Length of elements in a Minkowski basis for an order in a number field (or a ring of integers of a number field)

by

Val Chiche-lapierre

A thesis submitted in conformity with the requirements
for the degree of Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto

Abstract

Length of elements in a Minkowski basis for an order in a number field (or a ring of integers of a number field)

Val Chiche-lapierre
Doctor of Philosophy
Graduate Department of Mathematics
University of Toronto
2019

Suppose K is a number field of degree n, and R is an order in K with discriminant D. If K has r real embeddings and s pairs of complex embeddings then we can look at R as a lattice in $\mathbb{R}^r \times \mathbb{C}^s$. We call the length of elements of R their Euclidean length in $\mathbb{R}^r \times \mathbb{C}^s$ and denote it by $|.|$. Let $v_1 = 1, v_2, ..., v_n$ be a Minkowski basis for R. We are interested in the asymptotic lengths of these $v_i's$ for a family or orders with arbitrarily large discriminant D. By the theory of Minkowski bases we have that $1 \leq |v_2| \leq ... \leq |v_n|$ and $\prod_{i=1}^{n} |v_i| \asymp |D|^{1/2}$ and by [8], we also know that $|v_n| \ll |D|^{1/n}$.

We say a family of orders in number fields have **Minkowski type** $\delta_2, ..., \delta_n$ if the members of the family have arbitrarily large discriminant and each have a Minkowski basis of the form $v_1 = 1, v_2, ..., v_n$ with $|v_i| \asymp |D|^{\delta_i}$ for each i, where D is the discriminant.

In the thesis, we are interested in possible Minkowski types. The first question is: Can we find sufficient and necessary bounds on some **rational** numbers $\delta_2, ..., \delta_n$ such that there is a family of orders in number fields having Minkowski type $\delta_2, ..., \delta_n$?

We already know the following necessary conditions: $\delta_2 \leq ... \leq \delta_n$ and $\delta_2 + ... + \delta_n = 1/2$ by Minkowski basis theory, and $\delta_n \leq 1/n$ by [8]. We prove that bounds of the form $\delta_k \ll \delta_i + \delta_j$ for each $i + j = k$ are sufficient bounds, and if K has no non trivial subfield, we conjecture that these bounds are actually necessary. We can prove this in some cases (of n, i, j, k). In particular, for $n = 3, 4, 5, 6$, we prove that all these bounds are necessary.

The second question is: For some fixed $\delta_2, ...\delta_n$, "how many" orders in number fields have Minkowski type $\delta_2, ..., \delta_n$. We will make sense of what we mean by "how many" using the Delone-Faddeev correspondence ($n = 3$), and the correspondence of Bhargava ($n = 4, 5$). Using these correspondences and counting, we are also able to give a sieving argument to count those orders that are maximal (and therefore are ring of integers of number fields).

Contents

Introduction

Let us start by defining all the asymptotic notation that we will use.

Notation 0.0.1. *We write $f = O(g)$ or $f \ll g$ if there is a nonzero constant C such that $f \leq Cg$.*
We write $f = o(g)$ if $\lim \frac{|f|}{|g|} = 0$.
We write $f = \omega(g)$ if $\liminf \frac{|f|}{|g|} = \infty$.
We write $f \asymp g$ if there are two positive constants C_1 and C_2 such that $C_1|g| \leq |f| \leq C_2|g|$.

Let K be a number field of degree n, and let R be an order in K with discriminant D. If K has r real embeddings and s pairs of complex (conjugate) embeddings ($r + 2s = n$), then we have $K \hookrightarrow \mathbb{R}^r \times \mathbb{C}^s$, and we can look at R as a lattice in $\mathbb{R}^r \times \mathbb{C}^s$. We call the length of elements of R the Euclidean length of their image in $\mathbb{R}^r \times \mathbb{C}^s$ and denote it by $|.|$. Let $v_1 = 1, v_2, ..., v_n$ be a Minkowski basis for R. That is v_2 is the shortest vector that makes $\{1, v_2\}$ a primitive set, v_3 is the shortest vector that makes $\{1, v_2, v_3\}$ primitive and so on. By the theory of Minkowski bases we have that $1 \leq |v_2| \leq ... \leq |v_n|$ and $\prod_{i=1}^{n} |v_i| \asymp |D|^{1/2}$. We are interested in asymptotic lengths of these $v_i's$ for a family or orders with arbitrarily large discriminant D. One might ask if all the possible length satisfying this are attained. In other words if $\delta_1 = 0 \leq \delta_2 \leq ... \leq \delta_n$ and $\sum_{i=1}^{n} \delta_i = 1/2$, is there a family of orders in number fields with arbitrarily large discriminant and each order having Minkowski basis of the form $v_1 = 1, v_2, ..., v_n$ that satisfies $|v_i| \asymp |D|^{\delta_i}$ for each i, where D is the discriminant? We already know the answer is no for $n \geq 4$ as they proved in [7] that $|v_n| \ll |D|^{1/n}$, and thus $\delta_n \leq 1/n$. The next question is can we find sufficient and necessary bounds so that all the possible lengths satisfying these bounds are attained?

Note that the $\delta_i's$ might depend on D. For example, if $\delta_n = \frac{1}{n} - \frac{\log\log|D|}{\log|D|}$, then $|v_n| \asymp |D|^{\delta_n} = \frac{|D|^{1/n}}{\log|D|}$, which might be a possible asymptotic length for v_n. This makes the question harder to answer. We will thus consider the following weaker question that allow is to restrict our attention to the $\delta_i's$ being numbers not depending on D:

Can we find sufficient and necessary bounds on $\delta_2, ..., \delta_n$ such that there is a family of orders in number fields with arbitrarily large discriminant D and Minkowski bases of the form $v_1 = 1, v_2, ..., v_n$ with $|v_i| \asymp |D|^{\delta_i + o(1)}$ (or equivalently $log|v_i| \asymp \delta_i Log|D|$), for each i?

Remark 0.0.2. *Note that restricting our attention further to* **rational** *$\delta_i's$ is enough to prove sufficiency of the bounds, since it would give us a set that is dense in a set answering the above question.*

We will answer the following slightly stronger question:

Can we find sufficient and necessary bounds on the rational numbers $\delta_2, ..., \delta_n$ such that there is a family of orders in number fields with arbitrarily large discriminant D and Minkowski bases of the form $v_1 = 1, v_2, ..., v_n$ with $|v_i| \asymp |D|^{\delta_i}$, for each i?

To simplify our statements, we define a term that we will use a lot in this thesis:

Definition 0.0.3. *We say a family of orders in number fields have* **Minkowski type** $\delta_2, ..., \delta_n$ *if the members of the family have arbitrarily large discriminant and each have a Minkowski basis of the form* $v_1 = 1, v_2, ..., v_n$ *with* $|v_i| \asymp |D|^{\delta_i}$ *for each* i*, where* D *is the discriminant.*

We may then rephrase the question that we want to answer as:

Can we find sufficient and necessary bounds on some rational numbers $\delta_2, ..., \delta_n$ *such that there is a family of orders in number fields having Minkowski type* $\delta_2, ..., \delta_n$*?*

We now define the term "almost Minkowski" bases that we will often use as such a basis have the properties of a Minkowski bases that we are interested in.

Definition 0.0.4. *We say bases* $w_1, ..., w_n$ *for a family of lattices are* **almost Minkowski** *if for Minkowski bases* $v_1, ..., v_n$*, we have* $|w_i| \asymp |v_i|$*, for each* $i = 1, ..., n$*.*

Then clearly a family of orders in number fields have Minkowski type $\delta_2, ..., \delta_n$ if and only if it has almost Minkowski bases of the form $1, w_2, ..., w_n$ with $|w_i| \asymp |D|^{\delta_i}$, for each i.

It is also easy to see that we have the characterization of almost Minkowski bases:

Lemma 0.0.5. *Bases* $w_1, ..., w_n$ *for a family of lattices with discriminants* D *are almost Minkowski if and only if* $\prod |w_i| \asymp |D|^{1/2}$*.*

When dealing with finding bounds on the size of basis elements (and, as we will talk about later, counting), it will be convenient to also use the term "Minkowski type" to talk about a single order as opposed to a family:

Definition 0.0.6. *We say an order in a number field has* **Minkowski type** $\delta_2, ..., \delta_n$ *if it has a Minkowski basis of the form* $v_1 = 1, v_2, ..., v_n$ *with* $|v_i| \asymp |D|^{\delta_i}$ *for each* i*, where* D *is the discriminant, and where the implied constant is independent of the order and of its discriminant.*

If R is an order in a quadratic field, we know that $v_1 = 1$ and $|v_2| \asymp |D|^{1/2}$. So the answer to our question in the quadratic case is trivially:

$$\delta = 1/2.$$

If R is an order in a cubic field, let $v_1 = 1, v_2, v_3$ be a Minkowski basis for R. We already know by Minkowski basis theory and [7] ($|v_n| \ll |D|^{1/n}$) that

$$\begin{aligned} |v_2||v_3| &\asymp |D|^{1/2} & \delta_2 + \delta_3 &= 1/2 \\ |v_2| &\ll |v_2| & \delta_2 &\leq \delta_3 \\ |v_3| &\ll |D|^{1/3} & \delta_3 &\leq 1/3 \end{aligned}$$

which is equivalent to

$$\begin{aligned} |D|^{1/4} \ll |v_3| &\ll |D|^{1/3} & 1/4 \leq \delta_3 &\leq 1/3 \\ |v_2| &\asymp \frac{|D|^{1/2}}{|v_3|} & \delta_2 &= \frac{1}{2} - \delta_3 \end{aligned}$$

We will see that every rational δ_3 between these two bounds is attained for some family of cubic orders, and thus the answer to our question in the cubic case is:

$$1/4 \leq \delta_3 \leq 1/3$$
$$\delta_2 + \delta_3 = 1/2.$$

In the quartic case, as we will see in Chapter 4, some additional bounds are necessary if we want the quartic field to not have a quadratic subfield, but in the case where it does have a quadratic subfield, which is the case of about 9.356 % of all quartic fields, then everything between the bounds that we already know (from Minkowski basis theory and [7]) is attained. It it easy to see that these two cases will be different. We might for example fix an order in a quadratic field and consider a family of quadratic extensions of this fixed quadratic order. This would give us a family of Minkowski type $0, 1/4, 1/4$. On the other hand, if we have a family of orders in a quartic number field K that has no non trivial subfield and that have Minkowski type $\delta_2, \delta_3, \delta_4$, then we must have $\delta_2 \geq 1/12$. To see this, let $1, v_2, v_3, v_4$ be a Minkowski basis for one of these orders, say R, and suppose that $|v_2| = o(|D|^{1/12})$. Since K has no non trivial subfield, v_2 must have degree 4 and thus $< 1, v_2, v_2^2, v_2^3 >$ is a sublattice of R, and therefore

$$|D|^{1/2} \ll |v_2||v_2^2||v_2^3| = |v_2|^6,$$

which gives $|v_2| \ll |D|^{1/12}$. In fact we will need something even stronger.

We will then see that the answer to our question in the quartic case is:

$$\delta_2 \leq \delta_3 \leq \delta_4 \leq 1/4$$
$$\delta_2 + \delta_3 + \delta_4 = 1/2.$$

Now again, we can only attain every value in the above region only if we are also willing to consider families in number fields with a quadratic subfield. If, on the other hand, we restrict our attention to number fields with no non trivial subfield, the answer to our question becomes:

$$\delta_2 \leq \delta_3 \leq \delta_4 \leq 1/4$$
$$\delta_3 \leq 2\delta_2$$
$$\delta_2 + \delta_3 + \delta_4 = 1/2.$$

One can check that the above bounds do imply that $\delta_2 \geq 1/12$.

In Chapter 1, we find some bounds for general degree. As discussed above with the example of the quartic case, it makes sense focus on the case where the orders are in a number field K that has no non trivial subfield, for which we use a method that is inspired by the proof that $|v_n| \ll |D|^{1/n}$ in [7]. On the other hand, we construct the families explicitly for some region of the $\delta_i's$, which proves the bounds sufficient in some cases.

The following is the existence theorem that we prove for general degree with an explicit construction.

Theorem 0.0.7. *For any number field K of degree n, and any $\delta_2, ..., \delta_n \in \mathbb{Q}$ satisfying $\delta_2 \leq ... \leq \delta_n$, $\delta_2 + ... + \delta_n = 1/2$ and $\delta_i \leq \delta_j + \delta_{i+1-j}$ for all i, j, there is a family of orders in K with Minkowski type*

$\delta_2, ..., \delta_n$.

We construct these families by starting with an element $\alpha \in K$ of degree n, and looking at the order $R =< 1, \alpha, \alpha^2, ..., \alpha^{n-1} >$ in K. Note that as we pick different $\alpha's$ we get a family or orders and $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ are almost Minkowski bases and that correspond to $\delta_i = \delta_j + \delta_{i+1-j}$ for all i, j, which is an extreme point of the region described in the statement of the theorem. We then modify R a little bit to get whatever we want in the region.

The following is the bounds that we could prove for general degree.

Theorem 0.0.8. *Let R be an order in a number field K of degree n, with Minkowski basis $v_1 = 1, v_2, ..., v_n$. If K has no non trivial subfield, then*

1) For all $i \in \{2, ..., n-1\}$ we have

$$|v_n| \ll |v_i||v_{n+1-i}|.$$

2) For each $k \in \{3, ..., n\}$,

$$|v_k| \ll |v_2||v_{k-1}|.$$

3) If $n \geq 5$, we have

$$|v_5| \ll |v_3|^2.$$

When $n = 3, 4, 5, 6$, Theorem 0.0.8 may be simply formulated as the following Corollary:

Corollary 0.0.9. *Let R be an order in a number field K of degree $n = 3, 4, 5, 6$, with Minkowski basis $v_1 = 1, v_2, ..., v_n$. If K has no non trivial subfield, then*

$$|v_i| \ll |v_j||v_{i+1-j}| \quad \forall i, j$$

or if $|v_i| \asymp |D|^{\delta_i}$, then

$$\delta_i \leq \delta_j + \delta_{i+1-j} \quad \forall i, j$$

We can see that for $n = 3, 4, 5, 6$, the necessary bounds given by Corollary 0.0.9 meet the sufficient bounds given by Theorem 0.0.7, and we are then able to completely answer the question of this thesis:

$$\begin{aligned} \delta_2 \leq ... \leq \delta_n \\ \delta_i \leq \delta_j + \delta_{i+1-j} \quad \forall i, j \\ \delta_2 + ... + \delta_n = 1/2. \end{aligned}$$

It does seem that this should be true for any n, but we could not prove it for $n \geq 7$. The method we use to prove Theorem 0.0.8 seems to be usable similarly to get any bound of the form $\delta_i \leq \delta_j + \delta_{i+1-j}$ for some sufficiently large n. The first problem is this method would be far from proving all these bounds as n grows large. Indeed, there are about n^2 of these bounds and this would only proves about $\log n$ of them. The second problem is there are some difficulties that did not allow us to prove that $|v_6| \ll |v_3||v_4|$ even for arbitrarily large n.

In Chapter 2,5 and 7 we reprove Theorem 0.0.8 and Theorem 0.0.7 for the case $n = 3, 4$ and 5, respectively, using a different method. That is using a correspondence between cubic, quartic and

quintic rings and some nice homogeneous spaces. The advantage of this method is that we can further actually count, when ordered by discriminant, the number of orders with each Minkowski type, as we will in chapters 4,6 and 8. Note that we will no longer be looking at families of orders but at all orders with discriminant less that some number X. We will then use the term "Minkowski type" to talk about a single order, that is in the sense of Definition 0.0.6.

In the cubic case, the Delone-Faddeev correspondence (see [1] and [8]) provides is a natural bijection between the set of $GL_2(\mathbb{Z})$ (resp $GL_2(\mathbb{R})$) equivalence classes of integral (rep. real) binary cubic forms and the set of isomorphism classes of cubic rings over $\mathbb{Z}$ (resp. over $\mathbb{R}$). These bijections are compatible with each other so we can start with one order R and generate new ones by acting on it with an elements of $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})$. They also nicely carry on information about Minkowski bases.

We can then use this, in Chapter 2, to give another construction reproving the cubic case of Theorem 0.0.7. On the other hand we can also reprove that $|v_3| \ll |D|^{1/3}$ (that is the cubic case of Theorem 0.0.8).

In Chapter 3, we count the number of orders with given type of Minkowski basis, ordered by discriminant. We take $\delta \in (1/6, 1/4]$ and let $S_\delta \cap V_\mathbb{Z}$ be a subset of the above mentioned homogeneous space whose elements, under the Delone-Faddeev correspondence, correspond to cubic orders with Minkowski type $\delta, 1/2-\delta$. We will define S_δ more precisely in Chapter 3. For a $GL_2(\mathbb{Z})$ invariant subset S of the homogeneous space, we let $N(S;X)$ be the number of irreducible $GL_2(\mathbb{Z})$ orbits on S, having discriminant at most 1. $N(S_\delta \cap V_\mathbb{Z}; X)$ is then the number of irreducible cubic rings (that is cubic orders) with Minkowski type $\delta, 1/2-\delta$.

Theorem 0.0.10. *For any $\delta \in (1/6, 1/4] \cap \mathbb{Q}$, we have*

$$N(S_\delta \cap V_\mathbb{Z}; X) = C_\delta X^{1/2+2\delta} + O(X^{1-\delta}) + O(X^{3/4+\epsilon}),$$

for some positive explicit constant C_δ.

We might then combine this method with sieving arguments to count the **maximal** orders with a given type of Minkowski basis. Let $\mathcal{U}$ be the subset of the homogeneous space whose elements correspond to maximal orders.

Theorem 0.0.11. *For $\delta \in (1/5, 1/4] \cap \mathbb{Q}$, we have*

$$N(S_\delta \cap \mathcal{U} \cap V_\mathbb{Z}; X) = \mu(\mathcal{U}) C_\delta X^{1/2+2\delta} + O_\epsilon(X^{1-\delta/2+\epsilon}),$$

where C_δ is the same constant as in Theorem 0.0.10 and $\mu(\mathcal{U})$ is the p-adic density of $\mathcal{U}$ in the homogeneous space, which by [1], $\mu(\mathcal{U}) = \left(\prod_p \frac{(p^3-1)(p^2-1)}{p^5}\right)$.

Note that Theorem 0.0.11 does not cover all the possible values of δ as the error gets bigger than the main term for small δ's. Later, in Chapter 8, we will use a similar method combined with an explicit construction and sieving that will gives us a lower bound for $N(S_\delta \cap \mathcal{U} \cap V_\mathbb{Z}; X)$ that holds for any δ in the possible range (minus the end points) that is $(1/6, 1/4)$.

By [2] and [4] we have similar parameterizations for the quartic and quintic cases, that allow us to do the same thing in these cases. With a similar argument as in Chapter 2, we reprove Theorem 0.0.8

and Theorem 0.0.7 for the quartic and quintic case in Chapter 4 and 7, respectively. This method also allows us to see what happens in the case where K has a subfield (which is only in the quartic case since 3 and 5 are prime).

For the quartic case, we prove the following additional theorem for the case where K has a quadratic subfield.

Theorem 0.0.12. *For any quartic number field K that has a quadratic subfield, and any $\delta_2, \delta_3, \delta_4 \in \mathbb{Q}$ satisfying $\delta_2 \leq \delta_3 \leq \delta_4$, $\delta_4 \leq \delta_2 + \delta_3$ and $\delta_2 + \delta_3 + \delta_4 = 1/2$, there is a family of orders in K with Minkowski type $\delta_2, \delta_3, \delta_4$.*

Remark 0.0.13. *Or equivalently, we can replace the condition $\delta_4 \leq \delta_2 + \delta_3$ by $\delta_4 \leq 1/4$, which we know is necessary for such a family to exist by [7].*

We then use a similar method as in Chapter 3 to count quartic and quintic orders with a given type of Minkowski basis.

In Chapter 5, we let $S \cap V_{\mathbb{Z}} = S_{\delta_2,\delta_3,\delta_4} \cap V_{\mathbb{Z}}$ be a subset of the homogeneous space whose elements correspond to quartic orders with Minkowski type $\delta_2, \delta_3, \delta_4$. We will define S more precisely in Chapter 5.

Theorem 0.0.14. *For each rational $\delta_2, \delta_3, \delta_4$, we have*

$$N(S \cap V_{\mathbb{Z}}; X) = C_{\delta_2,\delta_4} X^{1-2(\delta_4-\delta_2)} + O(X^{11/12}),$$

for some positive explicit constant C_{δ_2,δ_4}.

Theorem 0.0.15. *For each rational $\delta_2, \delta_3, \delta_4$, we have*

$$N(S \cap \mathcal{U} \cap V_{\mathbb{Z}}; X) = \mu(\mathcal{U}) C_{\delta_2,\delta_4} X^{1-2(\delta_4-\delta_2)} + O_\epsilon(X^{71/72+\epsilon}),$$

where C_{δ_2,δ_4} is the same constant as in Theorem 0.0.14, and $\mu(\mathcal{U})$ is the p-adic density of $\mathcal{U}$ in the homogeneous space, which by [2], $\mu(\mathcal{U}) = \prod_p (p^4 + p^2 - p - 1)/p^4$.

Similarly, in Chapter 7, we let $S \cap V_{\mathbb{Z}} = S_{\delta_2,\delta_3,\delta_4,\delta_5} \cap V_{\mathbb{Z}}$ be a subset of the homogeneous space whose elements correspond to quintic orders with Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$.

We as usual need the $\delta_i's$ to be in the usual range described in Chapter 1, that is

$$\begin{cases} \delta_3 \leq 2\delta_2 \\ \delta_4 \leq \delta_2 + \delta_3 \\ \delta_5 \leq \delta_2 + \delta_4 \\ \delta_5 \leq 2\delta_3 \end{cases}$$

But we will see we also need this extra condition for out proof to work:

$$(\delta_3 - \delta_2) + (\delta_4 - \delta_2) + (\delta_5 - \delta_2) \leq 1/10. \tag{1}$$

Theorem 0.0.16. *For any rational $\delta_i's$ in the usual range such that (1) holds, we have*

$$N(S \cap V_{\mathbb{Z}}; X) = C_{\delta_2,\delta_3,\delta_4,\delta_5} X^{1-3(\delta_5-\delta_2)-(\delta_4-\delta_3))} + O_\epsilon(X^{199/200+\epsilon}),$$

for some positive constant $C_{\delta_2,\delta_3,\delta_4,\delta_5}$ that we will not compute explicitly for simplicity.

Theorem 0.0.17. *For any rational $\delta_i's$ in the usual range such that (1) holds, we have*

$$N(S \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = \mu(\mathcal{U}) C_{\delta_2,\delta_3,\delta_4,\delta_5} X^{1+(\delta_3-\delta_2)-(\delta_4-\delta_2)-3(\delta_5-\delta_2)} + O_\epsilon(X^{199/200+\epsilon}),$$

where C is the same constant as is Theorem 7.0.2, and $\mu(\mathcal{U})$ is the density of maximal elements in the homogeneous space, which by [4], $\mu(\mathcal{U}) = \prod_p (p-1)^8 p^{12} (p+1)^4 (p^2+1)^2 (p^2+p+1)^2 (p^4+p^3+p+1)(p^4+p^3+2p^2+2p+1)/p^{40}$.

In Chapter 8, we deal with the cubic case in a more elementary way that will reprove the cubic case of Theorem 0.0.7. We prove this by constructing $R = \mathbb{Z}[\alpha]$, for some conveniently chosen algebraic integer α. Note this construction also allows us to chose these families to be maximal orders, that is to be rings of integers in cubic number fields (with a Sieving argument). Sections 8.1 and 8.2 then prove the following theorem:

Theorem 0.0.18. *For all $\delta \in [1/6, 1/4] \cap \mathbb{Q}$, there is a family of rings of integers in cubic number fields with arbitrarily large discriminant with Minkowski type $\delta, 1/2 - \delta$.*

Finally, in the last section of this chapter, we use the counting method and the Delone-Faddeev correspondence, like in Chapter 3, combined with the above explicit construction and sieving that will gives us a lower bound for $N(S_\delta \cap \mathcal{U} \cap V_{\mathbb{Z}}; X)$, that is the number of maximal cubic orders with discriminant at most X and a Minkowski type $\delta, 1/2 - \delta$.

Theorem 0.0.19. *For any $\delta \in (1/6, 1/4) \cap \mathbb{Q}$, we have*

$$N(S_\delta \cap \mathcal{U} \cap V_{\mathbb{Z}}; X) \gg X^{1/2}.$$

The above theorem does prove existence of a family of maximal cubic rings of Minkowski type $\delta, 1/2-\delta$ for $\delta \in (1/6, 1/4)$ and thus reproving Theorem 0.0.18. Note that this is not strictly weaker than the estimate given in Chapter 3 since this holds for a any $\delta \in (1/6, 1/4)$ instead of just $\delta \in (1/5, 1/4)$.

Let us sum up how this thesis is organized. Chapter 1 gives the strongest result in the thesis about both necessity and sufficiency of some bounds in general degree in the case where the order are in number fields that have no non trivial subfield. This chapter is independent of the others.

In Section 2.1 (resp. 4.1, resp 6.1), we give a background on a correspondence between cubic (resp. quartic, resp, quintic) rings and some nice homogeneous space which will be used in chapters 2 and 3 (resp. 4 and 5, resp. 6 and 7).

The rest of Chapter 2 (resp. 4, resp. 6) is proving necessity and sufficiency of our bounds for the cubic (resp. quartic, resp. quintic) case using the correspondence. The reader who is only interested in the counting might skip this and go directly to Chapter 3 (resp. 5, resp. 7). We are now also able to consider the case where our orders are in number fields that have a non trivial subfield, which can only

happen for the quartic case as 3 and 5 are prime numbers. The cubic and quintic case are only reproving what was already proven in Chapter 1.

In Chapter 3 (resp. 5, resp. 7), we count the number of orders of certain Minkowski types, when ordered by discriminant, as well as the number of maximal such orders.

Finally, Chapter 8 is an explicit construction and sieving that leads to a lower bound for the count of maximal order of certain Minkowski types for the cubic case. We recall that this is not weaker than the result in Chapter 3 since we now cover a dense subset of the full range of possible Minkowski types.

Chapter 1

General degree

In this chapter, we prove things for general degree, in the case of orders in a number field that have no non trivial subfield. Note that if n is a prime, then number fields of degree K never have a non trivial subfield and then the condition can be dropped.

The work of this chapter completely answers the question of this thesis for $n = 3, 4, 5, 6$, that is

Can we find sufficient and necessary bounds on the rational numbers $\delta_2, ..., \delta_n$ such that there is a family of orders in number fields with arbitrarily large discriminant D and Minkowski type $v_1 = 1, v_2, ..., v_n$ with $|v_i| \asymp |D|^{\delta_i}$, for each i?

and the answer is:

$$\begin{aligned} \delta_2 \leq ... \leq \delta_n & \\ \delta_i \leq \delta_j + \delta_{i+1-j} \quad & \forall i, j \\ \delta_2 + ... + \delta_n = 1/2. & \end{aligned}$$

We will prove that these bounds are both sufficient and necessary.

We also prove some bounds for $n \geq 7$, but then what we can prove sufficient is strictly stronger than what we can prove necessary and thus we cannot completely answer our question.

First, in Section 1.1, we will prove Theorem 0.0.7 by constructing families of orders with certain Minkowski types, which proves sufficiency of the bounds

$$\begin{aligned} \delta_2 \leq ... \leq \delta_n & \\ \delta_i \leq \delta_j + \delta_{i+1-j} \quad & \forall i, j \\ \delta_2 + ... + \delta_n = 1/2, & \end{aligned}$$

for any $n \geq 3$.

Then, in Section 1.2, we will prove Theorem 0.0.8, which proves necessity of some bounds, namely

1) For all $i \in \{2, ..., n-1\}$ we have

$$|v_n| \ll |v_i||v_{n+1-i}|.$$

2) For each $k \in \{3, ..., n\}$,

$$|v_k| \ll |v_2||v_{k-1}|.$$

3) If $n \geq 5$, we have

$$|v_5| \ll |v_3|^2.$$

1.1 Construction - Proof of Theorem 0.0.7

In this section, we give an explicit construction to prove Theorem 0.0.7 that we recall:

Theorem 1.1.1. *For any number field K of degree n, and any $\delta_2, ..., \delta_n \in \mathbb{Q}$ satisfying $\delta_2 \leq ... \leq \delta_n$, $\delta_2 + ... + \delta_n = 1/2$ and $\delta_i \leq \delta_j + \delta_{i+1-j}$ for all i, j, there is a family of orders in K with Minkowski type $\delta_2, ..., \delta_n$.*

Remark 1.1.2. *Note that we do not need K to have no non trivial subfield, but if K has a subfield we can cover a bigger region of the $\delta_i's$.*

Proof. We construct these family by starting with a fixed element $\alpha \in K$ of degree n, and looking at the order $R =< 1, \alpha, \alpha^2, ..., \alpha^{n-1} >$ in K.

Note that as we pick different $\alpha's$ we get a family or orders and $1, \alpha, \alpha^2, ..., \alpha^{n-1}$ are almost Minkowski bases and that correspond to $\delta_i = \delta_j + \delta_{i+1-j}$ for all i, j, which is an extreme point of the region described in the statement of the theorem.

We now modify R a little bit to get other points in this region.

Lemma 1.1.3. *Let $a_2, ..., a_n$ be integers with the property that $a_i \mid a_{i+1}$ and $a_i \mid a_j a_{i+1-j}$ for each i, j, and consider $R' =< 1, a_2\alpha, a_3\alpha^2, ..., a_n\alpha^{n-1} >$. Then R' is also an order in K.*

Proof. We need to show that we can multiply any 2 of these basis elements together and get another element of R'. The multiplication of any two basis elements of R' is given by

$$(a_{i+1}\alpha^i)(a_{j+1}\alpha^j) = a_{i+1}a_{j+1}\alpha^{i+j}.$$

Now if $i + j \leq n - 1$, we have

$$a_{i+1}a_{j+1}\alpha^{i+j} = \frac{a_{i+1}a_{j+1}}{a_{i+j+1}}(a_{i+1+j}\alpha^{i+j}),$$

which is in R' since $a_{i+j+1} \mid a_{i+1}a_{j+1}$, and if $i + j > n - 1$, then for some integers $b_0, ..., b_{n-1}$, we have

$$\begin{aligned} a_{i+1}a_{j+1}\alpha^{i+j} &= (a_{i+1}a_{j+1})(b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}) \\ &= a_{i+1}a_{j+1}b_0 + \frac{a_{i+1}a_{j+1}}{a_2}b_1(a_2\alpha) + ... + \frac{a_{i+1}a_{j+1}}{a_n}b_{n-1}(a_n\alpha^{n-1}), \end{aligned}$$

which is in R' since for all $t = 2, ..., n$, we have $a_t \mid a_{i+j+1} \mid a_i a_j$. This proves that R' is a ring.

Now it is easy to see that if R' had a zero divisor, then so would R, and thus R' must be an integral domain, and therefore an order in K. □

Consider now a big integer M, and $\delta_2, ..., \delta_n$ satisfying the conditions of the theorem. Let each $a_i = M^{\delta_i}$. Then $\delta_i \leq \delta_{i+1}$ implies $a_i \mid a_{i+1}$ and $\delta_i \leq \delta_j + \delta_{i+1-j}$ implies $a_i \mid a_j a_{i+1-j}$, as needed for R'

to be an order in K. Also R' is given with a basis $1, a_2\alpha, a_3\alpha^2, ..., a_n\alpha^{n-1}$ with $|a_i\alpha^{i-1}| \asymp M^{\delta_i}$, for each i. As M varies, we get a family $\{R_M\}$ of orders in K.

For each M, R_M is given with a basis whose i-th element is $\asymp M^{\delta_i} \asymp |Disc(R_M)|^{\delta_i}$. Now, since $\delta_2 + ... + \delta_n = 1/2$, by Lemma 0.0.5, we have a family of almost Monkowski bases and therefore we have a family of Minkowski type $\delta_2, ..., \delta_3$, as needed. □

1.2 Bounds - Proof of Theorem 0.0.8

In this section, we prove Theorem 0.0.8 that we recall:

Theorem 1.2.1. *Let R be an order in a number field K of degree n, with Minkowski basis $v_1 = 1, v_2, ..., v_n$. If K has no non trivial subfield, then*

1) For all $i \in \{2, ..., n-1\}$ we have

$$|v_n| \ll |v_i||v_{n+1-i}|$$

2) For each $k \in \{3, ..., n\}$,

$$|v_k| \ll |v_2||v_{k-1}|.$$

3) If $n \geq 5$, we have

$$|v_5| \ll |v_3|^2.$$

As mentioned in the introduction (see Corollarry 0.0.9), for the cases $n = 3, 4, 5, 6$, these bounds are the same as the region for which, as we saw in the previous section, we can construct families and prove existence. We then have a proof that these bounds are both necessary and sufficient for existence of a family with these Minkowski types.

Proof. For 1) and 2), we will show that if they don't hold then there is a proper $\mathbb{Q}$-vector subspace L of K, and a non rational element α of K such that multiplication by α leaves L invariant. This implies that multiplication by $\mathbb{Q}(\alpha)$ leaves L invariant, which implies, we have natural maps $\mathbb{Q}(\alpha) \hookrightarrow L \hookrightarrow K$. But since K has no proper subfield, we must have $\mathbb{Q}(\alpha) = K$. We then have maps $K \hookrightarrow L \hookrightarrow K$, and thus $L = K$, which is a contradiction.

1) Suppose, on the contrary, that there exists $i, j \in \{2, ..., n-1\}$ with $i+j = n+1$ and $|v_i||v_j| = o(|v_n|)$. Since $v_1, ..., v_n$ is a Minkowski basis, we also have $|v_{i'}||v_{j'}| = o(|v_n|)$ for all $i' \leq i$ and $j' \leq j$, and by Minkowski basis theory, this implies that $v_{i'}v_{j'} \in < v_1, ..., v_{n-1} >$, the linear span of $\{v_1, ..., v_{n-1}\}$.

Consider the $(n-2) \times (n-2)$ symmetric matrix $A := (a_{lm})_{2 \leq l,m \leq n-1}$ where a_{lm} is the coefficient of v_n in the expansion of $v_l v_m$ with respect to the basis $v_1 = 1, v_2, ..., v_n$ (as in [7]). The above implies that this matrix has entries $a_{i'j'} = 0$ for all $i' \leq i$ and $j' \leq j$. One can check by induction on n that this matrix then has determinant zero. We can then find a vector

$$x = \begin{bmatrix} x_2 \\ \vdots \\ x_{n-1} \end{bmatrix} \text{ such that } Ax = 0.$$

Let $L =< v_1, ..., v_{n-1} >$ and $\alpha = x_2v_2 + ... + x_{n-1}v_{n-1}$. To see that multiplication by α leaves L invariant, it suffices to show, for each $k = 1, ..., n-1$, that $\alpha v_k \in L$. Or in other words that the coefficient

of v_n in the expansion of αv_k is 0. We compute

$$\alpha v_k = x_2 v_2 v_k + ... + x_{n-1} v_{n-1} v_k$$

has coefficient of v_n equal to

$$x_2 a_{2k} + ... + x_{n-1} a_{(n-1)k} = 0.$$

We then have a proper $\mathbb{Q}$-vector subspace L of K, and a non rational element α of K such that multiplication by α leaves L invariant, as needed.

2) Suppose there exists $k \in \{3, ..., n\}$ such that $|v_2||v_{k-1}| = o(|v_k|)$. Then for all $i \in \{1, ..., k-1\}$, we have that $|v_2||v_i| = o(|v_k|)$, which again by Minkowski basis theory implies that $v_2 v_i \in < v_1, ..., v_{k-1} >$. Let $L =< v_1, ..., v_{k-1} >$ and $\alpha = v_2$.

Then we again have a proper $\mathbb{Q}$-vector subspace L of K, and a non rational element α of K such that multiplication by α leaves L invariant, as needed.

3) Suppose $|v_3|^2 = o(|v_5|)$, then by Minkowski basis theory, we have

$$S := \{1, v_2, v_3, v_2^2, v_2 v_3, v_3^2\} \subset < 1, v_2, v_3, v_4 >$$

This inclusion defines a linear map from the 6-dimensional vector space generated by S (ignoring any possible relation between elements of S) and the 4-dimensional vector space $< 1, v_2, v_3, v_4 >$. The kernel of this map has dimension at least 2 and gives us 2 quadratics $f_1, f_2 \in \mathbb{Q}[x_2, x_3]$, that are not multiple of each other, and that both have (v_2, v_3) as a root.

We claim that f_1 and f_2 define algebraic varieties that do not share a common component. This will allow us to use Bézout's theorem to conclude that the have at most 4 common roots. But we know (v_2, v_3) and its n Galois conjugates are common roots of our quadratics, which is a contradiction since $n \geq 5$.

To see that they do not share a common component, first note that they are both irreducible over $\mathbb{Q}$. Indeed, if one of them was reducible in $\mathbb{Q}[x_2, x_3]$, then (v_2, v_3) would be a root of a linear polynomial over $\mathbb{Q}$, which is false since the $v_i's$ are linearly independent over $\mathbb{Q}$. Thus both f_1 and f_2 do not have a linear factor in $\mathbb{Q}[x_2, x_3]$. Second, note that they have to depend on both variables x_2 and x_3. Indeed, if one of them only depends on one variable, then either v_2 or v_3 would be a root of a quadratic polynomial, which is impossible since they both have degree $n \geq 5$.

Now by considering linear combinations of f_1 and f_2 if necessary, we may assume that f_1 has no x_2^2 coefficient. We can then apply the following lemma to f_1.

Lemma 1.2.2. *If a quadratic polynomial in $\mathbb{Q}[x, y]$ has no y^2 coefficient but does depend on y, and is irreducible in $\mathbb{Q}[x, y]$, then it is irreducible in $\overline{\mathbb{Q}}[x, y]$.*

Assuming we can prove Lemma 1.2.2, as we will shortly, we will have two quadratics polynomials f_1, f_2 with f_1 irreducible over $\overline{\mathbb{Q}}$, and thus they cannot share a common component unless they are multiple of each other, which they are not.

To complete the proof of 3), it remain to prove Lemma 1.2.2. Let $f(x, y)$ be a polynomial satisfing

the condictions of Lemma 1.2.2, and suppose that it is reducible in $\overline{\mathbb{Q}}[x, y]$. Then we can write

$$\begin{aligned} f(x, y) &= (a + bx + cy)(d + ex) \\ &= (ad) + (bd + ae)x + (be)x^2 + (dc)y + (ce)xy, \end{aligned}$$

for some $a, b, c, d, e \in \overline{\mathbb{Q}}$.

Since $f(x, y)$ depends on y, we must have $c \neq 0$, and since $f(x, y)$ does not have a linear factor in $Q[x, y]$, we must have $d \neq 0$ and $e \neq 0$.

Now since $f(x, y)$ is defined over $\mathbb{Q}$, we have $ad, cd, be, ce \in \mathbb{Q}$, which implies a/c and b/c are in $\mathbb{Q}$, and therefore $(\frac{a}{c} + \frac{b}{c}x + y) \in \mathbb{Q}[x, y]$ and is a linear factor of $f(x, y)$, which is a contradiction that completes the proof the Lemma 1.2.2. □

It does seem that we should have the bounds $|v_i| \ll |v_j||v_{i+1-j}|$ for each n, i, j, but we could not prove it for $n \geq 7$. The method we use to prove Theorem 0.0.8 seems to be usable similarly to get any bound of the form $\delta_i \leq \delta_j + \delta_{i+1-j}$ for some sufficiently large n, given i and j but there is an extra difficulty that comes with having more than two quadratic polynomials.

Chapter 2

The cubic case using the Delone-Faddeev correspondence

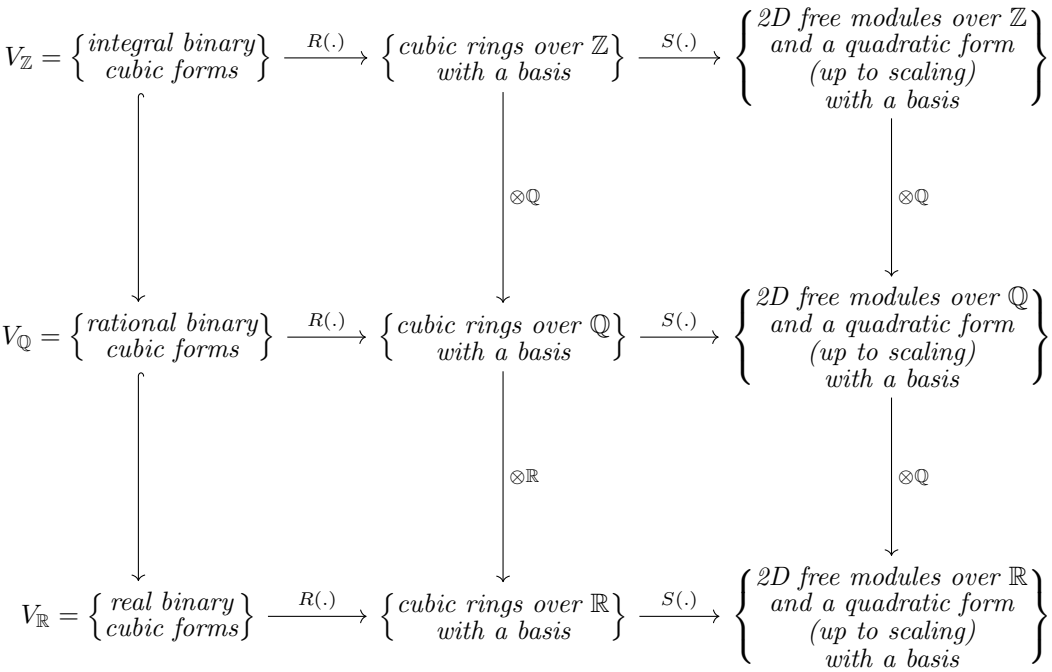
In this chapter, start by giving a background on the Delone-Faddeev correspondence, that is a correspondence between cubic rings and some homogeneous space that nicely carries information about Minkowski basis. In the background (Section 2.1), we give properties that will be used in the other sections on this chapter to reprove Theorem 0.0.7 (Existence) and Theorem 0.0.8 (bounds) for the case $n = 3$, as well as properties that will be useful in Chapter 3 when we count cubic orders of each form.

2.1 Background on the Delone-Faddeev Correspondance

Let $V_{\mathbb{R}}$ (resp. $V_{\mathbb{Q}}$, resp. $V_{\mathbb{Z}}$) be the set of real (resp. rational, resp. integral) binary cubic forms. For a binary cubic form ν in any of these sets, we may write $\nu = (a, b, c, d)$ as a vector whose components are the coefficients of ν, so that

$$(a, b, c, d)(x, y) = \nu(x, y) = ax^3 + bx^2y + cxy^2 + dy^3.$$

Theorem 2.1.1. *There are maps $R(\cdot)$ and $S(\cdot)$ that make the following diagram commute:*



The discriminant of an integral binary cubic form is equal to the discriminant of the corresponding cubic ring.

An integral cubic form corresponds to a cubic ring which is an integral domain if and only if it is irreducible as a polynomial over $\mathbb{Q}$.

In the middle column of the above diagram, the map $\otimes\mathbb{Q}$ sends cubic rings over $\mathbb{Z}$ that are orders in a cubic field with a basis map to the cubic field to which they are an order of with the same basis, and the map $\otimes\mathbb{R}$ takes cubic fields to $\mathbb{R}^3$ if they are totally real or to $\mathbb{R}\times\mathbb{C}$ otherwise, again with the same basis.

Remark 2.1.2. *A cubic ring is an order in a cubic field if and only if is an integral domain.*

Here are the maps, for a binary cubic form $\nu(x,y) = ax^3+bx^2y+cxy^2+dy^3$, let $R(\nu) =< 1, v_2, v_3 >$ with

$$\begin{aligned} v_2v_3 &= -ad \\ v_2^2 &= -ac - bv_2 + av_3 \\ v_3^2 &= -bd - dv_2 + cv_3 \end{aligned}$$

as described in [8]. It is clear that if the coefficients of ν are in some ring ($\mathbb{Z}$, $\mathbb{Q}$ or $\mathbb{R}$), then $R(\nu)$ will be a cubic ring over that same ring.

We now define $S(\nu)$ an call is the shape of $R(\nu)$. Roughly speaking $S(\nu)$ is the 2 dimensional lattice obtained from $R(\nu)$ by forgetting about the part that is generated by 1. In more precise term, we let $S(\nu) = \{x \in \mathbb{Z}+3R(\nu) : \mathrm{Tr(x)}=0\} =< w_2, w_3 >$, where

$$w_i = 3v_i - tr(v_i).$$

$S(\nu)$ is a 2-dimensional free module with a quadratic form $q(.)$ that is defined (up to scaling) by $q(.) = \sum_{\sigma:R\hookrightarrow\mathbb{C}} |\sigma(.)|^2 = |.|^2$, the square of the length. It may then be looked at in a plane, up the scaling and rotating. Given a basis for $S(\nu)$, one may put those vectors as the rows of a matrix which will be in $GL_2(\mathbb{R})$ if and only if ν is non degenerate. Scaling and rotating this basis is equivalent to right multiplication by the corresponding matrix by an element of $GO_2(\mathbb{R})$. If ν is non degenerate, we may then think of the a basis for $S(\nu)$ as an element of $GL_2(\mathbb{R})/GO_2(\mathbb{R})$.

Let us now state this consequence of Theorem 2.1.1 that we will really be using.

Theorem 2.1.3. *There is a map*

$$\{\textit{non degenerate elements of } V_{\mathbb{R}}\} \to \left\{ \begin{matrix} \textit{2D vector space over } \mathbb{R} \textit{ with a basis} \\ \textit{and a quadratic form (up to scaling)} \end{matrix} \right\} \simeq GL_2(\mathbb{R})/GO_2(\mathbb{R})$$

$$\nu \to \begin{bmatrix} \omega_\nu \\ \theta_\nu \end{bmatrix}$$

whose restriction to $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Q}}$ gives basis for shapes of cubic rings over $\mathbb{Z}$ (resp. $\mathbb{Q}$).

So why do we care so much about the shape that we will really be working with Theorem 2.1.3 instead of Theorem 2.1.1? In this paper, we are interested in the length of elements of a Minkowski basis $1, v_2, v_3$ for a cubic ring. We will see very soon that when interested in Minkowski bases, looking at $S(\nu)$ is much easier than looking at $R(\nu)$. Now if ν is an **integral** binary cubic form, then $R(\nu)$ is a cubic ring, and if ν gives $R(\nu)$ with a Minkowski basis, then

$$|w_i| = |3v_i - tr(v_i)| \asymp \max\{|v_i|, |tr(v_i)|\} \asymp |v_i|,$$

and thus looking at $S(\nu)$ will give us the information we want about $R(\nu)$. Let us recall here that $S(\nu)$ is a 2 dimensional free module with a quadratic $q(.)$ form that is defined up to scaling. The fact that $|v_i| \asymp |w_i|$ clearly implies that $\frac{|v_3|}{|v_2|} \asymp \frac{|w_3|}{|w_2|}$, and it makes sense to say that $\frac{|v_3|}{|v_2|} \asymp \frac{q(w_3)^{1/2}}{q(w_2)^{1/2}}$. We will from now on denote $q(.)$ simply by $|.|^2$ and remember that it is defined up to scaling. There should not be any confusion as we will be keep track of ratios.

Notation 2.1.4. *Let $\nu \in V_{\mathbb{R}}$ and its corresponding shape $S(\nu)$ with quadratic form $q(.)$ that is defined up to scaling. For some element $x \in S(\nu)$, we define the* **length** *of x, by*

$$|x| = q(x)^{1/2},$$

and remember that it is only defined up to scaling.

Let us record the above discussion in the following theorem:

Theorem 2.1.5. *For any $\nu \in V_{\mathbb{Z}}$, that maps to the cubic ring $R(\nu)$ with a basis $1, v_2, v_3$ and to the 2 dimensional lattice (up to scaling) represented by $S(\nu)$ with a basis w_2, w_3. Then*

1) $\frac{|v_3|}{|v_2|} \asymp \frac{|w_3|}{|w_2|}$

2) $1, v_2, v_3$ is a Minkowski basis for $R(\nu)$ if and only if w_2, w_3 is a Minkowski basis for $S(\nu)$.

Let us now look at the shapes of cubic rings. As we have seen above, shapes can be thought of as elements of $GL_2(\mathbb{R})/GO_2(\mathbb{R})$, where the rows of the matrices corresponds to the basis of the shape. The

easiest way to work with elements of $GL_2(\mathbb{R})/GO_2(\mathbb{R})$ is to look at rows of the matrices (that is the basis elements of the shape) in the complex plane in the natural way, that is $(x, y) \leftrightarrow x + iy = z$.

Now if R_α is the rotation matrix with angle α, we can compute

$$(x, y)R_\alpha = (x\cos(\alpha) + y\sin(\alpha), -x\sin(\alpha) + y\cos(\alpha)) \leftrightarrow ze^{i\alpha} = zR_\alpha,$$

so that on any basis ω, θ, the right action of $GO_2(\mathbb{R}) = \mathbb{R} \times O_2(\mathbb{R})$ is simply multiplying both basis element by the complex number corresponding to the desired scaling and rotation.

It is then easy to apply an element of $GO_2(\mathbb{R})$ to get a matrix of the form $1, z$, with $Im(z) > 0$.

$$\begin{bmatrix}\omega\\ \theta\end{bmatrix} \equiv \begin{bmatrix}\omega\\ \theta\end{bmatrix} \frac{1}{|\omega|} R_{-Arg(\omega)} = \begin{bmatrix}\omega\\ \theta\end{bmatrix} \frac{1}{\omega} = \begin{bmatrix}1\\ \theta/\omega\end{bmatrix}$$

We can then apply a reflection to ensure that $z = \theta/\omega$ has positive real part.

Let

$$\mathbb{H} = \left\{ \begin{bmatrix}1\\ z\end{bmatrix} : Im(z) > 0 \right\}$$

be our fundamental domain for $GL_2(\mathbb{R})/GO_2(\mathbb{R})$. For convenience we will often simply write z for an element $\begin{bmatrix}1\\ z\end{bmatrix}$ in $\mathbb{H}$.

We might then (conveniently) look at the map

$$V_\mathbb{R} \to \mathbb{H}$$

$$\nu \to z_\nu$$

2.1.1 Action of $GL_2(\mathbb{R})$

The reason why this map is so useful is because we can define an action of $GL_2(\mathbb{R})$ on both sides that makes this map equivariant which will enable us to fix a binary cubic form and apply elements of $GL_2(\mathbb{R})$ to obtain a new one, which is equivalent to building shapes of cubic rings by looking at the image under the map.

The advantage of looking at $S(f)$ instead of $R(\nu)$ is that we will see the action of $GL_2(\mathbb{Z})$ on the set of shapes with a basis is very easy to describe (and not so easy on the set on rings with a basis).

Define the (left) action of $GL_2(\mathbb{R})$ on $V_\mathbb{R}$: For $\gamma \in GL_2(\mathbb{R})$, and a binary cubic form $\nu \in V_\mathbb{R}$,

$$\gamma \cdot f(x, y) := \frac{1}{det(\gamma)} f((x, y) \cdot \gamma).$$

One can compute that the map of Theorem 2.1.3 induces the following left action of $GL_2(\mathbb{R})$ on $GL_2(\mathbb{R})/GO_2(\mathbb{R})$:

$$\gamma \cdot \begin{bmatrix}\omega\\ \theta\end{bmatrix} = \gamma \begin{bmatrix}\omega\\ \theta\end{bmatrix},$$

which correspond to the change of basis of the 2 dimensional vector space. The corresponding action of

$\mathbb{H}$ is then simply

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \pm \frac{c+dz}{a+bz},$$

where the $\pm$ is whatever ensures that $Im(\gamma \cdot z) > 0$.

It will be useful to keep in mind the Iwasawa (or NAK) decomposition (see [8]) of $GL_2(\mathbb{R})$ and how some elements in the decomposition acts on both sides of the (equivariant) map $V_{\mathbb{R}} \to \mathbb{H}$.

$$GL_2(\mathbb{R}) = NAK\Lambda,$$

where

$$N = \left\{ \begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} : u \in \mathbb{R} \right\}, A = \left\{ \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} : t > 0 \right\}, K' = O_2(\mathbb{R}), \Lambda = \left\{ \begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} : \lambda > 0 \right\}.$$

On $V_{\mathbb{R}}$:

$$\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot (a,b,c,d) = (t^{-3}a, t^{-1}b, tc, t^3 d)$$

$$\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} \cdot (a,b,c,d) = (a, 3ua+b, 3u^2a+2ub+c, u^3a+u^2b+uc+d)$$

$$\lambda \cdot (a,b,c,d) = \begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} \cdot \nu = (\lambda a, \lambda b, \lambda c, \lambda d)$$

and on $\mathbb{H}$:

$$\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot z = t^2 z$$

$$\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} \cdot z = z + u$$

$$\lambda \cdot z = z$$

The action of $SO_2(\mathbb{R})$ is not as neat as the other elements in the decomposition so we do not include the formulae here but we will see later in this section how the orbits of $\mathbb{H}$ under the action of $SO_2(\mathbb{R})$ on $\mathbb{H}$ look, as it will matter in Chapter 3.

2.1.2 Taking $G(\mathbb{R})$ orbits

So we have a $GL_2(\mathbb{R})$ equivariant map $V_{\mathbb{R}} \to GL_2(\mathbb{R})/GO_2(\mathbb{R})$. It induces a map on the $GL_2(\mathbb{Z})$ orbits:

$$GL_2(\mathbb{Z})\backslash V_{\mathbb{R}} \to GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})/GO_2(\mathbb{R})$$

Note this map *does not* induce a well defined action of $GL_2(\mathbb{R})$ as the left action of $GL_2(\mathbb{R})$ on $\mathcal{F}$ does not commute with the reduction modulo the left action of $GL_2(\mathbb{Z})$.

Since the left action of $GL_2(\mathbb{Z})$ on $GL_2(\mathbb{R})/GO_2(\mathbb{R})$ corresponds to the change of basis on the 2 dimensional lattice generated by the rows of the matrix, we might pick a specific type of basis to be our

fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})/GO_2(\mathbb{R})$. Let

$$\mathcal{F} = \left\{ \begin{bmatrix} 1 \\ z \end{bmatrix} \in \mathbb{H} : \text{ the rows form a Minkowski basis for the lattice that it generates} \right\}$$

be our fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})/GO_2(\mathbb{R})$. It turns out $\mathcal{F}$ is the usual fundamental domain for 2 dimensional lattices modulo scaling and rotating.

For $z \in \mathbb{H}$, define $\overline{z}$ to be its image in $\mathcal{F}$. We may then look at the map

$$GL_2(\mathbb{Z})\backslash V_{\mathbb{R}} \to \mathcal{F}$$

$$\nu \to \overline{z_\nu}$$

The action of $GL_2(\mathbb{Z})$ (resp. $GL_2(\mathbb{Q})$, resp. $GL_2(\mathbb{R})$) on an integral (resp. rational, resp. real) binary cubic form corresponds to the change of basis in the 2 dimensional free module over $\mathbb{Z}$ (resp. $\mathbb{Q}$, resp. $\mathbb{R}$). It then does not change the associated 2 dimensional module (the shape). In fact, it also does not change the associated cubic ring. We then have the following theorem that might also (and more appropriately) be referred to as the Delone-Fadeev correspondence.

Theorem 2.1.6. *(Delone-Faddeev correspondence) There are natural bijections*

$$GL_2(\mathbb{Z})\backslash V_{\mathbb{Z}} \leftrightarrow \{\textit{cubic rings over } \mathbb{Z}\}/\sim$$

$$GL_2(\mathbb{Q})\backslash V_{\mathbb{Q}} \leftrightarrow \{\textit{cubic rings over } \mathbb{Q}\}/\sim$$

$$GL_2(\mathbb{R})\backslash V_{\mathbb{R}} \leftrightarrow \{\textit{cubic rings over } \mathbb{R}\}/\sim$$

Proof. See [8] □

Remark 2.1.7. *Irreducible cubic rings over $\mathbb{Q}$ are cubic number fields*

Remark 2.1.8. *As mentioned before, the only cubic rings over $\mathbb{R}$ are $\mathbb{R}^3$ and $\mathbb{C} \times \mathbb{R}$.*

This tells us we can start with a fixed integral binary cubic form that corresponds to some order in a cubic field, and build new orders in the same cubic field by applying elements of $GL_2(\mathbb{Q})$, or in any other cubic field that maps to the same cubic ring over $\mathbb{R}$ by applying elements of $GL_2(\mathbb{R})$.

On the other hand, since there are only two cubic rings over $\mathbb{R}$ namely $\mathbb{R}^3$ and $\mathbb{R} \times \mathbb{C}$, Theorem 2.1.6 tells us that there are only two orbits for the action of $GL_2(\mathbb{R})$ on $V_{\mathbb{R}}$, namely $V_{\mathbb{R}}^{(1)}$, the elements of $V_{\mathbb{R}}$ that map to $\mathbb{R}^3$, or equivalently the elements of $V_{\mathbb{R}}$ with positive discriminant, and $V_{\mathbb{R}}^{(2)}$, the elements of $V_{\mathbb{R}}$ that map to $\mathbb{R} \times \mathbb{C}$, or equivalently the elements of $V_{\mathbb{R}}$ with negative discriminant. This fact will be convenient to prove the cubic case of Theorem 0.0.8 (bounds). Let ν_1 and ν_2 be two real binary cubic forms, with $R(\nu_1) \otimes \mathbb{R} = \mathbb{R}^3$ and $R(\nu_2) \otimes \mathbb{R} = \mathbb{R} \times \mathbb{C}$. That is we picked representatives for the two orbits of the action of $GL_2(\mathbb{R})$ on binary cubic forms. Then for any cubic ring R over $\mathbb{Z}$, there exist $i = 1, 2$, and $\gamma \in GL_2(\mathbb{R})$ such that

$$R = R(\gamma \cdot \nu_i).$$

Since multiplying γ by an element of $GL_2(\mathbb{Z})$ on $V_{\mathbb{Z}}$ corresponds to the change of basis of R, and thus does not change R, we may pick γ in a fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})$ that we pick so that $R(\gamma \cdot \nu_i)$ is given with a basis that is almost Minkowski.

For this reason, we define the following fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})$:

$$\mathcal{F}_G = \{\gamma \in GL_2(\mathbb{R}) : \text{ the image of } \gamma \text{ in } \mathbb{H} \text{ is in } \mathcal{F}\},$$

and note that elements of $\mathcal{F}_G$ do nicely take cubic rings with Minkowski bases to other cubic rings with almost Minkowski bases.

We can conveniently describe $\mathcal{F}_G$ using the NAK decomposition as in [8] by

$$\mathcal{F}_G = N'(t)A'K'\Lambda,$$

where

$$N'(t) = \left\{ \begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} : u \in I(t) \right\}, A' = \left\{ \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} : t \geq \sqrt[4]{3}/\sqrt{2} \right\}, K' = SO_2(\mathbb{R}), \Lambda = \left\{ \begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} : \lambda > 0 \right\},$$

where $I(t)$ is the union of one or two subintervals of $[-1/2, 1/2]$ depending on t. In particular, in $t \geq 1$, then $I(t) = [-1/2, 1/2]$.

In this chapter, when we prove the existence and bound theorems, we only really care about the fact that we can reach R from $R(\nu_i)$ with at least one element $\gamma \in \mathcal{F}_G$, and we will see that we can control how a Minkowski basis for R would look like depending on γ.

In Chapter 3, when we actually count orders with a given form of Minkowski basis, we care about double counting. It will then be best to think as $\mathcal{F}_G \cdot v_i$ as a multiset. One can easily check that $\mathcal{F}_G \cdot v_i$ is the union of n_i fundamental domains (that do overlap) for $GL_2(\mathbb{Z})\backslash V_{\mathbb{R}}$, where n_i is the order of the stabilizer of ν_i in $GL_2(\mathbb{R})$. Now by the Delone-Faddeev correspondence, the stabilizer of ν_i in $GL_2(\mathbb{R})$ is naturally isomorphic the group of ring automorphisms of $R(\nu_i)$ (see Proposition 12 in [8]). We then have $n_1 = Aut_{\mathbb{R}}(\mathbb{R}^3) = 6$ and $n_2 = Aut_{\mathbb{R}}(\mathbb{R} \times \mathbb{C}) = 2$.

Now for "most" $\nu \in V_{\mathbb{R}}^{(i)}$, ν will be represented exactly n_i times in $\mathcal{F}_G \cdot \nu_i$. This is explained in more details in [8]. We may then count everything as γ run though elements of the $\mathcal{F}_G$ and divide by n_i.

2.1.3 Orbits of $SO_2(\mathbb{R})$ in $\mathbb{H}$

We saw above that $SO_2(\mathbb{R})$ is the only element of the NAK decomposition whose action on $\mathbb{H}$ is not very easy to visualize. As it will matter in Chapter 3, when we will count rings with a given sort of Minkowski basis, let us see what the orbits look like.

Let's recall that the left action of $GL_2(\mathbb{R})$ on $\mathbb{H}$ is

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \cdot z = \pm \frac{c + dz}{a + bz},$$

where the $\pm$ is whatever ensures that the imaginary part is positive.

Let $k = k_\alpha = \begin{bmatrix} \cos(\alpha) & -\sin(\alpha) \\ \sin(\alpha) & \cos(\alpha) \end{bmatrix}$ be the rotation matrix with angle α. It is easy to see that $k \cdot i = i$. Now suppose that $z = it$, for some $t > 1$. We can compute

$$k_\alpha \cdot (it) = \left(\frac{\cos(\alpha)\sin(\alpha)(1 - t^2)}{\cos^2(\alpha) + \sin^2(\alpha)t^2} \right) + i \left(\frac{t}{\cos^2(\alpha) + \sin^2(\alpha)t^2} \right)$$

and see that the SO_2 orbits of it is a circle centered at $i\left(\frac{t^2+1}{2t}\right)$ and radius $\frac{t^2-1}{2t}$, which, as t varies from 1 to ∞, covers the whole upper half plane.

It is worth mentioning the lowest point on the orbit of it is $\frac{i}{t}$.

2.1.4 Image of a ball in $\mathbb{H}$

For some $C > 0$ that will be the "radius" of the ball, we define a ball in $V_{\mathbb{R}}$ by $B(C) := \{\nu = (a, b, c, d) \in V_{\mathbb{R}} : 3a^2+b^2+c^2+3d^2 \leq C^2 \text{ and } |Disc(\nu)| \geq 1\}$. One can check the advantage of defining balls this way is that they are $SO_2(\mathbb{R})$ invariant. Thus the image of $B(C)$ in $\mathbb{H}$ is of the form $\cup_{1<t\leq T} SO_2(\mathbb{R}) \cdot (it)$, for some $T > 1$ that grows with C, which by the above discussion on the $SO_2(\mathbb{R})$ orbits is the disc centered at $i\left(\frac{T^2+1}{2T}\right)$ and radius $\frac{T^2-1}{2T}$.

2.1.5 The totally real case

In the case where $R(\nu)$ is totally real, or equivalently that $R(\nu) \otimes \mathbb{R} = \mathbb{R}^3$, we can easily make the map $V_{\mathbb{R}} \to GL_2(\mathbb{R})/GO_2(\mathbb{R})$ very explicit. While it worth mentioning it, this will not be used anywhere in this paper.

Let's recall for a binary cubic form $\nu(x, y) = ax^3 + bx^2y + cxy^2 + dy^3$, $R(\nu) =< 1, v_2, v_3 >$ with

$$\begin{aligned} v_2v_3 &= -ad \\ v_2^2 &= -ac - bv_2 + av_3 \\ v_3^2 &= -bd - dv_2 + cv_3 \end{aligned}$$

Using this we can substitute $v_3 = -ad/v_2$ (resp. $v_2 = -ad/v_2$) in the second (resp. third) equation and get the minimal polynomial for v_3 (resp. v_2). We get

$$\begin{aligned} v_2^3 - cv_2^2 + bdv_2 + ad^2 &= 0 \\ v_3^3 + bv_3^2 + acv_3 + a^2d &= 0 \end{aligned}$$

Now if a, b, c, d are given we can actually solve these and we can then compute $Tr(v_2) = c, Tr(v_3) = -b$, and let

$$\begin{aligned} w_2 &= 3v_2 - c \\ w_3 &= 3v_3 + b \end{aligned}$$

so that w_3, w_2 is a basis for the 2-dimensional lattice $S(f)$. Again if a, b, c, d are given, we can actually compute all this explicitly and then have $S(f)$ explicitly.

But in the non totally real case, it is not easy to find a nice formula depending on a, b, c, d to express $S(\nu)$. The advantage of the totally real case it that we have $|v_2|^2 = c^2 - 2bd, |v_3|^2 = b^2 - 2ac$.

We can then compute

$$|w_3|^2 = \sum_{i=1}^{3} \sigma_i(3v_3 + b)^2 = 9|v_3|^2 + 6bTr(v_3) + 3b^2 = 6b^2 - 18ac$$

and similarly

$$|w_2|^2 = 6c^2 - 18bd$$

as well as the angle between them using

$$< w_3, w_2 >= \sum \sigma_i((3v_3 + b)(3v_2 - c)) = 9Tr(v_3v_2) + 3bTr(v_2) - 3cTr(v_3) - 3bc$$

$$= -27ad + 3bc$$

$$\implies Arg(w_3, w_2) = ArcCos\left(\frac{-27ad + 3bc}{\sqrt{(6b^2 - 18ac)(6c^2 - 18bd)}}\right).$$

In other words we have an explicite formula for the quadratic form on $S(\nu)$ namely (up to scaling)

$$\begin{aligned} Q(xw_3 + yw_2) &= x^2|w_3|^2 + 2xy < w_3, w_2 > +y^2|w_2|^2 \\ &= x^2(b^2 - 3ac) + xy(bc - 9ad) + y^2(c^2 - 3bd) \\ &= \begin{bmatrix} x & y \end{bmatrix} \begin{bmatrix} b^2 - 3ac & \frac{bc-9ad}{2} \\ \frac{bc-9ad}{2} & c^2 - 3bd \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix} \end{aligned}$$

We now can also write a formula for the image z of (a, b, c, d) in $\mathbb{H}$,

$$|z|^2 = \frac{c^2 - 3bd}{b^2 - 3ac}$$

$$Arg(z) = ArcCos\left(\frac{-27ad + 3bc}{\sqrt{(6b^2 - 18ac)(6c^2 - 18bd)}}\right).$$

2.2 Existence - Proof of the cubic case of Theorem 0.0.7

In this section, we give another proof, this time using the Delone-Faddeev correspondence, for the cubic case of Theorem 0.0.7 that we recall:

Theorem 2.2.1. *For any cubic number field K, and any $\delta_2, \delta_3 \in \mathbb{Q}$ satisfying $\delta_2 \leq \delta_3$, $\delta_2 + \delta_3 = 1/2$ and $\delta_3 \leq 2\delta_2$, there is a family of orders in K with Minkowski type δ_2, δ_3.*

Remark 2.2.2. *Or equivalently, we might replace "$\delta_3 \leq 2\delta_2$" by "$\delta_3 \leq 1/3$".*

Proof. Let $\nu_0 = (a_0, b_0, c_0, d_0)$ be a fixed non degenerate binary cubic form that corresponds, under the Delone-Faddeev correspondence (Theorem 2.1.1), to an order in a fixed field K of our choice. ν_0 gives a cubic ring and its shape with a basis $v_{0,2}, v_{0,3}$. Now for an integer n, we let

$$\nu_n = \begin{bmatrix} 2^n & \\ & 2^n \end{bmatrix} \cdot \nu_0 = (2^n a_0, 2^n b_0, 2^n c_0, 2^n d_0).$$

We get a family of orders all in K (the same cubic field that we started with). Each ν_n has discriminant $|D_n| \asymp 2^{4n}$, and gives a shape with a basis $v_{n,2}, v_{n,3}$ with

$$\begin{bmatrix} v_{n,2} \\ v_{n_3} \end{bmatrix} = \begin{bmatrix} 2^n & \\ & 2^n \end{bmatrix} \cdot \begin{bmatrix} v_{0,2} \\ v_{0_3} \end{bmatrix} = \begin{bmatrix} 2^n v_{0,2} \\ 2^n v_{0_3} \end{bmatrix}.$$

We then have $|v_{n,2}| \asymp |v_{n,3}| \asymp 2^n \asymp |D|^{1/4}$, and thus these $\nu_n' s$ correspond to a family of cubic orders with Minkowski type $1/4, 1/4$.

Now let

$$\nu_n' = \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot \nu_n = (t^{-3}2^n a_0, t^{-1}2^n b_0, t2^n c_0, t^3 2^n d_0)$$

then

$$\begin{bmatrix} v_{n,2}' \\ v_{n_3}' \end{bmatrix} = \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot \begin{bmatrix} v_{n,2} \\ v_{n_3} \end{bmatrix} = \begin{bmatrix} t^{-1} v_{n,2} \\ t v_{n_3} \end{bmatrix},$$

and thus

$$|v_{n,2}'| \asymp t^{-1}|D_n|^{1/4} \text{ and } |v_{n,3}'| \asymp t|D_n|^{1/4}$$

and

$$D_n' = D_n.$$

So for any $\delta_2 \in [1/6, 1/4] \cap \mathbb{Q}$, to get a family of orders with Minkowski type $\delta_2, 1/2 - \delta_2$, we want

$$t^{-1}|D_n|^{1/4} \asymp |D_n|^{\delta_2},$$

which is equivalent to

$$t^{-1}2^n \asymp 2^{4n\delta_2} \iff t \asymp 2^{n(1-4\delta_2)}.$$

Now we can pick suck t since for $\delta_2 \in [1/6, 1/4] \cap \mathbb{Q}$, we have $0 \leq (1 - 4\delta_2) \leq 1/3$, so for n big enough, we can take $t = 2^{n(1-4\delta_2)} \in \mathbb{Z}$, and $t^3 | 2^n$, so that ν_n' is integral as needed. □

2.3 Bounds - Proof of the cubic case of Theorem 0.0.8

In this section, we prove, using the Delone-Faddeev correspondence, the cubic case of Theorem 0.0.8 that we recall:

Theorem 2.3.1. *Let R be an order in a cubic number field K, with Minkowski basis $v_1 = 1, v_2, v_3$, then*

$$|v_3| \ll |v_2|^2,$$

or equivalently

$$|v_3| \ll |Disc(R)|^{1/3}.$$

Remark 2.3.2. *We dropped the condition that K has no non trivial subfield since cubic field never have a non trivial subfield.*

Proof. As mentioned in Section 2.1, since there are only two cubic rings over $\mathbb{R}$ namely $\mathbb{R}^3$ and $\mathbb{R} \times \mathbb{C}$, Theorem 2.1.6 tells us that there are only two orbits for the action of $GL_2(\mathbb{R})$ on $V_{\mathbb{R}}$, namely $V_{\mathbb{R}}^{(1)}$, the elements of $V_{\mathbb{R}}$ that map to $\mathbb{R}^3$, or equivalently the elements of $V_{\mathbb{R}}$ with positive discriminant, and $V_{\mathbb{R}}^{(2)}$, the elements of $V_{\mathbb{R}}$ that map to $\mathbb{R} \times \mathbb{C}$, or equivalently the elements of $V_{\mathbb{R}}$ with negative discriminant. Let ν_1 and ν_2 be two real binary cubic forms, with $R(\nu_1) \otimes \mathbb{R} = \mathbb{R}^3$ and $R(\nu_2) \otimes \mathbb{R} = \mathbb{R} \times \mathbb{C}$. That is we picked representatives for the two orbits of the action of $GL_2(\mathbb{R})$ on binary cubic forms. Then for any

cubic ring R over $\mathbb{Z}$, there exist $i = 1, 2$, and $\gamma \in GL_2(\mathbb{R})$ such that

$$R = R(\gamma \cdot \nu_i).$$

Since multiplying γ by an element of $GL_2(\mathbb{Z})$ on $V_{\mathbb{Z}}$ corresponds to the change of basis of R, and thus does not change R, any other γ in the same equivalence class modulo the left action of $GL_2(\mathbb{Z})$ on $GL_2(\mathbb{R})$ would do.

Let R be an order in a cubic field with big discriminant D. We want to find bounds on elements of a Minkowski basis for R. Let $\gamma \in GL_2(\mathbb{R})$ such that $R = R(\gamma \cdot \nu_i)$. We know that, for any choice of γ, we will have $\gamma \cdot \nu_i$ must be an irreducible integral cubic form. Now we want to pick γ such that $\gamma \cdot \nu_i$ gives a almost Minkowski basis for R.

Method 1: Look at the NAK decomposition of γ:

$$\gamma = \begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} \begin{bmatrix} t & \\ & t^{-1} \end{bmatrix} K\lambda,$$

for some $u \in \mathbb{R}, t \in \mathbb{R}^+, K \in O_2(\mathbb{R}), \lambda \in \mathbb{R}^+$. We already know that $\lambda = D/Disc(\nu_i)$.

Before and/or after applying each matrix in the decomposition, we might apply some matrix in $GL_2(\mathbb{Z})$ of our choice to keep the basis almost Minkowski. Before and after applying $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}$, for some $t \in \mathbb{R}^+$, we may apply $\begin{bmatrix} & 1 \\ 1 & \end{bmatrix}$, to obtain $\begin{bmatrix} t & \\ & t^{-1} \end{bmatrix}$, and therefore we may assume $t \geq 1$. After applying $\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix}$, for some $u \in \mathbb{R}$, let m be the closest integer to u, we may apply $\begin{bmatrix} 1 & \\ -m & 1 \end{bmatrix}$, and therefore we may assume $|u| \leq 1/2$.

We can then consider the subset of $GL_2(\mathbb{R})$ obtained by looking at the Iwasawa decomposition and restrict to $t \geq 1$ and $-1/2 \leq u \leq 1/2$. Note that this set contains Gauss's fundamental domain.

Method 2: We may assume that $\gamma \in \mathcal{F}_G$, our fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})$ as defined in Section 2.1 by

$$\mathcal{F}_G = \{\gamma \in GL_2(\mathbb{R}) : \text{ the image of } \gamma \text{ in } \mathcal{H} \text{ is in } \mathcal{F}\}.$$

By the definition of $\mathcal{F}_G$, $\mathbb{H}$ and $\mathcal{F}$, the rows of $\gamma \in \mathcal{F}_G$ are a Minkowski basis for the 2 dimensional lattice generated by them. Thus $\gamma \cdot v_i$ will give an almost Minkowski basis for the shape of R.

Now we can conveniently describe $\mathcal{F}_G$ using the NAK decomposition as in [8] by $\lambda > 0, t \geq \sqrt[4]{3}/\sqrt{2}, \lambda > 0, k \in SO_2(\mathbb{R})$ and u in some subinterval of $[-1/2, 1/2]$ (depending on t). Note this is looking pretty close (but a little stronger) to what we derived is way 1.

Let us start by saying we know $\lambda = (D/Disc(\nu_i))^{1/4}$. Now the action of λ, just multiply each basis element by λ, each coefficient of ν_i by λ and its discriminant by $\lambda^4 = D/Disc(\nu_i)$. $\lambda \cdot \nu_i$ then gives a cubic ring with discriminant D and a basis for its shape that clearly almost Minkowski and of Minkowski type $1/4, 1/4$. Also note that the coefficients of $\lambda \cdot \nu_i$ are all $\ll |D|^{1/4}$.

The action of k doesn't change the discriminant and the length of the basis elements. Thus $k\lambda \cdot \nu_i$ still gives a cubic ring with discriminant D and a basis for its shape that almost Minkowski and of Minkowski type $1/4, 1/4$. Also the coefficients of $\lambda \cdot \nu_i$ are still all $\ll |D|^{1/4}$.

The action of $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}$, for $t \geq 1$, on the shape multiplies the first basis element by t^{-1} and the second by t, and doesn't change the discriminant. So the new basis is still Minkowski but the first basis element will get shorter than second as t increases. Thus $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} k\lambda \cdot \nu_i$ gives a cubic ring of discriminant D and a basis for its shape that is Minkowski and of Minkowski type $\delta_2, \delta 3$, for some $\delta_2 \leq \delta_3$. We will see shortly (after applying the last element of the decomposition) that for the resulting form to be integral and irreducible we will get an upper bound on t ($t^3 \ll |D|^{1/4}$) which will induce an upper bound on δ_3 and therefore prove Theorem 2.3.1. Now its action on a cubic form is (a, b, c, d)

$$\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot (a, b, c, d) = (t^{-3}a, t^{-1}b, tc, t^3 d)$$

The action of $\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix}$, for $-1/2 \leq u \leq 1/2$ on the shape sends a basis v_2, v_3 to $v_2, uv_2 + v_3$. If v_2, v_3 is almost Minkowski, since $|u| \leq 1/2$, we have that $|uv_2 + v_3| \asymp |v_3|$. Thus $\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} k\lambda \cdot \nu_i$ still gives a cubic ring of discriminant D and a basis for its shape that is almost Minkowski and of the same form δ_2, δ_3 as the one that $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} k\lambda \cdot \nu_i$ gives. Now its action on a cubic form is (a, b, c, d)

$$\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} \cdot (a, b, c, d) = (a, 3au + b, 3au^2 + 2bu + c, au^3 + bu^2 + cu + d),$$

so for the resulting cubic form to be integral and irreducible, we need $|a| \geq 1$ (if $a = 0$ then $y|f(x, y)$), so we need the 1st coefficient of $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} k\lambda \cdot \nu_i$ (from the previous step) to have absolute value ≥ 1.

Since the coefficients of $k\lambda \cdot \nu_i$ as $\ll |D|^{1/4}$, we then need

$$t \ll |D|^{1/12},$$

which gives the bound

$$|v_3| \ll t|D|^{1/4} \ll |D|^{1/3},$$

and proves Theorem 2.3.1. □

Chapter 3

Counting cubic orders with a given form of Minkowski basis

In this chapter, we will use the Delone-Faddeev correspondence and a few properties, see Section 2.1 for background, to estimate, when ordered by discriminant, the number of cubic orders with a given form of Minkowski basis.

Let $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{R}}$) be the set of integral (resp. real) binary cubic forms. We know that the action of $GL_2(\mathbb{R})$ on $V_{\mathbb{R}}$ gives two orbits namely $V_{\mathbb{R}}^{(1)}$ the set of real binary cubic forms with positive discriminant and $V_{\mathbb{R}}^{(2)}$ the set of real binary cubic forms with negative discriminant. For each i, let $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$.

As in [8], for a $GL_2(\mathbb{Z})$-invariant subset S of $V_{\mathbb{Z}}^{(i)}$, let $N(S;X)$ be the number of irreducible $GL_2(\mathbb{Z})$-orbits on S having discriminant less than X.

Let us recall that by the Delone-Faddeev correspondence, we have the determinant preserving map

$$GL_2(\mathbb{Z})\backslash V_{\mathbb{Z}} \leftrightarrow \{ \text{ cubic rings over } \mathbb{Z}\},$$

where irreducible cubic forms corresponds to orders in cubic fields.

So S corresponds to a subset of the set of cubic rings over $\mathbb{Z}$, and thus $N(S;X)$ also counts the number of orders in cubic fields with discriminant less than X and that are in the subset corresponding to S.

We start by setting up the integral using is equation (20) in [8]. That is, we let $d\nu$ denote the usual Euclidean measure on $V_{\mathbb{R}}$ (normalized so that $V_{\mathbb{Z}}$ has co-volume 1) and let $dg = t^{-2}dud^{\times}tdkd^{\times}\lambda$ be the Haar measure of $GL_2(\mathbb{R})$ obtained from its Iwasawa decomposition (where dk is normalized to have measure 1 on $SO_2(\mathbb{R})$). And for a constant $C \geq 1$, let $B = B(C) = \{w = (a,b,c,d) \in V_{\mathbb{R}} : 3a^2 + b^2 + c^2 + 3d^2 \leq C^2, |Disc(w)| \geq 1\}$. Then one easily checks that B is $SO_2(\mathbb{R})$-invariant (this will matter). We have

$$N(S;X) = \frac{1}{M_i} \int_{g \in \mathcal{F}_G} \#\{x \in S^{irr} \cap gB : |Disc(x)| < X\} dg + O(X^{3/4+\epsilon}), \tag{3.1}$$

where

$$M_i = \frac{n_i}{2\pi} \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} |Disc(\nu)|^{-1} d\nu,$$

where we recall that $n_1 = Aut_{\mathbb{R}}(\mathbb{R}^3) = 6$ and $n_2 = Aut_{\mathbb{R}}(\mathbb{R} \times \mathbb{C}) = 2$ so that for any $\nu_i \in V_{\mathbb{R}}^{(i)}$, "most" elements in the multiset $\mathcal{F}_G \cdot \nu_i$ are represented exactely n_i times. The error term comes from those points (C_3 points) that no not appear exactly n_i times in $\mathcal{F}_G \cdot \nu_i$ as explained in [8].

From this (after a slight modification as we will see) we will use the following elementary proposition from the geometry of numbers. We state is as in [8] which itself refers of [10] for a proof. Before stating the proposition, we need the following definitions: A multiset $\mathcal{R} \in \mathbb{R}^n$ is said to be *measurable* if $\mathcal{R}_k$ is measurable for all k, where $\mathcal{R}_k$ denotes the set of those points in $\mathcal{R}$ having fixed multiplicity k. Given a measurable multiset $\mathcal{R} \subset \mathbb{R}^n$, we define its volume in the natural way, that is, $Vol(\mathcal{R} = \sum_k k \cdot Vol(\mathcal{R}_k)$, where $Vol(\mathcal{R}_k)$ denotes the usual Euclidean volume of $\mathcal{R}_k$.

Proposition 3.0.1. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most l. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation on $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$Vol(\mathcal{R}) + O(\max\{Vol(\overline{\mathcal{R}}, 1)\}),$$

where $Vol(\overline{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implies constant depends only on n, m, k and l.

Now, given $\delta \in (1/6, 1/4]$, we are interested in orders in cubic fields with a Minkowski basis of Minkowski type $\delta, 1/2 - \delta$. We need to define an appropriate set S, that will record this.

As in Section 2.1, for $\nu \in V_{\mathbb{R}}$, let $\overline{z_\nu}$ be the image of ν is $\mathcal{F}$, that our usual fundamental domain of $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})/GO_2(\mathbb{R})$. For $0 < c_1 < c_2$, (if $\delta = 1/4$, we insist that $c_1 > 2/\sqrt{3}$). We define

$$S_\delta = \{\nu \in V_{\mathbb{R}} : c_1 |Disc(\nu)|^{1/2-2\delta} \leq Im(\overline{z_\nu}) < c_2 |Disc(\nu)|^{1/2-2\delta}\}.$$

Lemma 3.0.2. *For $\nu \in S_\delta \cap V_{\mathbb{Z}}$, a Minkowski basis for $R(\nu)$, is of Minkowski type $\delta, 1/2 - \delta$.*

Proof. We have $|Disc(\nu)|^{1/2-2\delta} \asymp Im(\overline{z_\nu}) \asymp \frac{|v_3|}{|v_2|} \asymp \frac{|Disc(\nu)|^{1/2}}{|v_2|^2}$ and then $|v_2| \asymp |Disc(\nu)|^\delta$. □

In Section 3.1, we prove that

Theorem 3.0.3. *For each $i = 1, 2$ and $\delta \in (1/6, 1/4] \cap \mathbb{Q}$. We have*

$$N(S_\delta \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{\pi}{n_i}\left(\frac{1}{c_1} - \frac{1}{c_2}\right)\left(\frac{1}{2+8\delta}\right) X^{1/2+2\delta} + O(X^{1-\delta}) + O(X^{3/4+\epsilon}).$$

Note that the main term strictly beats the error term. Also note if $\delta = 1/4$, we get a main term of X, which makes sense since by [6] most irreducible cubic rings have a Minkowski basis of Minkowski type $1/4, 1/4$ with $\asymp X$ of them. In this case ($\delta = 1/4$), the first error term is smaller that the second one. Now if $\delta < 1/4$, then the second error term is smaller than the first one and as δ approaches $1/6$, we get both the main term and the error term approach $X^{5/6}$.

In Section 3.2, we combine this method with a Sieving argument that enable us to now count the cubic orders with a given form of Minkowski basis that are **maximal**, and therefore are ring of integers

of a cubic field. So if $\mathcal{U}$ denote the subset of elements of $V_{\mathbb{Z}}$ corresponding to a cubic ring that is maximal, we will prove the following theorem:

Theorem 3.0.4. *For $\delta \in (1/5, 1/4] \cap \mathbb{Q}$*

$$N(S_\delta \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = \left(\prod_p \frac{(p^3-1)(p^2-1)}{p^5}\right)\left(\frac{\pi}{n_i}\right)\left(\frac{1}{c_1}-\frac{1}{c_2}\right)\left(\frac{1}{2+8\delta}\right)X^{1/2+2\delta} + O_\epsilon(X^{1-\delta/2+\epsilon}).$$

Note this show that for $\delta \in (1/5, 1/4]$, a positive portion of the irreducible cubic rings of a given form of Minkowski basis are maximal.

Also note when counting cubic rings that are maximal, the main term only beats the error term when $\delta > 1/5$. This is due to the sieving argument increasing the error term.

3.1 An estimate for the number of cubic orders with a given form of Minkowski basis

In this section, we take

$$S_\delta = \{\nu \in V_{\mathbb{R}} : c_1|Disc(\nu)|^{1/2-2\delta} \leq Im(\overline{z_\nu}) < c_2|Disc(\nu)|^{1/2-2\delta}\},$$

so that $N(S_\delta \cap V_{\mathbb{Z}}^{(i)}; X)$ is the number of **irreducible** $GL_2(\mathbb{Z})$-orbits on $S_\delta \cap V_{\mathbb{Z}}^{(i)}$ having discriminant less than X, which by the Delone-Faddeev correspondence is also the number orders in cubic fields, with discriminant positive if $i = 1$ or negative if $i = 2$ and less than X in absolute value, and (by Lemma 3.0.2) with Minkowski type $\delta, 1/2 - \delta$.

We want to prove the following Theorem:

Theorem 3.1.1. *For each $i = 1, 2$ and any $\delta \in (1/6, 1/4] \cap \mathbb{Q}$, we have*

$$N(S_\delta \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{\pi}{n_i}\left(\frac{1}{c_1}-\frac{1}{c_2}\right)\left(\frac{1}{2+8\delta}\right)X^{1/2+2\delta} + O(X^{1-\delta}) + O(X^{3/4+\epsilon}).$$

Proof of Theorem 3.1.1

Applying (3.1) with $S = S_\delta \cap V_{\mathbb{Z}}^{(i)}$, we have

$$N(S_\delta \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{M_i}\int_{g=u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}\lambda \in N'(t)A'\Lambda} \#\{x \in S_\delta \cap B_i(u,t,\lambda,X) \cap V_{\mathbb{Z}}^{irr}\} t^{-2} du d^\times t d^\times \lambda dk + O(X^{3/4+\epsilon}), \tag{3.2}$$

where

$$B_i(u,t,\lambda,X) = u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}\lambda B \cap \{\nu \in V_{\mathbb{R}}^{(i)} : |Disc(\nu)| < X\}$$

and

$$M_i = \frac{n_i}{2\pi}\int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} |Disc(\nu)|^{-1} d\nu.$$

Now that for each fixed u, t, λ, we have that $S_\delta \cap B_i(u,t,\lambda,X)$ is a bounded, semi-algebraic multi-sets in $\mathbb{R}^4$ defined by a uniformly bounded number of polynomial inequalities of uniformly bounded degree. Note that we needed δ to be rational here. So, if we can get rid of "irr" in (3.2), we would be able apply Proposition 3.0.1. To do this we use the following lemma from [8]:

Lemma 3.1.2. *Let $\nu \in B$ be any point of non zero discriminant, where B is any fixed compact subset of $V_\mathbb{R}$ containing only elements having discriminant greater than 1. Then the number of integral binary cubic forms $(a,b,c,d) \in \mathcal{F}_G \cdot \nu$ with discriminant less than X, that are reducible with $a \neq 0$ is $O(X^{3/4+\epsilon})$, where the implied constant depends only on B.*

We can then modify (3.2) a little bit and get

$$N(S_\delta \cap V_\mathbb{Z}^{(i)}; X) = \frac{1}{M_i} \int_{g=u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}_{\lambda \in N'(t)A'\Lambda}} \#\{(a,b,c,d) \in S_\delta \cap B_i(u,t,\lambda,X) \cap V_\mathbb{Z} : a \neq 0\} t^{-2} du d^\times t d^\times \lambda dk + O(X^{3/4+\epsilon}). \tag{3.3}$$

We are now ready to apply Proposition 3.0.1 since after adding the condition $a \neq 0$ to $S_\delta \cap B_i(u,t,\lambda,X)$, we still have a bounded, semi-algebraic multi-sets in $\mathbb{R}^4$ defined by a uniformly bounded number of polynomial inequalities of uniformly bounded degree, and thus we can estimate

$$\#\{(a,b,c,d) \in S_\delta \cap B_i(u,t,\lambda,X) \cap V_\mathbb{Z} : a \neq 0\} = \begin{cases} 0 & \text{if } C\lambda < t^3 \\ Vol(S_\delta \cap B_i(u,t,\lambda,X)) + O(t^3\lambda^3) + O(1) & \text{otherwise} \end{cases} \tag{3.4}$$

Note that we will be interested in $t \asymp \lambda^{1-4\delta}$, in which case $\lambda = \omega(t^3)$, and thus the first line will not be used. In other words, we will not use the fact that we are counting irreducible elements or those with $a \neq 0$ in the following computations.

Let us first compute the main term. By the change of variable $\nu' = u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda \cdot \nu$, we compute

$$Vol(S_\delta \cap B_i(u,t,\lambda,X)) = \lambda^4 Vol(B \cap \{\nu \in V_\mathbb{R}^{(i)} : |Disc(\nu)| < X/\lambda^4 \text{ and}$$

$$c_1(\lambda^4|Disc(\nu)|)^{1/2-2\delta} \leq Im\left(\overline{u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda \cdot z_\nu}\right) < c_2(\lambda^4|Disc(\nu)|)^{1/2-2\delta}\})$$

Lemma 3.1.3. *For $n\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda \in N'(t)A'\Lambda$ with t big enough to contribute to the main term, we may assume (by making B smaller if necessary) that for all $\nu \in B$, we have*

$$c_1(\lambda^4|Disc(\nu)|)^{1/2-2\delta} \leq Im\left(\overline{u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda \cdot z_\nu}\right) < c_2(\lambda^4|Disc(\nu)|)^{1/2-2\delta}\})$$

$$\iff c_1(\lambda^4|Disc(\nu)|)^{1/2-2\delta} \leq t^2 Im(z_\nu) < c_2(\lambda^4|Disc(\nu)|)^{1/2-2\delta}\})$$

Proof. First note that

$$Im\left(\overline{u\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda \cdot z_\nu}\right) = Im(\overline{t^2 z_\nu + u})$$

Case 1 : $\delta > 1/4$. Let $M = max_{\nu \in B} \frac{1}{\sqrt{Im(z_\nu)}}$. If $t > M$, then $Im(t^2 z_\nu + u) = t^2 Im(z_\nu) > 1$ for all $\nu \in B$, and in this case

$$Im(\overline{t^2 z_\nu + u}) = t^2 Im(z_\nu)$$

We claim that only these big enough values of t will contribute to the main term.

If $t \leq M$, then for $\nu \in B_i(u, t, \lambda, X)$, we have $Im(\overline{z_\nu}) \ll 1$. So ν cannot be in S_δ unless $\lambda \ll 1$, and thus this case will can contribute to the error term.

Case 2 : $\delta = 1/4$. In this case, we insisted that $c_1 > 2/\sqrt{3}$, and we want to show that

$$c_1 \leq Im(\overline{t^2 z_\nu + u}) < c_2 \iff c_1 \leq t^2 Im(z_\nu) < c_2$$

Recall that $\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \in A'$ for $t > \sqrt[4]{3}/\sqrt{2}$. By taking B to be a smaller ball (after fixing c_1), we may assume that for any $\nu \in B$, we have

(1) $(\sqrt{3}/2) Im(z_\nu) > 1/c_1$

(2) $(\sqrt{3}/2) z_\nu$ is above the mess to send to $\mathcal{F}$

To see that this is possible, note that (1) is equivalent to $Im(z_\nu) > \frac{2/\sqrt{3}}{c_1}$, which is smaller than one. Now as we saw in Section 2.1, the lowest point in the image of B in $\mathbb{H}$ if i/T, where T can reach any value greater than one depending on the size of B.

If $t^2 z_\nu + u \in \mathcal{F} + \mathbb{Z}$, then $Im(\overline{t^2 z_\nu + u}) = t^2 Im(z_\nu)$, and we're done. If $t^2 z_\nu + u \notin \mathcal{F} + \mathbb{Z}$, there there exist $k \in \mathbb{Z}$ such that $t^2 z_\nu + u + k$ is in the unit circle, and has real part in $[-1/2, 1/2]$. By (2), it is above the mess, so that

$$\overline{t^2 z_\nu + u} = \frac{1}{t^2 z_\nu + u + k}.$$

We then have

$$\begin{aligned} Im(\overline{t^2 z_\nu + u}) &\leq \left| \frac{1}{t^2 z_\nu + u + k} \right| \\ &\leq \frac{1}{Im(t^2 z_\nu + u + k)} \\ &= \frac{1}{t^2 Im(z_\nu)} \\ &\leq \frac{1}{(\sqrt{3}/2) Im(z_\nu)}, \end{aligned}$$

which by (1) is $< c_1$. Thus in this case, $c_1 \leq Im(\overline{t^2 z_\nu + u}) < c_2$ and $c_1 \leq t^2 Im(z_\nu) < c_2$ are both false.

□

By the above lemma, we may assume that in our integral for the main term of $N(S_\delta^{(i)}; X)$, we have

$$Vol(S_\delta \cap B_i(u, t, \lambda, X)) = \lambda^4 Vol(B \cap \{\nu \in V_{\mathbb{R}}^{(i)} : |Disc(\nu)| < X/\lambda^4 \text{ and}$$

$$c_1(\lambda^4 |Disc(\nu)|)^{1/2-2\delta} \leq t^2 Im(z_\nu) < c_2(\lambda^4 |Disc(\nu)|)^{1/2-2\delta}\})$$

Thus, the main term of $N(S_\delta^{(i)};X)$ is

$$\begin{aligned}
MT &= \frac{1}{M_i}\int_{g\in N'(t)A'\Lambda}\lambda^4\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\left(\chi_{|Disc(\nu)|<X/\lambda^4}\right)\left(\chi_{c_1\frac{(\lambda^4|Disc(\nu)|)^{1/2-2\delta}}{Im(z_\nu)}\le t^2<c_2\frac{(\lambda^4|Disc(\nu)|)^{1/2-2\delta}}{Im(z_\nu)}}\right)d\nu dg\\
&= \frac{1}{M_i}\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\int_{0<\lambda<X^{1/4}/|Disc(\nu)|^{1/4}}\lambda^4\int_{c_1\frac{(\lambda^4|Disc(\nu)|)^{1/2-2\delta}}{Im(z_\nu)}\le t^2<c_2\frac{(\lambda^4|Disc(\nu)|)^{1/2-2\delta}}{Im(z_\nu)}}t^{-2}d^\times t d^\times\lambda d\nu\\
&= \frac{1}{2M_i}\left(\frac{1}{c_1}-\frac{1}{c_2}\right)\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\int_{0<\lambda<X^{1/4}/|Disc(\nu)|^{1/4}}\lambda^4\frac{Im(z_\nu)}{(\lambda^4|Disc(\nu)|)^{1/2-2\delta}}d^\times\lambda d\nu\\
&= \frac{1}{2M_i}\left(\frac{1}{c_1}-\frac{1}{c_2}\right)\left(\frac{1}{2+8\delta}\right)X^{1/2+2\delta}\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\frac{Im(z_\nu)}{|Disc(\nu)|}d\nu
\end{aligned}$$

We now compute the error term that comes from plugging the error term from (3.4) in (3.3),

$$\begin{aligned}
ET &\ll \left(\int_{1\ll\lambda\ll X^{1/4}}\int_{t\asymp\lambda^{1-4\delta}}\int_{N"(t)}(t^3\lambda^3+1)t^{-2}dud^\times t d^\times\lambda\right)+X^{3/4+\epsilon}\\
&\ll X^{1-\delta}+X^{3/4+\epsilon}.
\end{aligned}$$

We are pretty much done here. The last thing we would like to do it to express $\frac{1}{M_i}\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\frac{Im(z_\nu)}{|Disc(\nu)|}d\nu$ in a nicer way, which should not depend on B, as in the statement of Theorem 3.0.3/Theorem 3.1.1.Since B is SO_2-invariant, we can write

$$\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\frac{Im(z_\nu)}{|Disc(\nu)|}d\nu=\int_{\nu\in SO_2(\mathbb{R})\backslash B\cap V_{\mathbb{R}}^{(i)}}\frac{1}{|Disc(\nu)|}\int_{k\in SO_2(\mathbb{R})}Im(k\cdot z_\nu)dkd\nu$$

Lemma 3.1.4. *For any z in the complex upper half plane, we have*

$$\int_{k\in SO_2(\mathbb{R})}Im(k\cdot z)dk=1$$

This lemma implies that (remember dk is normalized so that $SO_2(\mathbb{R})$ has volume 1)

$$\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\frac{Im(z_\nu)}{|Disc(\nu)|}d\nu=\int_{\nu\in SO_2(\mathbb{R})\backslash B\cap V_{\mathbb{R}}^{(i)}}\frac{1}{|Disc(\nu)|}d\nu=\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\frac{1}{|Disc(\nu)|}d\nu=\frac{2\pi}{n_i}M_i,$$

which proves Theorem 3.0.3/Theorem 3.1.1.

Proof. (of Lemma 3.1.4) Let $k=k_\alpha=\begin{bmatrix}\cos(\alpha)&-\sin(\alpha)\\ \sin(\alpha)&\cos(\alpha)\end{bmatrix}$ be the rotation matrix with angle α. Recall the action of $GL_2(\mathbb{R})$ on the upper half plane $\mathbb{H}$, which is our fundamental domain for $GL_2(\mathbb{R})/GO_2(\mathbb{R})$, is given by the Möbius transformation

$$\begin{bmatrix}a&b\\ c&d\end{bmatrix}\cdot z=\frac{c+dz}{a+bz}.$$

We saw in Section 2.1 that the SO_2 orbits of $z=it$ is a circle centered at $i\left(\frac{t^2+1}{2t}\right)$ and radius $\frac{t^2-1}{2t}$, which, as t varies from 1 to ∞, covers the whole upper half plane. So we may pick a representative for

the orbit to be of the form $z = it$, some $t > 1$. Then

$$Im(k_\alpha \cdot (it)) = \frac{t}{\cos^2(\alpha) + t^2 \sin^2(\alpha)}.$$

Thus we can compute

$$\begin{aligned}
\int_{k \in SO_2(\mathbb{R})} Im(k \cdot z) dk &= \frac{1}{2\pi} \int_0^{2\pi} \frac{t}{\cos^2(\alpha) + t^2 \sin^2(\alpha)} d\alpha \\
&= \frac{1}{\pi} \int_{-\pi/2}^{\pi/2} \frac{1}{1 + (t \tan(\alpha))^2} \left(\frac{t d\alpha}{\cos^2(\alpha)} \right) \\
&= \frac{1}{\pi} \int_{-\infty}^{\infty} \frac{du}{1 + u^2} \\
&= \frac{1}{\pi} \tan^{-1}(u)|_{-\infty}^{\infty} \\
&= 1
\end{aligned}$$

□

3.2 An estimate for the number of maximal cubic orders with a given form of Minkowski basis

Let $\mathcal{U}$ denote the subset of elements of $V_\mathbb{Z}$ corresponding to a cubic ring that is maximal. We are now interested in $N(S_\delta \cap \mathcal{U} \cap V_\mathbb{Z}^{(i)}; X)$ that is the number of maximal orders in cubic fields with discriminant positive if $i = 1$ or negative if $i = 2$ and less than X in absolute value, with Minkowski type $\delta, 1/2 - \delta$.

As in [8], for a set S in $V_\mathbb{Z}$ definable by finitely many congruence conditions, let $\mu_p(S)$ be the p-adic density of the p-adic closure of S in $V_{\mathbb{Z}_p}$, where we normalize the additive measure of μ on $V_{\mathbb{Z}_p} = \mathbb{Z}_p^4$ so that $\mu(V_{\mathbb{Z}_p}) = 1$ (ie we have taken the product of the usual additive measures on $\mathbb{Z}_p$). And let $\mu(S) = \prod_p \mu_p(S)$.

Again by [8], we know that

$$\mu(\mathcal{U}_p) = \mu_p(\mathcal{U}_p) = \mu_p(\mathcal{U}) = \frac{(p^3 - 1)(p^2 - 1)}{p^5}$$

and thus

$$\mu(\mathcal{U}) = \prod_p \frac{(p^3 - 1)(p^2 - 1)}{p^5}.$$

Let us now recall the theorem that we will prove in this section:

Theorem 3.2.1. *For $\delta \in (1/5, 1/4] \cap \mathbb{Q}$*

$$N(S_\delta \cap \mathcal{U} \cap V_\mathbb{Z}^{(i)}; X) = \left(\prod_p \frac{(p^3 - 1)(p^2 - 1)}{p^5} \right) \left(\frac{\pi}{n_i} \right) \left(\frac{1}{c_1} - \frac{1}{c_2} \right) \left(\frac{1}{2 + 8\delta} \right) X^{1/2 + 2\delta} + O_\epsilon(X^{1 - \delta/2 + \epsilon}).$$

Proof of Theorem 3.2.1

If we follow the same line as in the previous section with $S = S_\delta \cap \mathcal{U} \cap V_Z^{(i)}$, we see the tricky part is

to try to estimate $\#\{(a,b,c,d) \in S_\delta \cap \mathcal{U} \cap B_i(u,t,\lambda,X) \cap V_\mathbb{Z} : a \neq 0\}$. By[8], we know that $\mathcal{U}$ is defined by infinitely many congruences modulo prime powers, which is not something we can estimate directly. But, in the same way as in Theorem 26 in [8], we could have estimated this if $\mathcal{U}$ was defined by only finietely many congruences modulo primes powers.

We will then deal with maximality at small primes and at big primes seperately. For a prime p, let $\mathcal{U}_p$ denote the subset of elements of $V_\mathbb{Z}$ that corresponds to cubic rings that are maximal at p, so that $\mathcal{U} = \cap_p \mathcal{U}_p$. On one hand, we can deal with maximality at small primes since we would then have finitely many congruences modulo prime power and therefore, along the same lines as Theorem 26 in [8], we can estimate the number of integral points that are maximal at these small primes in a ball, and on the other hand, to deal with big primes, we will use Proposition 29 in [8] that gives a uniform bound for $N(S_\delta \cap \overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) \ll X/p^2$, which gets small for large p. We can then put our results together.

Along the same lines as the proof of Theorems 3.0.3 (previous section), we fix C big enough so that $Vol(B) \neq 0$, and apply (3.1) with $S = S_\delta \cap \mathcal{U}$, to get

$$N(S_\delta \cap \mathcal{U} \cap V_\mathbb{Z}^{(i)}; X) = \frac{1}{M_i} \int_{g=u} \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}_{\lambda \in N'(t)A'\Lambda} \#\{x \in S_\delta \cap \mathcal{U} \cap B_i(u,t,\lambda,X) \cap V_\mathbb{Z}^{irr}\} t^{-2} du d^\times t d^\times \lambda dk, \tag{3.5}$$

where

$$B_i(u,t,\lambda,X) = u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \cap \{\nu \in V_\mathbb{R}^{(i)} : |Disc(\nu)| < X\}$$

and

$$M_i = \frac{n_i}{2\pi} \int_{\nu \in B \cap V_\mathbb{R}^{(i)}} |Disc(\nu)|^{-1} d\nu.$$

And by Lemma 3.1.2, we can modify (3.5) to

$$N(S_\delta \cap \mathcal{U} \cap V_\mathbb{Z}^{(i)}; X) = \frac{1}{M_i} \int_{g=u} \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix}_{\lambda \in N'(t)A'\Lambda} \#\{x \in S_\delta \cap \mathcal{U} \cap B_i(u,t,\lambda,X) \cap V_\mathbb{Z} : a \neq 0\} t^{-2} du d^\times t d^\times \lambda dk + (X^{3/4+\epsilon}). \tag{3.6}$$

We now need an estimate $\#\{x \in S_\delta \cap \mathcal{U} \cap B_i(u,t,\lambda,X) \cap V_\mathbb{Z} : a \neq 0\}$, for which we need the following Theorem that is mainly a consequence for Proposition 3.0.1. Recall that we know from [8] that the condition for an element of $V_\mathbb{Z}$ the be in $\mathcal{U}_p$ for some p is given by finitely many congruence relations modulo p^2. We will separate small primes and big primes shortly.

Theorem 3.2.2. *Suppose S is a subset of $V_\mathbb{Z}$ defined by finitely many congruence conditions modulo prime powers, and $\mu_p(S)$ denotes the p-adic density of S in $V_\mathbb{Z}$. Let m be the smallest integer such that S is defined by congruences modulo m. The number of lattice points (a,b,c,d) in $S_\delta \cap B_i(u,t,\lambda,X) \cap S$ with $a \neq 0$ is*

$$\prod_p \mu_p(S) Vol(S_\delta \cap B_i(u,t,\lambda,X)) + O\left(\prod_p \mu_p(S) m t^3 \lambda^3\right) + O\left(\prod_p \mu_p(S) m^2 t^4 \lambda^2\right)$$

$$+O\left(\prod_p \mu_p(S) m^3 t^3 \lambda\right) + O\left(\prod_p \mu_p(S) m^4\right),$$

Proof. The proof is very inspired from the proof of Theorem 26 in [8]. S may be viewed as the intersection with $V_{\mathbb{Z}}^{(i)}$ with the (disjoint) union of (say) k translates $L_1, ..., L_k$ of the lattice $m \cdot V_{\mathbb{Z}}$. For each $j = 1, ..., k$, the number of elements in $L_j \cap S_\delta \cap B_i(u, t, \lambda, X)$ is equal to the number of lattice points in some translate of $\frac{S_\delta \cap B_i(u,t,\lambda,X)}{m}$, for which we may apply Proposition 3.0.1 and get that this number is

$$\frac{Vol(S_\delta \cap B_i(u, t, \lambda, X))}{m^4} + O\left(\frac{t^3\lambda^3}{m^3}\right) + O\left(\frac{t^4\lambda^2}{m^2}\right) + O\left(\frac{t^3\lambda}{m}\right) + O(1).$$

Adding the points in these k lattices together, we get that the number of lattice points (a, b, c, d) in $S_\delta \cap B_i(u, t, \lambda, X) \cap S$ is

$$\frac{k}{m^4} Vol(S_\delta \cap B_i(u, t, \lambda, X)) + O\left(\frac{kt^3\lambda^3}{m^3}\right) + O\left(\frac{kt^4\lambda^2}{m^2}\right) + O\left(\frac{kt^3\lambda}{m}\right) + O(k),$$

and since $\frac{k}{m^4} = \prod_p \mu_p(S)$ is the p adic density of S in $V_{\mathbb{Z}}$, the above becomes

$$\prod_p \mu_p(S) Vol(S_\delta \cap B_i(u, t, \lambda, X)) + O\left(\prod_p \mu_p(S) m t^3 \lambda^3\right) + O\left(\prod_p \mu_p(S) m^2 t^4 \lambda^2\right)$$

$$+O\left(\prod_p \mu_p(S) m^3 t^3 \lambda\right) + O\left(\prod_p \mu_p(S) m^4\right),$$

as promised. □

Remark 3.2.3. *We did not use the condition $a \neq 0$ since, just like in the previous section, using it would not improve the error term, so we can just ignore this condition from now on.*

Now the naive way to separate small and big primes would be to consider $S = \cap_{p \leq Y} \mathcal{U}_p$, for some Y, and apply the above theorem. The problem with this idea is that we would have $m = \prod_{p \leq Y} p^2$, which would lead to an exponential (in Y) error term.

Instead, we consider the following sieve

$$\#S_\delta \cap B_i(u, t, \lambda, X) \cap \mathcal{U} = \sum_{n=1}^{\infty} \mu(n) \#S_\delta \cap B_i(u, t, \lambda, X) \cap \cap_{p|n} \overline{\mathcal{U}_p}$$

and separate small and big primes by considering $n \leq Y$ and $n > Y$ for some big number Y to be determined later. We then apply Theorem 3.2.2 to each $S_\delta \cap B_i(u, t, \lambda, X) \cap \cap_{p|n} \overline{\mathcal{U}_p}$, that is $S = \cap_{p|n} \overline{\mathcal{U}_p}$ and $m = n^2$. Now this is a lot better that the naive way nice now $m \leq Y^2$. Let us record this in the following Corollary:

Corollary 3.2.4. *For any integer n, the number of lattice points (a, b, c, d) in $S_\delta \cap B_i(u, t, \lambda, X) \cap \cap_{p|n} \overline{\mathcal{U}_p}$ with $a \neq 0$ is*

$$\prod_{p|n} \mu_p(\overline{\mathcal{U}_p}) Vol(S_\delta \cap B_i(u, t, \lambda, X)) + O(n^\epsilon t^3 \lambda^3) + O(n^{2+\epsilon} t^4 \lambda^2) + O(n^{4+\epsilon} t^3 \lambda) + O(n^{6+\epsilon}).$$

Proof. By [8],

$$\prod_{p|n} \mu_p(\overline{\mathcal{U}_p}) = \prod_{p|n} O\left(\frac{1}{p^2}\right) = O_\epsilon\left(\frac{1}{n^{2-\epsilon}}\right).$$

□

So we use Corollary 3.2.4 to deal with small primes. On the other hand, for big primes, we use the uniform bound given by the following lemma:

Lemma 3.2.5. *For any square free integer n, we have*

$$N(\cap_{p|n}\overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) \ll_\epsilon X/n^{2-\epsilon}.$$

Proof. Lemma 3 in [12] is a quintic analog of this that we adapt to the cubic case. The idea is to count rings that are not maximal by counting their overrings.

For a cubic number field K, if R is a subring of $\mathcal{O}_K$ with index m then $Disc(R) = m^2 Disc(\mathcal{O}_K)$. Now, as in [9], let $f_K(m)$ be the number of such orders and let $f(m) = \max_K f_K(m)$, so that

$$N(\cap_{p|n}\overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) \leq \sum_{m:n|m} f(m) N(V_Z^{(i)}; X/m^2) \tag{3.7}$$

$$\ll \sum_{m:n|m} f(m)\left(\frac{X}{m^2}\right). \tag{3.8}$$

We claim that a few things from [9] imply that $f(m) = \prod_{p^k||m} O_\epsilon(p^{\min\{(1+\epsilon)k-1,k/3\}})$. The above then gives

$$\begin{aligned} N(\cap_{p|n}\overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) &\ll X \sum_{m:n|m} \frac{1}{m} \prod_{p^k||m} O_\epsilon(p^{\min\{(1+\epsilon)k-1,k/3\}}) \\ &\ll_\epsilon X n^\epsilon \sum_{m:n|m} \prod_{p^k||m} \frac{p^{\min\{(1+\epsilon)k-1,k/3\}}}{p^{2k}} \\ &\ll X n^\epsilon \prod_{p|n} \sum_{k=1}^{\infty} \frac{p^{\min\{(1+\epsilon)k-1,k/3\}}}{p^{2k}} \\ &\ll \frac{X}{n^{2-\epsilon}}. \end{aligned}$$

To complete the proof, it remains to check that $f(m) = \prod_{p^k||m} O_\epsilon(p^{\min\{(1+\epsilon)k-1,k/3\}})$. Since f is multiplicative, if is enough to prove the case where m is a prime power, let $m = p^k$. By [9] (Chapter 5), we have $f(m) \ll m^{1/3}$ and as also stated in [9], we have

$$\sum_{m=1}^{\infty} \frac{f_K(m)}{m^s} = \frac{\zeta_K(s)}{\zeta_K(2s)}\zeta(2s)\zeta(3s-1),$$

which bounded independently of K for each $s > 1$. We then have

$$\sum_{k=1}^{\infty} \frac{f_K(p^k)}{p^{sk}} = o\left(\frac{1}{p}\right)$$

for each $s > 1$. By Taking $s = 1 + \epsilon$,

$$f_K(p^k) \ll_\epsilon p^{(1+\epsilon)k-1},$$

as needed. □

Summing over all $n > Y$, we get

$$\sum_{n>Y} \mu(n) \# B_i(u,t,\lambda,X) \cap \cap_{p|n} \overline{\mathcal{U}_p} \ll_\epsilon \frac{\lambda^4}{Y^{1-\epsilon}}. \tag{3.9}$$

Let's put all of this together in the following Corollary:

Corollary 3.2.6. *The number of lattice points in $S_\delta \cap B_i(u,t,\lambda,X) \cap \mathcal{U}$ (with $a \neq 0$ if we want) is*

$$A_Y Vol(S_\delta \cap B_i(u,t,\lambda,X)) + O_\epsilon(Y^{1+\epsilon} t^3 \lambda^3) + O_\epsilon(Y^{3+\epsilon} t^4 \lambda^2) + O_\epsilon(Y^{5+\epsilon} t^3 \lambda) + O_\epsilon(Y^{7+\epsilon}) + O_\epsilon\left(\frac{\lambda^4}{Y^{1-\epsilon}}\right),$$

where $A_Y = \left(\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}_p})\right)$. Note $A_Y > 0$ for all Y, and $\lim_{Y\to\infty} A_Y = \mu(\mathcal{U}) > 0$.

Now following the same computation as in Section 3.1, we can compute the main term of $N(S_\delta \cap \mathcal{U} \cap V_Z^{(i)}; X)$ to be

$$MT = A_Y \left(\frac{\pi}{n_i}\right)\left(\frac{1}{c_1} - \frac{1}{c_2}\right)\left(\frac{1}{2+8\delta}\right) X^{1/2+2\delta},$$

and we can evaluate the error term to be

$$ET = O_\epsilon(Y^{1+\epsilon}X^{1-\delta}) + O_\epsilon(Y^{3+\epsilon}X^{1-2\delta}) + O_\epsilon(Y^{5+\epsilon}X^{1/2-\delta}) + O_\epsilon(Y^{7+\epsilon}X^{2\delta-1/2}) + O_\epsilon\left(\frac{X}{Y^{1-\epsilon}}\right) + O(X^{3/4+\epsilon}).$$

The optimal choice is $Y = X^{\delta/2}$, which equates $YX^{1-\delta}$ and $\frac{X}{Y^{1-\epsilon}}$, and the error terms becomes

$$ET = O_\epsilon(X^{1-\delta/2+\epsilon}),$$

and therefore

$$N(S_\delta \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = A_{X^{\delta/4}} \left(\frac{\pi}{n_i}\right)\left(\frac{1}{c_1} - \frac{1}{c_2}\right)\left(\frac{1}{2+8\delta}\right) X^{1/2+2\delta} + O_\epsilon(X^{1-\delta/2+\epsilon}).$$

The the above error term is strictly smaller than the main term if and only if $\delta > 1/5$.

Finally, we can, up to a negligible error, replace $A_{X^{\delta/3}}$ by $\lim_{Y\to\infty} A_Y$, which (by [8] for example) is

$$\lim_{Y\to\infty} A_Y = \prod_p \mu(\mathcal{U}_p) = \mu(\mathcal{U}) = \prod_p \frac{(p^3-1)(p^2-1)}{p^5}.$$

To see the error is negligible,

$$\begin{aligned}
|\mu(\mathcal{U}) - A_Y| &= \sum_{n>Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}_p}) \\
&\leq \sum_{n>Y} \prod_{p|n} \left(1 - \frac{(p^3-1)(p^2-1)}{p^5}\right) \\
&= \sum_{n>Y} \prod_{p|n} \frac{p^3+p^2-1}{p^5} \\
&\ll \sum_{n>Y} \prod_{p|n} \frac{1}{p^2} \\
&= \sum_{n>Y} \frac{1}{n^2} \\
&\ll \frac{1}{Y}.
\end{aligned}$$

Thus the error term that is due to replacing $A_{X^{\delta/4}}$ by $\mu(\mathcal{U})$ is

$$O\left(\frac{X^{1/2+2\delta}}{X^{\delta/4}}\right),$$

which is strictly smaller than the error term $O_\epsilon(X^{1-\delta/2+\epsilon})$ that we already had since $\delta \leq 1/4$.

Chapter 4

The quartic case using Bhargava's correspondence

In this chapter, we start by giving a background on Bhargava's correspondence between quartic rings and some homogeneous space that, just like the Delone-Faddeev correspondence, nicely carries information about Minkowski basis. It will not be as detailed as Section 2.1 as most important properties will be very similar to the cubic case. We will state properties that will be used in the rest of this chapter and the next, with a particular attention to things that differ from the cubic case.

A few things in the chapter and the next will be very similar to the cubic case. We will skip the steps that are similar and invite the reader to refer to the cubic case.

Besides increasing the dimension, there is a significant difference between the cubic and quartic case that is due to the fact that 4 is not a prime, and thus a quadratic field might have a quadratic subfield, which is the case of about 9.356 % of all quartic fields. Indeed the bounds given by Theorem 0.0.8 only hold for orders in a number field that does not have any subfield.

Let K be a quartic field and R be an order in K with discriminant D. Let $v_1 = 1, v_2, v_3, v_4$ be a Minkowski basis for R. We have that $1 \leq |v_2| \leq |v_3| \leq |v_4|$ and $|v_2||v_3||v_4| \asymp |D|^{1/2}$. By [7], we know that

$$|v_4| \ll |D|^{1/4}. \tag{4.1}$$

We will see that that every asymptotic size respecting this bound is attained for a family of orders in a quartic field but again this can only happen for orders in fields that have a quadratic subfield. (otherwise we would have extra bounds given by Theorem 0.0.8).

In fact we will find that we need something stronger that is

$$|v_3|^3|v_4|^2 \ll |D|. \tag{4.2}$$

Let us now state the results that we will prove in the chapter as the two following theorems:

Theorem 4.0.1. *Let R be an order in a quartic number field K, with Minkowski basis $v_1 = 1, v_2, v_3, v_4$, then*

$$|v_4| \ll |D|^{1/4}$$

or if $|v_i| \asymp |D|^{\delta_i}$*, then*

$$\begin{cases} 1/6 \leq \delta_4 \leq 1/4 \\ 1/4 - \delta_4/2 \leq \delta_3 \leq \delta_4 \\ \delta_2 = 1/2 - \delta_3 - \delta_4 \end{cases} \tag{4.3}$$

and if K *does not have a quadratic subfield, then we also have*

$$|v_3|^3 |v_4|^2 \ll |D|$$

or equivalently

$$3\delta_3 + 2\delta_4 \leq 1 \tag{4.4}$$

Theorem 4.0.2. *For any quartic number field* K *that has a quadratic subfield, and any* $\delta_2, \delta_3, \delta_4$ *satisfying (4.3) there is a family of orders in* K *with Minkowski type* $\delta_2, \delta_3, \delta_4$*.*

And for any quartic number field K*, and any* $\delta_2, \delta_3, \delta_4$ *satisfying both (4.3) and (4.4), there is a family of orders in* K *with Minkowski type* $\delta_2, \delta_3, \delta_4$*.*

4.1 Background on Bhargava's correspondence between quartic rings and pairs of ternary quadratic forms

This secton is pretty much extracting what we will need from [2] and [3].

Let $V_{\mathbb{R}}$ (resp. $V_{\mathbb{Q}}$, resp. $V_{\mathbb{Z}}$) be the set of real (resp. rational, resp. integral) pairs of ternary quadratic forms.

For a pair of ternary quadratic form ν in any of these sets, we may write $\nu = (A, B)$, where $A = (a_{ij})_{1 \leq i,j \leq 3}$ and $B = (b_{ij})_{1 \leq i,j \leq 3}$ are 3×3 symmetric matrices, so that for a 3 dimensional column vector x,

$$(A, B)(x) = \nu(x) = (x^T A x, x^T B x).$$

We define the action of $G(\mathbb{R}) := GL_2(\mathbb{R}) \times SL_3(\mathbb{R})$ on $V_{\mathbb{R}}$ in the following way: For $\gamma_2 \in GL_2(\mathbb{R})$, let

$$\gamma_2 \cdot (A, B) = \gamma_2(A, B), \text{ (linear combinations of } A \text{ and } B) \ ,$$

and for $\gamma_3 \in SL_3(\mathbb{R})$, let

$$\gamma_3 \cdot \nu(x_1, x_2, x_3) = \nu((x_1, x_2, x_3)\gamma_3),$$

or equivalently,

$$\gamma_3 \cdot (A, B) = (\gamma_3 A \gamma_3^T, \gamma_3 B \gamma_3^T).$$

We define the discriminant of a pair (A, B) to be the fundamental invariant under the above action, namely

$$Disc(A, B) = Disc(4 \cdot det(Ax + By)).$$

Definition 4.1.1. *We say a pair* (A, B) *is* **degenerate** *if its discriminant* $Disc(A, B) = 0$*. Or equivalently* (A, B) *is degenerate if the binary cubic form* $det(Ax + By)$ *is. Otherwise we say it is* **non degenerate**.

Remark 4.1.2. *degenerate/ non degenerate is invariant under the action of* $G(\mathbb{R})$

It will be useful to know how each elements of the NAK decomposition of $GL_2(\mathbb{R})$ and of $SL_3(\mathbb{R})$ act on a pair $(A, B) \in V_{\mathbb{R}}$. Let's start with $GL_2(\mathbb{R})$:

$$\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot (A, B) = (t^{-1}A, tB)$$

$$\begin{bmatrix} 1 & \\ u & 1 \end{bmatrix} \cdot (A, B) = (A, uA + B)$$

$$\lambda \cdot (A, B) = \begin{bmatrix} \lambda & \\ & \lambda \end{bmatrix} \cdot (A, B) = (\lambda A, \lambda B).$$

Note the slight abuse of notation that we will often use. When we write $\lambda \cdot (A, B)$ as a scalar acting on the pair, we will always mean $\lambda I_{2\times 2}$ as above. We can also compute that

$$Disc(\lambda \cdot (A, B)) = Disc(4 \cdot Det(\lambda(Ax - By))) = Disc(4\lambda^3 \cdot Det((Ax - By)) = \lambda^{12} Disc(A, B).$$

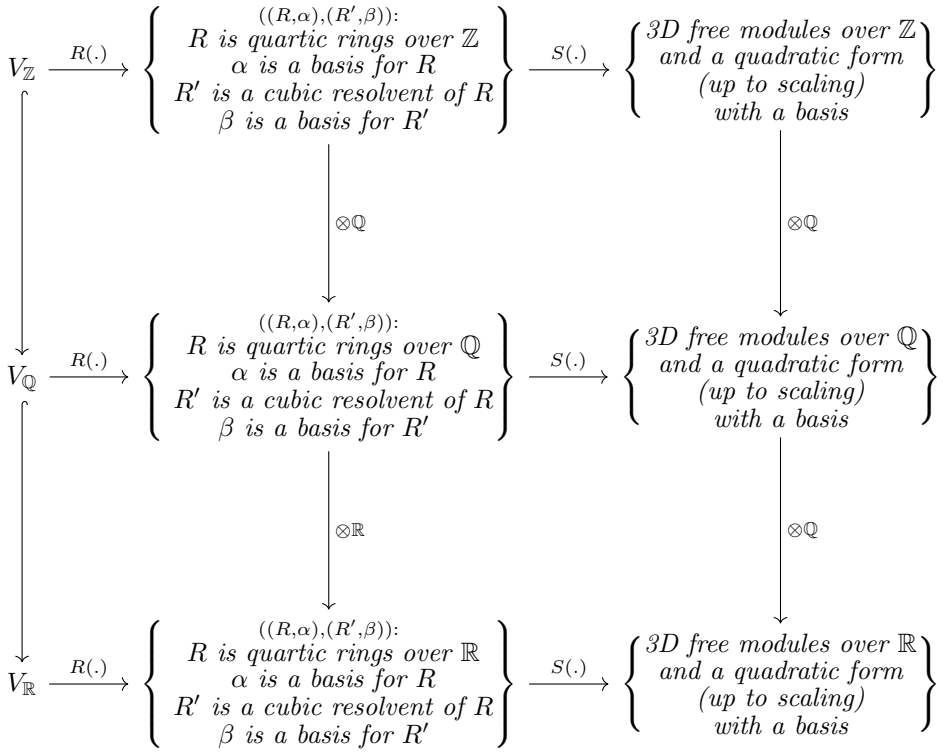
Now $SL_3(\mathbb{R})$ acts on a pair (A, B) by acting a both A and B separately in the same way. Thus we might only record how elements of $SL_3(\mathbb{R})$ act on one of them, for example A. The resulting matrices will always be symmetric, so to make it easier to read we will only write the values in the upper right triangle of the matrices.

$$\begin{bmatrix} (t_1t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix} \cdot (a_{ij}) = \begin{bmatrix} (t_1t_2)^{-2}a_{11} & t_2^{-1}a_{12} & t_1^{-1}a_{13} \\ \cdot & t_1^2 a_{22} & t_1t_2a_{23} \\ \cdot & \cdot & t_2^2 a_{33} \end{bmatrix}$$

$$\begin{bmatrix} 1 & & \\ u_1 & 1 & \\ u_2 & u_3 & 1 \end{bmatrix} \cdot (a_{ij}) = \begin{bmatrix} a_{11} & a_{12} + u_1a_{11} & a_{13} + u_2a_{12} + u_2a_{11} \\ \cdot & a_{22} + 2u_1a_{12} + u_1^2a_{11} & a_{23} + u_3a_{22} + u_1a_{13} + u_1u_3a_{12} + u_3a_{12} + u_1u_2a_{11} \\ \cdot & \cdot & a_{33} + 2u_3a_{23} + u_3^2a_{22} + 2u_2a_{13} + 2u_2u_3a_{12} + u_2^2a_{11} \end{bmatrix}.$$

We have the following theorem of Bhargava that is a quartic analogues of the Delone-Faddeev correspondence:

Theorem 4.1.3. *There are maps $R(\cdot)$ and $S(\cdot)$ that make the following diagram commute:*



The discriminant of an element of $V_{\mathbb{Z}}$ is equal to the discriminant of the corresponding quartic ring.

Note that, elements in the middle column are not only quartic rings with a basis (as we only have cubic rings in the cubic case) but pairs of quartic rings with a basis together with one of its cubic resolvent and a basis for it.

Let us state this consequence of Theorem 4.1.3 that we will really be using:

Theorem 4.1.4. *There is a map*

$$\{\textit{non degenerate elements of } V_{\mathbb{R}}\} \to \left\{\begin{matrix}\textit{3D vector spaces over } \mathbb{R} \textit{ with a basis} \\ \textit{and a quadratic form (up to scaling)}\end{matrix}\right\} \simeq GL_3(\mathbb{R})/GO_3(\mathbb{R})$$

$$\nu = (A,B) \to \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix},$$

where the z_i's are 1×3 row vectors, whose restriction to $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Q}}$) gives bases for shapes of quartic rings over $\mathbb{Z}$ (resp. $\mathbb{Q}$)

Analogously to the cubic case, we are interested in Minkowski basis of quartic rings, so we may just look at the shapes of these rings (that is elements in the right colomn of the diagram in Theorem 4.1.3). We will denote the square root of the quadratic form on the shape by $|.|$ and call it "length", remembering that it in only defined up to scaling. The scaling should not cause any confusion as we will keep track of ratios of lengths of basis elements, like in the following theorem. The reader may go back to the cubic case (Section 2.1) for more details on this discussion.

Theorem 4.1.5. *For any $\nu \in V_{\mathbb{Z}}$, that maps to the quartic ring $R(\nu)$ with a basis $1, v_2, v_3, v_4$ and to the 3 dimensional lattice $S(\nu)$ with a basis w_2, w_3, w_4. Then*

1) $\frac{|v_3|}{|v_2|} \asymp \frac{|w_3|}{|w_2|}$ *and* $\frac{|v_4|}{|v_2|} \asymp \frac{|w_4|}{|w_2|}$
2) $1, v_2, v_3, v_4$ *is a Minkowski basis for* $R(\nu)$ *if and only if* w_2, w_3, w_4 *is a Minkowski basis for* $S(\nu)$.

By Theorem 4.1.4, we may think of shapes of quartic rings with a given basis as an element of $GL_3(\mathbb{R})/GO_3(\mathbb{R})$, where the rows of the matrix represent the basis elements. Let's see how the left action of $G(\mathbb{R})$ on $GL_3(\mathbb{R})/GO_3(\mathbb{R})$, which contains the shapes is induced by the map in Theorem 4.1.4 and the action of $G(\mathbb{R})$ on $V_{\mathbb{R}}$. The left action of $GL_2(\mathbb{R})$ on $GL_3(\mathbb{R})/GO_3(\mathbb{R})$ given by:

$$\gamma_2 \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix} = det(\gamma_3) \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix},$$

that is the elements of $SL_2(\mathbb{R})$ act trivially, and

$$\lambda \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix} = \lambda^2 \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix}.$$

Now the left action of $SL_3(\mathbb{R})$ on $GL_3(\mathbb{R})/GO_3(\mathbb{R})$ is given by matrix multiplication:

$$\gamma_3 \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix} = \gamma_3 \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix}.$$

In particular

$$\begin{bmatrix} (t_1t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix} \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} (t_1t_2)^{-1}z_1 \\ t_1z_2 \\ t_2z_3 \end{bmatrix}$$

$$\begin{bmatrix} 1 & & \\ u_1 & 1 & \\ u_1 & u_3 & 1 \end{bmatrix} \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix} = \begin{bmatrix} z_2 \\ u_1z_2 + z_3 \\ u_2z_2 + u_3z_3 + z_4 \end{bmatrix}.$$

Let us describe a convenient fundamental domain for $GL_3(\mathbb{R})/GO_3(\mathbb{R})$: Let

$$\mathbb{H} = \left\{ \begin{bmatrix} 1, 0, 0 \\ z \\ w \end{bmatrix} : z \cdot (0,0,1) = 0, z \cdot (0,1,0) > 0, w \cdot (0,0,1) > 0 \right\}.$$

We might then (conveniently) look at the $G(\mathbb{R})$ equivariant map:

$$\{ \text{ non degenerate elements of } V_{\mathbb{Z}} \} \to \mathbb{H}$$
$$\nu = (A, B) \to \begin{bmatrix} 1, 0, 0 \\ z_\nu \\ w_\nu \end{bmatrix}$$

The general description the left action of $G(\mathbb{R})$ on $\mathbb{H}$ is not as compact as the cubic case (that was

just a Möbius transformation). First note that $GL_2(\mathbb{R})$ acts trivially on $\mathbb{H}$. We let's see how some elements of the NAK decomposition of $GL_2(\mathbb{R})$ act on $\mathbb{H}$:

$$\begin{bmatrix} 1 & & \\ u_1 & 1 & \\ u_2 & u_3 & 1 \end{bmatrix} \cdot \begin{bmatrix} 1,0,0 \\ z \\ w \end{bmatrix} = \begin{bmatrix} (1,0,0) \\ z + u_1(1,0,0) \\ w + u_2(1,0,0) + u_3 z \end{bmatrix}$$

$$\begin{bmatrix} (t_2t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix} \cdot \begin{bmatrix} 1,0,0 \\ z \\ w \end{bmatrix} = \begin{bmatrix} 1,0,0 \\ t_1^2 t_2 z \\ t_1 t_2^2 w \end{bmatrix}.$$

4.1.1 Taking $G(\mathbb{Z})$ orbits

So far we have a $G(\mathbb{R})$ equivariant map $V_{\mathbb{R}} \to GL_3(\mathbb{R})/GO_3(\mathbb{R})$. It induces a map on the $G(\mathbb{Z})$ orbits:

$$G(\mathbb{Z})\backslash V_{\mathbb{R}} \to G(\mathbb{Z})\backslash GL_3(\mathbb{R})/GO_3(\mathbb{R}) = GL_3(\mathbb{Z})\backslash GL_3(\mathbb{R})/GO_3(\mathbb{R})$$

Note this map DOES NOT induce a well defined action of $G(\mathbb{R})$ as the left action of $G(\mathbb{R})$ on $\mathbb{H}$ does not commute with the reduction modulo the left action of $G(\mathbb{Z})$.

Let $\mathcal{F} = \left\{ \begin{bmatrix} 1,0,0 \\ z \\ w \end{bmatrix} \in \mathbb{H} : \text{ the rows form a Minkowski basis for the lattice that it generates} \right\}$

Then $\mathcal{F}$ in a fundamental domain for $G(\mathbb{Z})\backslash GL_3(\mathbb{R})/GO_3(\mathbb{R})$. For $\begin{bmatrix} 1,0,0 \\ z \\ w \end{bmatrix} \in \mathbb{H}$, define $\begin{bmatrix} 1,0,0 \\ \overline{z} \\ \overline{w} \end{bmatrix}$ to be its image in $\mathcal{F}$.

To send $\begin{bmatrix} z_2 \\ z_3 \\ z_4 \end{bmatrix} \in GL_3(\mathbb{R})$ to $\mathcal{F}$, we first (left) apply the element of $GL_2(\mathbb{Z})$ needed to get a matrix whose rows form a Minkowski basis for the lattice that it generates. We can then send it to $\mathbb{H}$ by (right) applying an element of $GO_3(\mathbb{R})$.

Analogously to the cubic case, the action of $G(\mathbb{Z})$ (resp. $G(\mathbb{Q})$, resp. $G(\mathbb{Q})$) on $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Q}}$, resp. $V_{\mathbb{R}}$) corresponds to the change of basis of the quartic rings and of their cubic resolvent, which gives the following theorem:

Theorem 4.1.6. *Taking $G(\mathbb{Z})$ orbits in the first two columns of the diagram in Theorem 2.1.1 yields the following bijections:*

$$G(\mathbb{Z})\backslash V_{\mathbb{Z}} \leftrightarrow \{(R, R') : \text{ } R \text{ is a quartic ring over } \mathbb{Z} \text{ and } R' \text{ is a cubic resolvent of } R\}/\sim$$

$$G(\mathbb{Q})\backslash V_{\mathbb{Q}} \leftrightarrow \{(R, R') : R \text{ is a quartic ring over } \mathbb{Q} \text{ and } R' \text{ is a cubic resolvent of } R\}/\sim$$

$$G(\mathbb{R})\backslash V_{\mathbb{R}} \leftrightarrow \{(R, R') : R \text{ is a quartic ring over } \mathbb{R} \text{ and } R' \text{ is a cubic resolvent of } R\}/\sim$$

Remark 4.1.7. *Quartic rings over $\mathbb{Z}$ do not in general have a unique cubic resolvent but some do and are called primitive quartic rings. In particular, maximal quartic rings have a unique cubic resolvent. See [2] for me detail.*

Remark 4.1.8. *We will define irreducibility very soon and see that "irreducible" quartic rings over $\mathbb{Q}$ are quartic number fields. They each have a unique cubic resolvent.*

Remark 4.1.9. *Up to isomorphism, there are exactly 3 quartic rings over $\mathbb{R}$ namely $\mathbb{R}^4, \mathbb{C}\times\mathbb{R}^2, \mathbb{C}^2$ and then each have a unique cubic resolvent namely $\mathbb{R}^3$ if its discriminant is positive or $\mathbb{R}\times\mathbb{C}$ otherwise.*

We will also need a fundamental domain for $G(\mathbb{Z})\backslash G(\mathbb{R}) = GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R}) \times SL_3(\mathbb{Z})\backslash SL_3(\mathbb{R})$.

Let $\mathcal{F}_2$ be the fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})$ described in Chapter 2.1.

Similarly, let $\mathcal{F}_3$ be the fundamental domain for $SL_3(\mathbb{Z})\backslash SL_3(\mathbb{R})$ consisting in elements of $SL_3(\mathbb{R})$ whose image in $\mathbb{H}$ is in $\mathcal{F}$. We can also conveniently describe $\mathcal{F}_3$ using the NAK decomposition by

$$\mathcal{F}_3 = N'(t_1,t_2)A'K'\Lambda,$$

where

$$N'(t_1,t_2) = \left\{ \begin{bmatrix} 1 & & \\ u_1 & 1 & \\ u_2 & u_3 & 1 \end{bmatrix} : u_i \in I_i(t_1,t_2) \right\}, A' = \left\{ \begin{bmatrix} (t_1t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix} : 0 < (t_1t_2)^{-1} \leq \frac{1}{\sqrt{3}}t_1 \leq \frac{4}{3}t_2 \right\}, K' = SO_3(\mathbb{R}),$$

where $I_i(t_1,t_2)$ are subintervals of $[-1/2,1/2]$ depending on t_1 and t_2. In particular, if t_2/t_1 and $t_1/(t_1t_2)^{-1}$ are big enough, then $I(t_1,t_2) = [-1/2,1/2]$.

And finally, we let $\mathcal{F}_G = \mathcal{F}_2 \times \mathcal{F}_3$ be our fundamental domain for $G(\mathbb{Z})\backslash G(\mathbb{R})$.

4.1.2 Irreducible / Absolutely irreducible

In the quartic case (unlike in the cubic case), we have 2 different notion of irreducibility that needs to be clarified. It comes from the fact that quartic fields sometimes have quadratic subfields and we want to consider this case separately.

First recall that a pair (A,B) is **degenerate** if its discriminant $Disc(A,B) = 0$. Or equivalently (A,B) is degenerate if the binary cubic form $det(Ax+By)$ is. Otherwise, it is **non degenerate**.

Definition 4.1.10. *We say a non degenerate integral pair (A,B) is* **irreducible** *if it corresponds to an order in a quartic number field K, or equivalently if it corresponds to an integral domain.*

We say (A,B) is **absolutely irreducible** *if K is either an A_4 or an S_4 number field, or equivalently if K does not have a quadratic subfield.*

The degenerate case will not be interesting to us in this thesis. We will then always consider non degenerate elements of $V_{\mathbb{R}}$ for which we have the following very visual theorem:

Theorem 4.1.11. *If a pair (A,B) is non degenerate then the two ternary quadratic forms have exactly 4 common zeroes in $\mathbb{P}^2$ counting multiplicity.*

The field of definition of these zeroes is the quartic ring over $\mathbb{Q}$ corresponding to the pair (A,B).

Remark 4.1.12. *Irreducibility and absolute irreducibility are invariant under the action of $G(\mathbb{Q})$ but not under the action of $G(\mathbb{R})$.*

The following theorem is criterion for irreducibility that follows easily from the definition and Theorem 4.1.11:

Theorem 4.1.13. *A non degenerate pair (A, B) is irreducible if and only if A and B have a common zero in $\mathbb{P}^2$ having field of definition K, where K is a quartic number field.*

And this one is a more practical criterion for irreducibility:

Theorem 4.1.14. *A (non degenerate) pair (A, B) of integral ternary quadratic forms is irreducible if and only if the following two conditions are satisfied:*

1) there is no nonzero vector $v \in \mathbb{Q}^3$ such that $A(v) = B(v) = 0$

2) there is no 2-dimensional subspace V of $\mathbb{Q}^3$ and a non trivial $\mathbb{Q}-$linear combination $xA + yB$ of A and B such that $(xA + yB)(v) = 0$ for all $v \in V$.

"Similarly", the following two theorems are criterions for absolute irreducibility:

Theorem 4.1.15. *A non degenerate pair (A, B) is absolutely irreducible if and only if A and B have a common zero in $\mathbb{P}^2$ having field of definition K, where K is a quartic number field that is either A_4 or S_4.*

Theorem 4.1.16. *A (non degenerate) pair (A, B) is absolutely irreducible if and only if*

1) there is no nonzero vector $v \in \mathbb{Q}^3$ such that $A(v) = B(v) = 0$

2) the binary cubic form $f(x, y) = det(Ax - By)$ is irreducible over $\mathbb{Q}$.

Remark 4.1.17. *Condition 2 in Theorems 4.1.16 implies condition 2 in Theorem 4.1.14 which implies that the pair is non degenerate.*

This follows easily from the above theorems but is worth mentioning as it gives a condition for absolute irreduciblility given irreducibility:

Corollary 4.1.18. *Let (A, B) be a pair of integral ternary quadratic forms that corresponds to an order in a quartic field. The quartic field has a quadratic subfield if and only if the binary cubic form $det(Ax + By)$ is reducible.*

4.1.3 Characterization for irreducible / absolutely irreducible elements

We now would like a characterization for our two notions of irreducibility in terms of how the matrices representing A and B look like.

In the following sections, we will apply elements of $G(\mathbb{Q})$ to construct new elements of $V_{\mathbb{Z}}$. We will in particular apply element of $\mathcal{F}_G$, our fundamental domain for $G(\mathbb{Z})\backslash G(\mathbb{R})$, whose torus elements are of the form

$$\left(\begin{bmatrix} (t_1 t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix}, \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \right),$$

for some $0 < (t_1 t_2)^{-1} \leq t_1 \leq t_2$ and $t > 1$.

We will thus mostly deal with pairs (A, B) where coefficients of A are asymptotically smaller than coefficients of B and in each matrix, coefficients that are closer to the top left hand corner are asymptotically smaller. In other words, in A for example, if $i + j < i' + j'$, then a_{ij} is asymptotically smaller than $a_{i'j'}$.

We will see in the next sections of this chapter that having a lot of zeroes in the matrices gives allows us to apply a "wider" range of elements of $G(\mathbb{Q})$ while keeping an integral pair. For this reason, we

will be interested in characterizing irreducibility in terms of how many of the asymptotically smaller coefficients can be zero.

So let us see how many zeroes make a pair fail to be irreducible:

Theorem 4.1.19. *Given a pair $(A, B) \in V_{\mathbb{Z}}$, if either*

i) **both** *A and B are of the form*

$$A, B = \begin{bmatrix} 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix},$$

or

ii) A is of the form

$$A = \begin{bmatrix} 0 & 0 & \cdot \\ 0 & 0 & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix},$$

then (A, B) is not irreducible.

Proof. In the first case, we have $A(e_1) = B(e_1) = 0$, and thus condition 1 of Theorem 4.1.14 fails.

In the second case, we have that $A(v) = 0$ for all v in the vector space $V =< (1, 0, 0), (0, 1, 0) >$, and thus condition 2 of Theorem 4.1.14 fails. □

Now let's see how many zeroes make a pair fail to be **absolutely** irreducible:

Theorem 4.1.20. *Given a pair $(A, B) \in V_{\mathbb{Z}}$, if A is of the form*

$$A = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \cdot & \cdot \\ 0 & \cdot & \cdot \end{bmatrix},$$

then (A, B) is not **absolutely** *irreducible.*

Proof. In this case, $det(A) = 0$, which imply that y is a linear factor of the binary cubic form $f(x, y) = det(Ax - By)$, and thus condition 2 of Theorem 4.1.16 fails. □

The next question is: How many zeroes can the matrix A have to be in an irreducible or an absolutely irreducible pair (A, B)? We recall that irreducible elements are orders in any quartic field and absolutely irreducible elements are orders in a quartic field that does not have a quadratic subfield. So given any quartic field K, we cannot always hope for K to contain an order given by a pair (A, B) of a form given in Theorem 4.1.19 or Theorem 4.1.20 as if K has no quadratic subfield then all its orders are absolutely irreducible. The following theorem shows that the "next" smaller amount of zeroes works.

Theorem 4.1.21. *If K is any quartic field, it contains an order which can be given by a pair (A, B), where A is of the form*

$$A = \begin{bmatrix} 0 & 0 & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}.$$

Proof. Let K be a quartic number field. Let α be an integral primitive element of K, and let $P = [1, \alpha, \alpha^2]$ be a point in $\mathbb{P}^2$ whose field of definition is K. We are looking for a non degenerate pair (A, B) of ternary quadratic forms that have P as a common root and we want to construct them so that A is of the form

$$A = \begin{bmatrix} 0 & 0 & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}.$$

Let

$$A = x_2^2 - x_1 x_3 = \begin{bmatrix} 0 & 0 & -1/2 \\ 0 & 1 & 0 \\ -1/2 & 0 & 0 \end{bmatrix}.$$

Then A is of the desired form and P is clearly a root of A.

Let $x^4 + ax^3 + bx^2 + cx + d$ be the minimal polynomial of α, and let

$$B = x_3^2 + ax_2x_3 + bx_2^2 + cx_1x_2 + dx_1^2 = \begin{bmatrix} d & c/2 & 0 \\ c/2 & b & a/2 \\ 0 & a/2 & 1 \end{bmatrix}.$$

Then P is clearly a common root of A and B. It remains to check that (A, B) is non degenerate. We can compute

$$Disc(A, B) = Disc(4det(Ax + By)) = Disc(x^4 + ax^3 + bx^2 + cx + d),$$

which cannot be zero since $x^4 + ax^3 + bx^2 + cx + d$ is the minimal polynomial of α. Thus the pair is indeed non degenerate. □

As this might be interesting, here is another proof of Theorem 4.1.21 using linear algebra:

Proof. Start with a pair (A, B) that gives any order in K. If **both** A and B are of the form

$$A, B = \begin{bmatrix} \cdot & 0 & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix},$$

then we can apply an element of $GL_2(\mathbb{Q})$ to get another pair that gives another order in the same field K, where A has the form

$$A = \begin{bmatrix} 0 & 0 & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}.$$

To prove the theorem, it is then enough to show that to any pair (A, B) that gives any order in K, we can apply an element of $GL_3(\mathbb{Q})$ to get a new pair with both A and B of the form

$$A, B = \begin{bmatrix} \cdot & 0 & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}.$$

Equivalently, it is enough to show that we can apply an element of $GL_3(\mathbb{Q})$ to get a new pair with

$$\begin{bmatrix}0 & 1 & 0\end{bmatrix} A \begin{bmatrix}1\\0\\0\end{bmatrix} = \begin{bmatrix}0 & 1 & 0\end{bmatrix} B \begin{bmatrix}1\\0\\0\end{bmatrix} = 0.$$

Let u be any non zero vector in $\mathbb{Q}^3$, and look at the following two subspaces of $\mathbb{Q}^3$:

$$u^{\perp,A} = \{v \in \mathbb{Q}^3 : u^T A v = 0\}$$
$$u^{\perp,B} = \{v \in \mathbb{Q}^3 : u^T B v = 0\}$$

They both have dimension at least two so $S := u^{\perp,A} \cap u^{\perp,B}$ has dimension at least one. Thus there is a non zero vector in $v \in \mathbb{Q}^3$ such that

$$u^T A v = u^T B v = 0.$$

Now by condition 1 of Theorem 4.1.14, since (A, B) is irreducible, u and v must be linearly independent and thus there exists $\gamma \in GL_3(\mathbb{Q})$ such that $\gamma \begin{bmatrix}0\\1\\0\end{bmatrix} = u$ and $\gamma \begin{bmatrix}1\\0\\0\end{bmatrix} = v$. We then have

$$\begin{bmatrix}0 & 1 & 0\end{bmatrix} (\gamma^T A \gamma) \begin{bmatrix}1\\0\\0\end{bmatrix} = \left(\gamma \begin{bmatrix}0\\1\\0\end{bmatrix}\right)^T A \left(\gamma \begin{bmatrix}1\\0\\0\end{bmatrix}\right) = u^T A v = 0$$

and similarly

$$\begin{bmatrix}0 & 1 & 0\end{bmatrix} (\gamma^T B \gamma) \begin{bmatrix}1\\0\\0\end{bmatrix} = u^T B v = 0.$$

□

If we now consider a quartic field K that does have a quadratic subfield, then its orders are irreducible but not absolutely, and thus A might have more zeroes.

Theorem 4.1.22. *If K is a quartic field* **that has a quadratic subfield**, *then it contains an order that can be given by a pair (A, B), where A is of the form*

$$A = \begin{bmatrix}0 & 0 & 0\\0 & \cdot & \cdot\\0 & \cdot & \cdot\end{bmatrix}.$$

Proof. Let K be a quartic field that has a quadratic subfield K_0. We are looking for a non degenerate pair (A, B) of ternary quadratic forms that have P as a common root and we want to construct them so that A is of the form

$$A = \begin{bmatrix}0 & 0 & 0\\0 & \cdot & \cdot\\0 & \cdot & \cdot\end{bmatrix}.$$

Let α be an integral primitive element of K such that $\alpha^2 \in K_0$. The minimal polynomial of α over $\mathbb{Q}$ is then of the form $x^4 + ax^2 + b$. Let $P = [\alpha, 1, \alpha^2]$ be a point in $\mathbb{P}^2$ whose field of definition is K. Let

$$A = x_3^2 + ax_2x_3 + bx_2^2 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & b & a/2 \\ 0 & a/2 & 1 \end{bmatrix},$$

Then A is of the desired form and P is clearly a root of A.

Now let

$$B = x_1^2 - x_2x_3 = \begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & -1/2 \\ 0 & -1/2 & 0 \end{bmatrix}.$$

Then P is a common root of A and B. It remains to check that the pair (A, B) is non degenerate. We can compute

$$Disc(A, B) = Disc(4 \cdot det(Ax + BY)) = Disc(x^4 + ax^2 + b),$$

which cannot be zero since $x^4 + ax^2 + b$ is the minimal polynomial of α. Thus the pair is indeed non degenerate. □

As it might be interesting, here is another proof of Theorem 4.1.22 using linear algebra:

Proof. Start with any pair (A, B) that gives an order in K with a basis. The first step will be to apply an element of $GL_2(\mathbb{Q})$ to get a new pair corresponding to another order in K with $det(A) = 0$, and the second step will be to apply an element of $GL_3(\mathbb{Q})$ to get another pair with A of the form that we want, or equivalently with

$$A \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}.$$

By Corollary 4.1.18, since K has a quadratic subfield, the binary cubic form $det(Ax + By)$ is reducible. So there exists $\gamma_2 \in GL_2(\mathbb{Q})$ such that $(A', B') = \gamma \cdot (A, B)$ and y divides $det(A'x + B'y)$, or equivalently $det(A') = 0$.

Now since $det(A') = 0$, there exists a vector $v \in \mathbb{Q}^3 \backslash \{0\}$ such that $A'v = 0$. Let $\gamma_3 \in GL_3(\mathbb{Q})$ be such that $\gamma_3 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = v$. Then $\gamma_3^T A' \gamma_3 \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \gamma_3^T A' v = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$.

So if we let $(A'', B'') = \gamma_3 \cdot (A', B')$, then $A'' \begin{bmatrix} 1 \\ 0 \\ 0 \end{bmatrix} = \begin{bmatrix} 0 \\ 0 \\ 0 \end{bmatrix}$, as needed. □

4.2 Existence - Proof of the quartic case of Theorem 0.0.7

In this section, we use Bhargava's correspondence described in Section 4.1 to prove our existence theorem in the quartic case. Analogously to the cubic case, we will fix a quartic number field K, fix $\delta_2, \delta_3, \delta_4$ with the necessary conditions on them, and build a family of orders in K with Minkowski type $\delta_2, \delta_3, \delta_4$. We recall that the conditions on the δ_i' will be weaker if we know that K has a quadratic subfield than

if it doesn't necessarily have one. We will thus consider separately the case where K is known to have a quadratic subfield and the case where K can be any quartic field.

In both cases, the construction will be as follow: Let (A_0, B_0) be a fixed pair of ternary quadratic forms that corresponds to an order in a fixed quartic field K of our choice. Now for a (big) integer n, we let

$$(A_n, B_n) = 2^n \cdot (A_0, B_0) = \begin{bmatrix} 2^n & \\ & 2^n \end{bmatrix} \cdot (A_0, B_0)$$

We get a family of orders all in the same quartic field K that we started with, with discriminants $|D_n| \asymp 2^{12n}$, and with Minkowski type $1/6, 1/6, 1/6$. Also note that the coefficients of A_n and B_n are just the coefficients of A_0 and B_0 multiplied by 2^n, they are then either $\asymp 2^n \asymp |D|^{1/12}$ (if the corresponding coefficient of A_0 or B_0 is nonzero) or 0 (if the corresponding coefficient of A_0 or B_0 is 0).

Like in the cubic case, we now apply to (A_n, B_n) an element of the torus of $G(\mathbb{Q})$, that is an element of the form

$$\gamma = \left(\begin{bmatrix} (t_1 t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix}, \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \right).$$

We get a new of pair (A'_n, B'_n) with an almost Minkowski basis $1, v'_{n,2}, v'_{n,3}, v'_{n,4}$ and the same discriminant $|D_n|$ as (A_n, B_n). And we have $|v_{n,2}| \asymp (t_1 t_2)^{-1} |D_n|^{1/6}, |v_{n,3}| \asymp t_1 |D_n|^{1/6}, |v_{n,4}| \asymp t_2 |D_n|^{1/6}$.

Let us recall that

$$\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \cdot (A, B) = (t^{-1} A, tB)$$

and

$$\begin{bmatrix} (t_1 t_2)^{-1} & & \\ & t_1 & \\ & & t_2 \end{bmatrix} \cdot (a_{ij}) = \begin{bmatrix} (t_1 t_2)^{-2} a_{11} & t_2^{-1} a_{12} & t_1^{-1} a_{13} \\ \cdot & t_1^2 a_{22} & t_1 t_2 a_{23} \\ \cdot & \cdot & t_2^2 a_{33} \end{bmatrix}$$

Trying to build a family with Minkowski type $\delta_2, \delta_3, \delta_4$ would be taking $t_2 = 2^{12n(\delta_3 - 1/6)} \asymp |D_n|^{\delta_3 - 1/6}$ and $t_3 = 2^{12n(\delta_4 - 1/6)} \asymp |D_n|^{\delta_4 - 1/6}$ (and thus $(t_1 t_2)^{-1} \asymp |D|^{\delta_2 - 1/6}$ if $\delta_2 + \delta_3 + \delta_4 = 1/2$). Assuming there is $t \in \mathbb{Q}$ that makes $\gamma \cdot (A_n, B_n)$ integral, then we just constructed a family of orders if K with Minkowski type $\delta_2, \delta_3, \delta_4$.

We now state and prove our existence theorem for the case where K can be any quartic number field and thus possible doesn't have a quadratic subfield. The necessary conditions on the $\delta'_i s$ will then be the strongest.

Theorem 4.2.1. *Let K be any quartic field. For any $\delta_2, \delta_3, \delta_4$ satisfying*

$$\begin{aligned} &\delta_2 \leq \delta_3 \leq \delta_4 \\ &\delta_2 + \delta_3 + \delta_4 = 1/2 \\ &\delta_3 \leq 2\delta_2 \\ &\delta_4 \leq \delta_2 + \delta_3 \text{ (or equivalently } \delta_4 \leq 1/4), \end{aligned}$$

there is a family of orders in K with Minkowski type $\delta_2, \delta_3, \delta_4$.

Proof. By Theorem 4.1.21, K contains an order given by a pair of ternary quadratic forms (A_0, B_0),

where A_0 is of the form

$$A_0 = \begin{bmatrix} 0 & 0 & \cdot \\ 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot \end{bmatrix}.$$

As above, we have a family $(A_n, B_n) = 2^n \cdot (A_0, B_0)$ with discriminant $|D_n| \asymp 2^{12n}$, of Minkowski type 1/6,1/6,1/6, and whose coefficients are either zero if the corresponding coefficient in (A_0, B_0) is zero or a multiple of 2^n. Apply γ as above to (A_0, B_0) with $t_1 = 2^{12n(\delta_3 - 1/6)}, t_2 = 2^{12n(\delta_4 - 1/6)}$ and again, assuming there is $t \in \mathbb{Q}$ that makes $\gamma \cdot (A_n, B_n)$ integral, then we just constructed a family of orders in K with the desired Minkowski type.

In this family, the "smallest" possibly non zero coefficients are b_{11}, a_{13}, a_{22}. What we mean by smallest is that, assuming they are non zero, if we take γ to be in $\mathcal{F}_G$, our fundamental domain for $GL_2(\mathbb{Z})\backslash GL_2(\mathbb{R})$, and with its coefficient being powers of 2^n then any coefficient of (A'_n, B'_n) will be a (bounded rational times an possibly large power of 2) multiple of one of these 3 coefficients of (A'_n, B'_n). In other words, if, assuming they are non zero, these 3 coefficients of (A'_n, B'_n) integral, then (A'_n, B'_n) is integral.

Thus, it suffices to show that there exists $t > 1$ such that for n big enough, we have

$$\begin{aligned} (t_1 t_2)^{-2} t 2^n &\in \mathbb{Z} \\ t_1^{-1} t^{-1} 2^n &\in \mathbb{Z} \\ t_1^2 t^{-1} 2^n &\in \mathbb{Z}, \end{aligned}$$

which, since $t_1 = 2^{12n(\delta_3 - 1/6)}, t_2 = 2^{12n(\delta_4 - 1/6)}$ (and thus $(t_1 t_2)^{-1} = 2^{12n(\delta_2 - 1/6)}$), is equivalent to

$$\begin{aligned} t 2^{n(24\delta_2 - 3)} &\in \mathbb{Z} \\ t^{-1} 2^{n(3 - 12\delta_3)} &\in \mathbb{Z} \\ t^{-1} 2^{n(24\delta_3 - 3)} &\in \mathbb{Z}. \end{aligned}$$

For some $\alpha \geq 0$ to be determined later, let $t = 2^{n\alpha}$. Then the above is all equivalent to show that there exists $\alpha \geq 0$ such that

$$\begin{aligned} \alpha &\geq 3 - 24\delta_2 \\ 3 - 12\delta_3 &\geq \alpha \\ 24\delta_3 - 3 &\geq \alpha, \end{aligned}$$

and there exist such α if and only if

$$\begin{aligned} 3 - 12\delta_3 &\geq 0 \\ 24\delta_3 - 3 &\geq 0 \\ 3 - 12\delta_3 &\geq 3 - 24\delta_2 \\ 24\delta_3 - 3 &\geq 3 - 24\delta_2, \end{aligned}$$

or equivalently

$$\begin{aligned}
&\delta_3 \leq 1/4\\
&\delta_3 \geq 1/8\\
&\delta_3 \leq 2\delta_2\\
&\delta_2 + \delta_3 \geq 1/4,
\end{aligned}$$

which is true by assumption. □

We now look at what happens if we know our quartic number field K has a quadratic subfield.

Theorem 4.2.2. *Let K be any quartic field that has a quadratic subfield.For any $\delta_2, \delta_3, \delta_4$ satisfying*

$$\begin{aligned}
&\delta_2 \leq \delta_3 \leq \delta_4\\
&\delta_2 + \delta_3 + \delta_4 = 1/2\\
&\delta_4 \leq \delta_2 + \delta_3 \text{ (or equivalently } \delta_4 \leq 1/4 \text{) },
\end{aligned}$$

there is a family of orders in K with Minkowski type $\delta_2, \delta_3, \delta_4$.

Proof. By Theorem 4.1.22, K contains an order corresponding to a pair of ternary quadratic forms (A_0, B_0), where A_0 is of the form

$$A_0 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & \cdot & \cdot \\ 0 & \cdot & \cdot \end{bmatrix}.$$

Similarly to the proof of Theorem 4.2.1, apply γ to $(A_n, B_n) = 2^n \cdot (A_0, B_0)$ with $t_1 = 2^{12n(\delta_3 - 1/6)}$ and $t_2 = 2^{12n(\delta_4 - 1/6)}$ and assuming $\gamma \cdot (A_n, B_n)$ is integral for n large enough, we have a family of orders in K with Minkowski type $\delta_2, \delta_3, \delta_4$.

Now the difference with Theorem 4.2.1 is that now the "smallest" possibly non zero coefficient coefficients of (A_n, B_n) are b_{11} and a_{22}.

Thus, it suffices to show that there exists $t > 1$ such that for n big enough, we have

$$\begin{aligned}
&(t_1 t_2)^{-2} t 2^n \in \mathbb{Z}\\
&t_1^2 t^{-1} 2^n \in \mathbb{Z},
\end{aligned}$$

which is 2 out of the 3 conditions we had in the proof of Theorem 4.2.1. Now by the proof of Theorem 4.2.1, this is equivalent to

$$\begin{aligned}
&\delta_3 \leq 1/4\\
&\delta_3 \geq 1/8\\
&\delta_2 + \delta_3 \geq 1/4,
\end{aligned}$$

which is true by assumption. □

4.3 Bounds - Proof of the quartic case of Theorem 0.0.8

We now prove our bounds that we proved sufficient in the previous section are in fact necessary. That is we prove Theorem 4.0.1 that we recall:

Theorem 4.3.1. *Let R be an order with (big) discriminant D in a quartic number field K, with Minkowski basis $v_1 = 1, v_2, v_3, v_4$, then*

$$|v_4| \ll |D|^{1/4}$$

or, if $|v_i| \asymp |D|^{\delta_i}$, then

$$\delta_4 \leq 1/4$$

and if K does not have a quadratic subfield, then we also have

$$|v_3|^3 |v_4|^2 \ll |D|$$

or, if $|v_i| \asymp |D|^{\delta_i}$, then

$$3\delta_3 + 2\delta_4 \leq 1 \tag{4.5}$$

The argument is very similar to the cubic case. Since there are only 3 non degenerate quartic rings over $\mathbb{R}$, there are only 3 non degenerate orbits for the action of $G(\mathbb{R})$ on $V_{\mathbb{R}}$. Fix representatives for these 3 orbits ν_1, ν_2, ν_3. Now let R be any order in a quartic field K with (big) discriminant D. Let $i = 1, 2, 3$ and $\gamma \in G(\mathbb{R})$ such that $R = R(\gamma \cdot \nu_i)$. Now if we pick $\gamma \in \mathcal{F}_G$, then $\gamma \cdot v_i$ will give an almost Minkowski basis for the shape of R

For the same reason as the cubic case, we may assume that γ is of the form

$$\gamma = \left(\begin{bmatrix} (t_1 t_2)^{-1} & & \\ & t_1 & \\ & & t_1 \end{bmatrix}, \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \right) \lambda,$$

for $\lambda = (D/Disc(\nu_i))^{1/12}$, $t \gg 1$ and $0 < (t_1 t_2)^{-1} \ll t_1 \ll t_2$.

Let $(A, B) = \lambda \cdot \nu_i$. This pair corresponds to an order in a quartic field with the same discriminant D as R, and of Minkowski type $1/6, 1/6, 1/6$. Also every coefficients of (A, B) are $O(|D|^{1/12})$. Write $A = (a_{11}, a_{12}, a_{13}, a_{22}, a_{23}, a_{33})$ and $B = (b_{11}, b_{12}, b_{13}, b_{22}, b_{23}, b_{33})$.

Apply

$$\gamma_0 := \left(\begin{bmatrix} (t_1 t_2)^{-1} & & \\ & t_1 & \\ & & t_1 \end{bmatrix}, \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \right).$$

We get a new pair (A', B') (that gives R) with

$$A' = (t^{-1} t_1^{-2} t_2^{-2} a_{11}, t^{-1} t_2^{-1} a_{12}, t^{-1} t_1^{-1} a_{13}, t^{-1} t_1^2 a_{22}, t^{-1} t_1 t_2 a_{23}, t^{-1} t_2^2 a_{33})$$
$$B' = (t t_1^{-2} t_2^{-2} b_{11}, t t_2^{-1} b_{12}, t t_1^{-1} b_{13}, t t_1^2 b_{22}, t t_1 t_2 b_{23}, t t_2^2 b_{33})$$

and we have

$$|v_2'| \asymp (t_1 t_2)^{-1} |D|^{1/6}$$
$$|v_3'| \asymp t_1 |D|^{1/6}$$
$$|v_4'| \asymp t_2 |D|^{1/6}$$

Now, for example, to get a Minkowski type $\delta_2, \delta_3, \delta_4$, we need to take $t_1 \asymp |D|^{\delta_3 - 1/6}$ and $t_2 \asymp |D|^{\delta_4 - 1/6}$. We prove necessary bounds on the δ_i's by proving necessary bounds on the $t_i' s$.

Proposition 4.3.2. *If R is an order with (big) discriminant D in a quartic field, and has Minkowski basis $1, v_2', v_3', v_4'$, then*

$$|v_4'| \ll |D|^{1/4}.$$

Proof. Suppose $|v_4'| = \omega(|D|^{1/4})$, this means that $t_2 = \omega(|D|^{1/12})$. Then since the coefficients of (A, B) are $O(|D|^{1/12})$, we have

$$a_{11}' = t^{-1} t_1^{-2} t_2^{-2} a_{11} = o(t^{-1} t_1^{-2} |D|^{-1/12})$$
$$a_{12}' = t^{-1} t_2^{-1} a_{12} = o(t^{-1})$$

so for D big enough, for A' to be integral, we need $a_{11} = a_{12} = 0$. But then by Theorem 4.1.19, since (A', B') corresponds to an order in a quartic field, we need

$$a_{22} \neq 0 \text{ and } b_{11} \neq 0$$

and then for (A', B') to be integral, we need

$$\frac{t}{t_1^2} \ll |D|^{1/12} \text{ and } \frac{t_1^2 t_2^2}{t} \ll |D|^{1/12},$$

which multiplied together give,

$$t_2 \ll |D|^{1/12},$$

and thus a contradiction. □

Proposition 4.3.3. *If R is an order in a quartic field that does not have a quadratic subfield, and has Minkowski basis $1, v_2', v_3', v_4'$, we also need that*

$$|v_3'|^3 |v_4'|^2 \ll |D|$$

where D is the discriminant of R.

Proof. Suppose that $|v_3'|^2 |v_4'|^3 = \omega(|D|)$. This means that $t_1^3 t_2^2 = \omega(|D|^{1/6})$ and thus

$$a_{11}' = t^{-1} t_1^{-2} t_2^{-2} a_{11} = o(t^{-1}),$$

which forces $a_{11} = 0$ for (A', B') to be integral for D big enough. Now by Theorem 4.1.19, we have $b_{11} \neq 0$. We then have

$$t \gg \frac{t_1^2 t_2^2}{|D|^{1/12}}.$$

And by Theorem 4.1.20, we cannot have $a_{12} = a_{13} = 0$, but the above lower bound on t gives

$$a'_{12} = t^{-1}t_2^{-1}a_{12} \ll \frac{|D|^{1/6}}{t_1^3 t_2^2},$$

which is $o(1)$ by assumption, and thus $a_{12} = 0$.

Similarly,

$$a'_{13} = t^{-1}t_1^{-1}a_{13} = o\left(\frac{|D|^{1/6}}{t_1^3 t_2^2}\right) = o(1),$$

so $a_{13} = 0$. We proved that under these conditions, $a_{12} = a_{13} = 0$, which is a contradiction. □

Chapter 5

Counting quartic orders with a given form of Minkowski basis

In this chapter, we will use Bhargava's correspondence, see Section 4.1 for background, to estimate, when ordered by discriminant, the number of quartic orders with a given form of Minkowski basis.

Let $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{R}}$) be the set of integral (resp. real) pairs of ternary quadratic forms. We know that the action of $G(\mathbb{R}) = GL_2(\mathbb{R}) \times SL_3(\mathbb{R})$ on $V_{\mathbb{R}}$ gives three orbits namely $V_{\mathbb{R}}^{(i)}$, those that correspond to quartic rings with $4-2i$ real embeddings, for $i = 0, 1, 2$. For each i, let $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$.

In this chapter, we use the following notation for the torus of $G(\mathbb{R})$:

$$\begin{bmatrix} s_1^{-1} & & \\ & s_1 & \end{bmatrix}, \begin{bmatrix} s_2^{-2}s_3^{-1} & & \\ & s_2 s_3^{-1} & \\ & & s_2 s_3^2 \end{bmatrix},$$

which is in $\mathcal{F}_G$ if and only if $s_1 \geq \sqrt[4]{3}/\sqrt{2}$ and $s_2, s_3 \geq \sqrt[6]{3}/\sqrt[3]{2}$, as in [3].

As in [3], for a $G(\mathbb{Z})$-invariant subset S of $V_{\mathbb{Z}}^{(i)}$, let $N(S;X)$ be the number of absolutely irreducible $G(\mathbb{Z})$-orbits on S having discriminant less than X.

Let us recall that by Bhargava's correspondence, we have the determinant preserving map

$$G(\mathbb{Z})\backslash V_{\mathbb{Z}} \leftrightarrow \{(R, R') : \ R \text{ is a quartic ring over } \mathbb{Z} \text{ and } R' \text{ is a cubic resolvent of } R\}/\sim,$$

where absolutely irreducible pairs correspond to orders in a quartic fields that have no quadratic subfield, and thus $N(S;X)$ also counts the number of pairs (R, R') of orders R in a quartic field (that has no quadratic subfield field) and a cubic resolvent R' of R, with discriminant less than X and that are in the subset corresponding to S.

Note that as quartic rings over $\mathbb{Z}$ do not in general have a unique cubic resolvent, this will not exactly count the number of orders in a quartic field having the properties that we want. While this could be done using the method in [3], we will not do it in this thesis.

The first step of setting up the integral that will count $N(S;X)$ is the same thing as the cubic case replacing $V_{\mathbb{R}}, V_{\mathbb{Z}}$ and the group acting on it by their quartic analogs. That is, we let $d\nu$ denote the usual Euclidean measure on $V_{\mathbb{R}}$ (normalized so that $V_{\mathbb{Z}}$ has co-volume 1) and let $dg = s_1^{-2}s_2^{-6}s_3^{-6}dud^\times s dk d^\times\lambda$ (where $du = du_1du_2du_3$ and $d^\times s = d^\times s_1 d^\times s_2 d^\times s_3$) be the Haar measure of $G(\mathbb{R})$ obtained from its

Iwasawa decomposition (where dk is normalized to have measure 1 on $SO_2(\mathbb{R})\times SO_3(\mathbb{R})$). Fix a bounded $SO_2(\mathbb{R}) \times SO_3(\mathbb{R})$ invariant subset B of $V_{\mathbb{R}}$ whose elements have discriminant at least one. We have

$$N(S;X) = \frac{1}{M_i}\int_{g\in\mathcal{F}_G} \#\{x \in S^{\text{abs irr}} \cap gB : |Disc(x)| < X\}dg, \tag{5.1}$$

where

$$M_i = \frac{n_i}{2\pi}\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}} |Disc(\nu)|^{-1}d\nu,$$

where n_i is the order of the stabilizer of ν_i in $G(\mathbb{R})$. Now by the Bhargava correspondence, the stabilizer of ν_i in $G(\mathbb{R})$ is naturally isomorphic the group of ring automorphisms of $R(\nu_i)$. We then have $n_0 = Aut_{\mathbb{R}}(\mathbb{R}^4) = 24$, $n_1 = Aut_{\mathbb{R}}(\mathbb{R}^2\times\mathbb{C}) = 4$ and $n_2 = Aut_{\mathbb{R}}(\mathbb{C}^2) = 8$.

Note that, unlike the cubic case, there is no error term here since every absolutely irreducible elements in $V_{\mathbb{Q}}^{(i)}$ appears exactly n_i times in $\mathcal{F}_G\cdot\nu_i$. This comes from the fact that a quartic number field that does not have a quadratic subfield must have a trivial automorphism group, and the number of times an element $\nu\in V_{\mathbb{Q}}^{(i)}$ appears in $\mathcal{F}_G\cdot\nu_i$ is $n_i/Aut_{\mathbb{Q}}(R(\nu))$.

We will then use Proposition 3.0.1, like in the cubic case, that we recall:

Proposition 5.0.1. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most l. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation on $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$Vol(\mathcal{R}) + O(\max\{Vol(\overline{\mathcal{R}}, 1)\}),$$

where $Vol(\overline{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implies constant depends only on n, m, k and l.

Now given $0 < \delta_2 < \delta_3 < \delta_4$ with $\delta_2+\delta_3+\delta_4 = 1/2$ (and as we know will end up being necessary for the count to be positive $\delta_3 \le 2\delta_2$ and $\delta_4 \le \delta_2+\delta_3$). For $0 < c_1 < c_2$ and $0 < d_1 < d_2$, define

$$S_{\delta_2,\delta_3,\delta_4} = \{\nu\in V_{\mathbb{R}} : c_1|Disc(\nu)|^{\delta_3-\delta_2} \le \overline{z_\nu}\cdot(0,1,0) < c_2|Disc(\nu)|^{\delta_3-\delta_2}$$

$$\text{and } d_1|Disc(\nu)|^{\delta_4-\delta_2} \le \overline{w_\nu}\cdot(0,0,1) < d_2|Disc(\nu)|^{\delta_4-\delta_2}\}.$$

Note this is exactly the quartic analog of the way we defined S in the cubic case.

Lemma 5.0.2. *For $\nu\in S_{\delta_2,\delta_3,\delta_4}\cap V_{\mathbb{Z}}$, $R(\nu)$ has Minkowski type $\delta_2,\delta_3,\delta_4$.*

Proof. By definition of $\mathcal{F}$, $\{(1,0,0), \overline{z_\nu}, \overline{w_\nu}\}$ is a Minkowski basis for a rotated and scaled $S(\nu)$. So for $\nu\in S_{\delta_2,\delta_3,\delta_4}\cap V_{\mathbb{Z}}$ and a Minkowski basis $1, v_2, v_3, v_4$ for $R(\nu)$, we have

$$\frac{|v_3|}{|v_2|} \asymp |\overline{z_\nu}| \asymp \overline{z_\nu}\cdot(0,1,0) \asymp |Disc(\nu)|^{\delta_3-\delta_2}$$
$$\frac{|v_4|}{|v_2|} \asymp |\overline{w_\nu}| \asymp \overline{w_\nu}\cdot(0,0,1) \asymp |Disc(\nu)|^{\delta_4-\delta_2}.$$

Now since $1, v_2, v_3, v_4$ is Minkowski, we have $|v_2||v_3||v_4| \asymp |Disc(\nu)|^{1/2}$, putting these together, we get

$$|v_2| \asymp |Disc(\nu)|^{\delta_2}$$
$$|v_3| \asymp |Disc(\nu)|^{\delta_3}$$
$$|v_4| \asymp |Disc(\nu)|^{\delta_4}$$

□

With this method, we will give an estimate for the number of quartic orders with a given form of Minkowski basis in Section 5.1 and then estimate for the number of such orders that are maximal in Section 5.2.

5.1 An estimate for the number of quartic orders with a given form of Minkowski basis

In this section we take $0 < \delta_2 < \delta_3 < \delta_4$ with $\delta_2 + \delta_3 + \delta_4 = 1/2$. We also fix take constants $0 < c_1 < c_2$ and $0 < d_1 < d_2$, and we let

$$S = S_{\delta_2,\delta_3,\delta_4} = \{\nu \in V_{\mathbb{R}} : c_1|Disc(\nu)|^{\delta_3-\delta_2} \leq \overline{z_\nu} \cdot (0,1,0) < c_2|Disc(\nu)|^{\delta_3-\delta_2}$$

$$\text{and } d_1|Disc(\nu)|^{\delta_4-\delta_2} \leq \overline{w_\nu} \cdot (0,0,1) < d_2|Disc(\nu)|^{\delta_4-\delta_2}\}.$$

Let $N(S \cap V_{\mathbb{Z}}^{(i)}; X)$ denote the number of **absolutely irreducible** $G(\mathbb{Z})$-orbits on $S \cap V_{\mathbb{Z}}^{(i)}$ having discriminant less than X. It is also the number of pairs (R, R'), where R is an absolutely irreducible quartic ring Minkowski type $\delta_2, \delta_3, \delta_4$, and discriminant less than X and R' is a cubic resolvent ring of R.

Theorem 5.1.1. *For each $i = 1, 2, 3$ and for each rational $\delta_2, \delta_3, \delta_4$, we have*

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = C_{\delta_2,\delta_4} X^{1-2(\delta_4-\delta_2)} + O(X^{11/12}),$$

where

$$C_{\delta_2,\delta_4} = \left(\frac{1}{M_i}\right)\left(\int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} \frac{(w_\nu \cdot (0,0,1))^2}{|Disc(\nu)|} d\nu\right)\left(\frac{1}{18\sqrt{3}}\right)$$
$$\left(\frac{1}{d_1^2} - \frac{1}{d_2^2}\right)\left(\frac{1}{12 - 24(\delta_4 - \delta_2)}\right)(\ln(c_2) - \ln(c_1)),$$

for any bounded $SO_2(\mathbb{R}) \times SO_3(\mathbb{R})$ invariant subset B of $V_{\mathbb{R}}$ whose elements have discriminant at least one.

Proof of Theorem 5.1.1

Let B be a bounded $SO_2(\mathbb{R}) \times SO_3(\mathbb{R})$ invariant subset of $V_{\mathbb{R}}$ whose element have discriminant at least one. Applying (5.1), we have

$$N(S\cap V_{\mathbb{Z}}^{(i)};X)=\frac{1}{M_i}\int_{g\in\mathcal{F}_G}\#\{x\in S\cap B_i(g,X)\cap V_{\mathbb{Z}}^{\text{abs irr}}\}dg,$$

where

$$B_i(g,X)=g\cdot B\cap\{\nu\in V_{\mathbb{R}}^{(i)}:|Disc(\nu)|<X\}$$

and

$$M_i=\frac{n_i}{2\pi}\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}|Disc(\nu)|^{-1}d\nu,$$

and remember that since B is $SO_2(\mathbb{R})\times SO_3(\mathbb{R})$ invariant, we might only integrate over elements of $\mathcal{F}_G$ with trivial $SO_2(\mathbb{R})\times SO_3(\mathbb{R})$ part.

By Lemma 11 and 12 in [3], we can replace the condition that ν is absolutely irreducible by $a_{11}\neq 0$, up to an error of $O(X^{11/12})$. So we have

$$N(S\cap V_{\mathbb{Z}}^{(i)};X)=\frac{1}{M_i}\int_{g\in\mathcal{F}_G}\#\{x\in S\cap B_i(g,X)\cap V_{\mathbb{Z}}:a_{11}\neq 0\}dg+O(X^{11/12}).\tag{5.2}$$

Now Proposition 5.0.1 gives

$$\#\{\nu=(A,B)\in S\cap B_i(g,X)\cap V_{\mathbb{Z}}:a_{11}\neq 0\}=\begin{cases}Vol(S\cap B_i(g,X))+\text{Error , if } s_1s_2^2s_3\ll\lambda\ll X^{1/12}\\ 0,\text{ otherwise}\end{cases}\tag{5.3}$$

where the error term is the greatest d-dimensional volume of any projection of $B_i(g,X)$ onto a coordinate subspace obtained by equating $12-d$ coordinates to zero, where d takes all values from 0 to 11.

Let us first compute the main term.

$$MT=\frac{1}{M_i}\int_{\substack{g\in\mathcal{F}_G\\ s_1s_2^2s_3\ll\lambda\ll X^{1/12}}}Vol(S\cap B_i(g,X))dg$$

Note we might remove the restriction $\lambda\ll X^{1/12}$ in the integral since the integrand will be zero otherwise, and we might remove $s_1s_2^2s_3\ll\lambda$ since $Vol(S\cap B_i(g,X))\ll\lambda^{12}$ so the contribution of the part of the integral where $s_1s_2^2s_3\gg\lambda$ is

$$\begin{aligned}\int_{\substack{g\in\mathcal{F}_G\\ s_1s_2^2s_3\gg\lambda\\ \lambda\ll X^{1/12}}}Vol(S\cap B_i(g,X))dg&\ll\int_{\lambda\ll X^{1/12}}\lambda^{12}\int\int_{s_2s_3\gg 1}(s_2s_3)^{-6}\int_{s_1\gg\lambda/(s_2^2s_3)}s_1^{-2}d^\times s d^\times\lambda\\ &\ll\int_{\lambda\ll X^{1/12}}\lambda^{10}\int\int_{s_2,s_3\gg 1}s_2^{-2}s_3^{-4}d^\times s_2 d^\times s_3 d^\times\lambda\\ &\ll X^{10/12},\end{aligned}$$

which will be absorbed by the error term of $O(X^{11/12})$ that we already have.

By the change of variable $\nu'=g^{-1}\cdot\nu$, we compute

$$Vol(S\cap B_i(g,X))=\lambda^{12}Vol(B\cap\{\nu\in V_{\mathbb{R}}^{(i)}:|Disc(\nu)|<X/\lambda^{12}$$

$$\text{and } c_1(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2} \leq \overline{g\cdot z_\nu}\cdot(0,1,0) < c_2(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

$$\text{and } d_1(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2} \leq \overline{g\cdot w_\nu}\cdot(0,0,1) < d_2(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}\})$$

Lemma 5.1.2. *For $\delta_2 < \delta_3 < \delta_4$, for the sake of computing our main term, we may assume that for $\nu \in B$ and $g = (g_2, g_3) \in \mathcal{F}_G$ with $g_3 = \begin{bmatrix} 1 & & \\ u_1 & 1 & \\ u_2 & u_3 & 1 \end{bmatrix} \begin{bmatrix} s_2^{-2}s_3^{-1} & & \\ & s_2s_3^{-1} & \\ & & s_2s_3^2 \end{bmatrix}$ (no $SO_3(\mathbb{R})$ part), we have*

$$c_1(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2} \leq \overline{g\cdot z_\nu}\cdot(0,1,0) < c_2(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

$$d_1(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2} \leq \overline{g\cdot w_\nu}\cdot(0,0,1) < d_2(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}\})$$

$$\iff$$

$$c_1(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2} \leq gz_\nu\cdot(0,1,0) < c_2(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

$$d_1(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2} \leq gw_\nu\cdot(0,0,1) < d_2(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}\})$$

Proof. The torus part of g sends $(1,0,0)$ and z to $(1,0,0)$ and s_2^3z, which spans a 2 dimensional lattice that is in the plane orthogonal to $(0,0,1)$. So by the 2 dimensional case, that covered in the cubic analog of this lemma, if s_2^3 is "big enough", that is equivalent to gz "big enough", we have $\overline{gz} = gz + u_1(1,0,0)$, for some $u_1 \in \mathbb{Z}$, and then

$$\overline{gz}\cdot(0,1,0) = gz\cdot(0,1,0).$$

where "big enough" is bigger than an absolute constant (only depends on the choice of B).

Also, similarly, if s_3^2 is "big enough", or equivalently if gw is big enough compared to gz, we have $\overline{gw} = gw + u_2(1,0,0) + u_3z$, for some $u_2, u_3 \in \mathbb{Z}$, and then

$$\overline{gw}\cdot(0,0,1) = gw\cdot(0,0,1).$$

Now if s_2^3 is not "big enough", $s_2^3 \ll 1$, then both $g\cdot z_\nu\cdot(0,1,0)$ and $\overline{g\cdot z_\nu}\cdot(0,1,0)$ are $O(1)$, so since $\delta_3 > \delta_2$, both sides of the "equivalence" of this lemma will be false for $\lambda > \log(X)$. The case where $\lambda \leq \log(X)$ can just (lightly) contribute to the error term.

Now if s_2^2 is not "big enough", $s_3^2 \ll 1$, then both ratios $(g\cdot z_\nu\cdot(0,1,0))/(g\cdot w_\nu\cdot(0,0,1))$ and $(\overline{g\cdot z_\nu}\cdot(0,1,0))/(\overline{g\cdot w_\nu}\cdot(0,0,1))$ are $O(1)$, so since $\delta_4 > \delta_3$, both sides will be false for $\lambda > \log(X)$. And again the case where $\lambda \leq \log(X)$ can contribute to the error term. □

By the above lemma, we may assume that

$$Vol(S\cap B_i(g,X)) = \lambda^{12}Vol(B\cap\{\nu\in V_{\mathbb{R}}^{(i)} : |Disc(\nu)| < X/\lambda^{12}$$

$$\text{and } c_1(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2} \leq g\cdot z_\nu\cdot(0,1,0) < c_2(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

$$\text{and } d_1(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2} \leq g\cdot w_\nu\cdot(0,0,1) < d_2(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

and this is convenient because (if g has no $SO_3(\mathbb{R})$ part, which we may assume in the computation of this integral since B is $SO_2(\mathbb{R})\times SO_3(\mathbb{R})$ invariant),

$$(g\cdot z_\nu)\cdot(0,1,0) = s_2^3(z_\nu\cdot(0,1,0)) \text{ and } (g\cdot w_\nu)\cdot(0,0,1) = (s_2s_3)^3(w_\nu\cdot(0,0,1))$$

Thus, the main term of $N(S \cap V_{\mathbb{Z}}^{(i)}; X)$ is

$$MT = \frac{1}{M_i} \int_{g \in \mathcal{F}_G} \lambda^{12} \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} \left(\chi_{|Disc(\nu)|<X/\lambda^{12}}\right) \left(\chi_{c_1 \frac{(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}}{(z_\nu \cdot (0,1,0))} \leq s_2^3 < c_2 \frac{(\lambda^{12} Disc(\nu))^{\delta_3-\delta_2}}{(z_\nu \cdot (0,1,0))}}\right)$$
$$\left(\chi_{d_1 \frac{(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}}{(w_\nu \cdot (0,0,1))} \leq (s_2 s_3)^3 < d_2 \frac{(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}}{(w_\nu \cdot (0,0,1))}}\right) d\nu dg$$
$$= \frac{1}{M_i} \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} \int_{0<\lambda<\left(\frac{X}{|Disc(\nu)|}\right)^{1/12}} \lambda^{12} \int \int_{(s_2,s_3) \in \mathcal{R}} (s_2 s_3)^{-6} \int_{s_1 \geq \sqrt[4]{3}/\sqrt{2}} s_1^{-2} d^\times s d^\times \lambda d\nu,$$

Where

$$\mathcal{R} = \Big\{(s_2, s_3) \in (\mathbb{R}^+)^2 : c_1 \frac{(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}}{(z_\nu \cdot (0,1,0))} \leq s_2^3 < c_2 \frac{(\lambda^{12} Disc(\nu))^{\delta_3-\delta_2}}{(z_\nu \cdot (0,1,0))}$$
$$\text{and } d_1 \frac{(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}}{(w_\nu \cdot (0,0,1))} \leq (s_2 s_3)^3 < d_2 \frac{(\lambda^{12}|Disc(\nu)|)^{\delta_4-\delta_2}}{(w_\nu \cdot (0,0,1))}\Big\}.$$

We can compute

$$\int_{s_1 \geq \sqrt[4]{3}/\sqrt{2}} s_1^{-2} d^\times s_1 = \frac{1}{\sqrt{3}},$$

and

$$\int \int_{(s_2,s_3) \in \mathcal{R}} (s_2 s_3)^{-6} d^\times s_2 d^\times s_3 =$$

$$\frac{1}{18} \left(\frac{1}{d_1^2} - \frac{1}{d_2^2}\right) (w_\nu \cdot (0,0,1))^2 (\lambda^{12}|Disc(\nu)|)^{-2(\delta_4-\delta_2)} (\ln(c_2) - \ln(c_1)).$$

Thus

$$MT = \left(\frac{1}{M_i}\right) \frac{1}{18\sqrt{3}} \left(\frac{1}{d_1^2} - \frac{1}{d_2^2}\right) (\ln(c_2) - \ln(c_1)) \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} (w_\nu \cdot (0,0,1))^2$$
$$|Disc(\nu)|^{-2(\delta_4-\delta_2)} \int_{0<\lambda<\left(\frac{X}{|Disc(\nu)|}\right)^{1/12}} \lambda^{12[1-2(\delta_4-\delta_2)]} d^\times \lambda d\nu$$
$$= \left(\frac{1}{M_i}\right) \frac{1}{18\sqrt{3}} \left(\frac{1}{d_1^2} - \frac{1}{d_2^2}\right) (\ln(c_2) - \ln(c_1)) \left(\frac{1}{12 - 24(\delta_4 - \delta_2)}\right) X^{1-2(\delta_4-\delta_2)}$$
$$\int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} \frac{(w_\nu \cdot (0,0,1))^2}{|Disc(\nu)|} d\nu$$

Let's now compute the error term that comes from the error term in (5.3), that is the greatest d-dimensional volume of any projection of $B_i(g, X)$ onto a coordinate subspace obtained by equating $12 - d$ coordinates to zero, where d takes all values from 0 to 11.

We integrate all possible greatest d-dimensional volumes in Table 5.1 below. For the bounds of integration we have $0 < \lambda < X^{1/12}, s_i \gg 1, s_1 s_2^2 s_3 \ll \lambda$ (from (5.3) so that $a_{11} \neq 0$) ,$s_2 s_3 \asymp \lambda^{4(\delta_4-\delta_2)}, s_2 \asymp \lambda^{4(\delta_3-\delta_2)}$ (so that $(s_2, s_3) \in \mathcal{R}$).

Note that

$$s_2 s_3 \asymp \lambda^{4(\delta_4-\delta_2)} \text{ and } s_2 \asymp \lambda^{4(\delta_3-\delta_2)} \implies s_2 s_3 \ll \lambda,$$

so the sharpest bounds of integration are

$$\int_{0<\lambda \ll X^{1/12}} \int_{s_2 \asymp \lambda^{4(\delta_3-\delta_2)}} \int_{s_3 \asymp s_2^{-1} \lambda^{4(\delta_4-\delta_2)}} \int_{1 \ll s_1 \ll s_2^{-2} s_3^{-1} \lambda}$$

Table 5.1.0.1:

d	$\ll \int_{\square} dg$	$\ll \int_{\square} d^{\times} s d^{\times} \lambda$	$\ll \square$	$\ll \square$
1	$\lambda^1 s_1^1 s_2^2 s_3^4$	$\lambda^1 s_1^{-1} s_2^{-4} s_3^{-2}$	$X^{(1-8(\delta_3-\delta_2)-8(\delta_4-\delta_2))/12}$	$X^{1/12}$
2	$\lambda^2 s_1^2 s_2^4 s_3^5$	$\lambda^2 s_1^0 s_2^{-2} s_3^{-1}$	$X^{(2-4(\delta_3-\delta_2)-4(\delta_4-\delta_2))/12+\epsilon}$	$X^{2/12+\epsilon}$
2	$\lambda^2 s_1^0 s_2^4 s_3^8$	$\lambda^2 s_1^{-2} s_2^{-2} s_3^2$	$X^{(2-16(\delta_3-\delta_2)+8(\delta_4-\delta_2))/12}$	$X^{3/12}$
3	$\lambda^3 s_1^3 s_2^6 s_3^3$	$\lambda^3 s_1^1 s_2^0 s_3^{-3}$	$X^{(4+8(\delta_3-\delta_2)-16(\delta_4-\delta_2))/12}$	$X^{4/12}$
3	$\lambda^3 s_1^1 s_2^6 s_3^9$	$\lambda^3 s_1^{-1} s_2^0 s_3^3$	$X^{(3-12(\delta_3-\delta_2)+12(\delta_4-\delta_2))/12}$	$X^{4.5/12}$
3	$\lambda^3 s_1^3 s_2^3 s_3^6$	$\lambda^3 s_1^1 s_2^{-3} s_3^0$	$X^{(4-16(\delta_3-\delta_2)-4(\delta_4-\delta_2))/12}$	$X^{4/12}$
4	$\lambda^4 s_1^4 s_2^5 s_3^4$	$\lambda^4 s_1^2 s_2^{-1} s_3^{-2}$	$X^{(6-4(\delta_3-\delta_2)-16(\delta_4-\delta_2))/12}$	$X^{6/12}$
4	$\lambda^4 s_1^2 s_2^8 s_3^7$	$\lambda^4 s_1^0 s_2^2 s_3^1$	$X^{(4+4(\delta_3-\delta_2)+4(\delta_4-\delta_2))/12+\epsilon}$	$X^{5/12+\epsilon}$
4	$\lambda^4 s_1^0 s_2^8 s_3^{10}$	$\lambda^4 s_1^{-2} s_2^2 s_3^4$	$X^{(4-8(\delta_3-\delta_2)+16(\delta_4-\delta_2))/12}$	$X^{6/12}$
4	$\lambda^4 s_1^2 s_2^5 s_3^{10}$	$\lambda^4 s_1^0 s_2^{-1} s_3^4$	$X^{(4-20(\delta_3-\delta_2)+16(\delta_4-\delta_2))/12+\epsilon}$	$X^{6/12+\epsilon}$
5	$\lambda^5 s_1^5 s_2^4 s_3^2$	$\lambda^5 s_1^3 s_2^{-2} s_3^{-4}$	$X^{(8-4(\delta_3-\delta_2)-28(\delta_4-\delta_2))/12}$	$X^{8/12}$
5	$\lambda^5 s_1^3 s_2^7 s_3^8$	$\lambda^5 s_1^1 s_2^1 s_3^2$	$X^{(6-8(\delta_3-\delta_2)+4(\delta_4-\delta_2))/12}$	$X^{6.5/12}$
5	$\lambda^5 s_1^1 s_2^{10} s_3^8$	$\lambda^5 s_1^{-1} s_2^4 s_3^2$	$X^{(5+8(\delta_3-\delta_2)+8(\delta_4-\delta_2))/12}$	$X^{7/12}$
5	$\lambda^5 s_1^1 s_2^7 s_3^{11}$	$\lambda^5 s_1^{-1} s_2^1 s_3^5$	$X^{(5-16(\delta_3-\delta_2)+20(\delta_4-\delta_2))/12}$	$X^{7.5/12}$
6	$\lambda^6 s_1^6 s_2^0 s_3^0$	$\lambda^6 s_1^4 s_2^{-6} s_3^{-6}$	$X^{(10-16(\delta_3-\delta_2)-40(\delta_4-\delta_2))/12}$	$X^{10/12}$
6	$\lambda^6 s_1^4 s_2^6 s_3^6$	$\lambda^6 s_1^2 s_2^0 s_3^0$	$X^{(8-8(\delta_3-\delta_2)-8(\delta_4-\delta_2))/12}$	$X^{8/12}$
6	$\lambda^6 s_1^2 s_2^9 s_3^9$	$\lambda^6 s_1^0 s_2^3 s_3^3$	$X^{(6+12(\delta_4-\delta_2))/12+\epsilon}$	$X^{8/12+\epsilon}$
6	$\lambda^6 s_1^0 s_2^{12} s_3^6$	$\lambda^6 s_1^{-2} s_2^6 s_3^0$	$X^{(6+24(\delta_3-\delta_2))/12+\epsilon}$	$X^{8.4/12+\epsilon}$
6	$\lambda^6 s_1^0 s_2^6 s_3^{12}$	$\lambda^6 s_1^{-2} s_2^0 s_3^6$	$X^{(6-24(\delta_3-\delta_2)+24(\delta_4-\delta_2))/12}$	$X^{9/12}$
7	$\lambda^7 s_1^5 s_2^2 s_3^4$	$\lambda^7 s_1^3 s_2^{-4} s_3^{-2}$	$X^{(10-20(\delta_3-\delta_2)-20(\delta_4-\delta_2))/12}$	$X^{10/12}$
7	$\lambda^7 s_1^3 s_2^8 s_3^7$	$\lambda^7 s_1^1 s_2^2 s_3^1$	$X^{(8)/12+\epsilon}$	$X^{8/12+\epsilon}$
7	$\lambda^7 s_1^1 s_2^{11} s_3^7$	$\lambda^7 s_1^{-1} s_2^5 s_3^1$	$X^{(7+16(\delta_3-\delta_2)+4(\delta_4-\delta_2))/12}$	$X^{9/12}$
7	$\lambda^7 s_1^1 s_2^8 s_3^{10}$	$\lambda^7 s_1^{-1} s_2^2 s_3^4$	$X^{(7-8(\delta_3-\delta_2)+16(\delta_4-\delta_2))/12}$	$X^{9/12}$
8	$\lambda^8 s_1^4 s_2^4 s_3^5$	$\lambda^8 s_1^2 s_2^{-2} s_3^{-1}$	$X^{(10-12(\delta_3-\delta_2)-12(\delta_4-\delta_2))/12}$	$X^{10/12}$
8	$\lambda^8 s_1^2 s_2^{10} s_3^5$	$\lambda^8 s_1^0 s_2^4 s_3^{-1}$	$X^{(8+20(\delta_3-\delta_2)-4(\delta_4-\delta_2))/12+\epsilon}$	$X^{9.6/12+\epsilon}$
8	$\lambda^8 s_1^0 s_2^{10} s_3^8$	$\lambda^8 s_1^{-2} s_2^4 s_3^2$	$X^{(8+8(\delta_3-\delta_2)+8(\delta_4-\delta_2))/12}$	$X^{10/12}$
8	$\lambda^8 s_1^2 s_2^7 s_3^8$	$\lambda^8 s_1^0 s_2^1 s_3^2$	$X^{(8-4(\delta_3-\delta_2)+8(\delta_4-\delta_2))/12+\epsilon}$	$X^{9/12+\epsilon}$
9	$\lambda^9 s_1^3 s_2^6 s_3^3$	$\lambda^9 s_1^1 s_2^0 s_3^{-3}$	$X^{(10+8(\delta_3-\delta_2)-16(\delta_4-\delta_2))/12}$	$X^{10/12}$
9	$\lambda^9 s_1^1 s_2^9 s_3^6$	$\lambda^9 s_1^{-1} s_2^3 s_3^0$	$X^{(9+12(\delta_3-\delta_2))/12+\epsilon}$	$X^{10.2/12+\epsilon}$
9	$\lambda^9 s_1^3 s_2^3 s_3^6$	$\lambda^9 s_1^1 s_2^{-3} s_3^0$	$X^{(10-16(\delta_3-\delta_2)-4(\delta_4-\delta_2))/12}$	$X^{10/12}$
10	$\lambda^{10} s_1^2 s_2^5 s_3^4$	$\lambda^{10} s_1^0 s_2^{-1} s_3^{-2}$	$X^{(10+4(\delta_3-\delta_2)-8(\delta_4-\delta_2))/12+\epsilon}$	$X^{10/12+\epsilon}$
10	$\lambda^{10} s_1^0 s_2^8 s_3^4$	$\lambda^{10} s_1^{-2} s_2^2 s_3^{-2}$	$X^{(10+16(\delta_3-\delta_2)-8(\delta_4-\delta_2))/12}$	$X^{10.8/12}$
11	$\lambda^{11} s_1^1 s_2^4 s_3^2$	$\lambda^{11} s_1^{-1} s_2^{-2} s_3^{-4}$	$X^{(11+8(\delta_3-\delta_2)-16(\delta_4-\delta_2))/12}$	$X^{11/12}$

We can see from the table that they all give an error term that will be absorbed by the error of $O(X^{11/12})$ that we already have.

5.2 An estimate for the number of maximal quartic orders with a given form of Minkowski basis

We are now interested in $N(S \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X)$, the number of absolutely irreducible and **maximal** $G(\mathbb{Z})$-orbits on $S \cap V_{\mathbb{Z}}^{(i)}$ having discriminant less than X. It is also the number of pairs (R, R'), where R is an absolutely irreducible, maximal quartic ring having Minkowski type $\delta_2, \delta_3, \delta_4$, and discriminant less than X and R' is a cubic resolvent ring of R. Now since maximal quartic rings have a unique cubic resolvent, it is simply the number of absolutely irreducible, maximal quartic ring having Minkowski type $\delta_2, \delta_3, \delta_4$, and discriminant less than X.

Theorem 5.2.1. *For each $i = 1, 2, 3$ For each rational $\delta_2, \delta_3, \delta_4$, we have*

$$N(S \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = \mu(\mathcal{U}) C_{\delta_2, \delta_4} X^{1-2(\delta_4 - \delta_2)} + O_\epsilon(X^{71/72+\epsilon}),$$

where C_{δ_2,δ_4} is the same constant as in Theorem 5.1.1, that is

$$C_{\delta_2,\delta_4} = \left(\frac{1}{M_i}\right) \frac{1}{18\sqrt{3}} \left(\frac{1}{d_1^2} - \frac{1}{d_2^2}\right) (\ln(c_2) - \ln(c_1)) \left(\frac{1}{12 - 24(\delta_4 - \delta_2)}\right) \left(\int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} \frac{(w_\nu \cdot (0,0,1))^2}{|Disc(\nu)|} d\nu\right)$$

for any bounded $SO_2(\mathbb{R}) \times SO_3(\mathbb{R})$ invariant subset B of $V_{\mathbb{R}}$ whose elements have discriminant at least one.

Proof of Theorem 5.2.1

The idea is pretty much the same as the cubic case. We have

$$N(S \cap \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{M_i} \int_{g \in \mathcal{F}_G} \#\{x \in S \cap \mathcal{U} \cap B_i(g, X) \cap a_{11} \neq 0\} dg + O(X^{11/12}),$$

where

$$B_i(g, X) = g \cdot B \cap \{\nu \in V_{\mathbb{R}}^{(i)} : |Disc(\nu)| < X\}$$

and

$$M_i = \frac{n_i}{2\pi} \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} |Disc(\nu)|^{-1} d\nu.$$

We then need an analogue of Theorem 3.2.2:

Theorem 5.2.2. *Suppose V is a subset of $V_{\mathbb{Z}}^{(i)}$ defined by finitely many congruence conditions modulo prime powers, and $\mu_p(V)$ denotes the p-adic density of V in $V_{\mathbb{Z}}$. Let m be the smallest integer such that V is defined by congruences modulo m. The number of lattice points (A, B) in $B_i(g, X) \cap S$ with $a_{11} \neq 0$ is*

$$\begin{cases} \prod_p \mu_p(V) Vol(B_i(g, X)) + Error, \text{ if } s_1 s_2^2 s_3 \ll \lambda \\ 0, \text{ otherwise} \end{cases}$$

where the error term is the greatest of each d-dimensional volume of any projection of $B_i(g,X)$ onto a coordinate subspace obtained by equating $12-d$ coordinates to zero multiplied by $m^{12-d}\prod_p \mu_p(V)$, where d takes all values from 1 to 11.

Proof. Similar to the proof of Theorem 3.2.2 (cubic analog) □

Then we separate big and small primes in the same way as the cubic case that is by sieving

$$\#S \cap B_i(g,X) \cap \mathcal{U} = \sum_{n=1}^{\infty} \mu(n) \#S \cap B_i(g,X) \cap \cap_{p|n} \overline{\mathcal{U}_p}.$$

For big primes, we use the following lemma:

Lemma 5.2.3. *For any square free integer n, we have*

$$N(\cap_{p|n} \overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) \ll_\epsilon X/n^{2-\epsilon}.$$

Proof. Like in the cubic analog (Lemma 3.2.5), the idea is to count rings that are not maximal by counting their overrings. As mensioned in [3], by [11], the number of orders of index m in a maximal quartic order is $O\left(\prod_{p^k||m} p^{(2+\epsilon)\lfloor k/4 \rfloor}\right)$.

Unlike the cubic case we also need to count the number of cubic resolvents of each quartic ring. By [3], the number of cubic resolvents of a quartic ring of content r is $\sigma(r)$, where σ is the sum of divisors function.

For a quartic order R of content r that is not maximal at any prime dividing n, we have a chain of subrigs $R \subset R_{prim} \subset R_{max}$, where R_{prim} is the unique content 1 ring such that $R = \mathbb{Z} + rR_{prim}$, and R_{max} is the unique maximal order containing R (and R_{prim}). Let m be the index of R_{prim} in R_{max}. The condition that R is not maximal at any prime dividing n implies that for each prime p dividing n, we have $p|rm$. Since n is square free this is equivalent to $n|rm$. The last information we need here is that $Disc(R) = r^6 Disc(R_{prim}) = r^6 m^2 Disc(R_{max})$.

We are now ready to count

$$N(\cap_{p|n} \overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) \leq \sum_{r=1}^{\infty} \sigma(r) \sum_{\frac{n}{(n,r)}|m} O\left(\prod_{p^k||m} p^{(2+\epsilon)\lfloor k/4 \rfloor}\right) N\left(V_{\mathbb{Z}}^{(i)}; \frac{X}{r^6 m^2}\right) \ll_\epsilon \frac{X}{n^{2-\epsilon}}.$$

□

Thus for some big number Y to be determined later,

$$\#S \cap B_i(g,X) \cap \mathcal{U} = \sum_{n \leq Y} \mu(n) \#S \cap B_i(g,X) \cap \cap_{p|n} \overline{\mathcal{U}_p} + O_\epsilon\left(\frac{\lambda^4}{Y^{1-\epsilon}}\right),$$

We get that the main term for $N(S \cap \mathcal{U}_p \cap V_{\mathbb{Z}}^{(i)}; X)$ is just the main term for $N(S \cap V_{\mathbb{Z}}^{(i)}; X)$, that we already computed in the previous section, multiplied by $\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}})$. That is

$$MT = \left(\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}})\right) C_{\delta_2,\delta_4} X^{1-2(\delta_4-\delta_2)}.$$

We can change$\sum_{n\leq Y}\mu(n)\prod_{p|n}\mu_p(\overline{\mathcal{U}})$ to $\mu(\mathcal{U})=\prod_p\mu_p(\mathcal{U})$ in the same way as the cubic case since by [3], $\mu_p(\mathcal{U})=p^{-12}p(p^2-1)^2(p^3-1)(p^4+p^2-p-1)$, so

$$\begin{aligned}\left|\sum_{n\leq Y}\mu(n)\prod_{p|n}\mu_p(\overline{\mathcal{U}})-\mu(\mathcal{U}\right| &= \sum_{n>Y}\mu(n)\prod_{p|n}\mu_p(\overline{\mathcal{U}_p})\\ &\leq \sum_{n>Y}\prod_{p|n}\left(1-\frac{p(p^2-1)^2(p^3-1)(p^4+p^2-p-1)}{p^{12}}\right)\\ &\ll \sum_{n>Y}\prod_{p|n}\frac{1}{p^2}\\ &= \sum_{n>Y}\frac{1}{n^2}\\ &\ll \frac{1}{Y},\end{aligned}$$

which will be absorbed in the error that we already have, and thus we have

$$MT=\mu(\mathcal{U})C_{\delta_2,\delta_4}X^{1-2(\delta_4-\delta_2)}.$$

5.2.1 The error term from Theorem 5.2.2

Let us recap all the error terms that we have. We have $O(X^{11/12})$ that comes from changing the irreducible condition to $a_{11}\neq 0$, we have $O_\epsilon(X/Y^{1-\epsilon})$ that comes from big primes, and we have the error term from Theorem 5.2.2 that we call ET.

For each $d=0,...,11$, let ET_d be the error obtained by integrating over $g\in\mathcal{F}_G$ the greatest d-dimensional volume of any projection of $B_i(g,X)$ onto a coordinate subspace obtained by equating $12-d$ coordinates to zero, with the same bounds as in the previous section. Note that the $ET_d's$ are the same as in the previous section, and that since $\prod_{p|m}\mu_p(\overline{\mathcal{U}_p})=O_\epsilon\left(\frac{1}{m^{2-\epsilon}}\right)$, we have

$$ET\ll_\epsilon\sum_{d=0}^{11}Y^{2(10-d)+1+\epsilon}ET_d.$$

Using Table 5.1, we obtain Table 5.2.1.

The optimal choice for $ET+\frac{X}{Y^{1-\epsilon}}$ is $Y=X^{1/72}$, which gives

$$ET+\frac{X}{Y^{1-\epsilon}}\ll X^{71/72+\epsilon}.$$

Note this choice of Y is the one that optimized $Y^{10+\epsilon}ET_6+\frac{X}{Y^{1-\epsilon}}$. Depending on the values of the $\delta_i's$, it is not alway sharp, but it is the sharpest we can get uniformly with respect to the $\delta_i's$.

Thus we have

$$N(S\cap\mathcal{U}\cap V_{\mathbb{Z}}^{(i)};X)=\mu(\mathcal{U})C_{\delta_2,\delta_4}X^{1-2(\delta_4-\delta_2)}+O_\epsilon(X^{71/72+\epsilon}).$$

Table 5.2.1.1:

d	$Y^{2(10-d)+1+\epsilon}ET_d \ll \square$
1	$Y^{21+\epsilon}X^{1/12}$
2	$Y^{19+\epsilon}X^{3/12}$
3	$Y^{17+\epsilon}X^{4.5/12}$
4	$Y^{15+\epsilon}X^{6/12+\epsilon}$
5	$Y^{13+\epsilon}X^{8/12}$
6	$Y^{11+\epsilon}X^{10/12}$
7	$Y^{9+\epsilon}X^{10/12}$
8	$Y^{7+\epsilon}X^{10/12}$
9	$Y^{5+\epsilon}X^{10.2/12+\epsilon}$
10	$Y^{3+\epsilon}X^{10.8/12}$
11	$Y^{1+\epsilon}X^{11/12}$

Chapter 6

The quintic case using Bhargava's correspondence

In this chapter, we start by giving a background on Bhargava's correspondence between quintic rings and some homogeneous space that, just like in the cubic and quartic cases, nicely carries information about Minkowski basis. In the background (Section 6.1), We will state properties that will be used in the rest of this chapter and the next.

A few things in the chapter and the next will be very similar to the cubic (and quartic) case. We will skip the steps that are similar and invite the reader to refer to the cubic case.

For the rest of this chapter, we use the correspondence to give another construction reproving the quintic case of Theorem 0.0.7 (Section 6.2) and then reprove the bound for the quintic case of Theorem 0.0.8 (Section 6.3).

6.1 Background on Bhargava's correspondence between quintic rings and quadruples of 5×5 skew symmetric matrices

For simplicity, the background will contain a few statements of properties that we need with not much explaination. For more details on this correspondence, we refer the reader to [4] and [5].

Let $V_{\mathbb{R}}$ (resp. $V_{\mathbb{Q}}$, resp. $V_{\mathbb{Z}}$) be the set of real (resp. rational, resp. integral quadruples of 5×5 skew-symmetric matrices.

For a quadruples of 5×5 skew-symmetric matrices ν in any of these sets, we may write $\nu = (A, B, C, D)$, where $A = (a_{ij})_{1 \leq i,j \leq 3}, B = (b_{ij})_{1 \leq i,j \leq 3}, C = (c_{ij})_{1 \leq i,j \leq 3}, D = (d_{ij})_{1 \leq i,j \leq 3}$ are 5×5 skew-symmetric matrices.

Define the (left) action of $G(\mathbb{R}) := GL_4(\mathbb{R}) \times SL_5(\mathbb{R})$ on $V_{\mathbb{R}}$. For $\gamma_4 \in GL_4(\mathbb{R})$ let

$$\gamma_4 \cdot (A, B, C, D) = \gamma_4(A, B, C, D) \text{ (linear combinations of } A \text{ and } B) \ ,$$

and for $\gamma_5 \in SL_3(\mathbb{R})$ let

$$\gamma_5 \cdot (A, B, C, D) = (\gamma_5 A \gamma_5^T, \gamma_5 B \gamma_5^T, \gamma_5 C \gamma_5^T, \gamma_5 D \gamma_5^T).$$

The action of $G(\mathbb{Z})$ on $V_{\mathbb{R}}$ (or $V_{\mathbb{Z}}$) has a unique polynomial invariant, which we call the discriminant. It is a degree 40 polynomial in 40 variables.

Definition 6.1.1. *We say a quadruple (A, B, C, D) is* **degenerate** *if its discriminant $D(A, B, C, D) = 0$. Otherwise we say it is* **non degenerate**.

We have

$$Disc(\lambda \cdot \nu) = \lambda^{40} Disc(\nu).$$

We have the following theorems of Bharhava that are quintic analogues of the Delone-Faddeev correspondence:

Theorem 6.1.2. *There are maps $R(\cdot)$ and $S(\cdot)$ that make the following diagram commute:*

$$\begin{array}{ccccc}
V_{\mathbb{Z}} & \xrightarrow{R(.)} & \left\{ \begin{array}{c} ((R,\alpha),(R',\beta)): \\ R \text{ is quintic rings over } \mathbb{Z} \\ \alpha \text{ is a basis for } R \\ R' \text{ is a sextic resolvent of } R \\ \beta \text{ is a basis for } R' \end{array} \right\} & \xrightarrow{S(.)} & \left\{ \begin{array}{c} 4D \text{ free modules over } \mathbb{Z} \\ \text{and a quadratic form} \\ \text{(up to scaling)} \\ \text{with a basis} \end{array} \right\} \\
\downarrow & & \downarrow \otimes\mathbb{Q} & & \downarrow \otimes\mathbb{Q} \\
V_{\mathbb{Q}} & \xrightarrow{R(.)} & \left\{ \begin{array}{c} ((R,\alpha),(R',\beta)): \\ R \text{ is quintic rings over } \mathbb{Q} \\ \alpha \text{ is a basis for } R \\ R' \text{ is a sextic resolvent of } R \\ \beta \text{ is a basis for } R' \end{array} \right\} & \xrightarrow{S(.)} & \left\{ \begin{array}{c} 4D \text{ free modules over } \mathbb{Q} \\ \text{and a quadratic form} \\ \text{(up to scaling)} \\ \text{with a basis} \end{array} \right\} \\
\downarrow & & \downarrow \otimes\mathbb{R} & & \downarrow \otimes\mathbb{Q} \\
V_{\mathbb{R}} & \xrightarrow{R(.)} & \left\{ \begin{array}{c} ((R,\alpha),(R',\beta)): \\ R \text{ is quintic rings over } \mathbb{R} \\ \alpha \text{ is a basis for } R \\ R' \text{ is a sextic resolvent of } R \\ \beta \text{ is a basis for } R' \end{array} \right\} & \xrightarrow{S(.)} & \left\{ \begin{array}{c} 4D \text{ free modules over } \mathbb{R} \\ \text{and a quadratic form} \\ \text{(up to scaling)} \\ \text{with a basis} \end{array} \right\}
\end{array}$$

The discriminant of an element of $V_{\mathbb{Z}}$ is equal to the discriminant of the corresponding quintic ring.

Theorem 6.1.3. *There is a map*

$$\{ \text{ non degenerate elements of } V_{\mathbb{R}} \} \to \left\{ \begin{array}{c} 4D \text{ vector spaces over } \mathbb{R} \text{ with a basis} \\ \text{and a quadratic form (up to scaling)} \end{array} \right\} \simeq GL_4(\mathbb{R})/GO_4(\mathbb{R})$$

$$\nu = (A, B, C, D) \to \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix},$$

where the z_i's are 1×3 row vectors, whose restriction to $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Q}}$) gives bases for shapes of quintic rings (resp. $\mathbb{Q}$)

And similarly to the cubic and quartic case, as we are interested in Minskowski basis of quintic rings, we might look at the shapes of these rings, and we might record this in the following theorem:

Theorem 6.1.4. *For any $\nu \in V_{\mathbb{Z}}$, that maps to the quintic ring $R(\nu)$ with a basis $1, v_2, v_3, v_4, v_5$ and to the 4 dimensional lattice $S(\nu)$ with a basis w_2, w_3, w_4, w_5. Then*

1) $\frac{|v_3|}{|v_2|} \asymp \frac{|w_3|}{|w_2|}$ and $\frac{|v_4|}{|v_2|} \asymp \frac{|w_4|}{|w_2|}$ and $\frac{|v_5|}{|v_2|} \asymp \frac{|w_5|}{|w_2|}$

2) $1, v_2, v_3, v_4, v_5$ is a Minkowski basis for $R(\nu)$ if and only if w_2, w_3, w_4, w_5 is a Minkowski basis for $S(\nu)$.

This map in Theorem 6.1.3 induces a left action of $G(\mathbb{R})$ that we now describe. $GL_5(\mathbb{R})$ acts on 4 dimensional lattice with a basis given by:

$$\gamma_5 \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix} = det(\gamma_5) \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix},$$

that is elements of $SL_5(\mathbb{R})$ act trivially and

$$\lambda \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix} = \lambda^5 \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix}$$

Now the a left action of $SL_4(\mathbb{R})$ is given by matrix multiplication:

$$\gamma_4 \cdot \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix} = \gamma_4 \begin{bmatrix} z_2 \\ z_3 \\ z_4 \\ z_5 \end{bmatrix}.$$

Let us describe a convenient fundamental domain for $GL_4(\mathbb{R})/GO_4(\mathbb{R})$: let

$$\mathbb{H} = \left\{ \begin{bmatrix} 1,0,0,0 \\ z \\ w \\ t \end{bmatrix} : \begin{array}{c} z\cdot(0,0,1,0)=z\cdot(0,0,0,1)=0, z\cdot(0,1,0,0)>0, \\ w\cdot(0,0,0,1)=0, w\cdot(0,0,1,0)>0 \\ t\cdot(0,0,0,1)>0 \end{array} \right\}.$$

We might then (conveniently) look at the $G(\mathbb{R})$ equivariant map:

$$\{ \text{ non degenerate elements of } V_{\mathbb{Z}} \} \to \mathbb{H}$$

$$\nu = (A, B, C, D) \to \begin{bmatrix} 1,0,0,0 \\ z_\nu \\ w_\nu \\ t_\nu \end{bmatrix}.$$

6.1.1 Taking $G(\mathbb{Z})$ orbits

So far we have a $G(\mathbb{R})$ equivariant map $V_{\mathbb{R}} \to GL_4(\mathbb{R})/GO_4(\mathbb{R})$. It induces a map on the $G(\mathbb{Z})$ orbits:

$$G(\mathbb{Z})\backslash V_{\mathbb{R}} \to G(\mathbb{Z})\backslash GL_4(\mathbb{R})/GO_4(\mathbb{R}) = GL_4(\mathbb{Z})\backslash GL_4(\mathbb{R})/GO_4(\mathbb{R}).$$

Let

$$\mathcal{F} = \mathcal{F}_4 = \left\{ \begin{bmatrix} 1,0,0,0 \\ z \\ w \\ t \end{bmatrix} \in \mathbb{H} : \text{ the rows form a Minkowski basis for the lattice that it generates} \right\}$$

Then $\mathcal{F}$ in a fundamental domain for $G(\mathbb{Z})\backslash GL_4(\mathbb{R})/GO_4(\mathbb{R})$. For $\begin{bmatrix} 1,0,0,0 \\ z \\ w \\ t \end{bmatrix} \in \mathbb{H}$, define $\begin{bmatrix} 1,0,0,0 \\ \overline{z} \\ \overline{w} \\ \overline{t} \end{bmatrix}$ to be its image in $\mathcal{F}$.

Analogously to the cubic and quartic case, the action of $G(\mathbb{Z})$ (resp. $G(\mathbb{Q})$, resp. $G(\mathbb{Q})$) on $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{Q}}$, resp. $V_{\mathbb{R}}$) corresponds to the change of basis of the quintic rings and of their sextic resolvent, which gives the following theorem:

Theorem 6.1.5. *Taking $G(\mathbb{Z})$ orbits in the first two columns of the diagram in Theorem 2.1.1 yields the following bijections:*

$$G(\mathbb{Z})\backslash V_{\mathbb{Z}} \leftrightarrow \{(R, R') : \text{ } R \text{ is a quintic ring over } \mathbb{Z} \text{ and } R' \text{ is a sextic resolvent of } R\}/\sim$$

$$G(\mathbb{Q})\backslash V_{\mathbb{Q}} \leftrightarrow \{(R, R') : R \text{ is a quintic ring over } \mathbb{Q} \text{ and } R' \text{ is a sextic resolvent of } R\}/\sim$$

$$G(\mathbb{R})\backslash V_{\mathbb{R}} \leftrightarrow \{(R, R') : R \text{ is a quintic ring over } \mathbb{R} \text{ and } R' \text{ is a sextic resolvent of } R\}/\sim$$

Remark 6.1.6. *Up to isomorphism, there are exactly 3 quintic rings over $\mathbb{R}$ namely $\mathbb{R}^5, \mathbb{C} \times \mathbb{R}^3, \mathbb{C}^2 \times \mathbb{R}$ and they each have a unique sextic resolvent.*

We will also need a fundamental domain for $G(\mathbb{Z})\backslash G(\mathbb{R}) = GL_4(\mathbb{Z})\backslash GL_4(\mathbb{R}) \times SL_5(\mathbb{Z})\backslash SL_5(\mathbb{R})$.

Let $\mathcal{F}_4$ be the fundamental domain for $GL_4(\mathbb{Z})\backslash GL_4(\mathbb{R})$ and let $\mathcal{F}_5$ be the fundamental domain for $SL_5(\mathbb{Z})\backslash SL_5(\mathbb{R})$. They both can be described in the same way as the way we described $\mathcal{F}_3$ for the quartic case, that is elements whose image in their respective dimension version of $\mathbb{H}$ is in their respective dimension version of $\mathcal{F}$. We can also conveniently describe them similarly using their NAK decomposition.

And finally, we let $\mathcal{F}_G = \mathcal{F}_4 \times \mathcal{F}_5$ be our fundamental domain for $G(\mathbb{Z})\backslash G(\mathbb{R})$.

6.1.2 Irreduciblility

Definition 6.1.7. *We say a non degenerate integral quadruple $(A, B, C, D) \in V_{\mathbb{Z}}$ is* **irreducible** *if it corresponds to an order in a quintic field, or equivalently if it corresponds to an integral domain. Otherwise we say it is* **reducible**.

If $(A, B, C, D) \in V_{\mathbb{Z}}$, then one may consider the 4×4 sub-Pfaffians $Q_1(t_1, t_2, t_3, t_4), ..., Q_5(t_1, t_2, t_3, t_4)$ of the single 5×5 skew-symmetric matrix $At_1 + Bt_2 + Ct_3 + Dt_4$ whose entries are linear forms in t_1, t_2, t_3, t_4. In other words, $Q_i = Q_i(t_1, t_2, t_3, t_4)$ is defined as a canonical square root of the determinant of the 4×4 matrix obtained from $At_1 + Bt_2 + Ct_3 + Dt_4$ by removing its ith row and column. Thus these 4×4 Pfaffians $Q_1, ..., Q_5$ are quaternary quadratic forms and so define five quadratics in $\mathbb{P}^3$. If the element $(A, B, C, D) \in V_{\mathbb{Z}}$ has nonzero discriminant, then it is known that these five quadratics intersect in exactly five points in $\mathbb{P}^3$ (counting multiplicities). We refer to these five points as the zeroes of (A, B, C, D) in $\mathbb{P}^3$.

Theorem 6.1.8. *The field of definition of the zeroes of a quadruple is the quintic ring over $\mathbb{Q}$ corresponding to the quadruple.*

The following theorem is an obvious geometric criterion for irreducibility:

Theorem 6.1.9. *A non degenerate quadruple $(A, B, C, D) \in V_{\mathbb{Z}}$ is irreducible if and only it has a zero in $\mathbb{P}^3$ having field of definition K, where K is a quintic field.*

We now want a characterization of irreducibility in terms of how the matrices in the quadruple look like. Like explained in the quartic case, because we will apply elements of $\mathcal{F}_G$ to it, we will deal with matrices whose coefficients are "smaller" if they are closer to the top left hand corner and A is "smaller" than B, which is "smaller" than C, which is "smaller" than D. We will then be interested in characterizing irreducibility in terms of how many of these "smallest" coefficients can be zero.

First let's see how many zeroes make a pair fail to be irreducible:

Theorem 6.1.10. *Let $(A, B, C, D) \in V_{\mathbb{Z}}$ be an element such that all the variables in at least one of the following sets vanish:*

$$(i)\{a_{12}, a_{13}, a_{14}, a_{15}, a_{23}, a_{24}, a_{25}\}$$
$$(ii)\{a_{12}, a_{13}, a_{14}, a_{23}, a_{24}, a_{34}\}$$
$$(iii)\{a_{12}, a_{13}, a_{14}, a_{15}\} \cup \{b_{12}, b_{13}, b_{14}, b_{15}\}$$
$$(iv)\{a_{12}, a_{13}, a_{14}, a_{23}, a_{24}\} \cup \{b_{12}, b_{13}, b_{14}, b_{23}, b_{24}\}$$
$$(v)\{a_{12}, a_{13}, a_{14}\} \cup \{b_{12}, b_{13}, b_{14}\} \cup \{c_{12}, c_{13}, c_{14}\}$$
$$(vi)\{a_{12}, a_{13}, a_{23}\} \cup \{b_{12}, b_{13}, b_{23}\} \cup \{c_{12}, c_{13}, c_{23}\}$$
$$(vii)\{a_{12}, a_{13}\} \cup \{b_{12}, b_{13}\} \cup \{c_{12}, c_{13}\} \cup \{d_{12}, d_{13}\}$$

Then (A, B, C, D) is reducible

We now show that the "next" smaller amount of zeroes exists for some irreducible quadruples:

Theorem 6.1.11. *For any quintic number field K, there is an order R in K that can be obtained from*

a quadruple $(A, B, C, D) \in V_{\mathbb{Z}}$ *of the form*

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \neq 0 \\ 0 & 0 & 0 & \neq 0 & \cdot \\ 0 & 0 & \neq 0 & 0 & \cdot \\ 0 & \neq 0 & \cdot & \cdot & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & \neq 0 \\ 0 & 0 & 0 & \neq 0 & \cdot \\ 0 & 0 & 0 & \cdot & \cdot \\ 0 & \neq 0 & \cdot & 0 & \cdot \\ \neq 0 & \cdot & \cdot & \cdot & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 0 & \neq 0 & \cdot \\ 0 & 0 & \neq 0 & \cdot & \cdot \\ 0 & \neq 0 & 0 & \cdot & \cdot \\ \neq 0 & \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix}$$

$$D = \begin{bmatrix} 0 & 0 & \neq 0 & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot \\ \neq 0 & \cdot & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix}$$

Proof. Let K be a quintic number field. Let α be an integral primitive element of K, and let $P = [1, \alpha, \alpha^2, \alpha^3]$ be a point in $\mathbb{P}^2$ whose field of definition is K. We are looking for a non degenerate quadruple $(A, B, C, D) \in V_{\mathbb{Z}}$ that have P as a root, and we want to construct is so that the matrices have the desired form.

Let $x^5 + ax^4 + bx^3 + cx^2 + dx + e$ be the minimal polynomial of α over $\mathbb{Q}$ and let

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & e \\ 0 & 0 & 0 & e & 0 \\ 0 & 0 & -e & 0 & 0 \\ 0 & -e & 0 & 0 & 0 \end{bmatrix}, B = \begin{bmatrix} 0 & 0 & 0 & 0 & e \\ 0 & 0 & 0 & e & 0 \\ 0 & 0 & 0 & d & 0 \\ 0 & -e & -d & 0 & b \\ -e & 0 & 0 & -b & 0 \end{bmatrix},$$

$$C = \begin{bmatrix} 0 & 0 & 0 & e & 0 \\ 0 & 0 & e & 0 & 0 \\ 0 & -e & 0 & c & 0 \\ -e & 0 & -c & 0 & a \\ 0 & 0 & 0 & -a & 0 \end{bmatrix}, D = \begin{bmatrix} 0 & 0 & e & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 \\ -e & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & 1 \\ 0 & 0 & 0 & -1 & 0 \end{bmatrix}.$$

Then (A, B, C, D) is clearly of the desired form. We now show that it has P as a zero.

We compute

$$At_1 + Bt_2 + Ct_3 + Dt_4 = \begin{bmatrix} 0 & 0 & et_4 & et_3 & et_2 \\ 0 & 0 & et_3 & et_2 & et_1 \\ -et_4 & -et_3 & 0 & et_1 + dt_2 + ct_3 & 0 \\ -et_3 & -et_2 & -(et_1 + dt_2 + ct_3) & 0 & bt_2 + at_3 + t_4 \\ -et_2 & -et_1 & 0 & -(bt_2 + at_3 + t_4) & 0 \end{bmatrix}$$

so

$$\begin{aligned} Q_1 &= \left(det \begin{bmatrix} 0 & et_3 & et_2 & et_1 \\ -et_3 & 0 & et_1 + dt_2 + ct_3 & 0 \\ -et_2 & -(et_1 + dt_2 + ct_3) & 0 & bt_2 + at_3 + t_4 \\ -et_1 & 0 & -(bt_2 + at_3 + t_4) & 0 \end{bmatrix} \right)^{1/2} \\ &= et_3(bt_2 + at_3 + t_4) + et_1(et_1 + dt_2 + ct_3) \\ &= e(t_3t_4 + at_3^2 + bt_2t_3 + ct_1t_3 + dt_1t_2 + et_1^2) \end{aligned}$$

$$\begin{aligned} Q_2 &= \left(det \begin{bmatrix} 0 & et_4 & et_3 & et_2 \\ -et_4 & 0 & et_1 + dt_2 + ct_3 & 0 \\ -et_3 & -(et_1 + dt_2 + ct_3) & 0 & bt_2 + at_3 + t_4 \\ -et_2 & 0 & -(bt_2 + at_3 + t_4) & 0 \end{bmatrix} \right)^{1/2} \\ &= et_4(bt_2 + at_3 + t_4) + et_2(et_1 + dt_2 + ct_3) \\ &= e(t_4^2 + at_3t_4 + bt_2t_4 + ct_2t_3 + dt_2^2 + et_1t_2) \end{aligned}$$

$$\begin{aligned} Q_3 &= \left(det \begin{bmatrix} 0 & 0 & et_3 & et_2 \\ 0 & 0 & et_2 & et_1 \\ -et_3 & -et_2 & 0 & bt_2 + at_3 + t_4 \\ -et_2 & -et_1 & -(bt_2 + at_3 + t_4) & 0 \end{bmatrix} \right)^{1/2} \\ &= e^2(t_1t_3 - t_2^2) \end{aligned}$$

$$\begin{aligned} Q_4 &= \left(det \begin{bmatrix} 0 & 0 & et_4 & et_2 \\ 0 & 0 & et_3 & et_1 \\ -et_4 & -et_3 & 0 & 0 \\ -et_2 & -et_1 & 0 & 0 \end{bmatrix} \right)^{1/2} \\ &= e^2(t_1t_4 - t_2t_3) \end{aligned}$$

$$Q_5 = \left(det \begin{bmatrix} 0 & 0 & et_4 & et_3 \\ 0 & 0 & et_3 & et_2 \\ -et_4 & -et_3 & 0 & et_1 + dt_2 + ct_3 \\ -et_3 & -et_2 & -(et_1 + dt_2 + ct_3) & 0 \end{bmatrix} \right)^{1/2}$$
$$= e^2(t_2t_4 - t_3^2).$$

P is clearly a common root of these 5 quadratics. It is also easy to check that their common roots are exactly the 5 Galois conjugates of P and thus (A, B, C, D) is non degenerate. □

6.2 Existence - Proof of the quintic case of Theorem 0.0.7

We will first prove the following Theorem that gives a sufficient criterion for the existence of a family of orders with a given Minkowski basis.

Theorem 6.2.1. *For any quintic number field K, and $\delta_2, \delta_3, \delta_4, \delta_5 \in \mathbb{Q}$, such that there exists $a, b, c, d, x, y, z \in \mathbb{Q}$ with*

$$\delta_2 = 1/8 - x - y - z$$
$$\delta_3 = 1/8 + x$$
$$\delta_4 = 1/8 + y$$
$$\delta_5 = 1/8 + z$$

and

$$-a - b - c - d \leq a \leq b \leq c \leq d$$
$$-x - y - z \leq x \leq y \leq z$$

and

$$\begin{array}{lllll} -a & & -d + x & +y + z & \leq 1/40 \\ & -b - c & +x & +y + z & \leq 1/40 \\ a & +b + c & -x & & \leq 1/40 \\ -a & -c & -x & & \leq 1/40 \\ a & +b & +d & -y & \leq 1/40 \\ -a & -b & & -y & \leq 1/40 \\ a & +c & +d & -z & \leq 1/40 \end{array}$$

there a family of an orders in K with Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$.

We will then prove that this criterion is equivalent to the case $n = 5$ of Theorem 0.0.7. More precisely:

Theorem 6.2.2. *Let*

$$\begin{aligned} Q_1 = \{x,y,z : -x-y-z \le x \le y \le z \text{ and } & 3x+2y+2z \le 1/8, \\ & 2y+z \le 1/8 \\ & x+2z \le 1/8 \\ & z-2x \le 1/8\}, \end{aligned}$$

and let

$$\begin{aligned} Q_2 = \{x,y,z : -x-y-z \le x \le y \le z \text{ and } \exists a,b,c,d \text{ st } & -a-b-c-d \le a \le b \le c \le d \\ & -a-d+x+y+z \le 1/40 \\ & -b-c+x+y+z \le 1/40 \\ & a+b+c-x \le 1/40 \\ & -a-c-x \le 1/40 \\ & a+b+d-y \le 1/40 \\ & -a-b-y \le 1/40 \\ & a+c+d-z \le 1/40\}, \end{aligned}$$

then

$$Q_1 = Q_2.$$

These two theorems imply the following Corollary that is exactly the case $n = 5$ of Theorem 0.0.7.

Corollary 6.2.3. *For any quintic number field K, and $\delta_2, \delta_3, \delta_4, \delta_5 \in \mathbb{Q}$, such that $\delta_2 \le \delta_3 \le \delta_4 \le \delta_5$, $\delta_2+\delta_3+\delta_4+\delta_5 = 1/2$ and*

$$\begin{cases} \delta_3 \le 2\delta_2 \\ \delta_4 \le \delta_2+\delta_3 \\ \delta_5 \le \delta_2+\delta_4 \\ \delta_5 \le 2\delta_3 \end{cases} \tag{6.1}$$

there a family of an orders in K with Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$.

Proof. Q_1 is equivalent to the criterion is Theorem 0.0.7 by taking $\delta_2 = 1/8-x-y-z, \delta_3 = 1/8+x, \delta_4 = 1/8+y, \delta_5 = 1/8+z$. □

Proof of Theorem 6.2.1

By Theorem 6.1.11, for any quintic number field K, there is an order R in K that can be obtained

from a quadruple $(A, B, C, D) \in V_{\mathbb{Z}}$ of the form

$$A = \begin{bmatrix} 0 & 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 & \neq 0 \\ 0 & 0 & 0 & \neq 0 & \cdot \\ 0 & 0 & \neq 0 & 0 & \cdot \\ 0 & \neq 0 & \cdot & \cdot & 0 \end{bmatrix}$$

$$B = \begin{bmatrix} 0 & 0 & 0 & 0 & \neq 0 \\ 0 & 0 & 0 & \neq 0 & \cdot \\ 0 & 0 & 0 & \cdot & \cdot \\ 0 & \neq 0 & \cdot & 0 & \cdot \\ \neq 0 & \cdot & \cdot & \cdot & 0 \end{bmatrix}$$

$$C = \begin{bmatrix} 0 & 0 & 0 & \neq 0 & \cdot \\ 0 & 0 & \neq 0 & \cdot & \cdot \\ 0 & \neq 0 & 0 & \cdot & \cdot \\ \neq 0 & \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix}$$

$$D = \begin{bmatrix} 0 & 0 & \neq 0 & \cdot & \cdot \\ 0 & 0 & \cdot & \cdot & \cdot \\ \neq 0 & \cdot & 0 & \cdot & \cdot \\ \cdot & \cdot & \cdot & 0 & \cdot \\ \cdot & \cdot & \cdot & \cdot & 0 \end{bmatrix}.$$

By multiplying (A, B, C, D) by 2^m, for some arbitrarily large integer m, we get a family a quadruples $\nu_m = (A_m, B_m, C_m, D_m) = (2^m A, 2^m B, 2^m C, 2^m D)$ with discriminants $|Disc(\nu_m)| \asymp 2^{40m}$, with coefficients of each matrices $O(|D|^{1/40})$, and of Minkowski type $1/8, 1/8, 1/8/1/8$.

Now for x, y, z, a, b, c, d satisfying the condition of the theorem, apply the following element of $GL_4(\mathbb{Q}) \times SL_5(\mathbb{Q})$:

$$\gamma = \begin{bmatrix} 2^{40m(-x-y-z)} & & & \\ & 2^{40mx} & & \\ & & 2^{40my} & \\ & & & 2^{40mz} \end{bmatrix}, \begin{bmatrix} 2^{40m(-a-b-c-d)} & & & & \\ & 2^{40ma} & & & \\ & & 2^{40mb} & & \\ & & & 2^{40mc} & \\ & & & & 2^{40md} \end{bmatrix}$$

Note that this is indeed an element of $GL_4(\mathbb{Q}) \times SL_5(\mathbb{Q})$ for m large enough since x, y, z, a, b, c, d are rational numbers. Also the condition of the theorem implies that $\gamma \cdot (A_m, B_m, C_m, D_m)$ is integral for m large enough and gives an order in K of the Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$.

Proof of Theorem 6.2.2

Lemma 6.2.4. $Q_1 \supseteq Q_2$

Proof. If x, y, z, a, b, c, d satisfy Q_1, we have

$$\begin{bmatrix} -1 & 0 & 0 & -1 & 1 & 1 & 1 \\ 0 & -1 & -1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 0 & -1 & 0 & 0 \\ -1 & 0 & -1 & 0 & -1 & 0 & 0 \\ 1 & 1 & 0 & 1 & 0 & -1 & 0 \\ -1 & -1 & 0 & 0 & 0 & -1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & -1 \end{bmatrix} \begin{bmatrix} a \\ b \\ c \\ d \\ x \\ y \\ z \end{bmatrix} = \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \end{bmatrix},$$

some $w_i \leq 1/40$. We can then solve

$$\begin{bmatrix} a \\ b \\ c \\ d \\ x \\ y \\ z \end{bmatrix} = \frac{1}{10} \begin{bmatrix} -7 & 2 & 1 & -6 & -2 & -3 & -5 \\ 4 & -4 & -2 & 2 & 4 & -4 & 0 \\ 5 & 0 & 5 & 0 & 0 & 5 & 5 \\ 6 & 4 & 2 & 8 & 6 & 4 & 10 \\ 2 & -2 & -6 & -4 & 2 & -2 & 0 \\ 3 & 2 & 1 & 4 & -2 & -3 & 5 \\ 4 & 6 & 8 & 2 & 4 & 6 & 0 \end{bmatrix} \begin{bmatrix} w_1 \\ w_2 \\ w_3 \\ w_4 \\ w_5 \\ w_6 \\ w_7 \end{bmatrix} \tag{6.2}$$

and compute

$$\begin{aligned} 3x + 2y + 2z &= 2w_1 + w_2 + w_5 + w_7 \leq 1/8 \\ 2y + z &= w_1 + w_2 + w_3 + w_4 + w_7 \leq 1/8 \\ x + 2z &= w_1 + w_2 + w_3 + w_5 + w_6 \leq 1/8 \\ z - 2x &= w_2 + 2w_3 + w_4 + w_6 \leq 1/8, \end{aligned}$$

which gives the bounds in Q_1. □

Lemma 6.2.5. $Q_1 \subseteq Q_2$

Proof. Since they are convex, it is enough to show that the vertices of Q_1 are in Q_2. Q_1 consists in 7 inequalities with 3 variables. To get a candidate for a vertex, we pick 3 of these inequalities and solve them. We will get 35 points (with double counting). If all these points that belong to Q_1 also belong to Q_2, then the lemma is proved.

#	equation 1	equation 2	equation 3	x	y	z	$\in Q_1$?	$\in Q_2$?
1	$1/8 - 3x - 2y - 2z=0$	$1/8-2y-z=0$	$1/8 - x - 2z = 0$	$-1/40$	$1/40$	$3/40$	$True$	$True$
2	$1/8 - 3x - 2y - 2z=0$	$1/8-2y-z=0$	$1/8 + 2x - z = 0$	$-1/40$	$1/40$	$3/40$	$True$	$True$
3	$1/8 - 3x - 2y - 2z=0$	$1/8-2y-z=0$	$2x+y+z = 0$	$-1/8$	$-1/8$	$3/8$	$False$	$False$
4	$1/8 - 3x - 2y - 2z=0$	$1/8-2y-z=0$	$-x + y = 0$	$-1/8$	$-1/8$	$3/8$	$False$	$False$
5	$1/8 - 3x - 2y - 2z=0$	$1/8-2y-z=0$	$-y + z = 0$	$-1/72$	$1/24$	$1/24$	$True$	$True$
6	$1/8 - 3x - 2y - 2z=0$	$1/8 - x - 2z = 0$	$1/8 + 2x - z = 0$	$-1/40$	$1/40$	$3/40$	$True$	$True$
7	$1/8 - 3x - 2y - 2z=0$	$1/8 - x - 2z = 0$	$2x+y+z = 0$	$-1/8$	$1/8$	$1/8$	$False$	$False$
8	$1/8 - 3x - 2y - 2z=0$	$1/8 - x - 2z = 0$	$-x + y = 0$	0	0	$1/16$	$True$	$True$
9	$1/8 - 3x - 2y - 2z=0$	$1/8 - x - 2z = 0$	$-y + z = 0$	$-1/8$	$1/8$	$1/8$	$False$	$False$
10	$1/8 - 3x - 2y - 2z=0$	$1/8 + 2x - z = 0$	$2x+y+z = 0$	$-1/8$	$3/8$	$-1/8$	$False$	$False$
11	$1/8 - 3x - 2y - 2z=0$	$1/8 + 2x - z = 0$	$-x + y = 0$	$-1/72$	$-1/72$	$7/72$	$False$	$False$
12	$1/8 - 3x - 2y - 2z=0$	$1/8 + 2x - z = 0$	$-y + z = 0$	$-3/88$	$5/88$	$5/88$	$False$	$False$
13	$1/8 - 3x - 2y - 2z=0$	$2x+y+z = 0$	$-x + y = 0$	$-1/8$	$-1/8$	$3/8$	$False$	$False$
14	$1/8 - 3x - 2y - 2z=0$	$2x+y+z = 0$	$-y + z = 0$	$-1/8$	$1/8$	$1/8$	$False$	$False$
15	$1/8 - 3x - 2y - 2z=0$	$-x + y = 0$	$-y + z = 0$	$1/56$	$1/56$	$1/56$	$True$	$True$
16	$1/8 - 2y - z=0$	$1/8 - x - 2z = 0$	$1/8 + 2x - z = 0$	$-1/40$	$1/40$	$3/40$	$True$	$True$
17	$1/8 - 2y - z=0$	$1/8 - x - 2z = 0$	$2x+y+z = 0$	$-3/56$	$1/56$	$5/56$	$False$	$False$
18	$1/8 - 2y - z=0$	$1/8 - x - 2z = 0$	$-x + y = 0$	$1/24$	$1/24$	$1/24$	$False$	$False$
19	$1/8 - 2y - z=0$	$1/8 - x - 2z = 0$	$-y + z = 0$	$1/24$	$1/24$	$1/24$	$False$	$False$
20	$1/8 - 2y - z=0$	$1/8 + 2x - z = 0$	$2x+y+z = 0$	$-1/24$	$1/24$	$1/24$	$True$	$True$

21	$1/8 - 2y - z=0$	$1/8 + 2x - z = 0$	$-x + y = 0$	0	0	1/8	$False$	$False$
22	$1/8 - 2y - z=0$	$1/8 + 2x - z = 0$	$-y + z = 0$	$-1/24$	1/24	1/24	$True$	$True$
23	$1/8 - 2y - z=0$	$2x+y+z = 0$	$-x + y = 0$	$-1/8$	$-1/8$	3/8	$False$	$False$
24	$1/8 - 2y - z=0$	$2x+y+z = 0$	$-y + z = 0$	$-1/24$	1/24	1/24	$True$	$True$
25	$1/8 - 2y - z=0$	$-x + y = 0$	$-y + z = 0$	1/24	1/24	1/24	$False$	$False$
26	$1/8 - x - 2z=0$	$1/8 + 2x - z = 0$	$2x+y+z = 0$	$-1/40$	$-1/40$	3/40	$True$	$True$
27	$1/8 - x - 2z=0$	$1/8 + 2x - z = 0$	$-x + y = 0$	$-1/40$	$-1/40$	3/40	$True$	$True$
28	$1/8 - x - 2z=0$	$1/8 + 2x - z = 0$	$-y + z = 0$	$-1/40$	3/40	3/40	$False$	$False$
29	$1/8 - x - 2z=0$	$2x+y+z = 0$	$-x + y = 0$	$-1/40$	$-1/40$	3/40	$True$	$True$
30	$1/8 - x - 2z=0$	$2x+y+z = 0$	$-y + z = 0$	$-1/8$	1/8	1/8	$False$	$False$
31	$1/8 - x - 2z=0$	$-x + y = 0$	$-y + z = 0$	1/24	1/24	1/24	$False$	$False$
32	$1/8 + 2x - z=0$	$2x+y+z = 0$	$-x + y = 0$	$-1/40$	$-1/40$	3/40	$True$	$True$
33	$1/8 + 2x - z=0$	$2x+y+z = 0$	$-y + z = 0$	$-1/24$	1/24	1/24	$True$	$True$
34	$1/8 + 2x - z=0$	$-x + y = 0$	$-y + z = 0$	$-1/8$	$-1/8$	$-1/8$	$False$	$False$

□

6.3 Bounds - Proof of the quintic case of Theorem 0.0.8

We now prove our bounds that we proved sufficient in the previous section are in fact necessary.

Theorem 6.3.1. *If there is a family of orders in quintic number fields with Minkowski type* $\delta_2, \delta_3, \delta_4, \delta_5$

then there exists $a, b, c, d, x, y, z \in \mathbb{R}$ *such that*

$$\begin{aligned}\delta_2 &= 1/8 - x - y - z\\ \delta_3 &= 1/8 + x\\ \delta_4 &= 1/8 + y\\ \delta_5 &= 1/8 + z\end{aligned}$$

and

$$\begin{aligned}-a - b - c - d \leq a \leq b \leq c \leq d\\ -x - y - z \leq x \leq y \leq z\end{aligned}$$

and

$$\begin{array}{lllll}
-a & & -d+x & +y+z & \leq 1/40\\
 & -b-c & +x & +y+z & \leq 1/40\\
a & +b+c & -x & & \leq 1/40\\
-a & -c & -x & & \leq 1/40\\
a & +b & +d & -y & \leq 1/40\\
-a & -b & & -y & \leq 1/40\\
a & +c & +d & -z & \leq 1/40
\end{array}$$

The above theorem together with Theorem 6.2.2 gives the following Corollary that is exactly the case $n = 5$ of Theorem 0.0.8:

Corollary 6.3.2. *Let R be an order in a quintic number field K, with Minkowski basis $v_1 = 1, v_2, v_3, v_4, v_5$, then*

$$\begin{cases} v_3 \ll v_2^2\\ v_4 \ll v_2 v_3\\ v_5 \ll v_2 v_4\\ v_5 \ll v_3^2 \end{cases} \tag{6.3}$$

or if $|v_i| \asymp |D|^{\delta_i}$, then

$$\begin{cases} \delta_3 \leq 2\delta_2\\ \delta_4 \leq \delta_2 + \delta_3\\ \delta_5 \leq \delta_2 + \delta_4\\ \delta_5 \leq 2\delta_3 \end{cases} \tag{6.4}$$

Proof of Theorem 6.3.1

The argument is very similar to the cubic and quartic case. Since there are only a 3 non degenerate quintic rings over $\mathbb{R}$, there are only 3 non degenerate orbits for the action of $G(\mathbb{R})$ on $V_{\mathbb{R}}$. Fix represen-

tatives for these 3 orbits ν_0, ν_1, ν_2. Now let R be any order in a quintic field K with (big) discriminant D. Let $i = 0, 1, 2$ and $\gamma \in G(\mathbb{R})$ such that $R = R(\gamma \cdot \nu_i)$. Now if we pick $\gamma \in \mathcal{F}_G$, then $\gamma \cdot v_i$ will give an almost Minkowski basis for the shape of R

For the same reason as the cubic and quartic case, we may assume that γ is in the torus of $G(\mathbb{R})$, that is of the form

$$\gamma = \left(\begin{bmatrix} D^{-x-y-z} & & & \\ & D^x & & \\ & & D^y & \\ & & & D^z \end{bmatrix}, \begin{bmatrix} D^{-a-b-c-d} & & & \\ & D^a & & \\ & & D^b & \\ & & & D^c \\ & & & & D^d \end{bmatrix} \right) \lambda,$$

for $\lambda = (D/Disc(\nu_i))^{1/40}$, $-x-y-z \leq x \leq y \leq z$ and $-a-b-c-d \leq a \leq b \leq c \leq d$.

Let $(A, B, C, D) = \lambda \cdot \nu_i$. This quadruple corresponds to an order in a quintic field with the same discriminant D as R, and of Minkowski type $1/8, 1/8, 1/8, 1/8$. Also every coefficients of (A, B, C, D) are $O(|D|^{1/40})$.

Apply

$$\gamma_0 := \left(\begin{bmatrix} D^{-x-y-z} & & & \\ & D^x & & \\ & & D^y & \\ & & & D^z \end{bmatrix}, \begin{bmatrix} D^{-a-b-c-d} & & & \\ & D^a & & \\ & & D^b & \\ & & & D^c \\ & & & & D^d \end{bmatrix} \right)$$

We get a new quadruple (A', B', C', D') (that gives R).

For (A', B', C', D') to have Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$, we need

$$\begin{aligned} \delta_2 &= 1/8 - x - y - z \\ \delta_3 &= 1/8 + x \\ \delta_4 &= 1/8 + y \\ \delta_5 &= 1/8 + z, \end{aligned}$$

and since (A, B, C, D) is irreducible, by Theorem 6.1.10, we must have $a_{25}, a_{34}, b_{15}, b_{24}, c_{14}, c_{23}, d_{13} \neq 0$, and thus for (A', B', C', D') to have a chance to be integral, we need

$$\begin{array}{lllll} -a & & -d+x & +y+z & \leq 1/40 \\ & -b-c & +x & +y+z & \leq 1/40 \\ a & +b+c & -x & & \leq 1/40 \\ -a & -c & -x & & \leq 1/40 \\ a & +b & +d & -y & \leq 1/40 \\ -a & -b & & -y & \leq 1/40 \\ a & +c & +d & -z & \leq 1/40. \end{array}$$

Chapter 7

Counting quintic orders with a given form of Minkowski basis

In this chapter, we will use Bhargava's correspondence, see Section 6.1 for background, to estimate, when ordered by discriminant, the number of quintic orders with a given form of Minkowski basis.

Let $V_{\mathbb{Z}}$ (resp. $V_{\mathbb{R}}$) be the set of integral (resp. real) quadruple of 5×5 skew symmetric matrices. We know that the action of $G(\mathbb{R}) = GL_4(\mathbb{R}) \times SL_5(\mathbb{R})$ on $V_{\mathbb{R}}$ gives three orbits namely $V_{\mathbb{R}}^{(i)}$, those that correspond to quintic rings with $4-2i$ real embeddings, for $i = 0, 1, 2$. For each i, let $V_{\mathbb{Z}}^{(i)} = V_{\mathbb{Z}} \cap V_{\mathbb{R}}^{(i)}$.

In this chapter, we use the following notation for the torus of $G(\mathbb{R})$:

$$\begin{bmatrix} s_1^{-3}s_2^{-1}s_3^{-1} & & & & \\ & s_1^1 s_2^{-1} s_3^{-1} & & & \\ & & s_1^1 s_2^1 s_3^{-1} & & \\ & & & s_1^1 s_2^1 s_3^3 & \end{bmatrix}, \begin{bmatrix} s_4^{-4}s_5^{-3}s_6^{-2}s_7^{-1} & & & & \\ & s_4^1 s_5^{-3} s_6^{-2} s_7^{-1} & & & \\ & & s_4^1 s_5^2 s_6^{-2} s_7^{-1} & & \\ & & & s_4^1 s_5^2 s_6^3 s_7^{-1} & \\ & & & & s_4^1 s_5^2 s_6^3 s_7^4 \end{bmatrix},$$

which is in $\mathcal{F}_G$ if and only if $s_1, s_2, s_3, s_4, s_5, s_6, s_7 \gg 1$, where each implied constants can be made explicit but won't be interesting to us.

As usual, for a $G(\mathbb{Z})$-invariant subset S of $V_{\mathbb{Z}}^{(i)}$, let $N(S; X)$ be the number of absolutely irreducible $G(\mathbb{Z})$-orbits on S having discriminant less than X.

Now given $0 < \delta_2 < \delta_3 < \delta_4 < \delta_5$ with $\delta_2 + \delta_3 + \delta_4 + \delta_5 = 1/2$ (and as we know will end up being necessary for the count to be positive $\delta_3 \leq 2\delta_2$, $\delta_4 \leq \delta_2 + \delta_3, \delta_5 \leq \delta_2 + \delta_4, \delta_5 \leq 2\delta_3$). For $0 < c_1 < c_2, 0 < d_1 < d_2, 0 < e_1 < e_2$, define

$$\begin{aligned} S = \{\nu \in V_{\mathbb{R}} : c_1|Disc(\nu)|^{\delta_3-\delta_2} \leq \overline{z_\nu} \cdot (0,1,0,0) < c_2|Disc(\nu)|^{\delta_3-\delta_2} \\ \text{and } d_1|Disc(\nu)|^{\delta_4-\delta_2} \leq \overline{w_\nu} \cdot (0,0,1,0) < d_2|Disc(\nu)|^{\delta_4-\delta_2} \\ \text{and } e_1|Disc(\nu)|^{\delta_5-\delta_2} \leq \overline{t_\nu} \cdot (0,0,0,1) < e_2|Disc(\nu)|^{\delta_5-\delta_2}\}. \end{aligned}$$

Lemma 7.0.1. *For $\nu \in S \cap V_{\mathbb{Z}}$, $R(\nu)$ has Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$.*

Proof. Similar to the proof of Lemma 5.0.2 in the quartic case. □

Then $N(S \cap V_{\mathbb{Z}}^{(i)}; X)$ denote the number of irreducible $G(\mathbb{Z})$-orbits on $S \cap V_{\mathbb{Z}}^{(i)}$ having discriminant less than X. It is also the number of pairs (R, R'), where R is an irreducible quintic ring having a Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$, and discriminant less than X and R' is a sextic resolvent ring of R.

We as usual want the δ_i to be in the "usual range" described in Chapter 1, that is

$$\begin{cases} \delta_3 \leq 2\delta_2 \\ \delta_4 \leq \delta_2 + \delta_3 \\ \delta_5 \leq \delta_2 + \delta_4 \\ \delta_5 \leq 2\delta_3 \end{cases}$$

But we will also need this extra condition that will shortly make sense

$$(\delta_3 - \delta_2) + (\delta_4 - \delta_2) + (\delta_5 - \delta_2) \leq 1/10. \tag{7.1}$$

We will first, in Section 7.1, give the following estimate:

Theorem 7.0.2. *For each $i = 1, 2, 3$, and rational $\delta_i's$ in the usual range such that (7.1) holds, we have*

$$N(S \cap V_{\mathbb{Z}}^{(i)}; X) = CX^{1-3(\delta_5-\delta_2)-(\delta_4-\delta_3))} + O_\epsilon(X^{199/200+\epsilon}),$$

where C is a constant that depends on the $\delta_i's$ and on $c_1, c_2, d_1, d_2, e_1, e_2$ that we will not compute explicitly for simplicity.

Then, in Section 5.2, give the following estimate for the number of maximal orders in quintic fields:

Theorem 7.0.3. *For each $i = 1, 2, 3$, and rational $\delta_i's$ in the usual range such that (7.1) holds, we have*

$$N(S \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = \mu(\mathcal{U})CX^{1+(\delta_3-\delta_2)-(\delta_4-\delta_2)-3(\delta_5-\delta_2)} + O_\epsilon(X^{199/200+\epsilon}),$$

where C is the same constant as is Theorem 7.0.2, and $\mu(\mathcal{U})$ is the density of maximal elements in $V_{\mathbb{Z}}$.

7.1 An estimate for the number of quintic orders with a given form of Minkowski basis

The first step of setting up the integral that will count $N(S; X)$ is the same thing as the cubic and quartic case replacing $V_{\mathbb{R}}, V_{\mathbb{Z}}$ and the group acting on it by their quintic analogs. That is, we let $d\nu$ denote the usual Euclidean measure on $V_{\mathbb{R}}$ (normalized so that $V_{\mathbb{Z}}$ has co-volume 1) and let $dg = s_1^{-12}s_2^{-8}s_3^{-12}s_4^{-20}s_5^{-30}s_6^{-30}s_7^{-20}dud^\times sdkd^\times\lambda$ be the Haar measure of $G(\mathbb{R})$ obtained from its Iwasawa decomposition (where dk is normalized to have measure 1 on $SO_4(\mathbb{R}) \times SO_5(\mathbb{R})$). Fix a bounded $SO_4(\mathbb{R}) \times SO_5(\mathbb{R})$ invariant subset B of $V_{\mathbb{R}}$ whose elements have discriminant at least one. We have

$$N(S; X) = \frac{1}{M_i} \int_{g \in \mathcal{F}_G} \#\{x \in S^{\text{irr}} \cap gB : |Disc(x)| < X\} dg + \text{ Error }, \tag{7.2}$$

where

$$M_i = \frac{n_i}{2\pi} \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} |Disc(\nu)|^{-1} d\nu,$$

where n_i is the order of the stabilizer of ν_i in $G(\mathbb{R})$. Now by the Bhargava correspondence, the stabilizer of ν_i in $GL_2(\mathbb{R})$ is naturally isomorphic the group of ring automorphisms of $R(\nu_i)$. We then have $n_0 = Aut_{\mathbb{R}}(\mathbb{R}^5) = 120$, $n_1 = Aut_{\mathbb{R}}(\mathbb{R}^3 \times \mathbb{C}) = 12$ and $n_2 = Aut_{\mathbb{R}}(\mathbb{R} \times \mathbb{C}^2) = 8$.

The error is due to those point that appear in $\mathcal{F}_G \cdot \nu_i$ but not exactly n_i times. By Lemma 14 in [5], this error is $o(1)$ but we want a more precise error term that we will compute a bit later.

We then want to replace the condition "irreducible" by $a_{12} \neq 0$, up to some error. Note that this approache only has a chance to give us something if (7.1) holds. This is because $g \cdot \nu$ has a_{12} coordinate $\asymp s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}s_5^{-6}s_6^{-4}\lambda$, and

$$\begin{cases} s_1^4 \asymp \lambda^{40(\delta_3-\delta_2)} \\ s_1^4 s_2^2 \asymp \lambda^{40(\delta_4-\delta_2)} \\ s_1^4 s_2^2 s_3^4 \asymp \lambda^{40(\delta_5-\delta_2)} \end{cases} \implies s_1^3 s_2 s_3 \asymp \lambda^{10((\delta_3-\delta_2)+(\delta_4-\delta_2)+(\delta_5-\delta_2))}.$$

So if (7.1) does **not** hold, we have

$$\begin{cases} s_1^4 \asymp \lambda^{40(\delta_3-\delta_2)} \\ s_1^4 s_2^2 \asymp \lambda^{40(\delta_4-\delta_2)} \\ s_1^4 s_2^2 s_3^4 \asymp \lambda^{40(\delta_5-\delta_2)} \end{cases} \implies s_1^3 s_2 s_3 = \omega(\lambda) \text{ as } \lambda \to \infty,$$

which implies that the a_{12} coordinate of $g \cdot \nu$ is $o(1)$ as $\lambda \to \infty$, and therefore can only be a nonzero integer for $\lambda \ll 1$.

To replace "irreducible" by $a_{12} \neq 0$, we need analogues of Lemma 11 and 12 in [3] that we used in the quartic case, and as mensioned before, we do not quiet have a quintic analogue of Lemma 14 and thus we need to prove one. We will do this later.

For now let's just say that we have

$$N(S;X) \asymp \int_{g \in \mathcal{F}_G} \#\{x \in S \cap gB : |Disc(x)| < X \text{ and } a_{12} \neq 0\} dg + \text{ Error }, \tag{7.3}$$

for some Error that we will compute later.

We will then approximate the integrand in 7.2 using Proposition 3.0.1, like in the cubic and quartic case, that we recall:

Proposition 7.1.1. *Let $\mathcal{R}$ be a bounded, semi-algebraic multiset in $\mathbb{R}^n$ having maximum multiplicity m, and which is defined by at most k polynomial inequalities each having degree at most l. Let $\mathcal{R}'$ denote the image of $\mathcal{R}$ under any (upper or lower) triangular, unipotent transformation on $\mathbb{R}^n$. Then the number of integer lattice points (counted with multiplicity) contained in the region $\mathcal{R}'$ is*

$$Vol(\mathcal{R}) + O(\max\{Vol(\overline{\mathcal{R}}, 1)\}),$$

where $Vol(\overline{\mathcal{R}})$ denotes the greatest d-dimensional volume of any projection of $\mathcal{R}$ onto a coordinate subspace obtained by equating $n-d$ coordinates to zero, where d takes all values from 1 to $n-1$. The implies constant depends only on n, m, k and l.

Before going further with the proof, let look at the integral in (7.3) and when the integrand is non zero. Since for any $\nu \in B$, we have $|Disc(g \cdot \nu)| = \lambda^{40}|Disc(\nu)| \asymp \lambda^{40}$, and the integrand is only nonzero

when $|Disc(g\cdot\nu)|<X$, it is then only non zero for $\lambda\ll X^{1/40}$.

Also if $1,v_2,v_3,v_4,v_5$ a Minkowski basis for $R(g\cdot\nu)$, we have $\frac{v_3}{v_2}\asymp s_1^4, \frac{v_4}{v_2}\asymp s_1^4s_2^2, \frac{v_5}{v_2}\asymp s_1^4s_2^2s_3^4$, and the integrand is only nonzero when $g\cdot\nu\in S$, it is then only nonzero for $s_1^4\asymp\lambda^{40(\delta_3-\delta_2)}, s_1^4s_2^2\asymp\lambda^{40(\delta_4-\delta_2)}, s_1^4s_2^2s_3^4\asymp\lambda^{40(\delta_5-\delta_2)}$.

All the above bounds for the integrand to be non zero are also valid in (7.2), this will matter when we compute the first error term.

Finally, for the integrand in (7.3) to be non zero, we need $s_1^3s_2s_3s_4^3s_5^6s_6^4s_7^2\ll\lambda$ since otherwise we would have $a_{11}=0$.

7.1.1 Computing the main term

$$MT\asymp\int_{\substack{g\in\mathcal{F}_G\\ s_1^3s_2s_3s_4^3s_5^6s_6^4s_7^2\ll\lambda\ll X^{1/40}}} Vol(S\cap B_i(g,X))dg$$

By the change of variable $\nu'=g\cdot\nu$, we compute

$$Vol(S\cap B_i(g,X))=\lambda^{40}Vol(B\cap\{\nu\in V_{\mathbb{R}}^{(i)}:|Disc(\nu)|<X/\lambda^{12}$$

$$\text{and } c_1(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}\le\overline{g\cdot z_\nu}\cdot(0,1,0,0)<c_2(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}$$

$$\text{and } d_1(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}\le\overline{g\cdot w_\nu}\cdot(0,0,1,0)<d_2(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}$$

$$\text{and } e_1(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\le\overline{g\cdot t_\nu}\cdot(0,0,0,1)<e_2(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\})$$

Lemma 7.1.2. *For $\delta_2<\delta_3<\delta_4<\delta_5$, we may assume that for $\nu\in B$ and $g=(g_4,g_5)\in\mathcal{F}_G$ with g_4 having trivial $SO_4(\mathbb{R})$ part, we have*

$$c_1(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}\le\overline{g\cdot z_\nu}\cdot(0,1,0,0)<c_2(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

$$d_1(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}\le\overline{g\cdot w_\nu}\cdot(0,0,1,0)<d_2(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}\})$$

$$e_1(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\le\overline{g\cdot t_\nu}\cdot(0,0,0,1)<e_2(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\})$$

$$\Longleftrightarrow$$

$$c_1(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}\le g\cdot z_\nu\cdot(0,1,0,0)<c_2(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}\})$$

$$d_1(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}\le g\cdot w_\nu\cdot(0,0,1,0)<d_2(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}\})$$

$$e_1(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\le g\cdot t_\nu\cdot(0,0,0,1)<e_2(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\})$$

Proof. Very similar to quartic case. □

By the above lemma, we may assume that

$$Vol(S\cap B_i(g,X))=\lambda^{40}Vol(B\cap\{\nu\in V_{\mathbb{R}}^{(i)}:|Disc(\nu)|<X/\lambda^{40}$$

$$\text{and } c_1(\lambda^{12}|Disc(\nu)|)^{\delta_3-\delta_2}\le g\cdot z_\nu\cdot(0,1,0,0)<c_2(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}$$

$$\text{and } d_1(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}\le g\cdot w_\nu\cdot(0,0,1,0)<d_2(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}$$

$$\text{and } e_1(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2} \leq g\cdot t_\nu\cdot(0,0,0,1) < e_2(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}\})$$

and this is convenient because (if g has no $SO_4(\mathbb{R})$ part, which we may assume in the computation of this integral since B is $SO_4(\mathbb{R})\times SO_5(\mathbb{R})$ invariant),

$$(g\cdot z_\nu)\cdot(0,1,0,0) = s_1^4(z_\nu\cdot(0,1,0,0)) \text{ and } (g\cdot w_\nu)\cdot(0,0,1,0) = s_1^4s_2^2(w_\nu\cdot(0,0,1,0))$$

$$\text{and } (g\cdot t_\nu)\cdot(0,0,0,1) = s_1^4s_2^2s_3^4(t_\nu\cdot(0,0,0,1))$$

Thus, the main term is

$$\begin{aligned}
MT \asymp & \int_{g\in\mathcal{F}_G}\lambda^{40}\int_{\nu\in B\cap V_{\mathbb{R}}^{(i)}}\left(\chi_{|Disc(\nu)|<X/\lambda^{40}}\right)\left(\chi_{c_1\frac{(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}}{(z_\nu\cdot(0,1,0,0))}\leq s_1^4<c_2\frac{(\lambda^{40}|Disc(\nu)|)^{\delta_3-\delta_2}}{(z_\nu\cdot(0,1,0,0))}}\right)\\
& \left(\chi_{d_1\frac{(\lambda^{40}|Disc(\nu)|)^{\delta_4-\delta_2}}{(w_\nu\cdot(0,0,1,0))}\leq s_1^4s_2^2<d_2\frac{(\lambda^{40}Disc(\nu))^{\delta_4-\delta_2}}{(w_\nu\cdot(0,0,1,0))}}\right)\left(\chi_{e_1\frac{(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}}{(t_\nu\cdot(0,0,0,1))}\leq s_1^4s_2^2s_3^4<e_2\frac{(\lambda^{40}|Disc(\nu)|)^{\delta_5-\delta_2}}{(t_\nu\cdot(0,0,0,1))}}\right)d\nu dg\\
\asymp & \int_{0<\lambda\ll X^{1/40}}\int_{s_1\asymp\lambda^{10(\delta_3-\delta_2)}}\int_{s_2\asymp s_1^{-2}\lambda^{20(\delta_4-\delta_2)}}\int_{s_3\asymp s_1^{-1}s_2^{-1/2}\lambda^{10(\delta_5-\delta_2)}}\int_{1\ll s_4\ll(s_1^{-3}s_2^{-1}s_3^{-1}\lambda)^{1/3}}\\
& \int_{1\ll s_5\ll(s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}\lambda)^{1/6}}\int_{1\ll s_6\ll(s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}s_5^{-6}\lambda)^{1/4}}\int_{1\ll s_7\ll(s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}s_5^{-6}s_6^{-4}\lambda)^{1/2}}\\
& \lambda^{40}s_1^{-12}s_2^{-8}s_3^{-12}s_4^{-20}s_5^{-30}s_6^{-30}s_7^{-20}d^\times sd^\times\lambda
\end{aligned}$$

If we remove the bounds $s_1^3s_2s_3s_4^3s_5^6s_6^4s_7^2\ll\lambda$ in the above integral (and thus also the upper bounds on s_4,s_5,s_6,s_7), we can compute that we get the same thing up to an error of $O(X^{36/40})$, which would be absorbed in the error of $O_\epsilon(X^{199/200+\epsilon})$ that we already have. We then have

$$\begin{aligned}
MT \asymp & \int_{0<\lambda\ll X^{1/40}}\int_{s_1\asymp\lambda^{10(\delta_3-\delta_2)}}\int_{s_2\asymp s_1^{-2}\lambda^{20(\delta_4-\delta_2)}}\int_{s_3\asymp s_1^{-1}s_2^{-1/2}\lambda^{10(\delta_5-\delta_2)}}\int_{1\ll s_4}\\
& \int_{1\ll s_5}\int_{1\ll s_6}\int_{1\ll s_7}\lambda^{40}s_1^{-12}s_2^{-8}s_3^{-12}s_4^{-20}s_5^{-30}s_6^{-30}s_7^{-20}d^\times sd^\times\lambda\\
\asymp & \int_{0<\lambda\ll X^{1/40}}\int_{s_1\asymp\lambda^{10(\delta_3-\delta_2)}}\int_{s_2\asymp s_1^{-2}\lambda^{20(\delta_4-\delta_2)}}\int_{s_3\asymp s_1^{-1}s_2^{-1/2}\lambda^{10(\delta_5-\delta_2)}}\lambda^{40}s_1^{-12}s_2^{-8}s_3^{-12}d^\times s_3d^\times s_2d^\times s_1d^\times\lambda\\
\asymp & X^{1-3(\delta_5-\delta_2)-(\delta_4-\delta_3))}.
\end{aligned}$$

7.1.2 Computing the error term

There are 3 types of error term we need to compute. The first one is due to the points that appear but not exactly n_i times, the second is so we can replace "irreducible" by $a_{12}\neq 0$, and the third is from applying Proposition 3.0.1 (a.k.a Proposition 7.1.1). The first two of these error terms follow from the two following lemmas.

The following is Lemma 11 in [5]:

Lemma 7.1.3. *Let ν take a random value in B uniformly with respect to the measure $|Disc(\nu)|^{-1}d\nu$. Then the expected number of irreducible elements $(A,B,C,D)\in\mathcal{F}_G\cdot\nu$ such that $|Disc(A,B,C,D)|<X$ and $a_{12}=0$ is*

$$O(X^{39/40}).$$

The following is equation (8) in [12]:

Lemma 7.1.4. *Let $\nu \in B \cap V_{\mathbb{R}}^{(i)}$. Then the number of integral $(A,B,C,D) \in \mathcal{F}_G \cdot \nu \cap S$ such that $a_{12} \neq 0$, $|Disc(A,B,C,D)| < X$, and (A,B,C,D) does not correspond to an order in an S_5 field is*

$$O_\epsilon\left(X^{199/200+\epsilon}\right).$$

The following gives the the last error term that we have, that is the one that comes from applying Proposition 3.0.1 (a.k.a Proposition 7.1.1).

Lemma 7.1.5. *If ET_d is the error obtained by integrating over $g \in \mathcal{F}_G$ that makes $g \cdot \nu$ in S for some $\nu \in B$ and $a_{12} \neq 0$, the greatest d-dimensional volume of any projection of $B_i(g,X)$ onto a coordinate subspace obtained by equating $40-d$ coordinates to zero, then for each d, we have*

$$ET_d \ll X^{39/40}.$$

Proof. Each ET_d can be computed by integrating over $s_1^4 \asymp \lambda^{40(\delta_3-\delta_2)}, s_1^4 s_2^2 \asymp \lambda^{40(\delta_4-\delta_2)}, s_1^4 s_2^2 s_3^4 \asymp \lambda^{40(\delta_5-\delta_2)}$ (since we are counting elements in S) and $s_1^3 s_2 s_3 s_4^3 s_5^6 s_6^4 s_7^2 \ll \lambda$ (since we are counting elements with $a_{12} \neq 0$) each d dimensional projection of $B(g,X)$ onto the coordinate subspaces.

Note that similarly the quartic case, we have (because we assumes the $\delta_i' s$ saisfy (7.1))

$$s_1^4 \asymp \lambda^{40(\delta_3-\delta_2)}, s_1^4 s_2^2 \asymp \lambda^{40(\delta_4-\delta_2)}, s_1^4 s_2^2 s_3^4 \asymp \lambda^{40(\delta_5-\delta_2)} \implies s_1^3 s_2 s_3 \ll \lambda.$$

Thus the following bounds of integration, will give the sharpest possible estimate:

$$\int_{0<\lambda \ll X^{1/40}} \int_{s_1 \asymp \lambda^{10(\delta_3-\delta_2)}} \int_{s_2 \asymp s_1^{-2}\lambda^{20(\delta_4-\delta_2)}} \int_{s_3 \asymp s_1^{-1}s_2^{-1/2}\lambda^{10(\delta_5-\delta_2)}} \int_{1 \ll s_4 \ll (s_1^{-3}s_2^{-1}s_3^{-1}\lambda)^{1/3}}$$

$$\int_{1 \ll s_5 \ll (s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}\lambda)^{1/6}} \int_{1 \ll s_6 \ll (s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}s_5^{-6}\lambda)^{1/4}} \int_{1 \ll s_7 \ll (s_1^{-3}s_2^{-1}s_3^{-1}s_4^{-3}s_5^{-6}s_6^{-4}\lambda)^{1/2}}.$$

We integrate each volume of projection and keep the greatest one as the $\delta_i' s$ run over the usual range with (7.1), and record in table 7.2

Table 7.1.2.1:

d	$ET_d \ll$
1	$X^{1/40}$
2	$X^{2/40}$
3	$X^{3/40}$
4	$X^{4/40+\epsilon}$
5	$X^{8/40}$
6	$X^{12/40}$
7	$X^{16/40}$
8	$X^{20/40}$
9	$X^{24/40}$
10	$X^{28/40}$
11	$X^{28/40}$
12	$X^{28/40}$
13	$X^{28/40}$
14	$X^{28/40}$
15	$X^{28/40}$
16	$X^{28/40+\epsilon}$
17	$X^{28/40}$
18	$X^{28/40}$
19	$X^{30/40}$
20	$X^{32/40}$
21	$X^{32/40}$
22	$X^{32/40}$
23	$X^{32/40}$
24	$X^{32/40}$
25	$X^{32/40}$
26	$X^{32/40}$
27	$X^{32/40}$
28	$X^{33.3333/40+\epsilon}$
29	$X^{34.6667/40}$
30	$X^{36/40}$
31	$X^{36/40}$
32	$X^{36/40}$
33	$X^{36/40}$
34	$X^{36/40}$
35	$X^{36/40}$
36	$X^{36/40+\epsilon}$
37	$X^{37/40}$
38	$X^{38/40}$
39	$X^{39/40}$

□

7.2 An estimate for the number of maximal quintic orders with a given form of Minkowski basis

We are now interested in $N(S \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X)$, the number of absolutely irreducible and **maximal** $G(\mathbb{Z})$-orbits on $S \cap V_{\mathbb{Z}}^{(i)}$ having discriminant less than X. It is also the number of pairs (R, R'), where R is an irreducible, maximal quintic ring having Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$, and discriminant less than X and R' is a sextic resolvent ring of R. Now since maximal quintic rings have a unique sextic resolvent, it is simply the number of irreducible, maximal quintic rings having Minkowski type $\delta_2, \delta_3, \delta_4, \delta_5$, and discriminant less than X.

Just like the cubic and quartic case, we have

$$N(S \cap \cap \mathcal{U} \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{M_i} \int_{g \in \mathcal{F}_G} \#\{x \in S \cap \mathcal{U} \cap B_i(g, X) \cap a_{12} \neq 0\} dg + O_\epsilon(X^{199/200+\epsilon}),$$

where

$$B_i(g, X) = g \cdot B \cap \{\nu \in V_{\mathbb{R}}^{(i)} : |Disc(\nu)| < X\}$$

and

$$M_i = \frac{n_i}{2\pi} \int_{\nu \in B \cap V_{\mathbb{R}}^{(i)}} |Disc(\nu)|^{-1} d\nu.$$

We then need an analogue of Theorem 3.2.2:

Theorem 7.2.1. *Suppose V is a subset of $V_{\mathbb{Z}}^{(i)}$ defined by finitely many congruence conditions modulo prime powers, and $\mu_p(V)$ denotes the p-adic density of V in $V_{\mathbb{Z}}$. Let m be the smallest integer such that V is defined by congruences modulo m. The number of lattice points (A, B) in $B_i(g, X) \cap S$ is*

$$\prod_p \mu_p(V) Vol(B_i(g, X)) + Error,$$

where the error term is the greatest of each d-dimensional volume of any projection of $B_i(g, X)$ onto a coordinate subspace obtained by equating $40 - d$ coordinates to zero multiplied by $m^{40-d} \prod_p \mu_p(V)$, where d takes all values from 1 to 39

Proof. Similar to the proof of Theorem 3.2.2 (cubic analog) □

Then we separate big and small primes in the same way as the cubic and quartic case that is by sieving

$$\#S \cap B_i(g, X) \cap \mathcal{U} = \sum_{n=1}^{\infty} \mu(n) \#S \cap B_i(g, X) \cap \cap_{p|n} \overline{\mathcal{U}_p},$$

For big primes, we use the following lemma from [12]:

Lemma 7.2.2. *For any square free integer n, we have*

$$N(\cap_{p|n} \overline{\mathcal{U}_p} \cap V_Z^{(i)}; X) \ll_\epsilon X/n^{2-\epsilon}.$$

Thus for some big number Y to be determined later,

$$\#S \cap B_i(g,X) \cap \mathcal{U} = \sum_{n \leq Y} \mu(n) \#S \cap B_i(g,X) \cap \cap_{p|n} \overline{\mathcal{U}_p} + O_\epsilon\left(\frac{\lambda^4}{Y^{1-\epsilon}}\right),$$

We get that the main term for $N(S \cap \mathcal{U}_p \cap V_{\mathbb{Z}}^{(i)}; X)$ is just the main term for $N(S \cap V_{\mathbb{Z}}^{(i)}; X)$, that we already computed in the previous section, multiplied by $\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}})$. That is

$$MT = \left(\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}})\right) C_{\delta_2,\delta_4} X^{1-2(\delta_4-\delta_2)}.$$

We can change $\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}})$ to $\mu(\mathcal{U}) = \prod_p \mu_p(\mathcal{U})$ in the same way as the cubic and quartic case since by [5],

$$\mu_p(\mathcal{U}) = \frac{(p-1)^8 p^{12}(p+1)^4(p^2+1)^2(p^2+p+1)^2(p^4+p^3+p^2+p+1)(p^4+p^3+2p^2+2p+1)}{p^{40}},$$

so

$$\begin{aligned}
\left|\sum_{n \leq Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}}) - \mu(\mathcal{U}\right| &= \sum_{n > Y} \mu(n) \prod_{p|n} \mu_p(\overline{\mathcal{U}_p}) \\
&\leq \sum_{n > Y} \prod_{p|n} (1 - \mu_p(\mathcal{U})) \\
&\ll \sum_{n > Y} \prod_{p|n} \frac{1}{p^2} \\
&= \sum_{n > Y} \frac{1}{n^2} \\
&\ll \frac{1}{Y},
\end{aligned}$$

which will be absorbed in the error that we already have, and thus we have

$$MT = \mu(\mathcal{U}) C_{\delta_2,\delta_3,\delta_4,\delta_5} X^{1-2(\delta_4-\delta_2)}.$$

For the error term, we already have $O_\epsilon(X^{199/200+\epsilon})$ and we have the error term that comes from Theorem 7.2.1, that we compute in the following lemma:

Lemma 7.2.3. *If ET_d is the error obtained by integrating over $g \in \mathcal{F}_G$ that makes $g \cdot \nu$ in S for some $\nu \in B$ and $a_{12} \neq 0$, the greatest d-dimensional volume of any projection of $B_i(g,X)$ onto a coordinate subspace obtained by equating $40-d$ coordinates to zero, and some quantity E is bounded, for any Y by*

$$E \ll_\epsilon \frac{X}{Y^{1-\epsilon}} + \sum_{d=1}^{39} Y^{2(38-d)+1+\epsilon} ET_d,$$

then the optimal choice is $Y = X^{1/200}$, which gives

$$E \ll X^{199/200+\epsilon}.$$

Proof. We already computed each ET_d in the proof of Lemma 7.1.5.

Table 7.2.0.1:

d	$Y^{2(38-d)+1+\epsilon}ET_d \ll$
1	$Y^{77+\epsilon}X^{1/40}$
2	$Y^{75+\epsilon}X^{2/40}$
3	$Y^{73+\epsilon}X^{3/40}$
4	$Y^{71+\epsilon}X^{4/40+\epsilon}$
5	$Y^{69+\epsilon}X^{8/40}$
6	$Y^{67+\epsilon}X^{12/40}$
7	$Y^{65+\epsilon}X^{16/40}$
8	$Y^{63+\epsilon}X^{20/40}$
9	$Y^{61+\epsilon}X^{24/40}$
10	$Y^{59+\epsilon}X^{28/40}$
11	$Y^{57+\epsilon}X^{28/40}$
12	$Y^{55+\epsilon}X^{28/40}$
13	$Y^{53+\epsilon}X^{28/40}$
14	$Y^{51+\epsilon}X^{28/40}$
15	$Y^{49+\epsilon}X^{28/40}$
16	$Y^{47+\epsilon}X^{28/40+\epsilon}$
17	$Y^{45+\epsilon}X^{28/40}$
18	$Y^{43+\epsilon}X^{28/40}$
19	$Y^{41+\epsilon}X^{30/40}$
20	$Y^{39+\epsilon}X^{32/40}$
21	$Y^{37+\epsilon}X^{32/40}$
22	$Y^{35+\epsilon}X^{32/40}$
23	$Y^{33+\epsilon}X^{32/40}$
24	$Y^{31+\epsilon}X^{32/40}$
25	$Y^{29+\epsilon}X^{32/40}$
26	$Y^{27+\epsilon}X^{32/40}$
27	$Y^{25+\epsilon}X^{32/40}$
28	$Y^{23+\epsilon}X^{33.3333/40+\epsilon}$
29	$Y^{21+\epsilon}X^{34.6667/40}$
30	$Y^{19+\epsilon}X^{36/40}$
31	$Y^{17+\epsilon}X^{36/40}$
32	$Y^{15+\epsilon}X^{36/40}$
33	$Y^{13+\epsilon}X^{36/40}$
34	$Y^{11+\epsilon}X^{36/40}$
35	$Y^{9+\epsilon}X^{36/40}$
36	$Y^{7+\epsilon}X^{36/40+\epsilon}$
37	$Y^{5+\epsilon}X^{37/40}$
38	$Y^{3+\epsilon}X^{38/40}$
39	$Y^{1+\epsilon}X^{39/40}$

The optimal choice is $Y = X^{1/200}$, which gives

$$\frac{X}{Y^{1-\epsilon}} + \sum_{d=1}^{39} Y^{2(38-d)+1+\epsilon} ET_d \ll X^{199/200+\epsilon}.$$

Note the optimal choice is obtained by optimizing $\frac{X}{Y^{1-\epsilon}}$ with either $Y^{59+\epsilon} ET_{10}$, $Y^{39+\epsilon} ET_{20}$ or $Y^{19+\epsilon} ET_{30}$. □

Chapter 8

Explicit construction for the cubic case

In Chapter 8, we first deal with the cubic case in a more elementary way that will reprove the cubic case of Theorem 0.0.7.

Let us recall what we already know from Minkowski basis theory and from [7]. For an order R in a cubic field K. If $1, v_2, v_3$ is a Minkowski basis for R, we have

$$\begin{aligned} |v_2||v_3| &\asymp |D|^{1/2} \\ |v_2| &\ll |v_2| \\ |v_3| &\ll |D|^{1/3} \end{aligned}$$

which is equivalent to

$$\begin{aligned} |D|^{1/4} \ll |v_3| \ll |D|^{1/3} \\ |v_2| \asymp \frac{|D|^{1/2}}{|v_3|} \end{aligned}$$

We will prove that every values between these two bounds is attained for families of orders in cubic fields (in Section 8.1) and for ring of integers of cubic fields (in Section 8.2). More precisely, we take any $\delta_3 \in [1/6, 1/4]$ and we construct families or orders (and maximal orders) in cubic fields with Minkowski type $\delta, 1/2 - \delta$.

The strategy is to, in Section 8.1, define a cubic order $R = \mathbb{Z}[\alpha]$ for an algebraic integer α of degree 3 to be chosen so that a Minkowski basis for R has the desired property, which will reprove the cubic case of Theorem 0.0.7. Then we notice that what we need from α is conditions on the asymptotic size of the coefficients of its minimal polynomial, which leaves us a lot of choice.

Then in Section 8.2, we show that we can make a choice that forces these orders to be maximal, which makes then ring of integers of a cubic field.

Finally, in Section 8.3, we want to obtain something about maximal cubic rings with the full range of δ, that is any $\delta \in (1/6, 1/4]$. We will set up the integral in a similar fashion as for the previous estimate, but then use a different approach that only gives a lower bound. We will make some choices that are

a bit arbitrary and does make the lower bound a lot smaller than the estimate. The reason for these choices are to set up a sieve that is similar to the one we already computed in Chapter 8, and thus avoid more computation. This specific set up also have the advantage to make the discriminant factor in a nice way that turns out being very useful, as we saw in Chapter 8, maybe even needed to make the sieve computation doable.

We will prove the following:

Theorem 8.0.1. *For any $\delta \in (1/6, 1/4]$, let $S_\delta^{max} = \{\nu \in S_\delta : R(\nu)$ is maximal$\}$, then for each $i = 1, 2$,*

$$N((S_\delta \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}; X) \gg X^{1/2}.$$

For any $\delta \in (1/6, 1/4]$, this does prove again the existence of a family of cubic fields whose ring of integers have a Minkowski type $\delta, 1/2 - \delta$.

8.1 Explicit construction that proves the cubic case of Theorem 0.0.7

As mentioned above, in this section, we define a cubic order by letting $R = \mathbb{Z}[\alpha]$ for an algebraic integer α of degree 3 to be chosen so that a Minkowski basis for R has the desired property, which will reprove the cubic case of Theorem 0.0.7 that we recall: re

Theorem 8.1.1. *For all $\delta \in [1/6, 1/4]$, there is a family of orders in cubic fields with arbitrarily large discriminant whose Minkowski bases have their second element of length $\asymp |D|^\delta$ (and third element of length $\asymp |D|^{1/2-\delta}$).*

We will work backward, with a few steps, we derive some conditions that will lead us to α that we want. Note some of these conditions will not be necessary and then there will be other way to contruct another example of an α that works. The goal is to get sufficient conditions on the coefficients of the minimal polynomial of α and finish with its construction.

We recall that we already saw in the introduction examples where $\delta = 1/6$ and $\delta = 1/4$ is attained. So can now restrict our attention to $\delta \in (1/6, 1/4)$.

The following is a general fact about Minkowski bases theory.

Proposition 8.1.2. *Let L be a lattice with a Minkowski basis v_1, v_2. Then v_1 is the smallest non zero element of L and v_2 is the smallest element of L that is not in $< v_1 >$.*

We start by giving conditions for a cubic order R to has the property that we want. The condition is the existence of an element that we call α in $R - \mathbb{Z}$ with some properties. We will then construct $R = \mathbb{Z}[\alpha]$ and see that that same α has the properties of the proposition.

Proposition 8.1.3. *Let $\delta \in (1/6, 1/4)$, let R be a cubic order over $\mathbb{Z}$ with discriminant D and suppose there exists $\alpha \in R - \mathbb{Z}$ such that*

1) $|\alpha| \asymp |D|^\delta$

2) α is asymptotically minimal in $< 1, \alpha > -\mathbb{Z}$ in the sense that for any $x \in < 1, \alpha > -\mathbb{Z}$, we have that $|x| \gg |\alpha|$,

then for any Minkowski basis $v_1 = 1, v_2, v_3$ for R, we have that $|v_2| \asymp |\alpha| \asymp |D|^\delta$.

Proof. Follows from Proposition 8.1.2. □

We now want to define the algebraic integer α as a root of a monic irreducible polynomial ν of degree 3 with integer coefficients and we want conditions on the coefficients so that $R = \mathbb{Z}[\alpha]$ satisfies the condition of Proposition 8.1.3. We will chose ν to only have real roots, which is not a necessary condition but will simplify the construction as it is then easy to compute $|\alpha|$ in terms of the coefficients of ν.

Proposition 8.1.4. *Let $\nu(x) = x^3 + b_2x^2 + b_1x + b_0$ be a cubic irreducible monic polynomial with integer coefficients and suppose that all its roots are real and that they are not all asymptotically of the same size,*

then for any root α of ν, α is asymptotically minimal in $< 1, \alpha > -\mathbb{Z}$ (ie satisfies condition 2 of Proposition 8.1.3)

Proof. Let $\alpha_1, \alpha_2, \alpha_3$ be the roots of ν, with wlog $\alpha_1 \asymp A$, $\alpha_2 \ll A$ and $\alpha_3 = o(A)$, for some big integer A. For any root α of ν, let $K = Q(\alpha)$. K is a totally real cubic field, and thus can be embedded in $\mathbb{R}^3$. From now on, we treat α as an element of K. Wlog, we have $\alpha = (\alpha_1, \alpha_2, \alpha_3)$, and $1 = (1, 1, 1)$. Note that $|\alpha|^2 = \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \asymp \max\{\alpha_i^2\} \asymp A^2$.

Now suppose there is $x \in < 1, \alpha > -\mathbb{Z}$ with $|x| = o(|\alpha|) = o(A)$. We have $x = a\alpha + b = (a + b\alpha_1, a + b\alpha_2, a + b\alpha_3)$, for some $a, b \in \mathbb{Z}$, with $b \neq 0$, and

$$(a + b\alpha_1)^2 + (a + b\alpha_2)^2 + (a + b\alpha_3)^2 = |x|^2 = o(A^2)$$

which implies that

$$(a + b\alpha_i) = o(A) \text{ for each i.}$$

In particular $(a + b\alpha_1) = o(A)$. But since $\alpha_1 \asymp A$ and $b \neq 0$, we must have $a \asymp b\alpha_1 \asymp bA$. But then

$$(a + b\alpha_3) = a + o(bA) \asymp bA \neq o(A),$$

which is a contradiction. □

The condition that all the roots of ν are real easily translates in terms of its coefficient as its discriminant being positive. We can deal later with its irreducibility with a density argument since most polynomials are irreducible. We now want conditions on the coefficients to ensure that the roots are not all asymptotically of the same size, which, by Proposition 8.1.4, will give us a nice condition on the coefficients of ν so that its root α satisfies condition 2 of Proposition 8.1.3.

Proposition 8.1.5. *Let $\nu(x) = x^3 + b_2x^2 + b_1x + b_0$ be a polynomial with integer coefficients. All the roots are roughly of the same size A if and only if*

$$b_0 \asymp A^3 \text{ and } b_1^3 \ll b_0^2 \text{ and } b_2^3 \ll b_0$$

There are 2 bigger roots of roughly the same size A and a smaller root if and only if

$$b_1 \asymp A^2 \text{ and } b_0^2 = o(b_1^3) \text{ and } b_2^2 \ll b_1$$

there is 1 root bigger root of size A and 2 smaller if and only if

$$b_2 \asymp A \text{ and } b_0 = o(b_2^3) \text{ and } b_1 = o(b_2^2)$$

Proof. If all the roots are roughly of the same size A, then

$$b_0 \asymp A^3 \text{ and } b_1 \ll A^2 \text{ and } b_2 \ll A$$

$$\implies b_1^3 \ll b_0^2 \text{ and } b_2^3 \ll b_0$$

If there are 2 bigger roots of roughly the same size $A \gg 1$ and a smaller root of size $o(A)$, then

$$b_0 = o(A^3) \text{ and } b_1 \asymp A^2 \text{ and } b_2 \ll A$$

$$\implies b_0^2 = o(b_1^3) \text{ and } b_2^2 \ll b_1$$

If there is one root of size A and 2 roots of size $o(A)$, then

$$b_0 = o(A^3) \text{ and } b_1 = o(A^2) \text{ and } b_2 \asymp A,$$

$$\implies b_0 = o(b_2^3) \text{ and } b_1 = o(b_2^2)$$

Now to see these are sufficient conditions, note that each pair is inconsistent. □

In the following proposition, we are forcing ν to have 2 bigger roots and one smaller, which might look like an arbitrary choice as we said we only need the root to not all be roughly the same, but this is actually necessary choice here as we also would like to have $|\alpha| \asymp |D|^\delta$ so that α satisfies condition 1 of Proposition 8.1.3, which cannot happen if ν has one bigger root and 2 smaller. Indeed if the roots of ν are $\alpha_1 \asymp A$ and $\alpha_2, \alpha_3 = o(A)$, then $|D| = |(\alpha_1 - \alpha_2)^2(\alpha_1 - \alpha_3)^2(\alpha_2 - \alpha_3)^2| \asymp A^4 \asymp |\alpha|^4$.

Proposition 8.1.6. *Let $\nu(x) = x^3 + b_2x^2 + b_1x + b_0$ be an irreducible polynomial with integer coefficients, and let α be a root of ν.*

For some big (positive) integer A, suppose $b_0 = o(A^3), b_1 \asymp A^2, b_2 \ll A$, and $D = D(f) \asymp A^{1/\delta}$ (is positive).

Then $\mathbb{Z}[\alpha]$ has a Minkowski basis whose second basis element is $\asymp D^\delta$.

Proof. By Proposition 8.1.3 with $R = \mathbb{Z}[\alpha]$ since $D = D(f) = D(R)$, it is enough to show that

1) $|\alpha| \asymp D^\delta$

2) α is minimal in $< 1, \alpha > -\mathbb{Z}$

1) By Proposition 8.1.5 we are in the case 2 bigger roots $\asymp A$ and one smaller root $= o(A)$. We then have $|\alpha| \asymp A$, and since we assumed $D \asymp A^{1/\delta}$, we must have $D \asymp |\alpha|^{1/\delta}$.

2) By Proposition 8.1.5, the roots of ν are not all asymptotically of the same size, so 2) follows from Proposition 8.1.4. □

Construction

Let A be a big integer, and let $\nu(x) = x^3 + b_2x^2 + b_1x + b_0$, for some integers b_0, b_1, b_2 with $b_0 = o(A^3), b_1 \asymp A^2, b_2 \ll A$. The discriminant of ν can be expressed in terms of its coefficient by

$$D = -27b_0^2 + 18b_0b_1b_2 - 4b_0b_2^3 - 4b_1^3 + b_1^2b_2^2.$$

By Proposition 8.1.6 all we need to do is to pick such b_0, b_1, b_2 so that $D \asymp A^{1/\delta}$ and ν is irreducible. Let us leave the irreducibility condition aside for now.

Since $b_0 = o(A^3), b_1 \asymp A^2, b_2 \ll A$, note that

$$D = b_1^2(b_2^2 - 4b_1) + o(A^6)$$

It is appearant that we need $(b_2^2 - 4b_1) = o(A^4)$, otherwise, we would have $D \asymp A^6$ and we would only be able to get the case $\delta = 1/6$.

So we need $b_1 = b_2^2/4 + o(A^4)$. To make our expression for D as simple as possible, we pick $b_1 = b_2^2/4$, which gives

$$D = b_0(-27b_0 + b_2^3/2).$$

Now for any $b_2 \asymp A$ and $b_0 \asymp A^{1/\delta - 3}$, we have that $D \asymp A^{1/\delta}$. b_0 is in the right range for $\delta \in (1/6, 1/4)$. Since then $1/\delta - 3 \in (1, 3)$.

We have a lot of choice for b_0 and b_2. Finally, let us make sure that we can pick them so that ν is irreducible. Let $\gamma = 1/\delta - 3 \in (1, 3)$. We then have roughly $A^{\gamma+1}$ choices for the pair (b_0, b_2) to be in the range that we want. We claim that the number of such pairs that makes ν a reducible polynomial is $o(A^{\gamma+1})$, which implies there are still plenty of choices that makes ν irreducible.

Proposition 8.1.7. *For some integers b_0 and b_2, let $\nu(x) = x^3 + b_2x^2 + \left(\frac{b_2^2}{4}\right)x + b_0$, then*

$$\#\{b_0 \asymp A^\gamma, b_2 \asymp A : f \text{ is reducible } \} \ll A^2.$$

Proof. If ν is reducible, then there are integers a, b, c such that

$$\begin{aligned} f(x) = x^3 + b_2x^2 + \left(\frac{b_2^2}{4}\right)x + b_0 &= (x^2 + ax + b)(x + c) \\ &= x^3 + (a + c)x^2 + (ac + b)x + (bc) \end{aligned}$$

We can then count

$$\begin{aligned} \#\{b_0 \asymp A^\gamma, b_2 \asymp A : f \text{ is reducible } \} &= \#\{(a, b, c) : 4(ac + b) = (a + c)^2 \text{ and } a + c \asymp A \text{ and } bc \asymp A^\gamma\} \\ &= \#\{(a, b, c) : 4b = (a - c)^2 \text{ and } a + c \asymp A \text{ and } bc \asymp A^\gamma\} \\ &= \#\{(a, c) : a + c \asymp A \text{ and } (a - c)^2c \asymp A^\gamma\} \end{aligned}$$

Let $d = a + c$, then the above becomes

$$\#\{(c, d) : d \asymp A, (d - 2c)^2c \asymp A^\gamma\}$$

Now note that for $d \asymp A$, if $c = \omega(A)$, we would have that $(d-2c)^2 c \asymp c^3 = \omega(A^3) \not\asymp A^\gamma$, and thus

$$\#\{b_0 \asymp A^\gamma, b_2 \asymp A : f \text{ is reducible } \} = \#\{(c,d) : c \ll A \text{ and } d \asymp A\} = A^2$$

□

Summary of this section

We now know that for any $\delta \in (1/6, 1/4)$ and $\gamma = 1/\delta - 3$, for most $b_0 \asymp A^\gamma$ and $b_2 \asymp A$, the polynomial $\nu(x) = x^3 + b_2 x^2 + \left(\frac{b_2^2}{4}\right) x + b_0$ is irreducible, and for any root α of ν, $R = \mathbb{Q}[\alpha]$ is a cubic order that has a Minkowski basis whose second element has length $\asymp D^\delta$, which completes the proof of Theorem 8.1.1.

8.2 Sieve - Proof of Theorem 0.0.18

In this section, we use the construction given in the previous section and we show that a positive proportion of all the possible cubic orders that rise from our construction are actually maximal, and thus ring of integers of cubic fields. This will prove Theorem 0.0.18 that we recall:

Theorem 8.2.1. *For all $\delta \in [1/6, 1/4]$, there is a family of rings of integers in cubic number fields with arbitrarily large discriminant whose Minkowski bases have their second element of length $\asymp D^\delta$.*

We recall that we may focus on the case $\delta \in (1/6, 1/4)$ since we already know the existance of families for the end points.

From now on, we fix $\delta \in (1/6, 1/4)$ and let $\gamma = 1/\delta - 3 \in (1, 3)$. A will always be a big integer that we use as parameter for our family. We want to pick $b_0 \asymp A^\gamma$ and $b_2 \asymp A$ as in the previous such that $\nu(x) = x^3 + b_2 x^2 + \left(\frac{b_2^2}{4}\right) x + b_0$ is non only irreducible but also gives rise to a cubic order that is maximal.

A sufficient condition for a cubic order to be maximal is its discriminant being square free. In fact, we will be happy enough with the discriminant being "almost square free" in the sense that its non square free part is bounded. The discriminant of an order R in a cubic field K being almost square free forces the index of R in $\mathcal{O}_K$ to be bounded, and then a Minkowski basis for $\mathcal{O}_K$ will also have the property that we want, provided a Minkowski basis for R does. We will make this more precise shortly.

We then will show that

$$\#\{b_0 \asymp A^\gamma, b_2 \asymp A : Disc(x^3 + b_2 x^2 + \left(\frac{b_2^2}{4}\right) x + b_0) \text{ is almost square free } \} \asymp A^{\gamma+1}. \tag{8.1}$$

The following proposition is making precise the fact that (8.1) is all we need to prove Theorem 0.0.18/Theorem 8.2.1.

Proposition 8.2.2. *Let $\delta \in (1/6, 1/4)$. Suppose there exists an algebraic integer α of degree 3 such that the second element in a Minkowski basis for $R = \mathbb{Z}[\alpha]$ has length $\asymp |\alpha| \asymp D(R)^\delta$.*

Suppose further that the largest square that divides $D(R)$ is $\ll 1$ (we then say that $D(R)$ is almost square free).

Let $K = \mathbb{Q}(\alpha)$, then the second element in a Minkowski basis for $\mathcal{O}_K$ has length $\asymp |\alpha| \asymp D(\mathcal{O}_K)^\delta$.

Proof. Let v_2 and v_2' be the second element in a Minkowski basis for$R = \mathbb{Z}[\alpha]$ and $\mathcal{O}_K$, respectively. We want to show that $|v_2| \asymp |v_2'|$. Since $v_2 \in R - \mathbb{Z} \subset \mathcal{O}_K - \mathbb{Z}$, it is clear that $|v_2| \gg |v_2'|$, by Minkowski basis theory. Thus it remains to show that $|v_2| \ll |v_2'|$.

R is a sublattice of $\mathcal{O}_K$, so we have the equation

$$D(R) = (\mathcal{O}_K : R)^2 D(\mathcal{O}_K)$$

that gives us that $(\mathcal{O}_K : R)^2$ is a square dividing $D(R)$, and therefore is $\ll 1$ since $D(R)$ is almost square free.

There is then an integer $n \ll 1$ such that $nv_2' \in R - \mathbb{Z}$, so $|v_2| \ll |nv_2'| \ll |v_2'|$. □

It is then enough to prove (8.1), or equivalently, since $Disc(x^3+b_2x^2+\left(\frac{b_2^2}{4}\right)x+b_0) = b_0(-27b_0+b_2^3/2)$, that

$$\#\{b_0 \asymp A^\gamma, b_2 \asymp A : b_0(-27b_0 + b_2^3/2) \text{ is almost square free } \} \asymp A^{\gamma+1}.$$

Notation 8.2.3. *We write $n \approx X$ for $r_1X \le n < r_2X$, for some constants r_1, r_2 that are either both positive or both negative.*

Proposition 8.2.4. *Let $\gamma \in (1,3)$, let A be a big positive number, and let $Q(A) = \#\{n_1 \approx A^\gamma, n_2 \approx A : n_1(n_2^3 - n_1)$ is square free$\}$, then*

$$Q(A) = VA^{\gamma+1} + o(A^{\gamma+1}),$$

for some positive constant V.

Remark 8.2.5. *Then $Q(A) \ge 1$ for big enough A.*

Proof the Proposition 8.2.4 (for the rest of this section)

For simplicity we will assume that $n \approx X$ means $X \le n < 2X$ but the general case follows similarly.

The proof is mainly based on a few sieving arguments similar to the usual computation of the density of square free integers, namely

$$\begin{aligned}\#\{n \le x : n \text{ is square free } \} &= \sum_{d \le \sqrt{X}} \mu(d) \#\{n \le X : d^2 | n\} \\ &= \sum_{d \le \sqrt{X}} \mu(d) \left(\frac{X}{d^2} + O(1)\right).\end{aligned}$$

Note the fact that if $d^2|n$ for some $n \le X$, then $d \le \sqrt{X}$ is very important in this proof to get an error term of size $\sqrt{X}$. If we were to replace n by some polynomial of high degree, then it might be divisible by the square of a very big number, and then the error term would be too big. We will see there are ways to deal with bigger values of d but it is clear that it it a lot easier to count the square free values of a polynomial with degree as small as possible.

We are interested in the polynomial $n_1(n_2^3 - n_1)$. We will instead consider polynomials of smaller degree by "separating" n_1 and $(n_2^3 - n_1)$ since a product of two integers is square free if and only if they

are both square free and co-prime.

$$\begin{aligned} Q(A) &= \#\{n_1 \approx A^\gamma, n_2 \approx A : n_1(n_2^3 - n_1) \text{ is square free}\} \\ &= \#\{n_1 \approx A^\gamma, n_2 \approx A : (n_1, n_2) = 1, n_1 \text{ and } (n_2^3 - n_1) \text{ are square free}\}. \end{aligned}$$

We can then start sieving for square divisors of $(n_2^3 - n_1)$. Note that for $n_1 \approx A^\gamma$ and $n_2 \approx A$, we have $(n_2^3 - n_1) \asymp A^3$. So if $d^2 \mid (n_2^3 - n_1)$, we must have $d \ll A^{3/2}$.

$$Q(A) = \sum_{d \ll A^{3/2}} \mu(d) \#\{n_1 \approx A^\gamma, n_2 \approx A : (n_1, n_2) = 1, n_1 \text{ square free}, d^2 | n_2^3 - n_1\}$$

If we tried from here to simply follow the step of the usual computation of the density of square free integers, we would still get an error term that is too big, and again this is because of big values of d (even though we minimized the damage by "separating" the product n_1 and $(n_2^3 - n_1)$). We then need another way to deal with these big values.

So let us start by showing that big values of d will contribute to the error term (that is $o(A^{\gamma+1})$). For some Y to be determined later, let

$$\begin{aligned} Q_1(A) &:= \sum_{Y < d \ll A^{3/2}} \mu(d) \#\{n_1 \approx A^\gamma, n_2 \approx A : (n_1, n_2) = 1, n_1 \text{ square free}, d^2 | n_2^3 - n_1\} \\ &\leq \sum_{Y < d \ll A^{3/2}} \#\{n_1 \approx A^\gamma, n_2 \approx A : d^2 | n_2^3 - n_1\} \end{aligned}$$

When $d^2 | n_2^3 - n_1$, we have an integer D such that $(n_2^3 - n_1) = d^2 D$. Big values of d will corresponds to small values of D. It is then convenient to sum over D instead.

$$\begin{aligned} Q_1(A) &\ll \sum_{Y < d \ll A^{3/2}} \#\{n_1 \approx A^\gamma, n_2 \approx A, D \ll A^3/Y^2 : d^2 D = n_2^3 - n_1\} \\ &\ll \sum_{D \ll A^3/Y^2} \sum_{n_2 \approx A} \#\{n_1 \approx A^\gamma, d \ll A^{3/2} : d^2 D = n_2^3 - n_1\}. \end{aligned}$$

We now want a bound on the summand for each D and n_2 so we can sum over D and n_2 and get a bound on $Q_1(A)$.

Lemma 8.2.6. *For each $D \ll A^3/Y^2$ and $n_2 \approx A$,*

$$\#\{n_1 \approx A^\gamma, d \ll A^{3/2} : d^2 D = n_2^3 - n_1\} \ll 1 + A^{\gamma - 1.5}$$

This Lemma implies that

$$Q_1(A) \ll \frac{A^4}{Y^2} + \frac{A^{\gamma+2.5}}{Y^2}$$

which is $o(A^{\gamma+1})$ iff $Y = \omega(A^{(3-\gamma)/2} + A^{0.75})$. Note that since $\gamma > 1$, we have $\frac{3-\gamma}{2} < 1$, and thus $Y = A$ would do.

We then have that for $Y = A$, $Q_1(A) = o(A^{\gamma+1})$.

Proof. (of Lemma 8.2.6)

If there is one, let d be the smallest positive integer such that $d^2 D = n_2^3 - n_1$ for some $n_1 \approx A^\gamma$. We then must have that $d^2 D - n_2^3 = n_1 \asymp A^\gamma$.

Now suppose $d+a$, for some $a>0$, is another one. Then, again, we must have $(d+a)^2D - n_2^3 \asymp A^\gamma$. From this, we will find bounds on a, which will prove the lemma.

$$A^\gamma \asymp (d+a)^2D - n_2^3 = (d^2D - n_2^3) + a(2d+a)D$$

$$\implies A^\gamma \gg a(2d+a)D \gg adD$$

$$\implies a \ll \frac{A^\gamma}{dD}.$$

Aside from that, we know that

$$dD = \frac{d^2D}{d} = \frac{n_2^3 - n_1}{d} \asymp \frac{A^3}{d} \gg \frac{A^3}{A^{3/2}} = A^{1.5},$$

and thus

$$a \ll A^{\gamma-1.5}.$$

We just proved that the number of possible d that will contribute to $\#\{n_1 \approx A^\gamma, d \ll A^{3/2} : d^2D = n_2^3 - n_1\}$ is $\ll 1 + A^{\gamma-1.5}$ (we add 1 since $A^{\gamma-1.5} \to 0$ when $\gamma < 1.5$, but a bound on a is a bound for the number of other possible d assuming there is already one).

Finally note that for each d that contributes to $\#\{n_1 \approx A^\gamma, d \ll A^{3/2} : d^2D = n_2^3 - n_1\}$, that is d such that $d^2D = n_2^3 - n_1$ for some $n_1 \approx A^\gamma$, there is only one n_1 corresponding to that d, namely $n_1 = n_2^3 - d^2D$. We thus proved that

$$\#\{n_1 \approx A^\gamma, d : d^2D = n_2^3 - n_1\} \ll 1 + A^{\gamma-1.5}.$$

□

So far, we know that for $Y = A$, $Q_1(A) = o(A^{\gamma+1})$. To complete the proof of Theorem 0.0.18/Theorem 8.2.1, it remains to show that

$$\begin{aligned} Q(A) - Q_1(A) &= \sum_{d \le A} \mu(d) \#\{n_1 \approx A^\gamma, n_2 \approx A : (n_1, n_2) = 1, n_1 \text{ square free}, d^2 | n_2^3 - n_1\} \\ &= VA^{\gamma+1} + o(A^{\gamma+1}), \end{aligned}$$

for some positive constant V.

We can simplify this seeing that the condition $d^2 | n_2^3 - n_1$ only depends on the value of $n_1, n_2 \mod d^2$.

$$Q(A) - Q_1(A) = \sum_{d \le A} \mu(d) \sum_{\substack{c_1, c_2 \mod d^2 \\ c_1 \equiv c_2^3 \mod d^2}} \#\{n_1 \approx A^\gamma, n_2 \approx A : (n_1, n_2) = 1, n_1 \text{ is square free }, \\ n_1 \equiv c_1 \mod d^2, n_2 \equiv c_2 \mod d^2\}.$$

We will see it is not hard to get nice estimates for $\#\{n_1 \approx A^\gamma : n_1 \text{ is square free }, n_1 \equiv c_1 \mod d^2\}$ and for $\#\{n_2 \approx A : n_2 \equiv c_2 \mod d^2\}$ (see the following two lemmas). So if we didn't have the constraint that $(n_1, n_2) = 1$, then we would be able to write the above summand as a product of two things that we

can estimate nicely and we would be done. We will deal with the constraint $(n_1, n_2) = 1$ later by sieving again, let us forget about it for now and see how to estimate the number of $n_1's$ and $n_2's$ separately.

Lemma 8.2.7. *let q be a positive integer, and $c \in \{0, 1, ..., q-1\}$, then*

$$\#\{n \leq X : n \equiv c \mod q\} = \begin{cases} 0 & \text{if } q > X, c > X \\ 1 & \text{if } q > X, c \leq X \\ \frac{X}{q} + O(1) & \text{if } q \leq X \end{cases}$$

Proof. Obvious □

Remark 8.2.8. *The estimate $\frac{X}{q} + O(1)$ also holds for $q > X$, but it is in this case a bad estimate.*

Lemma 8.2.9. *Let d be a square free integer and $c \in \{0, 1, ..., d^2 - 1\}$.*

Let

$$R = \#\{n \leq X : n \text{ is square free }, n \equiv c \mod d^2\}.$$

Then

$$R = \begin{cases} 0 & \text{if } \left(d^2 > X \text{ and } (c > X \text{ or } c \text{ is not square free })\right) \text{ or } \left((d^2, c) \text{ is not square free }\right) \\ 1 & \text{if } d^2 > X \text{ and } c \leq X \text{ and } c \text{ square free} \\ \frac{T_d}{d^2} X + O(\sqrt{X}) & \text{otherwise (ie if } d^2 \leq X \text{ and } (d^2, c) \text{ is square free)} \end{cases}$$

where $T_d = \sum_{(e,d)=1} \frac{\mu(e)}{e^2} = \prod_{p \nmid d} \left(1 - \frac{1}{p^2}\right)^{-1} = \frac{1}{\zeta(2)} \prod_{p|d} (1 - \frac{1}{p^2})$.

Proof. The first 2 cases are trivial, so assume we are in the third case, that is $d^2 \leq X$ and (d^2, c) is square free.

We again apply the usual sieving argument for the condition "n is square free":

$$\begin{aligned} R &= \sum_{e \leq \sqrt{X}} \mu(e) \#\{n \leq X : n \equiv c \mod d^2, e^2 | n\} \\ &= \sum_{e \leq \sqrt{X}} \mu(e) \#\{m \leq X/e^2 : me^2 \equiv c \mod d^2\} \end{aligned}$$

We now estimate the above summand by considering 2 cases:

Case 1: If $(e, d) \neq 1$, then $\#\{m \leq X/e^2 : me^2 \equiv c \mod d^2\} = 0$. To see this suppose there is some m such that $me^2 \equiv c \mod d^2$, then $(e, d)^2$ is a square dividing (d^2, c), which would be a contradiction.

Case 2: If $(e, d) = 1$, then

$$me^2 \equiv c \mod d^2 \iff m \equiv e^{-2} c \mod d^2$$

and then, by Lemma 8.2.7,

$$\#\{m \leq X/e^2 : m \equiv e^{-2} c \mod d^2\} = \frac{X}{e^2 d^2} + O(1).$$

Plugging this estimate back in the sum, we get

$$\begin{aligned} R &= \sum_{\substack{e\leq\sqrt{X}\\(d,e)=1}} \mu(e)\left(\frac{X}{d^2e^2}+O(1)\right) \\ &= \frac{T_d}{d^2}X + O(\sqrt{X}). \end{aligned}$$

□

Let's go back our expression for $Q(A) - Q_1(A)$, that is

$$Q(A) - Q_1(A) = \sum_{d\leq A} \mu(d)\#\{n_1 \approx A^\gamma, n_2 \approx A : (n_1,n_2)=1, n_1 \text{ square free}, d^2|n_2^3 - n_1\}$$

We would like to use the above lemmas, for which we need to be able to count n_1 and n_2 separately, which is a problem because of the contraint $(n_1, n_2) = 1$. To fix this, sieve on the condition $(n_1, n_2) = 1$. Let

$$R_{t,d} := \#\{n_1 \approx A^\gamma, n_2 \approx A : t|(n_1,n_2), n_1 \text{ square free}, d^2|n_2^3 - n_1\}$$

so that

$$\begin{aligned} Q(A) - Q_1(A) &= \sum_{d\leq A}\mu(d)\sum_{t\leq 2A}\mu(t)R_{t,d} \\ &= \sum_{t\leq 2A}\mu(t)\sum_{d\leq A}\mu(d)R_{t,d}. \end{aligned}$$

The reason why this is looking better is because the condition $t \mid (n_1, n_2)$ is equivalent to $t \mid n_1$ and $t \mid n_2$, so we are now able to count n_1 and n_2 separately.

$$R_{t,d} = \sum_{\substack{c_1,c_2 \mod d^2\\ c_1\equiv c_2^3 \mod d^2}} \#\{n_1 \approx A^\gamma : t|n_1, n_1 \text{ is square free }, n_1 \equiv c_1 \mod d^2\}\cdot\{n_2 \approx A : t|n_2, n_2 \equiv c_2 \mod d^2\}.$$

Let

$$Q^t(A) = \sum_{d\leq A}\mu(d)R_{t,d}(A).$$

so that

$$Q(A) - Q_1(A) = \sum_{t\leq 2A}\mu(t)Q^t(A).$$

We will estimate each $Q^t(A)$ separately and hope to get error terms that we can sum over $t \leq 2A$ to get $o(A^{\gamma+1})$.

Now we use the above lemmas to estimate each $R_{t,d}$. Note that if $(d, t) \neq 1$, $t|n_2$ and $d^2|n_2^3 - n_1$, then $(d, t)^2|n_1$ and then n_1 cannot be square free. We then have $R_{t,d} = 0$ when $(d, t) \neq 1$, and thus

$$Q^t(A) = \sum_{\substack{d\leq A\\(t,d)=1}}\mu(d)R_{t,d}(A).$$

Now assume that $(t,d)=1$. We have

$$\begin{aligned}\{n_2 \approx A : t | n_2, n_2 \equiv c_2 \mod d^2\} &= \{n_2 \approx \frac{A}{t} : tn_2 \equiv c_2 \mod d^2\} \\ &= \#\{n_2 \approx \frac{A}{t} : n_2 \equiv t^{-1}c_2 \mod d^2\},\end{aligned}$$

which by Lemma 8.2.7 (and Remark 8.2.8) is

$$= \begin{cases} 0 & \text{if } d^2 > 2A/t, (t^{-1}c_2 \mod d^2) \not\approx A/t \\ 1 & \text{if } d^2 > 2A/t, (t^{-1}c_2 \mod d^2) \approx A/t \\ \frac{A}{td^2} + O(1) & \text{always} \end{cases}$$

and similarly

$$\begin{aligned}&\#\{n_1 \approx A^\gamma : t | n_1, n_1 \text{ is square free }, n_1 \equiv c_1 \mod d^2\} \\ &\leq \#\{n_1 \approx A^\gamma : t | n_1, n_1 \equiv c_1 \mod d^2\}\end{aligned}$$

which by Lemma 8.2.7 again is

$$= \begin{cases} 0 & \text{if } d^2 > 2A^\gamma/t, (t^{-1}c_1 \mod d^2) \not\approx A^\gamma/t \\ 1 & \text{if } d^2 > 2A^\gamma/t, (t^{-1}c_1 \mod d^2) \approx A^\gamma/t \\ \frac{A}{td^2} + O(1) & \text{always} \end{cases}$$

Let us first take care of the (big) values for d for which the number of $n_2's$ for each c_2 is 0 or 1 (ie for $d > \sqrt{2A/t}$). That is from the above we get

$$R_{t,d} \ll \begin{cases} \sum_{\substack{c_2 \mod d^2 \\ (t^{-1}c_2 \mod d^2) \approx A/t}} 1 & \text{if } d > \sqrt{2A^\gamma/t} \\ \sum_{\substack{c_2 \mod d^2 \\ (t^{-1}c_2 \mod d^2) \approx \frac{A}{t}}} \left(\frac{A^\gamma}{td^2} + O(1)\right) & \text{if } d > \sqrt{2A/t} \end{cases}$$

Thus if we let

$$Q_2^t(A) := \sum_{\sqrt{2A^\gamma/t} < d \leq A} \mu(d) R_{t,d}$$

and

$$Q_3^t(A) = \sum_{\sqrt{2A/t} < d \leq \sqrt{2A^\gamma/t}} \mu(d) R_{t,d}$$

then (recall that we denote by t^{-1} the inverse of t modulo d^2)

$$\begin{aligned}Q_2^t(A) &\ll \sum_{\sqrt{2A^\gamma/t} < d \leq A} \sum_{\substack{c_2 \mod d^2 \\ (t^{-1}c_2 \mod d^2) \approx A/t}} 1 \\ &\ll \frac{A^2}{t},\end{aligned}$$

which will contribute to the error term since $\sum_{t\leq 2A}\frac{A^2}{t}\ll A^2Log(A)=o(A^{\gamma+1})$. And

$$\begin{aligned}Q_3^t(A)&\ll\sum_{\sqrt{2A/t}<d\leq\sqrt{2A^\gamma/t}}\sum_{\substack{c_2 \mod d^2\\(t^{-1}c_2 \mod d^2)\approx\frac{A}{t}}}\left(\frac{A^\gamma}{td^2}+O(1)\right)\\&\ll\sum_{\sqrt{2A/t}<d\leq\sqrt{2A^\gamma/t}}\left(\frac{A^{\gamma+1}}{t^2d^2}+\frac{A}{t}\right)\\&\ll\frac{A^{\gamma+1/2}}{t^{3/2}}+\frac{A^{\gamma/2+1}}{t^{3/2}},\end{aligned}$$

which also contributes to the error term since $\sum_t\frac{1}{t^{3/2}}\ll 1$.

So far we proved that if we let

$$Q_4^t(A)=\sum_{d\ll\sqrt{A/t}}\mu(d)R_{t,d},$$

then

$$Q(A)=\sum_{t\leq 2A}Q_4^t(A)+o(A^{\gamma+1}).$$

Let's recall that

$$R_{t,d}=\sum_{\substack{c_1,c_2 \mod d^2\\c_1\equiv c_2^3 \mod d^2}}\#\{n_1\approx A^\gamma : t|n_1, n_1 \text{ is square free }, n_1\equiv c_1 \mod d^2\},$$

$$\cdot\#\{n_2\approx A : t|n_2, n_2\equiv c_2 \mod d^2\}$$

is zero when $(t,d)\neq 1$ (as explained earlier). So we will only consider $(t,d)=1$.

Also, the summand is zero when $(c_1,d)\neq 1$ (or equivalently when $(c_2,d)\neq 1$). To see this, note that when $c_1\equiv c_2^3 \mod d^2$, a divisor of (c_2,d) gives rise (by squaring) to a square divisor of (c_1,d^2), which would make impossible the existence of n_1 square free with $n_1\equiv c_1 \mod d^2$. So we will only consiter $(c_1,d)=(c_2,d)=1$.

Finally, because everything will eventually be multiplied by $\mu(d)$ and $\mu(t)$, we may only consiter d and t square free.

For $d\leq 2A/t$, we then have

$$\#\{n_2\approx A : t|n_2, n_2\equiv c_2 \mod d^2\}=\frac{A}{td^2}+O(1).$$

To estimate $\#\{n_1\approx A^\gamma : t|n_1, n_1 \text{ is square free }, n_1\equiv c_1 \mod d^2\}$ is not as easy as we need to sieve (again!) for the condition "n_1 is square free". We will need a few lemmas.

Lemma 8.2.10. *If $(t,d)=1$, t and d both square free, and $(c,d)=1$ then*

$$\#\{n\approx X : t|n, n \text{ is square free }, n\equiv c \mod d^2\}=\frac{T_dW_t}{d^2}X+O\left(\tau(t)\sqrt{\frac{X}{t}}\right),$$

where $T_d=\sum_{(e,d)=1}\frac{\mu(e)}{e^2}=\prod_{p|d}\left(1-\frac{1}{p^2}\right)^{-1}=\frac{1}{\zeta(2)}\prod_{p|d}(1-\frac{1}{p^2})$. (like in Lemma 8.2.9), and where W_t

is defined inductively by $W_1 = 1$ *and for* $t > 11$, $W_t = \frac{1}{t-\mu(t)} \sum_{\substack{e|t \\ e\neq t}} \mu(e) W_e$.

Proof. Note that the right hand side does not depend on c so we may abuse notation a little bit and let

$$Z_t(X) = \#\{n \approx X : t|n, n \text{ is square free }, n \equiv c \mod d^2\}$$

"ignoring" the dependence in c. The reason why this matters is we will give an induction argument where the induction hypothesis will involve different values for c.

We use induction on the number of prime divisors of t. The case $t = 1$ is just Lemma 8.2.9, it gives

$$Z_1(X) = \frac{T_d}{d^2} X + O\left(\sqrt{\frac{X}{t}}\right),$$

which is what we want since $W_1 = 1$ and $\tau(1) = 1$.

Now let $t \neq 1$ and suppose the lemma holds when t has less prime divisors.

$$\begin{aligned} Z_t(X) &= \#\{n \approx X : t|n, n \text{ is square free }, n \equiv c \mod d^2\} \\ &= \#\{n \approx \frac{X}{t} : n \text{ is square free }, (t,n) = 1, n \equiv t^{-1}c \mod d^2\} \end{aligned}$$

Now sieve to get rid of the condition $(t, n) = 1$, we sieve the above expression and get

$$\begin{aligned} Z_t(X) &= \sum_{e|t} \mu(e) \#\{n \approx \frac{X}{t} : n \text{ is square free }, e|n, n \equiv t^{-1}c \mod d^2\} \\ &= \sum_{e|t} \mu(e) Z_e\left(\frac{X}{t}\right) \\ &= \sum_{\substack{e|t \\ e\neq t}} \mu(e) Z_e\left(\frac{X}{t}\right) + \mu(t) Z_t\left(\frac{X}{t}\right). \end{aligned}$$

Now we can apply the same process to $Z_t\left(\frac{X}{t}\right)$ in the above expression et get

$$\begin{aligned} Z_t(X) &= \sum_{\substack{e|t \\ e\neq t}} \mu(e) Z_e\left(\frac{X}{t}\right) + \mu(t) \sum_{e|t} \mu(e) Z_e\left(\frac{X}{t^2}\right) \\ &= \sum_{\substack{e|t \\ e\neq t}} \mu(e) Z_e\left(\frac{X}{t}\right) + \mu(t) \sum_{\substack{e|t \\ e\neq t}} \mu(e) Z_e\left(\frac{X}{t^2}\right) + \mu(t)^2 \sum_{e|t} \mu(e) Z_e\left(\frac{X}{t^3}\right) \end{aligned}$$

We can keep doing this and since $Z_t\left(\frac{X}{t^i}\right) = 0$ for i big enough, we end up with

$$Z_t(X) = \sum_{i=1}^{\infty} \mu(t)^{i+1} \sum_{\substack{e|t \\ e\neq t}} \mu(e) Z_e\left(\frac{X}{t^i}\right),$$

that is a finite sum.

Now by induction,

$$\begin{aligned}
Z_t(X) &= \sum_{i=1}^{\infty} \mu(t)^{i+1} \sum_{\substack{e|t \\ e\neq t}} \mu(e) \left(\frac{T_d W_e}{d^2} \frac{X}{t^i} + O\left(\tau(e) \sqrt{\frac{X}{et^i}} \right) \right) \\
&= X \frac{T_d}{d^2} \sum_{\substack{e|t \\ e\neq t}} \mu(e) W_e \sum_{i=1}^{\infty} \frac{\mu(t)^{i+1}}{t^i} + O\left(\sqrt{X} \sum_{\substack{e|t \\ e\neq t}} \frac{\tau(e)}{\sqrt{e}} \sum_{i=1}^{\infty} \frac{1}{(\sqrt{t})^i} \right) \\
&= X \frac{T_d}{d^2} \frac{1}{t-\mu(t)} \sum_{\substack{e|t \\ e\neq t}} \mu(e) W_e + O\left(\frac{\sqrt{X}}{\sqrt{t}-1} \sum_{\substack{e|t \\ e\neq t}} \frac{\tau(e)}{\sqrt{e}} \right) \\
&= \frac{T_d W_t}{d^2} X + O\left(\sqrt{\frac{X}{t}} \sum_{\substack{e|t \\ e\neq t}} \frac{\tau(e)}{\sqrt{e}} \right),
\end{aligned}$$

and the result follows since $\tau(e) \ll \sqrt{e}$. □

Lemma 8.2.11. *For all square free integer t,*

$$W_t = \prod_{p|t} \frac{1}{p+1}$$

Proof. Let's recall that W_t is defined inductively by $W_1 = 1$ and for $t > 1$, $W_t = \frac{1}{t-\mu(t)} \sum_{\substack{e|t \\ e\neq t}} \mu(e) W_e$.

We first show that W_t is a multiplicative function of t. Let $(a, b) = 1$, then

$$\begin{aligned}
(ab - \mu(ab)) W_{ab} &= \sum_{\substack{e|ab \\ e\neq ab}} \mu(e) W_e \\
&= \left(\sum_{\substack{e|a \\ e\neq a}} \mu(e) W_e \right) \left(\sum_{\substack{e|b \\ e\neq b}} \mu(e) W_e \right) + \mu(a) W_a \left(\sum_{\substack{e|b \\ e\neq b}} \mu(e) W_e \right) \\
&\qquad + \mu(b) W_b \left(\sum_{\substack{e|a \\ e\neq a}} \mu(e) W_e \right) \\
&= W_a W_b \big((a - \mu(a))(b - \mu(b)) + \mu(a)(b - \mu(b)) + \mu(b)(a - \mu(a)) \big) \\
&= W_a W_b (ab - \mu(ab)).
\end{aligned}$$

W_t is then multiplicative and t is square free, so

$$W_t = \prod_{p|t} W_p = \prod_{p|t} \frac{1}{p+1}.$$

□

Using these lemmas, we have that when $(d,t)=1$, d and t are both square free and $(c,d)=1$,

$$\#\{n_1 \approx A^\gamma : t|n_1, n_1 \text{ is square free }, n_1 \equiv c_1 \mod d^2\} = \frac{T_d W_t}{d^2} A^\gamma + O\left(\tau(t)\sqrt{\frac{A^\gamma}{t}}\right).$$

This result, together with the estimate that we already had

$$\#\{n_2 \approx A : t|n_2, n_2 \equiv c_2 \mod d^2\} = \frac{A}{td^2} + O(1).$$

gives

$$R_{t,d} = \sum_{\substack{c_1,c_2 \mod d^2 \\ c_1 \equiv c_2^3 \mod d^2 \\ (c_i,d)=1}} \left(\frac{T_d W_t}{d^2} A^\gamma + O\left(\tau(t)\sqrt{\frac{A^\gamma}{t}}\right)\right)\left(\frac{A}{td^2} + O(1)\right).$$

The summand does not depend on c_1 and c_2, and

$$\sum_{\substack{c_1,c_2 \mod d^2 \\ c_1 \equiv c_2^3 \mod d^2 \\ (c_i,d)=1}} 1 = \phi(d^2) = d\phi(d).$$

Thus

$$\begin{aligned} R_{t,d} &= d\phi(d)\left(\frac{T_d W_t}{d^2} A^\gamma + O\left(\tau(t)\sqrt{\frac{A^\gamma}{t}}\right)\right)\left(\frac{A}{td^2} + O(1)\right) \\ &= \frac{\phi(d)}{d^3} T_d \frac{W_t}{t} A^{\gamma+1} + O(T_d W_t A^\gamma) + O\left(\frac{\tau(t)}{t\sqrt{t}} A^{1+\gamma/2}\right) + O\left(d^2 \frac{\tau(t)}{\sqrt{t}} A^{\gamma/2}\right) \end{aligned}$$

Now note that $T_d \ll 1$ and $W_t \leq 1/t$, so

$$R_{t,d} = \frac{\phi(d)}{d^3} T_d \frac{W_t}{t} A^{\gamma+1} + O\left(\frac{A^\gamma}{t}\right) + O\left(\frac{\tau(t)}{t\sqrt{t}} A^{1+\gamma/2}\right) + O\left(d^2 \frac{\tau(t)}{\sqrt{t}} A^{\gamma/2}\right),$$

and therefore

$$\begin{aligned} Q_4^t(A) &= \sum_{d \ll \sqrt{A/t}} \mu(d) R_{t,d} \\ &= \sum_{d \ll \sqrt{A/t}} \mu(d) \frac{\phi(d)}{d^3} T_d \frac{W_t}{t} A^{\gamma+1} + O\left(\frac{A^{\gamma+1/2}}{t^{3/2}}\right) + O\left(\frac{\tau(t)}{t^2} A^{\frac{\gamma+3}{2}}\right). \end{aligned}$$

Let us simplify the main term to a sum over every integers d,

$$\begin{aligned}\sum_{d\ll\sqrt{A/t}}\mu(d)\frac{\phi(d)}{d^3}T_d\frac{W_t}{t}A^{\gamma+1} &= \sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\frac{W_t}{t}A^{\gamma+1} + O\left(\sum_{d\gg\sqrt{A/t}}\frac{\phi(d)}{d^3}T_d\frac{W_t}{t}A^{\gamma+1}\right)\\ &= \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\frac{W_t}{t}A^{\gamma+1} + O\left(\sum_{d\gg\sqrt{A/t}}\frac{1}{d^2t^2}A^{\gamma+1}\right)\\ &= \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\frac{W_t}{t}A^{\gamma+1} + O\left(\frac{A^{\gamma+1/2}}{t^{3/2}}\right)\end{aligned}$$

so

$$Q_4^t(A) = \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\frac{W_t}{t}A^{\gamma+1} + O\left(\frac{A^{\gamma+1/2}}{t^{3/2}}\right) + O\left(\frac{\tau(t)}{t^2}A^{\frac{\gamma+3}{2}}\right),$$

and then

$$\begin{aligned}Q(A) &= \sum_{t\le 2A}\mu(t)Q_4^t(A) + o(A^{\gamma+1})\\ &= \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\left(\sum_{t\le 2A}\mu(t)\frac{W_t}{t}\right)A^{\gamma+1} + O(A^{\gamma+1/2}) + O\left(A^{\frac{\gamma+3}{2}}\right) + o(A^{\gamma+1})\\ &= \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\left(\sum_t \mu(t)\frac{W_t}{t} + O\left(\sum_{t\gg A}\frac{W_t}{t}\right)\right)A^{\gamma+1} + o(A^{\gamma+1})\\ &= \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\left(\sum_t \mu(t)\frac{W_t}{t}\right)A^{\gamma+1} + O\left(\sum_{t\gg A}\frac{A^{\gamma+1}}{t^2}\right) + o(A^{\gamma+1})\\ &= \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\left(\sum_t \mu(t)\frac{W_t}{t}\right)A^{\gamma+1} + o(A^{\gamma+1})\end{aligned}$$

So we have that

$$Q(A) = VA^{\gamma+1} + o(A^{\gamma+1}),$$

for some V. It remains to check that $V > 0$, where

$$V = \left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right)\left(\sum_t \mu(t)\frac{W_t}{t}\right).$$

$\mu(d)\frac{\phi(d)}{d^3}T_d$ is a multiplicative function of d, so

$$\left(\sum_d \mu(d)\frac{\phi(d)}{d^3}T_d\right) = \prod_p\left(1-\mu(p)\frac{\phi(p)}{p^3}T_p\right)^{-1} = \prod_p\left(1-\frac{p-1}{p^3}\frac{1}{\zeta(2)}\left(1-\frac{1}{p^2}\right)\right)^{-1} > 0,$$

since $\sum_p \frac{p-1}{p^3}\frac{1}{\zeta(2)}\left(1-\frac{1}{p^2}\right)$ converges, and similarty $\mu(t)\frac{W_t}{t}$ is a multiplicative function of t, so

$$\left(\sum_t \mu(t)\frac{W_t}{t}\right) = \prod_p\left(1-\mu(p)\frac{W_p}{p}\right)^{-1} = \prod_p\left(1-\frac{1}{p(p+1)}\right)^{-1} > 0,$$

since $\sum_p \frac{1}{p(p+1)}$ converges. We then have

$$V > 0.$$

8.3 A lower bound for the number of maximal cubic orders with a given form of Minkowski basis

In this section, we want to obtain a lower bound for the number maximal cubic rings with the full range of δ, that is any $\delta \in (1/6, 1/4]$. We will set up the integral in a similar fashion as for the previous sections, but then instead of using the geometry of number to estimate the number of lattice points in a ball, we use a different approach to get lower bound for this number constructing a few of these lattice points, as we did in Chapter 8, and then use the sieve that we already computed in Section 8.2.

Let us recall the theorem that we will prove here:

Theorem 8.3.1. *For any $\delta \in (1/6, 1/4] \cap \mathbb{Q}$, and for each $i = 1, 2$, we have*

$$N(S_\delta \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}; X) \gg X^{1/2}.$$

Proof of Theorem 8.3.1

Before using (3.1) again, we would like to replace $\mathcal{U}$ by $\mathcal{U}'$ that we define

$$\mathcal{U}' = \{\nu \in V_{\mathbb{Z}} : Disc(\nu) \text{ is almost square free}\},$$

where almost square free means that the largest square dividing it is bounded by an absolute constant that in this case can be $2^4 3^4 = 1296$.

Lemma 8.3.2. *There exists c_1' and c_2' such that if $S_\delta' = \{\nu \in V_{\mathbb{R}} : c_1' |Disc(\nu)|^{1/2-2\delta} \leq Im(\overline{z_\nu}) < c_2' |Disc(\nu)|^{1/2-2\delta}\}$, we have*

$$N(S_\delta \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}; X) \gg N(S_\delta' \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}'; X).$$

Proof. If ν' contributes to $N(S_\delta' \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}'; X)$, then $\nu \in V_{\mathbb{Z}}^{(i)} \cap V_{\mathbb{R}}^{irr}$, has discriminant almost square free and at most X, and has a Minkowski basis $1, v_2', v_3'$ with $|v_2| \asymp Disc(\nu')^\delta$, where what we mean by '$\asymp$' is that $\frac{|v_2'|}{Disc(\nu')^\delta}$ is in an interval that we can control by the choice of c_1' and c_2'.

Now $R(\nu')$ is an order in a cubic number field K. Let ν be an element of $V_{\mathbb{Z}}$ such that $R(\nu) = \mathcal{O}_K$ and note that the choice for ν is unique modulo $GL_2(\mathbb{Z})$. We claim that ν contributes to $N(S_\delta \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}; X)$, which will prove the lemma.

We already saw a similar argument is Chapter 8, that the second element in a Minkowski basis for $R(\nu)$ will also be $\asymp Disc(\nu')^\delta$ and thus by making c_1' and c_2' closer to each other if necessary, we may assume that $\nu \in S_\delta$, amd thus ν contributes to $N(S_\delta \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}; X)$.

To actually prove this, let $1, v_2, v_3$ be a Minkowski basis for $R(\nu) = \mathcal{O}_K$. Since $R(\nu')$ is a sublattice of $R(\nu) = \mathcal{O}_K$, it is clear that $|v_2| \leq |v_2'|$ and we have the equation

$$Disc(\nu') = (\mathcal{O}_K : R(\nu'))^2 Disc(\nu),$$

and thus $(\mathcal{O}_K : R(\nu'))^2$ is a square dividing $Disc(\nu')$, and therefore $(\mathcal{O}_K : R) \ll 1$ since $Disc(\nu')$ is almost square free. There is then an integer $n \ll 1$ such that $nv_2 \in R(\nu') - \mathbb{Z}$, so $|v_2'| \ll |nv_2| \ll |v_2|$, and thus $|v_2| \asymp |v_2'| \asymp Disc(\nu')^\delta$, as needed. □

To prove Theorem 8.3.1, it is then enough to show that

$$N(S_\delta' \cap V_{\mathbb{Z}}^{(i)} \cap \mathcal{U}'; X) \gg X^{1/2}.$$

Now as usuaul we use (3.1) to get

$$N(S_\delta' \cap \mathcal{U}' \cap V_{\mathbb{Z}}^{(i)}; X) = \frac{1}{M_i} \int_{g=u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda \in N'(t)A'\Lambda} \#\{x \in S_\delta' \cap \mathcal{U}' \cap B_i(u,t,\lambda,X) \cap V_{\mathbb{Z}}^{irr}\} t^{-2} du d^\times t d^\times \lambda dk,$$

where we might fix right now the "radius" of our ball $B = B(C)$ to be $C = 6\sqrt{8}$.

The first step is to restrict the range of t to one that ensures that any element of $B_i(u,t,\lambda,X)$ is automatically in S_δ', and to restrict the range of λ to one that ensures that any element of $u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \cap V_{\mathbb{R}}^{(i)}$ have discriminant less than X and thus is in $B_i(u,t,\lambda,X)$. This gives the following lower bound:

$$N(S_\delta' \cap \mathcal{U}' \cap V_{\mathbb{Z}}^{(i)}; X) \gg \int_{\lambda \asymp X^{1/4}} \int_{t \asymp \lambda^{1-4\delta}} \int_{N"(t)} \#\{x \in \mathcal{U}' \cap u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \cap V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}^{irr}\} t^{-2} dn d^\times t dk d^\times \lambda. \tag{8.2}$$

The next step is to find a lower bound for the above integrand, that is $P(u,t,\lambda) := \#\{x \in \mathcal{U}' \cap u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \cap V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}^{irr}\}$, for each n, t, λ in the ranges of the integral. To do this, we start by giving a sufficient conditions on the coefficients of elements of $V_{\mathbb{Z}}$ for it to be in $u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B$ that makes them easier to count:

Lemma 8.3.3.

$$u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \supset \{(a,b,c,d) \in V_{\mathbb{R}} : |a| \le 2\frac{\lambda}{t^3}, |b| \le 2\frac{\lambda}{t}, |c| \le 2\lambda t, |d| \le 2\lambda t^3, |Disc(a,b,c,d)| \ge \lambda^4\}.$$

Proof. Note that

$$B = \{(a,b,c,d) \in V_{\mathbb{R}} : 3a^2 + b^2 + c^2 + 3d^2 \le C^2, |Disc(a,b,c,d)| \ge 1\}$$

$$\supset \{(a,b,c,d) \in V_{\mathbb{R}} : |a|, |b|, |c|, |d| \le C/\sqrt{8} = 3, |Disc(a,b,c,d)| \ge 1\}$$

so that since $C = 6\sqrt{8}$, we have

$$\begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \supset \{(a,b,c,d) \in V_{\mathbb{R}} : |a| \le 6\frac{\lambda}{t^3}, |b| \le 6\frac{\lambda}{t}, |c| \le 6\lambda t, |d| \le 6\lambda t^3, |Disc(a,b,c,d)| \ge \lambda^4\}.$$

Now we recall that

$$u \cdot (a,b,c,d) = (a, 3au+b, 3au^3+2bu+c, au^3+bu^2+cu+d),$$

with $|u| \leq 1/2$, thus, using that $t \geq \sqrt[4]{3}/\sqrt{2}$, we also have

$$u \begin{bmatrix} t^{-1} & \\ & t \end{bmatrix} \lambda B \supset \{(a,b,c,d) \in V_{\mathbb{R}} : |a| \leq 2\frac{\lambda}{t^3}, |b| \leq 2\frac{\lambda}{t}, |c| \leq 2\lambda t, |d| \leq 2\lambda t^3, |Disc(a,b,c,d)| \geq \lambda^4\},$$

as claimed. □

This gives us the following lower bound on $P(u,t,\lambda)$:

Corollary 8.3.4.

$$P(u,t,\lambda) \gg \#\{(a,b,c,d) \in \mathcal{U}' \cap V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}^{irr} : |a| \leq 2\frac{\lambda}{t^3}, |b| \leq 2\frac{\lambda}{t}, |c| \leq 2\lambda t, |d| \leq 2\lambda t^3, |Disc(a,b,c,d)| \geq \lambda^4\}.$$

It is now time to make this choice that might seem very arbitrary but is motivated by what we did in Chapter 8, that is we let $a = 1$ and $c = 0$. Note this is not exactly the same choice as in Chapter 8 but the sieve will be the same since

$$Disc(1,b,0,-d) = Disc(1,2b,b^2,d) = d\left(4b^3 - 27d\right),$$

and thus we will be able to use the result from Section 8.2.

Note that we purposely did not take the exact same choice as in Chapter 8 since it would be making the discriminant smaller than λ^4, which we don't want.

So let's do this, taking $a = 1$ and $c = 0$, we have

$$P(u,t,\lambda) \gg \#\{(b,d) \in \mathbb{Z}^2 : \frac{\lambda}{t} \leq |b| \leq \lambda t^3 \leq 2\frac{\lambda}{t}, |d| \leq 2\lambda t^3 \text{ and } (1,b,0,-d) \in \mathcal{U}' \cap V_{\mathbb{R}}^{(i)} \cap V_{\mathbb{Z}}^{irr} \text{ and } |Disc(1,b,0,-d)| \geq \lambda^4\} \tag{8.3}$$

As it will make things look a little nicer, let $A = \frac{\lambda}{t} \asymp \lambda^{4\delta}$ and $\gamma = \frac{1-3\delta}{\delta}$ so that

$$\frac{\lambda}{t} \leq |b| \leq \lambda t^3 \leq 2\frac{\lambda}{t} \text{ and } |d| \leq 2\lambda t^3 \implies |b| \asymp A \text{ and } |d| \asymp A^{\gamma}.$$

The following two lemmas would give a lower bound for $P(u,t,\lambda)$ if we could ignore the irreducibility condition.

Lemma 8.3.5. *For λ big enough, we have*

$$\#\{(b,d) \in \mathbb{Z}^2 : \frac{\lambda}{t} \leq b \leq 2\frac{\lambda}{t}, \lambda t^3 \leq d \leq 2\lambda t^3 \text{ and } (1,b,0,-d) \in V_{\mathbb{R}}^{(i)} \text{ and } |Disc(1,b,0,-d)| \geq \lambda^4$$

$$\text{and } Disc(1,b,0,-d) \text{ is almost square free } \} \gg A^{\gamma+1}$$

or equivalently

$$\#\{(b,d) \in \mathbb{Z}^2 : \frac{\lambda}{t} \leq b \leq 2\frac{\lambda}{t}, \lambda t^3 \leq d \leq 2\lambda t^3 \text{ and } (1,b,0,-d) \in V_{\mathbb{R}}^{(i)} \text{ and } |Disc(1,b,0,-d)| \geq \lambda^4$$

$$\text{and } Disc(1,b,0,-d) \text{ is almost square free } \} \gg \lambda^{4(1-2\delta)}.$$

Proof. If $\frac{\lambda}{t} \leq |b| \leq 2\frac{\lambda}{t}$ and $\lambda t^3 \leq |d| \leq 2\lambda t^3$, then

$$|Disc(1,b,0,-d)| = |d\left(4b^3 - 27d\right)| \geq 4\lambda^4 + O(\lambda^2 t^6)$$

and since $t \asymp \lambda^{1-4\delta}$ and $\delta > 1/6$, the error term is $o(\lambda^4)$, so for λ big enough,

$$|Disc(1,b,0,-d)| \geq \lambda^4.$$

So we can get rid of the condition that discriminant is at least λ^4 and thus it remains to show that

$$\#\{(b,d) \in \mathbb{Z}^2 : \frac{\lambda}{t} \leq |b| \leq 2\frac{\lambda}{t}, \lambda t^3 \leq |d| \leq 2\lambda t^3 \text{ and } (1,b,0,-d) \in V_{\mathbb{R}}^{(i)}$$

$$\text{and } Disc(1,b,0,-d) \text{ is almost square free } \} \gg A^{\gamma+1},$$

which plugging in $t \asymp \lambda^{1-4\delta}$ to simplify the above, we want to show what

$$\#\{(b,d) \in \mathbb{Z}^2 : |b| \asymp A, |d| \asymp A^\gamma \text{ and } (1,b,0,-d) \in V_{\mathbb{R}}^{(i)} \text{ and } Disc(1,b,0,-d) \text{ is almost square free } \} \gg A^{\gamma+1}.$$

The condition $(1,b,0,-d) \in V_{\mathbb{R}}^{(i)}$ means its discriminant is positive (resp. negative) if $i = 1$ (resp. $i = 2$), and we can control the sign of the discriminant by changing the sign of d, for example.

It is then enough to show that

$$\#\{(b,d) \in \mathbb{Z}^2 : b \approx A, d \approx A^\gamma \text{ and } d(4b^3 - 27d) \text{ is almost square free } \} \gg A^{\gamma+1}, \tag{8.4}$$

where what we mean by $\approx$ is, just like in Section 8.2, $n \approx X$ if $r_1 X \leq n < r_2 X$, where r_1, r_2 are either both positive or both negative. But we saw in Section 8.2, Proposition 8.2.4, that for a big number A, and $\gamma \in (1,3)$, we have

$$\#\{n_1 \asymp A^\gamma, n_2 \asymp A : n_1(n_2^3 - n_1) \text{ is square free}\} \gg A^{\gamma+1},$$

which proves (8.4) since we may take $b = 3n_2$ and $d = 4n_1$. □

And finally, the following lemma enables us to "ignore" the irreducibility condition:

Lemma 8.3.6. *For a big integer A, we have*

$$R := \#\{b \asymp A, d \asymp A^\gamma : (1,b,0,-d) \text{ is reducible}\} \ll A^{1+\gamma/2}.$$

Proof. $(1,b,0,-d)$ corresponds to the binary cubic form $x^3 + bx^2y - dy^3$. If it is reducible, then for some B, C, D, we have

$$\begin{aligned} x^3 + bx^2y - dy^3 &= (x^2 + Bxy + Cy^2)(x + Dy) \\ &= x^3 + (D+B)x^2y + (DB + C)xy^2 + (DC)y^3 \end{aligned}$$

so we can write

$$\begin{aligned} R &= \#\{(B,C,D) : D+B \asymp A, DB+C=0, -DC \asymp A^\gamma\} \\ &= \#\{(B,D) : D+B \asymp A, D^2B \asymp A^\gamma\} \\ &= \sum_{E \asymp A} \#\{D : D^2(E-D) \asymp A^\gamma\}, \end{aligned}$$

where the last line is obtained by the change of variable $E = D+B$. Now if $D \neq E$, then $|D^2(E-D)| \geq D^2$, thus

$$\begin{aligned} R &\ll \sum_{E \asymp A} \left(1 + \#\{D : D^2 \ll A^\gamma\}\right) \\ &\ll A^{1+\gamma/2}. \end{aligned}$$

□

To sum this up, by the above lemmas, the integrand in (8.2) is $\gg_\delta \lambda^{4(1-2\delta)}$, and thus

$$\begin{aligned} N(S'_\delta \cap \mathcal{U}' \cap V_{\mathbb{Z}}^{(i)}; X) &\gg \int_{\lambda \asymp X^{1/4}/\gamma} \int_{t \asymp \lambda^{1-4\delta}} \int_{N"(t)} P(u,t,\lambda,X) t^{-2} dn d^\times t dk d^\times \lambda \\ &\gg \int_{\lambda \asymp X^{1/4}} \int_{t \asymp \lambda^{1-4\delta}} \int_{N"(t)} \lambda^{4(1-2\delta)} t^{-2} dn d^\times t dk d^\times \lambda \\ &\asymp X^{1/2}. \end{aligned}$$

Bibliography

[1] Manjul Bhargava. Higher composition laws ii: On cubic analogues of gauss composition. *Annals of mathematics*, 159(2):865–886, 2004.

[2] Manjul Bhargava. Higher composition laws iii: The parametrization of quartic rings. *Annals of mathematics*, pages 1329–1360, 2004.

[3] Manjul Bhargava. The density of discriminants of quartic rings and fields. *Annals of Mathematics*, pages 1031–1063, 2005.

[4] Manjul Bhargava. Higher composition laws iv: The parametrization of quintic rings. *Annals of Mathematics*, pages 53–94, 2008.

[5] Manjul Bhargava. The density of discriminants of quintic rings and fields. *Annals of mathematics*, pages 1559–1591, 2010.

[6] Manjul Bhargava and Piper Harron. The equidistribution of lattice shapes of rings of integers in cubic, quartic, and quintic number fields. *Compositio Mathematica*, 152(6):11111120, 2016.

[7] Manjul Bhargava, Arul Shankar, Takashi Taniguchi, Frank Thorne, Jacob Tsimerman, and Yongqiang Zhao. Bounds on 2-torsion in class groups of number fields and integral points on elliptic curves. *arXiv preprint arXiv:1701.02458*, 2017.

[8] Manjul Bhargava, Arul Shankar, and Jacob Tsimerman. On the davenport–heilbronn theorems and second order terms. *Inventiones mathematicae*, 193(2):439–499, 2013.

[9] Johannes Franciscus Brakenhoff et al. *Counting problems for number rings*. PhD thesis, Mathematical Institute, Faculty of Science, Leiden University, 2009.

[10] H. Davenport. On a principle of lipschitz. *Journal of the London Mathematical Society*, s1-26(3):179–183, 1951.

[11] Jin Nakagawa. *Orders of a quartic field*, volume 583. American Mathematical Soc., 1996.

[12] Arul Shankar and Jacob Tsimerman. Counting s_5-fields with a power saving error term. In *Forum of Mathematics, Sigma*, volume 2. Cambridge University Press, 2014.