ДОКЛАДЫ РОССИЙСКОЙ АКАДЕМИИ НАУК. МАТЕМАТИКА, ИНФОРМАТИКА, ПРОЦЕССЫ УПРАВЛЕНИЯ, 2020, том 492, с. 58–61

МАТЕМАТИКА

УДК 511.231

КОЛЬЦА ЦЕЛЫХ В ЧИСЛОВЫХ ПОЛЯХ И РЕШЕТКИ КОРНЕЙ

© 2020 г. Член-корреспондент РАН В. Л. Попов[1,2,*], Ю. Г. Зархин[3,]**

Поступило 20.03.2020 г.
После доработки 20.03.2020 г.
Принято к публикации 24.03.2020 г.

В работе исследуется, может ли корневая решетка быть подобна решетке $\mathbb{O}$ всех целых элементов числового поля K, снабженной внутренним произведением $(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(x \cdot \theta(y))$, где θ – инволюция поля K. Для каждого из следующих трех свойств (1), (2), (3) получена классификация всех пар K, θ, обладающих этим свойством: (1) $\mathbb{O}$ является решеткой корней; (2) $\mathbb{O}$ подобна четной решетке корней; (3) $\mathbb{O}$ подобна решетке $\mathbb{Z}^{[K:\mathbb{Q}]}$. Получены также необходимые условия подобия $\mathbb{O}$ решетке корней других типов. Доказано, что $\mathbb{O}$ не может быть подобна положительно определенной четной унимодулярной решетке ранга ≤ 48, в частности, решетке Лича.

Ключевые слова: числовое поле, кольцо целых, решетка корней

DOI: 10.31857/S2686954320030157

1. Числовые поля являются естественным источником решеток, т.е. пар (L, b), где L – свободный $\mathbb{Z}$-модуль конечного ранга, а $b : L \times L \to \mathbb{Z}$ – невырожденная симметрическая билинейная форма. А именно, пусть K – числовое поле, $n := [K : \mathbb{Q}] < \infty$, а $\mathbb{O}$ – кольцо всех целых элементов поля K. Пусть $\theta \in \mathrm{Aut}K$, $\theta^2 = \mathrm{id}$. Тогда отображение $\mathrm{tr}_{K,\theta}\colon K \times K \to \mathbb{Q}$, $\mathrm{tr}_{K,\theta}(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(x \cdot \theta(y))$ является такой невырожденной симметрической билинейной формой, что если I – ненулевой идеал в $\mathbb{O}$, то $(I, \mathrm{tr}_{K,\theta}) := (I, \mathrm{tr}_{K,\theta}|_{I\times I})$ – решетка ранга n.

Некоторые замечательные решетки имеют вид $(I, \mathrm{tr}_{K,\theta})$. Например, это так для некоторых решеток корней, решетки Кокстера–Тодда, решетки Лича и некоторых других (см. [2–5]). Это приводит к следующей задаче: определить по заданной решетке, изометрична ли она решетке $(I, \mathrm{tr}_{K,\theta})$ для подходящих K, θ, I.

Среди всех ненулевых идеалов кольца $\mathbb{O}$ имеется естественно выделенный, а именно, само $\mathbb{O}$. Это приводит к вопросу о том, какие замечательные решетки изометричны (или, более общо, подобны) решеткам вида $(\mathbb{O}, \mathrm{tr}_{K,\theta})$.

Мы исследуем здесь, может ли $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ быть подобна решетке корней, в частности, может ли сама $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ быть решеткой корней.

2. Для формулировки наших результатов (теорем 1–7) напомним сначала ряд определений и фактов (см. [5–7]), а также введем обозначения и терминологию.

Ненулевая решетка называется решеткой корней, если она изометрична ортогональной прямой сумме (обозначаемой далее $\oplus$) решеток, принадлежащих объединению двух бесконечных серий $\mathbb{A}_\ell$ ($\ell \geq 1$), $\mathbb{D}_\ell$ ($\ell \geq 4$) и четырех спорадических решеток $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$, явное описание которых можно найти в [5, 6]. Все решетки из этого объединения неразложимы (т.е. не представляются в виде ортогональных прямых сумм ненулевых слагаемых). Разложение решетки корней в ортогональную прямую сумму неразложимых решеток (называемых неразложимыми компонентами) однозначно. Мы обозначаем ортогональную прямую

[1] *Математический институт им. В.А. Стеклова Российской академии наук, Москва, Россия*
[2] *Национальный исследовательский университет “Высшая школа экономики”, Москва, Россия*
[3] *Department of Mathematics, Pennsylvania State University, University Park, USA*
**E-mail: popovvl@mi-ras.ru*
***E-mail: zarhin@math.psu.edu*

сумму s копий решетки (L, b) через $(L,b)^s$; при $(L,b) = \mathbb{Z}^1$ решетка $(L,b)^s$ обозначается через $\mathbb{Z}^s$. Характеризация решеток корней дается фундаментальной теоремой Витта [8, 6]: решетка (L, b) является решеткой корней тогда и только тогда, когда форма b положительно определена, а $\mathbb{Z}$-модуль L порожден множеством $\{x \in L \mid b(x,x) = 1$ или $2\}$. Мы говорим, что (L, b) – решетка корней типа I (соответственно, II), если $\mathbb{Z}$-модуль L порожден множеством $\{x \in L \mid b(x,x) = 1\}$ (соответственно, $\{x \in L \mid b(x,x) = 2\}$); первое эквивалентно изометричности (L, b) и $\mathbb{Z}^s$, а второе – четности (L, b). Если решетка корней (L, b) не относится к этим двум типам, мы говорим, что (L, b) – решетка смешанного типа. Решетка (L_1, b_1) называется подобной решетке (L_2, b_2), если существуют такие ненулевые числа $m_1, m_2 \in \mathbb{Z}$, что решетки $(L_1, m_1 b_1)$ и $(L_2, m_2 b_2)$ изометричны. Ненулевая решетка (L, b) называется примитивной, если НОД совокупности чисел $\{b(x,y) \mid x, y \in L\}$ равен 1. Если $(L, b) = (\mathbb{O}, \mathrm{tr}_\theta)$, этот НОД равен такому целому положительному числу m, что $\mathrm{Trace}_{K/\mathbb{Q}}(\mathbb{O}) = m\mathbb{Z}$. Решетка корней тогда и только тогда примитивна (соответственно, четна), когда хотя бы одна ее неразложимая компонента не изометрична $\mathbb{A}_1$ (соответственно, каждая ее неразложимая компонента не изометрична $\mathbb{Z}^1$).

3. Теорема 1 дает классификацию таких пар K, θ, что $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ – решетка корней.

Т е о р е м а 1. *Следующие два свойства пары* K, θ *эквивалентны*:

(a) $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *является решеткой корней*;

(b) K, θ *является одной из следующих пар*:

(b_1) $K = \mathbb{Q}$, $\theta = \mathrm{id}$;

(b_2) $K = \mathbb{Q}(\sqrt{-3})$, θ – *комплексное сопряжение*;

(b_3) $K = \mathbb{Q}(\sqrt{-1})$, θ – *комплексное сопряжение*.

В случаях (b_1), (b_2) *и* (b_3) *решетка* $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *изометрична соответственно решетке корней* $\mathbb{Z}^1$, $\mathbb{A}_2$ *и* $\mathbb{A}_1^2$.

4. Теорема 2 дает классификацию таких пар K, θ, что $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ подобна решетке корней типа I.

Т е о р е м а 2. *Следующие пять свойств пары* K, θ *эквивалентны*:

(a) $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна решетке корней* $\mathbb{Z}^n$;

(b) $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна решетке корней* $\mathbb{A}_1^n$;

(c) $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ *изометрична решетке корней* $\mathbb{Z}^n$;

(d) $(\mathbb{O}, 2\mathrm{tr}_{K,\theta}/m)$ *изометрична решетке корней* $\mathbb{A}_1^n$;

(e) *существует такое* $a \in \mathbb{Z}$, $a > 0$, *что* K *является* 2^a*-м круговым полем*, *а* θ – *комплексным сопряжением при* $a > 1$ *и* $\theta = \mathrm{id}$ *при* $a = 1$.

Если эти свойства выполнены, то $n = 2^{a-1}$ *и* $m = n$.

З а м е ч а н и е 1. В случае (e), пусть $\zeta_{2^a} \in K$ – примитивный корень степени 2^a из единицы, а $x_j := \zeta_{2^a}^j$. Тогда (см. [3], где для d-х круговых полей с $d = 2^a$ и 3^b доказано, что $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ – решетка корней, и описаны ее неразложимые компоненты) множество всех неразложимых компонент решетки $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ совпадает с множеством всех ее подрешеток $\mathbb{Z}x_j$, $0 \le j \le 2^{a-1} - 1$. Для каждого j значение tr_θ/m на (x_j, x_j) равно 1.

5. Теорема 3 дает классификацию пар K, θ, для которых $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ подобна четной примитивной решетке корней.

Т е о р е м а 3. *Следующие четыре свойства пары* K, θ *эквивалентны*:

(a) $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна четной примитивной решетке корней*;

(b) $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ *является четной примитивной решеткой корней*:

(c) n *четно и* $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ *изометрична решетке корней* $\mathbb{A}_2^{n/2}$;

(d) *существуют такие* $a, b \in \mathbb{Z}$, $a > 0$, $b > 0$, *что* K *является* $2^a 3^b$*-м круговым полем*, *а* θ – *комплексным сопряжением*.

Если эти свойства выполнены, *то* $n = 2^a 3^{b-1}$ *и* $m = n/2$.

З а м е ч а н и е 2. В случае (d), пусть ζ_{2^a} и $\zeta_{3^b} \in K$ – соответственно примитивные корни степеней 2^a и 3^b из единицы, а $x_{i,j} := \zeta_{2^a}^i \zeta_{3^b}^j$. Можно доказать, что множество всех неразложимых компонент решетки $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ совпадает с множеством всех ее подрешеток $\mathbb{Z}x_{i,j} + \mathbb{Z}x_{i,j+3^{b-1}}$, $0 \le i \le 2^{a-1} - 1$, $0 \le j \le 3^{b-1} - 1$. Для всех i, j значение tr_θ/m на $(x_{i,j}, x_{i,j})$, $(x_{i,j+3^{b-1}}, x_{i,j+3^{b-1}})$ и $(x_{i,j}, x_{i,j+3^{b-1}})$ равно соответственно 2, 2 и –1.

Поскольку теорема 2 дает классификацию пар K, θ, для которых $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ подобна не примитивной решетке корней, объединение теорем 2 и 3 дает классификацию пар K, θ, для которых $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ подобна решетке корней типа II.

6. Следующая группа наших результатов касается подобия решеток $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ решеткам корней смешанного типа. Ниже через μ_K обозначена (циклическая) группа всех корней из единицы в K.

Т е о р е м а 4. *Если* $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна решетке корней смешанного типа, то*

(a) $m = n > 1$;

(b) *все простые делители числа n разветвлены в расширении полей* $K/\mathbb{Q}$ *и если простое* $p \in \mathbb{Z}$ *разветвлено в* $K/\mathbb{Q}$, *то* $p \le n$; *дискриминант расширения* $K/\mathbb{Q}$ *делится на* n^n;

(c) $|\mu_K| = 2^a$ *для некоторого* $a \in \mathbb{Z}$, $a > 0$; *число* 2^{a-1} *делит n, но не равно ему*;

(d) $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ *изометрична решетке корней* $\mathbb{Z}^{2^{a-1}} \oplus L$, *где L — ненулевая четная решетка корней делящегося на* 2^{a-1} *ранга, а* $\mu_K = \{x \in \mathbb{O} \mid (\mathrm{tr}_{K,\theta}/m)\ (x, x) = 1\}$.

Т е о р е м а 5. *Если K — квадратичное (т.е.* $n = 2$) *поле, то следующие два свойства пары K,* θ *эквивалентны*:

(a) $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна решетке корней смешанного типа*;

(b) *либо K изоморфно* $\mathbb{Q}(\sqrt{2})$ и $\theta = \mathrm{id}$, *либо K изоморфно* $\mathbb{Q}(\sqrt{-2})$ *и* θ *— комплексное сопряжение*.

Если (a), (b) *выполнены, то* $(\mathbb{O}, \mathrm{tr}_{K,\theta}/2)$ *изометрична решетке корней* $\mathbb{Z}^1 \oplus \mathbb{A}_1$.

Т е о р е м а 6. *Если K — кубическое (т.е.* $n = 3$) *вполне вещественное поле и* $\theta = \mathrm{id}$, *то следующие свойства пары K,* θ *эквивалентны*:

(a) $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна решетке корней смешанного типа*;

(b) *K — максимальное вполне вещественное подполе 9-го кругового поля*.

Если (a), (b) *выполнены, то* $(\mathbb{O}, \mathrm{tr}_{K,\theta}/3)$ *изометрична решетке корней* $\mathbb{Z}^1 \oplus \mathbb{A}_2$.

Следующая группа примеров дает бесконечные серии пар K, θ, для которых $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ подобна решетке корней смешанного типа. Основой конструкции являются круговые поля $\mathbb{Q}(\zeta_d)$, где ζ_d — примитивный корень степени d из единицы, и их максимальные вполне вещественные подполя $\mathbb{Q}(\zeta_d)^+ := \mathbb{Q}(\zeta_d + \zeta_d^{-1})$.

П р и м е р ы. (1) Пусть $a \in \mathbb{Z}$, $a > 2$, а $K = \mathbb{Q}(\zeta_{2^a})^+$, $\theta = \mathrm{id}$. Тогда (см. [1]) $m = n = 2^{a-2}$ и $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ изометрична решетке корней $\mathbb{Z}^1 \oplus \mathbb{A}_1^{2^{a-2}-1}$.

(2) Пусть $b \in \mathbb{Z}$, $b > 1$, а $K = \mathbb{Q}(\zeta_{3^b})^+$, $\theta = \mathrm{id}$. Тогда (см. [3]) $m = n = 3^{b-1}$ и $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ изометрична решетке корней $\mathbb{Z}^1 \oplus \mathbb{A}_2^{(3^{b-1}-1)/2}$.

(3) Пусть $a \in \mathbb{Z}$, $a > 2$, а $K = \mathbb{Q}(\zeta_{2^a} - \zeta_{2^a}^{-1}) \subset \mathbb{Q}(\zeta_{2^a})$, θ — комплексное сопряжение (поле K является чисто мнимым квадратичным расширением вполне вещественного поля $\mathbb{Q}(\zeta_{2^{a-1}})^+$). Тогда (см. [4]) $m = n = 2^{a-2}$ и $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ изометрична решетке корней $\mathbb{Z}^1 \oplus \mathbb{A}_1^{2^{a-2}-1}$.

(4) Пусть $a, b \in \mathbb{Z}$, $a > 1$, $b > 1$, а $K = \mathbb{Q}(\zeta_{2^a}) \otimes_{\mathbb{Q}} \mathbb{Q}(\zeta_{3^b})^+ = \mathbb{Q}(\zeta_{2^a}(\zeta_{3^b} + \zeta_{3^b}^{-1})) \subseteq \mathbb{Q}(\zeta_{2^a 3^b})$, θ — комплексное сопряжение. Можно доказать тогда, что $m = n = 2^{a-1}3^{b-1}$ и $(\mathbb{O}, \mathrm{tr}_{K,\theta}/m)$ изометрична решетке корней $\mathbb{Z}^{2^{a-1}} \oplus \mathbb{A}_2^{2^{a-2}(3^{b-1}-1)}$.

7. Наш заключительный результат касается вопроса о том может ли $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ быть подобна положительно определенной четной унимодулярной решетке.

Т е о р е м а 7. *Не существует такой пары K,* θ, *что решетка* $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна положительно определенной четной унимодулярной решетке ранга* ≤ 48.

С л е д с т в и е. *Не существует такой пары K,* θ, *что решетка* $(\mathbb{O}, \mathrm{tr}_{K,\theta})$ *подобна решетке Лича*.

ИСТОЧНИК ФИНАНСИРОВАНИЯ

Ю.Г. Зархин выполнил работу при частичной поддержке Simons Foundation Collaboration, grant #585711.

СПИСОК ЛИТЕРАТУРЫ

1. *Andrade A.A., Interlando J.C.* Rotated $\mathbb{Z}^n$-lattices via real subfields of $\mathbb{Q}(\zeta_{2^r})$ // TEMA – Tend. em Mat. Apl. e Comput. 2019. V. 20. № 3. P. 445–456.
2. *Bayer-Fluckiger E.* Lattices and number fields // Contemporary Math. 1999. V. 241. P. 69–84.
3. *Bayer-Fluckiger E.* Upper bounds for Euclidean minima of algebraic number fields // J. Number Theory. 2006. V. 121. P. 305–323.
4. *Bayer-Fluckiger E., Maciak P.* Upper bounds for the Euclidean minima of abelian fields // J. Théorie des Nombres de Bordeaux. 2015. V. 27. P. 689–697.
5. *Conway J.H., Sloane N.J.A.* Sphere Packing, Lattices and Groups. N.Y.: Springer-Verlag, 1988.
6. *Martinet J.* Perfect Lattices in Euclidean Spaces. B.: Springer-Verlag, 2003.
7. *Milnor J., Husemoller D.* Symmetric Bilinear Forms. B.: Springer-Verlag, 1973.
8. *Witt E.* Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe // Abh. Math. Sem. Univ. Hamb. 1941. V. 14. P. 289–322.

RINGS OF INTEGERS IN NUMBER FIELDS, AND ROOT LATTICES

Corresponding Member of the RAS V. L. Popov[a,b] and Yu. G. Zarhin[c]

[a] *Steklov Mathematical Institute of the Russian Academy of Sciences, Moscow, Russian Federation*

[b] *National Research University "High School of Economics", Moscow, Russian Federation*

[c] *Department of Mathematics, Pennsylvania State University, University Park, USA*

This paper investigates whether a root lattice can be similar to the lattice $\mathbb{O}$ of integers of a number field K endowed with the inner product $(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(x \cdot \theta(y))$, where θ is an involution of the field K. For each of the following three properties (1), (2), (3), a classification of all the pairs K, θ with this property is obtained: (1) $\mathbb{O}$ is a root lattice; (2) $\mathbb{O}$ is similar to an even root lattice; (3) $\mathbb{O}$ is similar to the lattice $\mathbb{Z}^{[K:\mathbb{Q}]}$. The necessary conditions for similarity of $\mathbb{O}$ to a root lattice of other types are also obtained. It is proved that $\mathbb{O}$ cannot be similar to a positive definite even unimodular lattice of rank ≤ 48, in particular, to the Leech lattice.

Keywords: number field, ring of integers, root lattice