные g многочлены. Значит, $I = gK[t]$. $\square$

Свойство 3

Если $f, g, h, p \in K[t]$ *и* $h = f + pg$, *то* $(f, g) \sim (h, g)$.

Доказательство. • Пусть $I_f = \langle f, g \rangle$ и $I_h = \langle h, g \rangle$.

• Так как $h = f + pg$, линейная комбинация h и g является линейной комбинацией f и g. Следовательно, $I_f \supset I_h$.

• Так как $f = h - pg$, аналогично получаем $I_h \supset I_f$. Значит, $I_f = I_h = dK[t]$. Теперь из Теоремы 4 ясно, что $(f, g) \sim d \sim (h, g)$. $\square$

• Теорема 4 не помогает найти линейное представление НОД двух многочленов. А помогает алгоритм Евклида, который, как и для целых чисел, состоит в последовательном делении с остатком.

• Последний остаток (на который разделится предыдущий) и будет НОДом по Свойствам 2 и 3.

• Точно так же как для целых чисел, двигаясь по алгоритму Евклида назад, мы получим линейное представление НОД.

• С помощью следующей леммы строится линейное представление НОД нескольких многочленов.

Лемма 4

Пусть $n \ge 2$, $f_1, \dots, f_n \in K[t]$. *Положим* $d_2 = (f_1, f_2)$, $d_3 = (d_2, f_3)$, $\dots$, $d_n = (d_{n-1}, f_n)$. *Тогда* $d_n = (f_1, \dots, f_n)$.

Доказательство. • Индукцией по k докажем, что $\mathrm{OD}(f_1, \dots, f_k)$ — все делители d_k.

• База $k = 2$ доказана в Теореме 4.

• Переход $k \to k+1$. $\mathrm{OD}(f_1, \dots, f_k, f_{k+1})$ — это все многочлены из $\mathrm{OD}(f_1, \dots, f_k)$, являющиеся делителями f_{k+1}.

• Так как $\mathrm{OD}(f_1, \dots, f_k)$ — это все делители d_k, получаем, что $\mathrm{OD}(f_1, \dots, f_k, f_{k+1}) = \mathrm{OD}(d_k, f_{k+1})$, а это все делители $d_{k+1} = (d_k, f_{k+1})$ по Теореме 4.

• Итак, утверждение доказано и $\mathrm{OD}(f_1, \dots, f_n)$ — это все делители d_n. Наибольшую степень из них имеет d_n, значит, $d_n = (f_1, \dots, f_n)$. $\square$

Взаимно простые многочлены

Определение

Пусть K — поле, $f_1, \dots, f_n \in K[t]$

1) Многочлены $f_1, \dots, f_n$ взаимно просты, если $(f_1, \dots, f_n) \sim 1$.

2) Многочлены $f_1, \dots, f_n$ попарно взаимно просты, если любые два из них взаимно просты.

Свойство 1

Если $f, g, h \in K[t]$ и $(f, g) \sim 1$, то $(fh, g) \sim (h, g)$.

Доказательство. • Пусть $p = (h, g)$ и $q = (fh, g)$.

• Из $h \vdots p$ следует, что $fh \vdots p$. Значит, $p \in \mathrm{OD}(fh, g)$ и по Теореме 4 $q \vdots p$.

• Из $g \vdots q$ следует, что $gh \vdots q$. Значит, $q \in \mathrm{OD}(fh, gh)$.

• По Свойству 1 НОД и Теореме 4, $h \sim h(f, g) \sim (fh, gh) \vdots q$.

• Следовательно, $q \in \mathrm{OD}(h, g)$ и по Теореме 4 мы имеем $p \vdots q$.

• Из $p \vdots q$ и $q \vdots p$ по Свойству 5 делимости $p \sim q$. $\square$

Свойство 2

Если $f, g, h \in K[t]$, $(f, g) \sim 1$ и $fh \,\vdots\, g$, то $h \,\vdots\, g$.

Доказательство. По Свойству 1 $(h, g) \sim (fh, g) \sim g$ (последнее верно, так как $fh \,\vdots\, g$). Следовательно, $h \,\vdots\, g$. □

Свойство 3

Пусть $f_1, \dots, f_n, g_1, \dots, g_m \in K[t]$, причем $(f_i, g_j) \sim 1$ для всех $i \in \{1, \dots, n\}$ и $j \in \{1, \dots, m\}$. Тогда $(f_1 \dots f_n,\ g_1 \dots g_m) \sim 1$.

Доказательство. • Докажем, что $(f_1 \dots f_k, g_j) \sim 1$ для всех $j \in \{1, \dots, m\}$ и $k \in \{1, \dots, n\}$ индукцией по k.

База $k = 1$: дано в условии.

Переход $k \to k+1$: $(f_1 \dots f_k f_{k+1}, g_j) \sim (f_1 \dots f_k, g_j) \sim 1$ по индукционному предположению (переход верен так как $(f_{k+1}, g_j) \sim 1$).

• Пусть $F = f_1 \dots f_n$. Докажем, что $(F, g_1 \dots g_k) \sim 1$ для всех $k \in \{1, \dots, m\}$ индукцией по k.

База $k = 1$: доказано выше.

Переход $k \to k+1$: $(F, g_1 \dots g_k g_{k+1}) \sim (F, g_1 \dots g_k) \sim 1$ по индукционному предположению (так как $(F, g_{k+1}) \sim 1$). □

Свойство 4

Пусть $f, p_1, \dots, p_n \in K[t]$, причем $p_1, \dots, p_n$ попарно взаимно просты, а $f \,\vdots\, p_i$ для всех $i \in \{1, \dots, n\}$. Тогда $f \,\vdots\, p_1 p_2 \dots p_n$.

Доказательство. • Пусть $q_\ell = p_1 \dots p_\ell$. Докажем по индукции, что $f \,\vdots\, q_\ell$.

• База $\ell = 1$ очевидна.

Переход $\ell \to \ell + 1$. • По индукционному предположению $f = hq_\ell$, где $h \in K[t]$.

• Так как $hq_\ell = f \,\vdots\, p_{\ell+1}$ и $(q_\ell, p_{\ell+1}) \sim 1$ (по Свойству 3), по Свойству 2 имеем $h \,\vdots\, p_{\ell+1}$.

• Тогда $h = gp_{\ell+1}$ и $f = gp_{\ell+1}q_\ell = gq_{\ell+1}$. □

Неприводимые многочлены

Определение

Пусть $f \in K[t]$, $\deg(f) > 0$.

• Многочлен f называется приводимым, если $f = gh$, где $g, h \in K[t]$, $0 < \deg(g) < \deg(f)$ и $0 < \deg(h) < \deg(f)$

• Если такого разложения не существует, то f называется неприводимым.

• Если $f \in K[t]$ — неприводимый и $f = gh$ (где $g, h \in K[t]$), то один из многочленов g и h — константа, а другой тогда ассоциирован с f.

• Если $f \in K[t]$ — неприводимый, $f \,\vdots\, g$ и $0 < \deg(g)$, то $g \sim f$.

Свойство 1

Пусть $f, g \in K[t]$, g — неприводимый. Тогда либо $f \vdots g$, либо $(f, g) \sim 1$.

Доказательство. • Пусть $d = (f, g)$. Тогда $g \vdots d$, то есть $g = dh$, $h \in K[t]$.

• Тогда либо $\deg(d) = 0$ (в этом случае $(f, g) = d \sim 1$), либо $\deg(h) = 0$.

• Если $\deg(h) = 0$, то $h \in K$ — константа и $g \sim d$.

• Так как $f \vdots d$ и $d \sim g$, то $f \vdots g$. $\square$

Свойство 2

Пусть $g, f_1, \dots, f_n \in K[t]$ таковы, что $f_1 \dots f_n \vdots g$ и g — неприводимый. Тогда существует такое $i \in \{1, \dots, n\}$, что $f_i \vdots g$.

Доказательство. • Предположим противное, пусть $f_i \not\vdots\, g$ для всех $i \in \{1, \dots, n\}$. По Свойству 1 тогда $(f_i, g) \sim 1$.

• По Свойству 3 взаимно простых многочленов, тогда и $(f_1 \dots f_n,\ g) \sim 1$.

• Но тогда $f_1 \dots f_n \not\vdots\, g$ (в этом случае должно быть $(f_1 \dots f_n,\ g) \sim g$). Противоречие. $\square$

Основная теорема арифметики в кольце многочленов над полем

Теорема 5

Пусть K — поле, $f \in K[t]$, $\deg(f) \ge 1$, а c — старший коэффициент f. Тогда существует разложение $f = c \cdot p_1 \dots p_n$, где $p_1, \dots, p_n$ — неприводимые, со старшим коэффициентом 1. Такое разложение единственно с точностью до порядка сомножителей.

Доказательство. $\exists$. Индукция по $\deg(f)$. База — случай неприводимого f. Тогда $p = c^{-1} \cdot f$ — также неприводимый, со старшим коэффициентом 1, и $f = c \cdot p$ — искомое разложение,

Переход. • Пусть для многочленов степени меньше $\deg(f)$ утверждение доказано и f — приводимый. Тогда $f = gh$, где $g, h \in K[t]$, $\deg(g) < \deg(f)$ и $\deg(h) < \deg(f)$.

• Пусть a и b — старшие коэффициенты g и h соответственно. Тогда по индукционному предположению $g = a \cdot q_1 \dots q_s$, а $h = b \cdot r_1 \dots r_\ell$, где $q_1, \dots, q_s, r_1, \dots, r_\ell \in K[t]$ — неприводимые со старшими коэффициентами 1.

• Тогда $f = c \cdot q_1 \dots q_s r_1 \dots r_\ell$ — искомое разложение для f (очевидно, $ab = c$).

! Докажем единственность индукцией по $\deg(f)$.

База: • Пусть f — неприводимый и имеет разложение $f = cp_1 \dots p_n$, где $p_1, \dots, p_n \in K[t]$ — неприводимые.

• Тогда $f = p_1 g$, где $g \in K[t]$ и $\deg(p_1) > 0$. Следовательно, $f \sim p_1$, но тогда $f = cp_1$, а такое разложение ровно одно.

Переход. • Пусть единственность с точностью до перестановки доказана для многочленов степени меньше чем $\deg(f)$.

• Предположим, $f = cp_1 \dots p_n = cq_1 \dots q_m$. Тогда $q_1 \dots q_m \,\vdots\, p_1$.

• По Свойству 2 неприводимых многочленов $\exists i \in \{1, \dots m\}$ такое, что $q_i \,\vdots\, p_1$. НУО $i = 1$.

• Так как $q_1 \,\vdots\, p_1$, q_1 неприводим и $\deg(p_1) \geq 1$, имеем $q_1 \sim p_1$. Но оба многочлена имеют старшие коэффициенты 1, следовательно, $q_1 = p_1$.

• $f = c \cdot p_1 g$, где $g \in K[t]$, $\deg(g) \geq 1$ (иначе f неприводим, а этот случай разобран).

• Для многочлена g разложение на неприводимые единственно с точностью до перестановки, значит, разложения $g = p_2 \dots p_n$ и $g = q_2 \dots q_m$ могут отличаться только порядком сомножителей.

• Значит, два рассматриваемых разложения f также отличаются только порядком сомножителей.

Определение

Каноническое разложение многочлена $f \in K[t]$ — это представление его в виде

$$f = c \cdot p_1^{k_1} \dots p_m^{k_m},$$

где c — старший коэффициент f, а $p_1, \dots, p_m$ — различные неприводимые многочлены со старшими коэффициентами 1.

• Из ОТА следует, что каноническое разложение существует. Нужно взять разложение на неприводимые многочлены из Теоремы 5 и сгруппировать одинаковые многочлены — получится каноническое разложение.

Значение многочлена в точке. Корень многочлена.

Определение

Пусть $f = a_n t^n + \dots + a_1 t + a_0 \in K[t]$.

1) Значение многочлена f в точке $\beta \in K$ — это число $f(\beta) = a_n \beta^n + \dots + a_1 \beta + a_0$.

2) Если $f(\beta) = 0$, то β — корень многочлена f.

Теорема 6

Пусть K — поле, $f \in K[t]$, $\alpha \in K$. Тогда остаток от деления $f(t)$ на $t - \alpha$ равен $f(\alpha)$.

Доказательство. • По теореме о делении с остатком, $f(t) = (t - \alpha)q(t) + r(t)$, где $\deg(r) < \deg(t - \alpha) = 1$. Следовательно, $r(t) = r \in K$ — константа.

• Итак, $f(t) = (t - \alpha)q(t) + r$, где $r \in K$. Подставим α и получим $f(\alpha) = 0q(t) + r = r$, что нам и нужно. □

Следствие 1

Пусть K — поле, $f \in K[t]$, $\alpha \in K$ — корень f. Тогда $f(t) \,\vdots\, t - \alpha$.

Доказательство. Следует из Теоремы 6, так как $f(\alpha) = 0$. □

Кратность корня

Определение

Пусть Пусть $f \in K[t]$, $\alpha \in K$. Число α является *корнем кратности m* многочлена f, если $f(t) \,\vdots\, (t-\alpha)^m$, но $f(t) \not\vdots\, (t-\alpha)^{m+1}$.

• По Следствию 1 любой корень многочлена $f \in K[t]$ имеет кратность хотя бы 1.

Теорема 7

Пусть K — поле, $f \in K[t]$, $\deg(f) = n$, $\alpha_1, \dots, \alpha_k \in K$ — все различные корни f, причем корень α_i имеет кратность m_i. Тогда:

1) $\quad f(t) \,\vdots\, \prod\limits_{i=1}^{k} (t-\alpha_i)^{m_i}$;

2) $\quad m_1 + \dots + m_k \le n$. *В частности,* $k \le n$.

Доказательство. 1) • Для любых $i \ne j$, очевидно, $((t-\alpha_i)^{m_i}, (t-\alpha_j)^{m_j}) \sim 1$.

• Для каждого $i \in \{1, \dots, k\}$ имеем $f \,\vdots\, (t-\alpha_i)^{m_i}$. Теперь пункт 1 следует из Свойства 4 взаимно простых многочленов.

2) Прямое следствие пункта 1.

Производная многочлена

• Здесь K — поле. Значит, существует $1 \in K$. Будем использовать в поле K обозначение $n := \underbrace{1 + \dots + 1}_{n}$.

• В этих обозначениях из дистрибутивности следует, что $m \cdot n = (\underbrace{1 + \dots + 1}_{m}) \cdot (\underbrace{1 + \dots + 1}_{n}) = \underbrace{1 + \dots + 1}_{mn} = mn$, так что введенное обозначение корректно.

Определение

Пусть $f(t) = a_n t^n + a_{n-1} t^{n-1} + \dots + a_1 t + a_0 \in K[t]$.
Производная многочлена f — это

$$f'(t) := n a_n t^{n-1} + (n-1) a_{n-1} t^{n-2} + \dots + a_1.$$

Лемма 5

Для $f, g \in K[t]$ выполнено $(f + g)' = f' + g'$.

Доказательство. • Пусть $f(t) = a_n t^n + \dots + a_0$, $g(t) = b_n t^n + \dots + b_0$. (Степени можно считать одинаковыми, иначе допишем нулевых коэффициентов.)

• Тогда $(f + g)(t) = (a_n + b_n) t^n + \dots + (a_1 + b_1) t + (a_0 + b_0)$ и $(f + g)'(t) = n(a_n + b_n) t^{n-1} + \dots + (a_1 + b_1) = (n a_n t^{n-1} + \dots + a_1) + (n b_n t^{n-1} + \dots + b_1) = f'(t) + g'(t)$. $\square$

Лемма 6

Для $f, g \in K[t]$ выполнено $(fg)' = fg' + f'g$.

Доказательство. • Сначала рассмотрим случай одночлена:

$$((a_k t^k)(b_\ell t^\ell))' = (a_k b_\ell t^{k+\ell})' = (k+\ell)a_k b_\ell t^{k+\ell-1} =$$

$$(a_k t^k)\cdot(\ell b_\ell t^{\ell-1}) + (k a_k t^{k-1})\cdot(b_\ell t^\ell) = (a_k t^k)\cdot(b_\ell t^\ell)' + (a_k t^k)'\cdot(b_\ell t^\ell).$$

• Теперь общий случай $f(t) = a_n t^n + \dots + a_0$, $g(t) = b_m t^m + \dots + b_0$:

$$(fg)' = \left(\left(\sum_{i=0}^{n} a_i t^i\right)\cdot\left(\sum_{j=0}^{m} b_j t^j\right)\right)' = \left(\sum_{i=0}^{n}\sum_{j=0}^{m} a_i b_j t^{i+j}\right)' =$$

$$\sum_{i=0}^{n}\sum_{j=0}^{m}(a_i b_j t^{i+j})' = \sum_{i=0}^{n}\sum_{j=0}^{m}(a_i t^i)'(b_j t^j) + \sum_{i=0}^{n}\sum_{j=0}^{m}(a_i t^i)(b_j t^j)' =$$

$$\left(\sum_{i=0}^{n}(a_i t^i)'\right)\cdot\left(\sum_{j=0}^{m} b_j t^j\right) + \left(\sum_{i=0}^{n} a_i t^i\right)\cdot\left(\sum_{j=0}^{m}(b_j t^j)'\right) =$$

$$\left(\sum_{i=0}^{n} a_i t^i\right)'\cdot\left(\sum_{j=0}^{m} b_j t^j\right) + \left(\sum_{i=0}^{n} a_i t^i\right)\cdot\left(\sum_{j=0}^{m} b_j t^j\right)' = f'g + fg'. \quad \square$$

Лемма 7

Для $f(t)=\prod\limits_{i=1}^{n}(t-\alpha_i)$, где $\alpha_1,\dots,\alpha_n\in K$ (не обязательно все эти числа различны). Тогда $f'(t)=\sum\limits_{i=1}^{n}\frac{f(t)}{t-\alpha_i}$.

Доказательство. Индукция по n. База $n=1$ очевидна (тогда $f'(t)=1$).

Переход. Пусть $g(t)=\frac{f(t)}{t-\alpha_n}=\prod\limits_{i=1}^{n-1}(t-\alpha_i)$. По Лемме 6 и индукционному предположению,

$$f'(t)=(g(t)(t-\alpha_n))'=g'(t)(t-\alpha_n)+g(t)(t-\alpha_n)'=$$
$$\Big(\sum_{i=1}^{n-1}\frac{g(t)}{t-\alpha_i}\Big)(t-\alpha_n)+g(t)=\sum_{i=1}^{n}\frac{f(t)}{t-\alpha_i}. \quad \square$$

Следствие 2

Пусть $\alpha\in K$, $f(t)=(t-\alpha)^n$. Тогда $f'(t)=n(t-\alpha)^{n-1}$.

Доказательство. Воспользуемся Леммой 7 для $\alpha_1=\dots=\alpha_n=\alpha$. $\square$

Кратность корня и производная многочлена

• Для $f \in K[t]$ и $s \in \mathbb{N}$ через $f^{(s)}(t)$ обозначим s-ю производную многочлена f.

Теорема 8

Пусть K — поле, $\mathrm{char}(K) = 0$, $f \in K[t]$, $\alpha \in K$ — корень f. Тогда α — корень кратности m многочлена f, если и только если $f(\alpha) = 0$, $f'(\alpha) = 0$, $\dots$, $f^{(m-1)}(\alpha) = 0$, а $f^{(m)}(\alpha) \neq 0$.

Доказательство. $\Rightarrow$ • Если α — корень кратности m многочлена f, то $f(t) = (t-\alpha)^m g(t)$, где $g(t) \in K[t]$, $g(t) \not\,\vdots\, (t-\alpha)$.

• Тогда по Лемме 7 и Следствию 2

$$f'(t) = ((t-\alpha)^m \cdot g(t))' = ((t-\alpha)^m)' g(t) + (t-\alpha)^m g'(t) = m(t-\alpha)^{m-1} g(t) + (t-\alpha)^m g'(t) = (t-\alpha)^{m-1}(mg(t) + (t-\alpha)g'(t)). \quad (1)$$

• Понятно, что $f'(t) \,\vdots\, (t-\alpha)^{m-1}$. Так как $g(t) \not\,\vdots\, (t-\alpha)$ и $m \neq 0$ ввиду $\mathrm{char}(K) = 0$, из (1) следует, что $f'(t) \not\,\vdots\, (t-\alpha)^m$.

• Таким образом, при взятии производной кратность корня α понизилась ровно на 1. Значит, все производные до $m-1$ включительно, будут делиться на $t-\alpha$, а $f^{(m)} \not\,\vdots\, (t-\alpha)$.

• Так как $h(t) \,\vdots\, (t-\alpha) \iff h(\alpha)=0$ по Следствию 1, мы имеем $f(\alpha)=0$, $f'(\alpha)=0$, $\dots f^{(m-1)}(\alpha)=0$ и $f^{(m)}(\alpha)\neq 0$.

$\Leftarrow$ • Пусть α — корень кратности ℓ, понятно, что $\ell\in\mathbb{N}$.

• Тогда по доказанной ранее части $f(\alpha)=0$, $f'(\alpha)=0$, $\dots$, $f^{(\ell-1)}(\alpha)=0$, а $f^{(\ell)}(\alpha)\neq 0$, откуда следует, что $m=\ell$. $\square$

Основная теорема алгебры

Теорема 9

Любой многочлен из $\mathbb{C}[t]$ *имеет корень из* $\mathbb{C}$.

Следствие 3

Неприводимые многочлены в $\mathbb{C}[t]$ *— это в точности многочлены степени 1.*

Доказательство. • Многочлены степени 1 всегда являются неприводимыми, это следует из определения.

• Пусть $f \in \mathbb{C}[t]$ неприводимый, $\deg(f) > 1$. По Теореме 9, f имеет корень α.

• Тогда $f(t) = (t - \alpha)g(t)$, откуда видно, что $0 < \deg(g) < \deg(f)$, противоречие с неприводимость f. □

Следствие 4

Пусть $f(t) \in \mathbb{C}[t]$, $n = \deg(f)$, c *— старший коэффициент* f*. Тогда* $f(t) = c(t - \alpha_1)\dots(t - \alpha_n)$, *где* $\alpha_1, \dots, \alpha_n \in \mathbb{C}$ *(не обязательно все эти числа различны).*

Доказательство. По Теореме 5, существует разложение $f = c \cdot p_1 \dots p_n$, где $p_1, \dots, p_n$ — неприводимые, со старшим коэффициентом 1. По Следствию 3, $p_i = t - \alpha_i$, где $\alpha_i \in \mathbb{C}$. □

Сопряженные корни

- Для многочлена $f(t) = a_n t^n + \dots + a_0$ введем обозначение $\overline{f}(t) := \overline{a_n} t^n + \dots + \overline{a_0}$.
- Так как $\overline{xy} = \overline{x} \cdot \overline{y}$ и $\overline{x+y} = \overline{x} + \overline{y}$, мы имеем $\overline{f}(\overline{t}) = \overline{f(t)}$.

Лемма 8

Пусть $f \in \mathbb{C}[t]$, $\alpha \in \mathbb{C}$ — корень f кратности m. Тогда $\overline{\alpha}$ — корень $\overline{f}$ кратности m.

Доказательство. • По условию, $f(t) = (t-\alpha)^m g(t)$.

- тогда $\overline{f}(\overline{t}) = (\overline{t} - \overline{\alpha})^m \cdot \overline{g}(\overline{t})$, значит, $\overline{\alpha}$ — корень $\overline{f}$ кратности не менее m.
- Если бы $\overline{\alpha}$ оказался корнем $\overline{f}$ кратности $k > m$, то аналогично доказывается, что $\alpha = \overline{\overline{\alpha}}$ — корень $f = \overline{\overline{f}}$ кратности не менее k, что не так.
- Значит, $\overline{\alpha}$ — корень $\overline{f}$ кратности ровно m. $\square$

Теорема 10

Многочлен $f \in \mathbb{R}[t]$ степени $\deg(f) = n \geq 1$ со старшим коэффициентом c раскладывается в $\mathbb{C}[t]$ на множители

$$f(t) = c(t-\alpha_1)^{k_1} \dots (t-\alpha_s)^{k_s}(t-\beta_1)^{m_1}(t-\overline{\beta_1})^{m_1} \dots (t-\beta_\ell)^{m_\ell}(t-\overline{\beta_\ell})^{m_\ell},$$

где $\alpha_1, \dots, \alpha_s \in \mathbb{R}$, $\beta_1, \dots, \beta_\ell \in \mathbb{C} \setminus \mathbb{R}$ — различные числа, никакие два из $\beta_1, \dots, \beta_\ell$ не сопряжены друг другу и $n = \sum_{i=1}^{s} k_i + 2\sum_{j=1}^{\ell} m_j$ (возможно, одно из чисел k и ℓ равно 0).

Доказательство. • По Следствию 4, существует разложение $f(t) = c\prod_{i=1}^{p}(t-\alpha_i)^{k_i}$, где $\sum_{i=1}^{p} k_i = n$ (возьмем разложение на неприводимые многочлены из Следствия 4 и переделаем его в каноническое разложение, сгруппировав одинаковые).

• НУО можно считать, что $\alpha_1, \dots, \alpha_s \in \mathbb{R}$ (возможно, $s = 0$) а остальные корни не вещественны.

• По Лемме 8, если $\beta \in \mathbb{C} \setminus \mathbb{R}$ — корень f кратности m, то и $\overline{\beta}$ — корень $\overline{f} = f$ кратности m.

• Следовательно $p - s \,\vdots\, 2$. Если $p \neq s$, то $p - s = 2\ell$ и корни $\alpha_{s+1}, \dots, \alpha_p$ можно переобозначить $\beta_1, \overline{\beta_1}, \dots \beta_\ell, \overline{\beta_\ell}$ так, что кратности корней β_i и $\overline{\beta_i}$ одинаковы и равны m_i.

Теорема 11

Неприводимые многочлены в $\mathbb{R}[t]$ — это многочлены степени 1 и многочлены степени 2 с отрицательным дискриминантом.

Доказательство. • Пусть $f \in \mathbb{R}[t]$ — неприводимый и $\deg(f) = n > 1$.

• Если f имеет корень $\alpha \in \mathbb{R}$, то $f(t) = (t-\alpha)g(t)$, где $g \in \mathbb{R}[t]$, $0 < \deg(g) < n$, противоречие с неприводимостью f.

• Значит, f не имеет вещественных корней. По Теореме 9 тогда f имеет корень $\beta \in \mathbb{C} \setminus \mathbb{R}$, но тогда по Теореме 10 и $\overline{\beta}$ — корень f, причем $f(t) \vdots (t-\beta)(t-\overline{\beta}) = t^2 - 2\mathrm{Re}(\beta)t + N(\beta)$.

• При $n \geq 3$ имеем $f(t) = (t^2 - 2\mathrm{Re}(\beta)t + N(\beta))g(t)$, где $0 < \deg(g) < n$, противоречие с неприводимостью f.

• Если $n = 2$, то $f(t) = c(t^2 - 2\mathrm{Re}(\beta)t + N(\beta))$, где c — старший коэффициент f и его дискриминант $D(f) = 4c^2((\mathrm{Re}(\beta))^2 - N(\beta)) = -4c^2(\mathrm{Im}(\beta))^2 < 0$. $\square$

Следствие 5

Многочлен $f \in \mathbb{R}[t]$ нечетной степени обязательно имеет $\mathbb{R}$ корень.

Доказательство. • По Теореме 10, сумма кратностей всех комплексных корней f равна $\deg(f) \not\vdots\, 2$, а сумма кратностей невещественных корней четна.

• Значит, сумма кратностей вещественных корней f нечетна, то есть, такой корень есть. □

Следствие 6

Многочлен $f \in \mathbb{R}[t]$ степени $\deg(f) = n \geq 1$ со старшим коэффициентом c раскладывается в $\mathbb{R}[t]$ на множители

$$f(t) = c(t-\alpha_1)^{k_1} \dots (t-\alpha_s)^{k_s}(t^2+p_1t+q_1)^{m_1} \dots (t^2+p_\ell t+q_\ell)^{m_\ell},$$

где $D(t^2 + p_i t + q_i) = p_i^2 - 4q_i < 0$ для всех $i \in \{1, \dots, \ell\}$ (возможно, одно из чисел s и ℓ равно 0).

Доказательство. • По ОТА (Теореме 5) в $\mathbb{R}[t]$ существует разложение $\frac{1}{c}f$ в произведение неприводимых многочленов со старшим коэффициентом 1, которые имеют такой вид по Теореме 11. □

Теорема Виета

• Пусть K — коммутативное кольцо, $a_1, \dots, a_n \in K$ (не обязательно все числа различны). Введем обозначения:

$\sigma_1(a_1, \dots, a_n) = a_1 + a_2 + \dots + a_n$;

$\sigma_2(a_1, \dots, a_n) = \sum\limits_{1 \le i < j \le n} a_i a_j$ (сумма всех произведений по два числа); при $k \le n$

$\sigma_k(a_1, \dots, a_n) = \sum\limits_{1 \le i_1 < i_2 < \dots < i_k \le n} a_{i_1} a_{i_2} \dots a_{i_k}$ (сумма всех произведений по k чисел); $\sigma_n(a_1, \dots, a_n) = a_1 a_2 \dots a_n$.

Теорема 12

Пусть $f = c_n t^n + \dots + c_1 t + c_0 \in K[t]$, *причем* $f = c_n(t - a_1) \dots (t - a_n)$. *Тогда* $\frac{c_i}{c_n} = (-1)^{n-i} \sigma_{n-i}(a_1, \dots, a_n)$ *для каждого* $i \in \{0, \dots, n-1\}$.

Доказательство. • $\frac{c_i}{c_n}$ — это коэффициент многочлена $(t - a_1) \dots (t - a_n)$ при t^i.

• Из i скобок мы должны выбрать t, а из остальных $n - i$ скобок вида $(t - a_j)$ должны выбрать $-a_j$. Перемножим все выбранные числа, сложим по всем выборкам и вынесем $(-1)^{n-i}$ — получим в точности $\sigma_{n-i}(a_1, \dots, a_n)$.

Интерполяция

- Пусть K — поле, даны различные числа $x_0, x_1, \dots, x_n \in K$ и (не обязательно различные) $y_0, y_1, \dots, y_n \in K$.
- Нужно построить *интерполяционный многочлен* $f \in K[t]$: такой, что $\deg(f) \le n$ и $f(x_i) = y_i$ для всех $i \in \{0, 1, \dots, n\}$.

Лемма 9

Существует не более одного интерполяционного многочлена для заданных $x_0, x_1, \dots, x_n \in K$ (различных) и $y_0, y_1, \dots, y_n \in K$.

Доказательство. • Пусть f_1 и f_2 — два разных интерполяционных многочлена. Тогда $f_1 - f_2 \in K[t]$, $\deg(f_1 - f_2) \le \max(\deg(f_1), \deg(f_2)) \le n$.

- Однако, многочлен $f_1 - f_2$ имеет $n+1$ различных корней $x_0, \dots, x_n$ (так как $f_1(x_i) = f_2(x_i)$), противоречие с Теоремой 7. $\square$

Интерполяционный многочлен Лагранжа

- Построим такой многочлен f_i степени не более n, что $f_i(x_i) = 1$ и $f_i(x_j) = 0$ при $j \in \{1, \dots, n\}$, $j \neq i$.
- Пусть $\varphi(t) = (t - x_0)(t - x_1) \dots (t - x_n)$, а $\varphi_i(t) = \frac{\varphi(t)}{(t - x_i)}$ — это тоже многочлен из $K[t]$.
- Так как $f_i(x_j) = 0$ при $j \in \{1, \dots, n\}$, $j \neq i$, по Теореме 7 $f_i(t) \vdots \varphi_i(t)$. Так как $\deg(f_i) = \deg(\varphi_i)$, мы имеем $f_i = c_i\varphi_i(t)$, где $c_i \in K$.
- Подставим x_i, чтобы найти c_i: $\quad 1 = f_i(x_i) = c_i\varphi_i(x_i)$, откуда $c_i = \frac{1}{\varphi_i(x_i)}$.
- По Лемме 7, $\varphi'(t) = \sum\limits_{i=0}^{n} \varphi_i(t)$. При $j \neq i$ мы имеем $\varphi_j(x_i) = 0$. Следовательно, $\varphi'(x_i) = \varphi_i(x_i)$.
- Таким образом, $f_i(t) = \frac{\varphi_i(t)}{\varphi_i(x_i)} = \frac{\varphi(t)}{\varphi'(x_i) \cdot (t - x_i)}$.
- Следовательно,

$$f(t) = \sum_{i=0}^{n} y_i f_i(t) = \sum_{i=0}^{n} y_i \cdot \frac{\varphi(t)}{\varphi'(x_i) \cdot (t - x_i)}.$$

Интерполяция по Ньютону

• Будем по индукции строить такой многочлен $g_k(t)$, что $g_k(x_i) = y_i$ при $i \in \{0, \dots, k\}$ и $\deg(g_k) \le k$.

• База $k = 0$: подойдет $g_0(t) = y_0$.

• Переход $k \to k+1$. Пусть построен многочлен g_k. Будем искать g_{k+1} в виде

$g_{k+1}(t) = a_k(t - x_0) \dots (t - x_k) + g_k(t)$.

• Тогда $g_{k+1}(x_i) = y_i$ при $i \in \{0, \dots, k\}$ и $\deg(g_{k+1}) \le \max(k+1, \deg(g_k)) = k+1$.

• Остается найти коэффициент a_k. Для этого подставим x_{k+1}:

$$y_{k+1} = g_{k+1}(x_{k+1}) = a_k(x_{k+1} - x_0) \dots (x_{k+1} - x_k) + g_k(x_{k+1})$$

$$\iff a_k = \frac{y_{k+1} - g_k(x_{k+1})}{(x_{k+1} - x_0) \dots (x_{k+1} - x_k)}.$$

Поле рациональных функций

• Пусть K — поле. Очевидно, в кольце многочленов $K[t]$ нет делителей ноля (если $fg = 0$ в $K[t]$, то $f = 0$ или $g = 0$). Поэтому, следующее определение корректно.

Определение

Поле рациональных функций $K(t)$ — это поле частных кольца многочленов $K[t]$.

• Элементы $K(t)$ — дробно-рациональные функции вида $\frac{f(t)}{g(t)}$, где $f, g \in K[t]$, $g \neq 0$ (точнее говоря, классы эквивалентности таких функций). Мы будем называть такие функции просто дробями.

Определение

Правильная дробь в $K(t)$ — это дробь вида $\frac{f(t)}{g(t)}$, где $\deg(f) < \deg(g)$.

Свойство 1

Если дробь $\frac{f}{g} \in K(t)$ правильная и $\frac{f_1}{g_1} \sim \frac{f}{g}$, то дробь $\frac{f_1}{g_1}$ Тоже правильная.

Доказательство. • Если один из многочленов f и f_1 равен 0, то другой тоже. В этом случае утверждение очевидно.

• Далее пусть $f \neq 0$ и $f_1 \neq 0$.

• $\frac{f_1}{g_1} \sim \frac{f}{g} \iff f_1 g = g_1 f$, откуда следует, что $\deg(f_1) + \deg(g) = \deg(f_1 g) = \deg(f g_1) = \deg(f) + \deg(g_1)$.

• Так как $0 \leq \deg(f) < \deg(g)$, отсюда следует, что $\deg(f_1) < \deg(g_1)$, то есть, $\frac{f_1}{g_1}$ — правильная дробь. □

Свойство 2

Если дробь $\frac{f}{g} \in K(t)$ правильная и $c \in K$, то и $\frac{cf}{g}$ — правильная дробь.

Доказательство. Очевидно ввиду $\deg(cf) \leq \deg(f)$. □

Свойство 3

Если дроби $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in K(t)$ правильные, то и $\frac{f_1}{g_1} \cdot \frac{f_2}{g_2}$ — правильная дробь.

Доказательство. Тогда $\deg(f_1) < \deg(g_1)$ и $\deg(f_2) < \deg(g_2)$, откуда
$\deg(f_1 f_2) = \deg(f_1) + \deg(f_2) < \deg(g_1) + \deg(g_2) = \deg(g_1 g_2)$, а значит, дробь $\frac{f_1}{g_1} \cdot \frac{f_2}{g_2} = \frac{f_1 f_2}{g_1 g_2}$ — правильная. □

Свойство 4

Если дроби $\frac{f_1}{g_1}, \frac{f_2}{g_2} \in K(t)$ правильные, то и $\frac{f_1}{g_1} + \frac{f_2}{g_2}$ — правильная дробь.

Доказательство. $\frac{f_1}{g_1} + \frac{f_2}{g_2} = \frac{f_1 g_2 + g_1 f_2}{g_1 g_2}$. Нужно проверить, что $\deg(f_1 g_2 + g_1 f_2) < \deg(g_1 g_2)$:

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

так как $\deg(f_1) < \deg(g_1)$ и $\deg(f_2) < \deg(g_2)$. □

Лемма 10

Пусть $g_1, g_2 \in K[t]$ взаимно просты, а $\frac{f}{g_1g_2} \in K(t)$ — правильная дробь. Тогда $\exists f_1, f_2 \in K[t]$ такие, что $\frac{f}{g_1g_2} = \frac{f_1}{g_1} + \frac{f_2}{g_2}$ и обе дроби $\frac{f_1}{g_1}$ и $\frac{f_2}{g_2}$ правильные.

Доказательство. • Так как $(g_1, g_2) \sim 1$, существуют такие $p_1, p_2 \in K[t]$, что $p_1g_1 + p_2g_2 = 1$ (линейное представление НОД).

• Тогда $\frac{f}{g_1g_2} = \frac{f(p_1g_1+p_2g_2)}{g_1g_2} = \frac{fp_1g_1}{g_1g_2} + \frac{fp_2g_2}{g_1g_2} = \frac{fp_1}{g_2} + \frac{fp_2}{g_1}$.

• Недостаток полученного представления в том, что дроби могут оказаться неправильными. Поделим fp_1 на g_2 с остатком: $fp_1 = qg_2 + r$, где $\deg(r) < \deg(g_2)$.

• Тогда $\frac{fp_1}{g_2} = \frac{qg_2+r}{g_2} = q + \frac{r}{g_2}$.

• Следовательно, $\frac{f}{g_1g_2} = \frac{r}{g_2} + q + \frac{fp_2}{g_1} = \frac{r}{g_2} + \frac{qg_1+fp_2}{g_1}$.

• Так как дроби $\frac{f}{g_1g_2}$ и $\frac{r}{g_2}$ правильные, по Свойству 4 дробь $\frac{qg_1+fp_2}{g_1} = \frac{f}{g_1g_2} - \frac{r}{g_2}$ также правильная. □

Лемма 11

Пусть $\frac{f}{g} \in K[t]$ *— правильная дробь, а* $g = q_1^{k_1} \dots q_m^{k_m}$ *— каноническое разложение. Тогда существует разложение* $\frac{f}{g} = \frac{f_1}{q_1^{k_1}} + \dots + \frac{f_m}{q_m^{k_m}}$, *где дробь* $\frac{f_i}{q_i^{k_i}}$ *правильная для всех* $i \in \{1, \dots, m\}$.

Доказательство. • Докажем индукцией по ℓ, что существует разложение на правильные дроби $\frac{f}{q_1^{k_1} \dots q_\ell^{k_\ell}} = \frac{f_1}{q_1^{k_1}} + \dots + \frac{f_\ell}{q_\ell^{k_\ell}}$.

• База для $\ell = 1$ очевидна.

Переход $\ell \to \ell + 1$. Отметим, что многочлен $h = q_1^{k_1} \dots q_\ell^{k_\ell}$ взаимно прост с $q_{\ell+1}^{k_{\ell+1}}$.

• По Лемме 10 и индукционному предположению для $\frac{f^*}{h}$ существует разложение в сумму правильных дробей

$$\frac{f}{(q_1^{k_1} \dots q_\ell^{k_\ell}) q_{\ell+1}^{k_{\ell+1}}} = \frac{f}{h \cdot q_{\ell+1}^{k_{\ell+1}}} = \frac{f^*}{h} + \frac{f_{\ell+1}}{q_{\ell+1}^{k_{\ell+1}}}$$
$$= \frac{f_1}{q_1^{k_1}} + \dots + \frac{f_\ell}{q_\ell^{k_\ell}} + \frac{f_{\ell+1}}{q_{\ell+1}^{k_{\ell+1}}}. \qquad \square$$

Простейшие дроби

Определение

Дробь $\frac{f}{g} \in K(t)$ — простейшая, если $g = p^k$, где $p \in K[t]$ — неприводимый многочлен и $\deg(f) < \deg(p)$.

Теорема 13

Любая правильная дробь $\frac{f}{g} \in K(t)$ раскладывается в сумму простейших.

Доказательство. • Можно считать, что старший коэффициент g равен 1 (иначе сократим на него f).

• Пусть $g = q_1^{k_1} \dots q_m^{k_m}$ — каноническое разложение. Тогда по Лемме 11 существует разложение в сумму правильных дробей $\frac{f}{g} = \frac{f_1}{q_1^{k_1}} + \dots + \frac{f_m}{q_m^{k_m}}$.

• Теперь достаточно научиться раскладывать в сумму простейших правильную дробь вида $\frac{h}{p^k}$, где p — неприводимый многочлен.

• Докажем существование такого разложения индукцией по k. База $k = 1$ очевидна (тогда $\deg(h) < \deg(p)$ и дробь уже простейшая).

Переход $k \to k + 1$.

• Если $\deg(h) < \deg(p)$, то дробь $\frac{h}{p^{k+1}}$ простейшая.

• Если $\deg(h) \ge \deg(p)$, то поделим h на p с остатком: $h = qp + r$, где $\deg(r) < \deg(p)$.

• Тогда $\frac{h}{p^{k+1}} = \frac{qp+r}{p^{k+1}} = \frac{q}{p^k} + \frac{r}{p^{k+1}}$, где дробь $\frac{r}{p^{k+1}}$ простейшая.

• Так как $\frac{q}{p^k} = \frac{h}{p^{k+1}} - \frac{r}{p^{k+1}}$, а две последние дроби правильные, то $\frac{q}{p^k}$ — правильная дробь.

• Заменим $\frac{q}{p^k}$ на разложение у сумму простейших, которое существует по индукционному предположению, и получим искомое разложение. $\square$

Связь разложения на простейшие дроби с интерполяцией

• Пусть K — поле. Покажем простой способ разложения на простейшие правильной дроби $\frac{f(x)}{g(x)} \in K(x)$, где $g(x) = (x - a_1)\dots(x - a_n)$, и $a_1, \dots, a_n$ различны.

• Рассмотрим интерполяционную задачу с точками a_1, $\dots$, a_n и значениями $f(a_1)$, $\dots$, $f(a_n)$ в них соответственно.

• Так как $\deg(f) < n$, многочлен f и есть единственный интерполяционный многочлен для рассматриваемой задачи. Запишем формулу Лагранжа:

$$f(x) = \sum_{i=1}^{n} \frac{f(a_i)}{g'(a_i)} \frac{g(x)}{x - a_i} \quad \Rightarrow \quad \frac{f(x)}{g(x)} = \sum_{i=1}^{n} \frac{f(a_i)}{g'(a_i)} \frac{1}{x - a_i}.$$

• Мы получили разложение $\frac{f(x)}{g(x)}$ на простейшие.

• А как понять, что многочлен не имеет кратных корней?

Лемма 12

1) *Если K — поле и многочлен $g \in K[t]$ таков $(g, g') \sim 1$, то g не имеет кратных корней (то есть, корней кратности более 1).*

2) *Если многочлен $g \in \mathbb{C}[t]$ не имеет кратных корней, то $(g, g') \sim 1$.*

Доказательство. 1) Если g имеет корень α кратности не менее 2, то α — корень g' по Теореме 8. Тогда $(g, g') \,\vdots\, (t - \alpha)$, противоречие.

2) • Так как g не имеет кратных корней, по Теореме 8 ни один из корней g не является корнем g'.

• Если при этом $(g, g') \sim h$, $\deg(h) \geq 1$, то h по основной теореме алгебры, имеет корень, который является общим корнем g и g', противоречие. $\square$

Еще один вид поля $\mathbb{C}$

Теорема 14

$$\mathbb{C} \simeq \mathbb{R}[t]/(t^2+1)\mathbb{R}[t].$$

Доказательство. • Определим отображение $\varphi : \mathbb{R}[t] \to \mathbb{C}$ формулой $\varphi(f) := f(i)$.

• Докажем, что φ — гомоморфизм. Пусть $f, g \in K[t]$.

• $\varphi(f+g) = (f+g)(i) = f(i) + g(i) = \varphi(f) + \varphi(g)$;

• $\varphi(fg) = (fg)(i) = f(i) \cdot g(i) = \varphi(f) \cdot \varphi(g)$.

• Докажем, что φ — сюръекция. Пусть $z = a + bi \in \mathbb{C}$, где $a, b \in \mathbb{R}$. Тогда $bt + a \in \mathbb{R}[t]$ и $\varphi(bt+a) = a + bi$.

• Пусть $f \in \mathrm{Ker}(\varphi)$, разделим f с остатком на t^2+1: $f(t) = (t^2+1)g(t) + bt + a$ (степень остатка по определению не превосходит 1, значит, он представляется в виде $bt+a$).

• Тогда $0 = \varphi(f) = f(i) = (i^2+1)g(i) + bi + a = bi + a \iff a = b = 0 \iff f \vdots t^2+1$.

• Таким образом, $\mathrm{Im}(\varphi) = \mathbb{C}$, $\mathrm{Ker}(\varphi) = (t^2+1)\mathbb{R}[t]$ и по теореме о гомоморфизме колец имеем $\mathbb{C} = \mathrm{Im}(\varphi) \simeq \mathbb{R}[t]/\mathrm{Ker}(\varphi) = \mathbb{R}[t]/(t^2+1)\mathbb{R}[t]$. $\square$

Многочлен деления круга

- Напомним определение.

Определение

Пусть $n \in \mathbb{N}$. Число $\varepsilon \in \mathbb{C}$ такое, что $\varepsilon^n = 1$, но $\varepsilon^k \neq 1$ при натуральных $k < n$ называется *первообразным корнем из* 1 степени n.

- По Теореме 2.25 существует ровно $\varphi(n)$ первообразных корней из 1 степени n, и они имеют вид $\varepsilon_k = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$, где $k \in \{1, \dots, n-1\}$, $(k, n) = 1$.

Определение

Многочлен деления круга $\Phi_n(t) := \prod\limits_{1 \le k \le n,\ (k,n)=1} (t - \varepsilon_k)$.

- Из определения следует, что $\Phi_n \in \mathbb{C}[t]$. Мы докажем, что все коэффициенты этого многочлена целые.

Лемма 13

$t^n - 1 = \prod_{d \mid n} \Phi_d(t)$.

Доказательство. • Если $d \mid n$, то первообразный корень из 1 степени d, очевидно, является корнем из 1 степени n.

• Следовательно, $t^n - 1 \vdots \Phi_d(t)$.

• Так как каждый корень из 1 является первообразным корнем ровно одной степени, $t^n - 1 \vdots \prod_{d \mid n} \Phi_d(t)$.

• Пусть $\varepsilon_0, \dots, \varepsilon_{n-1}$ — все корни степени n из 1, $\varepsilon_k = (\cos(\frac{2\pi k}{n}), \sin(\frac{2\pi k}{n}))$.

• Пусть $(k, n) = d$, $k = k'd$, $n = n'd$. Тогда $\varepsilon_k = (\cos(\frac{2\pi k'}{n'}), \sin(\frac{2\pi k'}{n'}))$.

• Так как дробь $(k', n') = 1$, по Теореме 2.25 ε_k — первообразный корень степени n' из 1, причем $n' \mid n$.'

• Следовательно, все корни из 1 степени n являются первообразными корнями степеней-делителей n.

• Следовательно, $t^n - 1 \mid \prod_{d \mid n} \Phi_d(t)$. □

Теорема 15

1) $$\Phi_n(t) = \prod_{d \mid n} (t^d - 1)^{\mu(\frac{n}{d})}. \qquad (*)$$

2) $\Phi_n \in \mathbb{Z}[t]$ *— унитарный многочлен (то есть, старший коэффициент* Φ_n *равен 1).*

Доказательство. 1) • По Лемме 13 имеем $t^n - 1 = \prod\limits_{d \mid n} \Phi_d(t)$.

• Теперь $(*)$ непосредственно следует из мультипликативной формулы обращения Мёбиуса (Теоремы 2.22).

2) • Формулу $(*)$ можно переписать в виде $\Phi_n(t) = \frac{f(t)}{g(t)}$, где $f, g \in \mathbb{Z}[t]$ — унитарные многочлены (каждый из f и g представляется в виде произведения нескольких многочленов вида $x^d - 1$).

• При делении в столбик унитарного многочлена f с целыми коэффициентами на унитарный многочлен g с целыми коэффициентами нетрудно убедиться, что неполное частное будет унитарным многочленом с целыми коэффициентами.

• При этом, f разделится на g без остатка и частное получится равным $\Phi_n(t)$. □