К вопросу о количестве многочленов *f* девятой степени, задающих гиперэллиптическое поле с фундаментальной *S*-единицей степени 13 и периодическим разложением корня из *f*

Ю. Н. Штейников[1]

[1]НИЦ «Курчатовский институт» - НИИСИ, Москва, Российская Федерация, yriisht@yandex.ru;

Аннотация. Статья освещает некоторые вопросы о количестве многочленов с коэффициентами из поля алгебраических чисел k таких, что deg f =9 , при котором соответствующее гиперэллиптическое поле $k(x)(\sqrt{f})$ содержит фундаментальную S-единицу степени 13 и для которых разложение $\sqrt{f}$ в функциональную непрерывную дробь в поле k((x)) периодично. В этой статье доказано, что для любого поля k, являющегося полем алгебраических чисел, таких многочленов лишь конечное число и мы получаем универсальную оценку на это количество, не зависящее от поля k. Более того мы попутно доказываем, что множество таких многочленов непусто для некоторого такого поля k, являющегося полем определения набора коэффициентов f. При доказательстве основных результатов существенную роль играют символьные вычисления с базисами Гребнера.

Ключевые слова: гиперэллиптическое поле, фундаментальная S -единица.

1. Введение

В данной работе будем обозначать через $f(x) = f_0 + f_1 x + ... + f_{2g+1} x^{2g+1} \in k[x]$ - многочлен нечетной степени 2g+1 над некоторым полем k характеристики 0. Для дальнейших наших целей будем считать, что он является бесквадратным , и $f_0 = a^2$ где $a \in k \setminus \{0\}$, то есть первый коэффициент является квадратом некоторого числа.

Известно, что для функциональных непрерывных дробей в поле $k((x))$ из наличия периодических элементов в $k((x))$ следует периодичность элементов $\sqrt{f} / x^g$ и $\sqrt{f} / x^{g+1}$, где g – род кривой, соответствующий многочлену f степени 2g+1. Другие же элементы, например элементы вида $\sqrt{f} / x^s$, где $s \neq g, s \neq g+1,$ как правило могут быть непериодичны (см. [1]). Стоит напомнить, что свойство разлагаться в периодическую дробь для $\sqrt{f} / x^g$ в поле формальных степенных рядов k((x)) означает существование нетривиальных S -единиц в соответствующем гиперэллиптическом поле для множества нормирований S , которое состоит из одного из двух нормирований, продолжающих нормирование для поля $k(x)$, определяемого линейным многочленом x, и бесконечного нормирования (см. статью [1]).

Упомянем некоторые предшествующие результаты. В работе [3] были впервые найдены все такие нетривиальные многочлены f степени 3 над полем рациональных чисел, обладающих периодическим разложением $\sqrt{f}$.

В дальнейшем эти исследования были продолжены в следующем направлении. В работе [4] вышеуказанные результаты были обобщены и распространены на числовые поля констант k и данная проблема получила полное решение в отношении вопроса о периодичности для квадратичных и числовых полей k степени 3 над $\mathbb{Q}$. Далее в работе [5] был впервые получен результат о конечности таких многочленов f для числовых полей k, степень которых над полем $\mathbb{Q}$ не превосходит 6. Вывод этих результатов основан на символьных вычислениях в системе компьютерной алгебры и на параметризации пар: эллиптическая кривая и точка с фиксированным порядком кручения [6, 7].

В другом направлении отметим следующие результаты. В работе [8] в явном виде получены все такие многочлены $f(x)$ над произвольными

числовыми полями констант k, и для любой степени многочлена f, при специальном ограничении соответствующей степени U фундаментальной S-единицы соответствующего гиперэллиптического поля $k(x)(\sqrt{f})$. Эта величина U не больше чем 12, а также в случае четного U она не превышает 20 [8].

В настоящей статье мы преследуем следующую цель. Мы хотим доказать, что для любого поля k характеристики 0, существует не более чем конечное число попарно неэквивалентных многочленов $f(x)$ таких, что $degf = 9$ и $\sqrt{f}$ раскладывается в периодическую непрерывную дробь в $k((x))$, а кроме того соответствующее гиперэллиптическое поле $k(x)(\sqrt{f})$ содержит фундаментальную $S-$единицу степени 13.

2. Основной результат

Приведем некоторые дополнительные сведения, необходимые в дальнейшем. Для неприводимого над k многочлена h определим дискретное нормирование ν_h (элемента поля $k(x)$) равенством $\nu_h\left(h^m \frac{p}{q}\right) = m$, где взаимно простые многочлены p,q не делятся на h; бесконечное нормирование, в свою очередь, определим равенством $\nu_\infty\left(\frac{p}{q}\right) = degq - degp$.

Пусть нормирование ν_x поля $k(x)$ имеет два продолжения ν_x^+ и ν_x^- на поле $L = k(x)(\sqrt{f})$. Если $degf = 2g+1$ для $g \in \mathbb{N}$, то положим $S = \{\nu_x^+, \nu_\infty\}$. Группа обратимых S-целых элементов поля L называется группой S-единиц. Если существует хотя бы одна нетривиальная S-единица (то есть отличная от константы поля k), то в описанном нами случае группа S-единиц является прямым произведением $k\setminus\{0\}$ и бесконечной циклической группы. Образующие этой циклической группы называются фундаментальными S-единицами.

Если $\eta_1+\eta_2\sqrt{f}, \eta_1, \eta_2 \in k(x)$ — S-единица, то её норменное выражение имеет вид $\eta_1^2 - \eta_2^2 f = bx^m$, где $b \in k\setminus\{0\}$. Степенью S-единицы называется показатель m степени x в правой части выражения. Для рассматриваемого S порядок соответствующей точки кручения на якобиане гиперэллиптической кривой, связанной с нормированием ν_x^+, совпадает со степенью соответствующей S-единицы (см. [2]).

Также полезно ввести следующие понятия. Свойство периодичности разложения $\sqrt{f(x)}$ в непрерывную дробь равносильно периодичности любых элементов вида $\sqrt{a^2 f(bx)}$ в произвольных $a,b \in k^*$. Тем самым имеет смысл рассматривать искомые многочлены f с точностью до эквивалентности, определяемой преобразованиями, указанными выше. Основная теорема звучит следующим образом.

Теорема 1. *Для любого поля k характеристики 0, существует не более 284 попарно неэквивалентных многочленов $f(x) \in k[x]$ таких, что $degf = 9$, разложение элемента $\sqrt{f}$ в непрерывную дробь периодично, а гиперэллиптическое поле $k(x)(\sqrt{f})$ обладает фундаментальной $S-$единицей степени 13.*

Замечание к теореме 1. Можно доказать, что в случае поля $\mathbb{Q}$ многочленов с рациональными коэффициентами, удовлетворяющих условиям теоремеы 1 не существует. В настоящей статье мы доказываем существование таких многочленов, но над некоторыми полями алгебраических чисел k. Иными словами, существует хотя бы один такой многочлен степени 9 с коэффициентами из поля $\bar{\mathbb{Q}}$, обладающий вышеуказанными свойствами. С другой стороны главный результат теоремы 1 говорит о существовании эффективной верхней границы числа таких многочленов f. Явный вид таких многочленов или их классификация в случае разных полей k, является открытым вопросом ввиду слишком большого объема вычислений, требуемых для реализации предложенного нами подхода. Одним из главных препятствий в реализуемом нами подходе является трудоемкость вычислений в полиномиальных идеалах , а также адаптация и оптимизация соответствующих алгоритмов основанных на вычислениях базисов Гребнера.

3. Доказательство основной теоремы.

Приведем одно утверждение, которое потребуется для доказательства [1].

Лемма 1. [1] *Пусть многочлен f свободен*

от квадратов, $deg f = 2g+1$, *а поле* L *обладает фундаментальной* S*-единицей нечётной степени* m. *Элемент* $\sqrt{f}$ *периодичен тогда и только тогда, когда существуют* $\alpha, \beta \in k[x]$, $b \in k \setminus \{0\}$, *удовлетворяющие уравнению* $\alpha^2 - \beta^2 f = bx^m$ *такие, что* $deg\alpha \le \frac{m-2g-1}{2}$,

$$deg\beta = \frac{m-2g-1}{2}.$$

Для произвольного многочлена $p \in k[x]$ обозначим его коэффициенты через p_k, то есть $p = \sum_k p_k x^k$.

Определение 1. *Пусть для произвольного поля* k *заданы* $g, m \in \mathbb{N}$, $b \in k \setminus \{0\}$, $\alpha, \beta, f \in k[x]$, $\alpha_0 \neq 0, \beta_0 \neq 0$, $deg\, f = 2g+1$. *Будем называть набор* (α, β, f, b) *нетривиальным решением норменного уравнения над* k, *если выполнено норменное уравнение*

$$\alpha^2 - \beta^2 f = bx^m. \quad (1)$$

Нетривиальное решение этого норменного уравнения является по сути решением полиномиальной системы относительно переменных $\{\alpha_i\}, \{\beta_j\}, \{f_k\}$. Будем называть ее системой норменного уравнения. Введём отношение эквивалентности на нетривиальных решениях, продолжающее отношение эквивалентности на многочленах.

Определение 2. *Для* $\gamma \in k \setminus \{0\}$ *определим преобразования* $G_{i,\gamma}$, *действующее на наборах* $\Omega = (\alpha, \beta, f, b)$ *следующим образом:*

$$G_{1,\gamma}(\Omega) = \left(\alpha(\gamma x), \beta(\gamma x), f(\gamma x), \gamma^m b\right);$$

$$G_{2,\gamma}(\Omega) = \left(\gamma\alpha, \gamma\beta, f, \gamma^2 b\right);$$

$$G_{3,\gamma}(\Omega) = \left(\gamma\alpha, \beta, \gamma^2 f, \gamma^2 b\right).$$

По сути преобразования $G_{i,\gamma}$ определяют отношение эквивалентности на множестве нетривиальных решений вышеуказанной полиномиальной системы.

Обозначим через G_k группу порожденную этими коммутирующими преобразованиями. Элементы этой группы будем называть допустимыми преобразованиями.

Доказательство теоремы 1. Пусть в наших обозначениях фундаментальная S-единица имеет вид: $\alpha + \beta\sqrt{f}$, ее степень равна 13, $\alpha, \beta \in k[x]$, некоторые многочлены, соответственно выполнено норменное уравнение $\alpha^2 - \beta^2 f = bx^{13}, b \in k^*$. По лемме 1 получаем ограничения на их соответствущие степени, то есть $deg(\alpha), deg(\beta) \le 2$.

Легко показать, что $\alpha_0, \beta_2 \neq 0$. Если $\alpha_0 = 0$ (что равносильно $\beta_0 = 0$), то в результате сокращения степень фундаментальной единицы окажется строго меньше 13. В случае $\beta_2 = 0$, сравнение степеней при x^{13} приводит к аналогичному выводу.

С помощью группы преобразований G_k будем осуществлять специальную выборку значений переменных, являющихся решением полиномиальной системы норменного уравнения. Покажем, что для преобразований группы G_k для поля k являющегося возможно конечным расширением поля Q во множестве решений полиномиальной системы в переменных $\{\alpha_i\}, \{\beta_j\}, \{f_k\}$. можно выбрать соответствующий представитель в классе эквивалентности с $f_9 = \beta_2 = \alpha_0 = 1$. Действительно, пусть параметры $\gamma_1, \gamma_2, \gamma_3$ соответствуют элементарному преобразованию $G_{1,\gamma_1}(\Omega) G_{2,\gamma_2}(\Omega) G_{3,\gamma_3}(\Omega)$ согласно определению 2. Тогда неизвестные значения $\gamma_1, \gamma_2, \gamma_3$ определяются из уравнений:

$$f_9\gamma_1^9\gamma_3^2 = 1,\ \alpha_0\gamma_2\gamma_3 = 1,\ \beta_2\gamma_1^2\gamma_2 = 1$$

Из предыдущих соотношений следует, что

$$\frac{f_9\beta_2^2}{\alpha_0^2}\gamma_1^{13} = 1, \quad \gamma_2 = \frac{1}{\gamma_1^2\beta_2}, \quad \gamma_3 = \frac{1}{\gamma_2\alpha_0}.$$

Поэтому с учетом предыдущих уравнений можно положить:

$$f_9 = \alpha_0 = \beta_2 = 1.$$

После исключения всех неизвестных коэффициентов из системы норменного уравнения мы получаем систему от 4 неизвестных $\alpha_1, \alpha_2, \beta_1, \beta_0$ с 4 уравнениями.

$$30\beta_0^6\beta_1 - 140\beta_0^5\beta_1^3 + 168\beta_0^4\beta_1^5 +$$
$$-72\beta_0^3\beta_1^7 + 10\beta_0^2\beta_1^9 - \beta_0^2\alpha_2^2 + 1 = 0$$
$$-5\beta_0^6 + 120\beta_0^5\beta_1^2 - 385\beta_0^4\beta_1^4 +$$
$$+392\beta_0^3\beta_1^6 - 153\beta_0^2\beta_1^8 + 20\beta_0\beta_1^10 -$$
$$-2\beta_0\beta_1\alpha_2^2 + 2\alpha_1 = 0$$
$$30\beta_0^5\beta_1 - 70\beta_0^4\beta_1^3 - 56\beta_0^3\beta_1^5 +$$
$$+144\beta_0^2\beta_1^7 - 70\beta_0\beta_1^9 - 2\beta_0\alpha_2^2 +$$
$$+10\beta_1^{11} - \beta_1^2\alpha_2^2 + \alpha_1^2 + 2\alpha_2 = 0$$
$$-6\beta_0^5 + 105\beta_0^4\beta_1^2 - 280\beta_0^3\beta_1^4 +$$
$$+252\beta_0^2\beta_1^6 - 90\beta_0\beta_1^8 + 11\beta_1^{10} -$$
$$-2\beta_1\alpha_2^2 + 2\alpha_1\alpha_2 = 0$$

Далее, рассматриваем идеал, образованный этими 4-мя уравнениями в кольце $\mathbb{Q}[\beta_1, \beta_0, \alpha_1, \alpha_2]$.

Далее мы вычисляем отдельно базис Гребнера этого идеала I для степенного лексикографического порядка – deglex order. Напомним, что $deg\beta_1^{b_1}\ldots\alpha_2^{a_2} = b_1 + \ldots + a_2$. Порядок на мономах определяется следующим образом: сначала сравниваются степени мономов, в случае же равенства сравнение идет по стандартному лексикографическому порядку.

Более того, с помощью команды *normal-basis()* в системе Sage можно вывести и сам линейный базис $\mathbb{Q}[\beta_1, \beta_0, \alpha_1, \alpha_2]/I$, который и состоит из 284 монома.

Теперь покажем, что указанный многочлен существует с коэффициентами из подходящего поля k. Во-первых лемма 1 является критерием существования таких многочленов. Поэтому достаточно показать, что существует решение норменного уравнения с нужными нам свойствами.

Далее, мы выше вычислили базис Гребнера для взвешенного порядка для соответствующего идеала, отвечающего системе норменного уравнения с $f_9 = \beta_2 = \alpha_0 = 1$. Вычисленный нетривиальный (неконстантный) базис нам помимо всего прочего говорит о том, что множество решений соответствующей системы непусто. Напомним, если бы решений не существовало , то по известному критерию базис Гребнера состоял из ненулевой константы. Но это не так в нашем случае.

Дальнейшим нашим шагом будет доказательство того факта, что многочленов с неподходящими свойствами нет среди решений вышеуказанной системы. Иными словами во множестве решений системы норменного уравнения с $f_9 = \beta_2 = \alpha_0 = 1$ могут находиться многочлены с единственным неподходящим нам свойством $f_0 = 0$. В этом случае нельзя разложить в непрерывную дробь элемент $\sqrt{f}$ Поэтому достаточно проверить что $f_0 \neq 0$ во множестве решений вышеуказанной системы.

Мы подставляем условие $f_0 = 0$ в указанную систему выписанную выше и вычисляем базис Гребнера системы. Оказывается, что этот базис содержит константу, равную единице. Отсюда следует вывод, что таких многочленов с коэффициентами из поля $\bar{\mathbb{Q}}$ с $f_0 = 0$ не существует. Значит многочленов с единственным неподходящим свойством $f_0 = 0$ не существует, а среди непустого множества решений многочлен f указанного вида с условиями теоремы 1 действительно существует.

Теорема 1 полностью доказана.

Настоящая работа выполнена в рамках государственного задания НИЦ «Курчатовский институт» – НИИСИ по теме № FNEF-2024-0001 «Создание и реализация доверенных систем искусственного интеллекта, основанных на новых математических и алгоритмических методах, моделях быстрых вычислений, реализуемых на отечественных вычислительных системах», этап 2025 года.

On the Question of the Number of Polynomials f of Degree 9 Defining a Hyperelliptic Field with a Fundamental S-unit of Degree 13 and a Periodic Expansion of the square root of f

Y. N. Shteinikov

Abstract. This article is devoted to some questions about the number of polynomials with coefficients in an algebraic number field k such that deg f = 9, for which the corresponding hyperelliptic field $k(x)(\sqrt{f})$ has a fundamental S-unit of degree 13 and for which the continued fraction expansion of $\sqrt{f}$ is periodic. It is proved that for any algebraic number field k, there are only finitely many such polynomials, and we obtain a universal estimate for this number, independent of the field k. Moreover, we prove that for , the set of such polynomials is nonempty for some field k that is the definition field of the coefficient set of polynomial f. Symbolic computations with Gröbner bases play a significant role in the proof of the main results.

Keywords: hyperelliptic field, fundamental S-unit

Литература

1. 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.

2. 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.

3. Платонов В.П., Федоров Г.В. О проблеме периодичности непрерывных дробей в гиперэллиптических полях// *Математический сборник*. 2018, Т.209, № 4. С.54–94.

4. 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. Математика, информатика, процессы управления*. 2020. Т.495, № 1, С.48–54.

5. В. П. Платонов, В. С. Жгун, М. М. Петрунин, “О проблеме периодичности разложений в непрерывную дробь $\sqrt{f}$ для кубических многочленов f над полями алгебраических чисел”, Матем. сб., 213:3 (2022), 139–170.

6. Kubert D.S. Universal bounds on the torsion of elliptic curves // *Proc. London Math. Soc.* 1976. Vol. 33, № 2, P. 193–237.

7. Sutherland A. Constructing elliptic curves over finite fields with prescribed torsion// *Mathematics of Computation.* 2012. Vol. 81, № 278, P. 1131–1147.

8. Платонов В.П., Петрунин М.М. Новые результаты о проблеме периодичности непрерывных дробей элементов гиперэллиптических полей // *Труды МИАН*. 2023, № 320 , с. 278–286.

9. Schmidt W.M. On continued fractions and diophantine approximation in power series fields// *Acta arithmetica*. 2000. Vol. 95, №2. P.139–166.

10. В. П. Платонов, М. М. Петрунин, В. С. Жгун, Ю. Н. Штейников, “О конечности гиперэллиптических полей со специальными свойствами и периодическим разложением $\sqrt{f}$ ”, Докл. РАН, 483:6 (2018), 609–613.