ISSN 1729-5459. ЭКОЛОГИЧЕСКИЙ ВЕСТНИК НАУЧНЫХ ЦЕНТРОВ ЧЭС. 2018. Т. 15. № 3. С. 6–11

Математика

УДК 519.115.1 doi: 10.31429/vestnik-15-3-6-11

ФАКТОРИЗАЦИЯ ПОЛИНОМОВ НАД КОНЕЧНЫМИ ПОЛЯМИ

Сергеев А. Э.

FACTORIZATION OF POLYNOMIALS OVER FINITE FIELDS

A. E. Sergeev

Kuban State Agrarian University, Krasnodar, Russia
e-mail: galua1979@yandex.ru

Abstract. The laws of factorization of irreducible polynomials with integer coefficients over finite fields, a long-standing problem of number theory and algebra. The various reciprocity laws of number theory are connected with this problem. The Galois group of an irreducible polynomial $f(x)$ of degree n over the field of rational numbers, consider as a subgroup of the symmetric group S_n, actually describes possible types of factorization of $f(x)$ with respect to simple modules. The next problem is to describe prime numbers giving a certain type of factorization of the polynomial $f(x)$ in terms of invariants associated with this polynomial. For polynomials with Abelian Galois group this problem is solved in principle by a dap class field theory. For polynomials with a non-Abelian Galois group, little is known for certain classes of polynomials. In this paper we propose a method for solving this problem for irreducible over the field rational numbers of cubic polynomials.

Keywords: irreducible polynomial, Galois group, factorization.

Пусть $f(x)$ — полином степени $n \geqslant 2$ с рациональными коэффициентами, неприводимый над полем Q рациональных чисел, α — какой-нибудь его корень в алгебраическом замыкании поля Q.

Для поля $K = Q(\alpha)$ степень $[K : Q]$ равна n; пусть также L — наименьшее по включению расширение Галуа поля Q, содержащее поле L. Обозначим через $d(f)$ — дискриминант полинома $f(x)$, тогда $d(f)$ — целое число не равное 0. Пусть A_k и A_L — целые замыкания кольца целых чисел Z в полях K и L соответственно, тогда возникает вопрос изучения арифметики колец A_k и A_L — это одна из основных проблем алгебраической теории чисел.

Ответ на поставленный вопрос связан со строением группы Галуа $G(f)$ полинома f над полем Q и ее свойствами, а также зависит от законов факторизации полинома $f(x)$ по модулям различных простых чисел p, в частности от так называемых законов взаимности [1, 2].

Пусть неприводимый над полем рациональных чисел Q полином $f(x)$ с целыми коэффициентами степени n по простому модулю p имеет факторизацию вида

$$f(x) \equiv f_1(x)f_2(x) \cdot \ldots \cdot f_r(x) (\mathrm{mod}\, p), \quad (1)$$

где неприводимые полиномы $f_j(x)$ $(j = 1, 2, \ldots, r)$ по модулю p имеют соответственно степени $n_1, n_2, \ldots, n_r$, $n = n_1 + n_2 + \ldots + n$. Тогда будем считать, что по модулю p полином $f(x)$ имеет факторизационный тип $(n_1, n_2, \ldots, n_r)$. Заметим, что понятие факторизационный тип полинома тесно связано с понятием факторизационный спектр [3, 4].

При этом возникают следующие проблемы:

1) описать для конкретного неприводимого полинома $f(x)$ из $Q[x]$ степени n его возможные факторизационные типы по возможным простым модулям;

2) для конкретного неприводимого полинома $f(x)$ и возможного его факторизационного типа $(n_1, n_2, \ldots, n_r)$ описать все простые числа p, для которых по модулю p реализуется данный факторизационный тип в представлении (1).

В частности, если полином $f(x)$ расщепляется на линейные множители по модулю p, то его факторизационный тип $(1, 1, \ldots, 1)$ и простое число p принадлежит множеству $Spl(f(x))$, состоящему из всех таких простых чисел. Множество $Spl(f(x))$ обладает в рассматриваемой ситуации рядом замечательных свойств: оно не пусто и если для непри-

Сергеев Александр Эдуардович, канд. физ.-мат. наук, доцент Кубанского государственного аграрного университета; e-mail: galua1979@yandex.ru.

водимого над Q полиномом $g(x)$ степени n с целыми коэффициентами имеет равенство множеств

$$Spl(f(x)) = Spl(g(x)),$$

то поля расщеплений этих полиномов над Q совпадают.

В связи с этим возникает третья проблема:

3) описать для данного неприводимого полинома $f(x)$ степени $n \geqslant 2$ с целыми коэффициентами множества Spl наиболее простым способом.

Первую проблему можно решить для неприводимого полинома $f(x)$, вычисляя его группу Галуа $G(f)$ над полем Q и рассматривая ее как транзитивную подгруппу симметрической группы S_n, тогда используют теорему Фробениуса.

Теорема 1 (Фробениус). Если группа $G(f)$ содержит подстановку δ, являющуюся произведением непересекающихся циклов длин $n_1, \ldots, n_r$, то существует такое бесконечное множество P простых чисел, что для любого $p \in P$ имеет место факторизация $f(x)$ по модулю p вида (1), где $f_i(x)$ — неприводимые по модулю p полиномы степени n_i, $i = 1, 2, \ldots, r$.

Верна и обратная теорема, принадлежащая Дедекинду. Группы Галуа полиномов можно вычислять известными методами [5, 6] или с помощью компьютеров и соответствующих программ (Maple и др.), если степень неприводимого над Q полинома не превосходит 10.

Остальные проблемы далеки от своего решения, если группа Галуа $G(f)$ не является разрешимой. Если же $G(f)$ — абелева группа, теория полей классов решает указанные проблемы.

Пусть $m > 1$ натуральное число, тогда уравнение $x^m = 1$ имеет в поле комплексных чисел m корней, представимых в виде

$$E, E^2, \ldots, E^{(m-1)}, E^m = 1,$$

где $E = e^{2\pi/m}$ — первообразный корень m-ой степени из единицы.

Составим полином

$$\Phi_m(x) = \prod_a (x - E^a),$$

где $1 \leqslant a < m$ и НОД$(a, m) = 1$, тогда полином $\Phi_m(x)$ имеет целые коэффициенты, неприводим над полем рациональных чисел, имеет степень $q(m)$, где q — функция Эйлера. Полином $\Phi_m(x)$ называют m-м круговым полиномом, он имеет абелеву группу Галуа порядка $\phi(m)$, изоморфную мультипликативной группе кольца вычетов Z_m [7–9].

Например,

$$\Phi_4(x) = x^2 + 1, \quad \Phi_5(x) = x^4 + x^3 + x^2 + x + 1,$$

$$\Phi_6(x) = x^2 - x + 1, \quad \Phi_8(x) = x^4 + 1,$$

$$\Phi_7(x) = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1.$$

Имеет место следующая теорема [6].

Теорема 2. Если f — наименьший натуральный показатель такой, что $p^f \equiv \equiv 1 (\mathrm{mod}\, m)$, то полином $\Phi_m(x)$ факторизуется по модулю p на неприводимые множители степени f и его факторизационный тип по модулю p есть $(f_1, f_2, \ldots, f_r)$, где число компонент равно $r = \phi(m)/f$.

Число f вполне определяется арифметической прогрессии $b + mk$, в которой находится простое число p. Поэтому можно определить степень множителей, на которые факторизуется конкретный полином $\Phi_m(x)$ по модулю заданного простого числа p при конкретном значении m, если знать, в какой арифметической прогрессии вида $b + mk$ лежит простое число p.

В частности, если простое число $p = 1 + mk$ при некотором натуральном k, то $\Phi_m(x)$ факторизуется по модулю p на линейные множители; если же $p = g + mk$, где g — один из первообразных корней уравнения $x^{y(m)} \equiv 1 (\mathrm{mod}\, m)$, то $\Phi_m(x)$ неприводим по модулю p. При этом по теореме Гаусса первообразные корни по модулю m существуют только для $m = p$, $2p$, p^2, $2p^\alpha$, 4, где p — нечетное простое число.

Пример 1. Если p — простое число вида $8k + 1$ ($p = 17, 41 \ldots$), то $\Phi_8(x) = x^4 + 1$ по модулю такого p расщепляется на линейном множители, т.е. получаем $Spl(\Phi_8(x)) = \{p$ — простое, $p \equiv 1 (\mathrm{mod}\, 8)\}$. Если $p = 8k + 3$ ($p = 3, 11;\ 3 \ldots$) или $p = 8k + 5$ ($p = 5, 13, 39 \ldots$) или $p = 8k + 7$ ($p = 7, 23, 31 \ldots$), то $\Phi_8(x)$ факторизуется в произведении двух различных неприводимых по модулю p квадратных полиномов. Таким образом, полином $x^4 + 1$ приводим по любому простому модулю, хотя сам и неприводим над полем рациональных чисел.

Конечные расширения поля Q с абелевой группой Галуа описывает глубокая теорема Кронекера–Вебера [2].

Теорема 3 (Кронекер–Вебер). Пусть K — конечное абелево расширение поля Q рациональных чисел. Тогда существует натуральное число m такое, что $K = Q(e^{\frac{2\Pi i}{m}})$.

Эта теорема позволяет, в частности, описывать множество $Spl(f(x))$ для полиномов с целыми коэффициентами с абелевой группой Галуа над полем Q.

Пример 2. Пусть $f(x) = x^3 + x^2 - 2x - 1$, тогда $f(x)$ — неприводим над Q с циклической группой Галуа 3-го порядка, его корни $\alpha = E + E^{-1}$, $B = E^2E^{-2}$, $\gamma = E^3 + E^{-3}$, где $E = e2n/7$. Поле расщепления этого полинома над Q есть $Q(\alpha)$ и оно содержится в круговом поле $Q(E)$, тогда

$$Spl(f(x)) = \{p \text{ — простое;} \\ p = 1(\mathrm{mod}\,7) \text{ или } p = -1(\mathrm{mod}\,7)\}.$$

Пусть $f(x)$ — полином с целыми коэффициентами и старшим коэффициентом 1, неприводимый над полем Q множество всех таких простых p, что $f(x)$ расщепляется полностью в произведение различных линейных множителей по модулю p. Т.е. множество $Spl(f(x))$ определяется с помощью сравнений, если существует натуральное число $m < 1$ и взаимно-простые с m натуральные числа $a_1, \ldots, a_n$, зависящие от $f(x)$, для которых выполняется $p \in Spl(f(x))$, только если $p \equiv a_1(\mathrm{mod}\,m)$ или $p \equiv a_2(\mathrm{mod}\,m)$, $\ldots$ или $p \equiv a_3(\mathrm{mod}\,m)$.

Известно, что только полиномы с абелевой группой Галуа обладают этим свойством.

Простейшими полиномами с неабелевой группой Галуа является полиномы вида $x^3 - a$, где a — рациональное число, не являющееся кубом рационального числа.

Законы факторизаций кубических биномов по простым модулям, с помощью кубического закона взаимности изучали К.Ф. Гаусс и Г. Якоби.

Теорема 4 (Гаусс). Полином $x^3 - 2$ расщепляется в произведение различных линейных множителей по модулю простого числа p тогда и только тогда, когда символ Лежандра $\left(\frac{-3}{p}\right) = +1$ и $p = x^2 + 27y^2$ при некоторых целых x и y.

Теорема 5 (Якоби). Полином $x^3 - 3$ расщепляется в произведение различных линейных множителей по модулю простого числа p тогда и только тогда, когда символ Лежандра $\left(\frac{-3}{p}\right) = +1$ и $p = x^2 + xy + 61y^2$ при некоторых целых x и y.

Пусть $f(x) = x^3 + ax + b$, $a,\ b \in Q$ — неприводимый над Q полином, тогда его дискриминант $d(f) = -4a^3 - 27b^2$ и группа Галуа $Gal(f(x))$ полинома $f(x)$ есть циклическая 3-го порядка, если $d(f)$ — квадрат рационального числа и группа $Gal(f(x))$ — неабелева 6-го порядка, если $d(f)$ — не квадрат рационального числа.

Хассе с помощью теории полей классов исследовал арифметику поля расщепления над Q критических полиномов с неабелевой группой Галуа и описал множество $Spl(f(x))$ косвенным образом. Далее покажем, как можно более элементарным путем получать результаты, подобные результатам Гаусса и Якоби, привлекая символ Лежандра и теорию бинарных квадратичных форм.

Теорема 6 (Штилькельбергера–Вороной). Пусть $f(x)$ — неприводимый над полем Q полином n-ей степени, $n < 1$, с целыми коэффициентами, тогда, если простое число p не делит дискриминант d полинома $f(x)$, то число компонент факторизации по модулю p удовлетворяет равенству

$$\left(\frac{d}{p}\right) = (-1)^{n-r},$$

где $\left(\frac{d}{p}\right)$ символ Лежандра. Таким образом, если $f(x)$ — неприводимый над Q полином 3-ей степени и дискриминантом d, а p — простое число не делящее d, то факторизационный тип полинома кубического полинома $f(x)$ по модулю p будет (1, 2), только если выполняется равенство $\left(\frac{d}{p}\right) = -1$.

Справедлива следующая теорема [10, 11].

Теорема 7 (Вороной–Хассе). Пусть d_k — дискриминант кубического расширения полей K/Q, определенный каким-нибудь корнем неприводимого кубического полинома с целыми коэффициентами. Тогда все целочисленные квадратичные бинарные формы дискриминанта d_k распадаются на число классов n, которое делится на 3. Вполне определенная треть этих классов квадратичных форм представляет те и только те числа p, для которых

полином $f(x)$ по модулю p имеет факторизационный тип (1, 1, 1), а остальные две трети те и только те простые числа, для которых факторизационный тип по модулю p имеет вид (3), т.е. полином $f(x)$ неприводим по модулю p.

Пример 3. Пусть $f(x) = x^3 + x^2 - 2x - 1$, тогда этот полином имеет циклическую группу 3-го порядка в качестве группы Галуа, дискриминант $d(f) = 7^2 = 49$. Найдем бинарную квадратичную форму $ax^2 + bxy + cy^2$ с дискриминантом 7^2.

Из равенства $b^2 - 4ac = 7^2$ имеем

$$ax^2 + bxy + cy^2 = \\ = a\left(x - \frac{b+7}{2a}y\right)\left(x - \frac{b-7}{2a}y\right) = p. \quad (2)$$

Можно принять $a = 1$ и тогда из (2) получим две системы

$$\left\{ \begin{array}{l} x - \frac{b+7}{2} = 1; \\ x - \frac{b-7}{2} = p, \end{array} \right. \text{ и } \left\{ \begin{array}{l} x - \frac{b+7}{2} = p; \\ x - \frac{b-7}{2} = 1. \end{array} \right. \quad (3)$$

Из (3) имеем $p \equiv 1 \pmod 7$ и $p \equiv -1 \pmod 7$, следовательно, $Spl(f(x)) = \{p$ — простое : $p \equiv 1 \pmod 7$ или $p \equiv -1 \pmod 7\}$. Для остальных простых $p \equiv +2, +3 \pmod 7$ полином $x^3 + x^2 - 2x - 1$ неприводим по модулю p.

Пример 4. Пусть $f(x) = x^3 - 4x + 2$, он неприводим над полем Q дискриминант $d(x) = -4(-4)^3 - 27 \cdot 4 = 4 \cdot 37 = 148$. Этому дискриминанту соответствует ровно три неэвивалентные собственным образом неопределенные квадратичные формы $g_1 = x^2 - 37y^2$, $g_2 = 3x^2 + 2xy - 12y^2$, $g_3 = 3x^2 - 2xy - 12y^2$.

Области значений квадратичных форм g_2 и g_3 на множестве Z совпадают.

Имеем $g_1(20{,}3) = 400 - 333 = 67$ — простое число. Заметим, что $f(x) = x^3 - 4x + 2 = (x - 18)(x - 21) \pmod{67}$, следовательно, по теореме Вороного–Хассе только простые числа, представимые квадратичной формой $g_1(x, y)$, дают тип факторизации $(1, 1, 1)$ для полинома $f(x)$.

Далее $g_2(5, 2) = 3 \cdot 5^2 - 20 - 48 = 75 - 68 = 7$ — простое число и $f(x)$ по модулю 7 неприводим, следовательно, по теореме Вороного–Хассе простые числа, представимые формой $g_2(x, y)$ или $g_3(x, y)$ (что эквивалентно) дают факторизационный тип (3) для полинома $f(x)$, т.е. он неприводим по этим простым модулям. Если же символ Лежандра $\left(\frac{148}{p}\right) = -1$, т.е. все простые числа, которые удовлетворяют одному из условий

$$p \equiv 2,\ 8,\ 32,\ 17,\ 31,\ 13,\ 15,\ 23,\ 18,\ 35,\ 29,\\ 5,\ 20,\ 6,\ 24,\ 22,\ 12,\ 19 \pmod{37},$$

дают факторизационный тип (1, 2) для полинома $x^3 - 4x + 2$.

Пример 5. Пусть $p = 5$, тогда $p \equiv 5 \pmod 5$ и

$$x^3 - 4x + 2 = (x + 1)(x^2 - x - 3) \bmod 5.$$

Таким способом с помощью теории бинарных квадратичных форм можно исследовать типы факторизаций любых неприводимых полиномов 3-ей степени с целыми коэффициентами и описывать множества простых чисел, дающих определенный тип факторизации по простому модулю для конкретного полинома.

Если мы будем исследовать таким способом полином $x^2 - 2$, то получим теорему Гаусса в такой форме.

Теорема 8. Полином $x^3 - 2$ имеет по простым модулям p следующие типы факторизаций:

1) тип (1,1,1), только если символ Лежандра $\left(\frac{-3}{p}\right) = 1$ и простое число p представимо квадратичной формой $x^2 + 27y^2$;

2) тип (1, 2), только если символ Лежандра $\left(\frac{-3}{p}\right) = -1$;

3) тип (3), только если символ Лежандра $\left(\frac{-3}{p}\right) = 1$ и простое число p представимо квадратичной формой $4x^2 + 2xy + 7y^2$.

Пусть дан неприводимый над полем Q полином $f(x)$ 3-ей степени с неабелевой группой Галуа с целыми коэффициентами и дискриминантом $d(f)$. Пусть также дано простое число p с $\left(\frac{d(f)}{p}\right) = 1$ и две не эквивалентные собственным образом квадратичные формы $g_1(x, y)$ и $g_2(x, y)$ с дискриминантом $d(f)$. Известно, что простые числа, представимые формой $g_1(x, y)$, дают для $f(x)$ факторизационный тип (1,1,1), а простые числа, представимые квадратичной формой $g_2(x, y)$, дают факторизационный тип (3). Нужно определить, какой из этих двух квадратичных форм представили простое число p. Для решения

этого вопроса можно воспользоваться следующей теоремой, являющейся частным случаем более общей теоремы [12].

Теорема 9. Пусть $f(x) = x^3 + sx + r$ — неприводимый над Q полином с целыми коэффициентами, $d = s^2 - 4r^3$, Z_p — поле вычетов по простому модулю p, $GF(p^2)$ — конечное поле из p^2 элементов, тогда:

1) если $p = 3k + 2$, символ Лежандра $\left(\frac{d}{p}\right) = 1$, то полином $f(x)$ по модулю p имеет факторизационный тип $(1; 2)$;

2) если $p = 3k + 1$, $\left(\frac{d}{p}\right) = -1$, то полином $f(x)$ по модулю p имеет факторизационный тип $(1; 2)$;

3) если $p = 3k+1$, $\left(\frac{d}{p}\right) = 1$ и $\left(\frac{s+\sqrt{\delta}}{2}\right)^{\frac{p-1}{3}} = 1$, то полином $f(x)$ по модулю p имеет факторизационный тип $(1, 1, 1)$;

4) если $p = 3k+2$, $\left(\frac{d}{2}\right) = -1$ и $\left(\frac{s+\sqrt{\delta}}{2}\right)^{\frac{p-1}{3}} \neq +1$, то полином $f(x)$ по модулю p неприводим, т.е. имеет факторизационный тип (3);

5) если $p = 3k+2$, $\left(\frac{d}{2}\right) = -1$ и $\left(\frac{s+\sqrt{\delta}}{2}\right)^{\frac{p^2-1}{3}} = +1$ в $GF(p^2)$, то полином имеет по модулю p имеет факторизационный тип $(1, 1, 1)$;

6) если $p = 3k+2$, $\left(\frac{d}{2}\right) = -1$ и $\left(\frac{s+\sqrt{\delta}}{2}\right)^{\frac{p^2-1}{3}} \neq +1$ в $GF(p^2)$, то полином $f(x)$ по модулю p неприводим, т.е. имеет факторизационный тип (3).

Итак, если для данного простого числа p и неприводимого кубического полинома $f(x) = x^3 + sx + r$ с целыми коэффициентами символ Лежандра $\left(\frac{-4s^3-27r^2}{p}\right) = +1$ и выполняется либо пункт 3), либо 5) теоремы, то простое число p представляется квадратичной формой $g_1(x, y)$. Если же выполняется пункт 4) или пункт 6), то простое число p представляется квадратичной формой $g_2(x, y)$.

Для решения предыдущего вопроса можно также воспользоваться теоремой Коши [13].

Теорема 10 (Коши). Пусть A и B — целые числа и p — такое простое число, что $p < 2$ не делит $A \cdot B$, символ Лежандра $\left(\frac{-4s^3-27B^2}{p}\right) = +1$.

Определим целое A_1 из сравнения $A \equiv 3A_1 (\mathrm{mod}\, p)$ и пусть $\{U_n\} n = 0, 1, 2 \ldots$ — последовательность целых чисел определяемая в виде

$$U_n + 2 + BU_{n+1} = A_1^3,$$

$$U_n = 0, \quad U_0 = 2, \quad U_1 = -B.$$

Тогда полином $x^3 + Ax + B$ факторизуется по модулю p в произведение трех линейных множителей, если выполняются соотношения:

$$\frac{U(p-1)}{3} = 2 (\mathrm{mod}\, p) \text{ для } p \equiv 1 (\mathrm{mod}\, 3),$$

$$\frac{U(p+1)}{3} = -2A_1 (\mathrm{mod}\, p) \text{ для } p \equiv 2 (\mathrm{mod}\, 3).$$

Полином $x^3 + Ax + B$ неприводим по модулю p, если

$$\frac{U(p-1)}{3} = -1 (\mathrm{mod}\, p) \text{ для } p \equiv 1 (\mathrm{mod}\, 3),$$

$$\frac{U(p+1)}{3} = A1 (\mathrm{mod}\, p) \text{ для } p \equiv 2 (mod 3).$$

Заключение

Из содержания статьи следует, что для любого полинома $f(x)$ третьей степени с целыми коэффициентами, неприводимого над полем рациональных чисел Q, всегда можно найти условия, характеризующие простые числа p, по модулю которых полином $f(x)$ имеет определенный тип расщепления в произведение неприводимых по модулю p полиномов. В частности, можно описать множество простых чисел, входящих в $Spl(f(x))$. Отметим также, что для любого полинома четвертой степени с целыми коэффициентами подобная задача полностью еще не решена.

Литература

1. *Айерленд К., Раузен М.* Классическое введение в современную теорию чисел, М.: Мир, 1987.
2. Алгебраическая теория чисел / под ред. Дж. Кассельса, А. Фрёлиха. М.: Мир, 1969.
3. *Сергеев А.Э., Яковлев А.В.* О спектрах Галуа многочленов, зависящих от целочисленных параметров // Записки научных семинаров Санкт-Петербургского отделения математического института имени В.А. Стеклова РАН. 2005. Т. 321. С. 275–280.

4. *Sergeev A.E., Yakovlev A.V.* On Galois spectra of polynomials with integral parameters // Journal of Mathematical Sciences. 2006. Vol. 136. Iss. 3. C. 3984–3987.
5. *Чеботарев Н.* Основы теории Галуа. Л.: ГТТИ, 1934.
6. *Сергеев А.Э., Сергеев Э.А.* Основы теории Галуа. Краснодар: Изд-во КубГУ, 2014. 334 с.
7. *Сергеев А.Э., Сергеев Э.А., Титов Г.Н., Соколова И.В.* Теория чисел. Учеб.-метод. рекомендации и контрольные работы. Краснодар: Изд-во КубГУ, 2010.
8. *Лихарева Ю.А., Сергеев А.Э., Сергеев Э.А.* О функции Эйлера // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2017. № 127. С. 113–125.
9. *Сергеев А.Э., Соколова И.В.* Реализация групп Галуа триномами над полем рациональных чисел Q // Политематический сетевой электронный научный журнал Кубанского государственного аграрного университета. 2017. № 131. С. 1497–1524.
10. *Hasse H.* Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage // Math. Zeitchr. 1930. Bd. 31, No. 4. S. 565–582.
11. *Делоне Б., Фадеев Д.* Теория иррациональностей третьей степени. М.: Изд.. мат. ин-та АН СССР, 1940.
12. *Сергеев Э.А.* Научные труды Кубанского университета: Вып. 166: Исследования по алгебре. Краснодар: Кубанский университет, МВ и ССО РСФСР, 1973. 98 с.
13. *Cauchy A.* Exercices de mathématiques, volume 4. Paris, 1829. 420 p.

References

1. Ayerlend, K., Rauzen, M. *Classical introduction to the modern theory of numbers*. Mir, Moscow, 1987. (In Russian)
2. Kassel's, Dzh., Frelikh, A. (eds.) *Algebraic number theory*. Mir, Moscow, 1969. (In Russian)
3. Sergeev, A.E., Yakovlev, A.V. On Galois spectra of polynomials that depend on integer parameters. *Zapiski nauchnykh seminarov Sankt-Peterburgskogo otdeleniya matematicheskogo instituta imeni V.A. Steklova RAN* [Scientific seminars notes of the St. Petersburg branch of the Steklov mathematical Institute of RAS], 2005, vol. 321, pp. 275–280. (In Russian)
4. Sergeev, A.E., Yakovlev, A.V. On Galois spectra of polynomials with integral parameters. *J. of Mathematical Sciences*, 2006, vol. 136, iss. 3, pp. 3984–3987.
5. Chebotarev, N. *Foundations of Galois theory*, GTTI, Leningrad, 1934. (In Russian)
6. Sergeev, A.E., Sergeev, E.A. *Foundations of Galois theory*. Izd-vo KubGU, Krasnodar, 2014. (In Russian)
7. Sergeev, A.E., Sergeev, E.A., Titov, G.N., Sokolova, I.V. *Number theory. Educational and methodical recommendations and control works*, Izd-vo KubGU, Krasnodar, 2010. (In Russian)
8. Likhareva, Yu.A., Sergeev, A.E., Sergeev, E.A. About Euler function. *Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta* [Polythematic network electronic scientific journal of Kuban state agrarian University], 2017, no. 127, pp. 113–125. (In Russian)
9. Sergeev, A.E., Sokolova, I.V. Realization of Galois groups by trinoma over the field of rational numbers Q. *Politematicheskiy setevoy elektronnyy nauchnyy zhurnal Kubanskogo gosudarstvennogo agrarnogo universiteta* [Polythematic network electronic scientific journal of Kuban state agrarian University], 2017, no. 131, pp. 1497–1524. (In Russian)
10. Hasse, H. Arithmetische Theorie der kubischen Zahlkörper auf klassenkörpertheoretischer Grundlage. *Math. Zeitchr.*, 1930, bd. 31, no. 4, pp. 565–582.
11. Delone, B., Fadeev, D. *The theory of irrationalities of the third degree*, Mathematical Institute Academy of Science USSR Press., 1940. (In Russian)
12. Sergeev, E.A. *Scientific works of Kuban State University, vol. 166: Algebra Studies*. Kuban State University Press, Krasnodar, 1973. (In Russian)
13. Cauchy A. *Exercices de mathématiques*, vol. 4. Paris, 1829.

Статья поступила 28 июня 2018 г.