Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2024. Т. 24, вып. 2. С. 193–199
Izvestiya of Saratov University. Mathematics. Mechanics. Informatics, 2024, vol. 24, iss. 2, pp. 193–199
https://mmi.sgu.ru https://doi.org/10.18500/1816-9791-2024-24-2-193-199, EDN: XHDOSA

Научная статья
УДК 519.688

Алгоритмический поиск целых абелевых корней многочлена с целыми абелевыми коэффициентами

Л. М. Цыбуля

Московский педагогический государственный университет, Россия, 119435, г. Москва, ул. Малая Пироговская, д. 1, стр. 1

Цыбуля Лилия Михайловна, кандидат физико-математических наук, доцент кафедры алгебры, https://orcid.org/0000-0001-7062-8782, AuthorID: 505215, liliya-kinder@mail.ru

Аннотация. В работе рассматриваются операции над целыми абелевыми числами ранга n. Такие числа по определению являются элементами поля комплексных чисел и имеют вид многочленов с целыми коэффициентами от заданного первообразного корня из единицы степени n, при этом степени таких многочленов ограничены функцией Эйлера $\varphi(n)$. Приведен пример, показывающий, что внутри круга на комплексной плоскости можно найти бесконечно много целых абелевых чисел. Для описанных операций, в частности, представлен алгоритм вычисления обратного для данного целого абелева числа ранга n, что позволяет рассматривать не только кольца таких чисел, но и поля целых абелевых чисел. Естественная арифметика, возникающая для таких алгебраических структур, приводит к вопросу об изучении многочленов с целыми абелевыми коэффициентами. Исследуется задача поиска корней таких многочленов. Предложен алгоритм нахождения целых абелевых корней многочленов над кольцом целых абелевых чисел. Этот алгоритм основан на выдвинутом предложении о том, что все корни заданного многочлена ограничены некоторой областью. Проведены компьютерные вычисления, подтверждающие статистическую верность предложения.

Ключевые слова: абелево число, алгоритм, корень многочлена

Благодарности: Идейным руководителем данного исследования был профессор $\boxed{\text{А. В. Гришин}}$ (Московский педагогический государственный университет). Автор также весьма признателен А. А. Прокопцеву за помощь в компьютерных вычислениях.

Для цитирования: *Цыбуля Л. М.* Алгоритмический поиск целых абелевых корней многочлена с целыми абелевыми коэффициентами // Известия Саратовского университета. Новая серия. Серия: Математика. Механика. Информатика. 2024. Т. 24, вып. 2. С. 193–199. https://doi.org/10.18500/1816-9791-2024-24-2-193-199, EDN: XHDOSA

Article

Algorithmic search for integer Abelian roots of a polynomial with integer Abelian coefficients

L. M. Tsybulya

Moscow Pedagogical State University, 1/1 Malaya Pirogovskaya St., Moscow 119435, Russia

Liliya M. Tsybulya, liliya-kinder@mail.ru, https://orcid.org/0000-0001-7062-8782, AuthorID: 505215

Abstract. In this work, we consider the operations over Abelian integers of rank n. By definition, such numbers are elements of the complex field and have the form of polynomials with integer coefficients from the nth degree primitive root of 1. In contrast, the degrees of such polynomials are not greater than Euler's totient function $\varphi(n)$. We provide an example to show that there are infinitely many Abelian integers inside any zero-centered circle on the complex plane. In this work, for considered operations we give in particular the algorithm of calculation of the inverse for the Abelian integer of rank n. It allows us to analyze not only the rings of such numbers but also the fields of Abelian integers. Natural arithmetics for such algebraic structures leads us to study the polynomials with integer Abelian coefficients. Thus, in the presented work we also investigate the problem of finding roots of such polynomials. As a result, we provide an algorithm that finds the integer Abelian roots of the polynomials over the ring of Abelian integers. This algorithm is based on the proposed statement that all roots of the polynomial are bounded by some domain. The computer calculations confirm the statistical truth of the statement.

Keywords: Abelian number, algorithm, polynomial root

Acknowledgements: The ideological leader of this research was Professor $\boxed{\text{A. V. Grishin}}$ (Moscow Pedagogical State University). The author is also very grateful to A. A. Prokoptsev for help with computer calculations.

For citation: Tsybulya L. M. Algorithmic search for integer Abelian roots of a polynomial with integer Abelian coefficients. *Izvestiya of Saratov University. Mathematics. Mechanics. Informatics*, 2024, vol. 24, iss. 2, pp. 193–199 (in Russian). https://doi.org/10.18500/1816-9791-2024-24-2-193-199, EDN: XHDOSA

Введение

Как хорошо известно, абелевы поля, т. е. алгебраические расширения поля рациональных чисел с коммутативной группой Галуа, играют важную роль в алгебре и алгебраической теории чисел. Согласно теореме Кронекера – Вебера эти расширения описываются с помощью так называемых круговых (циклотомических) расширений. Сязанные с этим исследования весьма содержательны и интересны (см. [1]). При этом довольно часто возникают трудные вычислительные вопросы, ответить на которые без применения компьютера не представляется возможным. Именно таким вопросам и посвящена эта работа. Более конкретно, в ней рассматриваются вычисления в целых абелевых числах с применением компьютерной техники (см. [1–5]).

1. Базовые понятия, обозначения и терминология

Как обычно, $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$ — целые, рациональные, вещественные и комплексные числа, ζ — первообразный корень из единицы степени n, $\varphi(n)$ — функция Эйлера, $\Phi_n(x)$ — многочлен деления круга на n частей (минимальный многочлен для ζ).

Определение 1. *Абелево число ранга* n — это число из поля $\mathbb{C}$ вида

$$\alpha = a_0 + a_1\zeta + \ldots + a_{l-1}\zeta^{l-1}, \quad a_i \in \mathbb{Z}, \quad l = \varphi(n). \tag{1}$$

Определение 2. Представление (1) будем называть *каноническим видом числа* α.

Несложно видеть, что представление в каноническом виде единственно.

Определение 3. *Весом абелева числа*, заданного в каноническом виде, называется число $\omega(\alpha) = \max |a_i|$.

Соотношения между весом и модулем данного абелева числа могут быть разными: модуль может совпадать с весом, быть больше и меньше его.

Приведем следующий, на первый взгляд достаточно удивительный, пример того, что модуль целого абелева числа меньше единицы, а его вес при этом может быть сколь угодно большим. Этот пример интересен еще и тем, что он показывает, что внутри круга на комплексной плоскости может быть бесконечно много целых абелевых чисел. Рассмотрим

$$\alpha = 1 - \zeta + \zeta^2,$$

где $\zeta = e^{\pi i/5}$ является примитивным корнем из единицы 5-й степени, $\omega(\alpha) = 1$. Несложно проверить, что $|\alpha| < 1$. При возведении α в натуральную степень величина $|\alpha|$ уменьшается, а вес $\omega(\alpha)$ увеличивается.

Пусть $\mathbb{Q}(\zeta)$ — круговое поле (абелево поле ранга n), $[\mathbb{Q}(\zeta) : \mathbb{Q}] = \varphi(n)$, $\mathbb{Z}_{ab}$ — кольцо целых абелевых чисел, $\mathbb{Z}[\zeta] = \mathbb{Z}_{ab}(\zeta)$ — кольцо целых абелевых чисел ранга n вида (1), например, $\mathbb{Z}[i]$ — кольцо целых гауссовых чисел ранга 4.

Определение 4. Каждое целое абелево число α может быть представлено в виде

$$\alpha = p(\alpha) + q(\alpha),$$

где $p(\alpha)$ имеет вид $p(\alpha) = \Theta u$ и называется *главной частью числа* $p(\alpha)$, Θ — некоторый многочлен от ζ, а u — некоторое целое число, $|u| = \omega(\alpha)$, а $q(\alpha)$ — оставшиеся слагаемые, имеющие меньший вес.

Определение 5. Если $f = f(x) \in \mathbb{Z}[\zeta][x]$ — *многочлен с целыми абелевыми коэффициентами*, то его *весом* называется число $\omega(f) = \max\{\omega(c(f))\}$, где $c(f)$ — множество коэффициентов многочлена $f(x)$.

Пусть $\mathbb{Q}_{ab}(\zeta)$, $\mathbb{Z}_{ab}(\zeta)$ — поле абелевых чисел и кольцо целых абелевых чисел ранга n. Пусть далее $\mathbb{Q}_{ab}$ — поле, порожденное всеми $\mathbb{Q}_{ab}(\zeta)$, а $\mathbb{Z}_{ab}$ — кольцо, порожденное всеми $\mathbb{Z}_{ab}(\zeta)$. Обозначение и терминология объясняются тем, что согласно теореме Кронекера – Вебера $\mathbb{Q}_{ab}$ — максимальное абелево расширение поля $\mathbb{Q}$ (см. [6]).

Если $\lambda = (\lambda_1, \ldots, \lambda_s)$ — набор целых абелевых чисел, то можно рассмотреть соответствующий многочлен с корнями $\lambda_1, \ldots, \lambda_s$,

$$f_\lambda(x) = (x - \lambda_1) \ldots (x - \lambda_s) = x^s \pm \alpha_1 x^{s-1} \mp \ldots \pm \alpha_s,$$

где $\alpha_1 = \lambda_1 + \ldots + \lambda_s$, $\ldots$, $\alpha_s = \lambda_1 \ldots \lambda_s$ — элементарные симметрические функции от λ_i.

Определение 6. Пусть B — произвольное натуральное число. *Полосой ширины B* назовем множество целых абелевых чисел вида

$$S(B) = \{\alpha \in \mathbb{Z}_{ab}(\zeta) \mid \omega(\alpha) \leqslant B\}.$$

В полосе $S(B)$ по понятным причинам конечное число элементов, количество которых может быть очень большим, и это множество может описать компьютер.

2. Действия с абелевыми числами

I. Сложение и умножение абелевых чисел стандартным образом выполняется на компьютере.

II. Деление (деление с остатком) будем выполнять следующим образом. Пусть

$$\alpha = a_0 + a_1\zeta + \ldots + a_{l-1}\zeta^{l-1},$$
$$\beta = b_0 + b_1\zeta + \ldots + b_{l-1}\zeta^{l-1},$$
$$\gamma = \frac{\alpha}{\beta} = c_0 + c_1\zeta + \ldots + c_{l-1}\zeta^{l-1}, \quad a_i, b_i \in \mathbb{Z}, \quad c_i \in \mathbb{Q},$$
$$a(x) = a_0 + a_1 x + \ldots + a_{l-1}x^{l-1}, \quad \alpha = a(\zeta),$$
$$b(x) = b_0 + b_1 x + \ldots + b_{l-1}x^{l-1}, \quad \beta = b(\zeta).$$

Если $\beta \neq 0$, то $b(x)$ не делится на $\Phi_n(x)$. Следовательно, $\big(\Phi_n(x), b(x)\big) = 1$. Таким образом, существуют такие многочлены u и v, что $u\Phi_n(x) + vb(x) = 1$, $u(\zeta)\Phi_n(\zeta) + v(\zeta)b(\zeta) = 1$ и $v(\zeta)b(\zeta) = 1$, $v(\zeta)$ — обратный для $b(\zeta)$ и

$$\frac{\alpha}{\beta} = \frac{\alpha(\zeta)}{\beta(\zeta)} = \alpha(\zeta)v(\zeta) = c_0 + c_1\zeta + \ldots + c_{l-1}\zeta^{l-1}, \quad c_i \in \mathbb{Q}.$$

Пусть $\overline{c} = \overline{c_0} + \overline{c_1}\zeta + \ldots + \overline{c_{l-1}}\zeta^{l-1}$, $c \in \mathbb{Q}$, $\overline{c_i} \in \mathbb{Z}$, $\overline{c_i} = [c_i]$ — целая часть числа c_i. Тогда

$$a = bc, \quad a = bc - \overline{c}b + \overline{c}b, \quad a = b\overline{c} + bc - b\overline{c},$$

где a — делимое, b — делитель, $\overline{c}$ — неполное частное, $bc - b\overline{c} = r$ — остаток.

Определение 7. Назовем b *делителем* a, если остаток r равен нулю, а γ_1 — *собственным делителем числа* γ_2, если γ_1 делит γ_2 и $\omega(\gamma_1) \leqslant \omega(\gamma_2)$.

Псевдокод программы, осуществляющей поиск $v(\zeta)$ — обратного для $b(\zeta)$:
Вход: $b_0, b_1, \ldots, b_{l-1}$ и $f_0, f_1, \ldots, f_{l-1}$ — коэффициенты многочленов $b(x)$ и $\Phi_n(x)$
Выход: $v_0, v_1, \ldots, v_{l-1}$ — коэффициенты многочлена $v(\zeta)$
b := array$[b_i]$, $i = 0, \ldots, l-1$
f := array$[f_i]$, $i = 0, \ldots, l-1$
u := array [0], $i = 0, \ldots, l-1$
v := array [0], $i = 0, \ldots, l-1$
Function Euclidean Algorithm(array b, array f, array u, array v)
q := array [0], $i = 0, \ldots, l-1$
WHILE: размер $b \geqslant$ размера f
mul := последний элемент b / последний элемент f
q[размер b − размер f] := mul
for i from 0 to размер b do
$b[i]$:=$b[i] - mul * f[i]$
удаление лидирующих нулей в b
u_0 := array [0], $i = 0, \ldots, l-1$
v_0 := array [0], $i = 0, \ldots, l-1$
Euclidean Algorithm(f, b, u_0, v_0)
for i from 0 to размер u_0 do
for j from 0 to размер q do
$u[i+j]$:=$v_0[i] - q[j] * u_0[i]$
$v[i]$:=$u_0[i]$
Данная программа используется также для нахождения частного и остатка при делении абелевых чисел.

Пример 1. Абелевы числа ранга 7, деление без остатка:

$$1 + 2\zeta + 3\zeta^2 + 4\zeta^3 + 5\zeta^4 + 6\zeta^5 = (6 + 5\zeta + 4\zeta^2 + 3\zeta^3 + 2\zeta^4 + \zeta^5)(1 + \zeta + \zeta^2 + \zeta^3 + \zeta^4 + \zeta^5),$$
$$-2 - 5\zeta - 6\zeta^2 - \zeta^3 + 4\zeta^4 + 3\zeta^5 = (1 + 5\zeta + 10\zeta^2 + 10\zeta^3 + 5\zeta^4 + \zeta^5)(-1 + \zeta).$$

Пример 2. Абелевы числа ранга 8, деление с остатком:

$$8 + 13\zeta + 21\zeta^2 + 98\zeta^3 = (13 + 9\zeta + 6\zeta^2 + \zeta^3)(5 + 7\zeta^3) + 6 + 10\zeta - 2\zeta^2 + 2\zeta^3.$$

В качестве упражнения можно посмотреть деление с остатком в кольце целых гауссовых чисел $\mathbb{Z}[i]$ и исследовать возможность обобщения на кольцо $\mathbb{Z}_{ab}(\zeta)$.

3. Нахождение целых абелевых корней многочленов над кольцом целых абелевых чисел

Будет предложен алгоритм нахождения целых абелевых корней многочленов $f(x)$ с коэффициентами из $\mathbb{Z}_{ab}(\zeta)$. Возможны два случая:

1) идеальный случай $\deg f = s, \lambda_1, \ldots, \lambda_s$ — целые абелевы корни многочлена f;

2) смешанный случай $\lambda_1, \ldots, \lambda_r$ — целые абелевы корни многочлена f, $1 \leqslant r < \deg f$, а $\lambda_{r+1}, \ldots, \lambda_s$ — неабелевы алгебраические числа.

Случай, когда абелевых корней нет, не рассматривается.

Остановимся на идеальном случае. Пусть дан многочлен степени s вида

$$f(x) = (x - \lambda_1) \dots (x - \lambda_s) = x^s + \alpha_1 x^{s-1} + \dots + \alpha_s,$$

где α_i с точностью до знака — элементарные симметрические функции от корней многочлена f, λ_i — целые абелевы числа. Смешанный случай рассматривается аналогично.

Введем следующую *систему ограничений* L:

$$\omega(\lambda_i) \leqslant \omega(\Psi_1), \quad \omega(\lambda_i) \leqslant \omega(\Psi_2), \quad \dots, \quad \omega(\lambda_i) \leqslant \omega(\Psi_d),$$

где $\Psi_1, \dots, \Psi_d$ — некоторые многочлены с коэффициентами из $\mathbb{Q}$ от $\alpha_0, \alpha_1, \dots, \alpha_s$.

Определение 8. Скажем, что многочлен $f(x)$ является *L-регулярным*, если имеет место система ограничений L.

Нас будут интересовать в первую очередь следующие ограничения на λ_1 (здесь λ_1 — корень многочлена $f(x)$ наибольшего веса). Рассмотрим абелевы числа

$$\begin{gathered}
\Psi_1 = \lambda_1 + \dots + \lambda_s = -\alpha_1, \quad \Psi_2 = \lambda_1^2 + \dots + \lambda_s^2 = \alpha_1^2 - 2\alpha_2, \\
\Psi_3 = \lambda_1^4 + \dots + \lambda_s^4 = \alpha_1^4 - 4\alpha_1^2\alpha_2 + 2\alpha_2^2 + 4\alpha_1\alpha_3 - 4\alpha_4, \\
\Psi_4 = \pm\lambda_1 \dots \lambda_s = \alpha_n, \quad \Psi_5 = \max\bigl(\omega(\alpha_0), \dots, \omega(\alpha_s)\bigr), \quad \Psi_6 = \alpha_1^4, \\
W = \omega(\Psi_1) + \omega(\Psi_2) + \omega(\Psi_3) + \omega(\Psi_4) + \omega(\Psi_5) + \omega(\Psi_6)
\end{gathered}$$

и систему ограничений

$$\begin{gathered}
L_i : \omega(\lambda_1) \leqslant \omega(\Psi_i), \quad i = 1, \dots, 6, \\
L_7 : \omega(\lambda_1) \leqslant W.
\end{gathered}$$

Пусть $S(B_i)$ — *полоса ширины* B_i, заданная условием L_i.

При $i = \overline{1, 6}$ бывают как L_i-регулярные, так и не L_i-регулярные многочлены. Например, $(x - 1 - 3\zeta)(x + 3 + 2\zeta)(x + 2 - \zeta)$ и $(x + 2 + 3\zeta)(x - 1 - \zeta)$ — соответственно не L_3- и не L_5-регулярные многочлены над кольцом целых абелевых чисел ранга 3. Отметим, что не L_7-регулярных многочленов с помощью компьютерных вычислений найдено не было.

Возникает вопрос, как по коэффициентам α_i ограничить веса корней многочлена f, т. е. поместить их в некоторую полосу $S(B)$? Поскольку, как уже отмечалось, множество $S(B)$ конечно, то корни ищутся с помощью компьютера прямым перебором.

Другой возможный подход основан на ограничении модулей корней многочлена $f(x)$, помещении их в некоторый круг на комплексной плоскости и, пользуясь конечностью рассматриваемого множества в этом круге, на применении прямого перебора. Для этого полезно следующее

Предложение 1. *Пусть $f(x) = \alpha_0 x^n + \alpha_1 x^{n-1} + \dots + \alpha_n$, тогда корни $f(x)$ не превосходят по модулю следующих чисел* (см. [7]):

$I.$ $\quad 1 + \max\left|\frac{\alpha_k}{\alpha_0}\right|, \quad k = 1, 2, \dots, n;$

$II.$ $\quad p + \max\left|\frac{\alpha_k}{\alpha_0^{k-1}}\right|, \quad k = 1, 2, \dots, n$, p — *любое положительное число*;

$III.$ $\quad 2\max\sqrt[k]{\left|\frac{\alpha_k}{\alpha_0}\right|}, \quad k = 1, 2, \dots, n;$

$IV.$ $\quad \left|\frac{\alpha_k}{\alpha_0}\right| = \max\sqrt[k-1]{\left|\frac{\alpha_k}{\alpha_1}\right|}, \quad k = 1, 2, \dots, n.$

При этом нужно учесть, что, как показывают примеры, внутри круга может быть бесконечное множество целых абелевых чисел. Предложение 1 может быть использовано для отсеивания лишних чисел из полосы $S(B)$.

3.1. Алгоритм поиска ширины полосы

Мы будем использовать подход, основанный на ограничении веса корней многочлена $f(x)$. Пусть

$$W = \omega(\Psi_1) + \omega(\Psi_2) + \omega(\Psi_3) + \omega(\Psi_4) + \omega(\Psi_5) + \omega(\Psi_6).$$

Далее считаем $\omega(\lambda_1) \leqslant W$ — главная система ограничений, $S(W)$ — соответствующая полоса, имеющая очень большую ширину. Тогда с вероятностью, близкой к 1, корень λ_1 попадает в эту полосу. Можно считать, что с этой вероятностью имеет место

Предложение 2. *Справедливо следующее включение:* $\lambda_1 \in S(W)$.

Доказательство этого предложения основано на довольно сложной цепочке оценок главных частей целых абелевых чисел и здесь не приводится. Мы ограничимся здесь, так сказать, «статистическим доказательством»: предложение 2 имеет место с вероятностью, близкой к 1.

Замечание 1. Интересно, что для ограничения B просто суммы корней λ_i или суммы квадратов корней недостаточно. Эти суммы могут быть по весу меньше любого корня. Однако сумма квадратов намного точнее, чем просто сумма первых степеней. Например, над кольцом целых абелевых чисел третьего ранга 93.1% случайно выбранных многочленов с 20 корнями веса, не превосходящего 7, являются L_1-регулярными и 100% — L_2-регулярными.

Замечание 2. Как правило, проверить L-регулярность можно, только уже найдя корни многочленов, а действовать нужно, находя эти корни и проверяя их на соответствие определению.

Замечание 3. Предложение 2 показывает, что если L_7 — условие, представляющее собой $\omega(\lambda_1) \leqslant W$, то практически любой многочлен $f(x)$ является L_7-регулярным.

Псевдокод программы поиска корней многочлена:
Вход: $\alpha_0, \alpha_1, \ldots, \alpha_n$ — коэффициенты многочлена $f(x)$
Выход: $x_0, x_1, \ldots, x_m$ — корни многочлена $f(x)$
W:=$\omega(\Psi_1) + \omega(\Psi_2) + \omega(\Psi_3) + \omega(\Psi_4) + \omega(\Psi_5) + \omega(\Psi_6)$
F := array$[\alpha_i]$ $i = 0, \ldots, n$
$root$:= array $[-W]$ $i = 0, \ldots, l-1$
WHILE: следующий по весу root
If $F(root)$==0:
print root

4. Алгоритм вычисления вероятностей системы ограничений

Пусть A — множество целых абелевых чисел ранга n, веса $\leqslant 100$ вида

$$\alpha = \alpha_0 + \alpha_1\zeta + \ldots + \alpha_{l-1}\zeta^{l-1},$$

где ζ — первообразный корень из единицы степени n, $\alpha_i \in \{0, \pm 1, \ldots, \pm 100\}$. Рассмотрим сетку ранга n, веса 100 степени s, т. е. множество N неупорядоченных наборов $\lambda = (\lambda_1, \ldots, \lambda_s)$, $\lambda_i \in A$, причем $\omega(\lambda_1) \geqslant \omega(\lambda_2) \geqslant \ldots \geqslant \omega(\lambda_s)$. В множестве A содержится $D = 201^l$ элементов, а в множестве N содержится $\binom{201^l+s-1}{s}$ элементов.

Во время компьютерных вычислений случайным образом выбирались целые абелевы числа из фиксированной полосы, составлялся многочлен с корнями в этих целых абелевых числах и проверялись все 7 условий регулярности. Полученные вероятности для некоторых выборок отражены в таблице, где N_t — число тестов, а пропущенные вероятности $P(L_3)$ равны 1.

Вероятности L-регулярности многочленов с коэффициентами из $\mathbb{Z}_{ab}(\zeta)$
Table. Probabilities of L-regularity of polynomials with coefficients from $\mathbb{Z}_{ab}(\zeta)$

n	$\omega(\lambda_1)$	s	N_t	$P(L_1)$	$P(L_2)$	$P(L_4)$	$P(L_5)$	$P(L_6)$	$P(L_7)$
8	1 000 000	2	10 000	1	1	1	1	1	1
8	7	15	1000	0.996	1	1	1	1	1
8	7	20	1000	0.993	1	1	1	1	1
3	7	20	1000	0.931	1	0.972	1	0.997	1
3	3	2	100 000	0.746	0.980	0.940	0.995	0.894	1
97	10	5	100	1	1	1	1	1	1

Список литературы

1. *Боревич З. И., Шафаревич И. Р.* Теория чисел. Москва : Наука, 1985. 503 с.
2. *Гришин А. В.* О периодической части группы невырожденных 2x2-матриц // Международная конференция, посвященная 90-летию кафедры высшей алгебры механико-математического факультета МГУ. Москва, 2019. С. 26.
3. *Гришин А. В., Цыбуля Л. М.* О кручении в полной линейной группе и алгоритме диагонализации // Фундаментальная и прикладная математика. 2021. Т. 23, вып. 4. С. 55–71.
4. *Murty M. R., Esmond J.* Problems in Algebraic Number Theory. New York : Springer New York, 2004. 369 p. (Graduate Texts in Mathematics, vol. 190). https://doi.org/10.1007/b138452
5. *Гришин А. В., Прокопцев А. А., Цыбуля Л. М.* Алгебра и арифметика целых абелевых чисел и компьютерные вычисления // XIII Белорусская математическая конференция : материалы Междунар. науч. конф. (Минск, 22–25 ноября 2021 г.) : в 2 ч. Минск : Беларуская навука, 2021. Ч. 2. С. 38–39.
6. *Greenberg M. J.* An elementary proof of the Kronecker – Weber theorem // The American Mathematical Monthly. 1974. Vol. 81, iss. 6. P. 601–607. https://doi.org/10.1080/00029890.1974.11993623
7. *Фаддеев Д. К., Соминский И. С.* Сборник задач по высшей алгебре : Для физ.-мат. фак. ун-тов и пед. ин-тов. 10-е изд. Москва : Наука. Физматлит, 1972. 304 с.

References

1. Borevich Z. I., Shafarevich I. R. *Teoriya chisel* [Number Theory]. Moscow, Nauka, 1985. 503 p. (in Russian).
2. Grishin A. V. On the periodic part of the group of non-degenerate 2x2 matrices. In: *Mezhdunarodnaya konferentsiya, posvyashchennaya 90-letiyu kafedry vysshey algebry mekhaniko-matematicheskogo fakul'teta MGU* [International Conference Dedicated to the 90th Anniversary of the Department of Higher Algebra of the Faculty of Mechanics and Mathematics of Moscow State University]. Moscow, 2019, pp. 26 (in Russian).
3. Grishin A. V., Tsybulya L. M. On the torsion in the general linear group and the diagonalization algorithm. *Journal of Mathematical Sciences*, 2023, vol. 269, iss. 4, pp. 479–491. https://doi.org/10.1007/s10958-023-06294-4. Translated from *Fundamentalnaya i Prikladnaya Matematika*, 2021, vol. 23, iss. 4, pp. 55–71.
4. Murty M. R., Esmond J. *Problems in Algebraic Number Theory*. Graduate Texts in Mathematics, vol. 190. New York, Springer New York, 2004. 369 p. https://doi.org/10.1007/b138452
5. Grishin A. V., Prokoptsev A. A., Tsybulya L. M. Algebra and arithmetic of Abelian integers and computer calculations. *XIII Belarusian Mathematical Conference*: Proceedings of the International Scientific Conference, Minsk, November 22–25, 2021. Minsk, Belaruskaya navuka, 2021, pt. 2, pp. 38–39 (in Russian).
6. Greenberg M. J. An elementary proof of the Kronecker – Weber theorem. *The American Mathematical Monthly*, 1974, vol. 81, iss. 6, pp. 601–607. https://doi.org/10.1080/00029890.1974.11993623
7. Faddeev D. K., Sominsky I. S. *Sbornik zadach po vysshey algebre* [Collection of Problems in Higher Algebra]. 10th ed. Moscow, Nauka. Fizmatlit, 1972. 304 p. (in Russian).

Поступила в редакцию / Received 31.10.2022
Принята к публикации / Accepted 13.01.2023
Опубликована / Published 31.05.2024