

ON INDECOMPOSABLE ELEMENTS IN LATTICES

LENNY FUKSHANSKY AND FILIANA KOSTOPOULOU

ABSTRACT. We study the distribution of indecomposable elements in Euclidean lattices. A positive element in a lattice is called indecomposable if it cannot be represented as a sum of two other positive nonzero elements. The set of all indecomposables in a lattice forms the Hilbert basis for the positive lattice semigroup. We classify lattices that contain only finitely many indecomposables versus those that contain infinitely many. In the two-dimensional case, we prove that every positive element in a lattice can be represented as a positive integer linear combination of at most two indecomposables, which is a certain variation of the discrete Carathéodory's property. In the case of lattices coming from fractional ideals in real quadratic number fields, we obtain an explicit counting estimate for the number of indecomposables with bounded norm, showing logarithmic growth.

1. INTRODUCTION AND SUMMARY OF RESULTS

Let K be a totally real number field of degree $n \geq 2$ and let $\sigma_1, \dots, \sigma_n : K \hookrightarrow \mathbb{R}$ be its embeddings. The *norm* of an element $\alpha \in K$ is defined as

$$\mathbb{N}_K(\alpha) = \prod_{j=1}^n |\sigma_j(\alpha)|,$$

and the *house* of α is

$$H_K(\alpha) = \max\{|\sigma_1(\alpha)|, \dots, |\sigma_n(\alpha)|\}.$$

Write \mathcal{O}_K for the ring of integers of K and define the *semigroup of totally positive integers* in K to be

$$\mathcal{O}_K^+ = \{\alpha \in \mathcal{O}_K : \sigma_j(\alpha) \geq 0 \forall 1 \leq j \leq n\}.$$

A nonzero element $\alpha \in \mathcal{O}_K^+$ is called *decomposable* if there exist nonzero elements $\beta, \gamma \in \mathcal{O}_K^+$ such that $\alpha = \beta + \gamma$; otherwise, α is called *indecomposable*. Indecomposables in totally real number fields have been extensively studied, in particular in connection to the theory of universal quadratic forms (see [7] for a detailed survey). As discussed in [7], the number of indecomposables in \mathcal{O}_K^+ is always finite, up to multiplication by totally positive units; in fact, indecomposables can be described as elements of \mathcal{O}_K^+ of appropriately bounded norm ([8], Theorem 5). This being said, the group of units is infinite, and while multiplication by a unit does not change the norm of an element, it certainly changes its house. On the other

2020 *Mathematics Subject Classification*. Primary: 11H06; Secondary: 11R80, 52B20.

Key words and phrases. Euclidean lattice, indecomposable element, positive cone, algebraic numbers, house.

hand, the ring of integers \mathcal{O}_K can be viewed as a Euclidean lattice in \mathbb{R}^n under the standard *Minkowski embedding*

$$\Sigma_K = (\sigma_1, \dots, \sigma_n) : K \hookrightarrow \mathbb{R}^n,$$

where \mathcal{O}_K^+ becomes a positive lattice semigroup, which allows us to view indecomposables in the context of the geometry of numbers. In particular, the house $H_K(\alpha)$ of an element $\alpha \in K$ becomes the sup-norm $|\Sigma_K(\alpha)|$ of its image under the Minkowski embedding. The goal of the present note is to define indecomposables more generally in Euclidean lattices, study their properties using geometric tools, and then apply our observations in the context of real quadratic number fields.

Throughout this paper, we write $|\cdot|$ for the sup-norm and $\|\cdot\|$ for the Euclidean norm on vectors in \mathbb{R}^n . Let $L \subset \mathbb{R}^n$ be a lattice of rank $n \geq 2$ and define the positive lattice semigroup

$$L^+ = L \cap \mathbb{R}_{\geq 0}^n = \{\mathbf{x} \in L : x_i \geq 0 \forall 1 \leq i \leq n\}.$$

A nonzero vector $\mathbf{x} \in L^+$ is called *decomposable* if there exist nonzero vectors $\mathbf{y}, \mathbf{z} \in L^+$ such that $\mathbf{x} = \mathbf{y} + \mathbf{z}$; otherwise, \mathbf{x} is called *indecomposable*.

The first question we want to address is which lattices have finitely many and which infinitely many indecomposables. We start with some notation. A basis for L is called a *positive basis* if it is contained in L^+ . A lattice is called *rectangular* if it has an orthogonal basis. A lattice is called *virtually rectangular* if it has a rectangular sublattice of finite index; virtually rectangular lattices have been investigated in [9] and [4]. Let us also say that a lattice L is *positive rectangular*, abbreviated PR, if it contains a positive orthogonal basis, and L is called *positive virtually rectangular*, abbreviated PVR, if it contains a PR sublattice M of finite index. We can now state our first result.

Theorem 1.1. *If L is a PVR lattice of rank n , then L^+ contains at most $d+n-1$ indecomposable elements, where*

$$d = \min\{[L : M] : M \subseteq L \text{ is PR}\}.$$

Otherwise, L^+ contains infinitely many indecomposable elements.

We prove Theorem 1.1 in Section 2, where we also review some properties of lattice semigroups and cones, and prove that vectors corresponding to positive successive minima in a lattice are indecomposable. In fact, the indecomposables are precisely the unique minimal generating set for the semigroup L^+ , called the *Hilbert basis* for L^+ (Corollary 2.5). In Section 3, we discuss irreducible elements in lattice cones, observing that indecomposables are always irreducible but not vice versa. Each such cone contains only finitely many irreducibles, and they form the Hilbert basis for the lattice-point semigroup of this cone. Thus, it follows that while the semigroup L^+ of a non-PVR lattice L contains infinitely many indecomposables, every positive lattice cone of L contains only finitely many of these indecomposables.

In Section 4, we focus on indecomposable elements in planar lattices, showing in particular that consecutive pairs of such indecomposables always form a basis for the lattice. The main result of this section is the following theorem.

Theorem 1.2. *Let $L \subset \mathbb{R}^2$ be a lattice of full rank and let $\mathbf{0} \neq \mathbf{z} \in L^+$ be a decomposable element. Then there exist indecomposables $\mathbf{u}, \mathbf{v} \in L^+$ and positive integers α, β so that $\mathbf{z} = \alpha\mathbf{u} + \beta\mathbf{v}$. Hence, $|\mathbf{u}| + |\mathbf{v}| \leq |\mathbf{z}|$.*

In other words, every positive point of a lattice in \mathbb{R}^2 can be represented as a positive linear combination of at most two indecomposables. This result should be viewed in the context of Carathéodory's theorem which states that every point in a convex cone in \mathbb{R}^n can be represented as a positive linear combination of at most n of the cone generators. Furthermore, any point in a discrete cone (set of integer points in a convex cone) can be represented as a positive linear combination of irreducibles in this cone, which are precisely the elements of the Hilbert basis for the cone. This cone is said to have the *discrete Carathéodory's property* if such representation is possible by no more than n elements of the Hilbert basis for every element. It is known that every discrete cone in dimensions $n \leq 3$ has discrete Carathéodory's property, while it is no longer true in general for cones in dimensions $n \geq 6$; see [1] for details. Our Theorem 1.2 is the 2-dimensional analogue of the discrete Carathéodory's property for indecomposables in the positive orthant of a lattice: the key difference here, complicating things, is that $\mathbb{R}_{\geq 0}^2$ is not generated by vectors of L as a cone unless L is PVR.

We separately consider indecomposable elements in lattices coming from fractional ideals in real quadratic number fields, in which case we can obtain a counting estimate. Let K be a real quadratic field with ring of integers \mathcal{O}_K and discriminant Δ_K . Let $J \subseteq K$ be a fractional ideal, and write $\mathbb{N}_K(J)$ for the norm of J . Let $L = \Sigma_K(J)$, then $\det(L) = \mathbb{N}_K(J)\sqrt{|\Delta_K|}$. In this case, L contains infinitely many indecomposables, hence we can define a counting function

$$\begin{aligned} \mathcal{N}_{K,J}(T) &= \{ \mathbf{x} \in L^+ : \mathbf{x} \text{ indecomposable}, |\mathbf{x}| \leq T \} \\ (1) \qquad &= \{ \alpha \in J^+ : \alpha \text{ indecomposable}, H_K(\alpha) \leq T \}, \end{aligned}$$

for a positive real number T . In Section 5, we produce the following estimate.

Theorem 1.3. *Let the notation be as above, then*

$$\mathcal{N}_{K,J}(T) \leq \left(\log \left(\frac{1 + \sqrt{4(\det(L))^2 + 1}}{2 \det(L)} \right) \right)^{-1} (2 \log T + 1) + 1.$$

To prove this theorem, we first show that all indecomposables are contained under the hyperbola $y = \frac{(\det(L))^2}{x}$ in the plane. This observation is based on an elegant argument of Kala and Yatsyna [8], which employs Minkowski's Convex Body Theorem. We then obtain the counting estimate by using the basis property of consecutive indecomposables along with an area computation. We are now ready to proceed.

2. PROPERTIES OF INDECOMPOSABLE ELEMENTS IN LATTICES

In this section we develop some necessary notation and prove Theorem 1.1. A vector $\mathbf{x} \in L$ is called *primitive* if it is not a scalar multiple of another vector in L . Indecomposable vectors are primitive, however the converse is not necessarily true. It is our goal to understand the properties of indecomposable elements in L^+ . We start with two simple but useful lemmas. Let us say that $\mathbf{x} \leq \mathbf{y}$ (respectively, $\mathbf{x} < \mathbf{y}$) if $x_i \leq y_i$ (respectively, $x_i < y_i$) for every i .

Lemma 2.1. *Let $L \subset \mathbb{R}^n$ be a lattice of rank n and let $\mathbf{x} \in L^+$. Then \mathbf{x} is indecomposable if and only if there does not exist $\mathbf{0} \neq \mathbf{y} \in L^+$ such that $\mathbf{y} \leq \mathbf{x}$.*

Proof. Suppose there exists $\mathbf{0} \neq \mathbf{y} \in L^+$ such that $\mathbf{y} \leq \mathbf{x}$. Let $\mathbf{z} = \mathbf{x} - \mathbf{y}$, then $\mathbf{z} \in L^+$. Hence, $\mathbf{x} = \mathbf{y} + \mathbf{z}$. Now, suppose no such \mathbf{y} exists. If \mathbf{x} is decomposable, then there exist some nonzero $\mathbf{y}, \mathbf{z} \in L^+$ such that

$$\mathbf{x} = \begin{pmatrix} x_1 \\ \vdots \\ x_n \end{pmatrix} = \begin{pmatrix} y_1 + z_1 \\ \vdots \\ y_n + z_n \end{pmatrix} = \mathbf{y} + \mathbf{z},$$

and so $x_i = y_i + z_i \geq y_i$ for each $1 \leq i \leq n$, i.e. $\mathbf{y} \leq \mathbf{x}$, a contradiction. Hence, \mathbf{x} is indecomposable. \square

Lemma 2.2. *Every element in L^+ is a positive integer linear combination of finitely many indecomposables.*

Proof. Let $\mathbf{x} \in L^+$ and suppose it is not indecomposable, then there exist $\mathbf{x}_1, \mathbf{x}_2 \in L^+$ such that $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$, and so

$$\|\mathbf{x}_1\|, \|\mathbf{x}_2\| < \|\mathbf{x}\|.$$

We can continue decomposing $\mathbf{x}_1, \mathbf{x}_2$ in the same manner, each time obtaining elements in L^+ of smaller norm. Since a lattice L is a discrete subset of \mathbb{R}^n , there are only finitely many elements in L of norm $\leq \|\mathbf{x}\|$. Hence, this process must terminate, meaning that we obtain a positive integer linear combination of indecomposables equal to \mathbf{x} . \square

Let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subset L^+$ be a collection of linearly independent vectors. We define the *cone* of X to be

$$C(X) := \left\{ \sum_{i=1}^n a_i \mathbf{x}_i : a_1, \dots, a_n \in \mathbb{R}_{\geq 0} \right\}$$

and the *semigroup* of X to be

$$S(X) := \left\{ \sum_{i=1}^n a_i \mathbf{x}_i : a_1, \dots, a_n \in \mathbb{Z}_{\geq 0} \right\}.$$

If X is a basis for L , we refer to $C(X)$ and $S(X)$ as a *basis cone* and a *basis semigroup*, respectively. Properties of such positive cones and semigroups have been investigated in [3]. In particular, Lemma 2.1 of [3] guarantees that L contains infinitely many positive bases; more precisely, this lemma can be formulated as follows.

Lemma 2.3. *Let $\mathbf{x}_1 \in L^+$ be a primitive vector. Then there exists a positive basis $\mathbf{x}_1, \mathbf{x}_2, \dots, \mathbf{x}_n \in L^+$.*

The following observation will also be important to us; it is Lemma 2.2 of [3].

Lemma 2.4. *Let X be a positive basis for L . Then*

$$L^+ \cap C(X) = S(X).$$

We are now ready for the proof of the theorem.

Proof of Theorem 1.1. First suppose that $L \subset \mathbb{R}^n$ is a PR lattice and let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subset L^+$ be the corresponding positive orthogonal basis. Then these basis vectors must be multiples of the standard basis vectors $\mathbf{e}_1, \dots, \mathbf{e}_n$ in \mathbb{R}^n ; we

can assume without loss of generality that $\mathbf{x}_i = t_i \mathbf{e}_i$ with $t_i \in \mathbb{R}_{>0}$ for $1 \leq i \leq n$. Let $\mathbf{y} \in L^+$. Since X is a basis for L ,

$$\mathbf{y} = \sum_{i=1}^n a_i t_i \mathbf{e}_i,$$

for some integers a_1, \dots, a_n and for each $1 \leq i \leq n$, $y_i = a_i t_i \geq 0$. Then all $a_i \geq 0$, and so

$$L^+ = S(X).$$

Hence, $\mathbf{y} \in L^+$ is indecomposable if and only if $\mathbf{y} = \mathbf{x}_i$ for some $1 \leq i \leq n$. This implies that L^+ contains precisely n indecomposable elements.

Now, assume that L is a PVR lattice and $M \subset L$ is a PR sublattice of L of index d . We can always select coset representatives $\mathbf{z}_1, \dots, \mathbf{z}_d$ of M in L to be in L^+ . Indeed, suppose that, say, \mathbf{z}_1 is not in L^+ , i.e., $z_{1j} < 0$ for some $1 \leq j \leq n$. Then we can pick $\mathbf{v} \in M^+$ to be an element with $v_j > |z_{1j}|$ for every $1 \leq j \leq n$ and replace \mathbf{z}_1 with $\mathbf{z}_1 + \mathbf{v} \in L^+$. Hence, from here on fix a set of coset representatives $\mathbf{z}_1, \dots, \mathbf{z}_d \in L^+$ of M in L with $\mathbf{z}_1 = \mathbf{0}$. Let $\mathbf{y} \in L^+$, then $\mathbf{y} = \mathbf{z}_k + \mathbf{x}$ for some unique $1 \leq k \leq d$ and $\mathbf{x} \in M$. Suppose that \mathbf{y} is indecomposable, then we must have $\mathbf{x} \notin M^+$. Let us write $\mathbf{x} = \mathbf{x}_1 + \mathbf{x}_2$ where for each $1 \leq j \leq n$

$$x_{1j} = \begin{cases} x_j & \text{if } x_j < 0 \\ 0 & \text{if } x_j \geq 0 \end{cases}, \quad x_{2j} = \begin{cases} 0 & \text{if } x_j < 0 \\ x_j & \text{if } x_j \geq 0, \end{cases}$$

so $\mathbf{y} = (\mathbf{z}_k + \mathbf{x}_1) + \mathbf{x}_2$ with $\mathbf{z}_k + \mathbf{x}_1 \in \mathbb{R}_{\geq 0}^n$. Let $t_1 \mathbf{e}_1, \dots, t_n \mathbf{e}_n$ be a positive orthogonal basis for M , as above. Since $\mathbf{x} \in M$, we must have $x_j = a_j t_j$ for some integers a_j , $1 \leq j \leq n$, with $a_j > 0$ for j 's corresponding to nonzero coordinates of \mathbf{x}_2 and $a_j < 0$ for j 's corresponding to nonzero coordinates of \mathbf{x}_1 . Then $\mathbf{x}_1, \mathbf{x}_2 \in M$ and \mathbf{x}_2 is a positive integer linear combination of a positive basis in M , hence $\mathbf{x}_2 \in M^+ \subseteq L^+$. We have

$$\mathbf{z}_k + \mathbf{x}_1 = \mathbf{y} - \mathbf{x}_2 \in L,$$

since $\mathbf{y} \in L$ and $\mathbf{x}_2 \in M \subseteq L$. Hence, $\mathbf{z}_k + \mathbf{x}_1 \in L^+$, thus either $\mathbf{x}_1 = -\mathbf{z}_k$ or $\mathbf{x}_2 = \mathbf{0}$, since \mathbf{y} is indecomposable. If $\mathbf{x}_2 \neq \mathbf{0}$, we must have $\mathbf{z}_k = -\mathbf{x}_1 \in M$, which means that $\mathbf{x}_1 = \mathbf{z}_1 = \mathbf{0}$; there are only finitely many options for $\mathbf{y} = \mathbf{x}_2$ (specifically, \mathbf{x}_2 is an indecomposable in the orthogonal lattice M , of which there are finitely many as we showed above). If $\mathbf{x}_2 = \mathbf{0}$, then $\mathbf{y} = \mathbf{z}_k + \mathbf{x}_1 \in L^+$, and hence for each $1 \leq j \leq n$,

$$-z_{kj} \leq x_{1j} \leq 0,$$

i.e., \mathbf{x}_1 is an element of M in a box of side-lengths z_{k1}, \dots, z_{kn} ; this is a finite set. Putting these observations together, we proved that there are only finitely many indecomposables in L^+ . Further, these indecomposables are either coset representatives $\mathbf{z}_2, \dots, \mathbf{z}_d$ or elements of the positive orthogonal basis for M , hence there are at most $d + n - 1$ of them.

Next, suppose that L is not PVR. Arguing towards a contradiction, assume that L has only finitely many indecomposables, let $V = \{\mathbf{v}_1, \dots, \mathbf{v}_m\} \in L^+$ be their complete set. Let $C(V)$ be cone spanned by these indecomposables, i.e.

$$C(V) := \left\{ \sum_{i=1}^m a_i \mathbf{v}_i : a_1, \dots, a_m \in \mathbb{R}_{\geq 0} \right\} \subset \mathbb{R}_{\geq 0}^n$$

and let $C(V)^* = \mathbb{R}_{\geq 0}^n \setminus C(V)$. Since L is not PVR, $C(V)^*$ must be nonempty, and hence unbounded. Let us write $\mathbb{B}_n(r)$ for the ball of radius r centered at the origin in \mathbb{R}^n . Then $C(V)^*$ contains Euclidean balls of arbitrarily large radius; in particular, it contains some Euclidean ball B of radius at least $\mu(L)$, where

$$(2) \quad \mu(L) = \min \{r \in \mathbb{R}_{>0} : L + \mathbb{B}_n(r) = \mathbb{R}^n\}$$

is the covering radius of L . Then B must contain a point of L , call it \mathbf{y} . Since $\mathbf{y} \notin C(V)$, it cannot be represented as a nonnegative linear combination of elements of V . On the other hand, Lemma 2.2 implies that there must exist a representation of \mathbf{y} as a positive integer linear combination of indecomposables, meaning that there must exist indecomposables outside of the set V , a contradiction. This concludes the proof. \square

The *Hilbert basis* of an affine semigroup is the unique minimal generating set. We record here an immediate consequence of Lemma 2.2 and Theorem 1.1, characterizing indecomposables as the Hilbert basis for the semigroup L^+ .

Corollary 2.5. *The set of indecomposables in the semigroup L^+ is precisely the Hilbert basis for L^+ , which is finite if L is a PVR lattice and infinite otherwise.*

We can also obtain a bound on the Euclidean norm of the shortest indecomposable element in L^+ . For this, let us define the *positive successive minima* of L to be

$$(3) \quad \lambda_j^+(L) := \min \{r \in \mathbb{R}_{>0} : \dim_{\mathbb{R}} \text{span}_{\mathbb{R}}(\mathbb{B}_n(r) \cap L^+) \geq j\},$$

for each $1 \leq j \leq n$, so $0 < \lambda_1^+(L) \leq \dots \leq \lambda_n^+(L)$. We say that linearly independent vectors $\mathbf{x}_1, \dots, \mathbf{x}_n \in L^+$ correspond to these positive successive minima if $\|\mathbf{x}_j\| = \lambda_j^+(L)$. Positive successive minima with respect to the unit cube instead of the unit ball were considered in [3]. Since $\|\mathbf{x}\| \leq \sqrt{n}|\mathbf{x}|$ for any vector $\mathbf{x} \in \mathbb{R}^n$, Theorem 1.2 of [3] implies, in particular, that

$$(4) \quad \lambda_1^+(L) \leq \sqrt{n}(2\mu(L) + 1),$$

where $\mu(L)$ is the covering radius of L defined in (2).

Lemma 2.6. *Let $\mathbf{x}_1, \dots, \mathbf{x}_n \in L^+$ be vectors corresponding to the positive successive minima $\lambda_1^+(L), \dots, \lambda_n^+(L)$, respectively. Then they are indecomposable.*

Proof. Suppose some \mathbf{x}_j is decomposable and let $\mathbf{y}, \mathbf{z} \in L^+$ be nonzero elements so that $\mathbf{x}_j = \mathbf{y} + \mathbf{z}$. Then $\|\mathbf{y}\|, \|\mathbf{z}\| < \|\mathbf{x}_j\| = \lambda_j^+(L)$, and so the sets of vectors $\mathbf{x}_1, \dots, \mathbf{x}_{j-1}, \mathbf{y}$ and $\mathbf{x}_1, \dots, \mathbf{x}_{j-1}, \mathbf{z}$ are linearly dependent. This means that

$$\mathbf{y} = \sum_{i=1}^{j-1} c_{1i} \mathbf{x}_i, \quad \mathbf{z} = \sum_{i=1}^{j-1} c_{2i} \mathbf{x}_i,$$

for some real coefficients $c_{11}, \dots, c_{1(j-1)}$, not all zero, and $c_{21}, \dots, c_{2(j-1)}$, also not all zero. Then

$$\mathbf{x}_j = \mathbf{y} + \mathbf{z} = \sum_{i=1}^{j-1} (c_{1i} + c_{2i}) \mathbf{x}_i,$$

meaning that the set of vectors $\mathbf{x}_1, \dots, \mathbf{x}_j$ is linearly dependent. This is a contradiction, hence \mathbf{x}_j must be indecomposable. \square

As an immediate consequence of Lemma 2.6 combined with (4) we have a bound on the shortest indecomposable element in L^+ .

Corollary 2.7. $\min \{\|\mathbf{x}\| \in L^+ : \mathbf{x} \text{ is indecomposable}\} \leq \sqrt{n}(2\mu(L) + 1)$.

3. IRREDUCIBLE ELEMENTS IN POLYHEDRAL CONES

Let $L \subset \mathbb{R}^n$ be a lattice of full rank, as above, and let $X = \{\mathbf{x}_1, \dots, \mathbf{x}_n\} \subset L$ be a collection of linearly independent points. Define the parallelepiped

$$P(X) = \left\{ \sum_{i=1}^n a_i \mathbf{x}_i : 0 \leq a_i < 1 \forall 1 \leq i \leq n \right\}.$$

Let $M(X) = \text{span}_{\mathbb{Z}} X$, a finite-index sublattice of L and define

$$\det(X) := \det(M(X)) = \text{Vol}_n(P(X)).$$

Lemma 3.1. *The number of points of L in $P(X)$ is equal to the index $[L : M(X)]$, i.e.,*

$$|P(X) \cap L| = \frac{\det(X)}{\det(L)}.$$

In particular, the collection X is a basis for L if and only if $P(X) \cap L = \{\mathbf{0}\}$.

Proof. The index $[L : M(X)] = \frac{\det(X)}{\det(L)}$ is the number of cosets of $M(X)$ in L and $P(X)$ is a fundamental domain for $M(X)$ in \mathbb{R}^n , meaning that $P(X) \cap L$ is the full set of coset representatives of $M(X)$ in L . Then X is a basis for L if and only if $L = M(X)$, i.e., if and only if $[L : M(X)] = 1$. In other words, X is a basis if and only if the only coset representative of $M(X)$ in L is $\mathbf{0}$. \square

Now let X as above consist only of primitive points in L and consider the cone $C(X)$. A nonzero element $\mathbf{y} \in C(X) \cap L$ is called *irreducible* if there do not exist nonzero elements $\mathbf{z}_1, \mathbf{z}_2 \in C(X) \cap L$ such that $\mathbf{y} = \mathbf{z}_1 + \mathbf{z}_2$. The set of irreducible points forms the Hilbert basis for the semigroup $C(X) \cap L$.

Lemma 3.2. *Let $n = 2$ and let $X = \{\mathbf{x}_1, \mathbf{x}_2\} \subset L^+$. If a primitive point $\mathbf{y} \in C(X) \cap L$ is irreducible, then $\mathbf{y} \in P(X) \cup X$.*

Proof. We need to prove that there are no irreducible points in $C(X) \cap L$ outside of $X \cup P(X)$. Let $X = \{\mathbf{x}_1, \mathbf{x}_2\}$ and $\mathbf{y}_1, \dots, \mathbf{y}_m$ be primitive points in $P(X) \cap L$, ordered in the way that

$$\mathbf{a}(\mathbf{x}_1, \mathbf{y}_1) < \mathbf{a}(\mathbf{x}_1, \mathbf{y}_2) < \dots < \mathbf{a}(\mathbf{x}_1, \mathbf{y}_m) < \mathbf{a}(\mathbf{x}_1, \mathbf{x}_2),$$

where $\mathbf{a}(\mathbf{x}, \mathbf{y})$ stands for the angle between these two vectors. For each pair of vectors \mathbf{x}, \mathbf{y} we write

$$C(\mathbf{x}, \mathbf{y}) = \{a\mathbf{x} + b\mathbf{y} : a, b \geq 0\}, \quad P(\mathbf{x}, \mathbf{y}) = \{a\mathbf{x} + b\mathbf{y} : 0 \leq a, b < 1\}$$

for the cone and the parallelogram spanned by them. Then

$$(5) \quad C(\mathbf{x}_1, \mathbf{x}_2) = C(\mathbf{x}_1, \mathbf{y}_1) \cup C(\mathbf{y}_1, \mathbf{y}_2) \cup \dots \cup C(\mathbf{y}_{m-1}, \mathbf{y}_m) \cup C(\mathbf{y}_m, \mathbf{x}_2).$$

Now, let P be one of the parallelograms $P(\mathbf{x}_1, \mathbf{y}_1), P(\mathbf{y}_1, \mathbf{y}_2), \dots, P(\mathbf{y}_m, \mathbf{x}_2)$ and suppose that $\mathbf{z} \in P \cap L$ is not equal to $\mathbf{0}$. Notice that $P \cap P(\mathbf{x}_1, \mathbf{x}_2)$ cannot contain any nonzero point, since this would mean that there is another primitive point in $P(\mathbf{x}_1, \mathbf{x}_2)$ which is not among $\mathbf{y}_1, \dots, \mathbf{y}_m$. Suppose that there is $\mathbf{z} \in P \cap L$

outside of $P(\mathbf{x}_1, \mathbf{x}_2)$. This point must then belong to some coset $\mathbf{z}' + M(X)$ of $M(X)$ in L , where $\mathbf{z}' \in (P \cap P(\mathbf{x}_1, \mathbf{x}_2) \cap L) -$ again, a contradiction. Hence, $P \cap L$ contains no nonzero points. Then Lemma 3.1 implies that the pairs of vectors $\{\mathbf{x}_1, \mathbf{y}_1\}, \{\mathbf{y}_1, \mathbf{y}_2\}, \dots, \{\mathbf{y}_m, \mathbf{x}_2\}$ are positive bases for L . By Lemma (2.4), every lattice point in a positive basis cone is representable as a nonnegative integer linear combination of these basis vectors; thus, none of the cones in the decomposition (5) can contain irreducible elements in their interior. Hence, the only irreducibles in $C(X)$ are primitive lattice points in $P(X) \cup X$. \square

Remark 3.1. Notice that not all primitive points in $P(X)$ are necessarily irreducible. Indeed, it is possible that, say, some $\mathbf{y}_i = \mathbf{y}_{i-1} + \mathbf{y}_{i+1}$.

Let $r > 0$ and $\mathbb{B}_2(r) \subset \mathbb{R}^2$ be a ball of radius r centered at $\mathbf{0}$. Let $\mathbf{x}_1, \mathbf{x}_2 \in \mathbb{B}_2(r) \cap L^+$ be such that the cones $C(\mathbf{e}_1, \mathbf{x}_1)$ and $C(\mathbf{e}_2, \mathbf{x}_2)$ contain no points of L of norm less than r . Notice that this condition ensures that $\mathbf{x}_1, \mathbf{x}_2$ are indecomposable elements in L . Further, all indecomposables in $\mathbb{B}_2(r) \cap L^+$ must be irreducibles in $C(\mathbf{x}_1, \mathbf{x}_2)$, and hence, are primitive points contained in the parallelogram $P(\mathbf{x}_1, \mathbf{x}_2)$. This implies that the number of indecomposables of norm $\leq r$ is no larger than the number of primitive points in $P(\mathbf{x}_1, \mathbf{x}_2)$. We investigate the two-dimensional case more in depth in the next section.

4. INDECOMPOSABLES IN PLANAR LATTICES

The goal of this section is to prove Theorem 1.2. For this, we construct a cover of positive lattice points by indecomposable basis cones. Throughout this section, let $L \subset \mathbb{R}^2$ be a lattice of rank 2 with positive successive minima λ_1^+, λ_2^+ . Let $\mathbf{x}, \mathbf{y} \in L^+$ be vectors corresponding to these positive successive minima.

Lemma 4.1. *The vectors \mathbf{x}, \mathbf{y} form a basis for L .*

Proof. Let

$$P = \{\mathbf{a}\mathbf{x} + \mathbf{b}\mathbf{y} : 0 \leq a, b < 1\}$$

be the parallelogram spanned by \mathbf{x}, \mathbf{y} . As before, write $\mathbb{B}_n(\lambda_2^+)$ for the closed ball of radius λ_2^+ centered at $\mathbf{0}$ and let $\mathbb{B}_n^o(\lambda_2^+)$ be its interior, the open ball. Notice that $\mathbb{B}_n^o(\lambda_2^+) \cap P$ cannot contain any point of L linearly independent with \mathbf{x} : this would contradict the definition of λ_2^+ . Suppose P contains a point of L , call it \mathbf{z} , then $\mathbf{z} \in P \setminus \mathbb{B}_n^o(\lambda_2^+)$ as in Figure 1. Let ABC be the triangle with the vertex A at $\mathbf{x} + \mathbf{y}$ and vertices B, C at the intersection points of \bar{P} , the closure of P , and $\mathbb{B}_n(\lambda_2^+)$, as in Figure 1. Then the point D at \mathbf{z} is closer to the vertex A than at least one of B and C , since the furthest point from a vertex in a triangle is another vertex. The distance from A to D is $\|\mathbf{x} + \mathbf{y} - \mathbf{z}\|$, hence

$$\|\mathbf{x} + \mathbf{y} - \mathbf{z}\| < \max\{AB, AC\} \leq \|\mathbf{y}\| = \lambda_2^+.$$

Since $\mathbf{x} + \mathbf{y} - \mathbf{z} \in L^+$ and it is linearly independent with \mathbf{x} , this contradicts the definition of λ_2^+ . This means that $P \cap L = \{\mathbf{0}\}$. Hence, by Lemma 3.1, \mathbf{x} and \mathbf{y} form a positive basis for L . \square

Corollary 4.2. *With notation as above, the cone $C(\mathbf{x}, \mathbf{y})$ contains no indecomposable elements of L^+ except for \mathbf{x} and \mathbf{y} . In particular, every point $\mathbf{z} \in C(\mathbf{x}, \mathbf{y}) \cap L^+$ can be expressed as $\mathbf{z} = a\mathbf{x} + b\mathbf{y}$ for some $a, b \in \mathbb{Z}_{\geq 0}$.*

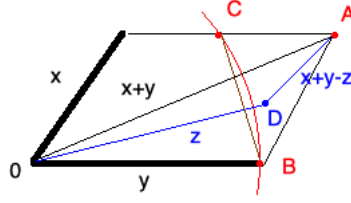


FIGURE 1. Proof of Lemma 4.1: Parallelogram P spanned by \mathbf{x}, \mathbf{y} with a vector \mathbf{z} in it. The red arc is the boundary of $\mathbb{B}_n(\lambda_2^+)$ intersecting P .

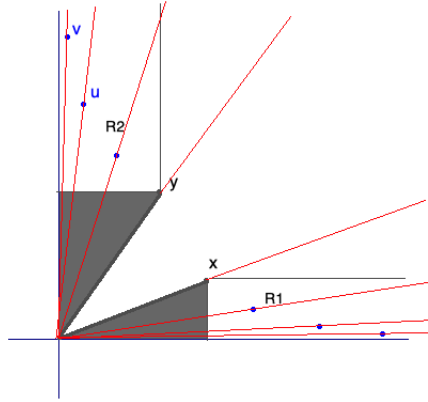


FIGURE 2. Distribution of indecomposables: \mathbf{x}, \mathbf{y} and the blue dots. Red lines indicate consecutive indecomposable cones, the union of all of which covers $\mathbb{R}_{\geq 0}^2$.

Proof. The statement follows immediately upon combining Lemmas 4.1 and 2.4. \square

Let us write $\mathbf{x} = (x_1, x_2)$ and $\mathbf{y} = (y_1, y_2)$, and assume without loss of generality that $x_1 > y_1$. Then we must have $x_2 \leq y_2$, since otherwise \mathbf{x} would be decomposable by Lemma 2.1. Define the regions

$$(6) \quad \mathcal{R}_1 = \{\mathbf{z} \in \mathbb{R}^2 : z_1 > x_1, z_2 < x_2\}, \quad \mathcal{R}_2 = \{\mathbf{z} \in \mathbb{R}^2 : z_1 < y_1, z_2 > y_2\}.$$

Then all the indecomposables are contained in these two regions (see Figure 2). Let us say that indecomposables \mathbf{u} and \mathbf{v} are *consecutive* if the cone $C(\mathbf{u}, \mathbf{v})$ contains no other indecomposables; for instance, \mathbf{u} and \mathbf{v} in \mathcal{R}_2 in Figure 2 are consecutive.

Lemma 4.3. *Let \mathbf{u} and \mathbf{v} be consecutive indecomposables. Then they form a basis for L .*

Proof. Our proof is illustrated by Figure 3. If the consecutive indecomposables are \mathbf{x}, \mathbf{y} , then the result follows from Lemma 4.1. Otherwise, without loss of generality, assume that $\mathbf{u}, \mathbf{v} \in \mathcal{R}_2$, $u_2 < v_2$, and let P be the parallelogram spanned by \mathbf{u} and \mathbf{v} (the argument is completely analogous if $\mathbf{u}, \mathbf{v} \in \mathcal{R}_1$). We will prove that P contains no point of the lattice L in its interior. Suppose it does, call this point \mathbf{z} .

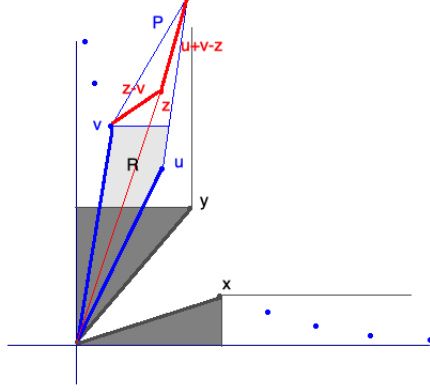


FIGURE 3. Proof of Lemma 4.3.

Then z is decomposable, since otherwise u and v would not be consecutive. Define the region

$$R = \{\mathbf{w} \in P : w_2 \leq v_2\},$$

and suppose that $z \in R$. Notice that we must have $z_2 > u_2$, since otherwise we would have $z < u$ contradicting the fact that u is indecomposable (Lemma 2.1). Then we have $z \in P$ with

$$z_1 < u_1, u_2 < z_2 \leq v_2.$$

Since z is decomposable, it must be a positive integer linear combination of some finite collection of indecomposables (Lemma 2.5). In particular, there must exist some indecomposable element t such that $t < z$. If $t_2 < u_2$, then $t < u$, again contradicting the fact that u is indecomposable (Lemma 2.1); by the same reasoning, we must have $t_1 > v_1$, since otherwise $t < v$, contradicting the fact that v is indecomposable. But then we must have

$$v_1 < t_1 < z_1 < u_1, u_2 < t_2 < z_2 < v_2,$$

and so $t \in P$, which contradicts the fact that u and v are consecutive indecomposables. Hence, $z \notin R$, so suppose $z \in P \setminus R$. Then we have

$$v < z < v + u,$$

and so $z - v, v + u - z \in L^+$. On the other hand, $u = (z - v) + (v + u - z)$, which contradicts the fact that u is indecomposable. Thus, we proved that P contains no point of the lattice L in its interior, and so u, v is a basis for L by Lemma 3.1. \square

Next, we want to prove that $\mathbb{R}_{\geq 0}^2$ is covered by the union of indecomposable cones. Without loss of generality, let us focus on consecutive indecomposables in the region \mathcal{R}_2 , as defined in (6) and illustrated in Figure 2 (the situation with those in \mathcal{R}_1 is completely analogous). Let us order indecomposables in \mathcal{R}_2 as $\mathbf{y} = \mathbf{u}_1, \mathbf{u}_2, \mathbf{u}_3, \dots$ in the order of increasing sup-norm, i.e., $|\mathbf{u}_i| < |\mathbf{u}_{i+1}|$ and $\mathbf{u}_i, \mathbf{u}_{i+1}$ is a consecutive pair of indecomposables for every $i \geq 1$.

Lemma 4.4. *Define $\mathcal{C}(\mathcal{R}_2) = \{a\mathbf{t} : a \geq 0, \mathbf{t} \in \mathcal{R}_2\}$. Then*

$$\mathcal{C}(\mathcal{R}_2) = \bigcup_{i=1}^{\infty} \mathcal{C}(\mathbf{u}_i, \mathbf{u}_{i+1}).$$

Proof. Suppose that \mathcal{R}_2 contains only finitely many indecomposables $\mathbf{u}_1, \dots, \mathbf{u}_m$. This means that the last one \mathbf{u}_m is a scalar multiple of the standard basis vector \mathbf{e}_2 , and so $\mathcal{R}_2 = \bigcup_{i=1}^{m-1} C(\mathbf{u}_i, \mathbf{u}_{i+1})$.

Then, assume that \mathcal{R}_2 contains infinitely many indecomposables. First notice that $u_{i1} > u_{i+1}$ for every $i \geq 1$, by Lemma 2.1. Let us prove that $\lim_{i \rightarrow \infty} u_{i1} = 0$. Suppose not, then there exists some $\varepsilon > 0$ such that $u_{i1} > \varepsilon$ for all $i \geq 1$. This means that the vertical strip

$$S = \{\mathbf{a} \in \mathbb{R}_{\geq 0}^2 : a_1 \leq \varepsilon\}$$

does not contain any indecomposable element, and thus any nonzero point of the lattice L . Hence, if $\alpha x_1 + \beta y_1 \geq 0$ for integers α, β , not both zero, then

$$\alpha x_1 + \beta y_1 > \varepsilon.$$

In particular, $\mathcal{L}_{x_1, y_1}(\alpha, \beta) := \alpha x_1 + \beta y_1 \neq 0$, so x_1, y_1 must be \mathbb{Q} -linearly independent. But then $\mathcal{L}_{x_1, y_1}(\mathbb{Z}^2) \cap [0, 1)$ must be dense in $[0, 1)$ by Kronecker's approximation theorem (see, e.g., [2]). This contradicts the assumption that $S \cap L = \{\mathbf{0}\}$, and so $\lim_{i \rightarrow \infty} u_{i1} = 0$. Additionally, $\lim_{i \rightarrow \infty} u_{i2} = \infty$. Suppose not, then there exists some real number R so that $u_{i2} \leq R$ for all $\mathbf{u}_i \in \mathcal{R}_2$. This implies that $|\mathbf{u}_i| \leq R$ since u_{i1} tends to 0, and hence there can be only finitely many such \mathbf{u}_i since L is discrete.

Now, let $\mathbf{z} \in \mathcal{C}(\mathcal{R}_2)$. There must exist some two consecutive indecomposables $\mathbf{u}_i, \mathbf{u}_{i+1}$ such that

$$\frac{u_{i2}}{u_{i1}} \leq \frac{z_2}{z_1} \leq \frac{u_{(i+1)2}}{u_{(i+1)1}},$$

i.e., the slope of the line through the origin and \mathbf{z} is between the slopes of the lines through the origin and $\mathbf{u}_i, \mathbf{u}_{i+1}$, respectively. Therefore, $\mathbf{z} \in C(\mathbf{u}_i, \mathbf{u}_{i+1})$, and thus $\mathcal{C}(\mathcal{R}_2)$ is covered by the union of consecutive indecomposable cones. \square

Remark 4.1. The same argument as in the proof of Lemma 4.4 applies to the region \mathcal{R}_1 . Hence, $\mathbb{R}_{\geq 0}^2 = \mathcal{C}(\mathcal{R}_1) \cup C(\mathbf{x}, \mathbf{y}) \cup \mathcal{C}(R_2)$ is covered by the union of all the consecutive indecomposable cones.

We are now ready for the main result of this section.

Proof of Theorem 1.2. Since $\mathbb{R}_{\geq 0}^2$ is covered by the union of consecutive indecomposable cones (Remark 4.1), there must exist some consecutive indecomposables \mathbf{u}', \mathbf{v}' such that $\mathbf{z} \in C(\mathbf{u}', \mathbf{v}')$. First, assume that \mathbf{z} lies on the boundary of this cone, then it is a multiple of either \mathbf{u}' or \mathbf{v}' , say, $\mathbf{z} = a\mathbf{u}'$. Then $a \geq 2$ is an integer since \mathbf{z} is decomposable. In this case, choose $\mathbf{u} = \mathbf{v} = \mathbf{u}'$ and take $\alpha = a - 1 > 0$, $\beta = 1$, so

$$\mathbf{z} = \alpha\mathbf{u} + \beta\mathbf{v}.$$

Next, suppose that \mathbf{z} is in the interior of this cone. Then take $\mathbf{u} = \mathbf{u}', \mathbf{v} = \mathbf{v}'$. Since \mathbf{u}, \mathbf{v} form a basis for L (Lemma 4.3), there must exist positive integers α, β such that $\mathbf{z} = \alpha\mathbf{u} + \beta\mathbf{v}$, by Lemma 2.4. In either of these two cases, $\mathbf{z}, \mathbf{u}, \mathbf{v} > \mathbf{0}$ and $\alpha, \beta > 0$, hence we have $|\mathbf{u}| + |\mathbf{v}| = |\mathbf{u} + \mathbf{v}| \leq |\mathbf{z}|$. \square

Remark 4.2. After producing our proof of the above theorem, we became aware of the nice work of Hejda and Kala [6]. Theorem 2 of that paper provides a similar result to our Theorem 1.2 for indecomposables in the ring of integers of a real quadratic number field, whereas our theorem applies to any planar lattice.

We finish this section by considering differences between pairs of consecutive indecomposables. Given a consecutive pair of indecomposables \mathbf{u}, \mathbf{v} , we define their difference vector $\mathbf{d}(\mathbf{u}, \mathbf{v}) = \mathbf{v} - \mathbf{u}$. We first prove that all such difference vectors are distinct.

Lemma 4.5. *Let \mathbf{u}, \mathbf{v} and \mathbf{t}, \mathbf{w} be two different pairs of consecutive indecomposables. Then $\mathbf{d}(\mathbf{u}, \mathbf{v})$ and $\mathbf{d}(\mathbf{t}, \mathbf{w})$ are linearly independent, i.e., $\mathbf{d}(\mathbf{u}, \mathbf{v}) \neq \alpha \mathbf{d}(\mathbf{t}, \mathbf{w})$ for any $\alpha \in \mathbb{R}$.*

Proof. Let λ_1^+, λ_2^+ be positive successive minima for L , as above, and let $\mathbf{x} = (x_1, x_2), \mathbf{y} = (y_1, y_2) \in L^+$ be vectors corresponding to these positive successive minima. Since \mathbf{x}, \mathbf{y} form a basis for L (Lemma 4.1), we can write

$$\mathbf{u} = a_1 \mathbf{x} + a_2 \mathbf{y}, \mathbf{v} = b_1 \mathbf{x} + b_2 \mathbf{y}, \mathbf{t} = c_1 \mathbf{x} + c_2 \mathbf{y}, \mathbf{w} = f_1 \mathbf{x} + f_2 \mathbf{y},$$

for some integers $a_1, a_2, b_1, b_2, c_1, c_2, f_1, f_2$. Suppose that $\mathbf{d}(\mathbf{u}, \mathbf{v}) = \alpha \mathbf{d}(\mathbf{t}, \mathbf{w})$ for some $\alpha \in \mathbb{R}$, then

$$(7) \quad (b_1 - a_1) \mathbf{x} + (b_2 - a_2) \mathbf{y} = \alpha (f_1 - c_1) \mathbf{x} + \alpha (f_2 - c_2) \mathbf{y}.$$

None of the difference coefficients in (7) can be equal to 0, since different indecomposables must have different coordinates. Thus, (7) is a nontrivial linear dependence relation for the vectors \mathbf{x}, \mathbf{y} , a contradiction. \square

We also briefly consider the distribution of these difference vectors.

Lemma 4.6. *Assume the lattice L is not PVR. Let us write $|\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})|$ and $\min \mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})$ for the maximum and minimum absolute value of coordinates of the difference vector $\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})$, respectively. Then*

$$\limsup_{i \rightarrow \infty} |\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})| = \infty, \quad \liminf_{i \rightarrow \infty} \min \mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1}) = 0.$$

Proof. Since L is not PVR, at least one of the regions \mathcal{R}_1 and \mathcal{R}_2 must contain infinitely many indecomposables; without loss of generality, assume it is \mathcal{R}_2 . Let us write d_{i1}, d_{i2} for the coordinates of the difference vector $\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})$, then $|d_{i1}| = \min \mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})$ and $d_{i2} = |\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})|$, since $\mathbf{u}_i, \mathbf{u}_{i+1} \in \mathcal{R}_2$. In particular, $y_1 > |d_{i1}|$ for every $i \geq 1$. Suppose that $\liminf_{i \rightarrow \infty} \min \mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1}) \neq 0$, then there exists some $\varepsilon > 0$ such that $|d_{i1}| > \varepsilon$ for all $i \geq 1$. This means that $u_{i1} < y_1 - \varepsilon(i-1) < 0$ for sufficiently large i . This contradicts \mathbf{u}_i being in L^+ .

On the other hand, suppose that $\limsup_{i \rightarrow \infty} |\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})| \neq \infty$, i.e., there exists some real number $T > 0$ such that $d_{i2} \leq T$. Since all of the difference vectors are distinct by Lemma 4.5, this implies that there are infinitely vectors of L satisfying $|\mathbf{d}(\mathbf{u}_i, \mathbf{u}_{i+1})| \leq T$. This contradicts discreteness of L . \square

5. COUNTING INDECOMPOSABLES FROM REAL QUADRATIC NUMBER FIELDS

The convex hull of indecomposables in L^+ for a planar lattice L forms a Klein polygon approximating the coordinate axes as close as possible by positive points of the given lattice. This suggests that the number of indecomposables of bounded sup-norm in L grows logarithmically as this bound tends to infinity. We aim to produce a precise version of this observation for lattices coming from the rings of integers of real quadratic fields.

The main goal of this section is to prove Theorem 1.3. Let K be a real quadratic field with ring of integers \mathcal{O}_K and discriminant Δ_K . Let $J \subseteq K$ be a fractional

ideal, then there exists an ideal $I \subset \mathcal{O}_K$ and an element $c \in K$ such that $J = cI$. Let $L = \Sigma_K(J)$ and observe that for any $\mathbf{0} \neq \mathbf{z} = (z_1, z_2) \in L$, $z_1, z_2 \neq 0$. Hence, L contains infinitely many indecomposables in both regions \mathcal{R}_1 and \mathcal{R}_2 , defined as in (6). The norm of J is then given by

$$\mathbb{N}_K(J) = |c| \mathbb{N}_K(I) = |c| |\mathcal{O}_K : I|.$$

and the determinant of the lattice L is

$$(8) \quad \det(L) = \mathbb{N}_K(J) \sqrt{|\Delta_K|}.$$

The following lemma is an adaptation of Theorem 5 of [8] along with its proof.

Lemma 5.1. *Let $L = \Sigma_K(J)$ be as above. Let $\mathbf{u} = (u_1, u_2) \in L^+$ be an indecomposable element. Then*

$$u_1 u_2 \leq (\det L)^2.$$

Proof. Suppose that $u_1 u_2 > (\det L)^2$, then there exists $\varepsilon > 0$ small enough so that

$$(\sqrt{u_1} - \varepsilon)(\sqrt{u_2} - \varepsilon) > \det L.$$

Define a box

$$B_\varepsilon = \{\mathbf{x} \in \mathbb{R}^2 : |x_i| \leq \sqrt{u_i} - \varepsilon, i = 1, 2\},$$

then $\text{Vol}_2(B_\varepsilon) = 2^2(\sqrt{u_1} - \varepsilon)(\sqrt{u_2} - \varepsilon) > 2^2 \det L$. Hence, Minkowski Convex Body Theorem (see, e.g., [5]) guarantees that there exists a nonzero point $\mathbf{y} \in B_\varepsilon \cap L$. This means that $\mathbf{y} = (\sigma_1(\beta), \sigma_2(\beta))$ for some $0 \neq \beta \in J$, so $\beta^2 \in J$. Then

$$\mathbf{z} = (z_1, z_2) = (\sigma_1(\beta)^2, \sigma_2(\beta)^2) = \Sigma_K(\beta^2) \in L^+,$$

and $z_1 < u_1, z_2 < u_2$. Then Lemma 2.1 implies that \mathbf{u} is not indecomposable. This completes the proof. \square

Define the region

$$R_L = \{\mathbf{x} \in \mathbb{R}_{\geq 0}^2 : x_1 x_2 \leq (\det L)^2\},$$

then, by Lemma 5.1, all the indecomposable elements of L lie in R_L . For any $T \geq 0$, define $R_L(T) = \{\mathbf{x} \in R_L : |\mathbf{x}| \leq T\}$. Then

$$(9) \quad \text{Area}(R_L(T)) = (\det(L))^2 + \int_{1/T}^T \frac{(\det(L))^2}{x} dx = (\det(L))^2 (2 \log T + 1).$$

Suppose that $R_L(T)$ contains n indecomposables $\mathbf{u}_1, \dots, \mathbf{u}_n$, written in the order of decreasing first coordinate. Then for each $1 \leq i \leq n-1$, $\mathbf{u}_i, \mathbf{u}_{i+1}$ is a consecutive pair of indecomposables, hence, a basis for L . Let $\mathbf{u}'_i, \mathbf{u}'_{i+1}$ be the intersection points of the lines $t\mathbf{u}_i, t\mathbf{u}_{i+1}$, respectively, with the curve $y = \frac{(\det(L))^2}{x}$. Let S_i, S'_i be the triangles, which are the convex hulls of $\mathbf{0}, \mathbf{u}_i, \mathbf{u}_{i+1}$ and $\mathbf{u}'_i, \mathbf{u}'_{i+1}$, respectively, so $S_i \subseteq S'_i$. Then

$$(10) \quad \text{Area}(S'_i) \geq \text{Area}(S_i) = \frac{\det(L)}{2},$$

since consecutive indecomposables $\mathbf{u}_i, \mathbf{u}_{i+1}$ form a basis for L (Lemma 4.3), and hence, the parallelogram spanned by $\mathbf{u}_i, \mathbf{u}_{i+1}$ is a fundamental domain for L . Write also C_i for the intersection of the cone $C(\mathbf{u}'_i, \mathbf{u}'_{i+1})$ with $R_L(T)$, then $C_i \subset S'_i$. In our next lemma, we estimate the area of the region $S_i \setminus C_i$, an example of which is colored yellow in Figure 4.

Lemma 5.2. *Let us write D for $\det(L)$. Then*

$$\text{Area}(S_i \setminus C_i) \leq \frac{D}{2} - D^2 \log \left(\frac{1 + \sqrt{4D^2 + 1}}{2D} \right).$$

Proof. First notice that $A_i := \text{Area}(S_i \setminus C_i)$ is maximized when $S_i = S'_i$, i.e., when the indecomposables $\mathbf{u}_i, \mathbf{u}_{i+1}$ lie on the hyperbola $x_2 = D^2/x_1$. From here on, assume this is the case. Let $\mathbf{u}_i = (u_{i1}, u_{i2})$, $\mathbf{u}_{i+1} = (u_{(i+1)1}, u_{(i+1)2})$, then

$$(11) \quad u_{i1}u_{i2} = u_{(i+1)1}u_{(i+1)2} = D^2,$$

and

$$(12) \quad D = \left| \det \begin{pmatrix} u_{i1} & u_{(i+1)1} \\ u_{i2} & u_{(i+1)2} \end{pmatrix} \right| = |u_{i1}u_{(i+1)2} - u_{(i+1)1}u_{i2}|.$$

Notice that A_i is the area of the region between the hyperbola $x_2 = D^2/x_1$ and the cord connecting the points $\mathbf{u}_i, \mathbf{u}_{i+1}$. Setting up the integral and using condition (11), we find that

$$(13) \quad A_i = D^2 \left(\frac{u_{i1}^2 - u_{(i+1)1}^2}{2u_{i1}u_{(i+1)1}} - \log \left(\frac{u_{i1}}{u_{(i+1)1}} \right) \right).$$

Let us write $R = u_{i1}/u_{(i+1)1}$, then $R > 1$. Substituting $u_{i2} = D^2/u_{i1}$ and $u_{(i+1)2} = D^2/u_{(i+1)1}$ from (11) into (12), we obtain

$$R - 1/R = 1/D,$$

since $R > 1/R$. Solving this equation for R , we obtain $R = \frac{1 + \sqrt{4D^2 + 1}}{2D}$. Now, substitute it in for $u_{i1}/u_{(i+1)1}$ into (13) to obtain

$$A_i = D^2 \left(\frac{R}{2} - \frac{1}{2R} - \log R \right) = D^2 \left(\frac{1}{2D} - \log \left(\frac{1 + \sqrt{4D^2 + 1}}{2D} \right) \right).$$

□

Proof of Theorem 1.3. Notice that

$$(14) \quad \sum_{i=1}^{n-1} \text{Area}(C_i) \leq \text{Area}(R_L(T)),$$

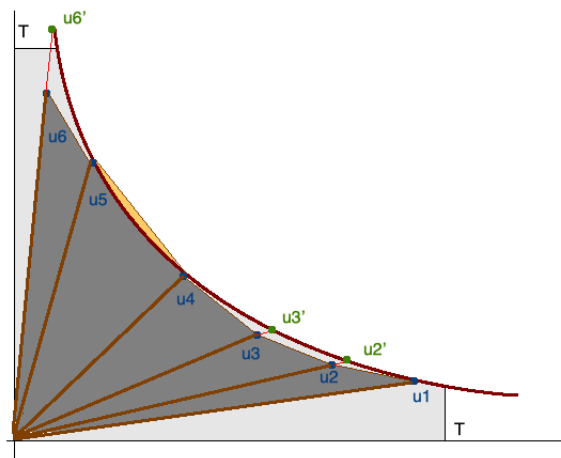
where

$$\text{Area}(C_i) = \text{Area}(S_i) - \text{Area}(S_i \setminus C_i) \geq D^2 \log \left(\frac{1 + \sqrt{4D^2 + 1}}{2D} \right),$$

by combining (10) with Lemma 5.2. Now, combining this last observation with (14) and (9), we obtain

$$n \leq \left(\log \left(\frac{1 + \sqrt{4D^2 + 1}}{2D} \right) \right)^{-1} (2 \log T + 1) + 1.$$

□

FIGURE 4. Region $R_L(T)$ with indecomposables in it.

REFERENCES

- [1] W. Bruns, J. Guberladze, M. Henk, A. Martin and R. Weismantel. A counterexample to an integer analogue of Carathéodory's theorem. *J. Reine Angew. Math.*, 510:179–185, 1999.
- [2] J. W. S. Cassels. *An introduction to Diophantine approximations*. Cambridge Univ. Press, 1957.
- [3] L. Fukshansky and S. Wang. Positive semigroups in lattices and totally real number fields. *Adv. Geom.*, 22(4):503–512, 2022.
- [4] L. Fukshansky, P. Guerzhoy and S. Kühnlein. On sparse geometry of numbers. *Res. Math. Sci.*, 8(1), Paper No. 2, 18 pp., 2021.
- [5] P. M. Gruber and C.G. Lekkerkerker. *Geometry of numbers*, Second edition. North-Holland Mathematical Library, 37. North-Holland Publishing Co., Amsterdam, 1987.
- [6] T. Hejda and V. Kala. Additive structure of totally positive quadratic integers. *Manuscripta Math.*, 163(1-2):263–278, 2020.
- [7] V. Kala. Universal quadratic forms and indecomposables in number fields: a survey. *Commun. Math.*, 31(2):81–114, 2023.
- [8] V. Kala and P. Yatsyna. On Kitaoka's conjecture and lifting problem for universal quadratic forms. *Bull. Lond. Math. Soc.*, 55:854–864, 2023.
- [9] S. Kühnlein. Well-rounded sublattices. *Int. J. Number Theory*, 8(5):1133–1144, 2012.

DEPARTMENT OF MATHEMATICS, 850 COLUMBIA AVENUE, CLAREMONT MCKENNA COLLEGE,
CLAREMONT, CA 91711

Email address: lenny@cmc.edu

DEPARTMENT OF MATHEMATICS, POMONA COLLEGE, 610 N. COLLEGE AVE, CLAREMONT, CA
91711, USA

Email address: tkxc2022@mymail.pomona.edu