ON WELL-ROUNDED IDEAL LATTICES

LENNY FUKSHANSKY AND KATHLEEN PETERSEN

Abstract. We investigate a connection between two important classes of Euclidean lattices: well-rounded and ideal lattices. A lattice of full rank in a Euclidean space is called well-rounded if its set of minimal vectors spans the whole space. We consider lattices coming from full rings of integers in number fields, proving that only cyclotomic fields give rise to well-rounded lattices. We further study the well-rounded lattices coming from ideals in quadratic rings of integers, showing that there exist infinitely many real and imaginary quadratic number fields containing ideals which give rise to well-rounded lattices in the plane.

1. Introduction

In this note we investigate a connection between two fundamental classes of Euclidean lattices, *well-rounded* and *ideal* lattices, which come up in a variety of mathematical contexts as well as in applications in discrete optimization and coding theory.

Let Λ be a lattice of full rank in the d-dimensional Euclidean space $\mathbb{R}^d$ for $d \geq 2$. The *minimum* of Λ is defined as

$$|\Lambda| := \min\{\|\boldsymbol{x}\|^2 : \boldsymbol{x} \in \Lambda \setminus \{\mathbf{0}\}\},$$

where $\| \ \|$ stands for the usual Euclidean norm on $\mathbb{R}^d$, and the set of *minimal vectors* of Λ is defined to be

$$S(\Lambda) := \{\boldsymbol{x} \in \Lambda : \|\boldsymbol{x}\|^2 = |\Lambda|\}.$$

The lattice Λ is called *well-rounded* (abbreviated WR) if the set $S(\Lambda)$ spans $\mathbb{R}^d$. WR lattices are important in discrete optimization, in particular in the investigation of sphere packing, sphere covering, and kissing number problems (see [14]), as well as in coding theory (see [1]). Properties of WR lattices have also been investigated in [15] in connection with Minkowski's conjecture.

Another class of lattices that comes up frequently in connection with optimization problems and in coding theory (see [16], [6]) are the ideal lattices. Let K be a number field of degree d over $\mathbb{Q}$, and let us write $\mathcal{O}_K$ for its ring of integers. Let

$$\sigma_1, ..., \sigma_{r_1}, \tau_1, ..., \tau_{r_2}, ..., \tau_{2r_2}$$

be the embeddings of K into $\mathbb{C}$ with $\sigma_1, ..., \sigma_{r_1}$ being the real embeddings and $\tau_n, \tau_{r_2+n} = \bar{\tau}_n$ for each $1 \leq n \leq r_2$ being the pairs of complex conjugate embeddings. For each $\alpha \in K$ and each complex embedding τ_n, write $\tau_{n1}(\alpha) = \Re(\tau_n(\alpha))$ and

2010 *Mathematics Subject Classification.* Primary: 11H06, 11R04, 11R11; Secondary: 11E16.
Key words and phrases. well-rounded lattices, ideal lattices, quadratic number fields, binary quadratic forms.

$\tau_{n2}(\alpha) = \Im(\tau_n(\alpha))$, where $\Re$ and $\Im$ stand respectively for real and imaginary parts of a complex number. Then $d = r_1 + 2r_2$, and we define an embedding

$$\sigma = (\sigma_1, \dots, \sigma_{r_1}, \tau_{11}, \tau_{12}, \dots, \tau_{r_2 1}, \tau_{r_2 2}) : K \to \mathbb{R}^d.$$

Then $\Lambda_K := \sigma(\mathcal{O}_K)$ is a lattice of full rank in $\mathbb{R}^d$. Following the notation of [5] (bottom of p. 438), we call such lattices *principal ideal lattices*. More generally, for any nonzero fractional ideal I of $\mathcal{O}_K$, $\Lambda_K(I) := \sigma(I)$ is a full rank lattice in $\mathbb{R}^d$, and if I is an ideal in $\mathcal{O}_K$ then $\Lambda_K(I)$ is a sublattice of Λ_K of finite index; throughout this paper, when we refer to ideals or fractional ideals, we always mean only the nonzero ones. A lattice Λ in $\mathbb{R}^d$ is called an *ideal lattice* if it can be realized as $\Lambda_K(I)$ for some fractional ideal I of the ring of integers of some number field K with $[K : \mathbb{Q}] = d$. For more information on ideal lattices see [2], [3], [5]. It should be remarked that the definition of ideal lattices (and principal ideal lattices in particular) in these papers is more general, our definition being a more concrete special case of that.

The importance and applicability of these two special classes of lattices motivates the following natural question: when are ideal lattices well-rounded? In this note we investigate this question for principal ideal lattices Λ_K and some of their ideal sublattices. This question is partially motivated by the first author's previous investigations [10], [11], [12], where the WR sublattices of $\mathbb{Z}^2 = \Lambda_{\mathbb{Q}(i)}$ and the hexagonal lattice $\Lambda_h := \Lambda_{\mathbb{Q}(\sqrt{-3})}$ were studied. Both of these lattices are WR themselves; in fact, these are the only two principal ideal WR lattices in $\mathbb{R}^2$, as we demonstrate in Section 2 by a direct verification argument (see Lemma 2.2). Moreover, all ideal sublattices of $\mathbb{Z}^2$ and Λ_h are also WR: this is a direct consequence of the well-known fact the ideal sublattices of $\mathbb{Z}^2$ and Λ_h are similar to $\mathbb{Z}^2$ and Λ_h, respectively. Let us recall here that two lattices Λ and Ω are said to be *similar* if there exists an $N \times N$ real orthogonal matrix A and a nonzero constant α such that $\Omega = \alpha A\Lambda$. Similarity is easily seen to be an equivalence relation, which preserves the WR property; we will denote it by writing $\Lambda \sim \Omega$. In Section 2 we further investigate the ideal lattices coming from quadratic number fields, proving in particular the following result.

Theorem 1.1. *There exist infinitely many real and imaginary quadratic number fields K whose rings of integers contain an ideal I such that the planar lattice $\Lambda_K(I)$ is WR.*

We give examples of ideals as in Theorem 1.1 in Tables 1 and 2 in Section 2.

Remark 1.1. We should remark that there also exist quadratic number fields K so that $\Lambda_K(I)$ is not WR for any ideal $I \subseteq \mathcal{O}_K$, for instance all class number one imaginary quadratic fields different from $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$, as we demonstrate in Corollary 2.4.

The distinguishing feature of $\mathbb{Q}(i)$ and $\mathbb{Q}(\sqrt{-3})$ $(= \mathbb{Q}(e^{\frac{2\pi i}{3}}))$ among imaginary quadratic number fields is that these are the only ones that are cyclotomic fields. In Section 3 we show that for number fields of any degree principal ideal lattices are WR only in the cyclotomic case. Recall that the *norm* of a nonzero ideal $I \subseteq \mathcal{O}_K$ in the number field K is defined as $\mathrm{N}(I) := |\mathcal{O}_K/I|$. We prove the following result.

Theorem 1.2. *Let K be a number field of degree $d \geq 2$ and $I \subseteq \mathcal{O}_K$ a nonzero ideal. Then $|\Lambda_K(I)| \geq (r_1 + r_2)\,\mathrm{N}(I)^{\frac{1}{r_1+r_2}}$. Moreover, $|\Lambda_K| = r_1 + r_2$,*

$$S(\Lambda_K) = \{\sigma(x) : x \in \mathcal{O}_K \text{ is a root of unity}\},$$

and Λ_K is WR if and only if K is a cyclotomic field, i.e., $K = \mathbb{Q}(\zeta_k)$ for some primitive k-th root of unity ζ_k, $k \geq 2$. If this is the case, then

$$|\Lambda_K| = r_2 = \frac{d}{2} = \frac{\varphi(k)}{2}.$$

Remark 1.2. The value of $|\Lambda_K|$ and a bound on $|\Lambda_K(I)|$ under a slightly different embedding into $\mathbb{R}^d$ also follow from Lemma 4.3 of [4], which is proved by a rather different argument from ours, however the results of [4] do not imply the result of Theorem 1.2 on WR ideal lattices.

As a corollary of Theorem 1.2, we also deduce that, as in the two dimensional case, all ideal lattices coming from cyclotomic fields are WR.

Corollary 1.3. *Let $K = \mathbb{Q}(\zeta_k)$ for some primitive k-th root of unity ζ_k, $k \geq 2$, and let I be a fractional ideal of $\mathcal{O}_K$. Then the lattice $\Lambda_K(I)$ is WR.*

The proof of Corollary 1.3 is also presented in Section 3.

2. Quadratic ideal lattices

In this section we study quadratic WR ideal lattices. Let us start by recording a general basic property of WR lattices in $\mathbb{R}^2$ which will be useful to us.

Lemma 2.1. *A full-rank lattice $\Lambda \subset \mathbb{R}^2$ contains 2, 4, or 6 minimal vectors, and it is WR if and only if $|S(\Lambda)| = 4, 6$. Moreover, $|S(\Lambda)| = 6$ if and only if Λ is similar to Λ_h, the hexagonal lattice. On the other hand, there are infinitely many distinct similarity classes of WR lattices in $\mathbb{R}^2$ with four minimal vectors.*

Proof. Notice that minimal vectors in a lattice always come in $\pm$ pairs, hence $S(\Lambda)$ contains at least two vectors, and it contains two linearly independent vectors if and only if its cardinality is greater than two. On the other hand, the angle θ between any pair of minimal vectors $\boldsymbol{x}, \boldsymbol{y}$ has to be at least $\pi/3$, since otherwise

$$\|\boldsymbol{x} - \boldsymbol{y}\|^2 = \|\boldsymbol{x}\|^2 + \|\boldsymbol{y}\|^2 - 2\|\boldsymbol{x}\|\|\boldsymbol{y}\|\cos\theta < \|\boldsymbol{x}\|^2 = \|\boldsymbol{y}\|^2.$$

Since all the minimal vectors must lie on the circle of the same radius,

$$|S(\Lambda)| \leq \frac{2\pi}{\pi/3} = 6,$$

and so Λ is WR if and only if $|S(\Lambda)| = 4, 6$.

Now suppose that $|S(\Lambda)| = 6$, then

$$S(\Lambda) = \{\pm\boldsymbol{x}_1, \pm\boldsymbol{x}_2, \pm\boldsymbol{x}_3\},$$

and we can choose a pair $\pm\boldsymbol{x}_i, \pm\boldsymbol{x}_j$, $1 \leq i < j \leq 3$, such that the angle between these two vectors is $\pi/3$. Then Λ is spanned over $\mathbb{Z}$ by these two vectors, and hence can be obtained from Λ_h by rotation and dilation, i.e. is similar to Λ_h. On the other hand, if Λ is similar to Λ_h, then

$$|S(\Lambda)| = |S(\Lambda_h)| = 6.$$

On the other hand, there are infinitely many distinct similarity classes of WR lattices in $\mathbb{R}^2$ (see [11]), and so, by our argument above, lattices in all but one of them cannot contain six minimal vectors; hence they must have four. This completes the proof. □

Remark 2.1. The statement of Lemma 2.1 is generally well-known with parts of it following from the work of Gauss (see Section 3 of [10] for some details). We present the proof here for completeness purposes.

We first consider principal ideal lattices in $\mathbb{R}^2$. Let $K = \mathbb{Q}(\sqrt{D})$ for some squarefree $D \in \mathbb{Z}$, $D \neq 1$, then

$$\mathcal{O}_K = \begin{cases} \mathbb{Z}[\sqrt{D}] & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4) \\ \mathbb{Z}[\frac{1+\sqrt{D}}{2}] & \text{if } D \equiv 1 (\mathrm{mod}\, 4), \end{cases} \tag{1}$$

and the two embeddings of K are given by

$$\sqrt{D} \mapsto \sqrt{D}, \ \sqrt{D} \mapsto -\sqrt{D}.$$

Let us use the notation Λ_D for Λ_K and $\Lambda_D(I)$ for any ideal $I \subset \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, so for instance $\mathbb{Z}^2 = \Lambda_{-1}$ and $\Lambda_h = \Lambda_{-3}$. Our first lemma stipulates that these are the only cases when Λ_D is well-rounded. While it is a special case of Lemma 3.4 below, we prove it here by a direct elementary argument.

Lemma 2.2. *The lattice Λ_D is WR if and only if $D = -1, -3$.*

Proof. First assume that $D \not\equiv 1 (\mathrm{mod}\, 4)$ is positive, then

$$\Lambda_D = \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} \mathbb{Z}^2.$$

Now for any nonzero

$$\boldsymbol{x} = \begin{pmatrix} 1 & \sqrt{D} \\ 1 & -\sqrt{D} \end{pmatrix} \begin{pmatrix} m \\ n \end{pmatrix} = \begin{pmatrix} m + n\sqrt{D} \\ m - n\sqrt{D} \end{pmatrix} \in \Lambda_D$$

we have

$$\|\boldsymbol{x}\|^2 = (m + n\sqrt{D})^2 + (m - n\sqrt{D})^2 = 2(m^2 + Dn^2) \geq 2,$$

with equality in this inequality if and only if $m = \pm 1, n = 0$, which means that $|\Lambda_D| = 2$ and

$$S(\Lambda_D) = \left\{ \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$

and so Λ_D cannot be WR.

Next assume that $D \not\equiv 1 (\mathrm{mod}\, 4)$ is negative, then

$$\Lambda_D = \begin{pmatrix} 1 & 0 \\ 0 & \sqrt{|D|} \end{pmatrix} \mathbb{Z}^2.$$

Hence $|\Lambda_D| = 1$, and for any nonzero

$$\boldsymbol{x} = \begin{pmatrix} m \\ n\sqrt{|D|} \end{pmatrix} \in \Lambda_D$$

we have $\|\boldsymbol{x}\|^2 = m^2 + |D|n^2 \geq 1$, with equality in this inequality if and only if $m = \pm 1, n = 0$, unless $D = -1$, in which case there are additional solutions $m = 0, n = \pm 1$. Hence Λ_D is not WR unless $D = -1$, and in this later case

$$S(\Lambda_{-1}) = \left\{ \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\}.$$

Therefore for negative $D \not\equiv 1 (\mathrm{mod}\, 4)$, Λ_D is WR if and only if $D = -1$.

Next assume that $D \equiv 1 (\mathrm{mod}\, 4)$ is positive, then $D \geq 5$ and

$$\Lambda_D = \begin{pmatrix} 1 & \frac{1+\sqrt{D}}{2} \\ 1 & \frac{1-\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2,$$

and so for any nonzero

$$\boldsymbol{x} = \begin{pmatrix} \frac{2m+n}{2} + \frac{n\sqrt{D}}{2} \\ \frac{2m+n}{2} - \frac{n\sqrt{D}}{2} \end{pmatrix} \in \Lambda_D$$

we have

$$\|\boldsymbol{x}\|^2 = \frac{1}{2}\left(4m^2 + (D+1)n^2 + 4mn\right) \geq 2m^2 + 3n^2 + 2mn \geq 2,$$

with equality in this inequality if and only if $m = \pm 1, n = 0$, which means that $|\Lambda_D| = 2$ and

$$S(\Lambda_D) = \left\{ \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$

and so Λ_D cannot be WR.

Finally suppose that $D \equiv 1 (\mathrm{mod}\, 4)$ is negative, then $D \leq -3$ and

$$\Lambda_D = \begin{pmatrix} 1 & \frac{1}{2} \\ 0 & \frac{\sqrt{|D|}}{2} \end{pmatrix} \mathbb{Z}^2.$$

Hence $|\Lambda_D| = 1$, and for any nonzero

$$\boldsymbol{x} = \begin{pmatrix} \frac{2m+n}{2} \\ \frac{n\sqrt{|D|}}{2} \end{pmatrix} \in \Lambda_D$$

we have

$$\|\boldsymbol{x}\|^2 = m^2 + mn + \frac{(|D|+1)n^2}{4} \geq 1$$

with equality if and only if $m = \pm 1, n = 0$, unless $D = -3$, in which case there are additional solutions $m = 0, n = \pm 1$, and $m = 1, n = -1$, as well as $m = -1, n = 1$. Hence Λ_D is not WR unless $D = -3$, and in this later case

$$S(\Lambda_{-3}) = \left\{ \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \pm \begin{pmatrix} \frac{1}{2} \\ \frac{\sqrt{3}}{2} \end{pmatrix}, \pm \begin{pmatrix} \frac{1}{2} \\ -\frac{\sqrt{3}}{2} \end{pmatrix} \right\}.$$

Therefore for negative $D \equiv 1 (\mathrm{mod}\, 4)$, Λ_D is WR if and only if $D = -3$. This completes the proof. □

Next we discuss more general WR ideal lattices coming from quadratic number fields. Notice that if K is a quadratic number field, then either it is an imaginary quadratic field (i.e. $K = \mathbb{Q}(\sqrt{D})$ with $D \leq -1$ a squarefree integer, so that $r_1 = 0, r_2 = 1$) or a real quadratic field (i.e. $K = \mathbb{Q}(\sqrt{D})$ with $D > 1$ a squarefree

integer, so that $r_1 = 2, r_2 = 0$). We first consider imaginary quadratic fields, and start by establishing a basic property of principal ideals.

Lemma 2.3. *Let K be an imaginary quadratic number field. If $I \subseteq \mathcal{O}_K$ is a principal ideal and $J = \alpha I$, $0 \neq \alpha \in K$, is a fractional ideal, then $\Lambda_K(J)$ is similar to Λ_K.*

Proof. Since I is a principal ideal, $I = \gamma \mathcal{O}_K$ for some $\gamma \in \mathcal{O}_K$, and so $J = \alpha' \mathcal{O}_K$, where $\alpha' = \alpha\gamma \in \mathbb{C}$. Writing $\alpha' = re^{i\theta}$ for $r, \theta \in \mathbb{R}$, the action of left multiplication by α' on an element $\beta = se^{i\phi}$ is $\alpha'\beta = rse^{i(\theta+\phi)}$ which is a dilation and a rotation. Since $\Lambda_K = \sigma(\mathcal{O}_K)$, this is the action of α' on the lattice, meaning that $\Lambda_K(J)$ is obtained from Λ_K by rotation and dilation. Hence the two lattices are similar. □

Corollary 2.4. *Let $K = \mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ and $I \subseteq K$ a fractional ideal, then $\Lambda_K(I)$ is WR. On the other hand, if K is an imaginary quadratic field $\neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ and I is a principal fractional ideal in K, then $\Lambda_K(I)$ is not WR.*

Proof. Both of the fields $\mathbb{Q}(i)$ or $\mathbb{Q}(\sqrt{-3})$ are principal ideal domains, and so the first statement follows by combining Lemma 2.2 with Lemma 2.3. On the other hand, Λ_K is not WR whenever $K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ by Lemma 2.2, and so the second statement follows by Lemma 2.3. □

We will next construct an infinite family of imaginary quadratic fields with ideals giving rise to WR ideal lattices. Our construction is based on a certain convenient choice of an integral basis for an ideal in any quadratic number field. Let D be a squarefree integer, and define

$$\delta = \begin{cases} -\sqrt{D} & \text{if } D \not\equiv 1 (\mathrm{mod}\, 4) \\ \frac{1-\sqrt{D}}{2} & \text{if } D \equiv 1 (\mathrm{mod}\, 4). \end{cases} \tag{2}$$

Let $K = \mathbb{Q}(\sqrt{D})$ and let I be an ideal in $\mathcal{O}_K$, where $\mathcal{O}_K$ is as in (1). It is a well-known fact (see for instance Theorem 6.9 on p. 94 of [7]) that there exist rational integers a, b, g with

$$0 \leq b < a, \ 0 < g \leq a, \ g \mid a, \ g \mid b, \tag{3}$$

so that

$$I = \{ax + (b + g\delta)y : x, y \in \mathbb{Z}\}. \tag{4}$$

In other words, $a, b + g\delta$ is an integral basis for I; moreover, an integral basis for I with these properties is unique. Further, if a triple $a, b, g \in \mathbb{Z}$ satisfying (3) in addition satisfies the condition

$$\mathrm{N}(b + g\delta) = kga, \text{ for some integer } k, \tag{5}$$

where N stands for the norm, then the corresponding ideal $I = \langle a, b + g\delta \rangle$ in $\mathcal{O}_K$ is of the form (4) (see Theorem 6.15 on p. 96 of [7]). The unique integral basis with these properties is called the canonical basis for the ideal. Our strategy in the arguments to follow is based on using the canonical basis for an ideal I in $\mathcal{O}_K$ to construct a basis for the lattice $\Lambda_K(I)$ whose corresponding norm form is Minkowski reduced. Given a basis matrix $A = (\boldsymbol{x} \ \boldsymbol{y})$ for a lattice in $\mathbb{R}^2$, the corresponding norm form is

$$Q(m, n) = c_1 m^2 + c_2 mn + c_3 n^2 := (m \ n) A^t A \begin{pmatrix} m \\ n \end{pmatrix}.$$

It is said to be reduced if $Q(m,n) \geq Q(0,1) \geq Q(1,0)$ for all $m,n \in \mathbb{Z}$ with $n \neq 0$, which is equivalent to saying that $|c_2| \leq c_1 \leq c_3$. If in addition Q is symmetric, meaning that $Q(1,0) = Q(0,1)$ (i.e., $c_1 = c_3$), the lattice must be WR.

We return to imaginary quadratic fields.

Lemma 2.5. *There exist infinitely many squarefree integers $D > 1$ with $-D \equiv 1 (\mathrm{mod}\, 4)$ for which the ring of integers $\mathcal{O}_K$ of the imaginary quadratic field $K = \mathbb{Q}(\sqrt{-D})$ contains an ideal I with the property that $\Lambda_K(I)$ is WR.*

Proof. Let t be an odd positive integer, and define

$$g = 1,\ b = \frac{t-1}{2},\ a = 2b+2 = t+1,$$
$$D = (t+2)(3t+2) = 3t^2+8t+4. \tag{6}$$

It is then easy to see that $D \equiv 3 (\mathrm{mod}\, 4)$, i.e. $-D \equiv 1 (\mathrm{mod}\, 4)$, and condition (3) is satisfied. Moreover, there exist infinitely many odd positive t for which D given by (6) is squarefree. Indeed, notice that the set $\{t+2 : t \in \mathbb{Z},\ 2 \nmid t\}$ contains the set $\mathbb{P}$ of all odd prime numbers. Then select t such that $p = t+2 \in \mathbb{P}$, so

$$D = p(3p-4),$$

and clearly $p \nmid 3p-4$. In this case, to ensure that D is squarefree we only need to select t in such a way that $3p-4$ is squarefree. The fact that there exist infinitely many prime numbers p such that $3p-4$ is squarefree follows from the theorem on p. 920 of [8]; for each such prime p, let $t = p-2$. For each such choice of t, let $K = \mathbb{Q}(\sqrt{-D})$ and

$$I = \langle 2b+2, b+\delta \rangle = \left\langle t+1, \frac{t}{2} - \frac{\sqrt{-D}}{2} \right\rangle \subseteq \mathcal{O}_K$$

be an ideal. Then

$$\begin{aligned} \mathrm{N}(b+\delta) &= \left(\frac{t-\sqrt{-D}}{2}\right)\left(\frac{t+\sqrt{-D}}{2}\right) = \frac{1}{4}(t^2+D) \\ &= \frac{1}{4}(4t^2+8t+4) = (t+1)^2 = a^2, \end{aligned}$$

and so the condition (5) is satisfied. Therefore $t+1, \frac{t}{2} - \frac{\sqrt{-D}}{2}$ is a canonical basis for I. Then $\Lambda_K(I) = A\mathbb{Z}^2$, where

$$A = \begin{pmatrix} t+1 & \frac{t}{2} \\ 0 & -\frac{\sqrt{D}}{2} \end{pmatrix}. \tag{7}$$

Then for any $\boldsymbol{x} = A\begin{pmatrix} m \\ n \end{pmatrix} \in \Lambda_K(I)$,

$$\begin{aligned} \|\boldsymbol{x}\|^2 &= Q(m,n) := (m\ n)A^tA\begin{pmatrix} m \\ n \end{pmatrix} \\ &= (t+1)^2m^2 + t(t+1)mn + \frac{1}{4}(t^2+D)n^2 = a^2m^2 + a(a-1)mn + a^2n^2, \end{aligned} \tag{8}$$

and hence the positive definite integral binary quadratic form $Q(m,n)$ is reduced and symmetric. By definition of Minkowski reduction, $Q(m,n) \geq Q(0,1) \geq Q(1,0)$ for all $m,n \in \mathbb{Z}$ with $n \neq 0$, and by symmetry $Q(0,1) = Q(1,0) = a^2$. This implies that $\Lambda_K(I)$ is WR, and thus we have constructed an infinite family of imaginary

quadratic number fields $\mathbb{Q}(\sqrt{-D})$ with $D > 1$, $-D \equiv 1 (\mathrm{mod}\, 4)$, each of which contains at least one ideal $I \subseteq \mathcal{O}_K$ so that $\Lambda_K(I)$ is WR. This completes the proof of the lemma. $\square$

We now turn to the case of real quadratic number fields, and establish a result analogous to Lemma 2.5.

Lemma 2.6. *There exist infinitely many squarefree integers $D > 1$ with $D \equiv 1 (\mathrm{mod}\, 4)$ for which the ring of integers $\mathcal{O}_K$ of the real quadratic field $K = \mathbb{Q}(\sqrt{D})$ contains an ideal I with the property that $\Lambda_K(I)$ is WR.*

Proof. Let t be an odd positive integer, and define

$$g = 1,\ b = \frac{t+1}{2},\ a = 2b+1 = t+2,$$
$$D = (t+2)(t-2) = t^2 - 4. \tag{9}$$

It is then easy to see that $D \equiv 1 (\mathrm{mod}\, 4)$ and condition (3) is satisfied. Moreover, we can show that there exist infinitely many odd positive t for which D given by (9) is squarefree, using the same type of argument as in the proof of Lemma 2.5. The set $\{t+2 : t \in \mathbb{Z},\ 2 \nmid t\}$ contains the set $\mathbb{P}$ of all odd prime numbers. Then select $t \geq 3$ such that $p = t+2 \in \mathbb{P}$, so

$$D = p(p-4),$$

and clearly $\gcd(p, p-4) = 1$. To ensure that D is squarefree we need to select t such that $p-4$ is squarefree. The fact that there exist infinitely many prime numbers p such that $p-4$ is squarefree again follows from the theorem on p. 920 of [8]; for each such prime p, let $t = p-2$. For each such choice of t, let $K = \mathbb{Q}(\sqrt{D})$ and

$$I = \langle 2b+1, b+\delta \rangle = \left\langle t+2, \frac{t+2}{2} - \frac{\sqrt{D}}{2} \right\rangle \subseteq \mathcal{O}_K$$

be an ideal. Then

$$\begin{aligned} \mathrm{N}(b+\delta) &= \left(\frac{(t+2)-\sqrt{D}}{2}\right)\left(\frac{(t+2)+\sqrt{D}}{2}\right) = \frac{1}{4}(t^2+4t+4-D) \\ &= t+2 = a, \end{aligned}$$

and so condition (5) is satisfied. Therefore $t+2, \frac{t+2}{2} - \frac{\sqrt{D}}{2}$ is a canonical basis for I. Then

$$\Lambda_K(I) = \begin{pmatrix} t+2 & \frac{t+2}{2} - \frac{\sqrt{D}}{2} \\ t+2 & \frac{t+2}{2} + \frac{\sqrt{D}}{2} \end{pmatrix} \mathbb{Z}^2 = A\mathbb{Z}^2,$$

where we make a change of basis so that

$$A = \begin{pmatrix} \frac{t+2}{2} + \frac{\sqrt{D}}{2} & \frac{t+2}{2} - \frac{\sqrt{D}}{2} \\ \frac{t+2}{2} - \frac{\sqrt{D}}{2} & \frac{t+2}{2} + \frac{\sqrt{D}}{2} \end{pmatrix}. \tag{10}$$

Then for any $\boldsymbol{x} = A \begin{pmatrix} m \\ n \end{pmatrix} \in \Lambda_K(I)$,

$$\begin{aligned} \|\boldsymbol{x}\|^2 &= Q(m,n) := (m\ n) A^t A \begin{pmatrix} m \\ n \end{pmatrix} \\ &= t(t+2)m^2 + 4(t+2)mn + t(t+2)n^2, \end{aligned} \tag{11}$$

and hence the positive definite integral binary quadratic form $Q(m,n)$ is reduced and symmetric for each $t \geq 5$. As in the proof of Lemma 2.5, this implies that $\Lambda_K(I)$ is WR. Thus we have constructed an infinite family of real quadratic number fields $\mathbb{Q}(\sqrt{D})$ with $D > 1$, $D \equiv 1 (\mathrm{mod}\, 4)$, each of which contains at least one ideal $I \subseteq \mathcal{O}_K$ so that $\Lambda_K(I)$ is WR. This completes the proof of the lemma. □

Remark 2.2. It is interesting to notice that the basis choices for the lattice $\Lambda_K(I)$ resulting in the reduced symmetric norm form in Lemmas 2.5 and 2.6 are different: in the imaginary quadratic case this basis is (7), which corresponds to the canonical basis for the ideal, while in the real quadratic case this is the basis (10), which is obtained from the canonical basis by an elementary change of basis operation.

Proof of Theorem 1.1. Theorem 1.1 now follows immediately from Lemmas 2.5 and 2.6. □

Remark 2.3. In Tables 1 and 2 we present a few examples of ideals I in quadratic number fields $K = \mathbb{Q}(\sqrt{-D})$ with $-D \equiv 1 (\mathrm{mod}\, 4)$ and $K = \mathbb{Q}(\sqrt{D})$ with $D \equiv 1 (\mathrm{mod}\, 4)$, respectively, so that $\Lambda_K(I)$ is WR, as discussed in Lemmas 2.5 and 2.6; for each such ideal, we give a presentation in terms of the canonical basis and explicitly write down elements of I that result in minimal vectors in $\Lambda_K(I)$ under the embedding σ (we call them *minimal elements*). Notice that these families consists only of some ideals for which the quadratic form Q, either corresponding to the unique choice of the basis as in (4) or obtained from it by one elementary change of basis operation, is reduced and symmetric. There may of course be many other such examples, as well as other more complicated situations when the form is not reduced, but is equivalent to a symmetric reduced form, in which case the lattice in question is again WR. In other words, there are likely many more WR lattices coming from ideals in real and imaginary quadratic fields than the proofs of Lemmas 2.5 and 2.6 demonstrate. In order for this to happen, it is necessary for the discriminant of the corresponding positive definite quadratic form Q to have a class represented by a symmetric reduced form; see pp. 19–20 of [7] for some computational data and p. 27 for related remarks.

TABLE 1. Examples of ideals in imaginary quadratic fields $K = \mathbb{Q}(\sqrt{-D})$ that give rise to WR lattices.

$-D$	Ideal $I \subset \mathcal{O}_K$	Minimal elements
-15	$\left\langle 2, \frac{1-\sqrt{-15}}{2} \right\rangle$	$\pm 2, \pm\frac{1-\sqrt{-15}}{2}$
-55	$\left\langle 4, \frac{3-\sqrt{-55}}{2} \right\rangle$	$\pm 4, \pm\frac{3-\sqrt{-55}}{2}$
-119	$\left\langle 6, \frac{5-\sqrt{119}}{2} \right\rangle$	$\pm 6, \pm\frac{5-\sqrt{119}}{2}$
-207	$\left\langle 8, \frac{7-\sqrt{207}}{2} \right\rangle$	$\pm 8, \pm\frac{7-\sqrt{207}}{2}$

TABLE 2. Examples of ideals in real quadratic fields $K = \mathbb{Q}(\sqrt{D})$ that give rise to WR lattices.

D	Ideal $I \subset \mathcal{O}_K$	Minimal elements
21	$\left\langle 7, \frac{7-\sqrt{21}}{2} \right\rangle$	$\pm\frac{7\pm\sqrt{21}}{2}$
165	$\left\langle 15, \frac{15-\sqrt{165}}{2} \right\rangle$	$\pm\frac{15\pm\sqrt{165}}{2}$
285	$\left\langle 19, \frac{19-\sqrt{285}}{2} \right\rangle$	$\pm\frac{19\pm\sqrt{285}}{2}$
957	$\left\langle 33, \frac{33-\sqrt{957}}{2} \right\rangle$	$\pm\frac{33\pm\sqrt{957}}{2}$

Finally notice that all examples in Tables 1 and 2 have 4 minimal elements. In fact, all elements of the infinite family of ideals we constructed in the proof of Lemma 2.5 have 4 minimal elements. We remark on this in our next lemma.

Lemma 2.7. *Let $D \neq \pm 3$ be a squarefree integer and $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field. Let $I \subset \mathcal{O}_K$ be an ideal, then $|S(\Lambda_K(I))| \leq 4$.*

Proof. Let D be a squarefree integer, $K = \mathbb{Q}(\sqrt{D})$ be a quadratic number field, and $I \subset \mathcal{O}_K$ an ideal. By Lemma 2.1, $|S(\Lambda_K(I))| \leq 4$ unless $\Lambda_K(I) \sim \Lambda_h$, in which case $S(\Lambda_K(I))$ contains 6 vectors. Assume this is the case, then there must exist $\boldsymbol{x}, \boldsymbol{y} \in S(\Lambda_K(I))$ such that the angle between these two vectors is $\pi/3$. In other words, one of these two vectors, say $\boldsymbol{y}$, is obtained from the other, $\boldsymbol{x} = \begin{pmatrix} x_{11} + x_{12}\sqrt{|D|} \\ x_{21} + x_{22}\sqrt{|D|} \end{pmatrix}$ with $x_{ij} \in \mathbb{Q}$, by rotating it by $\pi/3$, i.e.

$$\boldsymbol{y} = \begin{pmatrix} \frac{1}{2} & -\frac{\sqrt{3}}{2} \\ \frac{\sqrt{3}}{2} & \frac{1}{2} \end{pmatrix} \boldsymbol{x} \in \mathbb{Q}\left(\sqrt{|D|}\right)^2.$$

This readily implies that $\sqrt{3} \in \mathbb{Q}(\sqrt{|D|})$, meaning that $D = \pm 3$. This completes the proof. □

Remark 2.4. Both number fields $\mathbb{Q}(\sqrt{-3})$ and $\mathbb{Q}(\sqrt{3})$ contain ideals giving rise to WR lattices with six minimal vectors, i.e., similar to the hexagonal lattice. The fact that this is true for every ideal of $\mathbb{Q}(\sqrt{-3})$ is well-known (in particular, it follows from our Corollary 2.4). As for $\mathbb{Q}(\sqrt{3})$, it is easy to see that if $I = \langle 1 - \sqrt{3} \rangle \subset \mathcal{O}_{\mathbb{Q}(\sqrt{3})}$, then

$$\Lambda_K(I) = \begin{pmatrix} 1+\sqrt{3} & 2 \\ 1-\sqrt{3} & 2 \end{pmatrix} \mathbb{Z}^2$$

is a WR lattice with $S(\Lambda_K(I)) = \left\{ \pm \begin{pmatrix} 2 \\ 2 \end{pmatrix}, \pm \begin{pmatrix} 1+\sqrt{3} \\ 1-\sqrt{3} \end{pmatrix}, \pm \begin{pmatrix} 1-\sqrt{3} \\ 1+\sqrt{3} \end{pmatrix} \right\}$. This lattice is similar to Λ_h.

3. WR principal ideal lattices

In this section we investigate principal ideal lattices with the WR property in any dimension, proving that they come only from cyclotomic fields. We first need a simple minimization lemma, which is essentially the extremal case of the arithmetic mean - geometric mean inequality (from now on abbreviated AM-GM inequality).

Lemma 3.1. *Let $N \geq 1$ be an integer, and write $\boldsymbol{Y} = (Y_1, \ldots, Y_N)$ for a variable vector. Then*

$$\left(\prod_{n=1}^{N} Y_n \right)^{1/N} \leq \frac{1}{N} \sum_{n=1}^{N} Y_n \tag{12}$$

holds for all nonnegative real values of $Y_1, \ldots, Y_N$. Moreover, let A be a positive real number, and let

$$f(\boldsymbol{Y}) = \sum_{n=1}^{N} Y_n, \ g(\boldsymbol{Y}) = \prod_{n=1}^{N} Y_n - A.$$

Then the minimum of $f(\boldsymbol{Y})$ under the constraints $g(\boldsymbol{Y}) = 0$ and $Y_n > 0$ for all $1 \leq n \leq N$ is achieved if and only if

$$Y_1 = \cdots = Y_N,$$

in which case

$$\frac{1}{N} \sum_{n=1}^{N} Y_n = \left(\prod_{n=1}^{N} Y_n \right)^{1/N} = A^{1/N}.$$

In particular, if $A = 1$, this happens when $Y_n = 1$ for all $1 \leq n \leq N$, in which case the minimum of the sum $f(\boldsymbol{Y})$ is equal to N.

Proof. Formula (12) is the usual AM-GM inequality. The rest of the statement of this lemma is readily verified, for instance by the method of Lagrange multipliers. This is simply the well-known fact that the arithmetic mean of N positive numbers with a fixed geometric mean is minimized when all of these numbers are equal. The standard geometric interpretation of this fact is that among all N-dimensional boxes with a fixed volume, the sum of lengths of edges connected to each vertex is minimized in an N-dimensional cube of that volume. □

In order to proceed with the remainder of this section, we need to set up some basic notation of absolute values on number fields. We always write K for a number field of degree d over $\mathbb{Q}$ with r_1 real and $2r_2$ complex embeddings and $\mathcal{O}_K$ for its ring of integers, as specified in Section 1. Let $M(K)$ be the set of places of K. For each place $v \in M(K)$ we write K_v for the completion of K at v and let $d_v = [K_v : \mathbb{Q}_v]$ be the local degree of K at v. Then for each place $u \in M(\mathbb{Q})$ we have

$$\sum_{v \in M(K), v|u} d_v = d. \tag{13}$$

For each place $v \in M(K)$ we define the absolute value $|\ |_v$ to be the unique absolute value on K_v that extends either the usual absolute value $|\ |$ on $\mathbb{R}$ or $\mathbb{C}$ if $v|\infty$, or the usual p-adic absolute value on $\mathbb{Q}_p$ if $v|p$, where p is a prime. Therefore, the archimedean places are split into the real $v_1, \ldots, v_{r_1}$ and the complex $u_1, \ldots, u_{r_2}$, given by

$$|x|_{v_n} = |\sigma_n(x)|, \ \forall\ 1 \leq n \leq r_1,$$

and

$$|x|_{u_m} = |\tau_m(x)| = |\bar{\tau}_m(x)| = \sqrt{\tau_{m1}(x)^2 + \tau_{m2}(x)^2}, \ \forall\ 1 \leq m \leq r_2,$$

for each $x \in K$. For every finite place $v \in M(K)$, $v \nmid \infty$, we define the *local ring of v-adic integers* $\mathfrak{O}_v = \{x \in K : |x|_v \leq 1\}$, whose unique maximal ideal is

$\mathfrak{M}_v = \{x \in K : |x|_v < 1\}$. Then $O_K = \bigcap_{v \nmid \infty} \mathfrak{O}_v$. For each $0 \neq x \in K$ the *product formula* reads

$$\prod_{v \in M(K)} |x|_v^{d_v} = 1. \tag{14}$$

Then for each $0 \neq x \in \mathcal{O}_K$ we must have

$$|\,\mathrm{N}(x)| = \prod_{v|\infty} |x|_v^{d_v} \geq 1, \text{ since } \prod_{v \nmid \infty} |x|_v^{d_v} \leq 1, \tag{15}$$

where $\mathrm{N}(x)$ is the norm of x.

With this notation at hand, we can proceed to our next lemma, which provides a basic description of the set of minimal vectors for a principal ideal lattice.

Lemma 3.2. *Let K be a number field of degree d over $\mathbb{Q}$ with r_1 real and $2r_2$ complex embeddings, and let $I \subseteq \mathcal{O}_K$ be an ideal. Then*

$$|\Lambda_K(I)| \geq (r_1 + r_2)\,\mathrm{N}(I)^{\frac{1}{r_1+r_2}}, \tag{16}$$

and $|\Lambda_K| = r_1 + r_2$. Moreover, if $\sigma(x) \in S(\Lambda_K)$ for some $x \in \mathcal{O}_K$, then x is a root of unity. Hence we have

$$S(\Lambda_K) = \{\boldsymbol{x} \in \Lambda_K : \|\boldsymbol{x}\|^2 = r_1 + r_2\} = \{\sigma(x) : x \in \mathcal{O}_K \text{ is a root of unity}\}.$$

Proof. Fix $0 \neq x \in \mathcal{O}_K$, and order the real embeddings in such a way that

$$|\sigma_1(x)|, \ldots, |\sigma_k(x)| \geq 1, \ |\sigma_{k+1}(x)|, \ldots, |\sigma_{r_1}(x)| < 1, \tag{17}$$

for some $0 \leq k \leq r_1$. Then

$$\begin{aligned} 1 \ &\leq \ |\,\mathrm{N}(x)|^{\frac{1}{r_1+r_2}} = \left\{\prod_{v|\infty} |x|_v^{d_v}\right\}^{\frac{1}{r_1+r_2}} \\ &= \left(\prod_{n=1}^{k} |\sigma_n(x)| \times \prod_{n=k+1}^{r_1} |\sigma_n(x)| \times \prod_{m=1}^{r_2} (\tau_{m1}(x)^2 + \tau_{m2}(x)^2)\right)^{\frac{1}{r_1+r_2}} \qquad (18) \\ &\leq \left(\prod_{n=1}^{k} |\sigma_n(x)|^2 \times \prod_{n=k+1}^{r_1} \left(\frac{1+|\sigma_n(x)|^2}{2}\right) \times \prod_{m=1}^{r_2} (\tau_{m1}(x)^2 + \tau_{m2}(x)^2)\right)^{\frac{1}{r_1+r_2}} \end{aligned}$$

where the last inequality follows by the AM-GM inequality, since for every real number $a \geq 0$,

$$a = \sqrt{1 \times a^2} \leq \frac{1+a^2}{2}.$$

Applying the AM-GM inequality to (18) once again, we see that $|\,\mathrm{N}(x)|^{\frac{1}{r_1+r_2}}$ is

$$\begin{aligned} &\leq \ \frac{1}{r_1+r_2}\left(\sum_{n=1}^{k} \sigma_n(x)^2 + \frac{1}{2}\sum_{n=k+1}^{r_1} (1+\sigma_n(x)^2) + \sum_{m=1}^{r_2} (\tau_{m1}(x)^2 + \tau_{m2}(x)^2)\right) \\ &= \ \frac{1}{r_1+r_2}\left(\|\sigma(x)\|^2 + \frac{1}{2}\sum_{n=k+1}^{r_1} (1-\sigma_n(x)^2)\right) \leq \frac{\|\sigma(x)\|^2}{r_1+r_2}, \qquad (19) \end{aligned}$$

which implies that

$$\|\sigma(x)\|^2 \geq (r_1+r_2)|\,\mathrm{N}(x)|^{\frac{1}{r_1+r_2}} \geq r_1 + r_2 \tag{20}$$

for each $x \in \mathcal{O}_K$. On the other hand, one readily checks that $\|\sigma(1)\|^2 = r_1 + r_2$, and hence $|\Lambda_K| = r_1 + r_2$. Hence if $\sigma(x) \in S(\Lambda_K)$, we must have $|\,\mathrm{N}(x)| = 1$, meaning that x is a unit. Now suppose that $I \subseteq \mathcal{O}_K$ is an ideal and $x \in I$. By Lemma 5.1 of [9], we see that

$$|\,\mathrm{N}(x)| \geq \mathrm{N}(I). \tag{21}$$

Then (20) implies that $\|\sigma(x)\|^2 \geq (r_1 + r_2)\,\mathrm{N}(I)^{\frac{1}{r_1+r_2}}$, which proves (16).

For the rest of this proof, assume that $x \in \mathcal{O}_K$ is such that $\sigma(x) \in S(\Lambda_K)$, so $\|\sigma(x)\|^2 = r_1 + r_2$, which is the smallest possible. Then, combining (18) with (19), we obtain

$$\begin{aligned} 1 \quad &\leq \quad \left(\prod_{n=1}^{k} \sigma_n(x)^2 \times \prod_{n=k+1}^{r_1} \left(\frac{1+\sigma_n(x)^2}{2}\right) \times \prod_{m=1}^{r_2} (\tau_{m1}(x)^2 + \tau_{m2}(x)^2)\right)^{\frac{1}{r_1+r_2}} \\ &\leq \quad \frac{1}{r_1+r_2}\left(\sum_{n=1}^{k} \sigma_n(x)^2 + \frac{1}{2}\sum_{n=k+1}^{r_1} (1+\sigma_n(x)^2) + \sum_{m=1}^{r_2} (\tau_{m1}(x)^2 + \tau_{m2}(x)^2)\right) \\ &\leq \quad \frac{\|\sigma(x)\|^2}{r_1+r_2} = 1, \end{aligned} \tag{22}$$

and hence there must be equality throughout (22). By Lemma 3.1, this happens if and only if

$$\begin{aligned} &\sigma_1(x)^2 = \cdots = \sigma_k(x)^2 \\ &= \left(\frac{1+\sigma_{k+1}(x)^2}{2}\right) = \cdots = \left(\frac{1+\sigma_{r_1}(x)^2}{2}\right) \\ &= \tau_{11}(x)^2 + \tau_{12}(x)^2 = \cdots = \tau_{r_2 1}(x)^2 + \tau_{r_2 2}(x)^2 = 1. \end{aligned} \tag{23}$$

Combining this observation with (17), we conclude that $k = r_1$, and therefore x must be a root of unity, by Kronecker's Theorem. Conversely, if x is a root of unity, then

$$\sigma_1(x)^2 = \cdots = \sigma_{r_1}(x)^2 = \tau_{11}(x)^2 + \tau_{12}(x)^2 = \cdots = \tau_{r_2 1}(x)^2 + \tau_{r_2 2}(x)^2 = 1,$$

and so $\|\sigma(x)\|^2 = r_1 + r_2$, meaning that $\sigma(x) \in S(\Lambda_K)$. This completes the proof of the lemma. □

Next we show that principal ideal lattices coming from cyclotomic fields are always WR.

Lemma 3.3. *Let k be a positive integer, let ζ_k be primitive k-th root of unity, and let $K = \mathbb{Q}(\zeta_k)$ be k-th cyclotomic field. Then the lattice Λ_K is WR in $\mathbb{R}^d$, where $d = \varphi(k)$.*

Proof. If $k = 1, 2$, then $K = \mathbb{Q}$, and so $\Lambda_K = \mathbb{Z}$, which is WR. If $k = 3, 4$, the result follows from Lemma 2.2. If $k > 4$, it is clear that for $K = \mathbb{Q}(\zeta_k)$, $r_1 = 0$, and for each $1 \leq m \leq r_2 = d/2$ and $n \in \mathbb{Z}_{\geq 0}$,

$$|\tau_m(\zeta_k^n)|^2 = |\bar{\tau}_m(\zeta_k^n)|^2 = \tau_{m1}(\zeta_k^n)^2 + \tau_{m2}(\zeta_k^n)^2 = 1,$$

meaning that $\|\sigma(\zeta_k^n)\|^2 = r_2$, and so $\sigma(\zeta_k^n) \in S(\Lambda_K)$, by Lemma 3.2. Hence $S(\Lambda_K)$ contains $\varphi(k) = d$ linearly independent vectors, since the collection of elements $\{\zeta_k^n : 0 \leq n \leq \varphi(k) - 1\}$ forms an integral basis for $\mathcal{O}_K$, and so Λ_K is WR. □

Finally we prove that if K is not cyclotomic, then Λ_K cannot be WR.

Lemma 3.4. *Let K be a number field of degree $d = [K : \mathbb{Q}] \geq 2$ such that Λ_K is WR, then K is cyclotomic.*

Proof. First suppose that $r_1 > 0$, then the only roots of unity in K are ± 1, meaning that

$$S(\Lambda_K) = \{\sigma(1), \sigma(-1)\},$$

by Lemma 3.2. Then $\dim_{\mathbb{R}} \operatorname{span} S(\Lambda_K) = 1 < d$, and so Λ_K is not WR.

From now on assume that K is totally imaginary, then $r_1 = 0$ and $2r_2 = d = [K : \mathbb{Q}]$. Let $x \in \mathcal{O}_K$ such that $\sigma(x) \in S(\Lambda_K)$, then Lemma 3.2 implies that x is a root of unity. Let ζ_k be a root of unity of the highest order in K, then all other roots of unity in K are powers of ζ_k, and so are contained in $\mathbb{Z}[\zeta_k] \subseteq \mathcal{O}_K$, which means that they can be expressed as integral linear combinations of $1, \zeta_k, \dots, \zeta_k^{\varphi(k)-1}$, an integral basis for $\mathbb{Z}[\zeta_k]$. Hence at most $\varphi(k)$ roots of unity in K can be linearly independent over $\mathbb{Z}$, and so $S(\Lambda_K)$ can contain at most $\varphi(k)$ linearly independent vectors. In order for Λ_K to be WR, $\varphi(k)$ must be equal to d by Lemma 3.2, meaning that K is the cyclotomic field $\mathbb{Q}(\zeta_k)$. □

Proof of Theorem 1.2. Theorem 1.2 follows upon combining Lemmas 3.2, 3.3, and 3.4. □

As a consequence of Theorem 1.2, we can also prove that in fact all ideal lattices coming from cyclotomic fields are WR.

Proof of Corollary 1.3. Let I be a fractional ideal of $\mathcal{O}_K$, where $K = \mathbb{Q}(\zeta_k)$ for some primitive k-th root of unity ζ_k, $k \geq 2$. If $k = 2$, the result follows from Corollary 2.4, so assume that $k \geq 3$. Suppose that $\sigma(x) \in S(\Lambda_K(I))$ for some $x \in I$. Notice that, since K is a cyclotomic field,

$$\|\sigma(x)\|^2 = \sum_{n=1}^{\varphi(k)} \tau_n(x)\bar{\tau}_n(x).$$

Then for each $0 \leq m \leq k$,

$$\begin{aligned} \|\sigma(\zeta_k^m x)\|^2 &= \sum_{n=1}^{\varphi(k)} \tau_n(\zeta_k^m x)\bar{\tau}_n(\zeta_k^m x) \\ &= \sum_{n=1}^{\varphi(k)} \tau_n(\zeta_k^m)\bar{\tau}_n(\zeta_k^m)\tau_n(x)\bar{\tau}_n(x) \\ &= \sum_{n=1}^{\varphi(k)} \tau_n(x)\bar{\tau}_n(x) = \|\sigma(x)\|^2, \end{aligned} \tag{24}$$

and hence $\sigma(\zeta_k^m x) \in S(\Lambda_K(I))$ for each $0 \leq m \leq k$. Since the collection of elements $\{\zeta_k^m : 0 \leq m \leq \varphi(k) - 1\}$ forms an integral basis for $\mathcal{O}_K$, the collection $\{\zeta_k^m x : 0 \leq m \leq \varphi(k) - 1\}$ is linearly independent, which in turn implies that the collection of vectors

$$\{\sigma(\zeta_k^m x) : 0 \leq m \leq \varphi(k) - 1\} \subset S(\Lambda_K(I))$$

is linearly independent in $\mathbb{R}^{\varphi(k)}$, and so $\Lambda_K(I)$ is WR. □

Acknowledgment. We would like to thank Professors Wai Kiu Chan and Sinnou David for their highly helpful comments on the subject of this paper. We would also like to thank the referee for the very useful remarks.

References

[1] A. H. Banihashemi and A. K. Khandani. On the complexity of decoding lattices using the Korkin-Zolotarev reduced basis. *IEEE Trans. Inform. Theory*, 44(1):162–171, 1998.
[2] E. Bayer-Fluckiger. Lattices and number fields. Contemp. Math. 241, pages 69–84, 1999.
[3] E. Bayer-Fluckiger. Ideal lattices. In *A panorama of number theory or the view from Baker's garden (Zurich, 1999)*, pages 168–184. Cambridge Univ. Press, Cambridge, 2002.
[4] E. Bayer-Fluckiger. Upper bounds for Euclidean minima of algebraic number fields. *J. Number Theory*, 121(2):305–323, 2006.
[5] E. Bayer-Fluckiger and G. Nebe. On the Euclidean minimum of some real number fields. *J. Thor. Nombres Bordeaux*, 17(2):437454, 2005.
[6] E. Bayer-Fluckiger, F. Oggier, and E. Viterbo. Algebraic lattice constellations: bounds on performance. *IEEE Trans. Inform. Theory*, 52(1):319–327, 2006.
[7] D. A. Buell. *Binary Quadratic Forms*. Springer-Verlag, 1989.
[8] S. Clary and J. Fabrykowski. Arithmetic progressions, prime numbers, and squarefree integers. *Czechoslovak Math. J.*, 54(129)(4):915–927, 2004.
[9] H. Cohn and N. Heninger. Ideal forms of Coppersmith's theorem and Guruswami-Sudan list decoding. *preprint, arXiv:math.NT/1008.1284v1*.
[10] L. Fukshansky. On distribution of well-rounded sublattices of $\mathbb{Z}^2$. *J. Number Theory*, 128(8):2359–2393, 2008.
[11] L. Fukshansky. On similarity classes of well-rounded sublattices of $\mathbb{Z}^2$. *J. Number Theory*, 129(10):2530–2556, 2009.
[12] L. Fukshansky, D. Moore, R. A. Ohana, and W. Zeldow. On well-rounded sublattices of the hexagonal lattice. *Discrete Math.*, 310(23):3287–3302, 2010.
[13] D. A. Marcus. *Number Fields*. Springer-Verlag, 1977.
[14] J. Martinet. *Perfect Lattices in Euclidean Spaces*. Springer-Verlag, 2003.
[15] C. McMullen. Minkowski's conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.
[16] M. A. Tsfasman and S. G. Vladut. *Algebraic-Geometric Codes*. Kluwer Academic Publishers, 1991.

Department of Mathematics, 850 Columbia Avenue, Claremont McKenna College, Claremont, CA 91711
E-mail address: lenny@cmc.edu

Department of Mathematics, Florida State University, 208 Love Building, 1017 Academic Way, Tallahassee, FL 32306
E-mail address: petersen@math.fsu.edu