OPEN ACCESS
Bulletin of Mathematical Sciences
Vol. 11, No. 3 (2021) 2050021 (22 pages)

DOI: 10.1142/S1664360720500216

Root lattices in number fields

Vladimir L. Popov

Steklov Mathematical Institute, Russian Academy of Sciences
Gubkina 8, Moscow 119991, Russia
popovvl@mi-ras.ru

Yuri G. Zarhin*

Department of Mathematics, Pennsylvania State University
University Park, PA 16802, USA
zarhin@math.psu.edu

Received 9 March 2020
Accepted 11 August 2020
Published 18 September 2020

Communicated by Efim Zelmanov

We explore whether a root lattice may be similar to the lattice $\mathscr{O}$ 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 K. We classify all pairs K, θ such that $\mathscr{O}$ is similar to either an even root lattice or the root lattice $\mathbb{Z}^{[K:\mathbb{Q}]}$. We also classify all pairs K, θ such that $\mathscr{O}$ is a root lattice. In addition to this, we show that $\mathscr{O}$ is never similar to a positive-definite even unimodular lattice of rank ≤ 48, in particular, $\mathscr{O}$ is not similar to the Leech lattice. In Appendix B, we give a general cyclicity criterion for the primary components of the discriminant group of $\mathscr{O}$.

Keywords: Number field; lattice; root lattice; similarity.

Mathematics Subject Classification 2020: 11R04

1. Introduction

Number fields are natural sources of *lattices*, i.e. pairs (L, b), where L is a free $\mathbb{Z}$-module of finite rank and $b\colon L \times L \to \mathbb{Z}$ is a nondegenerate symmetric bilinear form; see [9]. Namely, let K be a number field,

$$n := [K : \mathbb{Q}] < \infty,$$

*Corresponding author.

and let $\mathscr{O}$ be the ring of integers of K. We fix a field automorphism

$$\theta \in \operatorname{Aut} K \quad \text{such that } \theta \text{ is involutive}, \quad \text{i.e. } \theta^2 = \mathrm{id}. \tag{1.1}$$

Then the map

$$\mathrm{tr}_{K,\theta}\colon K \times K \to \mathbb{Q}, \quad \mathrm{tr}_{K,\theta}(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(x \cdot \theta(y)) \tag{1.2}$$

is a nondegenerate symmetric bilinear form such that for every nonzero ideal I in $\mathscr{O}$, the pair $(I, \mathrm{tr}_{K,\theta}) := (I, \mathrm{tr}_{K,\theta}|_{I\times I})$ is a lattice of rank n.

This construction admits a natural generalization, see [2, 3, 10, Chap. 8, §7], and references therein. Namely, let J be a nonzero (fractional) ideal of K, let $a \in K$ be a nonzero element such that $\theta(a) = a$, $\mathrm{Trace}_{K/\mathbb{Q}}(ax \cdot \theta(y)) \in \mathbb{Z}$ for all $x, y \in J$, and let

$$\mathrm{tr}_{K,\theta,J,a}\colon J \times J \to \mathbb{Z}, \quad \mathrm{tr}_{K,\theta,J,a}(x, y) := \mathrm{Trace}_{K/\mathbb{Q}}(ax \cdot \theta(y)).$$

Then $(J, \mathrm{tr}_{K,\theta,J,a})$ is a lattice. The origins of this construction essentially go back to Gauss. Indeed, for $n = 2$ and $a = 1/\mathrm{Norm}_{K/\mathbb{Q}}(J)$, it turns into classical Gauss' construction, which yields correspondence between ideals and binary quadratic forms.

Some remarkable lattices are isometric to the lattices of the form $(J, \mathrm{tr}_{K,\theta,J,a})$. For instance, if K is an mth cyclotomic field, then this is so for the root lattices $\mathbb{A}_{p-1}$ (with prime p), $\mathbb{E}_6$, and $\mathbb{E}_8$, where, respectively, $m = p$, $m = 9$, and $m = 15$, 20, 24. If $m = 21$, this is so for the Coxeter–Todd lattice, and if $m = 35$, 39, 52, 56, 84, for the Leach lattice. A classification of root lattices isometric to the lattices of the form $(J, \mathrm{tr}_{K,\theta,J,a})$ for cyclotomic K is given in [5]. References and more examples see in [2, 3, 10, Chap. 8, §7]. So, given a lattice (L, b), it arises the problem of finding out whether it is isometric to $(J, \mathrm{tr}_{K,\theta,J,a})$ for suitable K, θ, J, a.

Another problem is to find out whether, for a given lattice (L, b) and a nonzero ideal J of K, there exist θ and a such that $(J, \mathrm{tr}_{K,\theta,J,a})$ is isometric to (L, b).

Among all nonzero ideals, there is a distinguished one, namely, $\mathscr{O}$ itself, for which $a = 1$ is a distinguished value suitable for every θ. This leads to the problem of finding remarkable lattices isometric (or, more generally, similar) to lattices of the form $(\mathscr{O}, \mathrm{tr}_{K,\theta})$.

This paper is aimed to explore whether $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ may be similar to a root lattice, in particular, whether $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ itself may be a root lattice. It naturally conjuncts with our previous publication [22]: both papers stem from our wish to explore realizations in number fields of objects associated with root systems.

There is a classical construction of geometric representation of algebraic numbers, which embeds K into a Euclidean space, see, e.g. [6, Chap. 2, Sec. 3; 24, 6.1.2, 10.3.1]. One can ask in which cases this embedding endows $\mathscr{O}$ with a structure of a lattice $(\mathscr{O}, b_K)$ isometric to a root lattice. If the latter holds, then necessarily $b_K(\mathscr{O} \times \mathscr{O}) \subseteq \mathbb{Q}$. In Proposition 2.1 below is proven that this inclusion is equivalent to the existence of an involutive automorphism $\theta \in \operatorname{Aut} K$ such that $b_K = \mathrm{tr}_{K,\theta}$. Therefore, the construction of geometric representation does not provide a new (in comparison with the one we explore here) possibility of naturally endowing $\mathscr{O}$ with a structure of lattice isometric (or even similar) to a root one.

Before formulating our results, we recall some definitions and facts (see [18, Chap. 4, 7, 10, 19]), and introduce some notation.

- A nonzero lattice is called a *root lattice* if it is isometric to orthogonal direct sum of lattices belonging to the union of two infinite series $\mathbb{A}_\ell$ ($\ell \geq 1$), $\mathbb{D}_\ell$ ($\ell \geq 4$), and four sporadic lattices $\mathbb{Z}^1$, $\mathbb{E}_6$, $\mathbb{E}_7$, $\mathbb{E}_8$, whose explicit description is recalled in Appendix A below. All lattices in this union are indecomposable (i.e. inexpressible as orthogonal direct sums of nonzero summands). By Eichler's theorem [19, Theorem 6.4] decomposition of a root lattice as orthogonal direct sum of indecomposable lattices (called its *indecomposable components*) is unique.
- Given a lattice (L, b), we denote the orthogonal direct sum of $s > 0$ copies of (L, b) by $(L, b)^s$. For $(L, b) = \mathbb{Z}^1$, we denote $(L, b)^s$ by $\mathbb{Z}^s$.
- A characterization of root lattices is given by fundamental Witt's theorem.

Theorem (Witt [26]; see also [18, Theorem 4.10.6]). *A lattice* (L, b) *is a root lattice if and only if the following two conditions hold*:

(i) *the form* b *is positive-definite*;
(ii) *the* $\mathbb{Z}$*-module* L *is generated by the set* $\{x \in L \mid b(x, x) = 1 \text{ or } 2\}$.

- The lattices (L_1, b_1) and (L_2, b_2) are called *similar* (equivalently, one of them is called *similar to* the other) if there are nonzero integers m_1, m_2 such that the lattices $(L_1, m_1 b_1)$ and $(L_2, m_2 b_2)$ are isometric.
- A nonzero lattice (L, b) is called a *primitive lattice* if the positive integer
$$d_{(L,b)} := \gcd\{b(x, y) \mid x, y \in L\}, \tag{1.3}$$
is 1. For every nonzero lattice (L, b), the lattice $(L, b/d_{(L,b)})$ is primitive. Two lattices (L_1, b_1) and (L_2, b_2) are similar if and only if the lattices $(L_1, b_1/d_{(L_1,b_1)})$ and $(L_2, b_2/d_{(L_2,b_2)})$ are isometric. A root lattice is nonprimitive if and only if it is isometric to $\mathbb{A}_1^{a_1}$ for some a_1.

We first consider a special case of the problem, namely, explore whether $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ may be a root lattice. The following examples show that such cases do exist.

Example 1.1. Let $n = 1$. Then we have $K = \mathbb{Q}$, $\mathscr{O} = \mathbb{Z}$, $\theta = \mathrm{id}$, and $\mathrm{Trace}_{K/\mathbb{Q}}(x) = x$ for every $x \in K$. Hence in this case $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is the root lattice $\mathbb{Z}^1$ (which is similar but not isometric to $\mathbb{A}_1$).

Example 1.2. Let $n = 2$ and let K be a 3rd cyclotomic field: $K = \mathbb{Q}(\sqrt{-3})$. Let θ be the complex conjugation. Then $\mathscr{O} = \mathbb{Z} + \mathbb{Z}\omega$, where $\omega = (1 + \sqrt{-3})/2$, and
$$\mathrm{Trace}_{K/\mathbb{Q}}(x) = x + \theta(x) = 2\mathrm{Re}(x) \quad \text{for every } x \in K. \tag{1.4}$$
This shows that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is a root lattice isometric to $\mathbb{A}_2$; see [22].

Example 1.3. Let $n = 2$ and let K be a 4th cyclotomic field: $K = \mathbb{Q}(\sqrt{-1})$. Let θ be the complex conjugation. Then $\mathscr{O} = \mathbb{Z} + \mathbb{Z}\sqrt{-1}$, and formula (1.4) still holds. This shows that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is a root lattice isometric to $\mathbb{A}_1^2$; see [22].

Our first main result, Theorem 1.1 below, yields the classification of all pairs K, θ for which $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is a root lattice.

Theorem 1.1. *The following properties of a pair K, θ are equivalent*:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is a root lattice*;
(b) K, θ *is one of the following pairs*:
  - (b_1) $K = \mathbb{Q}$, $\theta = \mathrm{id}$;
  - (b_2) $K = \mathbb{Q}(\sqrt{-3})$, θ *is the complex conjugation*;
  - (b_3) $K = \mathbb{Q}(\sqrt{-1})$, θ *is the complex conjugation.*

We then address the general problem of classifying all pairs K, θ such that the lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar (but not necessarily isometric) to a root lattice (L, b). It appears that such pairs are far from being exhausted by Examples 1.1–1.3. We obtain their complete classifications in both “unmixed” cases, namely, when the $\mathbb{Z}$-module L is generated by the set $\{x \in L \mid b(x, x) = 1\}$ and when it generated by the set $\{x \in L \mid b(x, x) = 2\}$. The first case is precisely the one in which (L, b) is isometric to $\mathbb{Z}^n$. The second is the one in which every indecomposable component of (L, b) is not isometric to $\mathbb{Z}^1$; the latter property, in turn, is equivalent to the evenness of the lattice (L, b). Our next two main results, Theorems 1.2 and 1.3 below, yield these classifications. In these theorems, m denotes the unique positive integer such that

$$\mathrm{Trace}_{K/\mathbb{Q}}(\mathscr{O}) = m\mathbb{Z} \tag{1.5}$$

(such m exists because $\mathrm{Trace}_{K/\mathbb{Q}} \colon \mathscr{O} \to \mathbb{Z}$ is a nonzero additive group homomorphism).

Theorem 1.2. *The following properties of a pair K, θ are equivalent*:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to* $\mathbb{Z}^n$;
(b) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to* $\mathbb{A}_1^n$;
(c) $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *is isometric to* $\mathbb{Z}^n$;
(d) $(\mathscr{O}, 2\mathrm{tr}_{K,\theta}/m)$ *is isometric to* $\mathbb{A}_1^n$;
(e) K *is a* 2^a*th cyclotomic field for a positive integer* a, *and* θ *is the complex conjugation if* $a > 1$, *and* $\theta = \mathrm{id}$ *if* $a = 1$.

If these properties hold, then $n = 2^{a-1}$ *and* $m = n$.

In (e), *let* $\zeta_{2^a} \in K$ *be a* 2^a*th primitive root of unity, and let* $x_j := \zeta_{2^a}^j$. *Then the set of all indecomposable components of the root lattice* $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *coincides with the set of all its sublattices*

$$\mathbb{Z}x_j, \quad 0 \le j \le 2^{a-1} - 1.$$

For every j, *the value of* $\mathrm{tr}_{K,\theta}/m$ *at* (x_j, x_j) *is* 1.

Theorem 1.3. *The following properties of a pair K, θ are equivalent*:

(a) $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is similar to an even primitive root lattice.*
(b) $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *is an even primitive root lattice.*
(c) n *is even and* $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *is isometric to* $\mathbb{A}_2^{n/2}$.
(d) K *is a* 2^a3^b*th cyclotomic field for some positive integers* a *and* b, *and* θ *is the complex conjugation.*

If these properties hold, then $n = 2^a3^{b-1}$ *and* $m = n/2$.

In (d), *let* ζ_{2^a} *and* $\zeta_{3^b} \in K$ *be respectively a primitive* 2^a*th and* 3^b*th root of unity, and let* $x_{i,j} := \zeta_{2^a}^i\zeta_{3^b}^j$. *Then the set of all indecomposable components of the root lattice* $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ *coincides with the set of all its sublattices*

$$\mathbb{Z}x_{i,j} + \mathbb{Z}x_{i,j+3^{b-1}} \quad 0 \le i \le 2^{a-1} - 1, \quad 0 \le j \le 3^{b-1} - 1.$$

For all i, j, *the values of* $\mathrm{tr}_{K,\theta}/m$ *at* $(x_{i,j}, x_{i,j})$, $(x_{i,j+3^{b-1}}, x_{i,j+3^{b-1}})$, *and* $(x_{i,j}, x_{i,j+3^{b-1}})$ *are, respectively*, 2, 2, *and* -1.

Note that if K is a dth cyclotomic field, and θ is the complex conjugation, then for $d = 2^a$, the similarity of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ to $\mathbb{Z}^{2^{a-1}}$ was observed in [4, Proposition 9.1(ii)], and for $d = 2 \cdot 3^b$, the similarity of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ to $\mathbb{A}_2^{3^{b-1}}$ can be deduced from [4, Proposition 9.1(i)].

Since $\mathbb{E}_8$ is the unique (up to isometry) positive-definite even unimodular lattice of rank 8 (see [19, §6]), Theorem 1.3 solves in the negative for $n = 8$ the existence problem of a lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ similar to a positive-definite even unimodular one. Our last main result, Theorem 1.4 below, shows that as a matter of fact the following more general statement holds.

Theorem 1.4. *Every positive-definite even unimodular lattice of rank* ≤ 48 *is not similar to a lattice of the form* $(\mathscr{O}, \mathrm{tr}_{K,\theta})$.

Corollary 1.1. *Every lattice* $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is not similar to the Leech lattice.*

Theorem 1.4 excludes many lattices from being similar to lattices of the form $(\mathscr{O}, \mathrm{tr}_{K,\theta})$: recall [19, Chap. 2, §6] that if $\Phi(r)$ is the number of pairwise nonisometric positive-definite even unimodular lattices of rank r, then $\Phi(8) = 1$, $\Phi(16) = 2$, $\Phi(24) = 24$, $\Phi(32) \ge 10^7$, $\Phi(48) \ge 10^{51}$.

This paper is organized as follows. Theorems 1.1–1.4 are proved, respectively, in Secs. 3–6. Section 2 contains several general auxiliary results used in these proofs and in the proof of Theorem B.1 (see below). At the end of this paper, two short appendices are placed. Appendix A recalls the explicit description of indecomposable root lattices. Appendix B contains a general cyclicity criterion for the primary components of the discriminant group of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ (Theorem B.1). In the first stage of this project, we used another approach to finding a classification of all pairs K, θ such that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to an indecomposable even root lattice. This approach led us to only a partial answer, see [21, Theorems 4, 5] (in contrast, in the present paper we obtain a complete classification, see Theorems 1.2 and 1.3).

However, within this approach we obtained and applied a general cyclicity criterion, which may be useful for other applications. Therefore, we consider it worthwhile to publish it in Appendix B as Theorem B.1.

Conventions, terminology, and notation

Given a lattice (L, b) of rank $r > 0$, we canonically embed L in the vector space $V = L \otimes_{\mathbb{Z}} \mathbb{Q}$ over $\mathbb{Q}$ and extend b to a nondegenerate symmetric bilinear form $V \times V \to \mathbb{Q}$, still denoted by b. If $(L, b) = (\mathscr{O}, \mathrm{tr}_{K,\theta})$, then $r = n$ and V is naturally identified with K. If M is a submodule of the $\mathbb{Z}$-module L, then $(M, b|_{M\times M})$ is called a *sublattice* of (L, b) and denoted just by M.

For every $s \in \mathbb{Z}$, we put

$$(L, b)[s] := \{x \in L \mid b(x, x) = s\}. \tag{1.6}$$

Thus (L, b) is an *even lattice* if and only if $(L, b)[s] = \varnothing$ for all odd s.

$\mathrm{discr}(L, b)$ is the *discriminant* of (L, b), i.e.

$$\mathrm{discr}(L, b) := \det(b(e_i, e_j)) \in \mathbb{Z}, \tag{1.7}$$

where $e_1, \ldots, e_r$ is a basis of L over $\mathbb{Z}$ (the right-hand side of (1.7) does not depend on the choice of basis).

L^* is the *dual of L with respect to b*, i.e.

$$L^* := \{x \in V \mid b(x, L) \subseteq \mathbb{Z}\} \supseteq L. \tag{1.8}$$

The *discriminant group* of (L, b) is the (finite Abelian) group L^*/L.

$\mathrm{discr}\, K/\mathbb{Q} := \mathrm{discr}(\mathscr{O}, \mathrm{tr}_{K,\mathrm{id}})$ is the discriminant of $K/\mathbb{Q}$.

$\mathrm{Trace}_{K/\mathbb{Q}}(x)$ and $\mathrm{Norm}_{K/\mathbb{Q}}(x)$ are, respectively, the trace and norm over $\mathbb{Q}$ of an element $x \in K$.

$\mathfrak{c}$ and $\mathfrak{d}$ are, respectively, the *codifferent* and *different* of $K/\mathbb{Q}$, i.e.

$$\mathfrak{c} \text{ is the dual of } \mathscr{O} \text{ with respect to } \mathrm{tr}_{K,\mathrm{id}}, \tag{1.9}$$

$$\mathfrak{d} := \mathfrak{c}^{-1} := \{x \in K \mid x\mathfrak{c} \subseteq \mathscr{O}\} \tag{1.10}$$

($\mathfrak{c}$ is a fractional ideal of K, $\mathscr{O} \subset \mathfrak{c}$, and $\mathfrak{d}$ is an ideal of $\mathscr{O}$) [14, 20].

If $\mathfrak{a}$ and $\mathfrak{b}$ are nonzero ideals of $\mathscr{O}$ and $\mathfrak{a}$ is prime, then $\mathrm{ord}_{\mathfrak{a}}\mathfrak{b}$ is the highest nonnegative integer t such that $\mathfrak{a}^t \supseteq \mathfrak{b}$.

$K^\theta := \{x \in K \mid \theta(x) = x\}$.

μ_K is the (finite cyclic) multiplicative group of all roots of unity in K.

φ is Euler's totient function.

$\overline{z}$ stands for the complex conjugate of $z \in \mathbb{C}$.

Given a field F, its multiplicative group is denoted by $F^\times$.

2. Generalities

In this section, several auxiliary results are collected. We do not claim priority for all of them and give a reference always when we know it. At the same time, we prove all the statements, wanting to make this paper reasonably self-contained, and because our proofs, while being rather short, provide somewhat more information than can be found in the literature.

Lemma 2.1. *The following properties of a prime p are equivalent*:

(i) $\mathrm{Trace}_{K/\mathbb{Q}}(x) \in p\mathbb{Z}$ *for all* $x \in \mathscr{O}$.
(ii) $\mathrm{Trace}_{K/\mathbb{Q}}(x^p) \in p\mathbb{Z}$ *for all* $x \in \mathscr{O}$.

Proof. (i) $\Rightarrow$ (ii) is clear. We shall prove the inclusion

$$\mathrm{Trace}_{K/\mathbb{Q}}(x^p) - (\mathrm{Trace}_{K/\mathbb{Q}}(x))^p \in p\mathbb{Z} \quad \text{for every } x \in \mathscr{O}, \tag{2.1}$$

which readily implies (ii) $\Rightarrow$ (i). The set of all field embeddings $K \hookrightarrow \mathbb{C}$ contains exactly n elements $\sigma_1, \ldots, \sigma_n$, and for every $x \in K$, we have

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) = x_1 + \cdots + x_n, \quad \text{where } x_i := \sigma_i(x) \tag{2.2}$$

(see, e.g. [13, Chap. 12]). From (2.2) we deduce the existence of a symmetric polynomial $f = f(t_1, \ldots, t_n)$ in variables $t_1, \ldots, t_n$ with integer coefficients such that

$$\begin{aligned} \mathrm{Trace}_{K/\mathbb{Q}}(x^p) - (\mathrm{Trace}_{K/\mathbb{Q}}(x))^p &= (x_1^p + \cdots + x_n^p) - (x_1 + \cdots + x_n)^p \\ &= p \cdot f(x_1, \ldots, x_n). \end{aligned} \tag{2.3}$$

Let $s_i = s_i(t_1, \ldots, t_n)$ be the elementary symmetric polynomial in $t_1, \ldots, t_n$ of degree i. Then f may be represented as a polynomial with integer coefficients in $s_1, \ldots, s_n$ (see, e.g. [17, Chap. V, Theorem 11]). Since, for $x \in \mathscr{O}$, we have $s_i(x_1, \ldots, x_n) \in \mathbb{Z}$ for all i, this implies that $f(x_1, \ldots, x_n) \in \mathbb{Z}$. The latter inclusion and (2.3) yield (2.1). □

Corollary 2.1. *The lattice* $(\mathscr{O}, \mathrm{tr}_{K,\mathrm{id}})$ *is even if and only if the integer* m *is even.*

Proof. This follows from (1.5) and Lemma 2.1 with $p = 2$. □

Lemma 2.2. *Let* (L, b) *be a nonzero lattice of rank* r.

(i) *If* $e_1, \ldots, e_r$ *is a basis of the* $\mathbb{Z}$*-module* L *and* $s_1, \ldots, s_r$ *are the invariant factors of the matrix* $(b(e_i, e_j))$ (*see* [11, (16.6)]), *then the group*

$$\bigoplus_{i=1}^{r} \mathbb{Z}/s_i\mathbb{Z}$$

is isomorphic to the discriminant group of (L, b). *In particular,* $s_1 \cdots s_r = |\mathrm{discr}(L, b)|$ *is the order of the latter group.*
(ii) $\mathrm{discr}(L, b) = d_{(L,b)}^r \mathrm{discr}(L, b/d_{(L,b)})$.
(iii) *If* $(L, b) = (\mathscr{O}, \mathrm{tr}_{K,\theta})$, *then*

(iii$_1$) $d_{(L,b)} = m$ (*in particular,* $d_{(L,b)}$ *is independent of* θ);
(iii$_2$) $n \equiv 0 \bmod m$.

(iv) *The discriminant group of* $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ *is isomorphic to* $\mathscr{O}/\mathfrak{d}$ (*in particular, up to isomorphism, this group is independent of* θ). *Its order is equal to* $|\mathrm{disc}\, K/\mathbb{Q}|$ (*cf.* [4, *Corollary* 2.4])).

(v) *Let* $(L, b/d_{(L,b)})$ *be an even lattice. Then* (L, b) *is also an even lattice, and if, moreover,* $(L, b) = (\mathscr{O}, \mathrm{tr}_{K,\theta})$, *then*

(v_1) $n \equiv 0 \bmod 2$ *and* $n/2 \equiv 0 \bmod m$;

(v_2) $n \equiv 0 \bmod 4$ *for* $\theta = \mathrm{id}$.

Proof. (i) Let $e_1^*, \ldots, e_r^*$ be the basis of V dual to $e_1, \ldots, e_r$ with respect to b, i.e. $b(e_i, e_j^*) = \delta_{ij}$. In view of (1.8), since $L = \mathbb{Z}e_1 \oplus \cdots \oplus \mathbb{Z}e_n$, we have $L^* = \mathbb{Z}e_1^* \oplus \cdots \oplus \mathbb{Z}e_n^*$. On the other hand, $e_i = \sum_{j=1}^r b(e_i, e_j)e_j^*$, i.e. $(b(e_i, e_j))$ is the change-of-basis matrix for passing from $e_1^*, \ldots, e_n^*$ to $e_1, \ldots, e_n$. Since the Smith normal form of this matrix is $\mathrm{diag}(s_1, \ldots, s_r)$, this implies the claim.

(ii) This follows from (1.3) and (1.7).

(iii_1) Since $\theta(\mathscr{O}) = \mathscr{O}$, and $1 \in \mathscr{O}$, we have $\{x \cdot \theta(y) \mid x, y \in \mathscr{O}\} = \mathscr{O}$. Combining this with (1.2), (1.3), (1.5), we obtain the desired equality.

(iii_2) This follows from (iii_1) and (1.3) because

$$\mathrm{tr}_{K,\theta}(1, 1) = \mathrm{Trace}_{K/\mathbb{Q}}(1) = n. \tag{2.4}$$

(iv) It follows from $\theta(\mathscr{O}) = \mathscr{O}$ and formulas (1.2), (1.8), (1.9), (1.10) that $\mathfrak{c}$ is the dual of $\mathscr{O}$ with respect to $\mathrm{tr}_{K,\theta}$. Therefore, the discriminant group of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is $\mathfrak{c}/\mathscr{O}$. By [11, (4.15), p. 85], the latter group is isomorphic to $\mathfrak{c}\mathfrak{d}/\mathscr{O}\mathfrak{d}$. Since $\mathfrak{c}\mathfrak{d} = \mathscr{O}$ and $\mathscr{O}\mathfrak{d} = \mathfrak{d}$, this proves the first claim.

By (i), the order of the discriminant group of $(\mathscr{O}, \mathrm{tr}_{K,\mathrm{id}})$ is $|\mathrm{disc}\, K/\mathbb{Q}|$. Since, by the first claim, this group is isomorphic to the discriminant group of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$, this proves the second claim.

(v) The first claim follows from (1.3). Let $(L, b) = (\mathscr{O}, \mathrm{tr}_{K,\theta})$. By ($\mathrm{iii}_1$), the lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is even. By (2.4) this implies that n/m is an even integer; whence (v_1). If, moreover, $\theta = \mathrm{id}$, then m is even by Corollary 2.1; whence (v_2) because of the second formula in (v_1). □

Remark 2.1. By Corollary 2.1 and Lemma 2.2(iii_1), if an even lattice (L, b) is isometric to a lattice of the form $(\mathscr{O}, \mathrm{tr}_{K,\mathrm{id}})$, then necessarily $d_{(L,b)}$ is even; in particular, (L, b) is not primitive. For instance, this shows that $(\mathscr{O}, \mathrm{tr}_{K,\mathrm{id}})$ cannot be a primitive even root lattice.

For any root lattice (L, b), the form b is positive-definite. Hence if (L, b) and $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ are similar, then $\mathrm{tr}_{K,\theta}$ is a definite form. The following Lemma 2.3 describes when the latter happens.

Lemma 2.3. *The following properties of a pair* K, θ *are equivalent*:

(i) $\mathrm{tr}_{K,\theta}$ *is a definite bilinear form*;

(ii) $\mathrm{tr}_{K,\theta}$ *is a positive-definite bilinear form*;

(iii) *either K is a totally real field and $\theta = \mathrm{id}$, or K is a CM-field and θ is the complex conjugation.*

Proof. By (2.4), $\mathrm{tr}_{K,\theta}(1,1) > 0$; whence (i) $\Leftrightarrow$ (ii).

Let r_1 (respectively, r_2) be the number of real (respectively, pairs of imaginary) field embeddings $K^\theta \hookrightarrow \mathbb{C}$. If $\theta \neq \mathrm{id}$, then $[K : K^\theta] = 2$ and $K = K^\theta(\sqrt{a})$ for $a \in K^\theta$; let s be the number of field embeddings $\iota\colon K^\theta \hookrightarrow \mathbb{R}$ such that $\iota(a) < 0$. The signature of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is then given by

$$\mathrm{sign}(\mathscr{O}, \mathrm{tr}_{K,\theta}) = \begin{cases} (r_1 + r_2, r_2) & \text{if } \theta = \mathrm{id}, \\ (r_1 + 2r_2 + s, r_1 + 2r_2 - s) & \text{if } \theta \neq \mathrm{id}; \end{cases} \tag{2.5}$$

see [2, Proposition 2.2]. From (2.5) one readily deduces (ii) $\Leftrightarrow$ (iii). □

Note that

$$\begin{aligned} &\text{if } K \text{ is a CM-field and } \theta \text{ is the complex} \\ &\text{conjugation, then } n \text{ is even, } [K^\theta : \mathbb{Q}] = n/2, \\ &\text{and } (\mathrm{discr}\, K^\theta/\mathbb{Q})^2 \text{ divides } \mathrm{discr}\, K/\mathbb{Q}; \end{aligned} \tag{2.6}$$

see, e.g. [20, Chap. III, Corollary (2.10)].

Corollary 2.2. *For a pair K, θ, if the lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to a root lattice, then either K is a totally real field and $\theta = \mathrm{id}$, or K is a CM-field and θ is the complex conjugation.*

Lemma 2.4 (cf. [1, Lemma 2]). *Let $\sigma_1, \ldots, \sigma_n$ be the set of all field embeddings $K \hookrightarrow \mathbb{C}$. Let $x \in \mathscr{O}$ be an element such that $\sigma_i(x)$ is a positive real number for every i. Then the following hold:*

(i) $\mathrm{Trace}_{K/\mathbb{Q}}(x)$ *is a positive integer and*

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) \geq n; \tag{2.7}$$

(ii) *the equality in* (2.7) *holds if and only if $x = 1$.*

Proof. The equalities

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) = \sum_{i=1}^{n} \sigma_i(x), \quad \mathrm{Norm}_{K/\mathbb{Q}}(x) = \prod_{i=1}^{n} \sigma_i(x) \tag{2.8}$$

(see, e.g. [13, Chap. 12]) imply that $\mathrm{Trace}_{K/\mathbb{Q}}(x)$ and $\mathrm{Norm}_{K/\mathbb{Q}}(x)$ are positive integers. Combining (2.8) with the classic inequality of arithmetic and geometric means (see, e.g. [23, Sec. 2]), we then obtain the inequalities

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) \geq n \cdot \mathrm{Norm}_{K/\mathbb{Q}}(x) \geq n \cdot 1 = n. \tag{2.9}$$

This proves (i).

If $x = 1$, then the equality in (2.7) holds by (2.4). Conversely, assume that the equality in (2.7) holds for some x. In view of (2.9) we then conclude that

$$\mathrm{Norm}_{K/\mathbb{Q}}(x) = 1 \tag{2.10}$$

and the equalities in (2.9) hold too. The classic inequality of arithmetic and geometric means tells us that the latter happens if and only if $\sigma_1(x) = \cdots = \sigma_n(x)$, i.e. x is a positive integer. From (2.10) and (2.8) we then obtain $x^n = 1$, hence $x = 1$. This proves (ii). □

The inequality in Lemma 2.5(ii) below can be found in [3, Corollary 4].

Lemma 2.5. *Suppose a pair K, θ enjoys one of the following properties*:

(TR) *K is a totally real field*, $\theta = \mathrm{id}$;
(CM) *K is a CM-field*, *θ is the complex conjugation.*

Then, *for every nonzero element $x \in \mathscr{O}$*, *the following hold*:

(i) *$\mathrm{tr}_{K,\theta}(x, x)$ is a positive integer*;
(ii) *$\mathrm{tr}_{K,\theta}(x, x) \geq n$ and the equality holds if and only if x is a root of unity.*

The condition $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)[s] \neq \varnothing$ (see (1.6)) implies the following:

(a) *$s \geq n/m$*;
(b) *if $s = 1$*, *then $m = n$*;
(c) *if $s = 2$ and $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is even*, *then $m = n/2$*,
(d) *if $s = 4$ and $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is even*, *then $m = n/2$ or $n/4$.*

Proof. First, we note that if $\sigma\colon K \hookrightarrow \mathbb{C}$ is a field embedding, then $\sigma(x \cdot \theta(x))$ is a positive real number. Indeed, if (TR) holds, then

$$\sigma(K) \subset \mathbb{R} \quad \text{and} \quad \sigma(x \cdot \theta(x)) = \sigma(x^2) = (\sigma(x))^2; \tag{2.11}$$

whence the claim in this case. If (CM) holds, then $\sigma(K)$ is stable with respect to the complex conjugation of $\mathbb{C}$ and $\sigma(\theta(x)) = \overline{\sigma(x)}$ (see, e.g. [25, p. 38]). Therefore,

$$\sigma(x \cdot \theta(x)) = \sigma(x)\sigma(\theta(x)) = \sigma(x)\overline{\sigma(x)} = |\sigma(x)|^2, \tag{2.12}$$

which proves the claim in this case.

In view of this, (i) and the inequality in (ii) follow from (1.2) and Lemma 2.4(i). By Lemma 2.4(ii), the equality in (ii) holds if and only if

$$x \cdot \theta(x) = 1. \tag{2.13}$$

Assume that (2.13) holds. Then, in the notation of Lemma 2.4, every complex number $\sigma_i(x)$ has the modulus 1. Since x is an algebraic integer, by Kroneker's theorem [15] (see also, e.g. [25, Lemma 1.6]) this implies that x is a root of unity. Conversely, if x is a root of unity, then, in the above notation, $\sigma(x)$ is a root of unity too, hence the right-hand sides of the equalities in (2.11), (2.12) are equal to 1. Whence, (2.13) holds. This completes the proof of (ii).

Suppose that $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)[s] \neq \varnothing$, i.e. there is an element $a \in \mathscr{O}$ such that $\mathrm{tr}_{K,\theta}(a,a)/m = s$. This and (ii) yield (a).

Since, by Lemma 2.2(iii$_2$), n/m is an integer, it follows from (a) that $m = n$ if $s = 1$. This proves (b).

Suppose, moreover, that $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is even. Then n/m is even by Lemma 2.2(v$_1$). This and (a) then imply that $m = n/2$ if $s = 2$. This proves (c). Finally, if $s = 4$, then (a) implies that $n/m = 2$ or 4. This proves (d). □

Lemma 2.6 (cf. [4, Proposition 9.1(ii)]). *Fix a positive integer a. Let K be a 2^ath cyclotomic field, let θ be the complex conjugation if $a > 1$ and $\theta = \mathrm{id}$ if $a = 1$, and let $\zeta \in K$ be a 2^ath primitive root of unity. Then the following hold*:

(i) $n = 2^{a-1}$;

(ii) $\{\zeta^j \mid 0 \leq j \leq 2^{a-1} - 1\}$ *is a basis of the $\mathbb{Z}$-module $\mathscr{O}$*;

(iii) *for every elements ζ^i and ζ^j of this basis*,

$$\mathrm{tr}_{K,\theta}(\zeta^i, \zeta^j) = \begin{cases} n & \text{if } i = j, \\ 0 & \text{if } i \neq j; \end{cases}$$

(v) $m = n$.

Proof. We have $n = \varphi(2^a)$ (see [17, Chap. VIII, §3, Theorem 6]); whence (i).

(ii) We have $K = \mathbb{Q}(\zeta)$; therefore, $\mathscr{O} = \mathbb{Z}[\zeta]$ (see [25, Theorem 2.6]). The latter yields (ii) because the degree of the minimal polynomial of ζ over $\mathbb{Q}$ is $n = \mathrm{rank}\,\mathscr{O}$.

(iii) Since θ is the complex conjugation and ζ is a root of unity, we have the equalities $\zeta^i \cdot \theta(\zeta^j) = \zeta^{i-j}$, hence by (1.2),

$$\mathrm{tr}_{K,\theta}(\zeta^i, \zeta^j) = \mathrm{Trace}_{K/\mathbb{Q}}(\zeta^{i-j}). \tag{2.14}$$

If $i = j$, then (2.14) and (2.4) yield $\mathrm{tr}_{K,\theta}(\zeta^i, \zeta^j) = n$.

Let $i \neq j$. The element ζ^{i-j} is a primitive 2^sth root of 1 for some positive integer $s \leq a$; hence its minimal polynomial over $\mathbb{Q}$ is $t^{2^{s-1}} + 1$ (see [17, Chap. VIII, §3]). Since $0 \leq i, j \leq 2^{a-1} - 1$, we have $s \geq 2$. Therefore, the degree of this polynomial is at least 2. This implies that $\mathrm{Trace}_{\mathbb{Q}(\zeta^{i-j})/\mathbb{Q}}(\zeta^{i-j}) = 0$. In turn, from this, (2.14), and the equality

$$\mathrm{Trace}_{K/\mathbb{Q}}(x) = [K : \mathbb{Q}(x)]\mathrm{Trace}_{\mathbb{Q}(x)/\mathbb{Q}}(x) \quad \text{for every } x \in K \tag{2.15}$$

(see, e.g. [27, Chap. II, §10, (9)]), we obtain that $\mathrm{tr}_{K,\theta}(\zeta^i, \zeta^j) = 0$.

(iv) follows from (iii), (1.3), and Lemma 2.2(iii$_1$). □

Lemma 2.7 (cf. [4, Proposition 9.1(i)]). *Fix a positive integer b. Let K be a 3^bth cyclotomic field, let θ be the complex conjugation, and let $\zeta \in K$ be a 3^bth* *primitive root of unity. Then the following hold*:

(i) $n = 2 \cdot 3^{b-1}$;
(ii) $\{\zeta^j \mid 0 \le j \le 2 \cdot 3^{b-1} - 1\}$ *is a basis of the* $\mathbb{Z}$*-module* $\mathscr{O}$;
(iii) *for every two elements* ζ^i *and* ζ^j *of this basis*,

$$\mathrm{tr}_{K,\theta}(\zeta^i, \zeta^j) = \begin{cases} n & \text{if } i = j, \\ 0 & \text{if } 3^{b-1} \text{ does not divide } i - j, \\ -n/2 & \text{if } i \neq j \text{ and } 3^{b-1} \text{ divides } i - j; \end{cases}$$

(iv) $m = n/2$.

Proof. The same argument as in the proof of Lemma 2.6 yields (i), (ii), and (iv).

(iii) Formula (2.14) still holds and the same argument as in the proof of Lemma 2.6(iii) yields the validity of (iii) for $i = j$. Assume now that $i \neq j$. Then ζ^{i-j} is a primitive 3^sth root of unity for some positive integer $s \le b$. The degree of its minimal polynomial over $\mathbb{Q}$ is

$$[\mathbb{Q}(\zeta^{i-j}) : \mathbb{Q}] = \varphi(3^s) = 2 \cdot 3^{s-1}. \tag{2.16}$$

Since the 3rd cyclotomic polynomial is t^2+t+1, this minimal polynomial is $t^{2\cdot 3^{s-1}} + t^{3^{s-1}} + 1$ (see [17, Chap. VIII, §3]). Given that $2 \cdot 3^{s-1} - 3^{s-1} = 1$ if and only if $s = 1$, from this we infer that

$$\mathrm{Trace}_{\mathbb{Q}(\zeta^{i-j})/\mathbb{Q}}(\zeta^{i-j}) = \begin{cases} 0 & \text{if } s \ge 2, \\ -1 & \text{if } s = 1. \end{cases} \tag{2.17}$$

From (i) and (2.16) we obtain that $[K : \mathbb{Q}(\zeta^{i-j})] = [K : \mathbb{Q}]/[\mathbb{Q}(\zeta^{i-j}) : \mathbb{Q}] = n/(2 \cdot 3^{s-1}) = 3^{b-s}$. This, (2.15), and (2.17) then yield

$$\mathrm{Trace}_{K/\mathbb{Q}}(\zeta^{i-j}) = \begin{cases} 0 & \text{if } s \ge 2, \\ -n/2 & \text{if } s = 1. \end{cases} \tag{2.18}$$

Clearly, (2.18) is equivalent to (iii) for $i \neq j$. □

Given a qth cyclotomic field K and a positive integer r dividing q, we denote by K_r and $\mathscr{O}_r$, respectively, the unique rth cyclotomic subfield of K and its ring of integers. They are $\mathrm{Aut}\, K$-stable; for $\alpha \in \mathrm{Aut}\, K$, we denote the restriction $\alpha|_{K_r}$ still by α. If α is the complex conjugation of K, this restriction is the complex conjugation of K_r.

Lemma 2.8. *Let i and j be coprime positive integers. Let K be a ijth cyclotomic field and let θ be the complex conjugation. Then the following hold*:

(i) *the natural* $\mathbb{Q}$*-algebra homomorphism*

$$K_i \bigotimes_{\mathbb{Q}} K_j \to K, \quad x \otimes y \mapsto xy, \tag{2.19}$$

is an isomorphism;

(ii) *for every* $x \in K_i$ *and* $y \in K_j$, *the following equality holds*:

$$\mathrm{Trace}_{K/\mathbb{Q}}(xy) = \mathrm{Trace}_{K_i/\mathbb{Q}}(x)\mathrm{Trace}_{K_j/\mathbb{Q}}(y), \tag{2.20}$$

(iii) *the restriction of homomorphism* (2.19) *to* $\mathscr{O}_i \bigotimes_{\mathbb{Z}} \mathscr{O}_j$ *is a ring isomorphism with* $\mathscr{O}$, *which is also a lattice isometry*

$$(\mathscr{O}_i, \mathrm{tr}_{K_i,\theta}) \otimes_{\mathbb{Z}} (\mathscr{O}_j, \mathrm{tr}_{K_j,\theta}) \to (\mathscr{O}, \mathrm{tr}_{K,\theta}).$$

Proof. Let $\zeta_i \in K_i$ and $\zeta_j \in K_j$ be respectively a primitive ith and a primitive jth root of unity. Then $\zeta_i\zeta_j$ is a primitive ijth root of unity, hence $K = \mathbb{Q}(\zeta_i\zeta_j)$. This shows that K is the compositum of K_i and K_j; whence (2.19) is a surjective homomorphism. The coprimeness of i and j implies that $[K : \mathbb{Q}] = \varphi(ij) = \varphi(i)\varphi(j) = [K_i : \mathbb{Q}][K_j : \mathbb{Q}]$; hence (2.19) is an injective homomorphism. This proves (i).

By definition of the trace of an element of a number field, the left-hand side of (2.20) is the trace of the $\mathbb{Q}$-linear transformation of K given by multiplication by xy. In view of (i), it is equal to the trace of the $\mathbb{Q}$-linear transformation of $\mathbb{Q}(\zeta_i) \bigotimes_{\mathbb{Q}} \mathbb{Q}(\zeta_j)$ given by multiplication by $x \otimes y$. Hence (see [8, Chap. VII, §5, no. 6]) it is equal to the product of traces of the $\mathbb{Q}$-linear transformations of $\mathbb{Q}(\zeta_i)$ and $\mathbb{Q}(\zeta_j)$ given by multiplications by respectively x and y. By the mentioned definition, the latter product is equal to the right-hand side of (2.20). This proves (ii).

In view of the equality $\mathscr{O} = \mathscr{O}_i\mathscr{O}_j$ (see [16, Chap. IV, §1, Theorem 4; 25, Theorem 2.6]) the first statement in (iii) follows from (i). The second follows from the first in view of (1.2), (2.20), and the definition of tensor product of lattices (see [19, Chap. 1, §5]). □

In the next lemma, we use that if K is totally real, then $\mathrm{discr}\, K/\mathbb{Q}$ is positive (see, e.g. [14, Proposition 1.2a]).

Lemma 2.9. *Let* K *be a totally real number field of degree* $n > 1$ *over* $\mathbb{Q}$.

(i) *If* $n \leq 24$, *then* $\sqrt[n]{\mathrm{discr}\, K/\mathbb{Q}} > n$.
(ii) *If* $3 \leq n \leq 75$, *then* $\sqrt[n]{\mathrm{discr}\, K/\mathbb{Q}} > (n+1)^2/2n$.

Proof. This readily follows from [12, Table 2 (Cas Totalement Réel), p. 1]. □

Lemma 2.10. *Let* K *be a CM-field of degree* $n > 2$ *over* $\mathbb{Q}$. *If* $n \leq 48$, *then* $\sqrt[n]{|\mathrm{discr}\, K/\mathbb{Q}|} > n/2$.

Proof. In view of (2.6), we have the inequality

$$\sqrt[n]{|\mathrm{discr}\, K/\mathbb{Q}|} \geq \sqrt[n/2]{\mathrm{discr}\, K^\theta/\mathbb{Q}}. \tag{2.21}$$

The claim then readily follows from the lower bounds on the right-hand side of (2.21), which is obtained by applying Lemma 2.9(i) to the totally real number field K^θ of degree $n/2$. □

Proposition 2.1. *Let E_K be the n-element set of all field embeddings $K \hookrightarrow \mathbb{C}$ and let b_K be the $\mathbb{Q}$-bilinear map*

$$b_K\colon K \times K \to \mathbb{C}, \quad b_K(x, y) := \sum_{\sigma \in E_K} \sigma(x)\overline{\sigma(y)}. \tag{2.22}$$

Then the following hold:

(i) *The $\mathbb{Q}$-linear span of $b_K(K \times K)$ is a proper subset of $\mathbb{R}$ containing $\mathbb{Q}$.*
(ii) *b_K is symmetric and positive-definite.*
(iii) *Properties* (a), (b), (c) *listed below are equivalent*:

- (a) $b_K(K \times K) = \mathbb{Q}$.
- (b) $b_K(\mathscr{O} \times \mathscr{O}) \subseteq \mathbb{Q}$.
- (c) *There is an involutive field automorphism $\tau \in \operatorname{Aut} K$ such that $b_K = \operatorname{tr}_{K,\tau}$.*

(iv) *If* (c) *holds*, *then either K is totally real and $\tau = \operatorname{id}$*, *or K is a CM-field and τ is the complex conjugation.*

Proof. Below we use the notation

$$\iota\colon \mathbb{C} \to \mathbb{C}, \quad \iota(z) := \overline{z}.$$

(i) In view of (2.22) and (2.8), for every $q \in \mathbb{Q}$, we have $b_K(q, 1) = nq$; whence the inclusion $\mathbb{Q} \subseteq b_K(K \times K)$.

For every $\sigma \in E_K$, we have $\iota \circ \sigma \in E_K$; therefore,

$$\iota \circ E_K := \{\iota \circ \sigma \mid \sigma \in E_K\} = E_K. \tag{2.23}$$

From (2.22) and (2.23), for every $x, y \in K$, we deduce the following:

$$\begin{aligned} \overline{b_K(x, y)} &= \sum_{\sigma \in E_K} \overline{\sigma(x)}\sigma(y) = b_K(y, x) \\ &= \sum_{\sigma \in E_K} (\iota \circ \sigma)(x)\overline{(\iota \circ \sigma)(y)} = \sum_{\delta \in \iota \circ E_K} \delta(x)\overline{\delta(y)} \\ &= \sum_{\delta \in E_K} \delta(x)\overline{\delta(y)} = b_K(x, y); \end{aligned} \tag{2.24}$$

whence the inclusion $b_K(K \times K) \subseteq \mathbb{R}$. Since K is countable, while $\mathbb{R}$ is not, this inclusion is proper.

(ii) follows from (2.24) and (2.22).

(iv) follows from (ii) and Lemma 2.3.

(iii) Since $\mathscr{O} \subset K$, we have (a) $\Rightarrow$ (b), and since K is the $\mathbb{Q}$-linear span of $\mathscr{O}$, we have (b) $\Rightarrow$ (a).

Next, (c) $\Rightarrow$ (a) because of (1.2).

Conversely, assume that (a) holds. Then we have two nondegenerate $\mathbb{Q}$-bilinear maps

$$K \times K \underset{b_K}{\overset{\mathrm{tr}_{K,\mathrm{id}}}{\rightrightarrows}} \mathbb{Q}.$$

Therefore, by [17, Chap. XIII, §5] and (1.2), there is a nondegenerate $\mathbb{Q}$-linear map $\tau\colon K \to K$ such that

$$b_K(x, y) = \mathrm{Trace}_{K/\mathbb{Q}}(x \cdot \tau(y)) \quad \text{for all } x, y \in K. \tag{2.25}$$

We claim that τ is an involutive field automorphism of K; if this is proved, then (2.25), (1.2) show that (c) holds.

To prove the claim, we notice that using (2.22) and (2.2), we can rewrite (2.25) as follows:

$$\sum_{\sigma \in E_K} \sigma(x)\overline{\sigma(y)} = \sum_{\sigma \in E_K} \sigma(x)\sigma(\tau(y)) \quad \text{for all } x, y \in K. \tag{2.26}$$

Since for every $\sigma \in E_K$, the map $K^\times \to \mathbb{C}^\times$, $x \mapsto \sigma(x)$, is a group homomorphism, by Artin's theorem on the linear independence of characters [17, Chap. VIII, §4, Theorem 7], we conclude from (2.26) that

$$\overline{\sigma(y)} = \sigma(\tau(y)) \quad \text{for all } \sigma \in E_K,\ y \in K. \tag{2.27}$$

In turn, (2.27) implies that the subfield $\sigma(K)$ of $\mathbb{C}$ is ι-stable and the following diagram, in which $\gamma := \iota|_{\sigma(K)}$, is commutative:

$$\underbrace{K \xrightarrow{\sigma} \sigma(K) \xrightarrow{\gamma} \sigma(K) \xrightarrow{\sigma^{-1}} K}_{\tau}. \tag{2.28}$$

Since each of the upper arrows in (2.28) is a field isomorphism, τ is a field automorphism. Moreover, since $\tau = \sigma^{-1} \circ \gamma \circ \sigma$ and γ (being the restriction of involution ι) is involutive, τ is involutive as well. This completes the proof. $\square$

3. When is $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ a Root Lattice?

Proof of Theorem 1.1. In view of Examples 1.1–1.3, the "if" part is clear. To prove the "only if" one, suppose that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is a root lattice. Then by Corollary 2.2, either K is a totally real field and $\theta = \mathrm{id}$, or K is a CM-field and θ is the complex conjugation.

There are two possibilities, which we will consider separately:

(a) The lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is primitive or, equivalently, at least one of its indecomposable components is not isometric to $\mathbb{A}_1$.

(b) The lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is nonprimitive or, equivalently, it is isometric to $\mathbb{A}_1^{a_1}$ for some a_1.

Our considerations below exploit the fact that

$$\mathrm{discr}\mathbb{A}_\ell = \ell + 1 \quad \text{for every } \ell. \tag{3.1}$$

We first assume that (a) holds. Then

$$m = 1. \tag{3.2}$$

If there is an indecomposable component of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ isometric to $\mathbb{Z}^1$, then $(\mathscr{O}, \mathrm{tr}_{K,\theta})[1] \neq \varnothing$. By Lemma 2.5(b), this and (3.2) imply that $n = 1$, i.e. $K = \mathbb{Q}$ and $\theta = \mathrm{id}$.

If every indecomposable component of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is not isometric to $\mathbb{Z}^1$, then $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is an even lattice and $(\mathscr{O}, \mathrm{tr}_{K,\theta})[2] \neq \varnothing$. By Lemma 2.5(c), from this and (3.2) we deduce that $n = 2$, i.e.

$$K = \mathbb{Q}(\sqrt{c}) \quad \text{for a square free integer } c. \tag{3.3}$$

Since the sum of ranks of all indecomposable components of $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is n, we infer from $n = 2$ and (a) that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is isometric to $\mathbb{A}_2$. This, (3.2), (3.1), and Lemma 2.2(ii), (iii_1), (iv) then imply that

$$|\mathrm{discr}\, K/\mathbb{Q}| = 3. \tag{3.4}$$

On the other hand, (3.3) yields

$$\mathrm{discr}\, K/\mathbb{Q} = \begin{cases} 4c & \text{if } c \equiv 2, 3 \mod 4, \\ c & \text{if } c \equiv 1 \mod 4 \end{cases} \tag{3.5}$$

(see, e.g. [13, Chap. 13, Proposition 13.1.2]). From (3.5) and (3.4) we conclude that $c = -3$; whence $K = \mathbb{Q}(\sqrt{-3})$ and θ is the complex conjugation. This completes the consideration of case (a).

Now we assume that (b) holds. Then $m = 2$ and $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is isometric to $\mathbb{Z}^{a_1}$. Hence $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)[1] \neq \varnothing$. By Lemma 2.5(b), this yields $n = a_1 = 2$, hence again (3.3) and (3.5) hold. From (3.1) and Lemma 2.2(iv) we obtain $|\mathrm{discr}\, K/\mathbb{Q}| = 4$. In view of (3.5), this yields $c = -1$; whence $K = \mathbb{Q}(\sqrt{-1})$ and θ is the complex conjugation. This completes the consideration of case (b). □

4. When is $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ Similar to $\mathbb{Z}^n$?

Proof of Theorem 1.2. Since $\mathbb{Z}^n$ is primitive, we have (a) ⇔ (c). If a lattice (L, b) is isometric to $\mathbb{Z}^1$, then $(L, 2b)$ is isometric to $\mathbb{A}^1$. This yields implications (a) ⇔ (b) and (c) ⇔ (d).

(a) ⇒ (e) Suppose that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to $\mathbb{Z}^n$. Then, by Corollary 2.2, either K is a totally real field and $\theta = \mathrm{id}$, or K is a CM-field and θ is the complex conjugation. Since $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ and $\mathbb{Z}^n$ are isometric, and the $\mathbb{Z}$-module $\mathbb{Z}^n$ is generated by $\mathbb{Z}^n[1]$, we deduce from Lemma 2.5(b) that

$$m = n, \tag{4.1}$$

and (4.1) implies by Lemma 2.5(ii) that

$$\mathscr{O} \ \text{ is the } \mathbb{Z}\text{-linear span of } \mu_K. \tag{4.2}$$

Suppose that the order of the cyclic group μ_K is divisible by an odd prime p. Then there is $x \in \mu_K$ which is a pth primitive root of unity. The minimal polynomial of x over $\mathbb{Q}$ is $t^{p-1} + t^{p-2} + \cdots + 1$, hence

$$\mathrm{Trace}_{\mathbb{Q}(x)/\mathbb{Q}}(x) = -1 \quad \text{and} \quad [\mathbb{Q}(x) : \mathbb{Q}] = p - 1 \geq 2. \tag{4.3}$$

Since $\mathrm{Trace}_{K/\mathbb{Q}}(x) = [K : \mathbb{Q}(x)]\mathrm{Trace}_{\mathbb{Q}(x)/\mathbb{Q}}(x)$, we obtain from (4.3) that

$$0 < \mathrm{Trace}_{K/\mathbb{Q}}(-x) = \frac{n}{p-1} < n. \tag{4.4}$$

However, in view of (1.5) and (4.1), the integer $\mathrm{Trace}_{K/\mathbb{Q}}(-x)$ is divisible by n. This contradicts (4.4). The obtained contradiction proves that there a positive integer a such that μ_K is a cyclic group of order 2^a. In view of (4.2), this implies that K is a 2^ath cyclotomic field. In particular, it is a CM-field, and therefore, θ is the complex conjugation. This proves implication (a) $\Rightarrow$ (e).

(e) $\Rightarrow$ (c) Let K be a 2^ath cyclotomic field for a positive integer a and let θ be the complex conjugation. By Lemma 2.6 (whose notation we use), $n = 2^{a-1}$, $m = n$, and $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ is the orthogonal direct sum of the sublattices $\mathbb{Z}\zeta^j$, $0 \leq j \leq 2^{a-1} - 1$, each of which is isometric to $\mathbb{Z}^1$. This proves implication (e) $\Rightarrow$ (c).

The last statement of Theorem 1.2 follows from Lemma 2.6(iii). □

5. When is $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ Similar to an Even Primitive Root Lattice?

Proof of Theorem 1.3. The implications (a) $\Leftrightarrow$ (b) and (c) $\Rightarrow$ (b) are clear.

(a) $\Rightarrow$ (d) Suppose that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to an even primitive root lattice (L, b). Then, by Corollary 2.2, either K is a totally real field and $\theta = \mathrm{id}$, or K is a CM-field and θ is the complex conjugation. Since $(\mathscr{O}, \mathrm{tr}_{K,\theta}/m)$ and (L, b) are isometric, and (L, b) is an even lattice generated by $(L, b)[2]$, we deduce from Lemma 2.5(c) that

$$m = n/2, \tag{5.1}$$

and (5.1) implies by Lemma 2.5(ii) that $\mathscr{O}$ is the $\mathbb{Z}$-linear span of μ_K. Hence K is a cyclotomic field and θ is the complex conjugation.

There is an odd prime p dividing the order of μ_K: otherwise, this order is 2^a for some a, hence $m = n$ by Theorem 1.2, which contradicts (5.1). Thus, we can find an element $x \in \mu_K$ which is a pth primitive root of unity. The same argument as in the above proof of implication (a) $\Rightarrow$ (e) of Theorem 1.2 shows that (4.4) holds. In view of (1.5) and (5.1), the integer $\mathrm{Trace}_{K/\mathbb{Q}}(-x)$ is divisible by $n/2$. This and (4.4) then yield $p-1=2$, i.e. $p=3$. Thereby we proved that K is a 2^a3^bth cyclotomic field for some $a \geq 0$, $b>0$. Since every 3^bth cyclotomic field is simultaneously a 2^13^bth cyclotomic field, we may assume that $a>0$. This completes the proof of implication (a) $\Rightarrow$ (d).

(d) $\Rightarrow$ (c) Let K be a 2^a3^bth cyclotomic field for some $a>0$, $b>0$. We use the notation introduced in the paragraph immediately preceding Lemma 2.8 and put

$$i := 2^a, \quad j := 3^b, \quad n_i := [K_i : \mathbb{Q}], \quad n_j := [K_j : \mathbb{Q}]. \tag{5.2}$$

By Lemma 2.8(i) we have $n = n_i n_j$. Hence by Lemma 2.8(iii) there is a lattice isometry

$$(\mathscr{O}_i, \mathrm{tr}_{K_i,\theta}/n_i) \otimes_{\mathbb{Z}} (\mathscr{O}_j, \mathrm{tr}_{K_j,\theta}/(n_j/2)) \to (\mathscr{O}, \mathrm{tr}_{K,\theta}/(n/2)). \tag{5.3}$$

In view of (5.2) and Lemmas 2.6, 2.7, the lattices $(\mathscr{O}_i, \mathrm{tr}_{K_i,\theta}/n_i)$ and $\big(\mathscr{O}_j, \mathrm{tr}_{K_j,\theta}/(n_j/2)\big)$ are isometric to respectively $\mathbb{Z}^{n_i}$ and $\mathbb{A}_2^{n_j/2}$. Since the lattices $\mathbb{Z}^1 \otimes_{\mathbb{Z}} \mathbb{A}_2$ and $\mathbb{A}_2$ are isometric, the existence of isomorphism (5.3) then implies that the lattice $(\mathscr{O}, \mathrm{tr}_{K,\theta}/(n/2))$ is isometric to $\mathbb{A}_2^{n/2}$. This completes the proof of implication (d) $\Rightarrow$ (c).

The last two statements of Theorem 1.3 follow from Lemma 2.6(iii), (iv), Lemma 2.7(iii), (iv), and Lemma 2.8(ii). □

6. When is $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ Similar to a Positive-Definite Even Unimodular Lattice of Rank ≤ 48?

Proof of Theorem 1.4. Arguing on the contrary, assume that $(\mathscr{O}, \mathrm{tr}_{K,\theta})$ is similar to a positive-definite even unimodular lattice (L, b) of rank n, where

$$8 \leq n \leq 48 \tag{6.1}$$

(the first inequality follows from the fact that 8 divides n, see, e.g. [10, Chap. 7, §6, Corollary 18]). Since (L,b) is unimodular, we have

$$|\mathrm{disc}\,(L,b)| = 1, \tag{6.2}$$

and (6.2) implies, by Lemma 2.2(ii), that (L,b) is primitive. Therefore, (L,b) is isometric to $(\mathscr{O}, \mathrm{tr}_{K,\theta})$. By Lemma 2.3, since (L,b) is positive-definite, the properties listed in item (iii) of this lemma hold. In view of Lemma 2.2(ii), (iv) and (6.2), we have

$$\sqrt[n]{|\mathrm{disc}\, K/\mathbb{Q}|} = m. \tag{6.3}$$

By Lemma 2.2(v), since (L,b) is even, $n/2 \equiv 0 \bmod m$. This and (6.3) yield

$$\sqrt[n]{|\mathrm{disc}\, K/\mathbb{Q}|} \leq n/2. \tag{6.4}$$

On the other hand, by Lemma 2.9(ii), Lemma 2.10, and (6.1), for $n \leq 48$, we have the inequality

$$\sqrt[n]{|\mathrm{disc}\, K/\mathbb{Q}|} > \begin{cases} (n+1)^2/2n > n/2 & \text{if } K \text{ is a totally real field,} \\ n/2 & \text{if } K \text{ is a CM-field,} \end{cases}$$

which contradicts (6.4). □

Appendix A. The $\mathbb{Z}^n$, $\mathbb{A}_n$, $\mathbb{D}_n$, and $\mathbb{E}_n$ Lattices

To be self-contained, here we briefly describe the lattices $\mathbb{Z}^n$, $\mathbb{A}_n$, $\mathbb{D}_n$, and $\mathbb{E}_n$ as they play a key role in this paper. For details and a discussion of their properties see [7, 10, 18].

Let $\mathbb{R}^m$ be the m-dimensional coordinate real vector space of rows endowed with the standard Euclidean structure

$$\mathbb{R}^m \times \mathbb{R}^m \to \mathbb{R}, \quad ((x_1, \dots, x_m), (y_1, \dots, y_m)) := \sum_{j=1}^{m} x_j y_j. \tag{A.1}$$

Denote by e_j the row $(0, \dots, 0, 1, 0, \dots, 0)$, where the number of 0's to the left of 1 is $j-1$.

If L is the $\mathbb{Z}$-linear span of a set of linearly independent elements of $\mathbb{R}^m$ such that $b(L \times L) \subseteq \mathbb{Z}$, where b is the restriction of map (A.1) to $L \times L$, then (L, b) is called a *lattice in* $\mathbb{R}^m$ and denoted just by L.

With these notation and conventions, we have:

$\mathbb{Z}^n$ is the lattice $\{(x_1, \dots, x_n) \mid x_j \in \mathbb{Z} \text{ for all } j\}$ in $\mathbb{R}^n$.
$\mathbb{A}_n$ is the lattice $\{(x_1, \dots, x_{n+1}) \in \mathbb{Z}^{n+1} \mid \sum_{j=1}^{n+1} x_j = 0\}$ in $\mathbb{R}^{n+1}$.
$\mathbb{D}_n$ is the lattice $\{(x_1, \dots, x_n) \in \mathbb{Z}^n \mid \sum_{j=1}^{n} x_j \equiv 0 \bmod 2\}$ in $\mathbb{R}^n$, $n \geq 4$.
$\mathbb{E}_8$ is the lattice $\mathbb{D}_8 \cup \left(\mathbb{D}_8 + \frac{1}{2}(e_1 + \cdots + e_8)\right)$ in $\mathbb{R}^8$.
$\mathbb{E}_7$ is the orthogonal in $\mathbb{E}_8$ of the sublattice $\mathbb{Z}(e_7 + e_8)$.
$\mathbb{E}_6$ is the orthogonal in $\mathbb{E}_8$ of the sublattice $\mathbb{Z}(e_7 + e_8) + \mathbb{Z}(e_6 + e_8)$.

Each of these lattices except $\mathbb{A}_1$ is primitive. Each of them except $\mathbb{Z}^n$ for every n is even.

Appendix B. Cyclicity Criterion

Theorem B.1 (Cyclicity Criterion). *Let $n > 1$ and let p be a prime ramified in K. Then the following properties of $\mathscr{O}$ are equivalent*:

(i) *The p-primary component of the additive group of ring $\mathscr{O}/\mathfrak{d}$ is a cyclic group* (*automatically nontrivial*).
(ii) *The following conditions hold*:
 (ii$_1$) *in $\mathscr{O}$, there is exactly one ramified prime ideal $\mathfrak{p}$ which lies over p*;
 (ii$_2$) *p is odd*, $\operatorname{ord}_{\mathfrak{p}} p\mathscr{O} = 2$, *and $\mathscr{O}/\mathfrak{p}$ is the field of p elements.*

Proof. Let $\mathfrak{r}_1, \dots, \mathfrak{r}_m$ be all pairwise distinct prime ideals of $\mathscr{O}$ ramified in $K/\mathbb{Q}$. For every $\mathfrak{r}_i$, there is a prime integer r_i and a positive integer f_i such that

$$\mathfrak{r}_i \cap \mathbb{Z} = r_i\mathbb{Z} \quad \text{and} \quad |\mathscr{O}/\mathfrak{r}_i^s| = r_i^{f_i s} \quad \text{for every positive integer } s \tag{B.1}$$

(see, e.g. [13, Chap. 12, §2, 3]). We put

$$e_i := \operatorname{ord}_{\mathfrak{r}_i} r_i \mathscr{O}. \tag{B.2}$$

As $\mathfrak{r}_i$ is ramified, $e_i \geq 2$. There are positive integers $d_1, \ldots, d_m$ such that

$$\mathfrak{d} = \mathfrak{r}_1^{d_1} \cdots \mathfrak{r}_m^{d_m} \tag{B.3}$$

(see, e.g. [20, Chap. III, Theorem 2.6]). By Dedekind's theorem (see, e.g. [20, Theorem 2.6, p. 199]), we have

$$d_i \geq e_i - 1, \quad \text{where the equality holds if and only if } r_i \nmid e_i. \tag{B.4}$$

By the Chinese remainder theorem (see, e.g. [13, Proposition 12.3.1]), decomposition (B.3) yields the following ring isomorphism:

$$\mathscr{O}/\mathfrak{d} \approx \mathscr{O}/\mathfrak{r}_1^{d_1} \oplus \cdots \oplus \mathscr{O}/\mathfrak{r}_m^{d_m}. \tag{B.5}$$

As every r_i is prime, (B.5), (B.1) imply that (i) is satisfied if and only if the following two conditions (a) and (b) hold:

(a) there is exactly one i such that $r_i = p$,
(b) the additive group of $\mathscr{O}/\mathfrak{r}_i^{d_i}$ is cyclic.

Clearly (a) is equivalent to (ii$_1$). We shall now show that (b) is equivalent to (ii$_2$) with $\mathfrak{p} = \mathfrak{r}_i$ and $p = r_i$; this will complete the proof.

Assume that (b) holds. By (B.2), we have $\mathfrak{r}_i^{e_i-1} \supseteq \mathfrak{r}_i^{e_i} \supseteq r_i\mathscr{O}$. Hence there are the ring epimorphisms

$$\mathscr{O}/r_i\mathscr{O} \twoheadrightarrow \mathscr{O}/\mathfrak{r}_i^{e_i} \twoheadrightarrow \mathscr{O}/\mathfrak{r}_i^{e_i-1}. \tag{B.6}$$

Since r_i is prime, it is the order of every nonzero element of the additive group of $\mathscr{O}/r_i\mathscr{O}$. The existence of epimorphisms (B.6) then implies that

$$\begin{aligned} r_i \quad &\text{is the order of every nonzero element of} \\ &\text{the additive groups of } \mathscr{O}/\mathfrak{r}_i^{e_i} \text{ and } \mathscr{O}/\mathfrak{r}_i^{e_i-1}. \end{aligned} \tag{B.7}$$

We consider two possibilities stemming from (B.4):

(T) $d_i = e_i - 1$ (tamely ramified $\mathfrak{r}_i$);
(W) $d_i \geq e_i$ (wildly ramified $\mathfrak{r}_i$).

First, assume that (T) holds. Then from (b), (B.7), and (B.1) we infer that $f_i = d_i = 1$, $|\mathscr{O}/\mathfrak{r}_i| = r_i$. Hence $e_i = 2$, and, by (B.4), r_i is odd. Thus, as claimed, in this case, (ii$_2$) is fulfilled.

Next, assume that (W) holds. Then $\mathfrak{r}_i^{e_i} \supseteq \mathfrak{r}_i^{d_i}$; whence there is a ring epimorphism

$$\mathscr{O}/\mathfrak{r}_i^{d_i} \twoheadrightarrow \mathscr{O}/\mathfrak{r}_i^{e_i}. \tag{B.8}$$

From (b), (B.7), (B.8), and (B.1) we then infer that $r_i = |\mathscr{O}/\mathfrak{r}_i^{e_i}| = r_i^{f_ie_i}$ contrary to the inequality $e_i \geq 2$. Thus, (W) is impossible.

This completes the proof of (b) $\Rightarrow$ (ii$_2$) with $\mathfrak{p} = \mathfrak{r}_i$ and $p = r_i$. The converse implication is immediate. □

Acknowledgments

We thank E. Bayer-Fluckiger for her interest in this work and help with references, and the referee, whose wish for the authors that they compare the two lattice constructions resulted in proving Proposition 2.1.

The work of V. L. Popov was performed at the Steklov International Mathematical Center and supported by the Ministry of Science and Higher Education of the Russian Federation (agreement no. 075-15-2019-1614).

The work of Y. G. Zarhin was partially supported by Simons Foundation Collaboration Grant #585711. Part of this work was done during his stay at the Weizmann Institute of Science (December 2019–January 2020), whose hospitality and support are gratefully acknowledged.

References

[1] E. Bayer-Fluckiger, Definite hermitian forms and the cancellation of simple knots, *Arch. Math.* **40** (1983) 182–185.

[2] E. Bayer-Fluckiger, Lattices and number fields, *Contemp. Math.* **241** (1999) 69–84.

[3] E. Bayer-Fluckiger, Ideal lattices, in *A Panorama of Number Theory or The View from Baker's Garden* (Cambridge University Press, Cambridge, 2002), pp. 168–184.

[4] E. Bayer-Fluckiger, Upper bounds for Euclidean minima of algebraic number fields, *J. Number Theory* **121** (2006) 305–323.

[5] E. Bayer-Fluckiger and J. Martinet, Réseaux liés à des algèbres semi-simples, *J. Reine Angew. Math.* **415** (1994) 51–69.

[6] Z. I. Borevich and I. R. Shafarevich, *Number Theory* (Academic Press, Orlando, 1966).

[7] N. Bourbaki, *Groupes et Algébres de Lie*, Chaps. IV–VI (Hermann, Paris, 1968).

[8] N. Bourbaki, *Algebra II*, Chaps. 4–7 (Springer-Verlag, Berlin, 1990).

[9] P. Conner and R. Perlis, *A Survey of Trace Forms of Algebraic Number Fields*, Series in Pure Mathematics, Vol. 2 (World Scientific, Singapore, 1984).

[10] J. H. Conway and N. J. A. Sloane, *Sphere Packing*, *Lattices and Groups*, Grundlehren der Mathematischen Wissenschaften, Bd. 290 (Springer-Verlag, New York, 1988).

[11] C. Curtis and I. Reiner, *Representation Theory of Finite Groups and Associative Algebras*, 2nd edn. (Interscience, New York, 1966).

[12] F. Diaz y Diaz, *Tables minorant la racine n-ieéme du discriminant d'un corps de degré n*, Publications Mathematiques d'Orsay, Vol. 80.06 (Université de Paris-Sud, Département de Mathématique, Paris, 1980); Available at http://sites.mathdoc.fr/PMO/feuilleter.php?id=PMO_1980.

[13] K. Ireland and M. Rosen, *A Classical Introduction to Modern Number Theory*, Graduate Texts in Mathematics, Vol. 87 (Springer-Verlag, New York, 1982).

[14] H. Koch, *Algebraic Number Theory*, Encyclopedia of Mathematical Sciences, Vol. 62 (Springer-Verlag, Berlin, 1997).

[15] L. Kronecker, Zwei Sätze über Gleichungen mit ganzzahligen Coefficienten, *J. Reine Angew. Math.* **53** (1857) 173–175.

[16] S. Lang, *Algebraic Numbers* (Addison-Wesley, Reading, MA, 1964).

[17] S. Lang, *Algebra* (Addison-Wesley, Reading, MA, 1965).

[18] J. Martinet, *Perfect Lattices in Euclidean Spaces*, Grundlehren der mathematischen Wissenschaften, Bd. 327 (Springer-Verlag, Berlin, 2003).

[19] J. Milnor and D. Husemoller, *Symmetric Bilinear Forms*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Bd. 73 (Springer-Verlag, Berlin, 1973).
[20] J. Neukirch, *Algebraic Number Theory* (Springer, Berlin, 1999).
[21] V. L. Popov, Root systems and root lattices in number fields, in *Abstracts*, *XVII International Conference on Algebra*, *Number Theory*, *and Discrete Geometry*: *Modern Problems*, *Applications and Problems of History*, Leo Tolstoy TSPU, Tula, September 23–28 (2019), pp. 286–289 (in Russian), ISBN 978-5-6042450-5-7, available at https://www.researchgate.net/profile/Vladimir_Popov12.
[22] V. L. Popov and Y. G. Zarhin, Root systems in number fields, *Indiana Univ. Math. J.*, preprint (2019), arXiv:1808.01136v3.
[23] J. M. Steele, *An Introduction to the Art of Mathematical Inequalities. The Cauchy–Schwarz Master Class*, MAA Problem Books Series (Cambridge University Press, Cambridge, 2004).
[24] M. Tsfaman, S. Vlăduţ and D. Nogin, *Algebraic Geometry Codes*: *Advanced Chapters*, Mathematical Surveys and Monographs, Vol. 238 (American Mathematical Society, Providence, RI, 2019).
[25] L. C. Washington, *Introduction to Cyclotomic Fields* (Springer-Verlag, New York, 1982).
[26] E. Witt, Spiegelungsgruppen und Aufzählung halbeinfacher Liescher Ringe, *Abh. Math. Sem. Univ. Hamb.* **14**(1) (1941) 289–322; Repr. in E. Witt, *Collected Papers–Gesammelte Abhandlungen* (Springer Verlag, Berlin, 1998), pp. 213–246.
[27] O. Zariski and P. Samuel, *Commutative Algebra*, Vol. 1 (Van Nostrand, Princeton, NJ, 1958).