

## Полиномы Чебышёва и их обращения

А. Г. Хованский

Полином Чебышёва степени  $n$  определяется следующей формулой:

$$T_n(x) = \cos n \arccos x.$$

Эти полиномы были открыты Чебышёвым в связи с задачей о наилучшем приближении заданной функции полиномами степени  $\leq n$ . Они играют большую роль в теории приближений. Удивительно, что эти полиномы оказались полезными и в алгебре: ведь задача, в связи с которой они возникли, от алгебры далека, а их исходное определение использует трансцендентные функции.

Тем не менее в ряде задач алгебры наряду с серией степенных полиномов  $x^n$  встречается серия полиномов  $T_n$ . С «философской» точки зрения появление этих двух серий полиномов связано с существованием двух серий конечных групп проективных преобразований пространства  $\mathbb{C}P^1$ : циклических групп  $C_n$  и групп диэдра  $D_n$ .

В комплексном анализе серия полиномов  $x^n$  расширяется до семейства многозначных аналитических функций  $x^\alpha$ ,  $\alpha \in \mathbb{R}$ , содержащего, наряду с полиномами  $x^n$ , их обращения  $x^{1/n}$  и удовлетворяющего прежним композиционным соотношениям  $(x^\alpha)^\beta = x^{\alpha\beta}$ .

Аналогично мы расширяем серию полиномов Чебышёва  $T_n$  до семейства многозначных аналитических функций  $T_\alpha$ ,  $\alpha \in \mathbb{R}$ , содержащего, наряду с полиномами  $T_n$ , их обращения  $T_{1/n}$  и удовлетворяющего прежним композиционным соотношениям  $T_\beta \circ T_\alpha = T_{\alpha\beta}$ .

Многозначную функцию можно определить без использования аналитического продолжения, описав множество ее значений в каждой точке. Это иногда дает возможность перенести определение функции на любое поле (над которым операция аналитического продолжения не определена). Например, при натуральном  $n$  функция  $x^{1/n}$  определена над любым полем  $\mathbb{k}$ : это многозначная функция, которая сопоставляет  $x \in \mathbb{k}$  множество элементов  $z$ , лежащих в замыкании поля  $\mathbb{k}$  и таких, что  $z^n = x$ .

Легче иметь дело с ростком однозначной функций, чем с многозначной функцией. Во многих вопросах этим можно ограничиться, если все значения многозначной функции получаются при аналитическом продолжении однозначного ростка.

В п. 1.1 определяется многозначная функция Чебышёва  $T_\alpha$ ,  $\alpha \in \mathbb{R}$ , комплексного переменного  $x$  при помощи описания множества ее значений. В п. 1.2 определяется ряд в точке  $x = 1$ , аналитическим продолжением которого она является (см. п. 1.3).

В п. 2.1 мы приводим алгебраическое определение полиномов Чебышёва и их обращений над любым полем, характеристика которого  $\neq 2$ . Если, дополнительно, характеристика поля  $\neq 3$ , то эти функции применимы для решения в радикалах уравнений степени три и степени четыре над этим полем (см. пп. 2.2–2.3).

В пп. 3.1–3.3 мы обсуждаем три классические задачи, в решении которых встретились серии полиномов  $x^n$  и  $T_n$ . В п. 3.1 обсуждается решенная Риттом задача об описании всех комплексных полиномов, обращения которых представимы в радикалах. В п. 3.2 обсуждается решенная Фридом проблема Шура об описании всех полиномов  $P \in \mathbb{Q}[x]$ , для которых отображения  $P: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  обратимы для бесконечного множества простых чисел  $p$ . В п. 3.3 мы формулируем результат Жулия, Фату и Ритта об аффинной классификации *интегрируемых* (см. определение из этого пункта) полиномиальных отображений комплексной прямой в себя.

## §1. ФУНКЦИИ ЧЕБЫШЁВА НАД КОМПЛЕКСНЫМИ ЧИСЛАМИ

### 1.1. МНОГОЗНАЧНЫЕ ФУНКЦИИ ЧЕБЫШЁВА

*Функцией Чебышёва степени  $\alpha \in \mathbb{R}$*  назовем многозначную функцию  $T_\alpha$  комплексного переменного  $x$ , определенную соотношением:

$$T_\alpha(x) = \frac{u^\alpha(x) + u^{-\alpha}(x)}{2}, \quad (1)$$

где  $u$  — двузначная функция, определенная соотношением

$$x = \frac{u(x) + u^{-1}(x)}{2}. \quad (2)$$

В формуле (1) имеется в виду, что каждое значение  $f(x)$  многозначной функции  $u^\alpha(x)$  складывается со значением  $f^{-1}(x)$  функции  $u^{-\alpha}(x)$  (а не с каким-либо другим ее значением). Согласно (2) функция  $u(x)$  удовлетворяет уравнению  $u^2(x) - 2xu(x) + 1 = 0$ . Его корни  $u_1(x)$ ,  $u_2(x)$  связаны соотношением  $u_1(x)u_2(x) = 1$ , поэтому не важно, какой из двух корней использовать в формуле (1). (Отметим, что эти корни вычисляются явно:  $u_{1,2}(x) = x \pm \sqrt{x^2 - 1}$ .) Выбор другого корня лишь переставляет слагаемые  $u^\alpha(x)$  и  $u^{-\alpha}(x)$  и не меняет их суммы.

**ТЕОРЕМА 1.** *Функцию  $T_\alpha$  можно определить соотношениями:*

$$x = \cos z(x), \quad T_\alpha(x) = \cos \alpha z(x).$$

ДОКАЗАТЕЛЬСТВО. Если  $x = \cos z_0$ , то  $z(x) = \pm(z_0 + 2k\pi)$  и

$$\cos(\alpha z(x)) = \frac{\exp(i\alpha z(x)) + \exp(-i\alpha z(x))}{2}.$$

При этом  $u_{1,2}(x) = \exp(\pm iz(x))$  и  $u_{1,2}^{\pm\alpha}(x) = \exp i\alpha(\pm z(x))$ . Откуда и вытекает теорема.

УТВЕРЖДЕНИЕ 2. *Функция  $T_n$  для натурального  $n$  является полиномом степени  $n$  с целыми коэффициентами. Справедлива формула*

$$T_n(x) = \sum_{0 \leq k \leq [n/2]} \binom{n}{2k} x^{n-2k} (x^2 - 1)^k.$$

ДОКАЗАТЕЛЬСТВО. Соотношение  $T_n(x) = (u^n(x) + u^{-n}(x))/2$  с учетом равенств  $u^n(x) = (x + \sqrt{x^2 - 1})^n$  и  $u^{-n}(x) = (x - \sqrt{x^2 - 1})^n$  и бинома Ньютона превращается в формулу для  $T_n(x)$ .

ОПРЕДЕЛЕНИЕ. Функция  $T_n$  называется *полиномом Чебышёва степени  $n$* .

Справедливо тождество  $T_n(\cos z) = \cos nz$  (см. теорему 1). Полином Чебышёва можно определить, пользуясь этим тождеством (собственно, так и сделал сам Чебышёв). Полином  $T_n$  является четной функцией при четном  $n$  и нечетной функцией при нечетном  $n$ . Старший коэффициент полинома  $T_n$  равен  $2^n$ . Ниже нам понадобится формула  $T_3(x) = 4x^3 - 3x$ .

СЛЕДСТВИЕ 3. *Уравнение  $T_n(x) = a$  явно решается в радикалах. Именно, его корни — значения в точке  $a$  многозначной функции  $T_{1/n}(a)$ .*

ДОКАЗАТЕЛЬСТВО. Если  $\cos z = a$  и  $x = \cos \frac{z}{n}$ , то  $x = T_{1/n}(a)$ . С другой стороны, в этом случае  $T_n(x) = a$ .

Эта «тригонометрическая» выкладка переносится в алгебру и позволяет решить уравнение  $T_n(x) = a$ , где  $a$  — элемент поля, характеристика которого не равна двум (см. п. 1.4). Отметим, что  $T_{1/n}$  —  $n$ -значная функция: выбор значения функции  $u(a)$  не меняет значений  $T_\alpha(a)$ , а функция  $u^{1/n}(a)$  принимает  $n$  значений.

## 1.2. Ростки функций Чебышёва в единице

Многозначная функция  $T_\alpha(x)$ , так же как и степенная функция  $x^\alpha$ , имеет выделенный росток в точке  $x = 1$ , значение которого равно 1. С однозначными ростками легче иметь дело, чем с их многозначными аналитическими продолжениями. Ниже символом  $x^\alpha$  мы обозначаем росток  $\sum \frac{\alpha \cdot \dots \cdot (\alpha - k + 1)}{k!} (x - 1)^k$ .

СВОЙСТВА РОСТКОВ СТЕПЕННЫХ ФУНКЦИЙ В ЕДИНИЦЕ:

- 1) *свойство композиции*: если  $f = x^\alpha$  и  $g = x^\beta$ , то  $f \circ g = x^{\alpha\beta}$ ; другими словами,  $(x^\beta)^\alpha = x^{\alpha\beta}$ ;
- 2) *свойство мультипликативности*:  $x^\alpha x^\beta = x^{\alpha+\beta}$ ;
- 3) *свойство алгебраичности*: для  $\alpha = 1/n$ , где  $n$  — натуральное число, росток  $z = x^\alpha$  удовлетворяет алгебраическому уравнению  $z^n = x$ .

АНАЛИТИЧЕСКИЕ РОСТКИ, ИНВАРИАНТНЫЕ ПРИ ИНВОЛЮЦИИ.

Инволюция  $\tau$  комплексной прямой  $\tau(u) = u^{-1}$  переводит точку  $u = 1$  в себя. Легко описать все ростки  $f$  аналитических функций в этой точке, инвариантные относительно инволюции  $\tau$ , т. е. такие, что  $f = f(\tau)$ .

УТВЕРЖДЕНИЕ 4. *Равенство  $f = f(\tau)$  справедливо, если и только если  $f(u) = \varphi(x)$ , где  $x = (u + u^{-1})/2$  и  $\varphi$  — росток аналитической функции в точке  $x = 1$ .*

ДОКАЗАТЕЛЬСТВО. Если  $f = f(\tau)$ , то функция  $\varphi(x) = f(u(x))$ , где  $u(x)$  — одна из двух ветвей функции, определенной уравнением  $(u(x) + u^{-1}(x))/2 = x$ , не зависит от выбора ветви и аналитична в проколотой окрестности точки  $x = 1$ . По теореме об устранимой особенности она аналитична и в этой точке тоже.

Ростки аналитических функции от  $u$ , не инвариантные относительно инволюции  $\tau$ , задают *двузначные ростки Пьюизо* от  $x$ .

Ростком функции Чебышёва  $T_\alpha$  в точке  $x = 1$  мы будем называть росток аналитической функции от  $x$ , такой, что росток функции  $\frac{u^\alpha + u^{-\alpha}}{2}$  (инвариантный при инволюции  $\tau$ ) равен  $T_\alpha(x(u))$ , где  $x(u) = (u + u^{-1})/2$ . В этом пункте мы будем обозначать росток функции Чебышёва тем же символом  $T_\alpha$ , что и саму многозначную функцию. Ростки  $T_\alpha$  наследуют свойства ростков степенных функций.

СВОЙСТВА РОСТКОВ ФУНКЦИИ ЧЕБЫШЁВА В ЕДИНИЦЕ:

- 1) *свойство композиции*:  $T_\alpha \circ T_\beta = T_{\beta\alpha}$ ;
- 2) *свойство мультипликативности*:  $T_\alpha T_\beta = (T_{\alpha+\beta} + T_{\alpha-\beta})/2$ ;
- 3) *свойства алгебраичности*: для  $\alpha = n$ , где  $n$  — натуральное число, росток  $T_\alpha$  является ростком полинома Чебышёва  $T_n$ . Росток  $T_{1/n}$  удовлетворяет алгебраическому уравнению  $T_n(T_{1/n}(x)) = x$ ;
- 4) *тригонометрическое свойство*:  $T_\alpha(\cos z) = \cos \alpha z$ . Под этим равенством мы подразумеваем равенство ростков функций от  $z$  в точке  $z = 0$ . Суперпозиция  $T_\alpha(\cos z)$  определена, так как  $\cos 0 = 1$ .

УТВЕРЖДЕНИЕ 5. Семейство ростков функций Чебышёва в единице удовлетворяет свойствам 1)–4).

ДОКАЗАТЕЛЬСТВО. 4) следует из теоремы 1. Это свойство полностью характеризует росток  $T_\alpha$ . Действительно, функция  $\cos z$  четная. По теореме о неявной функции росток в нуле функции  $z^2$  является аналитической функцией от ростка в единице функции  $\cos z$ . В свою очередь функция  $\cos \alpha z$  — аналитическая функция от  $z^2$ . 1)–3) — это простые свойства функции  $\cos$ : 1) если  $\cos v = \cos \beta z = T_\beta(\cos z)$ , то  $\cos \alpha v = T_\alpha(\cos v)$  и  $T_\alpha T_\beta \cos z = \cos \alpha \beta z$ ; 2) вытекает из тождества  $\cos \alpha z \cos \beta z = [\cos((\alpha + \beta)z) + \cos((\alpha - \beta)z)]/2$ ; 3) для  $\alpha = n$  доказано в утверждении 2, для  $\alpha = \frac{1}{n}$  вытекает из свойства композиции.

### 1.3. АНАЛИТИЧЕСКОЕ ПРОДОЛЖЕНИЕ РОСТКОВ

В этом пункте мы покажем, что множество значений многозначной функции, порожденной ростком  $T_\alpha$ , согласуется с определением из п. 1.1.

Обращение ростка в нуле функции  $\cos z$  — двузначный росток Пьюизо в точке  $x = 1$ , значения которого различаются знаком. Пусть  $\pi^{-1}(x)$  — одно из двух различающихся знаком многозначных обращений функции  $\cos z = x$ , имеющих в точке  $x = 1$  этот росток Пьюизо. Рассмотрим четную функцию  $\Phi_\alpha(z) = \cos \alpha z$  переменной  $z$ . По определению  $T_\alpha = \Phi_\alpha \circ \pi^{-1}$ .

Функция  $\cos z$  имеет некратные критические точки  $z = k\pi$  и два критических значения  $x = \pm 1$ . Скажем, что кривая  $x(t)$ , идущая из точки 1 в точку  $x_0$ , т. е.  $x(0) = 1$ ,  $x(1) = x_0$ , допустима, если  $x(t) \neq \pm 1$  при  $0 \leq t \leq 1$ . Росток Пьюизо в точке  $x = 1$  функции  $\pi^{-1}$  в следующем смысле продолжается вдоль допустимой кривой  $x(t)$ , идущей из  $x = 1$  в точку  $x_0$ : 1) любая из двух ветвей ростка аналитически продолжается вдоль  $x(t)$  вплоть до  $t = 1$ , если  $x_0 \neq \pm 1$ , и вплоть до любого  $t < 1$ , если  $x_0 = \pm 1$ . В последнем случае продолжение до  $t = 1$  — двузначный росток Пьюизо в точке  $x_0 = \pm 1$  (ветви которого в  $x_0$  совпадают).

Росток  $T_\alpha = \Phi_\alpha \circ \pi^{-1}$  в этом же смысле продолжается вдоль любой допустимой кривой  $x(t)$ . Росток  $T_\alpha$  регулярен и однозначен (а не двузначен, как  $\pi^{-1}$ ), поэтому он имеет *единственное продолжение* вдоль допустимой кривой. Для некоторых допустимых кривых, идущих из точки  $x = 1$  в точку  $x = k\pi$ , результат продолжения тоже может оказаться аналитическим ростком (а не двузначным ростком Пьюизо).

Покажем, что формулы (1), (2) описывают все значения многозначной функции, полученной продолжением ростка  $T_\alpha$ . Пусть  $x_0$  и  $a = T_\alpha(x_0)$  — любые числа, удовлетворяющие (1), (2).

УТВЕРЖДЕНИЕ 6. Существует допустимая кривая  $x(t)$ , идущая из точки  $x = 1$  в точку  $x_0$ , такая, что аналитический росток (или росток Пьюизо), полученный продолжением ростка  $T_\alpha$  вдоль  $x(t)$ , принимает в точке  $x_0$  значение  $a$ , определенное выше.

ДОКАЗАТЕЛЬСТВО. Выберем  $z_0$  так, чтобы  $\exp iz_0 = u(x_0)$ ,  $\exp(\alpha iz_0) = u^\alpha(x_0)$ . Пусть  $z(t)$  — кривая, такая, что  $z(0) = 0$ ,  $z(1) = z_0$  и  $z(t)$  не проходит через точки  $z = k\pi$  при  $0 < t < 1$ . Тогда кривая  $x(t) = \cos z(t)$  допустима, идет из точки  $x = 1$  в точку  $x_0$  и аналитическое продолжение вдоль этой кривой ростка  $T_\alpha = \cos \alpha(\cos^{-1})$  дает росток, принимающий в точке  $x_0$  значение  $a$ .

Для нас особенно важны полиномы Чебышёва  $T_n$  и функции  $T_{1/n}$ , обратные к ним. Благодаря утверждению 6, мы имеем описание множества значений функции  $T_{1/n}$  в точке  $a$ . Пусть  $u_1, u_2$  — корни уравнения  $\frac{u + u^{-1}}{2} = a$  (достаточно взять один из этих корней). Пусть  $\{v_{i,j}\}$  — корни уравнения  $v^n = u_i$ , где  $i = 1, 2$ ;  $1 \leq j \leq n$ . Множество  $\{T_{1/n}(a)\}$  всех значений функции в точке  $a$  равно множеству  $\left\{ \frac{v_{1,j} + v_{i,j}^{-1}}{2} \right\}$  и множеству  $\left\{ \frac{v_{2,j} + v_{2,j}^{-1}}{2} \right\}$ .

## §2. ФУНКЦИИ ЧЕБЫШЁВА НАД ПОЛЯМИ

### 2.1. АЛГЕБРАИЧЕСКОЕ ОПРЕДЕЛЕНИЕ

Полином Чебышёва  $T_n \in \mathbb{Z}[x]$  определен над любым полем  $\mathbb{k}$ . Если характеристика поля равна нулю, то  $\mathbb{Z} \subseteq \mathbb{k}$  и  $T_n \in \mathbb{k}[x]$ . Если поле имеет характеристику  $p > 0$ , то  $\mathbb{Z}_p \subseteq \mathbb{k}$  и полином, полученный из  $T_n$  приведением его коэффициентов по модулю  $p$  (который мы будем обозначать тем же символом  $T_n$ ), принадлежит  $\mathbb{k}[x]$ . Если  $p \neq 2$ , то  $\deg T_n = n$ , так как старший коэффициент полинома  $T_n$  равен  $2^{n-1}$ .

УТВЕРЖДЕНИЕ 7. Если характеристика поля  $\mathbb{k}$  не равна двум, то в поле рациональных функций  $\mathbb{k}(x)$  справедливо тождество

$$T_n \left( \frac{x + x^{-1}}{2} \right) = \frac{x^n + x^{-n}}{2}. \quad (3)$$

ДОКАЗАТЕЛЬСТВО. Вытекает из формул (1), (2).

СЛЕДСТВИЕ 8. Если характеристика поля  $\mathbb{k}$  не равна двум, то уравнение  $T_n(x) = a$  над полем  $\mathbb{k}$ , где  $a \in \mathbb{k}$ , явно решается в радикалах.

ДОКАЗАТЕЛЬСТВО. В тождество (3) подставим  $x = (v + v^{-1})/2$ . Получим  $(v^n + v^{-n})/2 = a$ . Решим квадратное уравнение  $u^2 - 2au + 1 = 0$

для  $u = v^n$ . Пусть  $u_1, u_2$  — его корни и  $\{v_{1,j}\}$  — множество всех корней степени  $n$  из  $u_1$ . Тогда элементы  $v_{2,j} = v_{1,j}^{-1}$  образуют множество всех корней степени  $n$  из  $u_2$ , так как  $u_1 u_2 = 1$ . Все корни уравнения  $T_n(x) = a$  представимы в виде  $x = (v_{1,j} + v_{1,j}^{-1})/2$ , а также в виде  $x = (v_{2,j} + v_{2,j}^{-1})/2$ .

Доказательство следствия 8 показывает, что уравнение  $T_n(x) = a$  над полем  $\mathbb{k}$ , характеристика которого не равна двум, решается явно при помощи формулы  $x = T_{1/n}(a)$ , которая имеет смысл и над полем  $\mathbb{k}$ .

## 2.2. УРАВНЕНИЯ СТЕПЕНИ ТРИ

Пусть  $F$  — полином степени  $n$  над полем  $\mathbb{k}$ , характеристика которого или равна нулю, или больше чем  $n$ . Положим  $Q(y) = aF(\lambda y + x_0)$ , где  $a \neq 0, \lambda \neq 0$  и  $x_0$  — элементы поля  $\mathbb{k}$  или его расширения. При сделанных предположениях о характеристике поля  $\mathbb{k}$  имеем

$$Q(y) = \sum \frac{a\lambda^k F^{(k)}(x_0)}{k!} y^k.$$

Линейная функция  $Q^{(n-1)}$  обращается в нуль в некоторой точке  $q$ . Положим  $x_0 = q$ , тогда коэффициент в  $Q$  при  $y^{n-1}$  обратится в нуль. Меняя  $a$  и  $\lambda$ , можно добиться, чтобы два ненулевых коэффициента полинома  $Q$  приняли заданные ненулевые значения.

Описанным преобразованием полином  $F(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$  можно привести либо к виду  $y^3 + c$ , либо к виду  $4y^3 - 3y + c$ . Полином  $F''$  обращается в нуль в точке  $x_0 = -a_2/3a_3$ . Возможны два случая:

1)  $F'(x_0) = 0$ . В этом случае полином  $F$  приводится к виду  $y^3 + c$  преобразованием  $aF(y + x_0)$ , где  $a = a_3^{-1}$ . При этом  $c = F(x_0)a$ .

2)  $F'(x_0) \neq 0$ . В этом случае полином  $F$  приводится к виду  $4y^3 - 3y + c$  преобразованием  $aF(\lambda y + x_0)$ , где

$$\lambda = (-4F'(x_0)/3a_3)^{1/2}; \quad a = -3(\lambda F'(x_0))^{-1}.$$

При этом  $c = F(x_0)a$ . (Знак  $\lambda$  можно выбрать любым: мы ищем одно преобразование, обладающее нужным свойством, а не описываем их все.)

СЛЕДСТВИЕ 9. Кубическое уравнение  $F(x) = a_3 x^3 + a_2 x^2 + a_1 x + a_0$  над полем  $\mathbb{k}$ , характеристика которого не равна двум и трем, следующим образом решается в радикалах. Пусть  $x_0 = -a_2/3a_3$  — корень полинома  $F''$ . Тогда:

- 1) если  $F'(x_0) = 0$ , то  $x = x_0 + (-F(x_0)/a_3)^{1/3}$ ;
- 2) если  $F'(x_0) \neq 0$ , то  $x = x_0 + \lambda T_{1/3}(-c)$ , где  $\lambda$  и  $c$  определены выше.

## 2.3. УРАВНЕНИЯ СТЕПЕНИ ЧЕТЫРЕ

Уравнение степени четыре можно свести к уравнению третьей степени (которое решается с помощью функции  $T_{1/3}$ ), рассматривая пучок плоских квадрик [4].

Пусть  $Q: V \rightarrow \mathbb{k}$  квадратичная форма и  $\dim_{\mathbb{k}} V = n$ . Квадратичную форму на плоскости и на прямой можно разложить на линейные множители (возможно, не над исходным полем  $\mathbb{k}$ , а над его квадратичным расширением  $K$ ). Пусть  $K$  — расширение поля  $\mathbb{k}$ , а  $V_K$  и  $Q_K$  — пространство и форма, соответствующие  $V$  и  $Q$  при расширении  $\mathbb{k} \subset K$ .

**ЛЕММА 10.** *Если  $Q_K$  раскладывается на множители, то  $\dim_{\mathbb{k}} \ker Q \geq n - 2$ . Если это неравенство выполнено, то можно явно найти разложение  $Q_K = L_1 L_2$  над квадратичным расширением  $K$  поля  $\mathbb{k}$ .*

**ДОКАЗАТЕЛЬСТВО.** Если  $Q_K = L_1 L_2$ , то  $\ker Q_K \supset \bigcap_{i=1,2} \{L_i = 0\}$  и  $\dim_K \ker Q_K \geq n - 2$ . Форма  $Q$  определена над  $k$ , поэтому  $\dim_{\mathbb{k}} \ker Q \geq n - 2$ . Если неравенство выполнено, то  $V$  представимо в виде  $V = \ker Q \oplus W$ , где  $\dim_{\mathbb{k}} W \leq 2$ . Пусть  $\pi: V \rightarrow W$  — проекция вдоль  $\ker Q$  и  $\tilde{Q}$  — ограничение формы  $Q$  на  $W$ . На  $W$  есть разложение  $\tilde{Q} = \tilde{L}_1 \tilde{L}_2$  и, следовательно,  $Q = (\pi^* \tilde{L}_1)(\pi^* \tilde{L}_2)$ .

**УТВЕРЖДЕНИЕ 10.** *Координаты  $x, y$  точек пересечения двух плоских квадрик  $\mathcal{P} = 0$  и  $\mathcal{R} = 0$ , где  $\mathcal{P}$  и  $\mathcal{R}$  — полиномы второй степени, можно найти, решая одно кубическое и несколько квадратных и линейных уравнений.*

**ДОКАЗАТЕЛЬСТВО.** Все квадрики пучка  $0 = \mathcal{Q}_\lambda = \mathcal{P} + \lambda \mathcal{R}$ , где  $\lambda$  — параметр, проходят через искомые точки. При некоторых  $\lambda$  квадрика  $\mathcal{Q}_\lambda = 0$  распадается на пару прямых, т. е.  $\mathcal{Q}_\lambda = \mathcal{L}_1 \mathcal{L}_2$ , где  $\mathcal{L}_1, \mathcal{L}_2$  — полиномы первой степени. Это  $\lambda$  удовлетворяет кубическому уравнению  $\det(Q_\lambda) = 0$ , где  $Q_\lambda = P + \lambda Q$  —  $(3 \times 3)$ -матрица квадратичной формы, соответствующей уравнению квадрики в однородных координатах. Действительно, при этом  $\lambda$  форма  $Q_\lambda$  имеет нетривиальное ядро, поэтому  $Q_\lambda = L_1 L_2$ , причем  $L_1, L_2$  можно найти, решая одно квадратное и несколько линейных уравнений. Возвращаясь к координатам  $x, y$ , из  $L_1, L_2$  получим нужные полиномы  $\mathcal{L}_1, \mathcal{L}_2$ . Остается решить квадратные уравнения для нахождения точек пересечения квадрики  $\mathcal{P} = 0$  и прямых  $\mathcal{L}_1 = 0$  и  $\mathcal{L}_2 = 0$ .

**СЛЕДСТВИЕ 11.** *Корни полинома  $a_0 x^4 + a_1 x^3 + a_2 x^2 + a_3 x + a_4$  можно найти, решая одно кубическое и несколько квадратных и линейных уравнений.*

**ДОКАЗАТЕЛЬСТВО.** Корни этого полинома — проекции на ось  $x$  точек пересечения квадрик  $y = x^2$  и  $a_0 y^2 + a_1 x y + a_2 y + a_3 x + a_4 = 0$ .



Полином  $F$  называется *композиционно разложимым*, если он представим в виде  $F = P(Q)$ , где  $P$  и  $Q$  — полиномы степени, большей чем один.

УТВЕРЖДЕНИЕ 12. *Полином  $F$  степени четыре композиционно разложим, если и только если выполнено одно из следующих эквивалентных условий:*

- 1) для некоторого  $x_0$  справедливо тождество  $F(x - x_0) \equiv F(x_0 - x)$ ;
- 2)  $F'(x_0) = 0$ , где  $x_0$  — такая точка, что  $F^{(3)}(x_0) = 0$ .

ДОКАЗАТЕЛЬСТВО. Если тождество справедливо, то  $F$  — полином второй степени от  $y^2$ , где  $y = x - x_0$ . По формуле Тейлора это свойство эквивалентно равенствам  $F'(x_0) = F^{(3)}(x_0) = 0$ . Пусть  $F = Q(P)$ , тогда так как полином  $P$  представим в виде  $P = a(x - x_0)^2 + b$ , имеем  $F(x - x_0) \equiv F(x_0 - x)$ .

### §3. О ТРЕХ КЛАССИЧЕСКИХ ЗАДАЧАХ

#### 3.1. ОБРАЩЕНИЕ ОТОБРАЖЕНИЙ В РАДИКАЛАХ

Когда полиномиальное отображение  $P : \mathbb{C} \rightarrow \mathbb{C}$  обратимо в радикалах? Начнем с примеров.

ПРИМЕР 1. Если  $P$  — степенной полином  $x^n$ , то обратное отображение  $x = z^{1/n}$ , по определению, представимо в радикалах. Если  $n = km$  — составное число, то отображение  $x^n$  раскладывается в композицию  $x^n = (x^m)^k$ . Для простого  $n$  полином  $x^n$  композиционно неразложим.

ПРИМЕР 2. Если  $P = T_n$  — полином Чебышёва, то обратное отображение  $T_{1/n}$  представимо в радикалах. Если  $n = km$  — составное число, то отображение  $T_n$  раскладывается в композицию  $T_n = T_k(T_m)$ . Для простого  $n$  полином  $T_n$  композиционно неразложим.

ПРИМЕР 3. Если  $P$  — полином степени четыре, то обратное отображение представимо в радикалах (так как уравнения четвертой степени решаются в радикалах). Как правило, полиномы степени четыре композиционно неразложимы. Исключения описаны в утверждении 12.

ТЕОРЕМА 13. *Если  $P = P_1 \circ \dots \circ P_k$ , где при  $1 \leq i \leq k$  полином  $P_i$  либо линеен, либо равен композиционно неразложимому полиному степени четыре, либо равен  $x^n$ , где  $n$  — простое число, либо равен  $T_n$ , где  $n > 2$  — простое число. Тогда отображение  $P : \mathbb{C} \rightarrow \mathbb{C}$  обратимо в радикалах.*

ДОКАЗАТЕЛЬСТВО. Следует из рассмотренных примеров 1)–3).

Ритт [14] доказал обратную теорему (см. также [3, 5]).

ТЕОРЕМА 14 (J. RITT). *Если отображение  $P: \mathbb{C} \rightarrow \mathbb{C}$  обратимо в радикалах, то полином  $P$  представим в виде, описанном в теореме 13.*

С теоремой 14 связан следующий интересный вопрос. Насколько единственно представление полинома в виде

$$P = P_1 \circ \dots \circ P_k, \quad (4)$$

где при  $1 \leq i \leq k$  полиномы  $P_i$  композиционно неразложимы? Ритт дал полный ответ на этот вопрос ([15], см. также [17]). Есть ряд соотношений

$$A \circ B = C \circ D, \quad (5)$$

в которых  $A, B, C, D$  — полиномы. Например, есть равенство  $T_m \circ T_n = T_n \circ T_m$ . Есть следующее обобщение равенства  $(x^m)^n = (x^n)^m$ : для всякого полинома  $H$  равенство (5) выполнено для  $A(x) = x^n$ ,  $B(x) = x^m H(x^n)$ ,  $C(x) = x^m H^n(x)$ ,  $D(x) = x^n$ . Ритт доказал, что по модулю выписанных равенств и композиционных соотношений с линейными функциями представление в виде (4) единственно.

Итак, Ритт полностью описал все полиномы, обратимые в радикалах. Семейства степенных полиномов и полиномов Чебышёва играют центральную роль в этом описании.

ЗАМЕЧАНИЕ. В статье [7] полностью описаны все полиномы, обратимые в  $k$ -радикалах, т. е. обратимые при помощи радикалов и решения алгебраических уравнений степени не выше  $k$  (где  $k$  — любое заданное натуральное число). Это обобщение теоремы Ритта опирается на принадлежащую Мюллеру классификацию полиномов [13], обращение которых имеет примитивную группу монодромии.

Ритту также удалось полностью описать рациональные отображения  $R: \mathbb{C} \rightarrow \mathbb{C}$  простой степени  $p$ , которые обратимы в радикалах [14]. В его описании фигурируют функции, связанные с делением аргумента эллиптической функции (подобно тому, как полином  $T_n$  связан с делением аргумента функции  $\cos$ ). Подробнее о таких отображениях см. [5, 6].

### 3.2. ОБРАТИМОСТЬ ОТОБРАЖЕНИЙ КОНЕЧНЫХ ПОЛЕЙ

Полином  $P \in \mathbb{Q}[x]$  можно определить над  $\mathbb{Z}_p$ , если простое число  $p$  не делит знаменатели его коэффициентов. Для каких  $P$  отображение  $P: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  обратимо (т. е. взаимно однозначно) для бесконечного множества простых чисел  $p$ ? Этот вопрос был поставлен Шуром [16], который нашел гипотетический ответ и получил ряд результатов в этом направлении. Фрид доказал гипотезу Шура даже в большей общности [8] — вместо поля  $\mathbb{Q}$  он рассматривал его конечное расширение  $K$ . Здесь мы ограничимся случаем  $K = \mathbb{Q}$ . Иногда нам понадобятся квадратичные расширения  $\mathbb{k}$  полей  $\mathbb{Z}_p$ , содержащие  $p^2$  элементов.

ПРИМЕР 4. При  $p > 2$  четный полином  $P \in \mathbb{Z}[x]$  (например,  $x^{2n}$  или  $T_{2n}$ ) задает необратимое отображение  $P: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$ , так как  $P(x) = P(-x)$  и число значений полинома не больше чем  $\frac{p-1}{2} + 1 < p$ .

ПРИМЕР 5. Для линейного полинома  $P(x) = \frac{a_1}{b_1}x + \frac{a_2}{b_2}$  отображение  $P: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  определено и обратимо, если  $b_1 b_2$  не делится на  $p$ .

ПРИМЕР 6. Отображение  $P: K \rightarrow K$  для  $P(x) = x^q$ , где  $q \neq 2$  — простое число и  $K$  — конечное поле, обратимо, если  $\#K \neq 1 \pmod q$ . Для  $K = \mathbb{Z}_p$  условие  $p \neq 1 \pmod q$ , в частности, выполнено для  $p = 2 \pmod q$ . Для квадратичного расширения  $\mathbb{k}$  поля  $\mathbb{Z}_p$  условие  $p \neq \pm 1 \pmod q$  при  $q > 3$ , в частности, выполнено, если  $p = 2 \pmod q$ .

УТВЕРЖДЕНИЕ 15. Пусть  $q > 2$ ,  $p > 2$  — простые числа и  $p \neq \pm 1 \pmod q$ . Тогда отображение  $T_q: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  обратимо.

ДОКАЗАТЕЛЬСТВО. Докажем, что при любом  $a \in \mathbb{Z}_p$  уравнение  $T_q(x) = a$  имеет решение в  $\mathbb{Z}_p$ . Пусть  $\mathbb{k}$  — расширение степени два поля  $\mathbb{Z}_p$ . Уравнение  $v^2 - av + 1 = 0$  имеет решения  $v_1, v_2 \in \mathbb{k}$ . Так как  $p \neq \pm 1 \pmod q$ , существует единственное решение  $u_1 \in \mathbb{k}$  уравнения  $u^q = v_1$ , где  $v_1$  — любое из решений  $v_1, v_2$ . Пусть  $g$  — нетривиальный элемент группы Галуа поля  $\mathbb{k}$  над  $\mathbb{Z}_p$ . Обозначим  $g(u_1)$  через  $u_2$ . Так как  $g(v_1) = v_2$ , то  $u_2^q = v_2$ . Из равенства  $(u_1 u_2)^q = v_1 v_2 = 1$  вытекает, что  $u_1 u_2 = 1$ . Откуда следует, что элемент  $x = (u_1 + u_2)/2$  — решение уравнения  $T_q(x) = a$ . Так как  $g(x) = x$ , то  $x \in \mathbb{Z}_p$ . Мы доказали, что отображение  $T_q: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  является отображением «на». Поскольку поле  $\mathbb{Z}_p$  конечно, это отображение обратимо.

ЗАМЕЧАНИЕ. Про  $T_3$  в утверждении 15 говорится лишь, что отображение  $T_3: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$  обратимо (что очевидно). Можно проверить, что отображение  $T_3: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  необратимо при  $p > 3$ .

ТЕОРЕМА 16. Пусть  $P = P_1 \circ \dots \circ P_k$ , где при  $1 \leq i \leq k$  полином  $P_i \in \mathbb{Q}[x]$  либо линеен, либо равен  $x^q$ , где  $q > 2$  — простое число, либо равен  $T_q$ , где  $q > 3$  — простое число. Тогда отображение  $P: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  обратимо для бесконечного множества простых чисел.

ДОКАЗАТЕЛЬСТВО. Обозначим через  $E$  конечное множество простых чисел  $p$ , для которых линейные полиномы, входящие в разложение полинома  $P$ , не определены над  $\mathbb{Z}_p$ . Пусть  $M = \{q_i\}$  — множество различных степеней полиномов  $T_{q_i}$  и  $x^{q_i}$ , входящих в разложение полинома  $P$ , и  $m = \prod_{q_i \in M} q_i$ . Пусть  $S$  — множество натуральных чисел, равных двойке по модулю  $m$ . Если  $a \in S$  и  $q_i \in M$ , то  $a \pmod{q_i} = 2$ . По теореме Дирихле в арифметической последовательности  $S$  есть бесконечно много простых чисел  $p > 2$ , не принадлежащих конечному множеству  $E$ . Для каждого из

таких простых чисел  $p$  каждое из отображений  $P_i: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  обратимо (см. примеры 5, 6 и утверждение 15). Теорема доказана.

**ТЕОРЕМА 17 (Фрида).** Пусть для  $P \in \mathbb{Q}[x]$  отображение  $P: \mathbb{Z}_p \rightarrow \mathbb{Z}_p$  обратимо для бесконечного множества простых чисел  $p$ , тогда  $P$  представим в виде  $P = P_1 \circ \dots \circ P_k$ , где при  $1 \leq i \leq k$  полином  $P_i$  либо линеен, либо равен  $x^q$ , либо равен  $T_q$ .

Статья Фрида [8] содержит красивые результаты о комплексных полиномах, близкие к теореме 14 Ритта. Она также использует связи между теорией чисел и алгебраической геометрией (в частности, некоторые результаты А. Вейля).

### 3.3. ИНТЕГРИРУЕМЫЕ ОТОБРАЖЕНИЯ

Итерации полиномиального отображения  $P: \mathbb{C} \rightarrow \mathbb{C}$  комплексной прямой в себя для полиномов  $x^n$  и  $T_n$  ведут себя очень необычно. Их динамика напоминает поведение вполне интегрируемых систем в гамильтоновой механике.

**ПРИМЕР 7.** Итерации отображения  $x \rightarrow x^n$  описываются явно:  $k$ -я итерация — это отображение  $x \rightarrow x^{n^k}$ . Если  $k \rightarrow \infty$ , то  $x_0^{n^k} \rightarrow 0$  при  $|x_0| < 1$  и  $x_0^{n^k} \rightarrow \infty$  при  $|x_0| > 1$ . Проекция  $x = \exp it$  прямой  $\mathbb{R}$  на окружность  $|x| = 1$  сопрягает растяжение  $t \rightarrow nt$  с отображением  $x \rightarrow x^n$ . Отрезок  $|t - t_0| \leq \varepsilon$  после  $k$ -й итерации растяжения переходит в отрезок  $|t - n^k t_0| \leq \varepsilon n^k$ . При  $k \gg 0$  каждая точка окружности имеет порядка  $\frac{\varepsilon}{\pi} n^k$  прообразов в этом отрезке. Точки  $\exp 2\pi i n^{-k}$  после  $k$ -й итерации попадут в точку 1 и останутся в этой точке при следующих итерациях. Хотя итерации отображения описаны явно, его динамика хаотична на окружности  $|x| = 1$ .

**ПРИМЕР 8.** Итерации отображения  $x \rightarrow T_n(x)$  описываются явно:  $k$ -я итерация — это отображение  $x \rightarrow T_{n^k}$ . Если  $k \rightarrow \infty$ , то  $T_{n^k}(x_0) \rightarrow \infty$  при  $x_0 \notin I$ , где  $I \subset \mathbb{R}$  отрезок, определенный неравенством  $|x| \leq 1$ . Проекция  $x = \frac{u + u^{-1}}{2}$  окружности  $|u| = 1$  на отрезок  $I$  сопрягает отображения  $u \rightarrow u^n$  с отображением  $x \rightarrow T_n(x)$ . На отрезке  $I$  динамика отображения  $T_n$  столь же хаотична, как динамика отображения  $u^n$  на окружности  $|u| = 1$ .

**ОПРЕДЕЛЕНИЕ.** Полиномиальное отображение  $P: \mathbb{C} \rightarrow \mathbb{C}$  интегрируемо (см. [1]), если существует полиномиальное отображение  $G: \mathbb{C} \rightarrow \mathbb{C}$ , такое, что  $P \circ G = G \circ P$ , причем: 1)  $\deg P > 1$ ,  $\deg G > 1$ ; 2)  $k$ -я итерация полинома  $P$  не совпадает с  $q$ -й итерацией полинома  $G$  для любых натуральных  $k, q$ .

Отображение  $x \rightarrow x^n$  интегрируемо, так как оно коммутирует со всеми степенными отображениями  $x \rightarrow x^m$ . Если  $m \neq n^{k/q}$ , где  $k, q \in \mathbb{Z}$ , то

итерации этих отображений различны. Отображение  $x \rightarrow T_n(x)$  интегрируемо, так как оно коммутирует со всеми отображениями  $x \rightarrow T_m(x)$ . Если  $m \neq n^{k/q}$ , где  $k, q \in \mathbb{Z}$ , то итерации этих отображений различны.

Полиномы  $P$  и  $G$  эквивалентны, если существует полином  $H(x) = ax + b$ ,  $a \neq 0$ , такой, что  $P \circ H = H \circ G$ . Ритт, Жулия и Фату описали все интегрируемые полиномиальные отображения с точностью до эквивалентности. Приведем их замечательный результат (см. [9, 10, 15]).

**ТЕОРЕМА 17.** *Отображение  $P: \mathbb{C} \rightarrow \mathbb{C}$  интегрируемо, если и только если полином  $P$  эквивалентен одному из полиномов  $x^n$ ,  $T_{2m}$ ,  $T_{2m+1}$ ,  $-T_{2m+1}$ .*

Жулия и Фату доказали эту теорему, используя методы динамики. Доказательство Ритта совершенно другое (ср. п. 3.1).

Ранее Латте привел примеры интегрируемых (в аналогичном смысле) рациональных отображений  $\mathbb{C}P^1$  в себя [11, 12]. Ритт доказал, что нет интегрируемых рациональных отображений, кроме отображений Латте. Динамическими методами, восходящими к Жулия и Фату, доказать эту теорему Ритта никто не мог, пока это не удалось Еременко [2].

Интересно, что все отображения Латте обратимы в радикалах. Ритт описал замечательный класс рациональных отображений, обратимых в радикалах (см. [5, 14]). Этот класс достаточно широк. Например, он содержит все отображения Латте и все обратимые в радикалах отображения простой степени.

Известны многомерные примеры интегрируемых полиномиальных и рациональных отображений (их можно найти в литературе, приведенной в обзоре Милнора [12]).

#### СПИСОК ЛИТЕРАТУРЫ

- [1] Веселов А. П. *Интегрируемые отображения* // УМН. Т. 45. Вып. 5 (281). 1991. С. 3–45.
- [2] Еременко А. Э. *О некоторых функциональных уравнениях, связанных с итерацией рациональных функций* // Алгебра и анализ. Т. 1. Вып. 4. 1989. С. 102–116.
- [3] Хованский А. Г. *Вариации на тему разрешимости в радикалах* // Тр. МИАН. Т. 259. 2007. С. 86–105.
- [4] Berger M. *Geometry*. New York, Berlin, Heidelberg: Springer. 1987.
- [5] Burda Y. *Around rational functions invertible in radicals*. arXiv:1005.4101. 2010.

- [6] Burda Y., Khovanskii A. *Signature of Branch Coverings*. arXiv:1207.1211. 2012.
- [7] Burda Y., Khovanskii A. *Polinomials invertible in  $k$ -radicals*. arXiv:1209.5137. 2012.
- [8] Fried M. *On conjecture of Schur* // Michigan Math. J. Vol. 17. 1970. P. 41–55.
- [9] Fatou P. *Sur l'itération analytique et les substitutions permutables* // J. math. pure appl. V. 23. 1924. P. 1–49.
- [10] Julia G. *Memoire sur la permutabilite des fractions rationale* // Ann. sci. Ec. super. Vol. 39. 1922. P. 131–215.
- [11] Lattès S. *Sur l'iteration des substitutions rationelles et les fonctions de Poincaré* // C.R. Acad. Sci. Paris. Vol. 166. 1918. P. 26–28.
- [12] Milnor J. *On Lattès Maps*. Stony Brook IMS Preprint #2004/01.
- [13] Muller P. *Primitive monodromy groups of polynomials* // Recent developments in the inverse Galois problem (Seattle, WA, 1993). Volume 186 of Contemp. Math. Providence, RI: AMS. 1995. P. 385–401.
- [14] Ritt J. F. *On algebraic functions which can be expressed in terms of radicals* // Trans. Amer. Math. Soc. Vol. 24. 1922. P. 21–30.
- [15] Ritt J. F. *Permutable rational functions* // Trans. Amer. Math. Soc. Vol. 25. No 4. 1923. P. 1–49.
- [16] Shur I. *Über den Zusammenhang zwischen einnem Problem der Zahlentheorie polynomials* // Acta Arith. B. 12. 1966/1967. S. 289–299.
- [17] Zieve M., Muller P. *On Ritt's polynomial decomposition theorems*. arXiv:0807.3578v1. 2008.