Математическая физика, анализ, геометрия
1995, т. 2, № 1, с. 68-86
УДК 517.547.2+512.772

О функциональном уравнении $f(p(z)) = g(q(z))$, где f и g — мероморфные функции, а p и q — полиномы

С. А. Лысенко

Физико-технический институт низких температур им. Б. И. Веркина НАН Украины, Украина, 310164, г. Харьков, пр. Ленина, 47

Статья поступила в редакцию 25 марта 1994 года

Пусть f и g — мероморфные функции в проколотой окрестности бесконечности в C, а p и q — полиномы. В данной статье решается функциональное уравнение $f(p(z)) = g(q(z))$ в двух частных случаях: 1) $\deg p = \deg q$, 2) $p(z) = z^n$, q — любой многочлен.

Введение

В статье [3] было доказано следующее утверждение.

Пусть $p,q \in \mathbb{C}[z]$ — полиномы одинаковых степеней. Пусть

$$f \circ p = g \circ q, \tag{0.1}$$

где f и g — непостоянные целые функции в C. Тогда либо
(i) $p(z) = \lambda q(z) + a$, *где* $\lambda, a \in \mathbb{C}$, *либо*
(ii) $p(z) = r^2(z) + a$, $q(z) = br^2(z) + cr(z) + d$, *где* $r(z)$ — *полином*, $b,c,d \in \mathbb{C}$, $b \neq 0$.

В обзоре [4] был поставлен вопрос (question 5, Flatto): существует ли аналог этого утверждения, когда p и q разных степеней?

Естественно рассмотреть более общие задачи.

Задача 1. *Найти все пары $p,q \in \mathbb{C}[z]\setminus\mathbb{C}$, для которых найдутся непостоянные функции f, g, мероморфные в проколотой окрестности бесконечности в C такие, что выполнено* (0.1).

Задача 2. *То же, что в* 1, *но f и g голоморфны в проколотой окрестности бесконечности в* C.

Целью данной статьи является решение этих задач в двух частных случаях:
А) $\deg p = \deg q$;
Б) $p(z) = z^n$, q — любой многочлен.

Результаты, относящиеся к произвольным p и q, анонсированы в разд. 6.

Естественно рассмотреть также следующую более простую задачу.

Задача 0. *Найти все пары $p,q \in \mathbf{C}[z]\backslash\mathbf{C}$, для которых найдутся рациональные функции f, $g \in \mathbf{C}(z)\backslash\mathbf{C}$ такие, что выполнено* (0.1).

Последняя задача относится к теории факторизации полиномов, разработанной впервые Риттом (см. [6]).

З а м е ч а н и е 0.1. Пусть $p,q,r \in \mathbf{C}[z]\backslash\mathbf{C}$. Пара p, q — решение задачи 1 тогда и только тогда, когда пара $p \circ r$, $q \circ r$ — решение 1. Утверждение останется в силе, если задачу 1 заменить на задачи 0,2. Поэтому можно предполагать, что p и q не имеют нетривиального общего правого фактора. В силу теоремы Люрота последнее эквивалентно тому, что $\mathbf{C}(p,q) = \mathbf{C}(z)$.

З а м е ч а н и е 0.2. Пусть $p,q \in \mathbf{C}[z]\backslash\mathbf{C}$, $\lambda(z) = az + b$, $\widetilde{\lambda}(z) = \widetilde{a}z + \widetilde{b}$, $a \neq 0$, $\widetilde{a} \neq 0$. Назовем внешней линейной заменой переход от пары p, q к паре $\lambda \circ p, \widetilde{\lambda}\circ q$; внутренней — переход к паре $p \circ \lambda$, $q \circ \lambda$. При таких заменах решения задачи 1 переходят снова в решения. (То же верно для задач 0,2).

Неявное решение задачи 0 дает теорема 2.1. В изучаемых нами частных случаях задачу 0 можно решить явно. Ответом служит следующее предложение.

Предложение 0.1.

1) *В случае А) пара p, q дает решение задачи 0 тогда и только тогда, когда $\mathbf{C}(p) = \mathbf{C}(q)$, т.е. p и q отличаются внешней линейной заменой.*

2) *В случае Б)* пара p, q дает решение задачи 0 *тогда и только тогда, когда с точностью до внешней линейной замены q имеет вид $q(z) = z^{\lambda}\widetilde{q}(z^n)$, где $\widetilde{q} \in \mathbf{C}[z]$, $0 \leq \lambda < n$. Для таких q имеем $\mathbf{C}(p \circ q) \subseteq \mathbf{C}(p)\bigcap\mathbf{C}(q)$.*

Опишем теперь решения задач 1 и 2, не являющиеся решениями задачи 0. Начнем с ключевых примеров.

П р и м е р 1. Целая функция $\cos 2\pi z$ выдерживает преобразования $z \to -z$, $z \to z + 1$. Поэтому она допускает правые факторы z^2, $(z + 1)^2$. Эта пара полиномов служит решением задачи 2, но не 0.

П р и м е р 2. $\wp^2(z;1,i)$ выдерживает преобразования $z \to z + 1$, $z \to iz$. Поэтому $\wp^2(z;1,i)$ допускает правые факторы z^4, $(z + 1)^4$. Эта пара полиномов служит решением задачи 1, но не 2,0. То же верно для пары $p(z) = z^2$, $q(z) = (z + 1)^4$.

П р и м е р 3. $(\wp')^2(z;1,w)$, где $w = e^{\pi i/3}$, выдерживает преобразования $z \to z + 1$, $z \to z + w$, $z \to wz$. Поэтому она допускает правые факторы z^6, $(z + 1)^6$. Это дает следующие примеры решений задачи 1 (все они не являются решениями задач 2,0):

$$p(z) = z^2, \quad q(z) = (z + 1)^6 \qquad\qquad p(z) = z^2, \quad q(z) = (z + 1)^3$$

$$p(z) = z^3, \quad q(z) = (z + 1)^3 \qquad\qquad p(z) = z^3, \quad q(z) = (z + 1)^6$$

$$p(z) = z^6, \quad q(z) = (z + 1)^6.$$

Суммируем сказанное в следующем виде.

Предложение 0.2. *Пусть* $p(z) = z^n$, $q(z) = (z+1)^m$; n, m, $НОК(n,m) \in \{2,3,4,6\}$. *Тогда пара* p, q *дает решение задачи* 1. *Если* $n = m = 2$, *то пара* p, q *дает также и решение задачи* 2.

Теоремы, изложенные ниже, означают, что других решений задача 1, по-существу, не имеет в двух изучаемых частных случаях. Ответ в случае А) дает

Теорема 0.1. *Пусть* $p,q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p,q) = \mathbb{C}(z)$, $\deg p = \deg q$. *Пара* p, q *дает решение задачи* 1, *но не* 0, *тогда и только тогда, когда после линейных замен* $p(z) = z^n$, $q(z) = (z+1)^n$, $n \in \{2,3,4,6\}$.

Следствие. *Пусть* $p,q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p,q) = \mathbb{C}(z)$, $\deg p = \deg q$. *Пара* p, q *дает решение задачи* 2, *но не* 0, *тогда и только тогда, когда после линейных замен* $p(z) = z^2$, $q(z) = (z+1)^2$.

Ответ в случае Б) дает

Теорема 0.2. *Пусть* $p(z) = z^n$, $q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p,q) = \mathbb{C}(z)$. *Для того чтобы пара* p, q *служила решением задачи* 1, *но не* 0, *необходимо и достаточно, чтобы после внешней линейной замены* q *принимал вид* $q = \tilde{q} \circ r$, *где* $r(z) = z^\lambda \tilde{r}(z^n)$, $\tilde{r}$ — *любой многочлен*, $0 < \lambda < n$, $НОД(\lambda, n) = 1$, $\tilde{q}(z) = (z+a)^m$, $a \neq 0$; n, m, $НОК(n,m) \in \{2,3,4,6\}$.

Следствие. *Пусть* $p(z) = z^n$, $q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p,q) = \mathbb{C}(z)$. *Пара* p, q *дает решение задачи* 2, *но не* 0, *тогда и только тогда, когда в обозначениях теоремы 0.2 имеем* $m = n = 2$.

Основная идея решения задачи 1 состоит в следующем. Обозначим через $\mathfrak{J}$ группу ростков конформных отображений: $(\overline{\mathbb{C}}, \infty) \to (\overline{\mathbb{C}}, \infty)$. Здесь $\overline{\mathbb{C}}$ — сфера Римана. Пусть F мероморфна в проколотой окрестности бесконечности в C. Тогда мы определяем группу $T_F = \{ g \in \mathfrak{J} \mid F \circ g = F \}$. Далее пусть $F = f \circ p$, где p — полином, f мероморфна в области $C < |z| < \infty$. Тогда T_p — подгруппа в T_F. Оказывается, что группа T_p полностью отражает поведение полинома p в окрестности бесконечности. (p восстанавливается по группе T_p с точностью до внешней линейной замены, см. разд. 2).

Будем называть подгруппу $\Gamma \subset \mathfrak{J}$ дискретной, если найдется непостоянная функция F, мероморфная в проколотой окрестности бесконечности такая, что $\Gamma \subset T_F$. В разд. 1 мы обсуждаем необходимое условие дискретности, которое называем формальной дискретностью. Это алгебраическое свойство группы Г. Наконец, если пара p, q — решение задачи 1, то T_p и T_q порождают дискретную подгруппу в $\mathfrak{J}$. Поэтому естественно рассмотреть следующую алгебраическую задачу.

Задача 3. *Найти все пары* $p,q \in \mathbb{C}[z]\backslash\mathbb{C}$, *для которых* T_p *и* T_q *порождают формально дискретную подгруппу в* $\mathfrak{J}$.

Решения задачи 1 содержатся среди решений задачи 3. Нам удается решить задачу 3 в случаях А) и Б). Оказывается, что в этих частных случаях задачи 1 и 3 эквивалентны.

Статья делится на аналитическую (разд. 1) и алгебраическую (все остальное) части. Все, что касается задачи 0, содержится в разд. 2. В разд. 3-5 решается задача 3 в указанных выше частных случаях. В разд. 6 мы анонсируем решение задачи 3 для произвольных p и q. Оказывается, что и без дополнительных предположений относительно p и q все решения задачи 3 являются решениями задачи 1 и, в некотором смысле, сводятся к рассмотренным выше примерам 1-3.

Автор выражает благодарность В. Г. Дринфельду за постоянную поддержку и многочисленные замечания, а также М. Л. Содину и А. Э. Еременко за внимание к работе.

1. Дискретность и формальная дискретность

Обозначим через $\mathfrak{I}$ группу ростков конформных отображений: $(\overline{\mathbb{C}}, \infty) \to (\overline{\mathbb{C}}, \infty)$. Введем фильтрацию

$$\mathfrak{I}_1 = \{ g(z) = a_1 z + a_0 + \frac{a_{-1}}{z} + \ldots \in \mathfrak{I} \mid a_1 = 1 \},\ \mathfrak{I}_0 = \{ g \in \mathfrak{I}_1 \mid a_0 = 0 \},$$
$$\mathfrak{I}_{-1} = \{ g \in \mathfrak{I}_0 \mid a_{-1} = 0 \} \text{ и т.д.}$$

$\mathfrak{I} \supset \mathfrak{I}_1 \supset \mathfrak{I}_0 \supset \mathfrak{I}_{-1} \supset \ldots.\ \mathfrak{I}_k$ — нормальная подгруппа в $\mathfrak{I}$.

Определение. *Назовем подгруппу* $\Gamma \subset \mathfrak{I}$ *дискретной, если найдется* $C > 0$ *и функция* $F(z)$, *мероморфная в области* $C < |z| < \infty$, $F \not\equiv const$ *такая, что* $F(g(z)) = F(z)$ *для всех* $g \in \Gamma$.

Целью этого раздела является установление необходимого условия дискретности группы Γ. Положим $\Gamma_k = \Gamma \cap \mathfrak{I}_k$, $k \leq 1$.

Теорема 1.1. *Пусть* $\Gamma \subset \mathfrak{I}$ *дискретная подгруппа. Тогда*

1) *среди факторгрупп* Γ_k/Γ_{k-1} $(k \leq 1)$ *имеется не более одной, отличной от нуля;*

2) *для всех* $k \leq 1$ *подгруппа* $\Gamma_k/\Gamma_{k-1} \subset \mathfrak{I}_k/\mathfrak{I}_{k-1} \cong (\mathbb{C}, +)$ *дискретна.*

Определение. Подгруппы в $\mathfrak{I}$, удовлетворяющие условиям 1) и 2), будем называть формально дискретными.

Замечание. Если подгруппа $\Gamma \subset \mathfrak{I}$ формально дискретна, то Γ_1 абелева, поскольку для всех k: $[\mathfrak{I}_k, \mathfrak{I}_k] \subset \mathfrak{I}_{k-1}$.

При доказательстве теоремы 1.1 мы используем результаты локальной динамики (теорию модулей Воронина-Экалля, см. [1]). Если выполнить замену переменных

$w = z^{-1}$, то группа $\mathfrak{I}_1$ перейдет в группу ростков конформных отображений: $(\overline{\mathrm{C}}, 0) \to (\overline{\mathrm{C}}, 0)$ с тождественной линейной частью. Обозначим ее через А. Обозначим также через A_p множество всех $f \in \mathrm{A}$ вида $f(z) = z + az^p + \ldots$, $a \neq 0$. Проколотая окрестность нуля в С покрывается системой $2p$ секторов вида

$$S_j = \left\{z\colon \left| \arg z - \frac{\pi j}{p} \right| < \alpha\right\}, \qquad \alpha \in \left(\frac{\pi}{2p}, \frac{\pi}{p}\right), \qquad j = 1,\ldots,2p.$$

Это покрытие называют хорошим p-покрытием. В [1], с.16, п. 2.5 было доказано следующее предложение.

Предложение 1.1. *Пусть* $f(z) = z + z^{p+1} + \ldots$, $f \in \mathrm{A}_{p+1}$. *В каждом секторе* S_j *хорошего* p*-покрытия существует единственное биголоморфное отображение* $H_j\colon z \to z + h_j(z)$, $h_j(z) = o(z^{p+1})$, *сопрягающее* f *с преобразованием за единичное время* g_w^1 *потока векторного поля* $w = w_{p,\lambda} = z^{p+1}(1 + \lambda z^p)^{-1} \frac{d}{dz}$.

З а м е ч а н и е. g_w^1 является формальной нормальной формой ростка f.

Продолжим главную ветвь $\ln z$ из сектора S_{2p} в S_1. Тогда отображение

$$z \to t(z) = -p^{-1}z^{-p} + \lambda \ln z \tag{1.1}$$

переведет сектор S_1 хорошего p-покрытия в область, содержащую сектор $|\arg t| \leq \frac{\pi}{2} + \varepsilon$ без большого круга $|t| \leq R$. Здесь $\varepsilon > 0$ достаточно мало. Поле $w = w_{p,\lambda}$ переходит при отображении (1.1) в постоянное поле $\frac{d}{dt}$. Соответственно g_w^1 переходит в сдвиг $t \to t + 1$.

Лемма 1.1. *Пусть* Δ *— полуплоскость вида* $\mathrm{Re}\, z \quad A$, $A \in \mathbf{R}$, $R(z) = z + 1$, $T(z)$ *голоморфна в* Δ, $T(z) - z \to 0$ *при* $z \to \infty$ *в* Δ. *Пусть* $F\ z)$ *мероморфна в* Δ, $F \not\equiv const$, $F(R(z)) = F(T(z)) = F(z)$. *Тогда* $T = id$.

Д о к а з а т е л ь с т в о. Пусть $K \subset \Delta$ компакт с непустой внутренностью, причем $F'(z) \neq 0$ при $z \in K$. Положим

$$a = \inf\left\{|z_1 - z_2| : z_1 \in K, z_2 \in \Delta, z_1 \neq z_2, F(z_1) = F(z_2)\right\}.$$

Тогда $a > 0$. Рассмотрим последовательность $f_n = R_{(-n)} \circ T \circ R_{(n)}$, т. е. $f_n(z) = T(z + n) - n$. Из условия следует, что $f_n(z) \to z$ при $n \to \infty$ равномерно по $z \in K$. Поэтому для большого $n \in \mathrm{N}$ имеем $\left| f_n(z) - z \right| < \frac{a}{2}$ для $z \in K$. Поскольку $F(f_n(z)) = F(z)$, то получаем $f_n(z) = z$ при $z \in K$, а тогда и $T = id$ по принципу аналитического продолжения. ◊

Предложение 1.2. *Пусть* $f \in \mathrm{A}_{p+1}$, $g \in \mathrm{A}_{q+1}$; $p, q \in \mathrm{N}$, $q > p$. *Тогда* f *и* g *порождают недискретную группу.*

Доказательство. Пусть это не так и найдется функция $F(z)$, мероморфная в проколотой окрестности нуля такая, что $F \not\equiv \mathrm{const}$, $F(f(z)) = F(g(z)) = F(z)$. Можно считать, что $f(z) = z + z^{p+1} + \dots$. Пусть $\{S_j\}$ — хорошее p-покрытие окрестности нуля, в которой f определено. В силу предложения 1.1 имеем в S_1 биголоморфное отображение H_1, сопрягающее f с ростком g_w^1: $H_1 \circ f \circ H_1^{-1} = g_w^1$. Пусть $t(z)$ задано формулой (1.1). Положим $R = t \circ H_1 \circ f \circ H_1^{-1} \circ t^{-1}$, $T = t \circ H_1 \circ g \circ H_1^{-1} \circ t^{-1}$. Тогда $R(z) = z + 1$, R и T определены в полуплоскости $\Delta = \{\mathrm{Re}\, z > A\}$ при достаточно большом $A > 0$. $T(z) - z \to 0$ при $z \to \infty$ в Δ из-за того, что $q > p$. Функция $\widetilde{F} = F \circ H_1^{-1} \circ t^{-1}$ мероморфна в Δ, $\widetilde{F}(R(z)) = \widetilde{F}(T(z)) = \widetilde{F}(z)$ в Δ. В силу леммы 1.1 $g = id$. Противоречие. ◊

Из предложения 1.2 следует утверждение 1) теоремы 1.1. Следующее предложение доказано в [1], с. 26, теор. 3, а также с. 23, теор. 1.

Предложение 1.3. *Пусть $g \in \mathrm{A}$, $g \neq id$.*

1) *Если g не включаемо в поток, то централизатор g в группе A изоморфен $\mathbb{Z}$.*

2) *Пусть g включаемо в поток и имеет формальную нормальную форму g_w^1 — преобразование за единичное время для поля $w = w_{p\lambda} = z^{p+1}(1 + \lambda z^p)^{-1} \frac{d}{dz}$. Тогда g аналитически эквивалентно g_w^1. Централизатор g_w^1 в A — это группа $\{g_w^t, t \in \mathbb{C}\}$.*

Замечание. В случае 2) централизатор g в A сопряжением приводится к виду $\{g_w^t, t \in \mathbb{C}\}$.

Предложение 1.4. *Пусть $p \in \mathbb{N}$, $\lambda \in \mathbb{C}$, $w = w_{p\lambda} = z^{p+1}(1 + \lambda z^p)^{-1} \frac{d}{dz}$, $\Gamma \subset \left\{g_w^\xi, \xi \in \mathbb{C}\right\}$ — подгруппа, $T_\Gamma = \left\{\xi \in \mathbb{C} \mid g_w^\xi \in \Gamma\right\}$. Пусть Γ — дискретная подгруппа в A. Тогда T_Γ — дискретная подгруппа в $(\mathbb{C}, +)$. Пусть вдобавок T_Γ — полная решетка в $\mathbb{C}$, $F(z)$ голоморфна в проколотой окрестности нуля, $F(g(z)) = F(z)$ для всех $g \in \Gamma$. Тогда $F \equiv \mathrm{const}$.*

Доказательство. Пусть $\{S_j\}$ — хорошее p-покрытие окрестности нуля. Зададим $t(z)$ формулой (1.1). Сопрягая все элементы Γ с помощью t в S_1, получим набор сдвигов $t \to t + \xi$, $\xi \in T_\Gamma$. Каждый из этих сдвигов будет определен в своей полуплоскости $\Delta_\xi = \{\mathrm{Re}\, t > A_\xi\}$ для некоторого $A_\xi > 0$. Пусть $F(z)$ мероморфна в проколотой окрестности нуля и Γ-инвариантна. Тогда $F \circ t^{-1}$ будет мероморфна в некоторой полуплоскости $\Delta = \{\mathrm{Re}\, t > A\}$, $A > 0$ и инвариантна относительно сдвигов из T_Γ. Если T_Γ сохраняет Δ, то получаем, что T_Γ — дискретная подгруппа в $\mathbb{C}$. Если не сохраняет, то функцию $F \circ t^{-1}$ можно продолжить до мероморфной в $\mathbb{C}$ с помощью сдвигов из T_Γ. Она станет T_Γ-инвариантной и поэтому всегда T_Γ — дискретная подгруппа в $\mathbb{C}$. Пусть, наконец, T_Γ — полная решетка в $\mathbb{C}$, а $F(z)$ голоморфна в проколотой окрестности нуля. Тогда $F \circ t^{-1}$ продолжается до голоморфной в $\mathbb{C}$ двоякопериодической функции, т. е. константы. По принципу аналитического продолжения $F \equiv \mathrm{const}$. ◇

С л е д с т в и е. *Пусть* $\Gamma \subset \mathfrak{I}$ *подгруппа,* $F(z)$ *голоморфна в области* $C < |z| < \infty$, $F \not\equiv const$. *Пусть* $F(g(z)) = F(z)$ *для всех* $g \in \Gamma$. *Тогда либо* $\Gamma_1 = 0$, *либо* $\Gamma_1 \simeq \mathbf{Z}$.

Второе утверждение теоремы 1.1 теперь получается, если сопоставить предложения 1.3 и 1.4. Доказательство теоремы 1.1 закончено.

З а м е ч а н и е. Теорема 1.1, в частности, означает, что дискретная подгруппа Γ в $\mathfrak{I}$ всегда разрешима. В статье [2] дана формальная и аналитическая классификация неабелевых разрешимых конечно-порожденных подгрупп в $\mathfrak{I}$.

2. Структура поля $\mathbf{C}(p)\cap\mathbf{C}(q)$, где $p, q \in \mathbf{C}[z]$

Решение задачи 0 (см. Введение) равносильно нахождению $\mathbf{C}(p)\cap\mathbf{C}(q)$ для заданных $p, q \in \mathbf{C}[z]\backslash\mathbf{C}$. Напомним, что для функции f, мероморфной в проколотой окрестности бесконечности, мы обозначаем $T_f = \{ g \in \mathfrak{I} \mid f \circ g = f \}$.

Предложение 2.1. *Пусть* $f(z)$ *голоморфна в проколотой окрестности бесконечности,* $f(z) = z^n + a_{n-1}z^{n-1} + \ldots$ — *ее ряд Тейлора,* $n \in \mathbf{N}$. *Тогда* T_f *сопряжением в* $\mathfrak{I}$ *приводится к виду* $\{ \varepsilon z \mid \varepsilon^n = 1 \}$, T_f *циклическая из* n *элементов.*

Д о к а з а т е л ь с т в о. Положим $g(z) = f(z)^{1/n} = z\left(1 + a_{n-1}z^{-1} + \ldots\right)^{1/n} \in \mathfrak{I}$. Вычисляя T_f, мы должны решить уравнение $f(w) = f(z)$, $w \in \mathfrak{I}$. Имеем $g(w)^n = g(z)^n \Leftrightarrow g(w) = \varepsilon g(z)$, где $\varepsilon^n = 1$. Отсюда $w = g^{-1}(\varepsilon g(z))$. ◇

С л е д с т в и е 1. Если $p \in \mathbf{C}[z]$, $\deg p = n$, то T_p — циклическая группа из n элементов.

С л е д с т в и е 2. Пусть p, q — пара полиномов, дающая решение задачи 0. Тогда T_p и T_q порождают конечную циклическую подгруппу в $\mathfrak{I}$.

Рассмотрим поле $\mathbf{C}((z^{-1}))$, снабженное нормированием ord_∞. Если $g \in \mathbf{C}((z^{-1}))$, $g = \sum_{k \le n} a_k z^k$, $a_n \neq 0$, то $ord_\infty g = -n$. Это полное поле. Обозначим через $\tilde{\tilde{\mathfrak{I}}}$ группу автоморфизмов $\mathbf{C}((z^{-1}))$ над $\mathbf{C}$, которые являются гомеоморфизмами метрического пространства $\mathbf{C}((z^{-1}))$. Обозначим через $\tilde{\mathfrak{I}}$ группу формальных рядов $\left\{a_1 z + a_0 + a_{-1}z^{-1} + \ldots \mid a_1 \neq 0,\ a_i \in \mathbf{C}\right\}$ с операцией композиции. Легко видеть, что отображение $\tilde{\tilde{\mathfrak{I}}} \to \tilde{\mathfrak{I}}$, переводящее τ в $\tau(z)$, устанавливает антиизоморфизм этих групп. Мы иногда отождествляем $\tilde{\mathfrak{I}}$ и $\tilde{\tilde{\mathfrak{I}}}$, имея в виду этот антиизоморфизм.

В $\tilde{\mathfrak{I}}$ имеется стандартная фильтрация

$$\tilde{\mathfrak{I}} \supset \tilde{\mathfrak{I}}_1 \supset \tilde{\mathfrak{I}}_0 \supset \tilde{\mathfrak{I}}_{-1} \supset \ldots,$$

которая вводится так же, как и для группы $\mathfrak{I}$ (см. разд. 1). Для подгрупп Γ в $\tilde{\mathfrak{I}}$ мы обозначаем $\Gamma_k = \tilde{\mathfrak{I}}_k \bigcap \Gamma$, $k \leq 1$.

Пусть $g \in \mathrm{C}((z^{-1}))$, $ord_\infty\, g < 0$. Обозначим через $\mathrm{C}((g^{-1}))$ образ поля $\mathrm{C}((z^{-1}))$ при непрерывном вложении в себя над C, когда $z \to g$. Это замкнутое подполе в $\mathrm{C}((z^{-1}))$. Можно показать, что любое замкнутое подполе F в $\mathrm{C}((z^{-1}))$, отличное от C, имеет такой вид. Ясно, что если $G \in \tilde{\tilde{\mathfrak{I}}}$ подгруппа, то ее неподвижное поле $\mathrm{C}((z^{-1}))^G$ замкнуто в $\mathrm{C}((z^{-1}))$.

Лемма 2.1.

1) *Пусть* $g \in \mathrm{C}((z^{-1}))$, $ord_\infty\, g = -n$, $n \in \mathrm{N}$. *Тогда* $\mathrm{C}((g^{-1})) \subset \mathrm{C}((z^{-1}))$ — *циклическое расширение Галуа степени* n, $Gal\left(\mathrm{C}((z^{-1}))/\mathrm{C}((g^{-1}))\right)$ — *подгруппа всех автоморфизмов из* $\tilde{\tilde{\mathfrak{I}}}$, *оставляющих* $\mathrm{C}((g^{-1}))$ *на месте.*

2) *Пусть* $G \subset \tilde{\tilde{\mathfrak{I}}}$ *подгруппа из* n *элементов. Тогда* $\mathrm{C}((z^{-1}))^G = \mathrm{C}((g^{-1}))$ *для некоторого* $g \in \mathrm{C}((z^{-1}))$, $ord_\infty\, g = -n$, G *сопряжением в* $\tilde{\tilde{\mathfrak{I}}}$ *приводится к виду* $\left\{h \in \tilde{\tilde{\mathfrak{I}}} \;\middle|\; h(z) = \varepsilon z,\ \varepsilon^n = 1\right\}$.

Доказательство.

1) Если $ord_\infty\, g = -n$, то в поле $\mathrm{C}((z^{-1}))$ извлекается корень n-ой степени из g. Отсюда, как и в предложении 2.1, заключаем, что $\left\{h \in \tilde{\mathfrak{I}} \;\middle|\; g \circ h = g\right\}$ — циклическая группа из n элементов, ее неподвижное поле есть $\mathrm{C}((g^{-1}))$, сопряжением в $\tilde{\mathfrak{I}}$ она приводится к виду $\left\{\varepsilon z, \;\middle|\; \varepsilon^n = 1\right\}$. Теперь по теореме Артина ([5], теор. 2, с. 221) получаем искомое.

2) Положим $g = \prod\limits_{h \in G} h(z)$, произведение берется в поле $\mathrm{C}((z^{-1}))$. Тогда $ord_\infty\, g = -n$, $g \in \mathrm{C}((z^{-1}))^G$. В силу пункта 1) имеем $\mathrm{C}((g^{-1})) = \mathrm{C}((z^{-1}))^G$, G циклична. ◇

Замечание. Пусть $p \in \mathrm{C}[z]\backslash\mathrm{C}$. Если $p \circ g = p$ для некоторого $g \in \tilde{\mathfrak{I}}$, то $g \in \mathfrak{I}$, т. е. $g \in T_p$. Можно сказать, что $T_p = Gal\left(\mathrm{C}((z^{-1}))/\mathrm{C}((p^{-1}))\right)$. Отметим особо, что по группе T_p восстанавливается поле $\mathrm{C}(p) = \mathrm{C}(z) \bigcap \mathrm{C}((z^{-1}))^{T_p}$.

По теореме Люрота любое поле F такое, что $\mathrm{C} \subset F \subset \mathrm{C}(z)$ имеет вид $\mathrm{C}(R)$, $R \in \mathrm{C}(z)$. Пусть $p \in \mathrm{C}[z]\backslash\mathrm{C}$ и пусть поле F таково, что $\mathrm{C}(p) \subset F \subset \mathrm{C}(z)$. Легко видеть, что найдется $r \in \mathrm{C}[z]$, для которого $F = \mathrm{C}(r)$. Полином r является правым фактором p.

Как и в теории Галуа конечных алгебраических расширений, стандартным образом доказывается следующее предложение.

Предложение 2.2. *Пусть* $p, q \in \mathrm{C}[z]\backslash\mathrm{C}$. *Пусть* $h \in \mathrm{C}[z]$ *таков, что* $\mathrm{C}(p,q) = \mathrm{C}(h)$. *Тогда* $T_h = T_p \bigcap T_q$.

Основной целью этого раздела является доказательство следующей теоремы.

Теорема 2.1. *Пусть $p,\ q \in \mathbb{C}[z]\setminus\mathbb{C}$. Пусть $G \subset \mathfrak{T}$ — подгруппа, порожденная T_p и T_q, $G_1 = G\bigcap \mathfrak{T}_1$. Имеется альтернатива:*
1) $G_1 = 0$, 2) $G_1 \neq 0$.
В случае 1) *имеем* $\mathbb{C}(p)\bigcap\mathbb{C}(q) = \mathbb{C}(h)$, *где* $h \in \mathbb{C}[z]$, $\deg h = HOK(\deg p, \deg q)$.
В случае 2) *имеем* $\mathbb{C}(p)\bigcap\mathbb{C}(q) = \mathbb{C}$.

Доказательство.

1) Если бы $\mathbb{C}(p)\bigcap\mathbb{C}(q) \neq \mathbb{C}$, то по следствию 2 из предложения 2.1 мы бы имели конечность G, что противоречит условию $G_1 \neq 0$.

2) Легко видеть, что $\#G = d$, где $d = HOK(\deg p, \deg q)$. В силу леммы 2.2 имеем $\mathbb{C}((z^{-1}))^G = \mathbb{C}((g^{-1}))$, где $g \in \mathbb{C}((z^{-1}))$, $ord_\infty g = -d$. Поскольку $g \in \mathbb{C}((p^{-1}))$, то $g = \tilde{g}(p)$, $\tilde{g} \in \mathbb{C}((z^{-1}))$. Аналогично $g = \hat{g}(q)$, $\hat{g} \in \mathbb{C}((z^{-1}))$.

Вообще, для $h = \sum\limits_{k \le m} a_k z^k$ положим $h_+ = \sum\limits_{0 \le k \le m} a_k z^k$. Если p — полином, то легко видеть, что $h(p)_+ = h_+(p)$. Применим эту процедуру к равенству $\tilde{g}(p) = \hat{g}(q)$. Получим $\tilde{q}_+(p) = \hat{q}_+(q) = h$, где $h \in \mathbb{C}[z]$, $\deg h = d$, $h \in \mathbb{C}(p)\bigcap\mathbb{C}(q)$. Если бы $\mathbb{C}(h) \neq \mathbb{C}(p)\bigcap\mathbb{C}(q)$, то $\mathbb{C}(p)\bigcap\mathbb{C}(q) = \mathbb{C}(h_1)$, где $h_1 \in \mathbb{C}[z]$, $\deg h_1 < \deg h = ord_\infty g^{-1}$. Это невозможно, т. к. $h_1 \in \mathbb{C}((g^{-1}))$. Итак, $\mathbb{C}(p)\bigcap\mathbb{C}(q) = \mathbb{C}(h)$. ◊

Замечание 1. Пусть $p,\ q \in \mathbb{C}[z]\setminus\mathbb{C}$, пусть h_p, h_q — образующие групп T_p и T_q соответственно. Случай 1) теоремы 2.1 эквивалентен тому, что h_p и h_q коммутируют.

Доказательство.

Если h_p и h_q коммутируют, то $G = \{\sigma \circ \tau \mid \sigma \in T_p,\ \tau \in T_q\}$ является группой. Поскольку $\#G < \infty$, то $G_1 = 0$. Обратное очевидно. ◊

Замечание 2. Теорема 2.1 дает также алгоритм, позволяющий по заданным $p,\ q \in \mathbb{C}[z]$ находить $\mathbb{C}(p)\bigcap\mathbb{C}(q)$. Достаточно решить линейную систему, соответствующую уравнению $h = f \circ p = g \circ q$, $\deg h = HOK(\deg p, \deg q)$.

Замечание 3. Тот факт, что если $\mathbb{C}(p)\bigcap\mathbb{C}(q) \neq \mathbb{C}$, то $\mathbb{C}(p)\bigcap\mathbb{C}(q) = \mathbb{C}(h)$ для некоторого $h \in \mathbb{C}[z]$, $\deg h = HOK(\deg p, \deg q)$, можно было доказать также, используя идеи Ритта (см. [6]).

Можно доказать, что для $h_1,\ h_2 \in \mathbb{C}[z]$ условие $\mathbb{C}(h_1) \subset \mathbb{C}(h_2)$ равносильно тому, что $T_{h_2} \subset T_{h_1}$.

Для доказательства предложения 0.1 мы воспользуемся следующим утверждением, доказанным в [6].

Предложение 2.3. *Пусть* $p \in \mathbf{C}[z]\backslash\mathbf{C}$, F_i — *поля* $(i = 1,2)$ *такие, что* $\mathbf{C}(p) \subset F_i \subset \mathbf{C}(z)$ *для* $i = 1,2$. *Если* $[\mathbf{C}(z): F_1] = [\mathbf{C}(z): F_2]$, *то* $F_1 = F_2$.

Отсюда вытекает первая часть предложения 0.1.

Доказательство второй части предложения 0.1. $p(z) = z^n$, $q \in \mathbf{C}[z]\backslash\mathbf{C}$. Пусть $\mathbf{C}(p)\bigcap\mathbf{C}(q) \neq \mathbf{C}$ и $h \in \mathbf{C}[z]$ таков, что $\mathbf{C}(p)\bigcap\mathbf{C}(q) = \mathbf{C}(h)$. Обозначим через $G = Gal(\mathbf{C}(z)/\mathbf{C}(p))$. Если $\sigma \in G$, то $\sigma(z) = \varepsilon z$, где $\varepsilon^n = 1$. Имеем для всякого $\sigma \in G$: $\mathbf{C}(h) \subset \mathbf{C}(\sigma q) \subset \mathbf{C}(z)$, $[\mathbf{C}(z) : \mathbf{C}(\sigma q)] = [\mathbf{C}(z) : \mathbf{C}(q)]$. В силу предложения 2.3 получаем $\mathbf{C}(\sigma q) = \mathbf{C}(q)$ для всех $\sigma \in G$. Отсюда следует, что q имеет требуемый вид.

Обратно, пусть $q(z) = z^\lambda \tilde{q}(z^n)$, $0 \leq \lambda < n$, $p(z) = z^n$. Положим $v(z) = z^\lambda\, \tilde{q}(z)^n$. Тогда $p \circ q = v \circ p$. Отсюда $\mathbf{C}(p \circ q) \subset \mathbf{C}(p)\bigcap\mathbf{C}(q)$. ◇

3. Подготовка к решению задачи 3

Задача 3 была сформулирована во Введении.

Лемма 3.1. *Пусть* $\sigma, \tau \in \mathfrak{I}$, $g \in \mathbf{C}((z^{-1}))$, $ord_\infty g = -n$, $n \in \mathbf{N}$. *Пусть* $\sigma = \alpha z + \ldots$, $\tau = \beta z + \ldots$ *и пусть*

$$g \circ \sigma = \tau \circ g. \tag{3.1}$$

Тогда $\beta = \alpha^n$. *Если вдобавок* $\alpha = 1$ *(т. е.* $\sigma \in \mathfrak{I}_1$*),* $\sigma \neq z$, *то найдется* $k \in \mathbf{N}$ *такое, что* $\sigma = z + az^{1-nk} + \ldots$, $a \in \mathbf{C}^*$, $\tau = z + bz^{1-k} + \ldots$. *При этом* $b = Ca$, *где* $C \in \mathbf{C}^*$ *зависит только от* g *и* k, *но не от* a.

Доказательство. Найдутся $\mu, \xi \in \mathfrak{I}$ такие, что $\mu \circ g_n \circ \xi = g$, где $g_n = z^n$. Теперь (3.1) можно переписать так $g_n \circ (\xi\sigma\xi^{-1}) = (\mu^{-1}\tau\mu) \circ g_n$ и тем самым свести доказательство к тривиальному частному случаю $g = g_n$. ◇

Предложение 3.1. *Пусть* $p, q, h \in \mathbf{C}[z]\backslash\mathbf{C}$. *Группы* T_p, T_q *порождают формально дискретную подгруппу в* $\mathfrak{I}$ *тогда и только тогда, когда* $T_{p\circ h}$ *и* $T_{q\circ h}$ *обладают этим свойством.*

Доказательство. Рассмотрим следующую диаграмму. Все участвующие расширения полей — Галуа.

Имеем $T_h \subset T_{p\circ h}$, $T_h \subset T_{q\circ h}$. Пусть G — группа, порожденная $T_{p\circ h}$ и $T_{q\circ h}$, G' — порожденная T_p и T_q. Можно считать, что $T_p = Gal\left(\mathbf{C}((h^{-1}))/\mathbf{C}(((p\circ h)^{-1}))\right)$, $T_q = Gal\left(\mathbf{C}((h^{-1}))/\mathbf{C}(((q\circ h)^{-1}))\right)$. Тогда $G \subset Aut\mathbf{C}((z^{-1}))$, $G' \subset Aut\mathbf{C}((h^{-1}))$. Из теории конечных расширений Галуа известно, что отображение сужения $T_{p\circ h} \ni \tau \to \tau\,\big|_{\mathbf{C}((h^{-1}))} \in T_p$ индуцирует эпиморфизм: $T_{p\circ h} \to T_p$ с ядром T_h. Аналогично, сужение элементов $T_{q\circ h}$ на $\mathbf{C}((h^{-1}))$ дает эпиморфизм $T_{q\circ h} \to T_q$ с ядром T_h.

$$\begin{tikzcd}[column sep=small]
 & \mathbb{C}((\frac{1}{z})) \arrow[d, no head] & \\
 & \mathbb{C}((\frac{1}{h})) \arrow[dl, no head] \arrow[dr, no head] & \\
\mathbb{C}((\frac{1}{p\circ h})) & & \mathbb{C}((\frac{1}{q\circ h}))
\end{tikzcd}$$

Рис. 1

Поэтому сужение μ: $G \ni \tau \to \tau \,\big|_{\mathbb{C}((h^{-1}))} \in G'$ индуцирует гомоморфизм G на G'. Ясно, что $Ker\,\mu = T_h$. Учитывая лемму 3.1, легко видеть, что сужая μ на G_1, получим изоморфизм $\mu\,\big|_{G_1} : G_1 \to G'_1$. В самом деле, если считать, что $G, G' \subset \mathfrak{I}$, то для всякого $\sigma \in G$ найдется единственный $\tau \in G'$ такой, что $h\circ\sigma = \tau\circ h$. Отображение μ переводит σ в τ. Из леммы 3.1 теперь следует искомое. В случае формальной дискретности решетки в C, соответствующие группам G_1 и G'_1, будут подобны (отличаются умножением на число). ◇

Доказанное предложение — это формальный аналог замечания 0.1. Мы можем теперь решать задачу 3 в предположении $\mathbb{C}(p,q) = \mathbb{C}(z)$. В силу предложения 2.2 это условие равносильно тому, что $T_p \cap T_q = 1$.

В дальнейшем в этом разделе будем предполагать, что $p, q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p) \cap \mathbb{C}(q) = \mathbb{C}$.

Пусть $\deg p = n$, $\deg q = m$. Пусть $h_p = \varepsilon z + \ldots$, $h_q = \delta z + \ldots$ — образующие групп T_p и T_q соответственно; ε — первообразный корень из 1 степени n, δ — степени m. В силу замечания 1 к теореме 2.1 h_p и h_q не коммутируют. Пусть

$$h_q^{-1} h_p^{-1} h_q h_p = z + \theta z^{-k} + \ldots, \quad \theta \neq 0, \quad k \geq 0. \tag{3.2}$$

Лемма 3.2. $\varepsilon^{k+1} \neq 1$, $\delta^{k+1} \neq 1$.

Доказательство. Число k зависит только от группы G, порожденной T_p и T_q в $\mathfrak{I}$, и не меняется при сопряжении в $\mathfrak{I}$. В силу предложения 2.1 найдется $\sigma \in \mathfrak{I}$ такой, что $\alpha = \sigma^{-1} \circ h_p \circ \sigma = \varepsilon z$. Положим $\beta = \sigma^{-1} \circ h_q \circ \sigma = \delta z + c_0 + c_{-1} z^{-1} + \ldots$. Имеем

$$\alpha\circ\beta = \varepsilon\delta z + \varepsilon c_0 + \varepsilon c_{-1} z^{-1} + \ldots;$$

$$\beta\circ\alpha = \varepsilon\delta z + c_0 + c_{-1}\varepsilon^{-1} z^{-1} + \ldots.$$

Число k определяется из того, что $\alpha \circ \beta$ и $\beta \circ \alpha$ впервые отличаются при z^{-k}. Поэтому $\varepsilon c_{-k} \neq \varepsilon^{-k} c_{-k}$, откуда $\varepsilon^{k+1} \neq 1$. Аналогично $\delta^{k+1} \neq 1$. ◇

Замечание 3.1.
1) Если $h = z + cz^{-k} + \ldots$, $\tau = bz + \ldots$; $h, \tau \in \mathfrak{I}$, то $\tau^{-1} h \tau = z + cb^{-1-k} z^{-k} + \ldots$.
2) Пусть $h_i = z + c_i z^{-k} + \ldots$, $(i = 1,2)$. Тогда $h_1 h_2 = z + (c_1 + c_2) z^{-k} + \ldots$.

Отметим, что ε^{k+1} — первообразный корень из 1 степени $n/НОД(n, k+1)$, δ^{k+1} — степени $m/НОД(m, k+1)$.

Предложение 3.2. *Пусть T_p и T_q порождают формально дискретную подгруппу Γ в $\mathfrak{I}$. Тогда $n/НОД(n, k+1)$, $m/НОД(m, k+1)$ и их наименьшее общее кратное* $\in \{2,3,4,6\}$.

Доказательство. Поскольку имеет место формула (3.2), то $\Gamma_{1-k}/\Gamma_{-k} \neq 0$. Γ_{1-k}/Γ_{-k} — это решетка в $\mathbf{C}$. В силу пункта 1) замечания 3.1 она выдерживает повороты $z \to \varepsilon^{k+1} z$, $z \to \delta^{k+1} z$. Вспоминая, что $\varepsilon^{k+1} \neq 1$, $\delta^{k+1} \neq 1$, получаем требуемое. ◇

4. Случай одинаковых степеней

Для доказательства теоремы 0.1 достаточно доказать следующее предложение.

Предложение 4.1. *Пусть $p, q \in \mathbf{C}[z] \backslash \mathbf{C}$, $\mathbf{C}(p,q) = \mathbf{C}(z)$, $\mathbf{C}(p) \cap \mathbf{C}(q) = \mathbf{C}$, $\deg p = \deg q = n$, T_p и T_q порождают формально дискретную группу Γ. Тогда после линейных замен $p(z) = z^n$, $q(z) = (z+1)^n$, $n \in \{2,3,4,6\}$.*

Настоящий раздел мы посвятим доказательству этого предложения.

Пусть p, q удовлетворяют условиям предложения 4.1. Пусть, как и выше, $h_p = \varepsilon z + \ldots$, $h_q = \varepsilon z + \ldots$ — образующие групп T_p и T_q соответственно, ε — первообразный корень из 1 степени n, $h_q^{-1} h_p^{-1} h_q h_p = z + \tilde{\theta} z^{-k} + \ldots$, $\tilde{\theta} \neq 0$. Имеем $h_q^{-1} h_p = z + \ldots$, $h_q^{-1} h_p \neq z$, т. к. $T_q \cap T_p = 1$ (см. замечание к предложению 3.1). Значит, в силу формальной дискретности $h_q^{-1} h_p = z + \theta z^{-k} + \ldots$, $\theta \neq 0$. В силу леммы 3.2 имеем $\varepsilon^{k+1} \neq 1$.

Лемма 4.1. *Для всех $j \in \mathbf{Z}$ имеем $h_q^{-1} h_p = z + \lambda_j z^{-k} + \ldots$, где*

$$\lambda_j = \theta \frac{1 - \varepsilon^{-j(k+1)}}{1 - \varepsilon^{-(k+1)}}.$$

Доказательство. Покажем, что для всех $j, t \in \mathbf{Z}$:

$$\lambda_j \varepsilon^{-t(k+1)} = \lambda_{t+j} - \lambda_t.$$

Отсюда непосредственно будет следовать искомая формула. Имеем

$$h_p^{-t}(h_q^{-j}h_p^j)h_p^t = (h_p^{-t}h_q^t)(h_q^{-t-j}h_p^{t+j}).$$

Чтобы вывести из последней формулы предпоследнюю, достаточно воспользоваться замечанием 3.1. ◇

Лемма 4.2. *НОД*$(k+1, n) = 1$, *т.е.* ε^{k+1} *— первообразный корень из* 1 *степени* n.

Доказательство.

Пусть $l \in \mathbf{Z}$, $l(k+1) \equiv 0 \bmod n$, тогда $h_q^{-l}h_p^l = z + \lambda_l z^{-k} + \ldots$, $\lambda_l = 0$ в силу леммы 4.1. Теперь $h_q^l = h_p^l$ из-за формальной дискретности. Вспоминая, что $T_p \cap T_q = 1$, получаем $l \equiv 0 \bmod n$. Значит, $k+1$ обратимо в кольце $\mathbf{Z}/n\mathbf{Z}$. ◇

Следствие. $n \in \{2,3,4,6\}$.

Доказательство. Применить предложение 3.2 к паре p, q. ◇

Итак, доказательство предложения 4.1 свелось к случаю "маленьких степеней".

Случай $n = 2$ особенно простой. Группа Γ, порожденная T_p и T_q, состоит из линейных преобразований, $\Gamma_1 \simeq \mathbf{Z}$. После линейных замен будем иметь $p(z) = z^2$, $q(z) = (z+1)^2$.

По условию предложения 4.1 группа Γ_1 абелева (см. замечание к теореме 1.1). Пусть $j, l \in \mathbf{Z}$; $j, l, j-l \not\equiv 0 \bmod n$. Условие коммутации $h_p^{-j}h_q^j$ и $h_p^{-l}h_q^l$ дает $h_p^{l-j}h_q^jh_p^{-l} = h_q^lh_p^{-j}h_q^{j-l}$. Легко видеть, что так получаются все соотношения вида

$$h_p^{l_1}\,h_q^{l_2}\,h_p^{l_3} = h_q^{-l_3}\,h_p^{-l_2}\,h_q^{-l_1}, \tag{4.1}$$

где (l_1, l_2, l_3) пробегают такие тройки, что $l_i \not\equiv 0 \bmod n$, $l_1 + l_2 + l_3 \equiv 0 \bmod n$.

Идея состоит в том, чтобы аналитически продолжать равенства вида (4.1) вдоль петель с началом (=концом) в точке ∞. При этом мы смотрим на $h_p^{l_1}\,h_q^{l_2}\,h_p^{l_3}$ как на элемент алгебраической функции в точке ∞. При таком продолжении могут получиться соотношения вида

$$h_p^{l_1}\,h_q^{l_2}\,h_p^{l_3} = h_q^{k_1}\,h_p^{k}\,h_q^{k_3} \tag{4.2}$$

где $l_i, k_i \not\equiv 0 \bmod n$ $(i = 1, 2, 3)$. Будем смотреть на соотношение (4.2) как на уравнение, в котором неизвестными являются $k_i, l_i \in \mathbf{Z}/n\mathbf{Z}$; $k_i, l_i \not\equiv 0 \bmod n$ $(i = 1, 2, 3)$.

Лемма 4.3. *Система* (4.2) *эквивалентна системе* (4.3), *где*

$$\begin{cases} \varepsilon^{l_1 + l_2 + l_3} = \varepsilon^{k_1 + k_2 + k_3} \\ \varepsilon^{l_1}(1 - \varepsilon^{l_2}) = \varepsilon^{k_1 + k_2}(1 - \varepsilon^{k_3}) + 1 - \varepsilon^{k_1}. \end{cases} \tag{4.3}$$

Доказательство. Пусть после сопряжения в $\mathfrak{I}$ h_p и h_q перейдут соответственно в $\alpha_p = \varepsilon z$, $\alpha_q = \varepsilon z + cz^{-k} + \ldots$, $c \neq 0$. Имеем для всякого $s \in \mathbf{Z}$:

$$\alpha_q^s = \varepsilon^s z + \frac{c}{\varepsilon^{(s-1)k}} \frac{1-\varepsilon^{s(k+1)}}{1-\varepsilon^{k+1}} \frac{1}{z^k} + \dots .$$

Теперь приравняв коэффициенты при z и z^{-k} в соотношении $\alpha_p^{l_1}\alpha_q^{l_2}\alpha_p^{l_3} = \alpha_q^{k_1}\alpha_p^{k_2}\alpha_q^{k_3}$, получим

$$\begin{cases} \varepsilon^{l_1+l_2+l_3} = \varepsilon^{k_1+k_2+k_3} & (4.4a) \\ \dfrac{\varepsilon^{l_1}(1-\varepsilon^{l_2(k+1)})}{\varepsilon^{(l_2+l_3-1)k}} = \dfrac{\varepsilon^{k_1+k_2}}{\varepsilon^{(k_3-1)k}}(1-\varepsilon^{k_3(k+1)}) + \dfrac{1-\varepsilon^{k_1(k+1)}}{\varepsilon^{(k_1+k_2+k_3-1)k}}. & (4.4b) \end{cases}$$

Система (4.4a), (4.4b) эквивалентна (4.2) в силу формальной дискретности Г. С помощью (4.4a) преобразуем (4.4b) к виду

$$\varepsilon^{l_1(k+1)}(1-\varepsilon^{l_2(k+1)}) = \varepsilon^{(k_1+k_2)(k+1)}(1-\varepsilon^{k_3(k+1)}) + 1 - \varepsilon^{k_1(k+1)}.$$

Так как ε^{k+1} — первообразный корень из 1 степени n, то найдется автоморфизм $\overline{\mathrm{Q}}$, переводящий ε^{k+1} в ε. Применив его к последнему равенству, придем к системе (4.3). ◇

Лемма 4.4. *Пусть $n \geq 3$, простое. Тогда любое решение системы* (4.3) *имеет вид* (4.1), *т. е.* $l_1 \equiv -k_3$, $k_1 \equiv -l_3$, $k_2 \equiv -l_2$, $l_1 + l_2 + l_3 \equiv 0 \bmod n$.

Д о к а з а т е л ь с т в о. Второе уравнение в (4.3) приводится к виду $m_1 + m_2\varepsilon + \dots + m_n\varepsilon^{n-1} = 0$, где $m_i \in \mathbf{Z}$, $m_1 + m_2 + \dots + m_n = 0$. Поскольку n просто, то неприводимый многочлен числа ε над Q равен $x^{n-1} + x^{n-2} + \dots + 1$. Поэтому $m_1 = \dots = m_n = 0$. Отсюда

$$\begin{cases} \varepsilon^{k_1+k_2+k_3} = 1 \\ \varepsilon^{l_1} = \varepsilon^{k_1+k_2} \\ \varepsilon^{k_1} = \varepsilon^{l_1+l_2}. \end{cases}$$

С учетом первого из уравнений (4.3) получаем $l_1 \equiv -k_3$, $k_1 \equiv -l_3$, $k_2 \equiv -l_2$, $l_1 + l_2 + l_3 \equiv 0 \bmod n$, что и требовалось доказать. ◇

Теперь мы можем рассмотреть случай $n = 3$. В силу леммы 4.4 среди соотношений вида (4.2) имеются ровно два:

$$h_p h_q h_p = h_q^2 h_p^2 h_q^2, \tag{4.5}$$

$$h_p^2 h_q^2 h_p^2 = h_q h_p h_q . \tag{4.6}$$

На множестве из этих двух равенств действует группа $\pi_1(\overline{\mathrm{C}} \backslash S, \infty)$, где $\overline{\mathrm{C}}$ — сфера Римана, а $S \subset \mathrm{C}$ конечно (появление S связано с тем, что равенства (4.5), (4.6) можно аналитически продолжать не вдоль любой петли). Отметим, что ∞ не является точкой ветвления для участвующих здесь (и в дальнейшем) алгебраических функций.

Пусть z_0 — точка ветвления для h_p, но не для h_q. Тогда найдется $\gamma \in \pi_1(\overline{\mathbb{C}}\setminus S, \infty)$ такая, что h_p продолжается вдоль γ до h_p^2, h_q продолжается до h_q, а тогда h_q^2 — до h_q^2. Продолжая (4.5) вдоль γ, приходим к противоречию. Значит, z_0 — точка ветвления для h_q. Аналогично, каждая точка ветвления h_q служит точкой ветвления h_p.

Лемма 4.5. *Пусть $p(z) = z^3 + az^2 + bz$.*

1) *Если $p'(z)$ имеет кратный корень, то h_p линейно и не имеет точек ветвления;*

2) *Если корни $p'(z)$ разные, то h_p имеет две точки ветвления, которые являются корнями уравнения*

$$\frac{3}{4}z^2 + \frac{az}{2} + \left(b - \frac{a^2}{4}\right) = 0. \tag{4.7}$$

В частности, по точкам ветвления h_p восстанавливаются коэффициенты a и b, т. е. полином p.

Из этой леммы заключаем, что если h_p и h_q имеют точки ветвления, то $C(p) = C(q)$, противоречие. Поэтому h_p и h_q линейны. После линейных замен $p(z) = z^3$, $q(z) = (z+1)^3$. В случае $n = 3$ предложение 4.1 доказано.

Случай четного n

В этом случае вместо соотношений (4.2) мы найдем все соотношения вида

$$h_q^{l_1} h_p^{l_2} = h_p^{k_1} h_q^{k_2}, \tag{4.8}$$

где k_i, $l_i \not\equiv 0 \bmod n$.

Лемма 4.6. *Система (4.8) эквивалентна системе (4.9), где*

$$\begin{cases} \varepsilon^{l_1 + l_2} = \varepsilon^{k_1 + k_2} \\ 1 - \varepsilon^{l_1} = \varepsilon^{k_1}(1 - \varepsilon^{k_2}). \end{cases} \tag{4.9}$$

В качестве неизвестных рассматриваются k_i, $l_i \in \mathbf{Z}/n\mathbf{Z}$, k_i, $l_i \not\equiv 0 \bmod n$.

Доказательство этой леммы вполне аналогично доказательству леммы 4.3, и мы его опускаем.

Лемма 4.7. *Любое соотношение (4.8) имеет вид*

$$h_q^l h_p^{-l+n/2} = h_p^{l+n/2} h_q^{-l}, \tag{4.10}$$

где $l \in \mathbf{Z}$, $2l \not\equiv 0 \bmod n$.

Доказательство. Решая систему (4.9), будем иметь $|1 - \varepsilon^{l_1}| = |1 - \varepsilon^{k_2}|$. Поскольку $\varepsilon^{k_1} \neq 1$, то $l_1 \not\equiv k_2 \bmod n$. Отсюда $l_1 + k_2 \equiv 0 \bmod n$. Отсюда $\varepsilon^{k_1} = \varepsilon^{l_1}$. Учитывая, что $\varepsilon^{n/2} = -1$, получаем $k_1 - l_1 \equiv n/2 \bmod n$ и т.д. ◇

Лемма 4.8. $h_p^{n/2}(z) = \alpha - z$, $h_q^{n/2}(z) = \beta - z$, *где* $\alpha, \beta \in \mathbb{C}$, $\alpha \neq \beta$.

Доказательство. На множестве соотношений вида (4.10) действует группа $\pi_1(\overline{\mathbb{C}}\backslash S, \infty)$, где $S \subset \mathbb{C}$ конечно (см. случай $n = 3$). Среди $h_p, \ldots, h_p^{n-1}$ в соотношениях (4.10) участвуют все, кроме $h_p^{n/2}$. Поэтому при аналитическом продолжении вдоль любого пути $h_p^{n/2}$ не может перейти в h_p^j, $j \neq n/2$. Это значит, что $h_p^{n/2}$ аналитически продолжается до однозначной алгебраической функции, т.е. $h_p^{n/2} \in \mathbb{C}(z)$. Так как $h_p^n = id$, $h_p^{n/2}(\infty) = \infty$, то $h_p^{n/2}(z) = \alpha - z$ для некоторого $\alpha \in \mathbb{C}$. Аналогично $h_q^{n/2}(z) = \beta - z, \beta \in \mathbb{C}$; $\beta \neq \alpha$, поскольку $T_p \bigcap T_q = 1$. ◇

В силу леммы 4.8 в группе Γ_1 имеется элемент $h = h_p^{-n/2} h_q^{n/2}$, $h(z) = z + c$, $c \neq 0$. Γ_1 абелева, а централизатором h в $\mathfrak{I}_1$ является однопараметрическая группа всех сдвигов $\{ z + t \mid t \in \mathbb{C} \}$. Поэтому Γ_1 состоит из линейных преобразований. Если $g = \alpha z + \ldots \in \Gamma$, то $g^{-1} h g = z + c/\alpha$. Отсюда легко следует линейность g. Итак, h_p и h_q линейны и, следовательно, $p(z) = a(z - z_0)^n + b$, $q(z) = c(z - z_1)^n + d$, $z_0 \neq z_1$. Теперь предложение 4.1 и теорема 0.1 полностью доказаны.

Следствие из теоремы 0.1 получается, если сопоставить теорему 0.1 и следствие из предложения 1.4.

5. Случай $p(z) = z^n$

В этом разделе мы доказываем теорему 0.2 и следствие из нее, сформулированное во Введении.

При решении задачи 3 важную роль играет следующая лемма.

Лемма 5.1. *Пусть* $p, q \in \mathbb{C}[z]\backslash\mathbb{C}$. *Обозначим* $H_{q,p} = \{ \sigma \in T_q \mid \sigma \circ \tau = \tau \circ \sigma$ *для всех* $\tau \in T_p \}$. *Пусть* $H_{q,p}$ *соответствует правому фактору* q, *т.е.* $H_{q,p} = T_r$, $q = \tilde{q} \circ r$; $r, \tilde{q} \in \mathbb{C}[z]$. *Тогда*

1) $\mathbb{C}(p) \bigcap \mathbb{C}(r) \neq \mathbb{C}$ *и найдутся* $g, \tilde{p} \in \mathbb{C}[z]$ *такие, что* $g = \tilde{p} \circ r$, $\mathbb{C}(p) \bigcap \mathbb{C}(r) = \mathbb{C}(g)$;

2) T_p *и* T_q *порождают форально дискретную группу тогда и только тогда, когда* $T_{\tilde{p}}$ *и* $T_{\tilde{q}}$ *обладают этим свойством.*

Доказательство. Элементы группы T_r коммутируют с элементами T_p. Отсюда в силу теоремы 2.1 получаем 1). T_p и T_r порождают T_g, а $T_r \subset T_q$. Поэтому группа, порожденная T_p и T_q совпадает с группой, порожденной T_g и T_q. Применяя предложение 3.1 к тройке $\tilde{p}, \tilde{q}, r$, получаем утверждение 2). ◇

Специфика случая $p(z) = z^n$ заключается в том, что группа T_p состоит из линейных преобразований (а расширение $\mathbb{C}(z)/\mathbb{C}(p)$ является расширением Галуа). Следующая лемма утверждает, что в этом случае выполнено условие леммы 5.1. (Это условие выполнено для любых p и q, но в настоящей работе это более сильное утверждение не понадобится).

Лемма 5.2. *Пусть* $p(z) = z^n$, $q \in \mathbb{C}[z]\backslash\mathbb{C}$. *Пусть* h_p *— образующая группы* T_p. *Обозначим* $q_j = q \circ h_p^j$, $q_i \in \mathbb{C}[z]$. *Пусть* $r \in \mathbb{C}[z]$ *таков, что* $\mathbb{C}(r) = \mathbb{C}(q_1, q_2, \ldots, q_n)$. *Тогда* $H_{q,p} = T_r$, r *— правый фактор* q, T_p *переводит поле* $\mathbb{C}(r)$ *в себя.*

Доказательство. $q_n = q$, $\mathbb{C}(q) \subset \mathbb{C}(r)$. Поэтому r — правый фактор q. Обозначим $H = \bigcap_{j=1}^{n} T_{q_j}$. В силу предложения 2.2 $T_r = H$. $T_{q_j} = h_p^{-j} T_q h_p^j$. Ясно, что $H_{q,p} \subset H$. С другой стороны, $T_q \bigcap T_{q_1} \subset H_{q,p}$, т.к. если $h_q^s \in h_p^{-1} T_q h_p$, то $h_p h_q^s h_p^{-1} \in T_q$, но $h_p h_q^s h_p^{-1} = \delta^s z + \ldots$, где $h_q(z) = \delta z + \ldots$. Поэтому $h_p h_q^s h_p^{-1} = h_q^s$, т. е. $h_q^s \in H_{q,p}$. Итак $H_{q,p} = H$.

Поскольку $\{q_j\}_j$ — это T_p-орбита полинома q, то T_p переводит поле $\mathbb{C}(q_1, q_2, \ldots, q_n)$ в себя. ◇

Достаточность в теореме 0.2 вытекает из предложений 0.1 и 0.2, а также замечания 0.1, нужно только заметить, что в обозначениях теоремы 0.2 $\mathbb{C}(p \circ r) = \mathbb{C}(p) \bigcap \mathbb{C}(r)$, поскольку $НОД(\lambda, n) = 1$.

Необходимость в теореме 0.2 вытекает из следующего предложения.

Предложение 5.1. *Пусть* $p, q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p,q) = \mathbb{C}(z)$, $p(z) = z^n$, $\mathbb{C}(p) \bigcap \mathbb{C}(q) = \mathbb{C}$, T_p *и* T_q *порождают формально дискретную группу* Γ. *Тогда после внешней линейной замены* $q = \tilde{q} \circ r$, *где* $r(z) = z^\lambda \tilde{r}(z^n)$, $\tilde{r} \in \mathbb{C}[z]$, $0 < \lambda < n$, $НОД(\lambda, n) = 1$, $\tilde{q}(z) = (z + a)^m$, $a \neq 0$; $n, m, НОК(n,m) \in \{2,3,4,6\}$.

Доказательство. Применяя лемму 5.2, получаем факторизацию $q = \tilde{q} \circ r$, $\tilde{q}, r \in \mathbb{C}[z]$, T_p переводит $\mathbb{C}(r)$ в себя. Поэтому после внешней линейной замены r принимает вид $r(z) = z^\lambda \tilde{r}(z^n)$, $\tilde{r} \in \mathbb{C}[z]$, $0 \leq \lambda < n$. Поскольку $\mathbb{C}(r) \supset \mathbb{C}(q)$ и $\mathbb{C}(p,q) = \mathbb{C}(z)$, то $\mathbb{C}(p,r) = \mathbb{C}(z)$, т.е. $НОД(\lambda, n) = 1$, в частности, $\lambda \neq 0$. Ясно, что $\mathbb{C}(p \circ r) = \mathbb{C}(p) \bigcap \mathbb{C}(r)$. В силу леммы 5.1 T_p и $T_{\tilde{q}}$ порождают формально дискретную группу, которую мы обозначим через G. Легко видеть, что $\mathbb{C}(p) \bigcap \mathbb{C}(\tilde{q}) = \mathbb{C}$, $\mathbb{C}(p, \tilde{q}) = \mathbb{C}(z)$.

Покажем, что $H_{\tilde{q},p} = 1$. В силу леммы 5.2 имеется факторизация $\tilde{q} = v \circ \tilde{r}$, $v, \tilde{r} \in \mathbb{C}[z]$, $H_{\tilde{q},p} = T_{\tilde{r}}$. Тогда по теореме 2.1 $\mathbb{C}(\tilde{r}) \bigcap \mathbb{C}(p) \neq \mathbb{C}$. Отсюда $\mathbb{C}(\tilde{r} \circ r) \bigcap \mathbb{C}(p) \neq \mathbb{C}$. Поэтому $T_{\tilde{r} \circ r} \subset H_{q,p} = T_r$, т. е. $T_{\tilde{r} \circ r} = T_r$. Это значит, что $H_{\tilde{q},p} = 1$.

Рассмотрим теперь $\tilde{q}_1 = \tilde{q} \circ h_p$. Имеем $T_{\tilde{q}_1} = h_p^{-1} T_{\tilde{q}} h_p$. $T_{\tilde{q}}$ и $T_{\tilde{q}_1}$ порождают некоторую подгруппу G' в G. Поэтому G' формально дискретна. Элемент $h_p^{-1} h_{\tilde{q}} h_p h_{\tilde{q}}^{-1} \in G'$. Он не равен id, поскольку $H_{\tilde{q},p} = 1$, и лежит в $\mathfrak{I}_1$. Поэтому $\mathbb{C}(\tilde{q}) \bigcap \mathbb{C}(\tilde{q}_1) = \mathbb{C}$. Далее $T_{\tilde{q}} \bigcap T_{\tilde{q}_1} = 1$, поскольку $H_{\tilde{q},p} = 1$. Это означает, что $\mathbb{C}(\tilde{q}, \tilde{q}_1) = \mathbb{C}(z)$. Применяя предложение 4.1 к паре $\widetilde{q}, \widetilde{q}_1$, видим, что после внешней линейной замены $\widetilde{q}(z) = (z + a)^m$, $a \neq 0$ из-за того, что $\mathbb{C}(\widetilde{q}, \widetilde{q}_1) = \mathbb{C}(z)$.

Для пары $p(z) = z^n$, $\widetilde{q}(z) = (z + a)^m$ группа, порожденная T_p и $T_{\widetilde{q}}$, устроена понятным образом. Если она формально дискретна, то n, m, $НОК(n,m) \in \{2,3,4,6\}$. ◇

Следствие из теоремы 0.2 получается, если принять во внимание следствие из предложения 1.4.

6. Формулировка результата для произвольных p и q

Здесь мы формулируем теоремы, которые будут доказаны в отдельной статье.

Предложение 6.1. *Пусть $p, q \in \mathbb{C}[z]\backslash\mathbb{C}$. Тогда среди полей F таких, что $\mathbb{C}(q) \subset F \subset \mathbb{C}(z)$ и $F \cap \mathbb{C}(p) \neq \mathbb{C}$ имеется наименьшее по включению. Обозначим его $F_{q,p}$.*

О п р е д е л е н и е. Назовем пару многочленов p, $q \in \mathbb{C}[z]\backslash\mathbb{C}$ неприводимой, если $F_{q,p} = F_{p,q} = \mathbb{C}(z)$.

По каждой паре многочленов p, $q \in \mathbb{C}[z]\backslash\mathbb{C}$ канонически строится неприводимая пара следующим образом. Положим $F = F_{p,q} \cap F_{q,p}$, $F_1 = \mathbb{C}(p) \cap F_{q,p}$, $F_2 = \mathbb{C}(q) \cap F_{p,q}$.

$$\begin{tikzcd}[column sep=small]
 & & \mathbb{C}(z) \arrow[dl, dash] \arrow[dr, dash] & & \\
 & F_{p,q} \arrow[dl, dash] \arrow[dr, dash] & & F_{q,p} \arrow[dl, dash] \arrow[dr, dash] & \\
\mathbb{C}(p) \arrow[dr, dash] & & F \arrow[dl, dash] \arrow[dr, dash] & & \mathbb{C}(q) \arrow[dl, dash] \\
 & F_1 & & F_2 &
\end{tikzcd}$$

Рис. 2.

Существуют многочлены $r, \widetilde{p}, \widetilde{q} \in \mathbb{C}[z]\backslash\mathbb{C}$ такие, что $F = \mathbb{C}(r)$, $F_1 = \mathbb{C}(\widetilde{p} \circ r)$, $F_2 = \mathbb{C}(\widetilde{q} \circ r)$. Утверждается, что пара $\widetilde{p}$, $\widetilde{q}$ — неприводима.

Предложение 6.2. *Пусть p, $q \in \mathbb{C}[z]\backslash\mathbb{C}$, $\mathbb{C}(p) \cap \mathbb{C}(q) = \mathbb{C}$. Пусть $\widetilde{p}$, $\widetilde{q}$ — соответствующая неприводимая пара. Тогда p, q — решение задачи 1 тогда и только тогда, когда $\widetilde{p}$, $\widetilde{q}$ — решение этой же задачи. Утверждение останется в силе, если задачу 1 заменить на задачу 3.*

Предложение 6.3. *Пусть p, q — неприводимая пара, дающая решение задачи 3, причем $\mathbb{C}(p) \cap \mathbb{C}(q) = \mathbb{C}$. Тогда $p = \lambda \circ p_1 \circ r$, $q = \mu \circ q_1 \circ r$, где λ, μ, r — линейные функ-*

ции, $p_1(z) = z^n$, $q_1(z) = (z+1)^m$, *кроме того* n, m, $НОК(n,m) \in \{2,3,4,6\}$. *Обратно, каждая такая пара неприводима и дает решение задачи 3 и даже задачи* 1.

Таким образом, задачи 1 и 3 эквивалентны.

Список литературы

1. *Yu. S. Il'yashenko*, Nonlinear Stokes Phenomena.— Adv. Sov. Math. (1993), v. 14, p. 1–55.
2. *P. M. Elizarov, Yu. S. Il'yashenko, A. A. Shcherbakov, and S. M. Voronin*, Finitely generated groups of germs of one-dimensional conformal mappings, and invariants for complex singular points of analytic foliations of the complex plane. - Adv. Sov. Math., (1993), v. 14, p. 57–105.
3. *L. Flatto*, A Theorem on Level Curves of Harmonic Functions.— J. London Math. Soc. (1969), v. 1, p. 470–472.
4. F. Gross, Factorization of meromorphic functions and some open problems.— Lecture Notes in Math. (1977), v. 599, p. 51–67.
5. *С. Ленг*, Алгебра.— Мир, Москва (1968), 564 с.
6. *J. F. Ritt*, Prime and composite polynomials.— Trans. Amer. Math. Soc. (1922), v. 23, p. 51–66.
7. *L. J. Hansen and H. S. Shapiro*, Graphs and functional equations.— Ann. Acad. Sci. Fennic., Ser. A. I. Math. (1993), v. 18, p. 125–146.

On the functional equation $f(p(z)) = g(q(z))$, where f and g are meromorphic functions, and p, q — polynomials

S. A. Lysenko

Let f and g be meromorphic functions in a punctured neighbourhood of infinity in C, and let p and q be polynomials. In this paper the functional equation $f(p(z)) = g(q(z))$ is solved in two special cases: 1) $\deg p = \deg q$, 2) $p(z) = z^n$, q is an arbitrary polynomial.

Про функціональне рівняння $f(p(z)) = g(q(z))$, де f та g — мероморфні функції, а p та q — поліноми

С. А. Лисенко

Нехай f та g — мероморфні функції у проколюваній місцевості нескінченності в C, а p та q — поліноми. У цій статті розв'язується функціональне рівняння $f(p(z)) = g(q(z))$ у двох окремих випадках: 1) $\deg p = \deg q$, 2) $p(z) = z^n$, q — довільний поліном.