Introduction to Minkowski's Conjecture

Ofir David

1 Motivation

We begin with probably one of the most well known theorems in mathematics.

Theorem 1.1. *The ring $\mathbb{Z}$ is Euclidean : For any $a, b \in \mathbb{Z}$ with $b \neq 0$, there are $q, r \in \mathbb{Z}$ such that $a = bq + r$ and $|r| < |b|$.*

Proof. The standard proof usually uses some induction argument. We shall use a more geometric approach.

Let $a, b \in \mathbb{Z}$ with $b \neq 0$. If $\frac{a}{b} \in \mathbb{Q}$ is actually in $\mathbb{Z}$, then we are done by taking $q = \frac{a}{b}$ and $r = 0$. Otherwise let $q \in \mathbb{Z}$ be the closest integer to $\frac{a}{b}$, so in particular we have that $\left|q - \frac{a}{b}\right| \leq \frac{1}{2}$. Letting $r = a - bq$ we obtain that

$$|r| = |a - bq| = |b| \left|\frac{a}{b} - q\right| = |b| \, |\tilde{q} - q| \leq |b| \, \frac{1}{2} < |b| \, ,$$

and we are done. □

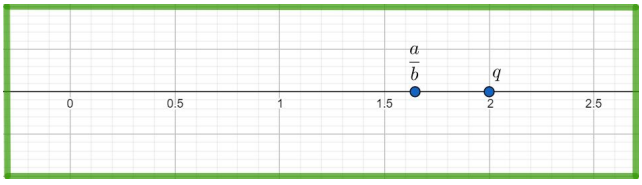

Figure 1.1: Every point $\tilde{q} \in \mathbb{Q}$ has a point $q \in \mathbb{Z}$ with $|q - \tilde{q}| \leq \frac{1}{2}$

The only properties that we needed in the proof are:

1. Multiplicative: The norm $|\cdot| : \mathbb{R} \to \mathbb{R}_{\geq 0}$ is multiplicative.
2. Discrete: The image of the norm on $\mathbb{Z}$ is in $\mathbb{Z}_{\geq 0}$.
3. Small covering radius: For any $\tilde{q} \in \mathbb{Q}$ (and even in $\mathbb{R} = \overline{\mathbb{Q}}$) there exists $q \in \mathbb{Z}$ such that $|q - \tilde{q}| < 1$.

We can now generalize this to other integer rings. For example, for rings inside $\mathbb{C}$ we can use the multiplicative norm $N(a+bi) = (a+bi)(a-bi) = a^2+b^2$. If we started with quadratic rings, then this is the algebraic norm, hence has integral values, so we only need to check the covering radius:

- $\mathbb{Z}[i]$ is Euclidean with covering radius is $\frac{1}{2}$.
- $\mathbb{Z}\left[\sqrt{2}i\right]$ is Euclidean with covering radius is $\frac{3}{4}$.
- $\mathbb{Z}\left[\sqrt{3}i\right]$ is <u>not</u> Euclidean with the norm $N\left(a+b\sqrt{3}i\right) = a^2+3b^2$. The distance of the third root of unity ω from $\mathbb{Z}\left[\sqrt{3}i\right]$ is exactly 1.
- $\mathbb{Z}[\omega] = \mathbb{Z}\left[\sqrt{3}i, \omega\right]$ (added the problematic point) is Euclidean with the norm $N(a+b\omega) = (a+b\omega)(a+b\bar{\omega}) = a^2-ab+b^2$ with covering radius $\frac{1}{\sqrt{3}} < 1$.

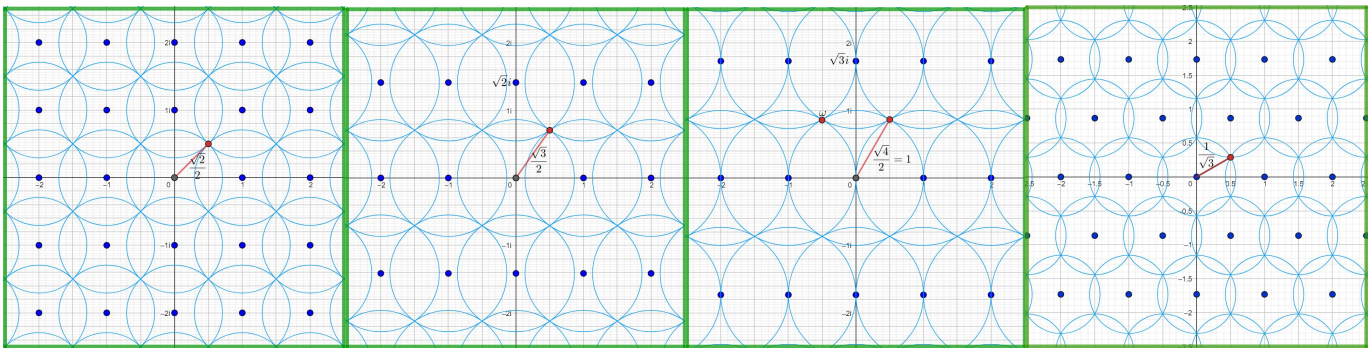

Figure 1.2: From left to right we have $\mathbb{Z}[i]$, $\mathbb{Z}\left[\sqrt{2}i\right]$, $\mathbb{Z}\left[\sqrt{3}i\right]$ and $\mathbb{Z}[\omega]$.

Remark 1.2. If the covolume of the lattice is too big, then the covering radius > 1 and then the Euclidean distance is not a Euclidean norm.

1.1 Totally real fields

In the last examples we had a ring $\mathcal{O}$ inside a complex quadratic field $\mathbb{K}$, namely $\mathbb{K} = \mathbb{Q}\left(\sqrt{-d}\right)$ for some $d > 1$ square free, which is then embedded as a lattice inside $\mathbb{C}$. What happens if this is not the case?

Let us consider the ring $\mathbb{Z}\left[\sqrt{2}\right] \hookrightarrow \mathbb{Q}\left(\sqrt{2}\right)$. We can think of it as embedded in $\mathbb{Q}\left(\sqrt{2}\right) \leq \mathbb{R}$ with the usual absolute value norm on $\mathbb{R}$ which is still multiplicative. Since $\mathbb{Z}\left[\sqrt{2}\right]$ is dense in $\mathbb{R}$, the covering radius is zero, however it also means that the image of the norm is not in $\mathbb{Z}$ (or even discrete). In order to fix this we add another dimension and consider the following embedding:

$$\begin{aligned}\varphi &: \mathbb{Q}\left(\sqrt{2}\right) \to \mathbb{R}\times\mathbb{R}\\ \varphi\left(a+b\sqrt{2}\right) &= \left(a+b\sqrt{2}, a-b\sqrt{2}\right) = \left(a+b\sqrt{2}, \sigma\left(a+b\sqrt{2}\right)\right)\end{aligned}$$

where σ is the nontrivial Galois conjugation on $\mathbb{Q}\left(\sqrt{2}\right)$. It is well known that under this embedding $\varphi\left(\mathbb{Z}\left[\sqrt{2}\right]\right)$ is a lattice in $\mathbb{R}^2$.

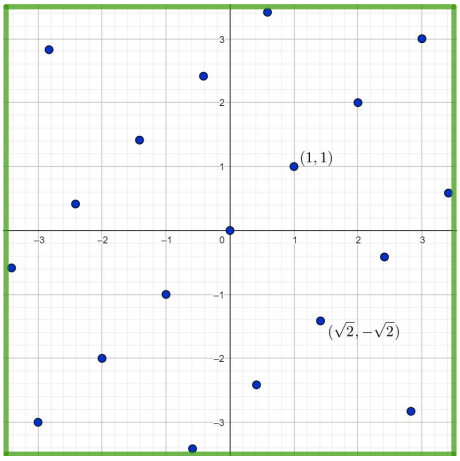

Figure 1.3: The lattice for $\mathbb{Z}\left[\sqrt{2}\right]$.

Considering $\mathbb{R}\times\mathbb{R}$ as a ring with pointwise multiplication, we see that φ is a ring homomorphism. It is now easy to check that the standard Euclidean distance on $\mathbb{R}^2$ will not define a multiplicative norm on $\mathbb{Z}\left[\sqrt{2}\right]$, so instead we will use the multiplicative norm

$$N : \mathbb{R}\times\mathbb{R} \to \mathbb{R}_{\geq 0}$$
$$N(x,y) = |xy|.$$

Note that for $a+b\sqrt{2} \in \mathbb{Z}\left[\sqrt{2}\right]$ the norm is just $N\left(\varphi\left(a+b\sqrt{2}\right)\right) = \left|\left(a+b\sqrt{2}\right)\sigma\left(a+b\sqrt{2}\right)\right| = \left|a^2-2b^2\right|$ which is the algebraic norm (in absolute value), and in particular it has integer values.

To sum up, the norm $N : \mathbb{Z}\left[\sqrt{2}\right] \to \mathbb{R}_{\geq 0}$ is multiplicative with values in the integers, and we are left asking whether it has *multiplicative* covering radius < 1. This means that $\mathbb{R}^2$ is covered by normalized hyperbolas centered on the lattice points as in the image below:

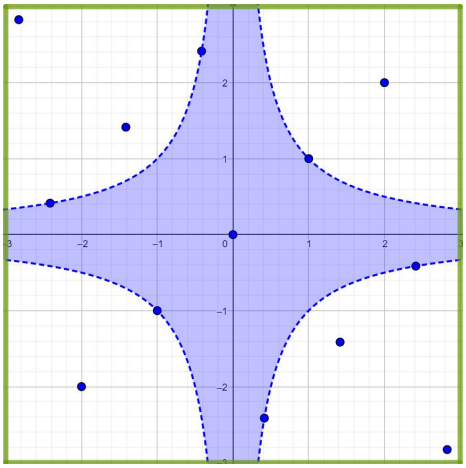

Figure 1.4: The "Multiplicative" ball around the origin in the lattice for $\mathbb{Z}\left[\sqrt{2}\right]$.

Generalizing this phenomenon, we begin with the definition of multiplicative covering radius.

Definition 1.3. Define the multiplicative norm $N:\mathbb{R}^n\to\mathbb{R}_{\geq 0}$ by $N(x_1,...,x_n)=\prod|x_i|$. For a set $\Omega\subseteq\mathbb{R}^n$, we write $L(\Omega)=\inf_{\omega\in\Omega}N(\Omega)$.

For a lattice $L\leq\mathbb{R}^n$ we define the norm cover to be $Ncov(L)=\sup_{v\in\mathbb{R}^n}N(v-L)$.

In other words, if $B^{(N)}(r)=\{\bar{x}\in\mathbb{R}^n \mid N(\bar{x})<r\}$ is the multiplicative "ball" of radius r, then $\mathbb{R}^n$ is covered by the translations of the closure $\overline{B^{(N)}(Ncov(L))}$ centered around the lattice points in L, namely $\mathbb{R}^n=L+\overline{B^{(N)}(Ncov(L))}$.

Next we generalize the lattice construction to other totally real field extensions.

Definition 1.4. Let $\mathbb{K}/\mathbb{Q}$ be a totally real field and let $\sigma_1,...,\sigma_n:\mathbb{K}\to\mathbb{R}$ be its distinct n real embeddings. Define $\varphi_{\mathbb{K}}:\mathbb{K}\to\mathbb{R}^n$ to be the map $\varphi_{\mathbb{K}}(\alpha)=(\sigma_1(\alpha),...,\sigma_n(\alpha))$, and denote by $Ncov(\mathbb{K}):=Ncov(\varphi_{\mathbb{K}}(\mathcal{O}_{\mathbb{K}}))$.

Note that $\mathbb{K}\overset{\varphi_{\mathbb{K}}}{\to}\mathbb{R}^n\overset{N}{\to}\mathbb{R}_{\geq 0}$ is just the standard algebraic norm $|Norm(\alpha)|=|\prod\sigma_i(\alpha)|$ (in absolute value), so in particular it is multiplicative, and for $\alpha\in\mathcal{O}_{\mathbb{K}}$ we have that $Norm(\alpha)\in\mathbb{Z}$. These are two of the conditions that we need to show that $\mathcal{O}_{\mathbb{K}}$ is Euclidean. The last condition is $N(\alpha-\mathcal{O}_{\mathbb{K}})<1$ for all $\alpha\in\mathbb{K}$, or in the lattice notation $N(v-L)<1$ for all $v\in\mathbb{Q}L$. Thus we obtain the following:

Corollary 1.5. *The ring $\mathcal{O}_{\mathbb{K}}$ is Norm-Euclidean (i.e. Euclidean with the norm N as above) if $Ncov(\mathbb{K})<1$.*

Remark 1.6. In the corollary above we don't have the "only if" part since $Ncov(\mathbb{K})$ consider the supremum over all points in $\mathbb{R}^n$ while in general we need only the points coming from $\mathbb{K}$. In Corollary 1 and 2 in [3], it is shown that if $Ncov(\mathbb{K})>1$, then there exists $\alpha\in\mathbb{K}$ such that $N(\alpha-\mathcal{O}_{\mathbb{K}})>1$, hence $\mathcal{O}_{\mathbb{K}}$ is not Norm-Euclidean. In addition, if $Ncov(\mathbb{K})=1$ and $[\mathbb{K}:\mathbb{Q}]\geq 3$ then similarly $\mathcal{O}_{\mathbb{K}}$ is not Norm-Euclidean.

Remark 1.7. An integer ring can be Euclidean but not Norm-Euclidean, for example the integer ring of $\mathbb{Q}(\sqrt{69})$ (see [4]???).

Remark 1.8. The only quadratic Norm-Euclidean fields are $\mathbb{Q}(\sqrt{m})$ where

$$m\in\{-11,-7,-3,-2,-1,2,3,5,6,7,11,13,17,19,21,29,33,37,41,57,73\}.$$

Returning to the examples that we had in the previous section, while $\mathbb{Z}[\sqrt{-1}]$ and $\mathbb{Z}[\sqrt{-2}]$ are norm-Euclidean (for the complex norm), $\mathbb{Z}[\sqrt{-3}]$ is not norm-Euclidean and the "reason" is that the covolume became too large and therefore the covering radius became too large. In general, if we fix the dimension d and some $M>0$, then there are only finitely many fields such that the corresponding lattice has covolume $<M$ (the covolume is exactly the square root of the discriminant of the field). Thus, we do not expect too many of them to have small multiplicative covering radius (and hence norm-Euclidean). While this direction will probably fail, we can still ask whether after normalization, the resulting lattice does have small multiplicative covering radius, and this question leads to Minkowski's conjecture.

2 The conjecture and first examples

Conjecture 2.1. *(Minkowski) For any lattice $L \leq \mathbb{R}^n$ we have that $Ncov(L) \leq \frac{covol(L)}{2^n}$.*

Remark 2.2. For lattices coming from field extension as in the previous section, the conjecture implies that $Ncov(\mathbb{K}) \leq \frac{\sqrt{D_{\mathbb{K}}}}{2^n}$ where $D_{\mathbb{K}}$ is the discriminant. In particular for $\mathbb{K} = \mathbb{Q}(\sqrt{2})$, the discriminant is 8 so the conjecture (which is a theorem in dimension 2) implies that $Ncov(\mathbb{Q}(\sqrt{2})) \leq \frac{\sqrt{8}}{4} < 1$, so that $\mathbb{Z}[\sqrt{2}]$ is Euclidean.

Remark 2.3. The conjecture actually asks to show that $Ncov(L) = \frac{covol(L)}{2^n}$ iff $L = \mathbb{Z}^n$ (up to normalization and a diagonal flow). We will ignore this condition and denote by MINK the conjecture stated above for unimodular lattices, namely $Ncov(L) \leq \frac{1}{2^n}$.

The first step to attack this conjecture is to notice the following. Let $L \leq \mathbb{R}^n$ be a lattice and consider the function $v \mapsto N(v - L)$. This function is invariant under translation by L, so in order to find its supremum, namely $Ncov(L) = \sup N(v - L)$, it is enough to consider the supremum only on a fundamental domain. More generally, a lattice L satisfies MINK if and only if it has a fundamental domain inside the multiplicative ball $\overline{B^{(N)}\left(\frac{1}{2^n}\right)} = \left\{\bar{x} \in \mathbb{R}^n \mid N(\bar{x}) = N(\bar{x} - \bar{0}) \leq \frac{1}{2^n}\right\}$.

Example 2.4. The simplest example of a lattice is $\mathbb{Z}^n \leq \mathbb{R}^n$. This lattice has fundamental domain inside $F = \left[-\frac{1}{2}, \frac{1}{2}\right]^n$ and every point in this set satisfies $\prod |x_i| \leq \frac{1}{2^n}$ implying that $Ncov(\mathbb{Z}^n) \leq \frac{1}{2^n}$. Note also that $N\left(\left(\frac{1}{2}, ..., \frac{1}{2}\right) - \mathbb{Z}^n\right) = \frac{1}{2^n}$, hence $Ncov(\mathbb{Z}^n) = \frac{1}{2^n}$.

Interestingly, between $F = \left[-\frac{1}{2}, \frac{1}{2}\right]^n$ and $\overline{B^{(N)}\left(\frac{1}{2^n}\right)}$ we have the closed Euclidean ball $\overline{B^{(E)}\left(\frac{\sqrt{n}}{2}\right)} = \left\{\bar{x} \in \mathbb{R}^n \mid \|\bar{x}\|_2 \leq \frac{\sqrt{n}}{2}\right\}$. Clearly $F \subseteq \overline{B^{(E)}\left(\frac{\sqrt{n}}{2}\right)}$, and on the other hand, if $(x_1, ..., x_n) \in \overline{B^{(E)}\left(\frac{\sqrt{n}}{2}\right)}$, then using the standard inequality of arithmetic and geometric means we get that

$$\left(\prod |x_i|\right)^{1/n} = \left(\left(\prod x_i^2\right)^{1/n}\right)^{1/2} \leq \left(\frac{\sum x_i^2}{n}\right)^{1/2} \leq \frac{1}{2}.$$

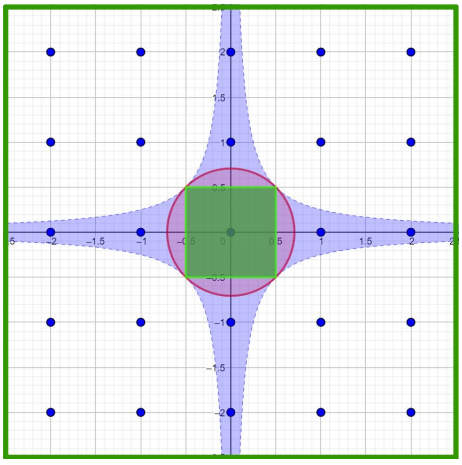

Figure 2.1: A fundamental domain of $\mathbb{Z}^2$ (the green square) is contained inside the ball of radius $\frac{\sqrt{2}}{2}$ (the red ball) which is contained inside the multiplicative ball $|xy| \leq \frac{1}{4}$ (the blue region).

More generally we see that:

Lemma 2.5. *If L has a fundamental domain in $\overline{B^{(E)}\left(\frac{\sqrt{n}}{2}\right)}$, then L satisfies MINK. In other words, covering radius $\leq \frac{\sqrt{n}}{2}$ implies multiplicative covering radius $\leq \frac{1}{2^n}$.*

Example 2.6. Let $U \leq \mathrm{SL}_n(\mathbb{R})$ be the group of upper triangular with 1's on the diagonal and $K = \mathrm{SO}_n(\mathbb{R})$.

- For any $u \in U$ the lattice $L = u\mathbb{Z}^n$ has a fundamental domain in $F = \left[-\frac{1}{2}, \frac{1}{2}\right]^n$, hence as before L satisfies MINK.
- Let $k \in SO_n(\mathbb{R})$. Then $kL = ku\mathbb{Z}^n$ has a fundamental domain in $kF \subseteq \overline{kB^{(E)}\left(\frac{\sqrt{n}}{2}\right)} = \overline{B^{(E)}\left(\frac{\sqrt{n}}{2}\right)}$, hence it satisfies MINK.

What happens if L doesn't have covering radius $\leq \frac{\sqrt{n}}{2}$? For example, think about $L_\varepsilon = span_{\mathbb{Z}}\left\{(\varepsilon, 0), \left(0, \frac{1}{\varepsilon}\right)\right\}$ for $\varepsilon > 0$ very small. In this case L_ε has covering radius $\sim \frac{1}{2\varepsilon}$ which is very big. Fortunately, we are looking for the **multiplicative** covering radius, and not the standard covering radius. In particular, the multiplicative covering radius is invariant under multiplication by elements from the positive diagonal group $A := \{diag\left(e^{t_1}, ..., e^{t_n}\right) \mid \sum t_i = 0\}$. Indeed, this follows from the fact that

$$N\left(diag\left(e^{t_1}, ..., e^{t_n}\right) \cdot (x_1, ..., x_n)\right) = N\left(\left(e^{t_1}x_1, ..., e^{t_n}x_n\right)\right) = \prod |x_i e^{t_i}| = e^{\sum t_i} N(\bar{x}) = N(\bar{x}).$$

The lattice above is just $diag\left(\varepsilon, \frac{1}{\varepsilon}\right)\mathbb{Z}^2$, so it still satisfies MINK.

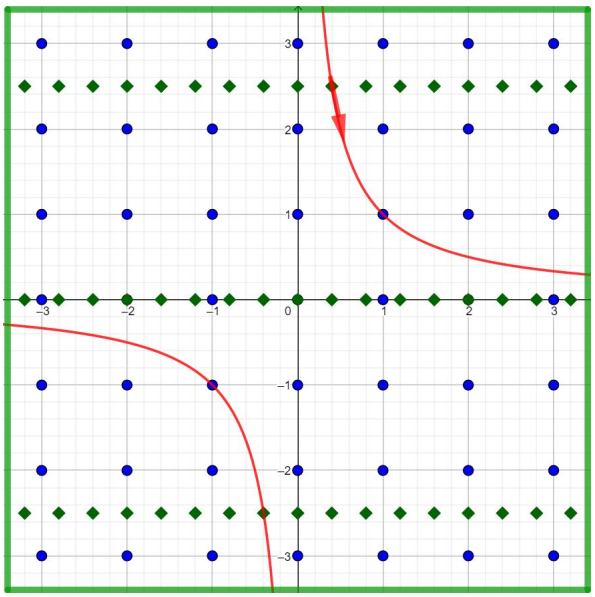

Figure 2.2: The blue points correspond to $\mathbb{Z}^2$ and the green diamonds to $diag\left(\frac{2}{5}, \frac{5}{2}\right)\mathbb{Z}^2$. Flowing along the diagonal group is the same as moving along hyperbolas.

More generally we proved the following:

Lemma 2.7. *For any lattice $L \leq \mathbb{R}^n$ and $a \in A$ we have $Ncov(L) = Ncov(aL)$.*

Definition 2.8. A matrix $g \in \mathrm{SL}_n(\mathbb{R})$ is called DOTU (Diagonal, Orthogonal, Triangular, Unimodular integral) if it is in $A \cdot \mathrm{SO}_n(\mathbb{R}) \cdot U \cdot \mathrm{SL}_n(\mathbb{Z})$.

Corollary 2.9 ([9])**.** *For any DOTU matrix $g \in \mathrm{SL}_n(\mathbb{R})$, the lattice $g\mathbb{Z}^n$ satisfies MINK.*

To sum up the ideas so far, we have the following: Let $x \in X_n$ be a unimodular lattice:

1. Show that Ax contains a "nice" lattice.
2. Show that every "nice" lattice has covering radius $\leq \frac{\sqrt{n}}{2}$.
3. Show that covering radius $\leq \frac{\sqrt{n}}{2}$ implies multiplicative radius $\leq \frac{1}{2^n}$.

We already know that (3) is always true. Up until now "nice" meant a lattice of the form $ku\mathbb{Z}^n$ with $k \in \mathrm{SO}_n(\mathbb{R})$ and $u \in U$. For these types of lattice we know that (2) is true as well, and we are left to check if (1) is true.

Note first that by Iwasawa's decomposition $\mathrm{SL}_n(\mathbb{R}) = AUK$ which would complete the proof if we instead had $\mathrm{SL}_n(\mathbb{R}) = AKU$. In dimension 2 it is true that any lattice has the form $aku\mathbb{Z}^n$. To see this, recall that if we consider 2-dimensional lattices up to $\mathrm{SO}_2(\mathbb{R})$, then we can parametrize them using the fundamental domain of the action of $\mathrm{SL}_2(\mathbb{Z})$ on the hyperbolic plane. Under this presentation, the lattices of the form $ku\mathbb{Z}^2$ correspond to the segment $\left\{x + i \mid |x| \leq \frac{1}{2}\right\}$, and its not hard to check that any geodesic passes through this segment. Thus, every 2-dimensional lattice has the form $aku\mathbb{Z}^2$.

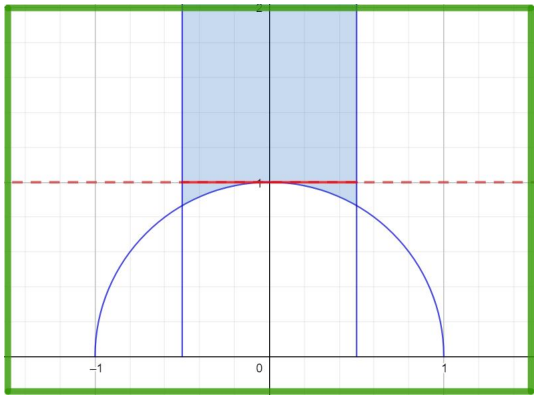

Figure 2.3: The fundamental domain is the blue set ($|x| \leq \frac{1}{2}$, $y \geq 0$ and $x^2 + y^2 \geq 1$). The red segment correspond to lattices of the form $ku\mathbb{Z}^2$.

In general, it is known that in dimension $n = 2, 3$ every matrix in $\mathrm{SL}_n(\mathbb{R})$ is DOTU (see [11, 12]). On the other hand, for n big enough this stops being the case (see 3.7 and also [1], or at least try). Thus we need to look for a better definition for "nice" lattices.

3 The space of unimodular lattice and A-orbits

Before continuing, let us recall some of the definitions for unimodular lattice and their A-orbits.

Recall that the space of unimodular lattices can be parametrized by $X_n := \mathrm{SL}_n(\mathbb{R})/\mathrm{SL}_n(\mathbb{Z})$ under the map $g\mathrm{SL}_n(\mathbb{Z}) \mapsto g\mathbb{Z}^n$. We then have the map $Ncov : X_n \to \mathbb{R}_{\geq 0}$, and Minkowski's conjecture can be formulated by saying that $Ncov$ is bounded from above by $\frac{1}{2^n}$. Moreover, the space X_n has a natural left A-action on it, and we have already seen that $Ncov$ is constant on A-orbits.

Under the topology of X_n inherited from $\mathrm{SL}_n(\mathbb{R})$, two lattices are close if we can write them as $g_1\mathbb{Z}^n, g_2\mathbb{Z}^n$ with $\|g_1 - g_2\|_\infty$ small, namely we can find bases for the two lattices which are close to each other. While the map $Ncov : X_n \to \mathbb{R}_{\geq 0}$ is not continuous, it is upper semicontinuous, so in particular if $x_i \to x_\infty$, then $\lim_{i\to\infty} Ncov(x_i) \leq Ncov(x)$.

Lemma 3.1. *The map $Ncov : X_n \to \mathbb{R}$ is upper semicontinuous.*

Proof. Recall that for a lattice $L \leq \mathbb{R}^n$ we have that $L + \overline{B^{(N)}(r)} = \mathbb{R}^n$ iff $r \geq Ncov(L)$, and further $L + B^{(N)}(r) = \mathbb{R}^n$ if $r > Ncov(L)$. Fix some $x \in X_n$ and let $R > 0$ be the covering radius of x and $r = Ncov(x)$. Since $\overline{B^{(E)}(2R)}$ is a compact, for any $1 > \varepsilon > 0$ the open cover $\overline{B^{(E)}(2R)} \subseteq \mathbb{R}^n = x + B^{(N)}(r+\varepsilon)$ has a finite subcover $\overline{B^{(E)}(2R)} \subseteq \bigcup_1^{n_\varepsilon} \left(\gamma^{(i)} + B^{(N)}(r+\varepsilon)\right)$ where $\gamma^{(i)} \in x$.

Given $1 > \delta > 0$, we can find a neighborhood $V_{\varepsilon,\delta}$ of x, such that any $y \in V_{\varepsilon,\delta}$ satisfies (1) y has covering radius $\leq 2R$ and (2) for each $i = 1, ..., n_\varepsilon$ the lattice y contains $\tilde{\gamma}^{(i)}$ with $\left\|\tilde{\gamma}^{(i)} - \gamma^{(i)}\right\| < \delta$. Each such y has a fundamental domain inside $\overline{B^{(E)}(2R)}$, so if we can show that $\overline{B^{(E)}(2R)} \subseteq \bigcup_1^{n_\varepsilon} \left(\tilde{\gamma}^{(i)} + B^{(N)}(r+2\varepsilon)\right)$ then $Ncov(y) \leq r + 2\varepsilon$. Proving this for any $\varepsilon > 0$ will complete the proof.

Let $v \in \overline{B^{(E)}(2R)}$ and $i \in \{1, ..., n_\varepsilon\}$ such that $N\left(v - \gamma^{(i)}\right) \leq r + \varepsilon$. Then

$$N\left(\tilde{\gamma}^{(i)} - v\right) = \prod_j \left|\tilde{\gamma}_j^{(i)} - v_j\right| \leq \prod_j \left(\left|\tilde{\gamma}_j^{(i)} - \gamma_j^{(i)}\right| + \left|\gamma_j^{(i)} - v_j\right|\right) \leq N\left(\gamma^{(i)} - v\right) + \delta\left(\|v\| + \left\|\gamma^{(i)}\right\| + 1\right)^{2^n}.$$

Taking $\delta = \frac{\varepsilon}{2}\min_i\left(\|v\| + \left\|\gamma^{(i)}\right\| + 1\right)^{-2^n}$, we get that $N\left(\tilde{\gamma}^{(i)} - v\right) < r + 2\varepsilon$. As v was arbitrary in $\overline{B^{(E)}(2R)}$ we conclude that $\overline{B^{(E)}(2R)} \subseteq \bigcup_1^{n_\varepsilon} \left(\tilde{\gamma}^{(i)} + B^{(N)}(r+2\varepsilon)\right)$ which is what we wanted to show. □

This upper semicontinuity let us improve the process mentioned in the previous section - instead of finding a "nice" lattice in Ax, it is enough to find one in $\overline{Ax}$.

Corollary 3.2. *Let $x \in X_n$ such that $\overline{Ax}$ contains a lattice which satisfies MINK. Then x satisfies MINK. In particular almost every $x \in X_n$ satisfies MINK.*

Proof. If $y \in \overline{Ax}$, then we can find $a_i \in A$ such that $a_i x \to y$. By the previous lemma $\lim_{i\to\infty} Ncov(a_i x) \leq Ncov(y)$. Since $Ncov$ is constant on A-orbits and we assumed that y satisfies MINK, we conclude that $Ncov(x) \leq Ncov(y) \leq \frac{1}{2^n}$, hence x satisfies MINK. The second claim follows from the fact that for almost every $x \in X_n$ the orbit Ax is dense, and we already know of lattice examples for which MINK holds. □

When studying the A-orbits , on which $Ncov$ is constant, it is helpful to distinguish between bounded and unbounded orbits. In the space X_n there is a simple criterion, called Mahler criterion, which checks when is a set bounded. For that we need to following definition:

Definition 3.3. For a lattice $L \leq \mathbb{R}^n$ denote by $|L| = \min\{\|v\| \mid 0 \neq v \in L\}$.

Theorem 3.4 (Mahler Criterion)**.** *A set $\Omega \subseteq X_n$ is bounded if and only if $\inf_{L\in\Omega} |L| > 0$.*

Mahler criterion states that Ω is bounded if we have a uniform positive lower bound on all the nonzero vector in all the lattices in Ω.

We now want to understand Mahler criterion for A-orbits. Let $L \leq \mathbb{R}^n$ be a unimodular lattice. One reason for AL to be unbounded is if L contains a nonzero vector v with a zero entry. Indeed, assuming that $v_1 = 0$, and letting $a_\varepsilon = diag\left(\frac{1}{\varepsilon^{n-1}}, \varepsilon, ..., \varepsilon\right)$, we get that $a_\varepsilon v \in a_\varepsilon L$ is a nonzero vector and $\|a_\varepsilon v\| \to 0$. As the next lemma shows, the parameter that measures the boundedness of AL is the multiplicative norm (and for vectors with zero entries the multiplicative norm is always zero!).

Lemma 3.5. *Let $L \leq \mathbb{R}^n$ be a unimodular lattice. Then the A-orbit AL is bounded if and only if $N(L\setminus\{0\}) > 0$.*

Proof. For any $\bar{t} \in \mathbb{R}^n_0$ and $0 \neq v \in L$ we have that

$$\frac{\|a(\bar{t})v\|_2^2}{n} = \frac{\sum_1^n (e^{t_i}v_i)^2}{n} \geq \left(\prod \left(e^{t_i}v_i\right)^2\right)^{1/n} = N(v)^{2/n} \geq N(L\setminus\{0\})^{2/n}.$$

It follows that if $N(L\setminus\{0\}) > 0$, then $\sqrt{n}N(L\setminus\{0\})^{1/n}$ is a uniform lower bound on $\{|aL|,\ a \in A\}$, and hence AL is bounded.

Suppose now that $N(L\setminus\{0\}) = 0$, so for any $\varepsilon > 0$ we can find $0 \neq v \in L$ such that $N(v) < \varepsilon$. If v has a zero entry, then we have already seen that AL is unbounded. Suppose that $v_i \neq 0$ for all i, and set $a_i = \frac{N(v)^{1/n}}{|v_i|}$ so that $a = diag(a_1, ..., a_n) \in \mathrm{SL}_n(\mathbb{R})$ and $|(av)_i| = N(v)^{1/n}$. It then follows that aL contains the vector av with $\|av\|_2^2 = nN(v)^{2/n} \leq n\varepsilon^{2/n}$. As $\varepsilon > 0$ was arbitrary, we get that AL is unbounded. □

The final detail that we need is Minkowski's lemma. As we seen above, boundedness is implied by a uniform positive lower bound on $|L|$. An upper bound always exists and we can find such bound which depends only on the dimension.

Theorem 3.6. *(Minkowski's Theorem): Let $L \leq \mathbb{R}^n$ be a lattice. Then $|L| \leq 2\left(\frac{covol(L)}{\left|B_n^{(E)}(1)\right|}\right)^{1/n}$ where $B_n^{(E)}(1)$ is the n-dimensional Euclidean ball of radius 1.*

Now that we have some of the definitions for the space of lattice, let us prove that not all of the lattices has the form DOTU.

Claim 3.7. There are lattices which are not DOTU.

Proof. If a lattice L has the form $aku\mathbb{Z}^n$ with $a \in A$, $k \in \mathrm{SO}_n(\mathbb{R})$ and $u \in U_n$, then its A-orbit contains $ku\mathbb{Z}^n$ which contains the vector $kue_1 = ke_1$ of length 1. Thus, to find a non DOTU matrix, it is enough to find a unimodular lattice L such that $|aL| > 1$ for all $a \in A$. Equivalently, using

again the same argument as in lemma 3.5 for a uniform lower bound, we want to find a lattice L with $N(L\setminus\{0\})^{1/n} > \frac{1}{\sqrt{n}}$. For that, we will use lattices coming from field extensions.

Let $\mathbb{K}/\mathbb{Q}$ be a totally real field extension with real embeddings $\sigma_1, ..., \sigma_k : \mathbb{K} \to \mathbb{R}$, $\mathcal{O}_\mathbb{K}$ its integer ring and $L_\mathbb{K} = \{(\sigma_1(\alpha), ..., \sigma_n(\alpha)) \mid \alpha \in \mathcal{O}_\mathbb{K}\}$ its corresponding lattice. Since any nonzero element in $\mathcal{O}_\mathbb{K}$ has a nonzero norm in $\mathbb{Z}$, we get that $N(L_\mathbb{K}\setminus\{0\}) \geq 1$. Normalizing $L_\mathbb{K}$ we obtain a unimodular lattice with

$$\left(N\left(D_\mathbb{K}^{-1/2n} L_\mathbb{K}\setminus\{0\}\right)\right)^{1/n} = \frac{1}{D_\mathbb{K}^{1/2n}} N(L_\mathbb{K}\setminus\{0\})^{1/n} \geq \frac{1}{D_\mathbb{K}^{1/2n}}.$$

Thus, to find a non DOTU matrix, it is enough to find such $\mathcal{O}_\mathbb{K}$ with $n > D^{1/n}$. Here we use the Golod-Shafarevich theorem [5] which states that there are $\mathbb{K}_i/\mathbb{Q}$ with $[\mathbb{K}_i : \mathbb{Q}] = n_i \to \infty$ such that D_i^{1/n_i} is uniformly bounded, hence $\frac{n_i}{D^{1/n_i}} \to \infty > 1$. □

4 Well rounded lattices

We now return to the search for another definition for "nice" lattices which hopefully implies that they have small covering radius. One reason for a lattice to have a small covering radius is if it is generated by small vectors. In particular we can consider well rounded lattices.

Definition 4.1. Let $L \leq \mathbb{R}^n$ and let $L_{\min} = span_\mathbb{Z}\{v \in L \mid \|v\| = |L|\}$ be the subgroup of L generated by the smallest nonzero vectors. We say that L is well rounded if $span_\mathbb{R}(L_{\min}) = \mathbb{R}^n$, or equivalently $[L : L_{\min}] < \infty$.

Note that if $v_1, ..., v_n \in L$ are independent vectors, then $\left\{\sum a_i v_i \mid |a_i| \leq \frac{1}{2}\right\}$ is a fundamental domain of $span_\mathbb{Z}\{v_1, ..., v_n\}$, and hence contains a fundamental domain of L. In particular, if the v_i are all small, we can hope that L would have a small covering radius.

Example 4.2.

- The simplest example is $\mathbb{Z}^n$, in which case the smallest nonzero vectors are $\{\pm e_i \mid i = 1, ..., n\}$ which generate the full lattice. For any other lattice in the A-orbit $\mathbb{Z}^n$, the smallest nonzero vector generate a lattice of dimension strictly less than n.
- Another two dimensional example is the lattice corresponding to $\mathbb{Z}[\omega]$ where ω is a primitive third root of unity. In this case, the smallest nonzero vectors are $\pm 1, \pm\omega, \pm\omega^2$ which generate the full lattice (note that even ignoring the signs, this is not a basis, but just a spanning set).
- Consider the lattice $L = \mathbb{Z}^n + \mathbb{Z}\cdot\left(\frac{1}{2}, ..., \frac{1}{2}\right)$. If $n \geq 5$, then the shortest nonzero vectors in L are exactly $\{\pm e_i \mid i = 1, ..., n\}$, which generate the lattice $\mathbb{Z}^n$ which has index 2 in L. It follows that L is well rounded, but the shortest vectors do not generate the full lattice.

Minkowski's conjecture can now be proven if we can show that:

(W_n). For any n-dimensional lattice L, its A-orbit $\overline{AL}$ contains a well rounded lattice.

(C_n). Any well rounded n-dimensional lattice has covering radius $\leq \frac{\sqrt{n}}{2}$.

In this section we will show the main ideas from McMullen's [10] in which he proved W_n for bounded A-orbits and for all n.

The covering conjecture C_n is known as conjecture Woods and was proved by him for $n \leq 6$ in [16] and was later proved by Hans-Gill, Raka, Sehmi, Kathuria for $n = 7, 8, 9$ in [8, 7, 6]. On the other

hand, it was shown by Regev, Shapira and Weiss in [13] that Woods' conjecture is false for dimension $n \geq 30$. Building on McMullen's ideas Shapira and Weiss proved a similar result with stable lattices instead of well rounded lattices in [14] for which the corresponding C_n conjecture is known for $n \leq 7$. Finally in [15] Solan upgraded the results of both McMullen's and Shapira and Weiss' and proved that every A-orbit contains both a well rounded lattice and a stable lattice (namely, don't need the closre, nor the bounded condition).

4.1 The $n = 2$ case

We begin with McMullen's ideas for dimension $n = 2$ in which the diagonal group A is isomorphic to $\mathbb{R}$ via $t \mapsto a(t) := \mathrm{diag}(e^t, e^{-t})$. We want to show that if $x \in X_2$ with Ax bounded, then there exists some $a \in A$ such that ax is well rounded. This case is easy - if x is already well rounded then we are done, and otherwise we can find a unique (up to a sign) vector $v = (v_1, v_2) \in L \setminus \{0\}$ of shortest length. Since the orbit is bounded, both v_1 and v_2 are nonzero, hence $\|a(t)v\| \to \pm\infty$ as $t \to \infty$. By theorem 3.6 we have that $|a(t)v| > |a(t)L|$ for $|t|$ large enough (since $|L| \leq \sqrt{\frac{2^n}{B^{(E)}(1)}}$ for L unimodular of rank n). Thus, using the intermediate value theorem, we can find the last time t for which $|a(t)v| = |a(t)L|$ which implies that $a(t)L$ has two linearly independent shortest vectors, and therefore it is well rounded.

Let us give a bit more complicated reasoning for this result, which is more suitable for generalizing to higher dimension.

We want to find some $a \in A$ for which $rank((aL)_{\min}) = 2$. Consider the open set $U_1 = \{a \in A \mid rank((aL)_{\min}) = 1\}$ and the map $a \mapsto M(a) := a^{-1}(aL)_{\min} \leq L$. Namely, $M(a)$ is the rank 1 subgroup of L such that after acting by a it contains the smallest nonzero vector in aL (in the argument above, $M(a) = \mathbb{Z}v$). We want to show that $U_1 \subsetneq A$.

The map $a \mapsto M(a)$ is locally constant - if av is the unique (up to sign) nonzero minimal vector in aL, then the same is true in a small neighborhood of a. The argument above shows that each connected component of U_1 is bounded. Moreover, this bound is uniform. The vectors av are all on the hyperbola $xy = N(v) \geq N(L \setminus \{0\})$, so the time in which this this hyperbola spends inside the ball of radius $\sqrt{\frac{2^n}{B^{(E)}(1)}}$ has an upper bound which depends only on the dimension and $N(L \setminus \{0\})$.

Thus, the $n = 2$ case follows from the fact that $A \cong \mathbb{R}$ cannot be covered by (1) open (2) connected sets (3) with uniformly bounded diameter which are disjoint.

4.2 The $n = 3$ case.

As in the $n = 2$ case, we now define

$$U_1 = \{a \in A \mid rank((aL)_{\min}) = 1\}$$
$$U_2 = \{a \in A \mid rank((aL)_{\min}) = 2\}$$

and we want to show that $U_1 \cup U_2 \subsetneq A \cong \mathbb{R}^2$. The same argument from before shows that (1) U_1 is an open set and the (2) diameters of its connected components are uniformly bounded. The set U_2 is no longer open, but for clearance of explanation we will ignore this problem here now and treat U_2 as though it is open.

Suppose that U_2 satisfies condition (2) as U_1 and $U_1 \cup U_2 = \mathbb{R}^2$. Then the connected components of U_1 and those of U_2 are open with uniformly bounded diameter, and each point in $\mathbb{R}^2$ is covered by

at most 2 such components. It is not hard to believe that this cannot be true. Unfortunately, things become more complicated in higher dimension.

The main problem that we have is as follows. Suppose that $rank(L_{\min}) = 2$ and $L_{\min}$ has 2 linearly independent vectors v_1, v_2 of length $|L|$. If we act by some small a and move to the lattice aL, the lengths of av_1, av_2 can become different so that we fall from U_2 to U_1 which is OK. Suppose now that we can find a direction in A in which $\|av_1\| = \|av_2\|$. As in the previous case, if we flow far enough the length of these vectors will go to infinity (the orbit is bounded), so at some point there should be another vector av_3 with $\pm v_1, \pm v_2, \pm v_3$ distinct, and $\|av_i\| = |aL|$ for $i = 1, 2, 3$. The problem now is that they no longer need to be linearly independent (think $\mathbb{Z}[\omega]$). If we continue to flow, then maybe $\|av_1\|$ increases while $\|av_2\| = \|av_3\|$ decrease, hence we can no longer show immediately that the connected components of U_2 are bounded.

As we don't want to keep track on all the short vectors, in particular when we go to even higher dimension, we will instead look on covolume of $(aL)_{\min}$ in $span_{\mathbb{R}}((aL)_{\min})$. Note that for rank one lattices, this is exactly the length of the shortest nonzero vector.

To study this covolume, we use the following notation.

Definition 4.3. Let $1 \leq d \leq n$. We shall denote by $\binom{[n]}{d}$ the subsets $I \subseteq [n]$ of size d. For $I = \{i_1, ..., i_d\} \in \binom{[n]}{d}$ with $i_1 < \cdots < i_d$ let $e_I = e_{i_1} \wedge \cdots \wedge e_{i_d} \in \bigwedge^d (\mathbb{R}^n)$.

For $w \in \bigwedge^d (\mathbb{R}^n)$ with $w = \sum_{I \in \binom{[n]}{d}} \alpha_I e_I$ write $\|w\|_2 = \sqrt{\sum \alpha_I^2}$ and $\|w\|_\infty = \sup |\alpha_I|$.

Note first that for $d = 1$, namely $\bigwedge^1 (\mathbb{R}^n) = \mathbb{R}^n$, the norms $\|w\|_2$ and $\|w\|_\infty$ are the standard Euclidean and supremum norm. In particular if $0 \neq v \in \mathbb{R}^n$, then $\|v\|_2 = |\mathbb{Z}v|$, and this can be generalized to higher dimension.

Claim 4.4. Let $v_1, ..., v_d \in \mathbb{R}^n$ linearly independent, and set $w = v_1 \wedge \cdots \wedge v_d \in \bigwedge^d (\mathbb{R}^n)$. Then the covolume of $span_{\mathbb{Z}}\{v_1, ..., v_n\}$ in $span_{\mathbb{R}}\{v_1, ..., v_n\}$ is $\|w\|_2$, which up to a bounded scalar the covolume is $\|w\|_\infty$.

Proof. The first part is just a special case of Cauchy-Binet's theorem, while the second follows from the fact that all the norms on $\mathbb{R}^{\binom{n}{d}}$ are equivalent. □

We now return to show that the connected components of U_2 are not "too big". As in U_1, the map $a \mapsto a^{-1}(aL)_{\min}$ for $a \in U_2$ is locally constant so each connected component correspond to some rank 2 sublattice $L' = span_{\mathbb{Z}}\{v_1, v_2\} \leq L$. We first note that the argument from the 1-dimensional case still holds: since $(aL)_{\min}$ is generated by the smallest vectors from L, and their size is uniformly bounded from above (by theorem 3.6), the covolume of $(aL)_{\min}$ is uniformly bounded from above. Thus, if aL' has large covolume, then it cannot be $(aL)_{\min}$ and therefore a is not in the connected component which correspond to L'.

Letting $w = v_1 \wedge v_2 = \sum_{|I|=2} \alpha_I e_I \in \bigwedge^2 (\mathbb{R}^n)$, if $a(\bar{t}) = \operatorname{diag}(e^{t_1}, e^{t_2}, e^{t_3})$, $\bar{t} \in \mathbb{R}^3_0$, then the covolume of $a(\bar{t}) L'$ is (up to a scalar)

$$\|a(\bar{t}) w\|_\infty = \left\| \sum_{|I|=2} e^{\sum_{i \in I} t_i} \alpha_I e_I \right\| = \max_{|I|=2} e^{\sum_{i \in I} t_i} |\alpha_I|.$$

If all the α_I are nonzero, then $\|t\| \to \infty$ implies that $\max_{|I|=2} \left(e^{\sum_{i \in I} t_i}\right) \to \infty$ and therefore $\|a(\bar{t}) w\|_\infty \to \infty$ and we continue along the same argument as in the case $n = 2$. If some of

the α_I are zero, for example $\alpha_{\{2,3\}} = 0$, then choosing $\bar{t} = (-2m, m, m)$ we get that

$$\|a(\bar{t})\, w\|_\infty = e^{-m} \max\left\{\left|\alpha_{\{1,2\}}\right|, \left|\alpha_{\{1,3\}}\right|\right\}.$$

But as $m \to \infty$, the covolume goes to zero, so that by theorem 3.6 the sublattice $a(\bar{t})\, L'$ and therefore $a(\bar{t})\, L$ contain nonzero vectors with length which converge to zero, contradicting the fact that AL is bounded.

Thus, we proved that any connected component of U_2 is still bounded (with uniform upper bound on the diameters). To summarize the arguments, we showed that given the pattern of nonzero coeficients in w we either have:

1. Many of the α_I are nonzero, so we could find a coefficient $e^{\sum_{i\in I} t_i}$ which goes to ∞.
2. Too few of the α_I are nonzero, so we could find big $\bar{t} \in \mathbb{R}^3_0$ for which all the coefficients $e^{\sum_{i\in I} t_i}$ for the nonzero α_I go to zero. This contradicts the boundedness of the orbit.

Since we are only in dimension $n = 3$, there are only 3 coefficients. As we shall see next, in higher dimension we have one more case in which some of the $e^{\sum_{i\in I} t_i}$ are equal to 1 while the rest might go to zero.

4.3 The $n \geq 4$ case

Given $w \in \bigwedge^k \mathbb{R}^n$, the main reason we should expect $\|a(\bar{t})\, w\|$ to be bounded for large $\bar{t}$ is if $a(\bar{t}_0)\, w = w$ for some $\bar{t}_0 \neq 0$, and then $a(m\bar{t}_0)\, w = w$ for all m.

Example 4.5. Consider the ring $\mathbb{Z}\left[\sqrt{2}, \sqrt{3}\right]$ and its corresponding lattice $L = \{(\beta, \sigma(\beta), \tau(\beta), \sigma\tau(\beta))\}$ where σ, τ are the Galois maps $\sigma : \sqrt{2} \leftrightarrow -\sqrt{2}$ and $\tau : \sqrt{3} \leftrightarrow -\sqrt{3}$. Equivalently, L is generated by

$$\begin{aligned} v_1 &= (1, 1, 1, 1) \\ v_2 &= \left(\sqrt{2}, -\sqrt{2}, \sqrt{2}, -\sqrt{2}\right) \\ v_3 &= \left(\sqrt{3}, \sqrt{3}, -\sqrt{3}, -\sqrt{3}\right) \\ v_6 &= \left(\sqrt{6}, -\sqrt{6}, -\sqrt{6}, \sqrt{6}\right). \end{aligned}$$

This lattice contains the sublattice $L' = span_{\mathbb{Z}}\{v_1, v_2\}$ which correspond to $\mathbb{Z}\left[\sqrt{2}\right]$. If $u \in \mathbb{Z}\left[\sqrt{2}\right]^\times$, then $u\mathbb{Z}\left[\sqrt{2}\right] = \mathbb{Z}\left[\sqrt{2}\right]$, which implies that for

$$a = \mathrm{diag}(u, \sigma(u), \tau(u), \sigma\tau(u)) = \mathrm{diag}(u, \sigma(u), u, \sigma(u))$$

we have that $aL' = L'$. This can also be seen by considering the wedge product

$$v_1 \wedge v_2 = -2\sqrt{2}e_{\{1,2\}} - 2\sqrt{2}e_{\{1,4\}} - 2\sqrt{2}e_{\{3,2\}} - 2\sqrt{2}e_{\{3,4\}}.$$

Acting by element of the form $a(t, -t, t, -t)$ doesn't change the covolume.

Note that in the example above the invariance of a k-dimensional subspace arose from a subfield extension of degree k over $\mathbb{Q}$. Moreover, the $stab_A(w)$ correspond to the invertible elements in the integer ring, which by Dirichlet's unit theorem has rank $k - 1$. This result can be shown directly without using the algebraic construction. Thus we expect $\|aw\|$ to increase as a gets further away from this $k - 1$ dimensional space in A.

Lemma 4.6. *Let $L \leq \mathbb{R}^n$ be a lattice with AL bounded and $U_d = \{a \in A \mid rank\left((aL)_{\min}\right) = d\}$. Then any connected component of U_d in $A \cong \mathbb{R}^{n-1}$ is contained in a set of the form $K \times \mathbb{R}^j$ where $j \leq d-1$ and the diameter of K is uniformly bounded (as a function of d, n and L).*

The lemma above was proved by McMullen in [10], though in a stronger form, where the U_d are chosen to be open sets a little bit larger than in the definition above. Finally, to prove that $\overline{AL}$ contains a well rounded lattice McMullen proved that the space $\mathbb{R}^{n-1}$ ($\cong A$) cannot be covered by $U_1, ..., U_{n-1}$ as in the previous lemma (up to a simplification of notation for clarity...).

Remark 4.7. Clearly, if an orbit AL is compact, then it is bounded. It is well known that all the compact orbit arise from algebraic constructions similar to the one above (see section §A). The other direction is not known, and it was conjectured by Margulis that for dimension $n \geq 3$ all the bounded A-orbits are compact, and hence come from algebraic constructions.

5 Unbounded A-orbits

Next we consider the proof for unbounded A-orbits which first appeard in [2]. The simplest reason for an A-orbit AL to be unbounded, is if L contains a nonzero vector with zero entries. To formulaize this, it means that we can find $I \subseteq [n]$ nontrivial such that $L \cap \mathbb{R}^I \neq \{0\}$ where $\mathbb{R}^I$ is the subspace of $\mathbb{R}^n$ supported on the coordinates in I. An even stronger reason is if there is some $I \subseteq [n]$ nontrivial such that $L \cap \mathbb{R}^I$ is a lattice in $\mathbb{R}^I$. As $L \cap \mathbb{R}^I$ is a lattice of smaller rank than L, this suggests an induction argument.

Definition 5.1. We say that a lattice $L \leq \mathbb{R}^n$ is axis reducible if there is some nontrivial $I \subseteq [n]$ such that $L \cap \mathbb{R}^I$ is a lattice in $\mathbb{R}^I$.

Lemma 5.2. *If MINK is true for dimension $\leq n-1$, then it is true for n-dimensional axis reducible lattices.*

Proof. Let $L \leq \mathbb{R}^n$ be an axis reducible lattice. By a permutation of the indices, we can write $n = n_1 + n_2$ and $\mathbb{R}^n = \mathbb{R}^{n_1} \oplus \mathbb{R}^{n_2}$ such that $L_1 := L \cap \mathbb{R}^{n_1}$ is a lattice in $\mathbb{R}^{n_1}$ (where we identify $\mathbb{R}^{n_i}$ as the axis subspaces of $\mathbb{R}^n$). Let $L_2 \leq L$ such that $L = L_1 \oplus L_2$. By acting with a suitable diagonal matrix on L, we may assume that $covol\left(\mathbb{R}^{n_1} : L_1\right) = 1$ and that $covol\left(\mathbb{R}^{n_2} : \pi\left(L_2\right)\right) = 1$ where $\pi : \mathbb{R}^n \to \mathbb{R}^{n_2}$ is the orthogonal projection.

Let $v = v_1 + v_2$ where $v_i \in \mathbb{R}^{n_i}$. By assumption we can find $\gamma^{(2)} \in L_2$ such that $N\left(\pi\left(\gamma^{(2)}\right) - v_2\right) \leq \frac{1}{2^{n_2}}$. Write $\gamma^{(2)} = \gamma_1^{(2)} + \gamma_2^{(2)}$ with $\gamma_i^{(2)} \in \mathbb{R}^{n_i}$. Again, by assumption, we can find $\gamma^{(1)} \in L_1$ such that $N\left(\gamma^{(1)} - \left(v_1 - \gamma_1^{(2)}\right)\right) \leq \frac{1}{2^{n_1}}$. It then follows that $\gamma = \gamma^{(1)} + \gamma^{(2)} \in L$ satisfies

$$N\left(\gamma - v\right) = N\left(\left[\gamma^{(1)} - \left(v_1 - \gamma_1^{(2)}\right)\right] + \left[\gamma_2^{(2)} - v_2\right]\right) = N\left(\gamma^{(1)} - \left(v_1 - \gamma_1^{(2)}\right)\right) N\left(\gamma_2^{(2)} - v_2\right) \leq \frac{1}{2^{n_1}} \cdot \frac{1}{2^{n_2}} = \frac{1}{2^n}.$$

□

Of course, if L is axis reducible, than its A-orbit is unbounded, but as we shall see next the converse is almost true as well. Similarly if $\overline{Ax}$ contains an axis reducible lattice, then Ax is unbounded. The next goal is to show that the converse is true as well, and then use this result to prove MINK for unbounded orbits.

5.1 Unbounded orbits - the $n = 2$ intuition.

The next goal is to show that unboundned orbits always satisfy MINK. In order to prove that we shall show that any such orbit contain in its closure an axis reducible lattice.

First, to get some intuition, let us consider the case $n = 2$. Let $x \in X_2$ be a lattice, $0 \neq v \in x$ its smallest nonzero vector, and without loss of generality assume that $v = \begin{pmatrix} \varepsilon_1 \\ \varepsilon_2 \end{pmatrix}$ with $\varepsilon_1 \geq \varepsilon_2 \geq 0$. As we consider unbounded orbits, we shall assume that $\varepsilon_1 > 0$ is very small (so that x is near the cusp). As v is a smallest nonzero vector, we can complete it to a basis $\{v, u\}$ of x. Acting with the matrix $a = diag\left(\frac{1}{\varepsilon_1}, \varepsilon_1\right)$, we get a new basis consisting of $v' = av = \begin{pmatrix} 1 \\ \varepsilon_1\varepsilon_2 \end{pmatrix}$ which is almost $\begin{pmatrix} 1 \\ 0 \end{pmatrix}$ and $u' = au$. The only vectors which complete e_1 to a unimodular lattice are of the form

$\alpha e_1 \pm e_2$ for some $\alpha \in \mathbb{R}$. Note that the lattices of the form $span_{\mathbb{Z}}\{e_1, \alpha e_1 \pm e_2\}$ are axis reducible. Let us show that $\{v', u'\}$ is almost of this form.

Since $v'_1 = 1$, we get that $u'' = u' - u'_1 \cdot v' \in \{0\} \times \mathbb{R}$, which is just the projection of u' to $\{0\} \times \mathbb{R}$ via the direction v' (see figure ???? below). Computing the covolume, we get that

$$|u''_2| = |\det(v', u'')| = |\det(v', u' - u'_1 v')| = |\det(v', u')| = 1$$

so that $u'' = (0, 1)$. Unfortunately, this is not necessarily a vector in our lattice, but we can lift it back to get $u''' = (0, 1) + \delta v'$ in the lattice where $|\delta| \leq \frac{1}{2}$. We conclude that ax can be written as $\begin{pmatrix} 1 & \delta \\ \varepsilon_1\varepsilon_2 & 1 + \delta\varepsilon_1\varepsilon_2 \end{pmatrix} \mathbb{Z}^2$. If we can find a sequence of such lattices with $\left\|v^{(i)}\right\| \to 0$ (so that $\left|\varepsilon_2^{(i)}\right|, \left|\varepsilon_1^{(i)}\right| \to 0$), then by restricting to a subsequence for which δ_i converge to some δ_∞, we get a limit lattice of the form $\begin{pmatrix} 1 & \delta_\infty \\ 0 & 1 \end{pmatrix} \mathbb{Z}^2$ which is axis reducible.

5.2 Unbounded orbits - the general case

Suppose now that the rank of the given lattice L is strictly greater than 2 with height $ht_\infty(L) = \sup\left\{\|v\|_\infty^{-1} \mid 0 \neq v \in L\right\}$ very large. We start the same way by acting with a diagonal matrix which takes the smallest nonzero vector $v \in L$ to be a vector v' which is almost one of the vectors in the standard basis, without loss of generality e_1. Note that the size of this matrix is at most $\frac{1}{\|v\|_\infty}$. As before, we project to the subspace $\{0\} \times \mathbb{R}^{n-1}$ via the direction of v to get a lattice $L' \leq \{0\} \times \mathbb{R}^{n-1}$. If this lattice doesn't contain short vectors, then the same argument as before will work, and we will get the A-orbit of L contains a lattice of the form $\begin{pmatrix} 1 & w \\ \bar{\epsilon} & B \end{pmatrix} \mathbb{Z}^3$ where the $w \in \mathbb{R}^2$ and $B \in \mathbb{R}^{2\times 2}$ are not too big (which are more or less correspond to δ from the rank 2 case, and to the basis of L). If L' does contain small vector, we need to use induction and maybe act with a second diagonal matrix a' (to "fix" B) and simultaneously not ruin $\bar{\epsilon}$. The reason this will work is that if u is the smallest nonzero vector in L' it cannot be "too" small with respect to $\|v\|$, hence the new diagonal matrix a' will not have too big entries.

Lemma 5.3. *For any sequence in X_n there is a subsequence $x_i \in X_n$, an integer $0 \leq d \leq n-1$ such that $a\left(\bar{t}^{(i)}\right) x_i = B^{(i)}\mathbb{Z}^n$ where*

1. *If the original sequence diverges to infinity we ay choose $d \geq 1$.*
2. *$B^{(i)}$ are $(d, n-d)$ block matrices $B^{(i)} = \begin{pmatrix} B_1^{(i)} & B_2^{(i)} \\ B_3^{(i)} & B_4^{(i)} \end{pmatrix}$,*
3. *the $\left\|B^{(i)}\right\|_\infty$ are uniformly bounded and $\left\|B_3^{(i)}\right\|_\infty \to 0$,*
4. *$t_k^{(i)} \leq 0$ for $k \geq d+1$ and $\max_k\left\{e^{t_k^{(i)}}\right\} \leq 2^n ht_\infty(x_i)$ for all i.*

Proof. If the sequence is bounded, then we can take $d = 0$ (so that $B^{(i)} = B_4^{(i)}$) and $\bar{t}^{(j)} = \bar{0}$ and we are done. In particular this is always true for $n = 1$.

Assume that the sequence contains (and without loss of generality is) an unbounded subsequence $x_i \to \infty$. Let $0 \neq v^{(i)} \in x_i$ with $\left\|v^{(i)}\right\|_\infty$ minimal, and rearrange the indices so that $\varepsilon_i := \left|v_1^{(i)}\right| = \left\|v^{(i)}\right\|_\infty$ and without loss of generality assume that $0 < \varepsilon_i < 1$ for all i. Let $\tilde{a}^{(i)} = diag\left(\frac{1}{\varepsilon_i}, \varepsilon_i^{\frac{1}{n-1}}, ..., \varepsilon_i^{\frac{1}{n-1}}\right)$, $\tilde{x}_i = \tilde{a}^{(i)} x_i$ and let $\tilde{v}^{(i)} = \tilde{a}^{(i)} v^{(i)}$. Note that $\tilde{v}^{(i)} = \left(1, \varepsilon^{\frac{1}{n-1}} v_2^{(i)}, ..., \varepsilon^{\frac{1}{n-1}} v_n^{(i)}\right)$ and for $k \geq 2$ we have that $\left|\tilde{v}_k^{(i)}\right| \leq \varepsilon_i^{\frac{n}{n-1}}$, so that $\tilde{v}^{(i)}$ is very close to $(1, 0, ..., 0)$.

Since $\tilde{v}_1^{(i)} \neq 0$, we get that $\mathbb{R}^n = \mathbb{R}\tilde{v}^{(i)} \oplus \left(\{0\} \times \mathbb{R}^{n-1}\right)$ and we let $\pi : \mathbb{R}^n \to \{0\} \times \mathbb{R}^{n-1}$ be the projection with kernel $\mathbb{R}\tilde{v}^{(i)}$. It then follows that $\pi\left(\tilde{x}_i\right) \leq \{0\} \times \mathbb{R}^{n-1}$ is a lattice, and moreover it is unimodualr since $\left|\tilde{v}_1^{(i)}\right| = 1$. In addition, if $u = (0, u_2, ..., u_n) \in \pi\left(\tilde{x}_i\right)$, then there exists some $|\delta| \leq \frac{1}{2}$ such that $u + \delta\tilde{v}^{(i)} \in \tilde{x}_i$. In particular, if $0 \neq u \in \pi\left(x_i\right)$ with $\|u\|_\infty$ minimal, then

$$\varepsilon_i \leq \left\|v^{(i)}\right\|_\infty \leq \left\|\left(\tilde{a}^{(i)}\right)^{-1}\left(u + \delta\tilde{v}^{(i)}\right)\right\|_\infty = \left\|\left(\tilde{a}^{(i)}\right)^{-1} u + \delta v^{(i)}\right\|_\infty \leq \left\|\left(\tilde{a}^{(i)}\right)^{-1} u\right\|_\infty + \frac{1}{2}\varepsilon_i = \varepsilon_i^{-\frac{1}{n-1}} \|u\|_\infty + \frac{\varepsilon_i}{2}.$$

Hence, we obtain that $\|u\|_\infty \geq \frac{1}{2}\varepsilon_i^{\frac{n}{n-1}}$, hence $ht_\infty\left(\pi\left(\tilde{x}_i\right)\right) \leq 2\varepsilon_i^{-\frac{n}{n-1}}$.

Use the induction hypothesis on $\pi\left(\tilde{x}_i\right) \in X_{n-1}$ so by restricting to a subsequence (which we still denote by $\tilde{x}_i$) we get that

$$a\left(\tilde{t}^{(i)}\right)\pi\left(\tilde{x}_i\right) = \tilde{B}^{(i)}\mathbb{Z}^{n-1},\ \tilde{B}^{(i)} = \begin{pmatrix} \tilde{B}_1^{(i)} & \tilde{B}_2^{(i)} \\ \tilde{B}_3^{(i)} & \tilde{B}_4^{(i)} \end{pmatrix},$$

where $\tilde{B}^{(j)}$ are $(d-1, (n-1)-(d-1))$ block matrix, $\left\|\tilde{B}^{(j)}\right\|_\infty$ are uniformly bounded, $\left\|\tilde{B}_3^{(j)}\right\|_\infty \to 0$. The conditions on $\tilde{t}^{(j)}$ are that $\tilde{t}^{(i)} = \left(\tilde{t}_2^{(i)}, ..., \tilde{t}_n^{(i)}\right) \in \mathbb{R}_0^{n-1}$ such that $t_k^{(i)} \geq 0$ for $k \leq d$, $t_k^{(i)} \leq 0$ for $k \geq d+1$ and $\max_k\left\{e^{t_k^{(i)}}\right\} \leq 2^{n-1} ht_\infty\left(\pi\left(\tilde{x}_j\right)\right) \leq 2^{n-1}\left(\frac{1}{2}\varepsilon_i^{\frac{n}{n-1}}\right)^{-1}$. Note that if $\mathcal{B}$ is a lift of a basis for $\pi\left(\tilde{x}_j\right)$, then $\mathcal{B} \cup \left\{\tilde{v}^{(i)}\right\}$ is a basis for $\tilde{x}_j$. We already saw that every vector in $\pi\left(\tilde{x}_j\right)$ can be lifted to a vector in $\tilde{x}_j$ by adding to it $\delta\tilde{v}^{(1)}$ with $|\delta| \leq \frac{1}{2}$, hence we can write

$$\tilde{x}^{(i)} = \left(\tilde{v}^{(1)} \mid a\left(0, -\tilde{t}^{(i)}\right)\begin{pmatrix} \bar{0} & \bar{0} \\ \tilde{B}_1^{(i)} & \tilde{B}_2^{(i)} \\ \tilde{B}_3^{(i)} & \tilde{B}_4^{(i)} \end{pmatrix}\right)\begin{pmatrix} 1 & \bar{\delta}^{(i)} \\ 0 & I_{n-1} \end{pmatrix}\mathbb{Z}^n,$$

where $\bar{\delta}^{(i)} \in \mathbb{R}^{n-1}$ with $\left\|\bar{\delta}^{(i)}\right\|_\infty \leq \frac{1}{2}$. We claim that $a\left(0, \tilde{t}^{(i)}\right)\tilde{x}^{(i)} = a\left(t^{(i)}\right)x^{(i)}$ where

$$t^{(i)} = \ln\left(\varepsilon_i\right)\left(-1, \frac{1}{n-1}, ..., \frac{1}{n-1}\right) + \left(0, \tilde{t}^{(i)}\right)$$

has the required $(d, n-d)$ block presentation. First, since $d-1 \geq 0$ (from the induction), then $k \geq d+1$ implies in particular that $k \geq 2$ and therefore $t_k^{(i)} = \frac{\ln(\varepsilon_i)}{n-1} + \tilde{t}_k^{(i)} \leq 0$. Moreover, for $k \geq 2$ we get that

$$e^{t_k^{(i)}} = \varepsilon_i^{\frac{1}{n-1}} \cdot e^{\tilde{t}_k^{(i)}} \leq \varepsilon_i^{\frac{1}{n-1}} \cdot 2^{n-1} ht_\infty\left(\pi\left(\tilde{x}_i\right)\right) \leq 2^{n-1}\varepsilon_i^{\frac{1}{n-1}}\left(\frac{1}{2}\varepsilon_i^{\frac{n}{n-1}}\right)^{-1} = 2^n\varepsilon_i \leq 2^n ht_\infty\left(x_i\right),$$

so the condition on $\bar{t}$ is satisfied.

Next we want to show that the max norm of

$$B^{(i)} = \left(a\left(0, \tilde{t}^{(i)}\right) \tilde{v}^{(1)} \mid \begin{pmatrix} \bar{0} & \bar{0} \\ \tilde{B}_1^{(i)} & \tilde{B}_2^{(i)} \\ \tilde{B}_3^{(i)} & \tilde{B}_4^{(i)} \end{pmatrix} \right) \begin{pmatrix} 1 & \bar{\delta}^{(i)} \\ 0 & I_{n-1} \end{pmatrix}$$

is unifomly bounded, and since we already know that it is true for the $\tilde{B}^{(i)}$ and for $\bar{\delta}$, it is enough to show it for $a\left(0, \tilde{t}^{(i)}\right) \tilde{v}^{(1)}$. The first coordinate of this vector is just 1 which is of course uniformly bounded. For $d \geq k \geq 2$ we get that

$$\left(a\left(0, \tilde{t}^{(i)}\right) \left|\tilde{v}^{(1)}\right|\right)_k \leq 2^{n-1} h t_\infty \left(\pi\left(\tilde{x}_i\right)\right) \left|\tilde{v}_k^{(1)}\right| \leq 2^n \varepsilon_i^{-\frac{n}{n-1}} \varepsilon_i^{\frac{n}{n-1}} = 2^n$$

is again uniformly bounded. Finally, we need to show that $\left\|B_3^{(i)}\right\|_\infty \to 0$, and since $\left\|\tilde{B}_3^{(i)}\right\|_\infty \to 0$ and $\left\|\bar{\delta}^{(i)}\right\|_\infty \leq \frac{1}{2}$, it is enough to show that $\left(a\left(0, \tilde{t}^{(i)}\right) \left|\tilde{v}^{(1)}\right|\right)_k \to 0$ for $k \geq d+1$. Indeed, for these indices we have that $\tilde{t}^{(i)} \leq 0$ so that

$$\left(a\left(0, \tilde{t}^{(i)}\right) \left|\tilde{v}^{(1)}\right|\right)_k \leq \left|\tilde{v}_k^{(1)}\right| \leq \varepsilon_i^{\frac{n}{n-1}} \to 0.$$

□

Corollary 5.4. *Let $x \in X_n$ such that Ax is unbounded. Then $\overline{Ax}$ contains an axis reducible lattice.*

Proof. By the previous lemma, Ax contains lattice of the form $B^{(i)}\mathbb{Z}^n$ where $B^{(i)} = \begin{pmatrix} B_1^{(i)} & B_2^{(i)} \\ B_3^{(i)} & B_4^{(i)} \end{pmatrix}$ are $(d, n-d)$ block matrices with $1 \leq d \leq n-1$, $\left\|B^{(i)}\right\|_\infty$ are uniformly bounded and $\left\|B_3^{(i)}\right\|_\infty \to 0$. Since these matrices are uniformly bounded, they have a converging subsequence to determinant 1 matrix of the form $B^{(\infty)} = \begin{pmatrix} B_1^{(\infty)} & B_2^{(\infty)} \\ 0_{d,n-d} & B_4^{(\infty)} \end{pmatrix}$, hence $\overline{Ax}$ contains $B^{(\infty)}\mathbb{Z}^n$ which is an axis reducible lattice. □

Corollary 5.5. *Suppose that MINK is true for dimension $\leq n-1$ and $x \in X_n$ such that Ax is unbounded. Then x satisfies MINK.*

Proof. By 5.4 $\overline{Ax}$ contains an axis reducible lattice y which satisfies MINK by lemma 5.2. Using the fact that $\overline{N}$ is constant on A-orbits and it is upper semicontinuous, we conclude that $\overline{N}(x) \leq \overline{N}(y) \leq \frac{1}{2^n}$, hence x satisfies MINK. □

The original proof for the corollary above was given in [2] by Birch and Swinnerton-Dyer.

A Compact A-orbits and their algebraic structure

In this section we will show the correspondence between compact A-orbits and full modules (up to equivalence - definition below) in totally real extensions. Recall that we identify the positive diagonal group $A \leq \mathrm{SL}_n(\mathbb{R})$ with $\mathbb{R}_0^n \cong \mathbb{R}^{n-1}$ via $\bar{t} \mapsto diag(e^{t_1}, ..., e^{t_n})$. In particular $Ax \cong {}^{A}/_{stab_A(x)}$ is compact exactly when $stab_A(x)$ is a lattice in A. Thus, compactness of the orbit implies in particular that x is invariant under nontrivial elements of A.

To get some intuition we begin with the usual example of $\mathbb{Z}[\sqrt{2}]$ viewed below.

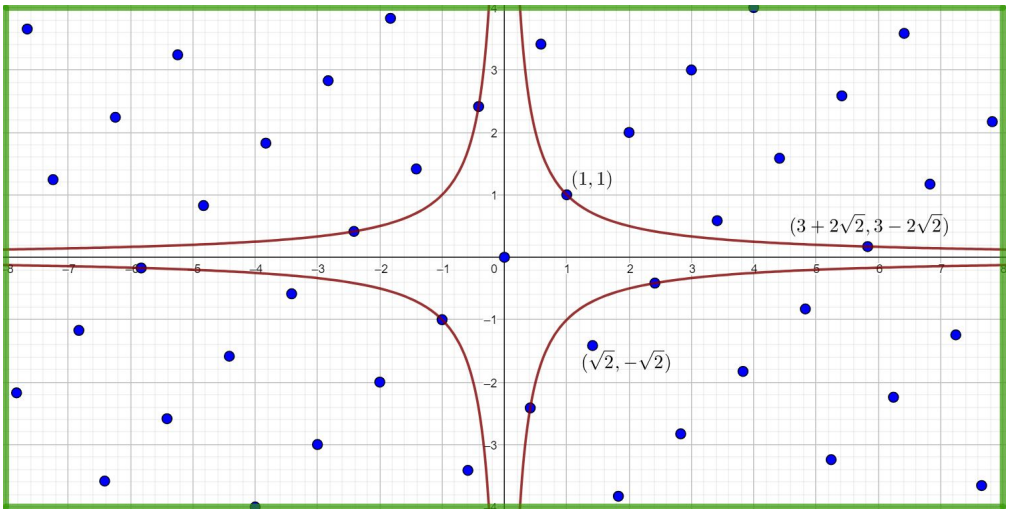

Figure A.1: The lattice corresponding to $\mathbb{Z}[\sqrt{2}]$ with the hyperbolas $xy = \pm 1$.

Let $L = span_{\mathbb{Z}}\{(1,1), (\sqrt{2}, -\sqrt{2})\} \leq \mathbb{R}^2$ be the (non normalized) lattice corresponding to $\mathbb{Z}[\sqrt{2}]$. Equivalently, $L = \{(\alpha, \sigma(\alpha)) \mid \alpha \in \mathbb{Z}[\sqrt{2}]\}$ where $\sigma(x + \sqrt{2}y) = x - \sqrt{2}y$ is the nontrivial Galois action on $\mathbb{Q}(\sqrt{2})$. In this 2-dimensional case, the group A is just $\left\{a(t) := \begin{pmatrix} e^t & 0 \\ 0 & e^{-t} \end{pmatrix} \mid t \in \mathbb{R}\right\}$ and acting by A means that the points of L move along the hyperbolas $xy = r$. For example, consider the points $p_1 = (1,1)$ and $p_2 = (3 + 2\sqrt{2}, 3 - 2\sqrt{2})$ which are on the hyperbola $xy = 1$. These points correspond to $1, u = 3 + 2\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$, and moreover their algebraic norms are 1, hence they are actually in $\mathbb{Z}[\sqrt{2}]^{\times}$. Taking $t_u := \ln(3 + 2\sqrt{2})$ we get that $a(t_u) p_1 = p_2$, so at least one point from L returns to L after acting by $a(t_u)$. We claim that L is actually invariant under $a(t_u)$, i.e. $a(t_u) L = L$, and the reason is that $u\mathbb{Z}[\sqrt{2}] = \mathbb{Z}[\sqrt{2}]$. Indeed, any point in L has the form $(\alpha, \sigma(\alpha))^{tr}$ for some $\alpha \in \mathbb{Z}[\sqrt{2}]$, hence

$$a(t_u) \cdot (\alpha, \sigma(\alpha))^{tr} = diag(u, \sigma(u)) (\alpha, \sigma(\alpha))^{tr} = (u\alpha, \sigma(u\alpha))^{tr} \in L.$$

We conclude that $a(t_u) L \leq L$, and with the same argument for the inverse map (which still applies since u^{-1} is also in $\mathbb{Z}[\sqrt{2}]^{\times}$) we get equality. It is easy to show that $t_u \in \mathbb{R}$ is the minimal positive number such that $a(t_u) L = L$ (there are no point between p_1 and p_2 on the hyperbola $xy = 1$).

Thus $stab_A(L) = \langle a(nt_u) \mid n \in \mathbb{Z} \rangle$ corresponds to the lattice $\mathbb{Z}t_u$ in $\mathbb{R}$, therefore $AL \cong \mathbb{R}/\mathbb{Z}$.

Let us generalize the example above.

Definition A.1. Let $\mathbb{K}/\mathbb{Q}$ be a totally real field of degree n. An additive subgroup $M \leq \mathbb{K}$ is called a full module if $M = span_{\mathbb{Z}}\{v_1, ..., v_n\}$ where $v_1, ..., v_n \in \mathbb{K}$ form a basis of $\mathbb{K}$ over $\mathbb{Q}$. If M is also a unital ring, then it is called an order in $\mathbb{K}$.

For the rest of this section, unless stated otherwise, $\mathbb{K}$ will always denote a totally real extension of $\mathbb{Q}$ of degree n, and $\sigma_i : \mathbb{K} \to \mathbb{R},\ i = 1, ..., n$ will be the distinct n embeddings.

Example A.2.

1. In $\mathbb{Q}$ the full modules are just $q\mathbb{Z}$ for $0 \neq q \in \mathbb{Q}$ and the only order is $\mathbb{Z}$.
2. In $\mathbb{Q}(\sqrt{2})$ we have many distinct orders - $span_{\mathbb{Z}}\{1, n\sqrt{2}\}$ is an order for any $0 \neq n \in \mathbb{N}$.

One way to find full modules in $\mathbb{K}$ is to begin with its integer ring $\mathcal{O}_{\mathbb{K}}$ and then any ideal in $\mathcal{O}_{\mathbb{K}}$ will be a full module. More over if $I \trianglelefteq \mathcal{O}_{\mathbb{K}}$, then αI is also a full module for any $0 \neq \alpha \in \mathbb{K}$, or in other words every fractional ideal is a full module. The other direction is almost true - every full module is a fractional ideal for some order in $\mathbb{K}$ (though not necessarily $\mathcal{O}_{\mathbb{K}}$). We begin with two useful results on full modules which will simplify this other direction.

Lemma A.3. *Let $M_1, M_2 \leq \mathbb{K}$ with M_1 finitely generated and $\mathbb{Q}M_2 = \mathbb{K}$. Then there exists $0 \neq m \in \mathbb{N}$ such that $mM_1 \subseteq M_2$.*

Proof. Write $M_1 = span_{\mathbb{Z}}\{\alpha_1, ..., \alpha_k\}$. Since $\alpha_i \in \mathbb{K} = \mathbb{Q}M_2$, we can find $m_i \in \mathbb{N}$ such that $m_i\alpha_i \in M_2$. Taking $m = \prod_1^k m_i$ we get that $m\alpha_i \in M_2$ for all i, which of course implies that $mM_1 \subseteq M_2$. □

Lemma A.4. *A subgroup $M \leq \mathbb{K}$ is a full module iff M is finitely generated and $\mathbb{Q}M = \mathbb{K}$.*

Proof. The $\Rightarrow$ direction follows directly from the definition. Assume now that M is finitely generated and $\mathbb{Q}M = \mathbb{K}$. Since these properties are satisfied by $\mathcal{O}_{\mathbb{K}}$ as well, we conclude from lemma A.3 that we can find m_1, m_2 such that $m_1m_2\mathcal{O}_{\mathbb{K}} \leq m_2M \leq \mathcal{O}_{\mathbb{K}}$. It is well known that $\mathcal{O}_{\mathbb{K}} \cong \mathbb{Z}^n$ where $n = [\mathbb{K} : \mathbb{Q}]$, so up to isomorphism we get that $m_1m_2\mathbb{Z}^n \leq m_2M \leq \mathbb{Z}^n$, implying that m_2M, and therefore M itself, have bases of size n. Since $\mathbb{Q}M = \mathbb{K}$ which has dimension n over $\mathbb{Q}$, the base of M over $\mathbb{Z}$ must also be a base of $\mathbb{K}$ over $\mathbb{Q}$, which completes the proof. □

Next, we find for any full module M an order $\mathcal{O}_M$ for which M is a fractional ideal.

Lemma A.5. *Let M be a full module in $\mathbb{K}$ and set $\mathcal{O}_M := \{\alpha \in \mathbb{K} \mid \alpha M = M\}$. Then $\mathcal{O}_M \leq \mathcal{O}_{\mathbb{K}}$ is an order and M is a fractional ideal of $\mathcal{O}_M$.*

Proof. Clearly, $\mathcal{O}_M$ is a unital ring. As in the previous lemma, in order to show that $\mathcal{O}_M$ is a full module, it is enough to show that $m\mathcal{O}_{\mathbb{K}} \leq \mathcal{O}_M \leq \mathcal{O}_{\mathbb{K}}$ for some $m \in \mathbb{N}$.

Clearly the product $\mathcal{O}_{\mathbb{K}} \cdot M$ is also a full module (finitely generated and $\mathbb{Q}\mathcal{O}_{\mathbb{K}}M = \mathbb{K}$), so by lemma A.3 we can find m such that $m\mathcal{O}_{\mathbb{K}}M \leq M$. Thus, by definition $m\mathcal{O}_{\mathbb{K}} \leq \mathcal{O}_M$. On the other hand, if $\alpha \in \mathcal{O}_M$, then $\alpha M \subseteq M$ and since M is finitely generated we conclude that α is an algebraic integer. Thus we proved that $\mathcal{O}_M \leq \mathcal{O}_{\mathbb{K}}$, implying that $\mathcal{O}_M$ is a full module.

The module M is finitely generated and $\mathcal{O}_M M \subseteq M$, thus it is a fractional ideal of $\mathcal{O}_M$. Alternatively, letting $0 \neq k \in \mathbb{N}$ such that $I = kM \subseteq \mathcal{O}_M$ we get that $\mathcal{O}_M I \subseteq I$ so $I \trianglelefteq \mathcal{O}_M$ is an ideal, and hence $M = \frac{1}{k}I$ is a fractional ideal of $\mathcal{O}_M$. □

Remark A.6. If M is any order in $\mathbb{K}$, then $M = \mathcal{O}_M$, so any order must be contained in $\mathcal{O}_{\mathbb{K}}$.

We can now define the lattices which correspond to full modules, similar to what we seen with $\mathbb{Z}\left[\sqrt{2}\right]$.

Definition A.7. Let $\mathbb{K}/\mathbb{Q}$ be a totally real extension and $\sigma_1, ..., \sigma_n : \mathbb{K} \to \mathbb{R}$ all the distinct real embeddings. For $\alpha \in \mathbb{K}$ we denote by $v_\alpha = (\sigma_1(\alpha), ..., \sigma_n(\alpha)) \in \mathbb{R}^n$, and if $\alpha \in \mathbb{K}^\times$, then we write $\ln|v_\alpha| = (\ln|\sigma_1(\alpha)|, ..., \ln|\sigma_n(\alpha)|) \in \mathbb{R}^n$. Note that if $Norm(\alpha) := \prod \sigma_i(\alpha) = \pm 1$, then $\sum \ln|\sigma_i(\alpha)| = 0$, so that $\ln|v_\alpha| \in \mathbb{R}^n_0$.

Theorem A.8. *Let M be a full module in $\mathbb{K}$. Then:*

1. *The set $L_M = \{v_\alpha \mid \alpha \in M\}$ is a lattice in $\mathbb{R}^n$.*
2. *The set $L_{\mathcal{O}_M^\times} = \left\{\ln|v_\alpha| \mid \alpha \in \mathcal{O}_M^\times\right\}$ is a lattice in $\mathbb{R}^n_0$.*

Proof.

1. It is well known that $L_{\mathcal{O}_{\mathbb{K}}}$ is a lattice in $\mathbb{R}^n$ (where the covolume squared is the discriminant). By lemma A.3 we can find m_1, m_2 such that $m_1 m_2 \mathcal{O}_{\mathbb{K}} \leq m_1 M \leq \mathcal{O}_{\mathbb{K}}$ so that $L_{m_1 M} = m_1 L_M$ is between $L_{\mathcal{O}_{\mathbb{K}}}$ and $m_1 m_2 L_{\mathcal{O}_{\mathbb{K}}}$, so it must be a lattice in itslef also.

2. By Dirichlet's unit theorem, the set $L_{\mathcal{O}_{\mathbb{K}}^\times}$ is a lattice in $\mathbb{R}^n_0$. While the same proof works for any order, we can also show that $L_{\mathcal{O}_M^\times}$ is a lattice by showing that it has finite index in $L_{\mathcal{O}_{\mathbb{K}}^\times}$. Since $\mathcal{O}_{\mathbb{K}}^\times$ is a finitely generated abelian group, it is enough to show that given $\alpha \in \mathcal{O}_{\mathbb{K}}^\times$, there exists some $m \in \mathbb{N}$ for which $\alpha^m \in \mathcal{O}_M^\times$. This claim is equivalent to saying that $\alpha^m \mathcal{O}_M \subseteq \mathcal{O}_M$. Recall that $[\mathcal{O}_{\mathbb{K}} : \mathcal{O}_M] = k < \infty$ is finite, and there are only finitely many index k subgroups in $\mathcal{O}_{\mathbb{K}}$. Hence by acting on these subgroups with α, we get that there must be some m for which $\alpha^m \mathcal{O}_M = \mathcal{O}_M$, which is what we wanted to show.

□

Finally we want to show that $stab_A(L_M)$ is a lattice in A. If we can show that $L_{\mathcal{O}_M^\times} = stab_A(L_M)$, then we are done. Unfortunately, we work with the positive diagonal subgroup so this is not the case, but it is almost true - elements from $L_{\mathcal{O}_M^\times}$ stabilize L_M up to a multiplication by -1's of some of the coordinates. In order to overcome this problem we need to go down to a finite index subgroup of $L_{\mathcal{O}_M^\times}$.

Definition A.9. An element in $\mathbb{K}$ is called totally positive if $\sigma_i(\alpha) > 0$ for all i. For an order $\mathcal{O}$ we denote by $\mathcal{O}^{\times,+} = \{\alpha \in \mathcal{O}^\times \mid \alpha \text{ is totally positive}\}$. Note that for any $\alpha \in \mathcal{O}^\times$ we have that $\alpha^2 \in \mathcal{O}^{\times,+}$, so that $[L_{\mathcal{O}^\times} : L_{\mathcal{O}^{\times,+}}] \leq 2^{n-1}$.

Lemma A.10. *Let M be a full module. Then the elements in $stab_A(L_M)$ are exactly the diagonal elements which correspond to $L_{\mathcal{O}^{\times,+}}$.*

Proof. Suppose that $a = diag(a_1, ..., a_n)$ satisfies $aL_M = L_M$. Given $0 \neq \beta \in M$, there exists $0 \neq \gamma = \gamma_{a,\beta} \in M$ such that $a \cdot v_\beta = v_\gamma$, implying that $a_i = \frac{\sigma(\beta_i)}{\sigma(\alpha_i)} = \sigma\left(\frac{\beta_i}{\alpha_i}\right)$. We conclude that $a = diag(v_\alpha)$ for some $\alpha = \frac{\gamma}{\beta} \in \mathbb{K}^\times$, and we want to show that $\alpha M = M$. The argument above can be restated as $diag(v_\alpha) \cdot v_\beta = v_{\alpha\beta}$, so that whenever $\beta \in M$ we also have that $\alpha\beta \in M$, hence $\alpha M \subseteq M$. Using the same argument for a^{-1}, we get that $\alpha^{-1} M \subseteq M$, and therefore $\alpha M = M$ (i.e. $\alpha \in \mathcal{O}_M^\times$). The other direction is also true - if we start with $\alpha \in \mathcal{O}_M^\times$ and $\beta \in M$, then $\alpha\beta \in M$ and therefore $diag(v_\alpha) \cdot v_\beta = v_{\alpha\beta} \in M$ so that $diag(v_\alpha) \in stab_A(L_M)$.

We conclude that the stabilizer of L_M in the full diagonal group is exactly $\left\{diag\left(v_\alpha\right) \mid \alpha \in \mathcal{O}_M^\times\right\}$. As we work with the positive diagonal matrices, we get that $stab_A\left(L_M\right) = L_{\mathcal{O}_M^{\times,+}}$ (up to the identification of A with $\mathbb{R}_0^n$). □

Corollary A.11. *For any full module M, the A-orbit AL_M is compact.*

For a lattice L, denote by $\hat{L}$ is normalized unimodular lattice, namely $\hat{L} = \frac{1}{covol(L)^{1/n}}L$. So far we have shown that $M \mapsto A\hat{L}_M$ maps full modules to compact orbits. One reason for two full modules to be sent to the same orbit is if they are equivalent as follows.

Definition A.12. Let M_1, M_2 be two full modules in $\mathbb{K}$. We say that they are equivalent if $M_1 = \alpha M_2$ for some $\alpha \in \mathbb{K}^\times$.

Remark A.13. This equivalence relation is exactly the one used to defined the ideal class group of a field.

Lemma A.14. *If M_1, M_2 are equivalent, then $A\hat{L}_{M_1} = RA\hat{L}_{M_2}$ for some ± 1 diagonal matrix R.*

Proof. Given $\alpha \in \mathbb{K}^\times$ such that $\alpha M_1 = M_2$, it is easy to see that $L_{M_2} = L_{\alpha M_1} = diag\left(v_\alpha\right) L_{M_1}$. Setting $r = |Norm\left(\alpha\right)| = |\det\left(diag\left(v_\alpha\right)\right)|$, the normalization of both sides produces

$$\hat{L}_{M_2} = \left(\frac{1}{r^{1/n}} diag\left(v_\alpha\right)\right) \hat{L}_{M_1}.$$

The matrix $\left(\frac{1}{r^{1/n}} diag\left(v_\alpha\right)\right)$ is diagonal with determinant ± 1, so we can write it as Ra where R is a ± 1 diagonal matrix and $a \in A$, hence $\hat{L}_{M_2} = Ra\hat{L}_{M_1}$, implying that $A\hat{L}_{M_2} = RA\hat{L}_{M_1}$. □

Remark A.15. We can work with $\mathrm{PGL}_n\left(\mathbb{R}\right)$ instead of $\mathrm{SL}_n\left(\mathbb{R}\right)$, to overcome the inconvenience of ± 1 diagonal matrices, but then of course we need to work with equivalence class of matrices.

Finally, we want to show that up to these ± 1 diagonal matrices, the map $[M] \mapsto A\hat{L}_M$ from equivalence classes of full modules to compact orbits is a bijection.

Theorem A.16. *Let Ax be a compact A-orbit. Then there is a unique totally real extension $\mathbb{K}/\mathbb{Q}$ such that $Ax = A\hat{L}_M$ for some full module M in $\mathbb{K}$. Moreover, this module is determined up to equivalence.*

Proof. If we knew that $Ax = A\hat{L}_M$ for a full module M in $\mathbb{K}$, then $stab_x\left(A\right) \cong L_{\mathcal{O}_M^{\times,+}}$. For any $a \in stab_x\left(A\right)$ we have $a_{i,i} = \sigma_i\left(a_{1,1}\right)$ (assuming that $\sigma_1 = Id$), hence the same holds for $\mathbb{L} = alg_{\mathbb{Q}}\left(stab_A\left(\hat{L}_M\right)\right)$. In particular, the map $a \mapsto a_{1,1}$ from $\mathbb{L}$ to $\mathbb{K}$ is injective, namely up to this embedding $\mathbb{L} \leq \mathbb{K}$. If $0 \neq \alpha \in \mathbb{L} \leq \mathbb{K}$, then α is algebraic so that $\mathbb{Q}\left(\alpha\right) = \mathbb{Q}\left[\alpha\right] \leq \mathbb{L}$, hence $\alpha^{-1} \in \mathbb{L}$ also so that $\mathbb{L}$ is actually a field. Moreover, it contains $\mathcal{O}_M^\times$ which is an $n-1$ dimensional group of algebraic units, hence $\mathbb{L}/\mathbb{Q}$ must be of degree at least $n = [\mathbb{K} : \mathbb{Q}]$, so we must have equality $\mathbb{L} = \mathbb{K}$.

With this in mind, let us start with a general compact orbit Ax and show that $\mathbb{L} = alg_{\mathbb{Q}}\left(stab_A\left(x\right)\right)$ is a totally real extension of dimension n over $\mathbb{Q}$. Consider first the unital ring $\mathcal{O} = span_{\mathbb{Z}}\left(stab_A\left(x\right)\right)$ which is contained in the set of digaonal matrices so in particular it is commutative. Identifying x with its corresponding lattice in $\mathbb{R}^n$, we see that it doesn't have any nonzero vectors with zero entries, since otherwise Ax wouldn't be bounded. In particular, if $0 \neq a \in \mathcal{O}$, then $\{0\} \neq ax \subseteq x$ hence a doesn't have zero entries on the diagonal, implying that $\mathcal{O}$ doesn't have zero divisors.

Write $x = g\mathbb{Z}^n$ for some $g \in \mathrm{SL}_n(\mathbb{R})$. If $0 \neq a \in \mathcal{O}$, then $ax \subseteq x$ so that $ag = g\gamma_a$ for some $0 \neq \gamma_a \in M_n(\mathbb{Z})$, implying that γ_a is diagonalizable where the diagonal entries of a are its eigenvalues and the rows of g are the eigenvectors. In particular, the diagonal elements of a are algebraic numbers of degree at most n. Let $a \in \mathcal{O}$ and let $f \in \mathbb{Z}[x]$ be the minimal polynomial for $a_{1,1}$. Since $f(a)_{1,1} = 0$ and $f(a) \in \mathcal{O}$, by the previous paragraph $f(a) = 0$. Writing $f(x) = x^d + \sum_0^{d-1} b_i x^i$, $b_i \in \mathbb{Z}$, and using the fact that $b_0 \neq 0$ (f is minimal), we get that $a \cdot \frac{-1}{b_0}\left(a^{d-1} + \sum_1^{d-1} b_i a^{i-1}\right) = 1$, so that a is invertible in $\mathbb{L} = \mathbb{Q}\mathcal{O}$. Since any element in $\mathbb{L}$ has the form $\frac{1}{m}a$ for some $a \in \mathcal{O}$ we get that $\mathbb{L}$ is an algebraic field extension of $\mathbb{Q}$.

The elements of $\mathcal{O}$ are algebraic integers so that $\mathcal{O} \leq \mathcal{O}_{\mathbb{L}}$. Furthermore $stab_A(x)$ is a subgroup of $\mathcal{O}^\times$ of rank $n-1$, so we must have that $[\mathbb{L} : \mathbb{Q}] \geq n$. On the other hand, the elements in $\mathcal{O}$ have degree at most n, hence $[\mathbb{L} : \mathbb{Q}] \leq n$, so there is equality.

To summarize, we proved that $\mathbb{L}/\mathbb{Q}$ must be a totally real extension of degree n, and $\mathcal{O}$ is an order in $\mathbb{L}$. Next we want to show that $x = a\hat{L}_M$ for some full module in $\mathbb{L}$ (and actually $\mathcal{O} = \mathcal{O}_M$).

As before, the map $a \mapsto a_{1,1}$ is injective (its domain is a field), so we can identify $\mathbb{L}$ with its restriction to the top left elements. Let $a \in \mathcal{O}$ be of degree n (namely $a_{1,1}$ is of degree n) so that and write $ag = g\gamma_a$ with $0 \neq \gamma_a \in M_n(\mathbb{Z})$. Since $\gamma_a - a_{1,1}I$ is singular, we can find a vector $v = (\alpha_1, ..., \alpha_n) \in \mathbb{Q}(a_{1,1})^n = \mathbb{L}^n$ such that $a_{1,1}v = v\gamma_a$. If $\sigma_i : \mathbb{L} \to \mathbb{R}$ are the distinct real embeddings of $\mathbb{L}$, then $\sigma_i(a_{1,1})\sigma_i(v) = \sigma_i(v)\gamma_a$ where all the $\sigma_i(a_{1,1})$ are distinct. It follows that (up to permutation of indices) we must have that $a_{i,i} = \sigma_i(a_{1,1})$ and the rows of g are $r_i\sigma_i(v)$ where $r_i \in \mathbb{R}^\times$ (since γ_a has n distinct eigenvalues and each eigenspace is one dimensional). In particular, if $M = span_{\mathbb{Z}}\{\alpha_1, ..., \alpha_n\}$ is the full module in $\mathbb{L}$, then $g\mathbb{Z}^n = diag(r_1, ..., r_n) L_M$, hence $Ax = A\hat{L}_M$. □

References

[1] N Akhmedov, N. "On the representation of matrices in the DOTU form (in connection with Minkowski's nonhomogeneous problem)." Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst 67 (1977): 86-94. On the representation of matrices in the DOTU form (in connection with Minkowski's nonhomogeneous problem). *Zap. Nauchn. Sem. Leningr. Otd. Mat. Inst*, 67:86–94, 1977.

[2] B. J. Birch and H. P. F. Swinnerton-Dyer. On the inhomogeneous minimum of the product of n linear forms. *Mathematika*, 3(1):25–39, June 1956.

[3] Jean-Paul Cerri. Inhomogeneous and Euclidean spectra of number fields with unit rank strictly greater than 1. *Journal fur die reine und angewandte Mathematik (Crelles Journal)*, 2006(592):49–62, 2006.

[4] David A. Clark. A quadratic field which is Euclidean but not norm-Euclidean. *Manuscripta Math*, 83(1):327–330, December 1994.

[5] E.S. Golod and I.R. Shafarevich. On the class field tower. *Izv. Akad. Nauk SSSR Ser. Mat.*, 28(2):261–272.

[6] R. J. Hans-Gill, Madhu Raka, and Ranjeet Sehmi. On conjectures of Minkowski and Woods for n=7. *Journal of Number Theory*, 129(5):1011–1033, May 2009.

[7] R. J. Hans-Gill, Madhu Raka, and Ranjeet Sehmi. On conjectures of Minkowski and Woods for n=8. *Acta Arithmetica*, 147:337–385, 2011.

[8] Leetika Kathuria and Madhu Raka. On Conjectures of Minkowski and Woods for n=9. *arXiv:1410.5743 [math]*, October 2014. arXiv: 1410.5743.

[9] A. M. Macbeath. Factorization of Matrices and Minkowski's Conjecture. *Glasgow Mathematical Journal*, 5(2):86–89, July 1961.

[10] Curtis McMullen. Minkowskis conjecture, well-rounded lattices and topological dimension. *J. Amer. Math. Soc.*, 18(3):711–734, 2005.

[11] Kh N. Narzullaev. Minkowskis conjecture on a system of linear inhomogeneous forms. *Mathematical Notes of the Academy of Sciences of the USSR*, 5(1):66–72, January 1969.

[12] Kh N. Narzullaev. Representation of unimodular matrices in the form DOTU for n=3. *Mathematical Notes of the Academy of Sciences of the USSR*, 18(2):713–719, August 1975.

[13] Oded Regev, Uri Shapira, and Barak Weiss. Counterexamples to a conjecture of Woods. *Duke Math. J.*, 166(13):2443–2446, September 2017.

[14] Uri Shapira and Barak Weiss. Stable lattices and the diagonal group. *J. Eur. Math. Soc.*, 18(8):1753–1767, June 2016.

[15] Omri N. Solan. Intersections of diagonal orbits. *arXiv:1612.08765 [math]*, December 2016. arXiv: 1612.08765.

[16] A. C. Woods. Covering six space with spheres. *Journal of Number Theory, vol. 4, no. 2, pp. 157-180*, 4:157–180, April 1972.