УДК 511.6

О ПРОБЛЕМЕ ПЕРИОДИЧНОСТИ РАЗЛОЖЕНИЯ В НЕПРЕРЫВНУЮ ДРОБЬ ЭЛЕМЕНТОВ ГИПЕРЭЛЛИПТИЧЕСКИХ ПОЛЕЙ СО СТЕПЕНЬЮ ФУНДАМЕНТАЛЬНОЙ S -ЕДИНИЦЫ НЕ ВЫШЕ 11

© 2021 г. Академик РАН В. П. Платонов^{1,2,*}, М. М. Петрушин^{1,**}, Ю. Н. Штейников^{1,***}

Поступило 26.08.2021 г.

После доработки 26.08.2021 г.

Принято к публикации 01.09.2021 г.

Решается проблема описания свободных от квадратов многочленов $f(x)$ с периодическим разложением $\sqrt{f(x)}$ в функциональную непрерывную дробь в $k((x))$, где k – числовое поле, при условии, что степень фундаментальной S -единицы соответствующего гиперэллиптического поля $k(x)(\sqrt{f(x)})$ не превосходит 11.

Ключевые слова: гиперэллиптическое поле, S -единицы, непрерывные дроби, периодичность, точки конечного порядка

DOI: 10.31857/S2686954321050088

ВВЕДЕНИЕ

Пусть поле k характеристики 0, и $f(x) \in k[x]$ – многочлен свободный от квадратов. В классическом случае функциональных непрерывных дробей в $k((1/x))$, первые результаты по которому были получены 200 лет назад Абелем и Чебышевым (см. [1–4]), важным элементом исследования свойств периодичности является элемент $\sqrt{f}$, где многочлен f определяет гиперэллиптическое поле $L = k(x)(\sqrt{f(x)})$. В отличие от классического случая, в случае непрерывных дробей в $k((x))$ наличие в поле L периодических элементов не гарантирует периодичности разложения элемента $\sqrt{f}$. В цикле работ по исследованию и нахождению элементов f с периодическим $\sqrt{f}$ было показано, что периодичность $\sqrt{f}$ – редкое явление, которое, впрочем, требует наличия нетривиальных S -единиц в соответствующем гиперэллиптическом поле L для множества нормирований S , индуцированного линейным многочленом x .

В работе [5] были найдены все такие многочлены f степени 3 с рациональными коэффициентами, рассматриваемые с точностью до естественной эквивалентности. В работах [6, 7] эти исследования были обобщены на числовые поля констант, и была полностью решена проблема периодичности $\sqrt{f}$ для квадратичных и числовых полей степени 3 над $\mathbb{Q}$, а также была доказана теорема конечности для расширений $\mathbb{Q}$ степени ≤ 6 . В работе [8] аналогичный результат был получен для случая многочленов f степени 4 над $\mathbb{Q}$, что завершило описание периодических $\sqrt{f}$ в эллиптическом случае над полем рациональных чисел. Аргументы и подходы работ [5–8] существенно опирались на параметризацию пар: эллиптическая кривая и точка с заданным порядком кручения (см. [9, 10]).

В случае многочленов f степени 5 и выше подобные параметризации неизвестны, и описание периодических $\sqrt{f}$ требует иных подходов. В работе [5] для гиперэллиптических полей, содержащих S -единицы малых степеней, с помощью метода, основанного на решении норменного уравнения, были получены рекуррентные соотношения на коэффициенты решения норменного уравнения. С помощью этих соотношений были найдены новые примеры $f \in \mathbb{Q}[x]$ с периодическим разложением $\sqrt{f}$ для произвольной степени f , причем в случае $\deg f = 3$ построенные примеры исчерпывали множество таких f . Однако даже уже в случае, когда многочлен имеет степень 3, для полей,

¹ Федеральный научный центр Научно-исследовательский институт системных исследований
Российской академии наук, Москва, Россия

² Математический институт им. В.А. Стеклова
Российской академии наук, Москва, Россия

*E-mail: platonov@mi-ras.ru

**E-mail: petrushkin@yandex.ru

***E-mail: yuriisht@yandex.ru

содержащих фундаментальные S -единицы нечетной степени начиная с 9, указанный выше метод становится вычислительно сложным.

В работе [11] был предложен новый эффективный метод для решения норменного уравнения, основанный на применении базисов Грёбнера. В [11] над произвольным полем k была показана конечность многочленов нечетной степени, отличной от 11, таких, что элемент $\sqrt{f}$ периодичен, а соответствующее гиперэллиптическое поле $k(x)(\sqrt{f})$ содержит S -единицу степени 11. Кроме того, было доказано, что в случае $k = \mathbb{Q}$ не существует многочленов нечетной степени отличной от 9 и 11 с указанными свойствами. В дальнейшем данный подход получил свое развитие в работе [14], где с помощью последовательных вычислений результатов и без использования параметризаций удалось получить альтернативное доказательство теоремы об описании кубических многочленов f над $\mathbb{Q}$ с периодическим разложением $\sqrt{f}$ в непрерывную дробь, а также были сделаны продвижения в обобщении полученных результатов на случай произвольных числовых полей.

В настоящей работе мы, развивая методы работы [11], решаем вышеописанную проблему для произвольной степени многочлена f , накладывая ограничение только лишь на степень фундаментальной S -единицы соответствующего гиперэллиптического поля. Отметим, что в [12] показано, что существование фундаментальной S -единицы является необходимым условием для наличия периодических элементов в поле L . В настоящей работе нами доказано, что если ограничить константой 11 степень соответствующей фундаментальной S -единицы, то для почти всех d не существует многочлена f степени d над произвольным числовым полем k с периодическим разложением $\sqrt{f}$ в непрерывную дробь в $k((x))$. Более того, нами явно приведены все многочлены f с периодическим $\sqrt{f}$ с указанным ограничением на степень соответствующей S -единицы. Оказывается, что с точностью до эквивалентности такой многочлен либо единственен для каждой пары d и фиксированной степени фундаментальной S -единицы соответствующего гиперэллиптического поля, либо это бесконечная серия $cx^d + 1$, $c \in k \setminus \{0\}$.

ОСНОВНЫЕ РЕЗУЛЬТАТЫ

Для неприводимого над k многочлена h определим дискретное нормирование v_h (элемента поля $k(x)$) равенством $v_h\left(h^m \frac{p}{q}\right) = m$, где взаимно простые многочлены p, q не делятся на h ; бесконечное нормирование, в свою очередь, определим равенством

$$v_\infty\left(\frac{p}{q}\right) = \deg q - \deg p.$$

Далее считаем, что $\deg h = 1$, и без ограничения общности положим $h = x$. Пусть нормирование v_x поля $k(x)$ имеет два продолжения v_x^+ и v_x^- на поле $L = k(x)(\sqrt{f})$. Поскольку в случае $\deg f = 2g + 1$ для $g \in \mathbb{N}$ бесконечное нормирование имеет одно продолжение, положим $S = \{v_x^+, v_\infty\}$. Группа S -целых элементов поля L называется группой S -единиц. Если существует хотя бы одна нетривиальная S -единица (т.е. отличная от константы поля k), то в описанном нами случае группа S -единиц является прямым произведением $k^\times$ и бесконечной циклической группы. Образующие этой циклической группы называются фундаментальными S -единицами. Для S -единицы $\alpha + \beta\sqrt{f}$, $\alpha, \beta \in k(x)$, выполнено $\alpha^2 - \beta^2 f = bx^m$, $b \in k \setminus \{0\}$, для некоторого целого m , называемого степенью S -единицы. Для фундаментальной S -единицы с положительной степенью m существует k -точка кручения порядка m в якобиане соответствующей гиперэллиптической кривой.

Будем говорить, что элементы поля L разлагаются в формальные степенные ряды $\sum_{j \geq s} \gamma_j x^j$, где $\gamma_j \in k$, если существует вложение L в поле формальных степенных рядов $k((x))$. Подробные сведения о разложении в ряд Лорана, функциональных непрерывных дробях и их связи с S -единицами содержатся в работе [3].

Под периодичностью разложения в непрерывную дробь мы понимаем периодичность последовательности полных частных. Периодичность разложения $\sqrt{f(x)}$ в непрерывную дробь равносильна периодичности $\sqrt{f^\sigma(x)}$, где $\sigma \in \text{Aut}(k/\mathbb{Q})$ — автоморфизм поля k постоянный на $\mathbb{Q}$, а также периодичности $\sqrt{a^2 f(bx)}$ для некоторых $a, b \in k \setminus \{0\}$. Поэтому мы будем рассматривать многочлены с точностью до эквивалентности, определяемой преобразованиями, указанными выше. Отношение эквивалентности зависит от поля k , и в зависимости от контекста мы будем рассматривать его или над $\overline{\mathbb{Q}}$, или над полем определения многочлена f . Мы будем называть полем определения многочлена f минимальное поле $k \subseteq \overline{\mathbb{Q}}$, содержащее все его коэффициенты.

Теорема 1. *Зафиксируем натуральное число $U \leq 11$. Для каждого нечетного d , $1 < d < U$, с точностью до эквивалентности существует не более одного бесквадратного многочлена $f \in \overline{\mathbb{Q}}[x]$, $\deg f = d$, для которого выполнены следующие условия:*

(i) разложение в непрерывную дробь в $\bar{\mathbb{Q}}((x))$ элемента $\sqrt{f}$ периодично;

(ii) гиперэллиптическое поле $L = \bar{\mathbb{Q}}(x)(\sqrt{f})$ содержит фундаментальную S -единицу степени U для $S = \{v_\infty, v_x^+\}$.

Все такие многочлены приводятся ниже.

В случае $\deg f = U$ такой многочлен единственен и равен $x^U + 1$. Многочленов с $\deg f = 1$ или $\deg f > U$ нечетной степени, удовлетворяющих условиям (i) и (ii), не существует.

Отметим, что если условия (i) и (ii) выполнены над $\bar{\mathbb{Q}}$, то они выполнены и над полем определения многочлена f . А множество таких многочленов для $\deg f = U$ над любым полем k , $[k : \mathbb{Q}] < \infty$, образует семейство $f = cx^U + 1$, $c \in k \setminus \{0\}$.

Перечислим все многочлены $f_{d,U}$, обладающие периодическим разложением $\sqrt{f_{d,U}}$ в непрерывную дробь, в условиях теоремы 2:

$$\begin{aligned} f_{3,5} &= 12x^3 - 8x^2 + 4x + 1, \\ f_{3,7} &= 6(9\sqrt{21} - 41)x^3 - 4(3\sqrt{21} - 13)x^2 + 4x + 1, \\ f_{3,8} &= 12x^3 - 5x^2 + 2x + 1, \\ f_{3,9} &= x^3 - (6z^2 + 6)x^2 + (249z^2 + 105z + 360)x + \\ &\quad + \frac{2397}{2}z^2 + \frac{2055}{4}z + \frac{3495}{2}, \\ f_{3,10} &= -120x^3 + 25x^2 + 2x + 1, \\ f_{3,11} &= x^3 + \frac{1}{11}(-24z^4 + 72z^3 - 70z^2 + 112z - 76)x^2 + \\ &\quad + \frac{1}{11}(2877z^4 - 9984z^3 + 13080z^2 - 23436z + 24318)x + \\ &\quad + \frac{1}{4}(10224z^4 - 35451z^3 + 46509z^2 - 83811z + 87129), \end{aligned}$$

$$\begin{aligned} f_{5,7} &= \frac{125}{256}x^5 - \frac{25}{32}x^4 + \frac{15}{16}x^3 - x^2 + x + 1, \\ f_{5,9} &= \left(-\frac{15401}{400}z^2 + \frac{592891}{6400}z + \frac{5225741}{6400}\right)x^5 + \\ &\quad + \left(\frac{4221}{400}z^2 - \frac{20517}{800}z - \frac{88921}{400}\right)x^4 + \\ &\quad + \left(\frac{57}{16}z^2 - \frac{33}{4}z - \frac{1237}{16}\right)x^3 + \\ &\quad + \left(-\frac{19}{10}z^2 + \frac{22}{5}z + \frac{409}{10}\right)x^2 + x + 1, \\ f_{7,9} &= \frac{16807}{4096}x^7 - \frac{2401}{512}x^6 + \frac{1029}{256}x^5 - \\ &\quad - \frac{49}{16}x^4 + \frac{35}{16}x^3 - \frac{3}{2}x^2 + x + 1, \end{aligned}$$

$$\begin{aligned} f_{9,11} &= \frac{4782969}{65536}x^9 - \frac{531441}{8192}x^8 + \frac{177147}{4096}x^7 - \\ &\quad - \frac{6561}{256}x^6 + \frac{3645}{256}x^5 - \frac{243}{32}x^4 + \frac{63}{16}x^3 - 2x^2 + x + 1. \end{aligned}$$

Выше z обозначает порождающий соответствующее числовое поле элемент из табл. 1. В силу громоздкости коэффициентов многочленов $f_{5,11}$, $f_{7,11}$, мы не приводим их в настоящей статье, и намерены их опубликовать в планируемой полной версии изложения.

ПЕРИОДИЧЕСКИЙ КОРЕНЬ

Далее мы приводим результаты о существовании фундаментальных S -единиц и критерии периодичности $\sqrt{f}$ из статей [13, 12].

Предложение 1. Пусть многочлен f свободен от квадратов, $\deg f = 2g + 1$, а степень фундаментальной S -единицы равна n . Тогда для подходящих $\mu_1, \mu_2, d_1, d_2 \in k[x] \setminus \{0\}$, $b \in k \setminus \{0\}$, $f = d_1 d_2$, выполнено соотношение $\mu_1^2 d_1 - \mu_2^2 d_2 = bx^m$, где если n — четно, то $n = 2m$, а в противном случае $n = m$, $d_1 \in k$. Более того, указанный n является минимально возможным, при котором выполняется это соотношение.

Уравнение из предложения 1 будем называть обобщенным норменным уравнением, а если $d_2 = f$, то просто норменным.

Теорема 2. Пусть многочлен f свободен от квадратов, а $\deg f = 2g + 1$. Элемент $\sqrt{f}$ периодичен тогда и только тогда, когда некоторого $m \in \mathbb{N}$, существует решение $\mu_1, \mu_2, d_1, d_2 \in k[x]$, $b \in k \setminus \{0\}$, $f = d_1 d_2$, уравнения

$$\mu_1^2 d_1 - \mu_2^2 d_2 = bx^m, \tag{1}$$

и решение для наименьшего такого m удовлетворяет условиям:

$$\begin{aligned} \deg \mu_2 &= \frac{m - \deg d_2}{2}, \\ \deg \mu_1 &\leq \frac{m + \deg d_2}{2} - (2g + 1). \end{aligned}$$

Вообще говоря, теорема 2 дает критерий квазипериодичности $\sqrt{f}$, но в работе [12] было доказано, что квазипериодичность $\sqrt{f}$ равносильна периодичности.

НЕТРИВИАЛЬНЫЕ РЕШЕНИЯ

Зафиксируем m , $\deg f$ и $\deg d_1$, тогда степени всех многочленов определяются из теоремы 2. Определим коэффициенты a_i, b_i, h_j, f_l из следующих равенств:

Таблица 1.

$D = \deg f$	Степень S -единицы U	Поле k	Многочлен $F_{d,U}(t)$
3	5	$\mathbb{Q}$	—
3	7	$\mathbb{Q}(\sqrt{21})$	$t^2 - 21$
3	8	$\mathbb{Q}$	—
3	9	$\mathbb{Q}(z), F_{3,9}(z) = 0$	$t^3 - t^2 + \frac{1}{2}t - \frac{1}{12}$
3	10	$\mathbb{Q}$	—
3	11	$\mathbb{Q}(z), F_{3,11}(z) = 0$	$t^5 - t^4 - 4t^3 + 3t^2 - \frac{35}{3}t + 21$
5	7	$\mathbb{Q}$	—
5	9	$\mathbb{Q}(z), F_{5,9}(z) = 0$	$t^3 - 27t - 51$
5	11	$\mathbb{Q}(z), F_{5,11}(z) = 0$	$t^7 - t^6 - 53t^5 - 133t^4 + 195t^3 + 1000t^2 + 1165t + 955$
7	9	$\mathbb{Q}$	—
7	11	$\mathbb{Q}(z), F_{7,11}(z) = 0$	$t^4 - 2t^3 - 81t^2 - 303t - 321$
9	11	$\mathbb{Q}$	—

Примечание. Для указанных d и U приведены $F_{d,U}$, поле k и $f_{d,U}$, где $F_{d,U}(t) \in \mathbb{Q}[t]$ неприводимый над $\mathbb{Q}$ многочлен, задающий поле алгебраических чисел $k = \mathbb{Q}[t]/(F_{d,U})$, которое является полем определения многочлена $f_{d,U}$ с периодическим разложением $\sqrt{f_{d,U}}$ в непрерывную дробь.

$$\begin{aligned} \mu_1 &= \sum_i a_i x^i; & \mu_2 &= \sum_i b_i x^i; \\ d_1 &= \sum_j h_j x^j; & d_2 &= \sum_l f_l x^l. \end{aligned} \tag{2}$$

Определение 1. Пусть заданы $g, m \in \mathbb{N}$. Будем называть набор $(\mu_1, \mu_2, d_1, d_2, b)$, где $b \in k \setminus \{0\}$, $\mu_1, \mu_2, d_1, d_2 \in k[x]$, $d_1 \neq 0$, $d_2 \neq 0$, $a_0 \neq 0$, $\deg d_1 + \deg d_2 = 2g + 1$, а произведение $f = d_1 d_2$ свободно от квадратов, нетривиальным решением обобщенного норменного уравнения над k , если выполнено соотношение (1).

Мы будем писать нетривиальное решение норменного уравнения, если $d_1 = 1$. Мы будем писать просто нетривиальное решение, если из контекста ясно, что речь идет о нетривиальном решении норменного или обобщенного норменного уравнения.

Введем отношение эквивалентности на нетривиальных решениях, продолжающее и сохраняющее отношение эквивалентности на многочленах f из [11].

Определение 2. Будем называть преобразованием нетривиального решения обобщенного норменного уравнения над полем k допустимым преобразованием, если для

некоторого $\gamma \in k \setminus \{0\}$ оно переводит набор $\Omega = (\mu_1, \mu_2, d_1, d_2, b)$ в один из следующих наборов:

- $\Gamma_{1,\gamma}(\Omega) = (\mu_1(\gamma x), \mu_2(\gamma x), d_1(\gamma x), d_2(\gamma x), \gamma^m b)$,
- $\Gamma_{2,\gamma}(\Omega) = (\gamma \mu_1, \gamma \mu_2, d_1, d_2, \gamma^2 b)$,
- $\Gamma_{3,\gamma}(\Omega) = (\gamma \mu_1, \mu_2, d_1, \gamma^2 d_2, \gamma^2 b)$,
- $\Gamma_{4,\gamma}(\Omega) = (\mu_1, \mu_2, \gamma d_1, \gamma d_2, \gamma b)$,

или преобразование, полученные путем последовательного применения вышеперечисленных преобразований. Мы определили группу $\Gamma_k = \Gamma_{1,\gamma}(\Omega) \Gamma_{2,\gamma}(\Omega) \Gamma_{3,\gamma}(\Omega) \Gamma_{4,\gamma}(\Omega)$. Будем называть нетривиальные решения эквивалентными над k , если существует допустимое преобразование над k переводящее одно в другое.

Определение 3. Нетривиальное решение норменного уравнения (1) является также решением полиномиальной системы с переменными a_i, b_i, h_j, f_l . Назовем такую систему системой обобщенного норменного уравнения.

Предложение 2. Пусть заданы $m > 0$, $\deg f = 2g + 1$ и $\deg d_2$. Тогда решение системы обобщенного норменного уравнения соответствует периодическому $\sqrt{f}$ тогда и только тогда, ко-

гда $m \bmod 2 = \deg d_2 \bmod 2$ и $h_0, f_0, b_0, a_0, b_{(m-\deg d_2)/2}, h_{\deg d_1}, f_{\deg f - \deg d_1} \in k \setminus \{0\}$.

Доказательство. Нетрудно видеть, что если обнуляется свободный коэффициент любого из многочленов d_1, d_2, μ_1, μ_2 , то нетривиальное решение (1) не является решением с минимальным m . Оставшиеся требования напрямую следуют из теоремы 2.

Для многочлена h через $\text{lc}(h)$ обозначим старший ненулевой коэффициент. Напомним лемму, доказанную ранее в статье [14].

Лемма 1. Пусть $m \in \mathbb{N}$ — наименьшее такое число, что существует нетривиальное решение обобщенного норменного уравнения над k , тогда для данного m :

- 1) существует нетривиальное решение над k с $h_0 = f_0 = 1 = \text{lc}(\mu_1)$ и $f_1 = 0$ или $f_1 = 1$;
- 2) существует нетривиальное решение над k с $h_0 = f_0 = 1 = \text{lc}(\mu_2)$ и $f_1 = 0$ или $f_1 = 1$;
- 3) при условии $b_i, b_j, f_j, h_i \in k \setminus \{0\}$ существует нетривиальное решение над $\bar{k}$ с $b_i = b_j = f_j = h_i = 1$.

Лемма 2. Пусть λ — один из коэффициентов μ_1, μ_2, d_1, d_2 , не совпадающий с $f_{\deg d_2}, b_{(m-\deg d_2)/2}, b_0$, и пусть не существует нетривиального решения над $\bar{k}$ с условиями $f_{\deg d_2} = b_{(m-\deg d_2)/2} = b_0 = 1, \lambda = 0$, тогда над полем k не существует нетривиальных решений с условием $\lambda = 0$.

Доказательство. Пусть нетривиальное решение с $\lambda = 0$ существует. Тогда в силу того, что группа $\Gamma_{\bar{k}}$ сохраняет нулевые коэффициенты, и того, что по предложению 2 получаем $f_{\deg d_2} \neq 0, b_{(m-\deg d_2)/2} \neq 0, b_0 \neq 0$, по лемме 1 с помощью преобразования группы $\Gamma_{\bar{k}}$ можно получить нетривиальное решение над $\bar{k}$ с условиями $f_{\deg d_2} = b_{(m-\deg d_2)/2} = b_0 = 1, \lambda = 0$. Противоречие.

ДОКАЗАТЕЛЬСТВО ОСНОВНОЙ ТЕОРЕМЫ

Доказательство. Рассмотрим критерий периодичности $\sqrt{f}$ из теоремы 2, в частности, рассмотрим неравенства на $m, \deg f$ и $\deg d_2, \deg d_1 = \deg f - \deg d_2$. Легко видеть, что для решения (1) с наименьшим m выполнено одно из двух: или $\deg d_1 = 0$ и m — нечетное число, или $\deg d_1 > 0$ и $\deg d_2 > 0$. Первый случай соответствует фундаментальной S -единице нечетной степени $U = m$, а второй — фундаментальной S -единице степени $U = 2m$. Из критерия также нетрудно вывести, что для $m = \deg f$ периодичность $\sqrt{f}$ возможна лишь в случае S -единицы нечетной степени $U = m$ и

$f = cx^m + 1$. По теореме 2 случаи $m < 2\deg f - \deg d_2$ или $m < \deg d_2$ не дают периодического $\sqrt{f}$. Откуда видно, что нам заведомо не подходят случаи $\deg d_2 = \deg f > m$, а также случаи $m < \deg f$. Следовательно, нам достаточно рассмотреть случаи $\deg f = 3, 5, 7, 9$. Причем выполнено $\deg f < m \leq 5$ и $U = 2m$ или $\deg f < m \leq 11$ и $U = m, m = 2l + 1, l \in \mathbb{N}$. Откуда, в случае фундаментальной S -единицы четной степени нам достаточно рассмотреть только случай $\deg f = 3$, который для произвольной четности U был рассмотрен в работе [7]. Случай $m = \deg f + 2, U = m$ разобран для произвольной степени f в [5]. Таким образом, чтобы завершить доказательство теоремы 1, нам остается рассмотреть три случая: $U = m = 9, \deg f = 5$ и $U = m = 11, \deg f = 5, 7$.

Доказательство каждого из этих случаев состоит из несколько частей. Сначала мы доказываем, что при вырожденных условиях на коэффициенты многочленов уравнения (1) нет искомого многочленов. Далее мы рассматриваем только невырожденные случаи, что позволяет провести преобразования системы из введенной нами группы преобразований, которые облегчают вычислительную процедуру. Наконец, мы строим базис Грёбнера преобразованной системы, и проводим вычисление всех требуемых нам решений.

По теореме 2 и лемме 1 во всех интересующих нас случаях можно считать, что $d_2 = f, d_1 = h_0 = 1$. Чтобы провести вышеуказанные преобразования, нам необходимо убедиться, что не существует решений системы (1) с $f_1 = 0$, где f_1 и другие коэффициенты определяются из (2). По предложению 2 мы можем положить $f_{\deg d_2} = b_{(m-\deg d_2)/2} = b_0 = 1$. Подставим их в систему норменного уравнения, а также подставим $f_1 = 0$. Базис Грёбнера системы норменного уравнения с подставленными параметрам состоит из единицы, а значит решений с $f_{\deg d_2} = b_{(m-\deg d_2)/2} = b_0 = 1, f_1 = 0$ не существует, что по лемме 2 позволяет считать $f_1 \neq 0$.

Дальнейшую процедуру подробно опишем только для случая $\deg f = 5$ и степени соответствующей S -единицы равной 9. Остальные случаи рассматриваются по аналогичной схеме, и полное их изложение выходит за рамки объема настоящей статьи.

По теореме 2 в этом случае периодичность $\sqrt{f}$ влечет $\deg(\mu_1) \leq \deg(\mu_2) = 2$. Воспользуемся тем, что $f_1 \neq 0$ и леммой 1, и подставим в систему норменного уравнения $b_2 = 1, f_0 = 1, f_1 = 1$. В результа-

те подстановки получим систему из 9 уравнений и 9 неизвестных:

$$\begin{aligned} -a_0^2 + b_0^2 &= 0, \\ -2a_0a_1 + b_0^2 + 2b_0b_1 &= 0, \\ b_0^2f_2 - a_1^2 - 2a_0a_2 + 2b_0b_1 + b_1^2 + 2b_0 &= 0, \\ 2b_0b_1f_2 + b_0^2f_3 - 2a_1a_2 + b_1^2 + 2b_0 + 2b_1 &= 0, \\ b_1^2f_2 + 2b_0b_1f_3 + b_0^2f_4 - a_2^2 + 2b_0f_2 + 2b_1 + 1 &= 0, \\ b_1^2f_3 + 2b_0b_1f_4 + b_0^2f_5 + 2b_1f_2 + 2b_0f_3 + 1 &= 0, \\ b_1^2f_4 + 2b_0b_1f_5 + 2b_1f_3 + 2b_0f_4 + f_2 &= 0, \\ b_1^2f_5 + 2b_1f_4 + 2b_0f_5 + f_3 &= 0, \\ 2b_1f_5 + f_4 &= 0. \end{aligned}$$

Мы можем упростить систему, выразив явно переменные и подставив в систему их выражения:

$$\begin{aligned} a_0 &= -b_0, \\ a_1 &= -\frac{1}{2}b_0 - b_1, \\ a_2 &= -\frac{1}{2}b_0f_2 + \frac{1}{8}b_0 - \frac{1}{2}b_1 - 1, \\ f_4 &= -2b_1f_5, \\ f_3 &= (3b_1^2 - 2b_0)f_5, \\ f_2 &= -2(2b_1^3 - 3b_0b_1)f_5. \end{aligned}$$

В силу того, что $b_0 \neq 0$, сократим множитель b_0 в уравнении $\frac{1}{8}(16b_0b_1^3f_5 - 32b_1^4f_5 - 24b_0^2b_1f_5 + 72b_0b_1^2f_5 - 16b_0^2f_5 + b_0 - 2b_1 + 8)b_0 = 0$. После преобразования получается система из трех уравнений от переменных f_5, b_1, b_0 :

$$\begin{aligned} 2b_0b_1^3f_5 - 4b_1^4f_5 - 3b_0^2b_1f_5 + 9b_0b_1^2f_5 - \\ - 2b_0^2f_5 + \frac{1}{8}b_0 - \frac{1}{4}b_1 + 1 &= 0, \\ -(2b_1^3 - 2b_0b_1)^2b_0^2f_5^2 - \frac{1}{4}(2b_1^3 - 3b_0b_1)b_0^2f_5 + \\ + (2b_1^3 - 3b_0b_1)b_0b_1f_5 + 2(3b_1^2 - 2b_0)b_0b_1f_5 - \\ - 2b_0^2b_1f_5 - 2(2b_1^3 - 3b_0b_1)b_1^2f_5 - 2(2b_1^3 - 3b_0b_1)b_0f_5 - \\ - \frac{1}{64}b_0^2 + \frac{1}{8}b_0b_1 - \frac{1}{4}b_1^2 + \frac{1}{4}b_0 + b_1 &= 0, \\ (2b_1^2 - 2b_0)b_1^2f_5 - 4b_0b_1^2f_5 + 2(3b_1^2 - 2b_0)b_0f_5 + \\ + b_0^2f_5 - 4(2b_1^3 - 3b_0b_1)b_1f_5 + 1 &= 0. \end{aligned}$$

Условия, приведенные выше, задают идеал, базис Грёбнера которого состоит из трех многочленов:

$$\begin{aligned} -1717986918400f_5 + 326637322633083916475b_0^7 - \\ - 678886113588907584640b_0^6 + \\ + 290630257938398815744b_0^5 + \\ + 320000000000b_0^4 - 1392640000000b_0^3 + \\ + 1073152000000b_0^2 - 419430400000b_0 + \\ + 838860800000, \\ 335544320b_1 + 137055178600025b_0^7 - \\ - 284859639128960b_0^6 + \\ + 121950976802816b_0^5 - 51200000b_0^4 + \\ + 196608000b_0^3 + 104857600b_0^2 - \\ - 587202560b_0 - 268435456, \\ b_0^5 \cdot (60025b_0^3 - 129360b_0^2 + 62976b_0 - 4096). \end{aligned}$$

Опишем последний этап для всех случаев в виде некоторого алгоритма.

1. Берем последний многочлен P в найденном базисе Грёбнера для соответствующего лексикографического порядка. Он является многочленом над $\mathbb{Q}$ от одной переменной и в данном случае равен

$$b_0^5 \cdot (60025b_0^3 - 129360b_0^2 + 62976b_0 - 4096).$$

2. Берем последовательно каждый неприводимый множитель многочлена P , и возьмем его корень α в соответствующем расширении $\mathbb{Q}$.

3. Подставляем α в остальные многочлены из базиса Грёбнера и последовательно находим все значения неизвестных. В нашем случае оказывается, что все они лежат в поле, полученном при соединении к $\mathbb{Q}$ исходного корня α .

Среди найденных решений системы обобщенного нормального уравнения отбрасываем те, которые не соответствуют предложению 2. Во всех случаях оказывалось, что мы с точностью до эквивалентности находим лишь один многочлен.

В табл. 1 и ниже приведены многочлены $f_{5,9}$ и $F_{5,9}$, корнем которого является α , преобразованные с целью приведения коэффициентов к более аккуратному виду.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Работа выполнена в рамках государственного задания по проведению фундаментальных научных исследований по проекту № 0580-2021-0011.

СПИСОК ЛИТЕРАТУРЫ

1. *Abel N.H.* Ueber die integration der differential-formel $pdx/\sqrt{R}$ wenn r und p ganze functionen sind // Journal

- für die reine und angewandte Mathematik. 1826. V. 1. P. 185–221.
2. *Tchebicheff P.* Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisième ou du quatrième degré // *Journal des math. pures et appl.* 1857. V. 2. P. 168–192.
 3. *Платонов В.П.* Теоретико-числовые свойства гиперэллиптических полей и проблема кручения в якобианах гиперэллиптических кривых над полем рациональных чисел // *УМН.* 2014. Т. 69. № 1(415). С. 3–38.
 4. *Wolfgang M. Schmidt.* On continued fractions and diophantine approximation in power series fields // *Acta arithmetica.* 2000. V. 95. № 2. P. 139–166.
 5. *Платонов В.П., Федоров Г.В.* О проблеме периодичности непрерывных дробей в гиперэллиптических полях // *Матем. сб.* 2018. Т. 209. № 4. С. 54–94.
 6. *Платонов В.П., Петрунин М.М., Жгун В.С.* О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над числовыми полями // *Доклады РАН. Математика, информатика, процессы управления.* 2020. Т. 493. № 1. С. 32–37.
 7. *Платонов В.П., Петрунин М.М.* О конечности числа периодических разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов над полями алгебраических чисел // *Доклады РАН. Математи-*
 - ка, информатика, процессы управления. 2020. Т. 495. № 1. С. 48–54.
 8. *Платонов В.П., Федоров Г.В.* О проблеме классификации периодических непрерывных дробей в гиперэллиптических полях // *Успехи математических наук.* 2020. Т. 75. № 4(454). С. 211–212.
 9. *Kubert D.S.* Universal bounds on the torsion of elliptic curves // *Proc. London Math. Soc.* 1976. V. 33. № 2. P. 193–237.
 10. *Sutherland A.* Constructing elliptic curves over finite fields with prescribed torsion // *Mathematics of Computation.* 2012. V. 81. № 278. P. 1131–1147.
 11. *Платонов В.П., Петрунин М.М., Жгун В.С. и др.* О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ // *Доклады РАН.* 2018. Т. 483. № 6. С. 609–613.
 12. *Платонов В.П., Петрунин М.М.* Группы S -единиц и проблема периодичности непрерывных дробей в гиперэллиптических полях // *Труды МИАН.* 2018. Т. 302. С. 354–376.
 13. *Петрунин М.М.* S -единицы и периодичность квадратного корня в гиперэллиптических полях // *Доклады РАН.* 2017. Т. 474. № 2. С. 155–158.
 14. *Платонов В.П., Петрунин М.М., Штейников Ю.Н.* О конечности числа эллиптических полей с заданными степенями S -единиц и периодическим разложением $\sqrt{f}$ // *Доклады РАН.* 2019. Т. 488. № 3. С. 9–14.

ON THE PERIODICITY PROBLEM FOR THE CONTINUED FRACTION EXPANSION OF ELEMENTS OF HYPERELLIPTIC FIELDS WITH FUNDAMENTAL S -UNIT DEGREE LESS OR EQUAL TO 11

Academician of the RAS **V. P. Platonov^{a,b}**, **M. M. Petrunin^a**, and **Yu. N. Shteinikov^a**

^a *Scientific Research Institute for System Analysis, Russian Academy of Sciences, Moscow, Russian Federation*

^b *Steklov Mathematical Institute, Russian Academy of Sciences, Moscow, Russian Federation*

We solve the problem of describing square-free polynomials $f(x) \in k[x]$ with periodic expansion of $\sqrt{f(x)}$ into a functional continued fraction in $k((x))$, where k is a number field and the degree of the corresponding fundamental S -unit of hyperelliptic field $k(x)(\sqrt{f(x)})$ is less or equal to 11.

Keywords: hyperelliptic field, S -units, continued fractions, periodicity, torsion points