Integral bases

Trung Nguyen

April 16, 2021

1 Introduction

It was a great breakthrough in algebraic number theory when Minkowski realized that certain geometric ideas are very powerful in dealing with arithmetic problems. He was able to prove that in a number field K of degree n, every ideal class in a number ring can be represented by an ideal with norm less than a constant multiple of $\sqrt{\Delta}$, where Δ is the discriminant of the number ring. His proof relies on two crucial ideas. First, the natural embedding $K \mapsto \mathbb{R}^n$ allows us to regard the ring of integer R as a lattice in $\mathbb{R}^n$ whose fundamental parallelotope F has volume a constant multiple of $\sqrt{\Delta}$. Second, a lattice in $\mathbb{R}^n$ contains a nonzero lattice point in a convex, measurable, centrally symmetric subset of $\mathbb{R}^n$, as long as the volume of the set is larger than 2^n times the volume of the fundamental parallelotope of the lattice.

The motivation for this paper is a partial converse to Minkowski's first idea. He showed that given a basis for a number ring, we have a set of volume a constant multiple of $\sqrt{\Delta}$ that contains the image of the basis under the natural embedding $K \mapsto \mathbb{R}^n$. We will show that in poly-quadratic field K, there exists a set with volume a constant multiple of Δ that does not contain the image of any integral basis under the natural map $K \mapsto \mathbb{R}^n$.

Theorem 1 *Consider a poly-quadratic extension* $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_n})$ *where all of* $m_1, m_2, ..., m_n$ *are positive and pairwise coprime. Then there exists a convex, measurable, centrally symmetric subset* E *of* $\mathbb{R}^n$ *with volume a constant multiple of* Δ *that does not contain the image under the natural embedding* $K \mapsto \mathbb{R}^n$ *of any integral basis for the number ring* R *of* K*.*

Theorem 2 *Consider a poly-quadratic extension* $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_n})$ *where not all of* $m_1, m_2, ..., m_n$ *are positive and* $m_1, m_2, ..., m_n$ *are pairwise coprime. Then there exists a convex, measurable, centrally symmetric subset* E *of* $\mathbb{R}^n$ *with volume a constant multiple of* Δ *that does not contain the image under the natural embedding* $K \mapsto \mathbb{R}^n$ *of any integral basis for the number ring* R *of* K*.*

2 Preliminaries

First, we would like to state explicitly the definition of the natural embedding $K \mapsto \mathbb{R}^n$.

Definition 1 *Let K be a number field with real embeddings $\sigma_1, \sigma_2, ..., \sigma_r$, and $\tau_1, \bar{\tau}_1, ..., \tau_s, \bar{\tau}_s$ as the remaining embeddings of $K \mapsto \mathbb{C}$. Thus, $r + 2s = n$. A mapping $K \mapsto \mathbb{R}^n$ is obtained by sending each α in K to the n-tuple $\big(\sigma_1(\alpha)$,..., $\sigma_r(\alpha)$,$Re(\tau_1(\alpha))$, $Im(\tau_1(\alpha))$,..., $Re(\tau_s(\alpha))$, $Im(\tau_s(\alpha))$ $\big)$*

The first step of proving the theorems is to find the Galois group of K. In order to do so, we first need the degree of $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_n})$. As we would expect, the degree is 2^n.

Lemma 1 *Let K be a field, a and b are elements of K. Then the field $L = K[\sqrt{a}, \sqrt{b}]$ has degree 4 over K if and only if $\sqrt{a}$, $\sqrt{b}$ and $\sqrt{ab}$ are not elements of K.*

Proof. Assume the field L has degree 4 over K. Notice that $K' = K[\sqrt{a}]$ is a subfield of L such that $L = K'[\sqrt{b}]$. Thus, $[L : K] = [L : K'][K' : K] \leq 2.2 = 4$. This forces $[K' : K]$ to be 2, or equivalently $\sqrt{a}$ is not in K. The proofs for $\sqrt{b}$ and $\sqrt{ab}$ are similar.

Conversely, suppose $\sqrt{a}$, $\sqrt{b}$ and $\sqrt{ab}$ are not elements of K. Then certainly $K' = K[\sqrt{a}]$ is an extension field of degree 2 over K, so it suffices to show that L is an extension field of degree 2 over $K[\sqrt{a}]$, as then we would have $[L : K] = [L : K[\sqrt{a}]][K[\sqrt{a}] : K] = 4$. Indeed, we rewrite L as $K'[\sqrt{b}]$. If $[L : K']$ is not 2, then we would have that $K'[\sqrt{b}] = L = K'$. This in turn implies that $\sqrt{b}$ is an element of $K' = K[\sqrt{a}]$. Hence we see that there exists some x, y in K such that:

$$\sqrt{b} = x + y\sqrt{a}$$

Squaring both sides and rearrange the terms we have:

$$(b - x^2 - y^2a).1 - (2xy\sqrt{a}) = 0 \tag{1}$$

Recall that $K[\sqrt{a}]$ is an extension field of degree 2 over K, so 1 and $\sqrt{a}$ are linearly independent over K. This implies that the coefficient of $\sqrt{a}$ in (1), xy, must be 0. If $x = 0$, then we have that $\sqrt{b} = y\sqrt{a}$. This implies $\sqrt{ab} = ya$, an element of K, a contradiction. If $y = 0$, then we have that $\sqrt{b} = x$, an element of K, a contradiction. Hence we have that $[L : K'] = 2$, which is exactly what we want.

With the help of lemma 1, we can now find the degree of our poly-quadratic extension field K.

Proposition 1 *Let $a_1, a_2, ..., a_n$ be n distinct, square free integers. Let $K = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_n})$. Then K has degree 2^n over $\mathbb{Q}$ if and only if $\prod_{k \in I} a_i$ is not a perfect square, for all subset I of {1,2,. . . , n}*

Proof. Suppose that K has degree 2^n over $\mathbb{Q}$, and $\prod_{k\in I} a_i$ is a square for some I. Relabel the a_i's if necessary, we can assume that $a_1a_2...a_k = c^2$ for some integer c. Taking the square root of both sides we have:

$$\sqrt{a_1} = \frac{c}{\sqrt{a_2...a_k}}.$$

This implies that $\mathbb{Q}(\sqrt{a_1}) \subset \mathbb{Q}(\sqrt{a_2}, \sqrt{a_3}, ..., \sqrt{a_k}) \subset \mathbb{Q}(\sqrt{a_2}, \sqrt{a_3}, ..., \sqrt{a_n})$. Thus, $K = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_n}) = \mathbb{Q}(\sqrt{a_2}, \sqrt{a_3}, ..., \sqrt{a_n})$. Then K has degree at most 2^{n-1} over $\mathbb{Q}$, a contradiction.

Conversely, suppose that $\prod_{k\in I} a_i$ is not a perfect square, for all subset I of $\{1,2,\dots, n\}$. We will show by induction on n that K has degree 2^n over $\mathbb{Q}$. The base case $n = 1$ is trivial, and the case $n = 2$ is our lemma 1.

Now suppose the proposition is true for all $k \leq (n-1)$. The inductive hypothesis gives us that $K_0 = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_{n-2}})$ has degree 2^{n-2} over $\mathbb{Q}$. Notice that $K = K_0[\sqrt{a_{n-1}}, \sqrt{a_n}]$, so we would be done if we are able to show that $[K : K_0] = 4$. By lemma 1, this is true if $\sqrt{a_{n-1}}$, $\sqrt{a_n}$, and $\sqrt{a_{n-1}a_n}$ are not in K_0.

However, again by induction, $\mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_{n-1}})$ has degree 2^{n-1} over $\mathbb{Q}$, so $\sqrt{a_{n-1}}$ cannot be in $K_0 = \mathbb{Q}(\sqrt{a_1}, \sqrt{a_2}, ..., \sqrt{a_{n-2}})$, as we know K_0 only has degree 2^{n-2} over $\mathbb{Q}$. With a similar reasoning as above, we can also see that $\sqrt{a_n}$ and $\sqrt{a_{n-1}a_n}$ are not in K_0. Now we can apply lemma 1 to show that $[K : K_0] = 4$.

Remark 1 *With the help of this proposition, we can see that $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_n})$ where $m_1, m_2, ..., m_n$ are relatively prime, is a number field of degree 2^n over $\mathbb{Q}$.*

Remark 2 *One interesting corollary of this proposition is that the degree of $K = \mathbb{Q}(\sqrt{p_1}, \sqrt{p_2}, ..., \sqrt{p_n})$ where $p_1, p_2, ..., p_n$ are primes, is 2^n.*

Remark 3 *The Galois group G of $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_n})$ where $m_1, m_2, ..., m_n$ are relatively prime must have order 2^n, and hence $Gal(K/\mathbb{Q}) \cong \prod_{i=1}^{n} Gal(\mathbb{Q}(\sqrt{m_i})/\mathbb{Q}) \cong (\mathbb{Z}/2\mathbb{Z})^n$.*

Continue to let $m_1, \dots, m_n$ be integers such that they are pairwise co-prime.

Let o_K be the ring of integers for a number field K. Let K denote the poly-quadratic extension $\mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_n})$ and K^i denote the extension $(\sqrt{m_1}, \dots, \sqrt{m_{i-1}}, \sqrt{m_{i+1}}, \dots, \sqrt{m_n})$. Then by proposition 1, we see that $[K : \mathbb{Q}] = 2^n = d_n$. Let

$$O_K := \mathbb{Z}1+\mathbb{Z}\sqrt{m_1}+\cdots+\mathbb{Z}\sqrt{m_1m_2}+\cdots+\mathbb{Z}\sqrt{m_im_j}+\cdots+\mathbb{Z}\sqrt{m_{i_1}m_{i_2}\cdots m_{i_k}}+\cdots+\mathbb{Z}\sqrt{m_1m_2\cdots m_n}$$

where $0 \leq i_1, i_2, \dots i_k \leq n$, $i \neq j$, $i_r \neq i_s$. O_K consists of $\mathbb{Z}$-linear combinations of square roots of all possible combinations of products of $m_1, \dots, m_n$ with each appearing at most once (there are 2^n of them). We immediately see that $O_K \subseteq o_K$. Also, since m_i are pairwise co-prime, the products under the square root are square-free and these specifically correspond to the 2^n quadratic subfields of K.

Proposition 2 *For any polyquadratic extension $K = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_n})$ where $m_1, m_2, ..., m_n$ are pairwise coprime,*

$$O_K \subseteq o_K \subseteq O_K/d_n$$

where $d_n = [K : \mathbb{Q}] = 2^n$.

Proof. We know that if $K \subseteq L$ are number fields and $\alpha \in o_L$ then $Tr_{L/K}(\alpha) \in o_K$. Let $\alpha \in o_{K_n}$. Then,

$$\alpha = a_1 + a_2\sqrt{m_1} + \cdots + a_{n+2}\sqrt{m_1 m_2} + \cdots + a_s\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}} + \cdots a_{2^n}\sqrt{m_1 m_2 \cdots m_n}$$

where $a_i \in \mathbb{Q}$ since these form a basis of K over $\mathbb{Q}$. Now, consider $\beta_1 = Tr_{K/K^1}(\alpha)$ where $K^1 = \mathbb{Q}(\sqrt{m_2}, \ldots \sqrt{m_n})$, as above.

We have that $Tr_{K/K^1}(\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}}) = \begin{cases} 0 & \text{if } m_{i_j} = m_1 \text{ for any } 1 \leq j \leq k, \\ 2\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}} & \text{if } m_{i_j} \neq m_1 \text{ for any } 1 \leq j \leq k \end{cases}$

Therefore, it follows that

$$\beta_1 = 2a_1 + a_2 \cdot 0 + 2a_3\sqrt{m_2} + \cdots + a_{n+2} \cdot 0 + \cdots + a_{2^n} \cdot 0 \tag{2}$$

By induction hypothesis, we have that $\beta_1 \in o_{K^1} \subseteq O_{K^1}/d_{n-1} = O_{K^1}/2^{n-1} \subseteq O_K/2^{n-1}$ since $O_{K^1} \subseteq O_K$. Let a_s be the coefficient of a term $\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}}$ in α which does not contain m_1, for example $\sqrt{m_2 m_3}$. Then, $\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}} \in O_{K^1}$ and from equation (2), it follows that $2a_s \in \mathbb{Z}/2^{n-1}$, or $a_s \in \mathbb{Z}/2^n$.

Now, for all such $\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}}$ where $0 \leq i_1, i_2, \ldots i_k \leq n,\ i \neq j,\ i_r \neq i_s$ except $\sqrt{m_1 m_2 \cdots m_n}$, there is at least one m_t, $1 \leq t \leq n$ such that $m_{i_j} \neq m_t$ for any $1 \leq j \leq k$. Thus by varying i over $1 \leq i \leq n$ and considering $Tr_{K/K^i}(\alpha)$, we get that $a_s \in \mathbb{Z}/2^n$ for all $1 \leq s \leq 2^n - 1$, similarly as above. So, we are only left to prove the claim for a_{2^n}, the coefficient of $\sqrt{m_1 m_2 \cdots m_n}$.

To prove this, we consider $\gamma = Tr_{K/L}(\alpha)$, with $L = \mathbb{Q}[\sqrt{m_1}, \sqrt{m_2}, ..., \sqrt{m_{n-1} m_n}]$. Let $< \sigma >= (K/L)$ where σ maps $\sqrt{m_{n-1}} \mapsto -\sqrt{m_{n-1}}$, $\sqrt{m_n} \mapsto -\sqrt{m_n}$ and acts as identity on everything else. Then, $Tr_{K/L}(\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}}) =$ $\begin{cases} 0 & \text{if } \sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}} \text{ contains either } m_{n-1} \text{ or } m_n \text{ but not both,} \\ 2\sqrt{m_{i_1} m_{i_2} \cdots m_{i_k}} & \text{otherwise} \end{cases}$

Thus,

$$\gamma = Tr_{K/L}(\alpha) = 2a_1 + a_2\sqrt{m_1} + \cdots + 2a_{2^n}\sqrt{m_1 m_2 \cdots m_n}$$

and again by induction hypothesis we see that $2a_{2^n} \in \mathbb{Z}/2^{n-1}$, since $\gamma \in o_L \subseteq O_L/2^{n-1} \subset O_K/2^{n-1}$. This implies that $a_{2^n} \in \mathbb{Z}/2^n$ and this completes our proof.

We finally have,

$$O_K \subseteq o_K \subseteq O_K/d_n$$

where $d_n = [K : \mathbb{Q}] = 2^n$, for any poly-quadratic extension $K = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_n})$ where m_i are relatively prime.

The bound $d_n = 2^n$ is the best possible one in the case when $m_1, m_2, ..., m_n$ are congruent to $1(mod 4)$. In order to prove this, we will state without proof a lemma:

Lemma 2 *Let K and L be number fields with ring of integers R and S, respectively. Let T be the ring of intergers of the compositum KL. Assume that disc R and disc S are relatively prime. Then $T = RS$ and disc $T =$ disc $R^{[L:\mathbb{Q}]}$ disc $S^{[K:\mathbb{Q}]}$*

This is proposition 12 and Exercise 23 in Marcus, Number fields.

Now let $K_i = \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_i})$. We know that each K_i is Galois over $\mathbb{Q}$ and we have the tower of fields

$$K_0 = \mathbb{Q} \subset K_1 \subset K_2 \subset \cdots \subset K_n,$$

where $[K_i : \mathbb{Q}] = 2^i$ for all $0 \leq i \leq n$. We observe that $K_{i+1} = K_i\mathbb{Q}(\sqrt{m_{i+1}})$ for all $0 \leq i < n$ and $K_i \bigcap \mathbb{Q}(\sqrt{m_{i+1}}) = \mathbb{Q}$ since m_i are relatively prime.

Let $L_i = \mathbb{Q}(\sqrt{m_i})$. Now, we know that $\Delta_{L_i} = m_i$ and from this we can find the discriminant of K_i for all $1 \leq i \leq n$. Thus, we see that $\Delta_{K_1} = m_1$ and $(\Delta_{K_1}, \Delta_{L_2}) = 1$ which gives $\Delta_{K_2} = (\Delta_{K_1})^2 \cdot (\Delta_{L_2})^2 = (\Delta_{L_1} \cdot \Delta_{L_2})^2$. Proceeding inductively, it follows that $(\Delta_{K_{i-1}}, \Delta_{L_i}) = 1$ and $\Delta_{K_i} = (\Delta_{K_{i-1}})^2 \cdot (\Delta_{L_i})^{2^{i-1}}$ for all $2 \leq i \leq n$. So, we get

$$\Delta_{K_i} = (\Delta_{K_{i-1}})^2 \cdot (\Delta_{L_i})^{2^{i-1}} = \left((\Delta_{K_{i-2}})^2 \cdot (\Delta_{L_{i-1}})^{2^{i-2}}\right)^2 (\Delta_{L_i})^{2^{i-1}} = \cdots = \left(\prod_{k=1}^{i} \Delta_{L_k}\right)^{2^{i-1}} = (\prod_{k=1}^{i} m_k)^{2^{i-1}}$$

Thus, we can see that $(\Delta_{K_i}, \Delta_{L_{i+1}}) = 1$.

Since $(\Delta_{K_{i-1}}, \Delta_{L_i}) = 1$, $K_1 = L_1$ and we know the integral basis of each L_i, inductively using lemma 2, we can find an integral basis for K_i by multiplying pairwise the integral basis of K_{i-1} and L_i. Let B_i be the integral basis of K_i. Then we see that

$$B_1 = \left\{1, \frac{1+\sqrt{m_1}}{2}\right\}, \quad B_2 = \left\{1, \frac{1+\sqrt{m_1}}{2}, \frac{1+\sqrt{m_2}}{2}, \left(\frac{1+\sqrt{m_1}}{2}\right) \cdot \left(\frac{1+\sqrt{m_2}}{2}\right)\right\}$$

and inductively it follows that

$$B_n = \left\{1, \frac{1+\sqrt{m_1}}{2}, \frac{1+\sqrt{m_2}}{2}, \ldots, \left(\frac{1+\sqrt{m_1}}{2}\right) \cdot \left(\frac{1+\sqrt{m_2}}{2}\right), \ldots, \prod_{k=1}^{n} \left(\frac{1+\sqrt{m_k}}{2}\right)\right\}$$

We see that the last element of the integral basis of K_n is $\frac{1}{2^n} \prod_{k=1}^{n} \left(1 + \sqrt{m_k}\right) = e$(say) and $e \in O_{K_n}/2^n$. Thus, we see that the bound is sharp for this case.

Lemma 3 *Let $\mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \cdots, \sqrt{m_n})$ be an extension of degree 2^n over $\mathbb{Q}$. Then this extension can be rewritten as $\mathbb{Q}(\sqrt{x_1}, \sqrt{x_2}, \cdots, \sqrt{x_n})$ where at least $n-2$ of the x_i are $1(mod 4)$.*

Proof. By the finiteness of the extension, we can assume that $\mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_n})$ is written such that the maximal number of $m_i \equiv 1 \pmod 4$. Also, we assume for the purpose of contradiction that there are three $m_i \not\equiv 1 \pmod 4$. We will call them m_1, m_2, m_3.

If two of these, WLOG, m_1 and m_2 are 3 mod 4, then

$$m = \frac{m_1 m_2}{(m_1, m_2)^2} \equiv 1 \pmod 4$$

since the both the numerator and denominator will be 1 mod 4. Note that we could write the extension as

$$\mathbb{Q}(\sqrt{m}, \sqrt{m_2}, \sqrt{m_3}, \ldots, \sqrt{m_n})$$

and that this extension would have more roots that are 1 mod 4, contradicting our assumption of maximality.

If two of these, WLOG, m_1 and m_2 are 2 mod 4 such that $m_1/2 \equiv m_2/2 \pmod 4$, then $m \equiv 1 \pmod 4$ where m is defined as above and the same contradiction would result.

In the last case, WLOG, we can assume that $m_1 \equiv 3 \pmod 4$ and $m_2, m_3 \equiv 2 \pmod 4$ such that $m_2/2 \not\equiv m_3/2 \pmod 4$. Let m be defined as above and note that $m \equiv 3 \pmod 4$. Additionally,

$$k = \frac{m_2 m_3}{(m_2, m_3)^2} \equiv 3 \pmod 4$$

Thus, we can rewrite our extension as

$$\mathbb{Q}(\sqrt{m}, \sqrt{k}, \sqrt{m_3}, \ldots, \sqrt{m_n})$$

where $m \equiv k \equiv 3 \pmod 4$ which puts us back in the first case and results in a contradiction. This completes all possible cases. Therefore, the extension can be written such that at least $n-2$ of the square roots are 1 mod 4.

Corollary 1 *Let $L = \mathbb{Q}(\sqrt{m_1}, \ldots \sqrt{m_n})$. Then there exists an element of o with denominator greater than or equal to 2^{n-1}.*

Proof. From the lemma 3, we write

$$L = \mathbb{Q}(\sqrt{x_1}, \sqrt{x_2})(\sqrt{m_1}, \ldots, \sqrt{m_{n-2}})$$

where each $m_i \equiv 1 \pmod 4$, $x_1, x_2 \not\equiv 1 \pmod 4$. Note that (x_1, x_2) has an element in the ring of integers with denominator 2. Adjoining the other $n-2$ roots which are all 1 mod 4 one at a time and as we have seen in the discussion after proposition 2, we have that there exists an element in the ring of integers with denominator 2^{n-1} since every adjoined root that is 1 mod 4 has been shown to increase the denominator of some term by 2.

Remark 4 *This corollary shows that the bound $d_n = 2^n$ is very close to be optimal.*

In order to find the discriminant, we assume the following proposition that can be deduced from the conductor-discriminant formula of class field theory.

Proposition 3 *Let K be a poly-quadratic extension of $\mathbb{Q}$. Then the discriminant of K equals the product of the discriminants of all quadratic subfields of K.*

Using the proposition above, we will prove

Proposition 4 *Let $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2}, \cdots, \sqrt{m_n})$ with m_i distinct and relatively prime, $n \geq 3$. Then $\Delta_K = c(m_1 m_2 \cdots m_n)^{2^{n-1}}$ where c is a constant depending only on n. Indeed, c equals one of $1, 16^{2^{n-2}}, 64^{2^{n-2}}$.*

Proof. Since the m_i are coprime, there can only at most one m_i that is $2(mod 4)$.
Case 1: there is no m_i that is $2(mod 4)$.

Suppose among n integers $m_1, m_2, ..., m_n$, we have k numbers congruent to 1 mod 4, and $n-k$ numbers congruent to 3 mod 4. According to proposition 3, we know that discriminant of K equals the product of the discriminant of $\mathbb{Q}(m_I)$, where $I \subset \{1, 2, \ldots, n\}$. We also know that the discriminant of $\mathbb{Q}(m)$ equals m when m is 0 or 1 mod 4, and it equals $4m$ when m is 2 or 3 mod 4. Hence, we have that

$$\Delta_K = 4^t \prod_{I \subset \{1,2,\ldots,n\}} m_I$$

where t is the number of subsets I such that m_I is not congruent to 1 mod 4.

Note that m_I is congruent to 3 mod 4 if and only if m_I contains an odd number of m_i that is congruent to 3 mod 4. Thus, the number of such subsets I is equal to the number of subsets of $\{m_1, m_2, \ldots, m_n\}$ that contains an odd number of m_i that is congruent to 3 mod 4. That number is

$$2^{n-k}(\binom{k}{1} + \binom{k}{1} + ...) = 2^{k-1}2^{n-k} = 2^{n-1}$$

Thus,

$$\Delta_K = 4^{2^{n-1}} \prod_{I \subset \{1,2,\ldots,n\}} m_I = 4^{2^{n-1}}(m_1 m_2 \cdots m_n)^{2^{n-1}}$$

Case 2: there is one m_i that is $2(mod 4)$,say m_1. As above, we still have that

$$\Delta_K = 4^t \prod_{I \subset \{1,2,\ldots,n\}} m_I$$

where t is the number of subsets I such that m_I is not congruent to 1 mod 4. Note that m_I is not congruent to 1 mod 4 if and only if m_I contains m_1 or m_I contains an odd number of m_i that is congruent to 3 mod 4 without containing m_1. In the first case, the number of such subsets I is 2^{n-1}, in the second case the number of such subsets is 2^{n-2}. Thus, in total, we have 3.2^{n-2} such sets I. Hence

$$\Delta_K = 4^{3.2^{n-2}} \prod_{I \subset \{1,2,\ldots,n\}} m_I = 64^{2^{n-2}} (m_1 m_2 \cdots m_n)^{2^{n-1}}$$

Now we are ready to prove the main theorems.

3 Totally real poly-quadratic fields

In this section, we will construct a set having volume a constant multiple of the discriminant and not having the image under the Minkowski embedding defined in section 1 of any integral basis of a poly-quadratic field generated by square roots of relatively prime positive integers.

By propositiiton 4, $\Delta K = c(m_1 m_2 \cdots m_n)^{2^{n-1}}$ where c is a constant depending on n. Also, recall that the image of any integral basis under the Minkowski embedding is a $\mathbb{R}$-basis for $\mathbb{R}^n$.

We construct the set for a biquadratic extension($n = 2$), and then extend the same idea to poly-quadratic extensions.

Let $K = \mathbb{Q}(\sqrt{m_1}, \sqrt{m_2})$. Consider the $\mathbb{Z}$-module O_K/d_2 and the lattice L_O generated by the Minkowski embedding of O_K/d_2.

Consider

$$L_O = \frac{\mathbb{Z}}{d_2}(1,1,1,1) + \frac{\mathbb{Z}}{d_2}(\sqrt{m_1}, -\sqrt{m_1}, \sqrt{m_1}, -\sqrt{m_1}) + \frac{\mathbb{Z}}{d_2}(\sqrt{m_2}, \sqrt{m_2}, -\sqrt{m_2}, -\sqrt{m_2})$$
$$+ \frac{\mathbb{Z}}{d_2}(\sqrt{m_1 m_2}, -\sqrt{m_1 m_2}, -\sqrt{m_1 m_2}, \sqrt{m_1 m_2})$$

and

$$L_O^i = \frac{\mathbb{Z}}{d_2}(1,1,1,1) + \frac{\mathbb{Z}}{d_2}(\sqrt{m_1}, -\sqrt{m_1}, \sqrt{m_1}, -\sqrt{m_1}) + \frac{\mathbb{Z}}{d_2}(\sqrt{m_2}, \sqrt{m_2}, -\sqrt{m_2}, -\sqrt{m_2})$$
$$+ \frac{i}{d_2}(\sqrt{m_1 m_2}, -\sqrt{m_1 m_2}, -\sqrt{m_1 m_2}, \sqrt{m_1 m_2}), \qquad i \in \mathbb{Z}$$

So, we see that $L_0 = \bigcup_{i \in \mathbb{Z} L_O^i}$. For $x = (x_1, x_2, x_3, x_4)$, define $f(x) = x_1 - x_2 - x_3 + x_4$. If $x \in L_O^i$ we see that x satisfies the equation

$$f(x) = x_1 - x_2 - x_3 + x_4 = \frac{d_2 \cdot i}{d_2}\sqrt{m_1 m_2} = i\sqrt{m_1 m_2} \tag{3}$$

Consider the convex centrally symmetric compact set $C = [-\frac{\sqrt{m_1 m_2}}{2d_2}, \frac{\sqrt{m_1 m_2}}{2d_2}]^{d_2}$ in $\mathbb{R}^{d_2}$. We know that $\Delta_K \asymp (m_1 m_2)^2$ and we see that $Vol(C) = \frac{1}{d_2^{d_2}}(m_1 m_2)^2 \asymp (m_1 m_2)^2 \asymp \Delta_K$.

Now, if there exists $x \in L_O^i \bigcap C$ for $i \neq 0$, then we have

$$\sqrt{m_1 m_2} \le |i\sqrt{m_1 m_2}| = |f(x)| = |x_1 - x_2 - x_3 + x_4| \le |x_1| + |x_2| + |x_3| + |x_4| \le \frac{\sqrt{m_1 m_2}}{2}$$

which is a contradiction.

Thus, $L_O^i \bigcap C = \phi$ for $i \neq 0$ and C can contain points from only L_O^0 and hence,

$L_O \bigcap C \subset L_O^0 \subset \frac{\mathbb{R}}{d_2}(1,1,1,1)+\frac{\mathbb{R}}{d_2}(\sqrt{m_1},-\sqrt{m_1},\sqrt{m_1},-\sqrt{m_1})+\frac{\mathbb{R}}{d_2}(\sqrt{m_2},\sqrt{m_2},-\sqrt{m_2},-\sqrt{m_2})$, which is a d_2-1 dimensional $\mathbb{R}$ vector space and hence cannot contain d_2 $\mathbb{R}$-linearly independent elements.

Now, let L be the lattice formed using the Minkowski embedding of the ring of integers o_K of K. Since we have $o_K \subset O_K/d_2$ from proposition 2, we see that $L \subset L_O$. Hence $L \bigcap C \subset L_O \bigcap C \subset L_O^0$ and from above, $L \bigcap C$ can only contain $\leq (d_2-1)$ linearly independent elements. Thus, C cannot contain any $\mathbb{Z}$-basis of L.

Now we are ready to prove theorem 1.

Proof (of theorem 1). Let $\alpha_{2^j} = \sqrt{m_j}$ and $\alpha_0 = 1$.

Now we define α_i for all $1 \leq i \leq 2^n - 1$ inductively from α_{2^k}. Expand i in the binary system and let $i = \sum_{k=0}^{n-1} \delta(k)2^k$ where $\delta(k) = 0$ or 1. Then $\alpha_i = \sqrt{\prod_{1\leq k\leq n-1,\delta(k)=1} m_k}$ and we see that

$\{\alpha_i |\, 0 \leq i \leq 2^n - 1\} = \left\{ \sqrt{\prod_{j\in J} m_j} |\, J \subset \{0,\ldots,n-1\} \right\}$

Let $G = Gal(K/\mathbb{Q})$. Let σ_0 denote the identity automorphism in G and σ_{2^p}, $0 \leq p \leq n-1$ be elements of G_n defined by

$$\sigma_{2^p}(\alpha_p) = -\alpha_p \text{ and } \sigma_{2^p}(\alpha_k) = \alpha_k \text{ for } k \neq p \text{ and } 0 \leq k \leq n-1$$

Let G_p be the subgroup $\{\sigma_0, \sigma_{2^p}\}$ of G_n and we know that $G_n = \prod_{p=0}^{n-1} G_p$, as $[K : \mathbb{Q}] = 2^n$.

Now we define all 2^n elements σ_i of G as follows: expand i in the binary system and let $i = \sum_{k=0}^{n-1} \delta(k)2^k$ where $\delta(k) = 0$ or 1. If $k_1, \ldots, k_t$ are the ones for which $\delta(k) = 1$, then $\sigma_i = \sigma_{2^{k_1}} \circ \cdots \circ \sigma_{2^{k_t}}$.

Now, for $\beta \in K_n$ let the Minkowski embedding be $(\sigma_0(\beta), \sigma_1(\beta), \ldots, \sigma_{2^n-1}(\beta))$. Let L_O be the lattice corresponding to O_K/d_n and L be the lattice formed by the Minkowski embedding of the ring of integers. As in the bi-quadratic case, consider

$$L_O = \sum_{i=0}^{2^n-1} \frac{\mathbb{Z}}{d_n}(\sigma_0(\alpha_i), \sigma_1(\alpha_i), \ldots, \sigma_{2^n-1}(\alpha_i))$$

and for each $j \in \mathbb{Z}$, consider

$$L_O^j = \sum_{i=0}^{2^n-2} \frac{\mathbb{Z}}{d_n}(\sigma_0(\alpha_i), \sigma_1(\alpha_i), \ldots, \sigma_{2^n-1}(\alpha_i)) + \frac{j}{d_n}(\sigma_0(\alpha_{2^n-1}), \sigma_1(\alpha_{2^n-1}), \ldots, \sigma_{2^n-1}(\alpha_{2^n-1}))$$

We know that $\alpha_{2^n-1} = \sqrt{m_{2^0} \cdots m_{2^{n-1}}} \asymp \Delta_K^{(1/2^n)}$. Also, $L_0 = \bigcup_{j \in} L_O^j$.

Now we define $f(x)$ for $x \in \mathbb{R}^{d_n}$. Let $a(i)$ for $0 \leq i \leq 2^n - 1$ be such that

$$a(i) = \begin{cases} 1 & \text{if the binary expression of } i \text{ has even number of ones,} \\ -1 & \text{if the binary expression of } i \text{ has odd number of ones.} \end{cases}$$

Then, define

$$f(x) = \sum_{i=0}^{2^n-1} a(i)x_i$$

We have the following observations-

(i) We see that f is linear, i.e., $f(x+y) = f(x) + f(y)$ for $x, y \in \mathbb{R}^{d_n}$ and for $c \in \mathbb{R}$, $f(cx) = cf(x)$.

(ii) $\sigma_i(\alpha_{2^n-1}) = a(i)\alpha_{2^n-1}$ for all $0 \leq i \leq 2^n - 1$. This is because each σ_i will flip the sign of $\sqrt{m_k}$ if and only if the coefficient of 2^k in the binary expansion of i is 1. This implies the number of times σ_i will flip the sign of $\alpha_{2^n-1} = \sqrt{m_1 m_2 \cdots m_n}$ is the same as the number of 1 in the binary expansion of i, and thus $\sigma_i(\alpha_{2^n-1}) = a(i)\alpha_{2^n-1}$.

This implies that

$$f(\frac{j}{d_n}(\sigma_0(\alpha_{2^n-1}), \sigma_1(\alpha_{2^n-1}), \ldots, \sigma_{2^n-1}(\alpha_{2^n-1}))) = j\alpha_{2^n-1} = j\sqrt{m_{2^0} \cdots m_{2^{n-1}}} \text{ for } j \in \mathbb{Z}$$

(iii) For $0 \leq i \leq 2^n - 2$, $f\left(\frac{k}{d_n}(\sigma_0(\alpha_i), \sigma_1(\alpha_i), \ldots, \sigma_{2^n-1}(\alpha_i))\right) = 0$.

Notice that each σ_j will flip or keep the sign of α_i, so it suffices to show that the number of σ_j that fixes α_i is equal to the number of σ_j that flips α_i. Recall that σ_j will flip the sign of $\sqrt{m_k}$ if and only if the coefficient of 2^k in the binary expansion of j is 1. Thus, based on the way α_i is defined, σ_j will flip the sign of α_i if and only if the number of common 1 in the binary expansion of i and j is odd. Thus, the problem of counting σ_j that will flip the sign of α_i is reduced to the following lemma:

Lemma 4 *Given an integer $i, 0 \leq i \leq 2^n - 2$, the number of integers $j, 0 \leq i \leq 2^n - 1$ such that the number of common 1 in the binary expansion of i and j is odd is 2^{n-1}.*

Proof. Suppose the number of 1 in the binary expansion of i is x. Then the j that would satisfies the lemma would have $1, 3, 5, \cdots$ 1 in common with i's binary expansion in its binary expansion. Such number of j is

$$\binom{x}{1}2^{n-x} + \binom{x}{3}2^{n-x} + \binom{x}{5}2^{n-x} + \cdots = 2^{n-x}(\binom{x}{1} + \binom{x}{3} + \binom{x}{5} + \cdots) = 2^{n-x}.2^{x-1} = 2^{n-1}$$

Thus, we see that for $x \in L_O^j$, $f(x) = j\alpha_{2^n-1} = j\sqrt{m_1 \cdots m_n}$ for $j \in \mathbb{Z}$.

Consider the convex centrally symmetric compact set

$$C = [-\frac{\sqrt{m_1 \cdots m_n}}{2d_n}, \frac{\sqrt{m_1 \cdots m_n}}{2d_n}]^{d_n}$$

The volume

$$Vol(C) = \frac{(m_1 \cdots m_n)^{2^{n-1}}}{d_n^{d_n}} \asymp (m_{2^0} \cdots m_{2^{n-1}})^{2^{n-1}} \asymp \Delta_{K_n}$$

Now, if there exists $x \in L_O^j \bigcap C$ for $j \neq 0$, then we have $\sqrt{m_1 \cdots m_n} \leq \left|j\sqrt{m_1 \cdots m_n}\right| = |f(x)| = \left|\sum_{i=0}^{2^n-1} a(i)x_i\right| \leq \sum_{i=0}^{2^n-1} |x_i| \leq \sqrt{m_1 \cdots m_n}/2$.

This is a contradiction. After this, we can repeat the same argument as in the case $n = 2$. We have that $L_O^j \bigcap C = \phi$ for $j \neq 0$ and C can contain points from only L_O^0 and hence,

$L_O \bigcap C \subset L_O^0 \subset \sum_{i=0}^{2^n-2} \frac{\mathbb{R}}{d_n}(\sigma_0(\alpha_i), \sigma_1(\alpha_i), \ldots, \sigma_{2^n-1}(\alpha_i))$ which is a $2^n - 1$ dimensional $\mathbb{R}$ vector space and hence cannot contain 2^n $\mathbb{R}$-linearly independent elements.

Now, let L be the lattice formed using the Minkowski embedding of the ring of integers o_K of K. Since we have $o_K \subset O_K/d_n$ from proposition 2, we see that $L \subset L_O$. Hence $L \bigcap C \subset L_O \bigcap C \subset L_O^0$ and from above, $L \bigcap C$ can only contain $\leq (d_n - 1)$ linearly independent elements. Thus, C cannot contain any $\mathbb{Z}$-basis of L.

4 Totally imaginary poly-quadratic fields

The previous section covers the case of poly-quadratic field $K = \mathbb{Q}[\sqrt{m_1}, \cdots, \sqrt{m_n}]$ where all the m_i are greater than 0. Now we consider the case where one or more of the m_i are negative.

Lemma 5 *If K is a number field which is Galois over $\mathbb{Q}$, then it is either totally real or totally imaginary.*

Proof. The lemma follows from the fact that if K has one real embedding then all the embeddings are real and similarly for the other case.

To see the above fact look at composition $K \xrightarrow{\phi} K \xrightarrow{\rho} \mathbb{R}$ where $\phi \in Gal(K/\mathbb{Q})$ and ρ is a real embedding of K. Now, since ρ is injective, $\rho \circ \phi$ for $\phi \in Gal(K/\mathbb{Q})$ are all distinct, which means they are all the embeddings of K into $\mathbb{C}$, since we have only $n = [K : \mathbb{Q}]$ embeddings of K. Thus, all the embeddings are real if one of them is real and a similar argument works for the other case.

Since we know that poly-quadratic fields are Galois, from the above lemma, we conclude that poly-quadratic fields are totally real if and only if all the m_i are greater than zero. If K is a poly-quadratic field with at least one of the $m_j < 0$, we have an identity embedding of $K \to \mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_n}) \subset \mathbb{C}$ and $\mathbb{Q}(\sqrt{m_1}, \ldots, \sqrt{m_n}) \not\subset \mathbb{R}$. Hence, K is totally imaginary and $r = 0, s = \frac{[K:\mathbb{Q}]}{2} = 2^{n-1}$.

Now we can finally prove theorem 2.

Proof (of theorem 2). Let $K = \mathbb{Q}(\sqrt{m_1}, \dots, \sqrt{m_n})$ with at least one of the $m_i < 0$. We choose a family $\mathcal{F}$ of embeddings σ such that $\{\sigma, \overline{\sigma} | \sigma \in \mathcal{F}\}$ covers all the embeddings $K \to \mathbb{C}$. Also, we can assume that

For $I \subseteq \{1, 2, \dots, n\}$, let $m_I = \prod_{i \in I} m_i$ and we fix the notation that if $I = \phi$, then $m_I = 1$. Let $G = Gal(K/\mathbb{Q})$ and $\sqrt{x}$ denote the positive square root of x for $x > 0$ and $i\sqrt{|x|}$ for $x < 0$. Consider the $\mathbb{Z}$-module $O_k/d_n = \sum_{I \subset \{1,\dots,n\}} \frac{\mathbb{Z}}{d_n}\sqrt{m_I}$ as in proposition 2. The image of it under the Minkowski embedding is

$$L_O = \sum_{I \subset \{1,\dots,n\}} \frac{\mathbb{Z}}{d_n} e_{m_I}$$

where e_{m_I} are as follows:

$$e_{m_I} = \begin{cases} (x_\sigma),\ x_\sigma = 1,\ x_{\overline{\sigma}} = 0 \text{ for } \sigma \in \mathcal{F} & \text{if } I = \phi \text{ and hence } m_I = 1 \\ (x_\sigma),\ x_\sigma = \sigma(\sqrt{m_I}) = \pm\sqrt{m_I},\ x_{\overline{\sigma}} = 0 \text{ for } \sigma \in \mathcal{F} & \text{if } I \neq \phi, m_I > 0 \\ (x_\sigma),\ x_\sigma = 0,\ x_{\overline{\sigma}} = -i\sigma(m_I) = \pm\sqrt{|m_I|} \text{ for } \sigma \in \mathcal{F} & \text{if } I \neq \phi, m_I < 0 \end{cases}$$

Let

$$L_O^j = \sum_{I \subsetneq \{1,\dots,n\}} \frac{\mathbb{Z}}{d_n} e_{m_I} + \frac{j}{d_n} e_{m_1 \cdots m_n}$$

Now, we know that

$$|\Delta_K| \asymp_{d_n} \left(\left| \prod_{j=1}^n m_j \right| \right)^{2^{n-1}} = \left(\left| \prod_{j=1}^n m_j \right| \right)^{\frac{d_n}{2}}$$

Consider the set $B \subset \mathbb{R}^{d_n}$

$$B = \left\{ (x_\sigma) \in \mathbb{R}^{d_n} |\, x_\sigma^2 + x_{\overline{\sigma}}^2 \leq \frac{\left|\prod_{j=1}^n m_j\right|}{(2d_n)^2} \text{ for } \sigma \in \mathcal{F} \right\}$$

Then

$$\mathrm{Vol}(B) = \prod_{\sigma \in \mathcal{F}} \left(\pi \cdot \frac{\left|\prod_{j=1}^n m_j\right|}{(2d_n)^2} \right) = \frac{\pi^{\frac{d_n}{2}}}{(2d_n)^{d_n}} \cdot \left| \prod_{j=1}^n m_j \right|^{\frac{d_n}{2}} \asymp_{d_n} |\Delta_K|$$

Observe that $L_O = \bigcup_{j \in} L_O^j$. Define a function $f : L_O \mapsto \mathbb{R}$ such that $f(x) = \sum_{\sigma \in \mathcal{F}} x_\sigma^2 + x_{\overline{\sigma}}^2$. We want to show that $f(x) \geq \frac{j^2}{2d_n} \cdot \left|\prod_{j=1}^n m_j\right|$ if $x \in L_O^j$.

Case 1: If $\prod_{j=1}^n m_j \geq 0$:

Then $f(x) = \sum_{\sigma \in \mathcal{F}} x_\sigma^2 + x_{\overline{\sigma}}^2 \geq \sum_{\sigma \in \mathcal{F}} x_\sigma^2$

Suppose $x = \sum_{I \subsetneq \{1,\dots,n\}} \frac{a_I}{d_n} e_{m_I} + \frac{j}{d_n} e_{m_1 \cdots m_n}$.

Then

$$\sum_{\sigma\in\mathcal{F}} x_\sigma^2 = \sum_{\sigma\in\mathcal{F}} (\frac{j}{d_n}\sigma(\sqrt{m_1m_2\cdots m_n}) + \sum_{m_I\geq 0, I\subsetneq\{1,\ldots,n\}} \frac{a_I}{d_n}\sigma(\sqrt{m_I}))^2$$

$\geq \frac{d_n}{2}(\frac{j}{d_n})^2 m_1m_2\cdots m_n + \sum_{\sigma\in\mathcal{F}, m_I, m_J\geq 0} 2\frac{j}{d_n}\frac{a_I}{d_n}\sigma(\sqrt{m_Im_J})$

Note that since $m_Im_J \geq 0$, $2\sigma(\sqrt{m_Im_J}) = \sigma(\sqrt{m_Im_J}) + \overline{\sigma}(\sqrt{m_Im_J})$. Thus,

$$\sum_{\sigma\in\mathcal{F}} 2\frac{j}{d_n}\frac{a_I}{d_n}\sigma(\sqrt{m_Im_J}) = \frac{j}{d_n}\frac{a_I}{d_n}Tr_{K/\mathbb{Q}}(\sqrt{m_Im_J}) = 0$$

This gives us

$$\sum_{\sigma\in\mathcal{F}} x_\sigma^2 \geq \frac{d_n}{2}(\frac{j}{d_n})^2 m_1m_2\cdots m_n = \frac{j^2}{2d_n}\prod_{j=1}^n m_j$$

Case 2: If $\prod_{j=1}^n m_j \leq 0$: This case is entirely similar to case 1.
Now, if there exists $x = (x_\sigma) \in B\bigcap L_O^j$ for $j \neq 0$, then

$$\begin{aligned}
\frac{\left|\prod_{j=1}^n m_j\right|}{2d_n} &\leq \frac{j^2}{2d_n}\cdot\left|\prod_{j=1}^n m_j\right| \\
&\leq f(x) = \sum_{\sigma\in\mathcal{F}} x_\sigma^2 + x_{\overline{\sigma}}^2 \qquad [\text{ Since } x = (x_\sigma)\in L_O^j \text{ }] \\
&\leq \sum_{\sigma\in\mathcal{F}} \frac{\left|\prod_{j=1}^n m_j\right|}{(2d_n)^2} \qquad [\text{ Since } x = (x_\sigma)\in B \text{ }] \\
&= \frac{\left|\prod_{j=1}^n m_j\right|}{(2d_n)^2}\cdot\frac{d_n}{2} = \frac{\left|\prod_{j=1}^n m_j\right|}{8d_n}
\end{aligned}$$

which is a contradiction. So, we get that $B\bigcap L_O^j = \phi$ for $j \neq 0$. Hence,

$$L_O\bigcap B \subset L_O^0 \subset \sum_{I\subsetneq\{1,\ldots,n\}} \frac{\mathbb{R}}{d_n}e_{m_I}$$

Thus, $L_O\bigcap B$ is contained in a $2^n - 1$ dimensional $\mathbb{R}$ vector space and hence cannot contain 2^n $\mathbb{R}$-linearly independent elements.

Now, let L be the lattice formed using the Minkowski embedding of the ring of integers o_K of K. Since we have $o_K \subset O_K/d_n$ from proposition 2, we see that $L \subset L_O$. Hence $L\bigcap C \subset L_O\bigcap C \subset L_O^0$ and from above, $L\bigcap B$ can only contain $\leq (d_n - 1)$ linearly independent elements. Thus, B cannot contain any $\mathbb{Z}$-basis of L.

Reference

[1] Daniel A. Marcus. *Number fields*. Springer International Publishing, 2018.
[2] Jürgen Neukirch. *Algebraic Number Theory*. Springer-Verlag Berlin Heidelberg, 1999.