Записки научных
семинаров ПОМИ
Том 304, 2003 г.

**А. Шляпентох**

# ДИОФАНТОВА НЕРАЗРЕШИМОСТЬ ДЛЯ НЕКОТОРЫХ ФУНКЦИОНАЛЬНЫХ ПОЛЕЙ БЕСКОНЕЧНОЙ СТЕПЕНИ ТРАНСЦЕНДЕНТНОСТИ И ПОЛОЖИТЕЛЬНОЙ ХАРАКТЕРИСТИКИ

## 1. Введение

Интерес к задачам диофантовых представлений и диофантовой разрешимости восходит к вопросу, поставленному Гильбертом: существует ли унивесальный алгоритм, который по заданному полиномиальному уравнению от нескольких переменных над $\mathbb{Z}$ определяет, имеет ли данное уравнение решения в $\mathbb{Z}$? На этот вопрос, известный также как десятая проблема Гильберта, в работах М. Дейвиса, Х. Патнама, Дж. Робинсон и Ю. Матиясевича был дан отрицательный ответ (см. [6] и [7]). После установления этого результата аналогичные вопросы ставились для других полей и колец. Бесспорно, двумя наиболее интересными и сложными открытыми проблемами в этой области являются вопросы диофантовой разрешимости над $\mathbb{Q}$ и над кольцами алгебраических целых чисел произвольных числовых полей. Один из способов решения вопроса о диофантовой разрешимости над кольцом характеристики 0 состоит в построении диофантова представления множества $\mathbb{Z}$ над этим кольцом. Это понятие определяется далее.

**1.1. Определение.** Пусть $R$ – кольцо, а $A \subset R$. Мы говорим, что $A$ обладает диофантовым представлением над $R$, если существует такой многочлен $f(t, x_1, \dots, x_n) \in R[t, x_1, \dots, x_n]$, что для всякого $t \in R$ имеем

$$\exists x_1, \dots, x_n \in R, f(t, x_1, ..., x_n) = 0 \Longleftrightarrow t \in A.$$

При поддержке NSF (грант DMS-9988620).
Перевод с английского М. А. Всемирного.

Можно показать, что если поле частных кольца $R$ не является алгебраически замкнутым, то допустимы диофантовы представления состоящие из нескольких многочленов; при этом суть отношения не изменяется. (Дальнейшие подробности см. в [7].) В общем случае, если поле частных рассматриваемого кольца не является алгебраически замкнутым, то с точки зрения обсуждения диофантовых представлений и диофантовой разрешимости конечная система полиномиальных уравнений всегда эквивалентна одному полиномиальному уравнению. Другими словами, конечная система полиномиальных уравнений может быть эффективным образом заменена на единственное полиномиальное уравнение, которое имеет решения в рассматриваемом кольце тогда и только тогда, когда разрешима и исходная система.

Были получены диофантовы представления множества $\mathbb{Z}$ над некоторыми подкольцами следующих числовых полей: вполне вещественных расширений поля $\mathbb{Q}$, их вполне комплексных расширений степени 2, полей с ровно одной парой сопряженных комплексных вложений, некоторых полей степени 4 и некоторых вполне вещественных бесконечных расширений поля $\mathbb{Q}$. Дальнейшие детали, касающиеся этих результатов см. в [8, 11, 12, 25, 27, 37, 28, 29, 32] и [33]. Однако, в решении диофантовой проблемы[1] поля $\mathbb{Q}$ прогресс не столь значителен. Более того, одним из следствий серии гипотез Барри Мазура и Коллио–Телена, Суиннертон–Дайера и Скоробогатова является то, что $\mathbb{Z}$ не имеет диофантового представления над $\mathbb{Q}$, и поэтому следует искать другие методы решения диофантовой проблемы поля $\mathbb{Q}$. (Гипотезы Мазура можно найти в [20–22] и [23]. Коллио–Телен, Суиннертон–Дайер и Скоробогатов нашли контрпример к самой сильной из гипотез Мазура. Их модификацию гипотезы Мазура в свете этого контрпримера можно найти в [4].) По поводу обсуждения теоретико-модельных аспектов гипотез Мазура мы отсылаем читателя к [5] и [38].

Остается открытым общий вопрос о существовании диофантовых представлений целых рациональных и алгебраических чисел над целозамкнутыми подкольцами числовых полей (включая сами поля).

[1]Здесь и далее под диофантовой проблемой некоторого поля автор подразумевает аналог 10-й проблемы Гильберта над соответствующим полем. — *Прим. перев.*

Над функциональными полями задача в большей степени поддается усилиям. По поводу наилучших известных результатов для функциональных полей характеристики 0 отсылаем читателя к [9, 16, 18] и [41]. Однако гораздо больше известно о функциональных полях и кольцах положительной характеристики. В частности, были получены следующие результаты. Т. Фейдас доказал диофантову неразрешимость для поля рациональных функций над конечным полем констант характеристики большей двух (см. [26]). К. Видела доказал аналогичный результат, когда характеристика равна двум (см. [39]). Ким и Роуш распространили результат Фейдаса на произвольное поле рациональных функций $K$ характеристики $p$ большей двух, не содержащее алгебраического замыкания конечного поля (см. [17]). Автор настоящей статьи распространила результат Фейдаса на произвольное поле функций одной переменной над конечным полем констант характеристики большей двух (см. [31]). Далее, в [34] автор данной статьи доказала следующее утверждение.

**1.2. Теорема.** *Пусть $K$ – поле алгебраических функций характеристики $p > 2$. Пусть $C$ – алгебраическое замыкание конечного поля в $K$. Предположим, что $C$ обладает расширением степени $p$. Предположим также, что $K$ содержит подполе $K_1$, возможно совпадающее с $C$, и такие элементы $u, x$, что $u$ трансцендентен над $K_1$, $x$ алгебраический над $C(u)$ и $K = K_1(u, x)$. Тогда диофантова проблема поля $K$ неразрешима.*

В [36] автор настоящей статьи показала, что десятая проблема Гильберта неразрешима в любом поле, конечнопорожденном над конечным полем характеристики большей двух. Затем в [13] Кирстин Айзентрагер доказала теорему 1.2 в случае, когда характеристика равна двум. В настоящей работе мы обобщаем теорему 1.2 и основной результат из [36] и доказываем следующую теорему

**1.3. Теорема.** *Пусть $M$ – произвольное поле функций характеристики $p > 0$, такое, что алгебраическое замыкание конечного поля в $M$ обладает расширением степени $p$. Пусть $L$ – произвольное поле, конечнопорожденное над $C$ и такое, что $L$ и $M$ линейно разделены над $C$. Положим $K = ML$. Тогда диофантова проблема поля $K$ неразрешима.*

Доказательство этого результата следует методу, применяемому практически во всех результатах, связанных с диофантовыми представлениями над полями положительной характеристики. Этот метод был разработан Денефом в [10] и применен Фейдасом в [24]. Для того чтобы объяснить суть этого метода, нам потребуется дать определение и сформулировать лемму.

**1.3. Определение.** Пусть $m, n, p \in \mathbb{N}$ и $p$ – простое число. Символ "$n|_p m$" означает $\exists s \in \mathbb{N}, m = np^s$.

**1.4. Лемма.** *Тогда не существует общего алгоритма, который по заданному набору $\{P_i(z_{i,1}, \ldots, z_{i,k_i}), Q_i(z_{i,1}, \ldots, z_{i,m_i})\}$ многочленов над $\mathbb{Z}$, степень которых не превосходит 1, определял бы разрешимость следующей системы в $\mathbb{N}$:*

$$P_i(z_{i,1}, \ldots, z_{i,k_i})|_p Q_i(z_{i,1}, \ldots, z_{i,m_i}) \tag{1.1}$$

*(см. [24] теорема1).*

Эта лемма, доказанная Фейдасом, применяется в предложении 1.6 для того, чтобы наметить путь к доказательству диофантовой неразрешимости над полем функций. Прежде чем формулировать предложение, нам необходимо ввести первый набор обозначений, используемых в этой статье.

**1.5. Обозначения.**

- Пусть $K$ – поле функций положительной характеристики $p$, сепарабельно порожденное над полем констант $C_K$.
- Пусть элемент $u \in K \setminus C_K$ таков, что расширение $K/C_K(u)$ сепарабельно.
- Пусть поле $C$ алгебраично над конечным полем характеристики $p$. Предположим, что $C$ алгебраически замкнуто в $C_K$.
- Пусть $F$ – алгебраическое замыкание поля $C(u)$ в $K$.

**1.6. Предложение.** *Пусть $\mathfrak{p}$ – простой дивизор поля $F$ неразветвленный в расширении $K/F$. Пусть $INT(\mathfrak{p})$ – произвольное подмножество поля $K$, обладающее следующими свойствами. Если $w \in INT(\mathfrak{p})$, то $w$ является целым во всех делителях простого $\mathfrak{p}$ в $K$. Далее, $INT(\mathfrak{p})$ содержит все целые в $\mathfrak{p}$ элементы из $F$. Положим $P(K) = \{(x, y) \in K^2 | \exists s \in \mathbb{N}, y = x^{p^s}\}$. Тогда, если множества $INT(\mathfrak{p})$ и $P(K)$ диофантовы над $K$, то десятая проблема Гильберта над $K$ неразрешима.*

**Доказательство.** Доказательство этого предложения весьма сходно с доказательством леммы 1.5 из [31], однако некоторые детали требуют изменения. Пусть $\mathfrak{p} = \prod \mathfrak{p}_i$ – факторизация дивизора $\mathfrak{p}$ в $K$. (Такая факторизация имеет смысл с учетом леммы 5.1 из приложения.) Рассмотрим отображение $f$ множества $\mathbb{N}$ в множество всех подмножеств $K$, определенное следующим образом: $f(n) = \{x \in K | \mathrm{ord}_{\mathfrak{p}_1} x = n\}$. Согласно слабой теореме об аппроксимации (см. предложение 2.1 на стр. 14 из [14]), для всякого $n$ имеем $f(n) \cap F \neq \emptyset$. Таким образом, для произвольных натуральных чисел $n_1, n_2, n_3 \in \mathbb{N}$ равенство $n_1 = n_2 + n_3$ равносильно существованию $z_i \in f(n_i)$, таких, что $z_1 = z_2 z_3$. Далее, для произвольных натуральных чисел $n, m$ условие $n|_p m$ равносильно существованию $x \in f(n), y \in f(m), w \in K$, таких, что $(x, w) \in P(K), (y/w), (w/y) \in INT(\mathfrak{p})$.

Следующие два раздела статьи посвящены диофантовым представлениям множеств $INT(\mathfrak{p})$ и $P(K)$, соответственно. В четвертом разделе доказывается результат о неразрешимости.

## 2. Целочисленность в конечном числе простых

Доказательство, приведенное ниже, очень близко к доказательствам из [34]. Основное различие состоит в том, что здесь мы не предполагаем, что выбранный простой дивизор из $F$ остается простым и в $K$. Мы только предполагаем, что он неразветвлен. Прежде чем мы перейдем к техническим деталям, нам потребуется новый набор обозначений и предположений.

### 2.1. Обозначения и предположения.

- Предположим, что $C$ обладает расширением степени $p$ и содержит все решения уравнения $x^{p^2} - x = 0$.
- Пусть $\tilde{C}$ – алгебраическое замыкание поля $C$.
- Пусть $\mathfrak{q}$ – простой дивизор поля $F$ степени 1.
- Пусть $\mathfrak{q}_{K,1}, \ldots, \mathfrak{q}_{K,m}$ – это все сомножители $\mathfrak{q}$ в $K$; кроме того предположим, что $\deg_K(\mathfrak{q}_{K,i}) = e(\mathfrak{q}_{K,i}/\mathfrak{q}) = 1$ для $i = 1, \ldots, m$.
- Пусть $\alpha \in \tilde{C}$ – элемент степени $p$ над $C$.
- Пусть $w \in K$.
- Пусть $f \in F$ – это функция, $F$-дивизор которой имеет вид $\frac{\mathfrak{q}^a}{\prod \mathfrak{t}_i^{a_i}}$, где $a, a_i \in \mathbb{N} \setminus \{0\}, a \not\equiv 0 \mod p$.

- Положим $h = f^{-1}w^{ap^3} + f^{-p^2}$.
- Положим $z = b^{p^2} - b$ для некоторого $b \in C \setminus \{0\}$.
- Пусть $\beta$ – корень уравнения

$$X^{p^2} - X - h^{-1} - z + f^2 = 0. \tag{2.2}$$

- Пусть $\{\mathfrak{q}_{K(\beta),i,j}\}$ – множество всех сомножителей дивизора $\mathfrak{q}_{K,i}$ в $K(\beta)$.
- Если $w \in F$, то через $\{\mathfrak{t}_{i,j}\}$ обозначим множество всех сомножителей дивизора $\mathfrak{t}_i$ в $F(\beta)$.

**2.2. Лемма.** *Справедливы следующие утверждения:*

(1) *Поле $C(u)$ алгебраически замкнуто в $C_K(u)$.*
(2) *$F/C(u)$ – конечное сепарабельное расширение.*

**Доказательство.** Предположим, что $C(u)$ не является алгебраически замкнутым в $C_K(u)$. Тогда для некоторого $Z(u) \in C_K(u) \setminus C(u)$, $Z(u)$ является алгебраическим над $C(u)$. Так как поле $C$ алгебраически замкнуто в $C_K$, то $Z(u) \in \tilde{C}C_K(u) \setminus \tilde{C}(u)$. (В противном случае, все коэффициенты приведенных числителя и знаменателя были бы в $C_K \cap \tilde{C} = C$.) Тогда по лемме 2.3 из [30] для некоторого $a \in \tilde{C}$ элемент $Z(a) \in \tilde{C}C_K \setminus \tilde{C}$ и является алгебраическим над $C$, то есть лежит в $\tilde{C}$, что невозможно.

Согласно теореме 11 на стр. 280 из [1], всякий элемент поля $F$ имеет ту же степень над $C(u)$, что и над $C_K(u)$. Так как расширение $K/C_K(u)$ конечно, то степень всякого элемента из $F$ над $C(u)$ ограничена, и следовательно, $F/C(u)$ расширение также конечно. Предположим теперь, что расширение $F/C(u)$ несепарабельно. Пусть $\omega$ – элемент поля $F$ несепарабельный над $C(u)$. Как и выше, $\omega$ имеет один и тот же неприводимый многочлен над $C(u)$ и $C_K(u)$. Таким образом, $\omega$ оставался бы несепарабельным и над $C_K(u)$. Это, однако, не может произойти, поскольку расширение $K/C_K(u)$ сепарабельно.

**2.3. Теорема.** *Пусть $w \in K$, и предположим, что уравнение*

$$\mathbf{N}_{K(\alpha,\beta)/K(\beta)}(x) = h \tag{2.3}$$

*имеет решение $x \in K(\alpha, \beta)$. Тогда $\mathrm{ord}_{\mathfrak{q}_{K,i}} w \geq 0$. Далее, если $w \in F$ и $\mathrm{ord}_{\mathfrak{q}} w \geq 0$, то уравнение (2.3) имеет решения в $K(\alpha, \beta)$.*

**Доказательство.** Предположим, что $w$ имеет полюс в $\mathfrak{q}_{K,i}$ для некоторого $i$, $1 \leq i \leq m$. Тогда справедливы следующие утверждения.

- $\operatorname{ord}_{\mathfrak{q}_{K,i}} f^{-1}w^{ap^3} = ap^3 \operatorname{ord}_{\mathfrak{q}_{K,i}} w - a < -ap^2 = \operatorname{ord}_{\mathfrak{q}_{K,i}} f^{-p^2}$. Следовательно

$$\begin{aligned} \operatorname{ord}_{\mathfrak{q}_{K,i}} h &= \operatorname{ord}_{\mathfrak{q}_{K,i}} (f^{-1}w^{ap^3} + f^{-p^2}) = \operatorname{ord}_{\mathfrak{q}_{K,i}} f^{-1}w^{ap^3} \\ &= ap^3 \operatorname{ord}_{\mathfrak{q}_{K,i}} w - a \not\cong 0 \ \text{ по модулю } \ p. \end{aligned} \tag{2.4}$$

- $\operatorname{ord}_{\mathfrak{q}_{K,i}} h < 0$, а значит, $h^{-1}$ является целым в $\mathfrak{q}_{K,i}$. Следовательно, $h^{-1} + z - f^2$ является целым в $\mathfrak{q}_{K,i}$. Таким образом, применяя рассуждение, подобное использовавшемуся в доказательстве леммы 3.1 из [34], можно показать, что $\mathfrak{q}_{K,i}$ неразветвлен в расширении $K(\beta)/K$. Далее заметим, что дискриминант многочлена, определяющего $\beta$, есть константа. Таким образом, по теореме 7.6 на стр. 32 и предложению 7.7, на стр. 33 из [15], степенной базис, порожденный $\beta$ является целым относительно $\mathfrak{q}_{K,i}$ базисом, и факторизация левой части уравнения (2.2) по модулю $\mathfrak{q}_{K,i}$ определяет факторизацию $\mathfrak{q}_{K,i}$ в расширении $K(\beta)/K$. Здесь следует заметить, что $h^{-1} + z - f^2 \cong z = b^{p^2} - b \mod \mathfrak{q}_{K,i}$, а значит, левая часть уравнения (2.2) полностью распадается по модулю $\mathfrak{q}_{K,i}$, поскольку по предположению поле $C$ содержит все решения уравнения $x^{p^2} - x = 0$. Таким образом, либо $\beta \in K$, либо в $K(\beta)$ все сомножители $\mathfrak{q}_{K(\beta),i,j}$ diwizora $\mathfrak{q}_{K,i}$ имеют над $\mathfrak{q}_{K,i}$ относительную степень 1, и, таким образом, их поля вычетов совпадают с $C_K$. Это также показывает, что расширение $K(\beta)/K$ не содержит расширения поля констант. Таким образом, $\alpha$ по-прежнему имеет степень $p$ над $K(\beta)$, и $\alpha$ имеет степень $p$ над полем вычетов относительно $\mathfrak{q}_{K(\beta),i,j}$ для всех $j$. Следовательно, по теореме 7.6 на стр. 32 и предложению 7.7 на стр. 33 из [15] (на этот раз примененным к степенному базису, порожденному $\alpha$) $\mathfrak{q}_{K(\beta),i,j}$ не распадается в расширении $K(\beta,\alpha)/K(\beta)$. Следовательно, если (2.3) имеет место для некоторого $x \in K(\alpha,\beta)$, то $\operatorname{ord}_{\mathfrak{q}_{K(\beta),i,j}} h = \operatorname{ord}_{\mathfrak{q}_{K,i}} h \cong 0 \mod p$ по лемме 5.2. Это сравнение противоречит равенству (2.4), а значит, (2.3) не имеет решений в $K(\alpha,\beta)$.

Далее мы рассмотрим случай, когда $w$, а значит, и $h$ лежат в $F$, а $w$ является целым в $\mathfrak{q}$, и следовательно во всех $\mathfrak{q}_{K,i}$. В этом случае мы можем заключить следующее.

- Заметим, что в предположении $w \in F$ элемент $\beta$ является алгебраическим над $F$, и по теореме 13 на стр. 281 из [1] поле $F(\alpha,\beta)$ алгебраически замкнуто в $K(\alpha,\beta)$, так как $\alpha,\beta$ сепарабельны над $F$.
- Пусть $x \in F(\alpha,\beta)$. Тогда $\mathbf{N}_{K(\alpha,\beta)/K(\beta)}(x) = \mathbf{N}_{F(\alpha,\beta)/F(\beta)}(x)$. Таким образом, достаточно показать, что уравнение
$$\mathbf{N}_{F(\alpha,\beta)/F(\beta)}(x) = h \tag{2.5}$$
разрешимо в $F(\alpha,\beta)$.
- Прежде всего заметим, что $\mathrm{ord}_{\mathfrak{q}} h = -ap^2 \cong 0 \mod p^2$, и $\mathfrak{q}$ – полюс $h$.
- Следовательно, $\mathrm{ord}_{\mathfrak{q}}(h^{-1}+z-f^2) \geq 0$ и $h^{-1}+z-f^2 \cong (b^{p^2}-b) \mod \mathfrak{q}$. Таким образом, $\mathfrak{q}$ полностью распадается в расширении $F(\beta)/F$. Так как $\mathfrak{q}$ – простой дивизор степени 1, то мы вновь заключаем, что расширение $F(\beta)/F$ не содержит расширения поля констант, и что степень $\alpha$ над $F(\beta)$ равна $p$.
- Далее, заметим, что так как степень дивизора функции $f$ равна 0, то $a \deg_F \mathfrak{q} = \sum a_i \deg_F(\mathfrak{t}_i)$. Таким образом, $a \geq \sum a_i$.
- Предположим теперь, что $\mathrm{ord}_{\mathfrak{t}_i} w = 0$. Тогда $\mathrm{ord}_{\mathfrak{t}_i} h = \min(\mathrm{ord}_{\mathfrak{t}_i} f^{-1}, \mathrm{ord}_{\mathfrak{t}_i} f^{-p^2}) = a_i$. Таким образом, $\mathrm{ord}_{\mathfrak{t}_i}(h^{-1} + z - f^2) = \min(-a_i, -2a_i) = -2a_i < 0$. В этом случае рассуждения подобные применявшимся в доказательстве леммы 3.1 из [34] дают, что-либо $2a_i \cong 0 \mod p^2$, либо $\mathfrak{t}_i$ разветвляется в расширении $F(\beta)/F$, причем степень ветвления делится на $p$, если $2a_i \cong 0 \mod p$, или делится на $p^2$, если $2a_i \ncong 0 \mod p$.

  Теперь предположим, что $\mathrm{ord}_{\mathfrak{t}_i} w > 0$. Тогда $\mathrm{ord}_{\mathfrak{t}_i} h = \min(ap^3 \mathrm{ord}_{\mathfrak{t}_i} w + a_i, p^2 a_i) = p^2 a_i . \mathrm{ord}_{\mathfrak{t}_i}(h^{-1} + z - f^2) = \min(-p^2 a_i, -2a_i) = -p^2 a_i \cong 0 \mod p^2$.

  Наконец, предположим, что $\mathrm{ord}_{\mathfrak{t}_i} w < 0$. Тогда $\mathrm{ord}_{\mathfrak{t}_i} h = \min(p^3 a \mathrm{ord}_{\mathfrak{t}_i} w + a_i, p^2 a_i) = p^3 a \mathrm{ord}_{\mathfrak{t}_i} w + a_i < 0$. Следовательно, $\mathrm{ord}_{\mathfrak{t}_i}(h^{-1} + z - f^2) = \min(-p^3 a \mathrm{ord}_{\mathfrak{t}_i} w - a_i, -2a_i) = -2a_i < 0$. Опять, как и в случае, когда $w$ – единица в $\mathfrak{t}_i$, используя рассуждения, подобные приведенным в доказательстве леммы 3.1, получаем, что либо $2a_i \cong 0 \mod p^2$, либо $\mathfrak{t}_i$ разветвлен в расширении $F(\beta)/F$, причем степень ветвления делится на $p$, если $2a_i \cong 0 \mod p$, и делится на $p^2$, если $2a_i \ncong 0 \mod p$.

Таким образом, в любом случае $\mathrm{ord}_{\mathfrak{t}_{i,j}} h \cong 0 \mod p^2$ для всех $i$

- Пусть $\mathfrak{l} \neq \mathfrak{t}_i$ – нуль функции $h$. Тогда $\mathrm{ord}_{\mathfrak{l}}(h^{-1} + z - f^2) = -\mathrm{ord}_{\mathfrak{l}} h$, так как $z - f^2$ имеет полюсы только в $\mathfrak{t}_i$. Так же, как и выше, либо $\mathrm{ord}_{\mathfrak{l}} h \cong 0 \mod p^2$, либо $\mathfrak{l}$ разветвляется в расширении $F(\beta)/F$, причем степень ветвления делится на $p$, если $\mathrm{ord}_{\mathfrak{l}} h \cong 0 \mod p$, и делится на $p^2$, если $\mathrm{ord}_{\mathfrak{l}} h \ncong 0 \mod p$. Следовательно, если $\mathfrak{l}_i$ лежит над $\mathfrak{l}$ в $F(\beta)$, то $\mathrm{ord}_{\mathfrak{l}_i} h \cong 0 \mod p^2$.
- Если $\mathfrak{m}$ – полюс функции $h$ и $\mathfrak{m} \neq \mathfrak{q}, \mathfrak{m} \neq \mathfrak{t}_i$, то $\mathrm{ord}_{\mathfrak{m}} h = \mathrm{ord}_{\mathfrak{m}} w^{ap^3} \cong 0 \mod p^2$.
- По лемме 5.4, существует подполе $G \subset F(\beta)$, удовлетворяющее следующим требованиям:

(1) $G$ – глобальное поле, содержащее $h$.
(2) Никакой простой из $G$ не разветвляется в расширении $F(\beta)/G$. Расширение $F(\beta)/G$ является сепарабельным (но не обязательно конечным) расширением, получающимся расширением поля констант.
(3) Степень $\alpha$ над $G$ равна $p$.

Из свойства 2 следует, что, $\mathrm{ord}_{\mathfrak{k}} h \cong 0 \mod p^2$ для любого простого $\mathfrak{k}$ из $G$. Таким образом, по лемме 3.3 из [34], $h$ является локальной нормой во всех простых из $G$ в расширении $G(\alpha)/G$; по сильному принципу норм Хассе (см. [2, стр. 185] или [40, предложения 10, 11, стр7 182–183;теорема 2, стр. 206]) $h$ является глобальной нормой. Следовательно, существует $x \in G(\alpha)$, такой, что $\mathbf{N}_{G(\alpha)/G}(x) = h$. Теперь либо $x \in G$, либо $x \notin G$. Если $x \in G$, то $h$ является $p$-ой степенью в $G$ и $h$ – норма в расширении $F(\alpha, \beta)/F(\beta)$. Если $x \notin G$, то $G(x) = G(\alpha)$, так как $[G(\alpha) : G] = p$. Тогда $p \geq [F(x, \beta) : F(\beta)] = [F(\alpha, \beta) : F(\beta)] = p$. Таким образом, степень $x$ над $F(\beta)$ равна $p$ и норма $x$ над $F(\beta)$ должна быть такой же, как и над $G$. Следовательно, $h$ – норма в расширении $F(\alpha, \beta)/F(\beta)$.

**2.4. Предложение.** *Существует множество $A_K \subset K$, удовлетворяющее следующим условиям.*

(1) *Если* $w \in A_K$, *то* $\mathrm{ord}_{\mathfrak{q}_{K,i}} w \geq 0$ *для всех* $i$.
(2) *Если* $w \in F$ *и* $\mathrm{ord}_{\mathfrak{q}} w \geq 0$, *то* $w \in A_K$.
(3) *Множество* $A_K$ *диофантово над* $K$.

**Доказательство.** Прежде всего отметим, что из доказательства теоремы 2.3 следует, что при любом выборе $w$ степень $\alpha$ над $K(\beta)$ равна $p$. Далее, в введенных выше обозначениях, положим

$$A_K = \{w \in K | \exists x \in K(\alpha, \beta), \mathbf{N}_{K(\alpha,\beta)/K(\beta)}(x) = h\}.$$

Нам потребуется переписать $\mathbf{N}_{K(\alpha,\beta)/K(\beta)}(x) = h$ в виде многочлена, значения переменных которого пробегают поле $K$. Заметим, что формула $\exists x \in K(\alpha, \beta), \mathbf{N}_{K(\alpha,\beta)/K(\beta)}(x) = h$ эквивалентна формуле

$$\exists x_0, \dots, x_{p-1} \in K(\beta), \prod_{j=1}^{p} \left( \sum_{i=0}^{p-1} x_i \alpha_j^i \right) = h, \tag{2.6}$$

где $\alpha_1 = \alpha, \dots, \alpha_p$ – это все сопряженные с $\alpha$ над $K$ и $K(\beta)$. Коэффициенты многочлена $P(x_0, \dots, x_{p-1}) = \prod_{j=1}^{p} \left( \sum_{i=0}^{p-1} x_{i,j} \alpha_j^i \right)$ инвариантны относительно действия группы $\mathrm{Gal}(K(\alpha,\beta)/K(\beta)) \cong \mathrm{Gal}(K(\alpha)/K)$, и следовательно, $P(x_0, \dots, x_{p-1}) \in K[x_0, \dots, x_{p-1}]$. Остается лишь позаботиться о том, что переменные $x_i$ пробегают $K(\beta)$. Это можно сделать при помощи леммы 2.12 из [36].

**2.5. Теорема.** *Пусть* $K_0$ *– поле функций, сепарабельно порожденное над полем констант* $C_{K_0}$. *Пусть элемент* $z \in K_0 \setminus C_{K_0}$ *таков, что расширение* $K_0/C_{K_0}(z)$ *сепарабельно. Через* $C_0$ *обозначим алгебраическое замыкание в* $K_0$ *конечного поля, а через* $F_0$ *– алгебраическое замыкание поля* $C_0(z)$ *в* $K_0$. *Пусть* $\mathfrak{q}_0$ *– простой дивизор поля* $F_0$, *лежащий над простым поля* $C_0(z)$, *не разветвленным в расширении* $K_0/C_0(z)$. *Тогда существует множество* $A_0(\mathfrak{q}_0)$, *удовлетворяющее следующим условиям.*

(1) *Если* $w \in A_0(\mathfrak{q}_0)$, *то* $w$ *является целым во всех сомножителях* $\mathfrak{q}_0$ *в* $K_0$.
(2) *Если* $w \in F_0$ *и* $w$ *является целым в* $\mathfrak{q}_0$, *то* $w \in A_0(\mathfrak{q}_0)$.
(3) *Множество* $A_0(\mathfrak{q}_0)$ *диофантово над* $K_0$.

**Доказательство.** Пусть $\mathfrak{q}_{C_0(z)}$ – простой в $C_0(z_0)$, лежащий под $\mathfrak{q}_0$. Не умаляя общности, можно считать, что он не является полюсом $z$ и, таким образом, соответствует неприводимому над $C_0$

многочлену от $z$. Так как поле $C_0$ алгебраически замкнуто в $C_{K_0}$, то этот простой не разветвляется и не распадается в расширении $C_{K_0}(z)/C_0(z)$. Пусть $\mathfrak{q}_{C_{K_0}(z)}$ – простой, лежащий над $\mathfrak{q}_{C_0(z)}$ в $C_{K_0}(z)$. Тогда $\mathfrak{q}_{C_{K_0}(z)}$ не разветвляется в расширении $K_0/C_{K_0}(z)$. Пусть $\mathfrak{q}_{K_0,1},\dots,\mathfrak{q}_{K_0,m_0}$ – все сомножители $\mathfrak{q}_{C_0(z)}$ в $K_0$. Мы утверждаем, что поле вычетов каждого из $\mathfrak{q}_{K_0,i}$ сепарабельно над $C_{K_0}$. Действительно, так как $\mathfrak{q}_{K_0,i}$ неразветвлен над $C_{K_0}(z)$, то его поле вычетов сепарабельно над полем вычетов для $\mathfrak{q}_{C_{K_0}(z)}$. С другой стороны, поле вычетов относительно $\mathfrak{q}_{C_{K_0}(z)}$ порождается элементом, алгебраическим над конечным полем. Следовательно, поле вычетов относительно $\mathfrak{q}_{C_{K_0}(z)}$ сепарабельно над $C_{K_0}$. Таким образом, поле вычетов относительно $\mathfrak{q}_{K_0,i}$ сепарабельно над $C_{K_0}$. По лемме 6.14 из [34], существует конечное сепарабельное расширение $K$ поля $K_0$, получающееся расширением поля констант, и такое, что все сомножители $\mathfrak{q}_{C_{K_0}(z)}$ в $K$ имеют степень 1, все сомножители $\mathfrak{q}_{C_0(z)}$ в $F$ (алгебраическом замыкании поля $C_0(z)$ в $K$) также имеют степень 1, и $C$ – алгебраическое замыкание поля $C_0$ в $K$ – содержит все корни многочлена $X^{p^2}-X=0$. Пусть $\mathfrak{q}_{0,i}$ – сомножитель $\mathfrak{q}_0$ в $F$. Тогда по лемме 5.5, существует функция $f_i$, такая, что ее дивизор имеет вид $\frac{\mathfrak{q}_{0,i}^a}{\prod \mathfrak{t}_{j,0}^{a_j}}$, где $a \not\equiv 0 \mod p$, $a, a_j \in \mathbb{N}$ и $\mathfrak{t}_j \neq \mathfrak{q}_{0,i}$. Далее, из свойств конечных полей (см. теорему 13 на стр. 185 из [19]) вытекает, что $C$ обладает расширением степени $p$. Таким образом, по предложению 2.4 существует множество $A(\mathfrak{q}_{0,i})$, удовлетворяющее следующим условиям.

(1) Если $w \in A(\mathfrak{q}_{0,i})$, то $w$ является целым во всех сомножителях $\mathfrak{q}_{0,i}$ в $K$.
(2) Если $w \in F$ и $w$ является целым в $\mathfrak{q}_{0,i}$, то $w \in A(\mathfrak{q}_{0,i})$.
(3) Множество $A(\mathfrak{q}_{0,i})$ является диофантовым над $K$.

Заметим, во-первых, что множество $A=\cap_i A(\mathfrak{q}_{0,i})$ диофантово над $K$. Во-вторых, используя метод "вверх и вниз"[2] (см. раздел 2.2 в [35]), мы можем заключить, что над $K_0$ имеется диофантово представление $A\cap K_0$. Остается показать, что множество $A\cap K_0$ обладает требуемыми свойствами. Сначала предположим, что $w \in A\cap K_0$. Тогда $w$ является целым во всех сомножителях всех $\mathfrak{q}_{0,i}$ в $K$. Таким образом, $w$ являетя целым во всех сомножителях $\mathfrak{q}_0$ в $K$. Наконец, последнее утверждение влечет, что $w$ является целым во всех сомножителях $\mathfrak{q}_0$ в $K_0$. Предположим теперь, что

[2] В оригинале "Going up and then down method". – *Прим. перев.*

$w \in F_0$ и является целым в $\mathfrak{q}_0$. Тогда $w \in F$ и является целым во всех $\mathfrak{q}_{0,i}$. Таким образом, по построению множеств $A(\mathfrak{q}_{0,i})$ и $A$ имеем $w \in A$. Так как $w \in A$ и $w \in F_0 \subset K_0$, то $w \in A \cap K_0$.

## 3. Уравнения степени $p$

Мы начнем обсуждение с обозначений и предположений, относящихся к этому разделу.

**3.1. Обозначения и предположения.**

- Пусть $M$ – произвольное поле функций характеристики $p > 0$, такое, что $C$ – алгебраическое замыкание конечного поля в $M$ – обладает расширением степени $p$.
- Пусть $L$ – произвольное конечно порожденное над $C$ поле, удовлетворяющее следующим условиям: $L = C(u_1, \dots, u_n, w)$, где $u_1, \dots, u_n$ алгебраически независимы над $C$; элемент $w$ является алгебраическим и сепарабельным над $C(u_1, \dots, u_n)$.
- Положим $d = [L : C(u_1, \dots, u_n)]$.
- Для $k = 1, \dots, n$ через $F_k$ обозначим алгебраическое замыкание поля $C(u_1, \dots, u_k)$ в $L$.
- Предположим, что $M$ и $L$ линейно разделены над $C$.
- Положим $K = ML = M(u_1, \dots, u_n, w)$.
- Пусть $C_{K,i}$ $(i = 1, \dots, n)$ – алгебраическое замыкание поля $M(u_1, u_2, \dots, u_{i-1}, u_{i+1}, \dots, u_n)$ в $K$. Положим $C_K = C_{K,1}$.
- Через $\tilde{C}_{K,i}$ обозначим алгебраическое замыкание поля $C_{K,i}$, а через $\tilde{C}_K$ – алгебраическое замыкание поля $C_K$.
- Положим $\tilde{K} = \tilde{C}_K K$ и $\tilde{K}_i = \tilde{C}_{K,i} K$.
- Через $F$ обозначим алгебраическое замыкание поля $C(u_1)$ в $K$.
- Через $g_i$ обозначим количество простых, разветвляющихся в расширении $\tilde{K}_i/\tilde{C}_{K,i}(u_i)$, $i = 1, \dots, n$.

Основная цель этого раздела состоит в том, чтобы свести общий случай, когда поле $K$ имеет конечную степень трансцендентности над $M$, к случаю поля степени трансцендентности 1 над $M$, т. е. к случаю, уже решенному для $p > 2$ в [34] и для $p = 2$ в [13].

**3.2. Предложение.** *Имеют место следующие утверждения.*

(1) *Поля $F$ и $M$ линейно разделены над $C$.*
(2) *Поле $F$ алгебраически замкнуто в $K$.*

(3) *Поле $FM$ алгебраически замкнуто в $K$.*
(4) $\bigcap_{i=2}^{n} C_{K,i} = FM$.

**Доказательство.**

(1) Предположим, что $F$ и $M$ не являются линейно разделенными над $C$. По лемме 9.1 из [14] это влечет, что существует множество $x_1, \ldots, x_l \in F$, которое линейно независимо над $C$, но не над $M$. Так как $F \subset L$, то существование такого множества противоречит тому, что поля $L$ и $M$ линейно разделены.

(2) По лемме 2.2 поле $C(u_1)$ алгебраически замкнуто в $C_K(u_1)$, а $F/C(u_1)$ – конечное сепарабельное расширение. Пусть элемент $v$ таков, что $F = C(u_1, v)$. Предположим теперь, что существует $w_1 \in K$, такой, что $w_1$ является алгебраическим над $C(u_1)$, но не лежит в $F = C(u_1, v)$. Положим $F_1 = F(w_1) = C(u_1, v, w_1)$. Так как $C(u_1)$ является алгебраически замкнутым в $C_K(u_1)$, то по теореме 11 на стр. 280 из [1] неприводимый многочлен для $w_1$ над $C_K(u_1)$ совпадает с неприводимым многочленом для $w_1$ над $C(u_1)$. Так как $u_1, \ldots, u_n$ – разделяющий трансцендентный базис поля $L$ над $C$, то расширение $L/C(u_1, \ldots, u_n)$ сепарабельно. Таким образом, $K/M(u_1, \ldots, u_n)$ и $K/C_K(u_1)$ – сепарабльные расширения. Следовательно, элемент $w_1$ сепарабелен над $C_K(u_1)$ и, тем самым, над $C(u_1)$. Значит, $F(w_1)/C(u_1)$ – сепарабельное расширение, и следовательно, простое. Пусть $w_2 \in F(w_1)$ порождает $F(w_1)$ над $C(u_1)$. Тогда степень элемента $w_2$ над $C(u_1)$ должна быть больше, чем $[F : C(u_1)]$. Но опять по теореме 11 на стр. 280 из [1] степень $w_2$ над $C(u_1)$ такая же, как и степень $w_2$ над $C_K(u_1)$. Последняя не превосходит степени $w$ над $C(u_1)$, поскольку $w_2 \in K = C_K(u_1, w)$. Таким образом, наше предположение, о том, что $K$ содержит элемент алгебраический над $F$, но не лежащий в $F$, приводит к противоречию. Следовательно, поле $F$ алгебраически замкнуто в $K$.

(3) Заметим сначала, что $u_2, \ldots, u_n$ алгебраически независимы над $MF$, потому что $u_1, \ldots, u_n$ алгебраически независимы над $M$. Далее, пусть $v \in K$ является алгебраическим над $MF$. Так как поле $F$ алгебраически замкнуто в $K$, то оно алгебраически замкнуто в

$MF(v)$. Далее, $u_2,\dots,u_n$ также алгебраически независимы над $MF(v)$. Следовательно, используя рассуждения подобные тем, что применялись при доказательстве леммы 2.2, мы заключаем, что поле $F(u_2,\dots,u_n)$ алгебраически замкнуто в $MF(v)(u_2,\dots,u_n)$. Предположим, что $v_1$ порождает $L$ над $F(u_2,\dots,u_n)$ и, следовательно, $K$ над $MF(v)(u_2,\dots,u_n)$. По теореме 11 на стр. 280 из [1] элемент $v_1$ должен иметь один и тот же неприводимый многочлен над $F(u_2,\dots,u_n)$, $MF(u_2,\dots,u_n)$ и $MF(v)(u_2,\dots,u_n)$. Это невозможно, если расширение $MF(v)/MF$ не является тривиальным.

(4) Пусть $x \in \bigcap_{i=2}^n C_{K,i}$. Тогда коэффициенты нормированного неприводимого многочлена для $x$ над $M(u_1,\dots,u_n)$ на самом деле лежат в $M(u_1)$. Таким образом, $x$ является алгебраическим над $MF$. Далее, поле $MF \subset \bigcap_{i=2}^n C_{K,i}$ и алгебраически замкнуто в $K$. Значит, $x \in MF$.

**3.3. Лемма.** *Предположим, что имеют место следующие равенства:*

$$(a_k w + b) - t_k = v_k^{p^s} - v_k, \tag{3.7}$$

$$(a_k w + b)^{-1} - t_k^{-1} = u_k^{p^s} - u_k, \tag{3.8}$$

*где* $w, v_1,\dots,v_{d+1}, u_1,\dots,u_{d+1} \in K, b, t_1,\dots,t_{d+1}, a_0, a_1,\dots,a_{d+1} \in C_{K,i}$ *для некоторого* $i = 2,\dots,n$, *причем* $s = 1$, *если* $p > 2$, *и* $s = 2$ *если* $p = 2$, *и где для* $k, j \in \{0,\dots,d+1\}$, $k \neq j$, *имеем* $t_k \neq t_j, a_k \neq a_j$. *Предположим также, что* $w$ *не имеет полюсов в простых, разветвленных в расширении* $\tilde{K}_i/\tilde{C}_{K,i}(u_i)$, *а* $a_0,\dots,a_{d+1}, b$ *являются алгебраическими над конечным полем характеристики* $p$, *но не равны нулю, и для всех* $k$ *функции* $a_k w + b$ *не имеют нулей в простых, разветвленных в расширении* $\tilde{K}_i/\tilde{C}_{K,i}(u_i)$. *Тогда* $w \in C_{K,i}$.

**Доказательство.** Заметим, прежде всего, что $[\tilde{K}_i : \tilde{C}_{k,i}(u_i)] \le d$. Предположим, что $w \in K \setminus C_{K,i}$. Тогда $w \in \tilde{K}_i \setminus \tilde{C}_{K,i}$. Тогда для всех $k$ имеем $(a_k w + b)^{\pm 1} - t_i \notin \tilde{C}_{K,i}$. Следовательно, для всех $k$ имеем $v_k, u_k \notin \tilde{C}_{K,i}$. Так как для каждого $k$ функция $a_k w + b$ не принадлежит $\tilde{C}_{K,i}$, то она имеет полюс для некоторого не разветвленного в расширении $\tilde{K}_i/\tilde{C}_{K,i}(u_i)$ простого $\mathfrak{P}$ поля $\tilde{K}_i$. Тогда согласно уравнению (3.7) $\mathfrak{P}$ является полюсом $v_k^{p^s} - v_k$ для всех $k$. Следовательно, по лемме 5.6, $\mathfrak{P}$ является полюсом для $v_k^{p^s} - v_k$, порядок которого делится на $p^s$. Значит, порядок любого полюса для $a_k w + b$ в $\tilde{K}_i$ делится на $p^s$. Аналогичным образом, используя уравнение (3.8), заключаем что для всех $k$ все нули функции $a_k w+b$ в $\tilde{K}_i$ имеют порядки, делящиеся на $p^s$. Таким образом, для всех $k$ дивизор функции $w + \frac{b}{a_k}$ является $p^s$-ой степенью другого дивизора из $\tilde{K}_i$. Так как функции $w+\frac{b}{a_k}$ не имеют нулей или полюсов, разветвленных в расширении $\tilde{K}_i/\tilde{C}_{K,i}(u_i)$, то дивизоры этих элементов в $\tilde{C}_{K,i}(u_i, w)$ также являются $p$-ыми степенями других дивизоров.

Таким образом, дивизор нормы $\mathbf{N}_{\tilde{C}_{K,i}(w,u_i)/\tilde{C}_{K,i}(u_i)}(w+\frac{b}{a_k})$ является $p^s$-ой степенью другого дивизора, и следовательно, поскольку $\tilde{C}_{K,i}$ – совершенное поле, является $p^s$-й степенью. Так как $a_k$ есть $p^s$-ая степень в $K$, то по лемме 2.2 из [34] в случае характеристики $p > 2$ и по следствию 4.2 из [13] в случае $p = 2$ имеем, что $w$ есть $p^s$-ая степень в $\tilde{K}_i$. Аналогичным образом, $a_k w + b$ является $p^s$-ой степенью в $\tilde{K}_i$. Пусть элемент $\tilde{w} \in \tilde{K}_i$ таков, что $\tilde{w}^{p^s} = w$. Для каждого $k$ возьмем $\tilde{a}_k$ таким, что $\tilde{a}_k^{p^s} = a_k$ и возьмем $b$ таким, что $\tilde{b}^{p^s} = b$. Заметим, что $\frac{\tilde{b}}{\tilde{a}_k}$ также является $p^s$-ой степенью в $\tilde{K}_i$. Далее заметим, что теперь можно переписать уравнения (3.7) и (3.8) в виде

$$(\tilde{a}_k \tilde{w} + \tilde{b}) - t_k = (v_k - \tilde{a}_k \tilde{w} - \tilde{b})^{p^s} - (v_k - \tilde{a}_k \tilde{w} - \tilde{b}), \tag{3.9}$$

$$(\tilde{a}_k \tilde{w} + \tilde{b})^{-1} - t_k^{-1} = (u_k - (\tilde{a}_k \tilde{w} + \tilde{b})^{-1})^{p^s} - (u_k - (\tilde{a}_k \tilde{w} - \tilde{b})^{-1}). \tag{3.10}$$

Значит мы можем применить предыдущее рассуждение к $(\tilde{a}_k \tilde{w}+\tilde{b})$. Заметим, что высота $a_k w + b$ равна высоте $w$, а высота $(\tilde{a}_k \tilde{w} + \tilde{b})$ равна высоте $a_k w+b$ деленной на $p^s$. Таким образом, после конечного числа повторений описанной выше процедуры мы получим, что высота нового элемента $\tilde{a}_k \tilde{w} + \tilde{b}$ меньше, чем $p^s$, а значит, должна обращаться в 0. Иначе говоря, мы придем к заключению, что $\tilde{a}_k \tilde{w} + \tilde{b} \in \tilde{C}_{K,i}$. Однако в этом случае $a_k w + b$ также является элементом $\tilde{C}_{K,i}$ как степень другого элемента из $\tilde{C}_{K,i}$. Наконец, заметим, что $w \in \tilde{C}_{K,i} \cap K = C_{K,i}$, так как поле $C_{K,i}$ алгебраически замкнуто в $K$.

Теперь мы введем новый набор предположений и обозначений, который наряду с обозначениями и предположениями 3.1 потребуется при доказательстве леммы 3.5, следствия 3.6, леммы 3.7 и теоремы 3.8.

**3.4. Обозначения и предположения.**

- Существует такой элемент $t \in F$, что для некоторых $m, h \in \mathbb{N}$ и $c_0 = 0, c_1, \ldots, c_m \in C$ выполнены следующие условия.
- Расширение $F/C(t)$ сепарабельно.
- Для всех $i = 0, \ldots$ дивизор элемента $t + c_i$ из $F$ имеет вид $\mathfrak{p}_i/\mathfrak{q}$, где $\mathfrak{p}_i$, $\mathfrak{q}$ – простые дивизоры $F$ степени $p^h$. Положим $\mathfrak{p} = \mathfrak{p}_0$.
- Пусть $\prod \mathfrak{P}_i$ – факторизация дивизора $\mathfrak{p}$ в $\tilde{K}$, а $\prod \mathfrak{Q}_j$ – факторизация дивизора $\mathfrak{q}_i$ в $\tilde{K}$. (Таким образом, мы предполагаем, что $\mathfrak{p}$ и $\mathfrak{q}$ неразветвлены в $\tilde{K}/\tilde{C}_K(t)$.)
- Для всех $s \in \mathbb{N}$ и $i \neq j$ имеем $c_i^{p^s} \neq c_j$.
- Пусть $g$ – число простых дивизоров, разветвленных в расширении $\tilde{K}/\tilde{C}_K(t)$.
- Предположим, что $m \geq d + 2(g + g_2 \ldots + g_n) + 6 + [K : C_K(t)]$.
- Для каждого $c_i, i = 0, \ldots, m$, через $r_i$ обозначим наименьшее натуральное число, такое, что $c_i^{p^{r_i}} = c_i$.
- Для всех $i = 0, \ldots, m$ и $j_i = 1, \ldots, r_i$, положим $d_{i,j_i} = c_i^{j_i}$.

**3.5. Лемма.** *Пусть $s = 1$, если $p > 2$, и $s = 2$, если $p = 2$. Пусть $w, u, u_{i,j_i,k,j_k}, v_{i,j_i,k,j_k}$, где $i, k = 0, \ldots, m, j_i = 1, \ldots, r_i, j_k = 1, \ldots, r_k$, – элементы поля $K$, удовлетворяющие следующим уравнениям при всех $k = 0, \ldots, m$ для некоторых $1 \leq j_k \leq r_k$ и при всех $i = 0, \ldots, m$, для некоторых $1 \leq j_i \leq r_i$.*

$$w - t = u^{p^s} - u, \tag{3.11}$$

$$w^{-1} - t^{-1} = v^{p^s} - v, \tag{3.12}$$

$$w_{i,j_i,k,j_k} = \frac{w - d_{i,j_i}}{w - d_{k,j_k}}, \tag{3.13}$$

$$t_{i,k} = \frac{t - c_i}{t - c_k}, \tag{3.14}$$

$$w_{i,j_i,k,j_k} - t_{i,k} = u_{i,j_i,k,j_k}^{p^s} - u_{i,j_i,k,j_k}, \tag{3.15}$$

$$\frac{1}{w_{i,j_i,k,j_k}} - \frac{1}{t_{i,k}} = v_{i,j_i,k,j_k}^{p^s} - v_{i,j_i,k,j_k}. \tag{3.16}$$

*Тогда $w = t^{p^a}$ для некоторого натурального числа $a \geq 0$.*

**Доказательство.** Сначала мы покажем, что предположения этой леммы влекут, что $w, u_{i,j_i,k,j_k}$, $v_{i,j_i,k,j_k}, u, v \in FM$. Затем, для получения требуемого утверждения мы применим лемму 2.6 из [34] в случае $p > 2$ и лемму 3.5 из [13] в случае $p = 2$. Чтобы показать, что $w \in FM$, достаточно показать, что $w \in C_{K,i}$, $i = 2, \ldots, n$, поскольку $\bigcap_{i=2}^{n} C_{K,i} = FM$ согласно предложению 3.2.

Для каждого $l = 2, \ldots, n$, зафиксируем $d + 2$ значений $h$ таким образом, чтобы для некоторого значения $j_h$ функция $w - d_{h,j_h}$ не делилась бы ни на какой простой из поля $\tilde{K}_l$ (рассматриваемого как поле функций от $u_l$), разветвленный в расширении $\tilde{K}_l/\tilde{C}_l(u_l)$. Такие значения $h$ существуют, поскольку общее число возможных значений $h$ больше, чем $2g_l + d + 6$, и при $h_1 \neq h_2$ для всех $j_{h_1}, j_{h_2}$ функции $w - d_{h_1,j_{h_1}}$ и $w - d_{h_2,j_{h_2}}$ не могут иметь общих дивизоров нулей. Заметим, что каждый разветвленный простой исключает только одно значение $h$. Следовательно, всего может быть исключено $g_l$ значений, что оставляет более чем $d + 2$ значения для индексов. Пусть $h_1, \ldots, h_{d+2}$ выбраны так, чтобы для любого значения $j_{h_r}$ функции $w - d_{h_r,j_{h_r}}$ не имели нулей в простых, разветвленных в расширении $\tilde{K}/\tilde{C}_l(u_l)$. Положим $k = h_1$ и возьмем $i \in \{h_2, \ldots, h_{d+2}\}$. Далее заметим, что уравнения (3.11)–(3.16) справедливы при $k = h_1$ для некоторого $j_{h_1}$ и при всех $i \in \{h_2, \ldots, h_{d+2}\}$ для некоторых $j_i$. Рассмотрим следующие уравнения:

$$w_{i,j_i,k,j_k} = \frac{w - d_{i,j_i}}{w - d_{k,j_k}} = \frac{w - d_{k,j_k} + d_{k,j_k} - d_{i,j_i}}{w - d_{k,j_k}} = 1 + \frac{d_{k,j_k} - d_{i,j_i}}{w - d_{k,j_k}}.$$

Заметим, что по предположению для $i \neq k$ имеем $d_{k,j_k} - d_{i,j_i} \neq 0$. Далее, $t_k \in C_{K,j}$ при $j = 2, \ldots, n$. Таким образом, по лемме 3.3. имеем $w - d_{k,j_k} \in C_{K,j}$ при $j = 2, \ldots, n$. Следовательно, $w \in \bigcap_{j=2}^{n} C_{K,j} = FM$. Наконец, $u_{i,j_i,k,j_k}, v_{i,j_i,k,j_k}, v, u$ являются алгебраическими над $FM$, и значит, лежат в $FM$, поскольку поле $FM$ алгебраически замкнуто в $K$.

**3.6. Следствие.** *Множество* $\{x \in K | \exists a \in \mathbb{N} x = t^{p^a}\}$ *является диофантовым над* $K$.

**Доказательство.** Доказательство этого следствия идентично доказательству следствия 2.7 из [34].

Следующая лемма аналогична лемме 2.8 из [34] и лемме 4.4 из [13] однако нам приходится дополнить некоторые детали, в основном касающиеся того факта, что мы более не предполагаем, что простые, составляющие дивизор функции $t$ остаются простыми в $K$ (хотя мы предполагаем, что они неразветвлены).

**3.7. Лемма.** *Пусть $\sigma, \mu \in K$. Предположим, что все простые, являющиеся полюсами $\sigma$ или $\mu$, неразветвлены в расширении $\tilde{K}/\tilde{C}_K(t)$. Далее предположим, что справедливо следующее равенство:*

$$t(\sigma^{p^s} - \sigma) = \mu^{p^s} - \mu, \tag{3.17}$$

*где $s = 2$ для $p = 2$ и $s = 1$ для $p > 2$. Тогда $\sigma^{p^s} - \sigma = \mu^{p^s} - \mu = 0$.*

**Доказательство.** Рассмотрим это уравнение над $\tilde{K}$. Пусть $\mathfrak{A}$, $\mathfrak{B}$ – такие взаимно простые друг с другом и с $\mathfrak{P}_1, \dots, \mathfrak{P}_l, \mathfrak{Q}_1, \dots, \mathfrak{Q}_s$ целые дивизоры поля $\tilde{K}$, что дивизор элемента $\sigma$ имеет вид $\frac{\mathfrak{A}}{\mathfrak{B}} \prod \mathfrak{P}_f^{a_f} \prod \mathfrak{Q}_g^{b_g}$, где $a_f, b_g \in \mathbb{Z}$. Тогда нетрудно видеть, что для некоторого целого дивизора $\mathfrak{C}$, взаимно простого с $\mathfrak{B}$, и с $\mathfrak{P}_1, \dots, \mathfrak{P}_l, \mathfrak{Q}_1, \dots, \mathfrak{Q}_s$, дивизор элемента $\mu$ имеет вид $\frac{\mathfrak{C}}{\mathfrak{B}} \prod \mathfrak{P}_f^{d_f}$ $\prod \mathfrak{Q}_g^{e_g}$, где $d_f, e_g \in \mathbb{Z}$. Действительно, пусть $\mathfrak{t}$ – такой полюс $\mu$, что $\mathfrak{t} \notin \{\mathfrak{P}_1, \dots, \mathfrak{P}_l, \mathfrak{Q}_1, \dots, \mathfrak{Q}_s\}$. Тогда

$$0 > p^s \mathrm{ord}_{\mathfrak{t}} \mu = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^s} - \mu) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^{p^s} - \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\sigma^{p^s} - \sigma) = p^s \mathrm{ord}_{\mathfrak{t}} \sigma.$$

И наоборот, пусть $\mathfrak{t}$ – полюс $\sigma$, такой, что $\mathfrak{t} \notin \{\mathfrak{P}_1, \dots, \mathfrak{P}_l, \mathfrak{Q}_1, \dots, \mathfrak{Q}_s\}$. Тогда

$$0 > p^s \mathrm{ord}_{\mathfrak{t}} \sigma = \mathrm{ord}_{\mathfrak{t}}(\sigma^{p^s} - \sigma) = \mathrm{ord}_{\mathfrak{t}}(t(\sigma^{p^s} - \sigma)) = \mathrm{ord}_{\mathfrak{t}}(\mu^{p^s} - \mu) = p^s \mathrm{ord}_{\mathfrak{t}} \mu.$$

Наконец, заметим, что для некоторого $f = 1, \dots, a$ мы имеем $\mathrm{ord}_{\mathfrak{P}_f} \sigma < 0$ тогда и только тогда, когда для этого же $f$ имеем $\mathrm{ord}_{\mathfrak{P}_f} t(\sigma^{p^s} - \sigma) \cong 1 \mod p^s$ и $\mathrm{ord}_{\mathfrak{P}_f} t(\sigma^{p^s} - \sigma) < 0$. Последнее неравенство справедливо тогда и только тогда, когда $\mathrm{ord}_{\mathfrak{P}_f}(\mu^{p^s} - \mu) < 0$ и $\mathrm{ord}_{\mathfrak{P}_f}(\mu^{p^s} - \mu) \cong 0 \mod p$. Аналогичным образом, если для некоторого $g$ имеем $\mathrm{ord}_{\mathfrak{Q}_g} \sigma < 0$, то для этого же $g$, $\mathrm{ord}_{\mathfrak{Q}_g} t(\sigma^{p^s} - \sigma) \cong -1 \mod p^s$ и $\mathrm{ord}_{\mathfrak{Q}_f}(\mu^{p^s} - \mu) \cong 0 \mod p^s$. Следовательно, для всех $f = 1, \dots, l$ и $g = 1, \dots, s$ имеем $a_f \geq 0, b_g \geq 0, d_f \geq 0, e_g \geq 0$.

Согласно сильной теореме об аппроксимации существует такой элемент $b \in K$, что дивизор $b$ имеет вид $\mathfrak{B}\mathfrak{D}/\mathfrak{Q}_1^k$, где $\mathfrak{D}$ – целый дивизор, взаимно простой с $\mathfrak{A}$, $\mathfrak{C}$, $\mathfrak{P}_1, \dots, \mathfrak{P}_l, \mathfrak{Q}_1, \dots, \mathfrak{Q}_s$, а $k$ – натуральное число. Тогда $b\sigma = s_1, b\mu = s_2$, где $s_1, s_2$ являются целыми над $C_K[t]$. Действительно, рассмотрим дивизоры для

$s_1 = b\sigma$:

$$\frac{\mathfrak{B}\mathfrak{D}}{\mathfrak{Q}_1^k}\frac{\mathfrak{A}}{\mathfrak{B}}\prod \mathfrak{P}_f^{a_f}\prod \mathfrak{Q}_g^{b_g} = \frac{\mathfrak{D}\mathfrak{A}\prod \mathfrak{P}_f^{a_f}\prod \mathfrak{Q}_g^{b_g}}{\mathfrak{Q}_1^{k-b_1}}$$

Следовательно, $\mathfrak{Q}_1$ – единственный полюс функции $s_1$, делающий ее целой над $C_K[t]$. Аналогичное рассуждение применимо и к $s_2$.

Умножая на $b^{p^s}$, мы получаем следующее равенство:

$$t(s_1^{p^s} - b^{p^s-1}s_1) = s_2^{p^s} - b^{p^s-1}s_2. \tag{3.18}$$

Теперь можно переписать (3.18) в виде

$$(s_1^{p^s}t - s_2^{p^s}) = b^{p^s-1}(s_1 t - s_2). \tag{3.19}$$

Пусть $\mathfrak{t}$ – произвольный простой сомножитель $\mathfrak{B}$ в $\tilde{K}$. Тогда $\mathfrak{t}$, как полюс $\sigma$ и $\mu$, не разветвляется в расширении $\tilde{K}/C_{\tilde{K}}(t)$. Далее, так как $p^s - 1 \geq 2$, то $\mathrm{ord}_{\mathfrak{t}}(s_1^{p^s}t - s_2^{p^s}) \geq 2$. Так как $\mathfrak{t}$ не разветвлен в расширении $\tilde{K}/C_{\tilde{K}}(t)$, то по лемме 4.4 из [31] имеем $\mathrm{ord}_{\mathfrak{t}} d(s_1^{p^s}t - s_2^{p^s})/dt > 0$. Но $d(s_1^{p^s}t - s_2^{p^s})/dt = s_1^{p^s}$. По построению, дивизор функции $s_1$ не содержит простых из $\mathfrak{B}$. Таким образом, $\mathfrak{B}$ – тривиальный дивизор. Значит, $\sigma, \mu$ не имеют полюсов и, следовательно, являются константами. Но левая часть равенства (3.17) является константой тогда и только тогда, когда $\sigma^{p^s} - \sigma = 0$. Следовательно, также и $\mu^{p^s} - \mu = 0$.

Имея в распоряжении леммы (3.5) и (3.7), можно продолжить в точности так же, как в [34] и [13], и доказать следующую теорему.

**3.8. Теорема.** *Множество $P(K) = \{(x, y) \in K^2 | \exists s \in \mathbb{N}\, y = x^{p^s}\}$ является диофантовым над $K$.*

**3.9. Предложение.** *Пусть $K_0$ – поле функций сепарабельно порожденное над полем констант $C_{K_0}$, и удовлетворяющее предположениям из раздела "Обозначения и предположения 3.1", но не обязательно удовлетворяющим предположениям из раздела "Обозначения и предположения 3.4". Тогда $K_0$ обладает конечным сепарабельным расширением $K$, таким, что множество $\{(x, y) \in K^2 | \exists s \in \mathbb{N}\, y = x^{p^s}\}$ является диофантовым над $K$.*

**Доказательство.** Мы покажем, что существует конечное сепарабельное расширение $K$ поля $K_0$, для которого выполнены предположения 3.4. Пусть $C_0$ – алгебраическое замыкание конечного поля в $K_0$. Пусть $F_0$ – алгебраическое замыкание поля $C_0(u_1)$ в $K_0$. Мы должны рассмотреть два случая: поле $C_0$ бесконечно и поле $C_0$ конечно. В первом случае согласно теореме 6.11 из [34] существует такое конечное расширение $C$ поля $C_0$, что поле $F = CF_0$ содержит элемент $t$ и бесконечно много констант $c_0 = 0, c_1, \dots$, для которых дивизор функции $t + c_i$ в $F$ имеет вид $\mathfrak{p}_i/\mathfrak{q}$, где степень обоих простых равна $p^h$ для некоторого неотрицательного целого числа $h$. Положим $K = FK_0$. Так как имеется бесконечно много констант $c_i$, и каждая константа $c_i$ имеет только конечное число $p^s$-ых степеней, то можно выбрать $c_0, \dots, c_m$, где $m > d + 6 + [K : C_K(t)] + g + g_2 + \dots + g_n$, так, чтобы $c_i^{p^s} \neq c_j$ для всех $i \neq j$ и для всех $s \in \mathbb{N}$.

Теперь рассмотрим случай, когда поле $C_0$ конечно. Пусть $F_0$ – алгебраическое замыкание поля $C_0(u_1)$ в $K_0$. Пусть $C'_0$ – поле, получающееся из $C_0$ добавлением корней всех неприводимых многочленов, степень которых не делится на $p$. Тогда из свойств конечных полей (см. теорему 13 на стр. 185 книги [19]) следует, что $C'_0$ является бесконечным полем, обладающим расширением степени $p$, и что расширение $C'_0/C_0$ алгебраическое и сепарабельное. Положим $F'_0 = C'_0F_0$. Тогда расширение $F'_0/F_0$ также алгебраическое и сепарабельное, и по теореме 13 на стр. 281 книги [1] поле констант поля $F'_0$ бесконечно и совпадает с $C'_0$. Далее, рассуждения, подобные приведенным выше показывают, что для поля $F'_0$ существует конечное сепарабельное расширение $F'$, получающееся расширением поля констант, такое, что $F'$ содержит неконстантный элемент $t$ и константы $c_0 = 0, c_1, \dots, c_{m'}$, удовлетворяющие всем требованиям обозначений 3.4 при $m' > d_0 + 6 + [K' : C_{K'}(t)] + g' + g'_2 + \dots + g'_n$, где $d_0 = [K_0 : C_0(u_1, \dots, u_n)]$, $g'$ – число простых, разветвленных в расширении $\tilde{K}'/\tilde{C}_{K'}(t)$, а $g'_i$ – число простых, разветвленных в расширении $\tilde{K}'_i/\tilde{C}_{K',i}(u_i)$. (Здесь $C'$ есть поле констант поля $F'$, $K' = F'K_0 = C'K_0$, а $\tilde{K}', \tilde{C}_{K'}, \tilde{C}_{K',i}, \tilde{K}'_i$ определены по аналогии с $\tilde{K}, \tilde{C}_K, \tilde{C}_{K,i}, \tilde{K}_i$.) Так как расширение $C'/C$ сепарабельно, то вновь по теореме 13 на стр. 281 из [1] имеем $C_{K'} = C'C_{K_0}$.

Так как $F'/F'_0$ и $F'_0/F_0$ являются конечным и алгебраическим, соответственно, сепарабельными расширениями, получающимися расширениями полей констант, то $F'/F_0$ – (бесконечное) алгебраическое сепарабельное расширение, получающееся расширением поля констант. Положим $F = F_0(t, c_0, \dots, c_{m'}) \subset F'$. Тогда

$F/F_0$ – конечное сепарабельное расширение, получающееся расширением поля констант. Пусть $C$ – поле констант для $F$. Тогда $C \subset C'$, и $C'/C$ есть сепарабельное алгебраическое расширение. Положим $K = CK_0$. Тогда $C_K = C_{K_0}C$, вновь по теореме 13 на стр. 281 из [1]. Далее, $C_K \subset C_{K'}$, и $C_{K'}/C_K$ – алгебраическое расширение. Аналогичным образом, $C_{K,i} \subset C_{K',i}$, и $C_{K',i}/C_{K,i}$ – алгебраическое расширение. Следовательно, $\tilde{C}_{K'} = \tilde{C}_K$, $\tilde{C}_{K',i} = \tilde{C}_{K,i}, \tilde{K} = \tilde{K}', \tilde{K}_i = \tilde{K}'_i$. Таким образом, $g' = g, g_i = g'_i$ и $d_0 \geq d$.

Так как $F'/F$ – сепарабельное (бесконечное) расширение, получающееся расширением поля констант, то по теореме 9 на стр. 279 из [1] все дивизоры поля $F$ сохраняют свою степень в $F'$. Рассмотрим дивизоры полюсов и нулей функции $t$ в $F'$. По построению, оба дивизора являются простыми дивизорми степени $p^h$ для некоторого $h \in \mathbb{N}$. Следовательно, то же самое утверждение верно и для дивизоров полюсов и нулей функции $t$ в $F$. Аналогичным образом, дивизоры нулей функций $t + c_i, i = 1, \ldots, m$, в $F$ также являются простыми дивизорами степени $p^h$.

Далее мы рассмотрим требование того, чтобы полюс и нуль функции $t$ не разветвлялись в расширении. По построению $m$, для некоторых $c_1 \neq c_2$ функция $\frac{t+c_1}{t+c_2}$ имеет нуль и полюс в простых, не разветвляющихся в расширении $\tilde{K}/\tilde{C}_K(t)$. Положим $t' = \frac{t+c_1}{t+c_2}$. Тогда $C_K(t') = C_K(t)$, и можно подобрать $c_0 = 0, c'_1, \ldots, c'_m$, удовлетворяющие всем требованиям относительно $t'$.

Наконец, положим $K = FK_0$. Тогда предположения из раздела предположения и обозначения 3.4 выполнены по построению $F$, и теорема 3.8 справедлива для $K$. С другой стороны, так как $F/F_0$ – конечное сепарабельное расширение, то же самое верно и для расширения $K/K_0$, поскольку поле $F_0$ алгебраически замкнуто в $K_0$.

**3.10. Следствие.** *Пусть $K_0$ – произвольное поле, удовлетворяющее предположениям из раздела "Обозначения и предположения 3.1." Тогда множество $P(K_0) = \{(x, y) \in K_0^2 | \exists s \in \mathbb{N}\, y = x^{p^s}\}$ является диофантовым над $K_0$.*

**Доказательство.** Сначала заметим, что $P(K_0) = P(K) \cap K_0^2$. Далее, используя метод "вверх и вниз"[3] (см. раздел 2.2 из [35)], заключаем, что множество $P(K) \cap K_0^2$ обладает диофантовым представлением над $K_0$.

[3] См. примечание на стр. 8. – *Прим. перев.*

## 4. Диофантова неразрешимость

**4.1. Теорема.** *Пусть $M$ – произвольное поле функций характеристики $p > 0$, такое, что алгебраическое замыкание $C$ конечного поля в $M$ обладает расширением степени $p$. Пусть $L$ – произвольное поле, конечно порожденное над $C$, такое что $L$ и $M$ линейно разделены над $C$. Положим $K = ML$. Тогда диофантова проблема поля $K$ неразрешима.*

**Доказательство.** Прежде всего заметим, что согласно следствию 9.6 на стр. 111 из [14], поле $L$ сепарабельно порождено над $C$, и следовательно, поле $K$ удовлетворяет предположениям из раздела "Обозначения и предположения 3.1." Таким образом, множество $P(K)$ диофантово над $K$ по следствию 3.10. Пусть теперь $u$ – часть разделяющего трансцендентного базиса поля $L$ над $C$. Рассмотрим $K$ как поле функций от переменной $u$. Иными словами, если $u_1 = u, u_2, \dots, u_n$ – разделяющий трансцендентный базис поля $L$ над $C$, то возьмем в качестве $C_K$ алгебраическое замыкание поля $M(u_2, \dots, u_k)$ в $K$ и заметим, нчто $K/C_K(u)$ есть конечное сепарабельное расширение. Пусть $F$ – алгебраическое замыкание поля $C(u)$ в $K$. Тогда по теореме 2.5 для всех за исключением конечного числа простых $\mathfrak{p}_F$ поля $F$ существует диофантово над $K$ множество $A \subset K$, такое, что если элемент $w \in A$, то $w$ целый во всех сомножителях дивизора $\mathfrak{p}_F$ в $K$, тогда как все $w \in F$, целые в $\mathfrak{p}_F$, лежат в $A$. Таким образом, согласно предложению 1.6, диофантова проблема поля $K$ неразрешима.

## 5. Приложение

**5.1. Лемма.** *Пусть $K, F, u, C, C_K$ таковы, как в обозначениях 1.5. Пусть $\mathfrak{q}$ – простой дивизор поля $F$. Тогда в $K$ имеется по крайней мере один простой над $\mathfrak{q}$. Далее, имеется лишь конечное число простых в $K$, лежащих над $\mathfrak{q}$. Наконец, все кроме конечного числа простых из $F$ не разветвлены в расширении $K/F$.*

**Доказательство.** Существование в $K$ по крайней мере одного простого, лежащего над $\mathfrak{q}$, следует из теоремы 1 на стр. 52 из [3]. Пусть $\mathfrak{Q}$ – некий простой из $C(u)$, лежащий под $\mathfrak{q}$. Не умаляя общности предположим, что $\mathfrak{Q}$ не является полюсом $u$, и следовательно, отвечает неприводимому многочлену $P(u)$ от переменной $u$. Так как поле $C$ алгебраически замкнуто в $C_K$, то $P(u)$ остается простым в $C_K(u)$, и следовательно, в $C_K(u)$ имеется только один простой $\bar{\mathfrak{Q}}$ над $\mathfrak{Q}$. Таким образом, простые $\mathfrak{q}_i$ из $K$ лежат над $\bar{\mathfrak{Q}}$ тогда и только тогда они лежат над $\mathfrak{Q}$. Следовательно, вновь по теореме 1 на стр. 52 из [3] %цитеЦ имеется только конечное число простых из $K$, лежащих над $\mathfrak{Q}$. По лемме 2 на стр. 71 из [3] лишь конечное число простых $\bar{\mathfrak{Q}}$ может разветвляться в расширении $K/C_K(u)$. Таким образом, лишь конечное число простых может разветвляться в расширении $K/C(u)$. Так как каждый простой из $K$, лежащий над $\mathfrak{q}$, также лежит над $\mathfrak{Q}$, отсюда следует заключение леммы.

**5.2. Лемма.** *Пусть $N/G$ – циклическое расширение полей функций. Пусть $\mathfrak{p}$ – простой дивизор поля $G$, остающийся простым в этом расширении. Тогда, если $y \in G$ и $\mathbf{N}_{N/G}(x) = y$, для некоторого $x \in N$ то $\mathrm{ord}_{\mathfrak{p}} y \cong 0 \mod [N:G]$.*

**Доказательство.** Пусть $x, y$ удовлетворяют условиям леммы. Пусть $\mathfrak{P}$ – простой дивизор в $N$, лежащий над $\mathfrak{p}$. Пусть $\mathfrak{P}^a\mathfrak{U}$ – дивизор функции $x$, где $a \in \mathbb{Z}$, а $\mathfrak{U}$ – дивизор в $N$, взаимно простой с $\mathfrak{P}$. Тогда дивизор нормы $\mathbf{N}_{N/G}(x)$ есть $\mathbf{N}_{N/G}(\mathfrak{P}^a\mathfrak{U}) = \mathbf{N}_{N/G}(\mathfrak{P}^a)\mathbf{N}_{N/G}(\mathfrak{U}) = \mathfrak{P}^{fa}\mathbf{N}_{N/G}(\mathfrak{U})$, где $f$ – относительная степень дивизора $\mathfrak{P}$ над $\mathfrak{p}$. (См. стр. 35–37 в [15]). Так как по предеположению дивизор $\mathfrak{p}$ остается простым в расширении $N/G$, то $f = [N:G]$.

**5.3. Лемма.** *Пусть $L/N$ – сепарабельное расширение полей функций, получающееся расширением поля констант. Тогда ни один простой из $N$ не разветвляется в этом расширении.*

**Доказательство.** Предположим, что $\mathfrak{p}$ – простой дивизор поля $N$, разветвляющийся в этом расширении. Тогда в $L$ существует такой простой $\mathfrak{P}$, что $\mathfrak{P}^2$ появляется в разложении $\mathfrak{p}$ на множители. Пусть элемент $x \in N$ таков, что $\mathrm{ord}_{\mathfrak{P}} x = 1$. Рассмотрим расширения $L/N(x)$ и $N(x)/N$. Пусть $\mathfrak{P}_x$ – простой, лежащий в $N(x)$ под $\mathfrak{P}$ (и над $\mathfrak{p}$ в $N(x)$). Тогда $e(\mathfrak{P}/\mathfrak{P}_x) = 1$, и следовательно, $\mathfrak{p}$ должен быть разветвлен в расширении $N(x)/N$. Таким образом, не умаляя общности, можно считать, что расширение $L/N$ конечно. Пусть $C_L$ – поле констант поля $L$, и $\alpha \in C_L$ – элемент, порождающий это расширение. Тогда по предложению 7.7 на стр. 33 из [15] степенной базис, порожденный $\alpha$, является целым базисом по отношению к каждому простому из $N$. Далее, так как никакой простой не делит дискриминант этого базиса, то по лемме 2 на стр. 71 из [3] никакой простой не разветвляется в этом расширении. Таким образом мы получаем противоречие с нашим предположением относительно $\mathfrak{p}$.

**5.4. Лемма.** *Пусть $u, \beta, h, \alpha, z, C, F, w$ таковы, как в обозначениях 2.1. Предположим, что $w \in F$. Тогда существует поле $G \subseteq F$, удовлетворяющее следующим требованиям:*

(1) *Поле $G$ – глобальное поле, содержащее $h$.*
(2) *Никакой простой из $G$ не разветвляется в расширении $F(\beta)/G$. Расширение $F(\beta)/G$ является сепарабельным (но необязательно конечным) расширением поля констант.*
(3) *Степень элемента $\alpha$ над $G$ равна $p$.*

**Доказательство.** Так как $F/C(u)$ – конечное сепарабельное расширение, и $F(\beta)/F$ – конечное сепарабельное расширение, то $F(\beta)/C(u)$ является простым расширением. Пусть $\gamma$ – образующий элемент этого расширения. Пусть $A_0, \dots, A_s \in C(u)$ – коэффициенты нормированного неприводимого многочлена для $\gamma$ над $C(u)$. Пусть $C_{finite} \subset \tilde{C}$ – наименьшее поле, содержащее $F_{p^2}$ (конечное поле из $p^2$ элементов) и коэффициенты нормированного неприводимого многочлена для $\alpha$ над $C$, и такое, что $A_1, \dots, A_s \in C_{finite}(u)$. Тогда $C_{finite}$ – конечное поле, и $C_{finite} \subseteq C$. Положим $G = C_{finite}(u, \gamma, w) \subset F(\beta)$. Тогда $G$ является глобальным полем. Пусть $C_G$ – это поле констант поля $G$. Так как поле констант поля $F(\beta)$ есть $C$ (см. доказательство теоремы 2.3), то $C_G \subset C$. Теперь рассмотрим следующую диаграмму полей.

$$\begin{array}{ccc} G & \longrightarrow & F(\beta) \\ \downarrow & & \downarrow \\ C_G(u) & \longrightarrow & C(u) \end{array}$$

Утверждаем, что $F(\beta)/G$ – расширение, получающееся расширением поля констант. Другими словами, $F(\beta) = CG$. Действительно, это следует из того, что $F(\beta) = C(u, \gamma) \subseteq CG = CC_G(u, \gamma, w)$. Так как поле $C$ совершенно, то это поле расширения констант является сепарабельным. Таким образом, согласно лемме 5.3 никакой простой не разветвляется в расширении $F(\beta)/G$.

**5.5. Лемма.** *Пусть $F$ – поле функций, $\mathfrak{q}$ – произвольный простой поля $F$, а $p$ – произвольное рациональное простое число. Тогда су-*

*ществует элемент* $f \in F$ *с* $F$*-дивизором вида* $\frac{\mathfrak{q}_F^a}{\prod \mathfrak{t}_i^{a_i}}$, *где* $\mathfrak{t}_i \neq \mathfrak{q}$ *для всех* $i$, *а* $a \not\equiv 0 \mod p$.

**Доказательство.** По следствию к теореме Римана–Роха (см. 4(d), на стр. 20 в [14]) для достаточно больших $a$ размерность (как векторного пространства над полем констант) множества всех функций с единственным полюсом в $\mathfrak{q}$ порядка, не превосходящего $a$, и целых во всех остальных простых равна $a \deg(\mathfrak{q}) - g + 1$, где $g$ – род $F$. В то же самое время, для достаточно больших $a$ размерность (как векторного пространства на полем констант) множества всех функций с единственным полюсом в $\mathfrak{q}$ порядка строго меньшего $a$ и целых во всех остальных простых равна $(a-1)\deg(\mathfrak{q}) - g + 1$. Следовательно, для достаточно больших $a \in \mathbb{N}$ множество функций с единственным полюсом в $\mathfrak{q}$ порядка в точности $a$ непусто.

**5.6. Лемма.** *Пусть* $F$ *– поле функций от одной переменной. Пусть* $s \in \mathbb{N}$, $w \in F$, *а* $\mathfrak{P}_F$ *– простой дивизор поля* $F$. *Если* $\mathrm{ord}_{\mathfrak{P}_F}(w^{p^s} - w) < 0$, *то* $\mathrm{ord}_{\mathfrak{P}_F} w < 0$ *и* $\mathrm{ord}_{\mathfrak{P}_F}(w^{p^s} - w) \cong 0 \mod p^s$.

**Доказательство.** Если $\mathrm{ord}_{\mathfrak{P}_F}(w^p - w) < 0$, то $\mathrm{ord}_{\mathfrak{P}_F} w < 0$ и $\mathrm{ord}_{\mathfrak{P}_F}(w^p - w) = \mathrm{ord}_{\mathfrak{P}_F}(w^p) \cong 0 \mod p$.

## Литература


1. E. Artin, *Algebraic Numbers and Algebraic Functions.* — Gordon Breach Science Publishers, New York (1986).
2. J. W. S Cassels and A. Frölich, *Algebraic Number Theory.* — Thompson Book Co, Washington, D. C. (1967).
3. C. Chevalley, *Introduction to the theory of Algebraic Functions of One Variable*, vol. 6 of *Mathematical Surveys.* — AMS, Providence, RI, 1951.
4. J.-L. Colliot-Thélène, A. Skorobogatov, and P. Swinnerton-Dyer, *Double fibres and double covers: Paucity of rational points.* — *Acta Arithmetica*, **79** (1997), 113–135.
5. G. Cornelissen and K. Zahidi, *Topology of diophantine sets: Remarks on Mazur's conjectures.* — In: Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, vol. 270 of *Contemporary Mathematics*, pages 253–260. American Mathematical Society, 2000.
6. M. Davis, *Hilbert's tenth problem is unsolvable.* — American Mathematical Monthly, **80** (1973), 233–269.
7. M. Davis, Yurii Matijasevich, and Julia Robinson, *Positive aspects of a negative solution.* — In *Proc. Sympos. Pure Math.*, vol. 28, pages 323– 378. Amer. Math. Soc., 1976.
8. J. Denef, *Hilbert's tenth problem for quadratic rings.* — Proc. Amer. Math. Soc., **48** (1975), 214–220.

9. J. Denef, *The diophantine problem for polynomial rings and fields of rational functions.* — Transactions of American Mathematical Society, **242** (1978), 391–399.
10. J. Denef, *The diophantine problem for polynomial rings of positive characteristic.* — In: M. Boffa, D. van Dalen, and K. MacAloon, editors, *Logic Colloquium 78*, pages 131 –145. North Holland (1979).
11. J. Denef, *Diophantine sets of algebraic integers,* II. — Transactions of American Mathematical Society, **257** (1) (1980), 227–236.
12. J. Denef and L. Lipshitz, *Diophantine sets over some rings of algebraic integers.* — Journal of London Mathematical Society, **18** (2) (1978), 385–391.
13. K. Eisenträeger, *Hilbert's tenth problem for algebraic function fields of characteristic* 2. — To appear.
14. M. Fried and M. Jarden, *Field Arithmetic.* — Springer-Verlag, New York (1986).
15. G. Janusz, *Algebraic Number Fields.* — Academic Press, New York (1973).
16. H. K. Kim and F. W. Roush, *Diophantine undecidability of* $\mathbb{C}(t_1, t_2)$. — Journal of Algebra, **150** (1) (1992), 35–44.
17. H. K. Kim and F. W. Roush, *Diophantine unsolvability for function fields over certain infinite fields of characteristic* $p$. — Journal of Algebra, **152** (1) (1992), 230–239.
18. H. K. Kim and F. W. Roush, *Diophantine unsolvability over p-adic function fields.* — Journal of Algebra, **176** (1995), 83–110.
19. S. Lang, *Algebra.* — Addison Wesley, Reading, Ma (1971).
20. B. Mazur, *The topology of rational points.* — Experimental Mathematics, **1** (1) (1992), 35–45.
21. B. Mazur, *Questions of decidability and undecidability in number theory.* — Journal of Symbolic Logic, **59** (2) (June 1994), 353–371.
22. B. Mazur, *Speculation about the topology of rational points: An up-date.* — Asterisque, **228** (1995), 165–181.
23. B. Mazur, *Open problems regarding rational points on curves and varieties.* — In: A. J. Scholl and R. L. Taylor, editors, *Galois Representations in Arithmetic Algebraic Geometry.* Cambridge University Press (1998).
24. Th. Pheidas, *An undecidability result for power series rings of positive characteristic.* II. — Proc. Amer. Math. Soc., **100** (3) (1987), 526–530.
25. Th. Pheidas, *Hilbert's tenth problem for a class of rings of algebraic integers.* — Proceedings of American Mathematical Societ, **104** (2) (1988), 611–620.
26. Th. Pheidas, *Hilbert's tenth problem for fields of rational functions over finite fields.* — Inventiones Mathematicae, **103** (1991), 1–8.
27. H. Shapiro and A. Shlapentokh, *Diophantine relations between algebraic number fields.* — Communications on Pure and Applied Mathematics, XLII:1113–1122 (1989).
28. A. Shlapentokh, *Extension of Hilbert's tenth problem to some algebraic number fields.* — Communications on Pure and Applied Mathematics, XLII:939–962 (1989).
29. A. Shlapentokh, *Diophantine undecidability in some rings of algebraic numbers of totally real infinite extensions of* $\mathbb{Q}$. — Annals of Pure and Applied Logic, **68** (1994), 299–325.
30. A. Shlapentokh, *Algebraic and turing separability of rings.* — Journal of Algebra, **185** (1996), 229–257.

31. A. Shlapentokh, *Diophantine undecidability of algebraic function fields over finite fields of constants.* — Journal of Number Theory, **58** (2) (June 1996), 317–342.
32. A. Shlapentokh, *Diophantine definability over some rings of algebraic numbers with infinite number of primes allowed in the denominator.* — Inventiones Mathematicae, **129** (1997), 489–507.
33. A. Shlapentokh, *Defining integrality at prime sets of high density in number fields.* — Duke Mathematical Journal, **101** (1) (2000), 117–134.
34. A. Shlapentokh, *Hilbert's tenth problem for algebraic function fields over infinite fields of constants of positive characteristic.* — Pacific Journal of Mathematics, **193** (2) (2000), 463–500.
35. A. Shlapentokh, *Hilbert's tenth problem over number fields, a survey.* — In: Jan Denef, Leonard Lipshitz, Thanases Pheidas, and Jan Van Geel, editors, *Hilbert's Tenth Problem: Relations with Arithmetic and Algebraic Geometry*, vol. 270 of *Contemporary Mathematics*, pages 107–137. American Mathematical Society (2000).
36. A. Shlapentokh, *Diophantine undecidability of function fields of characteristic greater than 2 finitely generated over a field algebraic over a finite field.* — Compositio Mathematica, **132** (1) (May 2002), 99–120.
37. A. Shlapentokh, *On diophantine definability and decidability in large subrings of totally real number fields and their totally complex extensions of degree 2.* — Journal of Number Theory, **95** (2002), 227–252.
38. A. Shlapentokh, *A ring version of Mazur's conjecture on topology of rational points.* — International Mathematics Research Notices, 2003:7: 411–423 (2003).
39. C. Videla, *Hilbert's tenth problem for rational function fields in characteristic 2.* — Proceedings of the American Mathematical Society. — **120** (1) (January 1994) 249–253.
40. A. Weil, *Basic Number Theory.* — Springer-Verlag (1974).
41. K. Zahidi, *The existential theory of real hyperelliptic fields.* — Journal of Algebra, **233** (1) (2000), 65–86.

Shlapentokh A. Diophantine undecidability for some function fields of infinite transcendence degree and positive characteristic.

Let $M$ be a field of positive characteristic $p > 0$ such that $C$, the closure of a finite field in $M$, has an extension of degree $p$. Let $L$ be a field finitely generated over $C$ and such that $M$ and $L$ are linearly disjoint over $C$. Then Hilbert's Tenth problem is not decidable over $ML$.

Department of Mathematics
East Carolina University
*E-mail*: shlapentokha@mail.ecu.edu

Поступило 2 апреля 2003 г.